



Linux System Recovery Guide

Version 8.2

STORIX[®]
S O F T W A R E

Trademarks and Copyrights

© Copyright Storix, Inc. 1999-2018

SBAdmin is a registered trademark of Storix, Inc.

SBAdmin is a trademark of Storix, Inc in the USA and other countries

Intel is a registered trademark of Intel, Inc.

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.

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 Kneschke, 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

Storix 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. Storix 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. Introduction	7
When to Use this Guide	7
Terminology	7
System and Program Requirements	8
Kernel Support Requirements	8
System Memory	9
UEFI Firmware Support Requirements	9
Programs for Creating and Writing Bootable CDROMs	9
The Device Filesystem (Devfs)	9
Boot Loaders	10
Initial Ramdisk (initrd/initramfs) Support	10
2. Creating System Recovery Boot Media	11
When to Create Boot Media	11
When You Should Create New Boot Media	11
Creating System Installation Boot Media	11
CDROM image	12
Tape	13
Hard Disk	14
Network	14
Customizing the Boot Media	16
Select SCSI Modules	16
Network Modules	17
Boot console device	18
Kernel Release Level	19
No-prompt Installation	19
Enabling Remote Installation Manager	20
Configuring RIM when Creating Boot Media	20
Configuring RIM after Booting from the Boot Media	21
Connecting to the Remote Install Process	21
3. Network Boot/Install Configuration	23
Understanding Network Boot and Network Installation	23
Enable/Disable Client for Network Boot/Install	23
Disable a Network Install Client	26
Using an Alternate Network to Restore the Data	26
Using a Different Install Server than the Boot Server	26
Using the Same Boot Server to Install Different Linux Versions	27
Updating Network Boot Images	28
4. Booting to the System Installation Process	29
Booting the Various System Types	29
Booting to the System Installation Process	29
CDROM or Tape	29
Hard Disk	29
Network Boot	30
Tape Boot	32
Completing the Boot Process	33
Troubleshooting a Network Boot	34
Determining the Network Adapter Hardware Address	35
5. Reinstall from a System Backup	36
Cloning Systems	36
Installing onto UEFI-Based Firmware Systems	36

No-Prompt Installation.....	36
Installing from an Encrypted Backup	37
Enter a HEX Key	38
Enter an ASCII (text) Key	38
System Installation Process	38
After booting from a network boot server.....	38
Verifying the hardware configuration	38
The System Installation and Maintenance Menu	39
Using Keys and Getting Help	39
Select Installation Device/Backup	40
Select Local Tape Device Drives(s).....	40
Select Local Disk Backup.....	42
Install From Local NFS Mount	43
NFS Considerations	44
Set or Change Network Configuration	44
Select Remote Tape Device	45
Select Remote Disk Backup	45
TSM Configuration	46
TSM Client Configuration	48
TSM Server Configuration.....	48
TSM Administrator Configuration.....	48
Change the Installation Settings.....	48
Install the System with Current Settings	48
6. View/Change Installation Settings	50
Select Disks to Use for Installation	50
View/Change Partition Table	51
Assign All Contents of a Disk to a Different Disk	53
Migrate a Partition to a Different Disk	53
Select Not to Restore Data to a Disk	53
Change Partition Tables.....	53
Logical Volume Management	54
Add or Remove Physical Volumes.....	55
Add or Change Volume Groups.....	55
Add or Change Logical Volumes	57
Add or Change Meta-disks	59
RAID 0+1	61
Add or Change Filesystems	61
External Journals	63
Minimum Filesystem Size versus Device Size	63
Add or Change Swap Devices.....	64
Change Boot Options.....	64
7. Install the System	66
Verification Process	66
Starting the Installation	67
Configuration Files	67
Making the System Bootable.....	67
The Boot Loader	67
Initial Ramdisk Image.....	68
The /boot filesystem	68
Doing it yourself	69
Installation Errors.....	70
System Boot Problems.....	70
Network Re-configuration (avoiding conflicts).....	70
8. System Recovery Utilities	72
Load Additional Device Adapter Modules	72
Start a Maintenance Shell	73

Configure Remote Install Manager	74
Configure Backup Group ID	75
Index	76

1. Introduction

The [SBAdmin for Linux System Recovery Guide](#) is a supplement to the [SBAdmin User Guide](#), providing details on reinstalling a Linux system from a **SBAdmin System Backup**. Note that a System Backup is not limited to reinstalling the same system from which it was made, but it may also be used to “clone” the original system onto different systems containing the same or different hardware.

When to Use this Guide

This guide provides instructions for booting and reinstalling a system from a SBAdmin System Backup. This document should be reviewed after first installing the software to become familiar with this process and its requirements BEFORE a system recovery is required.

Installation from a System Backup is fairly intuitive, but there is information and steps that must be taken to be prepared in the event that a system re-installation is required. The System Backup contains all of the backup data and the information needed to recreate the system and restore the data. To access the System Installation Process, boot media must first be created. This may be either a bootable CDROM, network boot image, system backup disk, or tape (for systems which support tape boot).

This guide will refer to information found in the [SBAdmin User Guide](#). When doing so, the reference term or section will be shown in [Blue Text](#). If you need to refer to that information in the [SBAdmin User Guide](#), highlighted sections (**in bold**) can be found in the [Table of Contents](#), and other terms can be found in the [Index](#).

Terminology

The system recovery process is straight-forward and provides instruction and help screens to guide you through the process. Even when creating and changing devices, filesystems, partition maps, logical volumes, etc, the information provided should make the process fairly intuitive. There are a few terms you should understand before beginning this process:

- **Linux kernel:** This is the first “program” that gets executed when your Linux system starts. It is considered the “base operating system” from which all other processes are run. Various kernels provide support for different types of hardware and software devices and filesystem types.
- **Kernel modules:** These are individual programs providing support for various devices and filesystems. If the modules are compiled into the kernel, they are considered “built-in”. Otherwise, they are compiled into binary programs outside of the kernel (but may only be executed by the kernel) and are just referred to as “**modules**”. These are placed in a specific directory where the kernel knows where to find them. This directory is `/lib/modules/kernel-name`, where **kernel-name** is the name of your kernel. The kernel “name” is compiled into the kernel, and usually includes the kernel release level and an optional suffix, often referring to the Linux distribution (i.e. “`/lib/modules/2.4.18mdk`”). You can query the kernel name on your system by typing “`uname -r`” at the command line.
- **Boot Loader:** This is a program that exists on the boot disk or CDROM that is used to find and execute the Linux kernel. It usually will install an initial filesystem in memory, and execute programs within to load device modules needed to access the root (`/`) filesystem. The boot loader depends on the *firmware* of the system, since the firmware must know how to load and execute the boot loader.
- **Firmware:** The firmware of a machine is a mini-operating system that is used to detect available boot devices (disks, CDs, tapes or network adapters) and load and execute the “real” operating system. The following table shows the system firmware supported by SBAdmin:

Firmware	Supported Systems	Boot Media Types	Boot loaders
BIOS	Intel-based (32-bit, AMD64 and EM64T)	Disk, CDROM, network	LILLO, GRUB, GRUB2
OpenFirmware (IEEE-1275 Standard)	IBM POWER, System p and System i (CHRP-based systems)	Disk, tape, CDROM, network, tape	Yaboot
UEFI	64-bit Intel-based (x86_64)	Disk, CDROM, network	ELILO

The firmware typically reads a *boot loader* from the boot media, which must be written in a manner that the firmware understands how to find. The boot loader is an additional program that is designed to read and execute the Linux kernel, providing it information needed to configure additional devices, etc.

- **LVM:** This is **Logical Volume Management**, and provides the ability to create devices similar to “software partitions”, that are easily resizable, relocatable, and provide optional data striping (RAID 0) for enhanced performance. LVM is supported by most Linux distributions today. If it is available on your system it will be automatically included on the SBAAdmin boot media even if you are not using it. This allows you to implement LVM during the install process if you are not already doing so.
- **Metadisks:** Also referred to as “multi-disks”, this is a form of “software RAID” that provides different RAID types, such as striping (RAID 0), mirroring (RAID 1), striping with parity (RAID 4), striping with striped parity (RAID 5), striping with double striped parity (RAID 6), and striping of mirrors (RAID 10). It also provides the ability to combine devices into a single sequential device they refer to as “linear” RAID. Meta-disk, or “md” devices are supported by most Linux distributions. If available on your system it will be automatically included on the SBAAdmin boot media even if you are not using it. This allows you to implement meta-disk devices if you are not already doing so.
- **Filesystems:** There are numerous filesystem types available on Linux. Different Linux distributions automatically provide support for different filesystems, and others may be added to the kernel or compiled as modules. Others not included in the distribution may usually be found on the internet, downloaded and built into the kernel. SBAAdmin supports most popular filesystem types, including **ext2**, **ext3**, **ext4**, **ReiserFS**, **JFS**, **XFS**, **Minix**, **MSDOS** (3.1) and **Vfat** (win95 and later). Filesystems build on ext2, for instance, may be changed to a JFS filesystem during the system recovery process, providing simple conversion to more robust filesystems.

System and Program Requirements

Every Linux distribution is different, and this poses certain challenges since SBAAdmin must depend on some common programs or support to be installed on your system. The requirements are few, and most Linux distributions provide the base support by default, or as an optional package. This section describes requirements of SBAAdmin that differ most commonly between distributions.

Kernel Support Requirements

To be able to boot from the SBAAdmin boot media (or most any media), you must have **RAM disk support and Initial RAM disk support built into the kernel**. Also, the process of creating the media uses either RAM disks or loopback devices. If your RAM disk driver is only configured to support the default of 4 MB, then **the loopback device support** will also be required (may be compiled as a module). Refer to your documentation for rebuilding the kernel or adding kernel modules. We recommend the following settings:

Block Devices:

Loopback device support:	Module
RAM disk support:	Built into kernel
Default RAM disk size:	32768 (This will allow up to a 32MB ramdisk to be created)
Initial RAM disk (initrd) support:	Built into kernel

System Memory

The SBAAdmin System Installation process requires that the system have at least 64 MB of memory to operate, although a minimum of 256 MB is recommended.

UEFI Firmware Support Requirements

Performing recovery to a system that boots from UEFI firmware requires that you boot from UEFI firmware using SBAAdmin boot media, and then restore from a backup that supports UEFI firmware. SBAAdmin determines that a system has support for UEFI firmware based on the following requirements:

UEFI Support Requirements:

- x86_64 systems (output of `uname -m` command)
- 2.6.21 kernel level or later (output of `uname -r` command)
- CONFIG_EFI support enabled in kernel (typically found in `/boot/config-RELEASE`)
- Support for creating VFAT filesystem (`mkfs.vfat` command)

Programs for Creating and Writing Bootable CDRoms

The program “**mkisofs**” or “**genisofs**” is a free program that must exist on the system from which you will create the bootable CDRom. This program is included on most distributions but may not be installed by default. If you receive a message that this program is missing, you will need to install it from your distribution media or download a copy from the internet. This program will be used to generate the “ISO” image, which is a CDRom format compatible with many operating systems.

To create a bootable CDRom, this software will generate the CDRom image file. It is then up to you to copy that image to a CD Writer device using your own CD Writer software. On most Linux systems, the “**cdrecord**” program exists. If not, then you can usually install it from your distribution media or download a copy from the internet. You will need to refer to the instructions or “man” pages that accompany that program. If you choose any other program to copy the CDRom image to the CD Writer, then you must be sure to specify, if necessary, that this is an **ISO** image.

The Device Filesystem (Devfs)

The **Device Filesystem** is a function implemented on some Linux systems for management of devices. It has, however, been replaced in more recent Linux distributions by **Udev**. Devfs is not a requirement of SBAAdmin, but its existence or use can pose certain problems, so it deserves mention here. Its function is to provide a consistent naming convention for devices based on their physical location, rather than allowing the system to name the devices (possibly differently) each time the system is booted based on their order of detection.

Unfortunately, this presents many problems for products designed to work with the “classic” Linux device naming conventions, and also creates quite lengthy filenames and symbolic links between old and new names that are more difficult to manage. A classic partition name such as “**/dev/hda1**”, for example, will be named “**/dev/ide/host0/bus0/target0/lun0/part1**” under Devfs. Devfs often creates another link to this file “**/dev/hd/c0b0t0u0p1**”.

SBAAdmin must be able to scan for devices on the system, and does so by looking for devices of the classic Linux convention, as this is most widely used. To look also for Devfs filenames would probably result in detecting the same physical devices under multiple different names, so SBAAdmin will only recognize devices by the known “classic” device names.

The product will work quite well on systems with Devfs implemented as long as the system maintains the classic device naming conventions as well. This is the default for most Linux implementations using Devfs. All functions of the product will work the same on a Devfs system as for those not using Devfs, but all references to disks, partitions and tape devices will use the classic names. SBAdmin also attempts to cross-reference the devfs names to the classic names whenever the system configuration files use the devfs names (as occurs automatically when some Linux distros are installed). System configuration files which may use either devfs or classic names include:

- **/etc/fstab** – Filesystem definitions
- **/etc/raidtab** – Software RAID device definitions
- **/etc/mtab** – Mounted filesystem table (automatically updated by the system)

To avoid any potential problems if you are using Devfs, you should make sure these files reference the classic disk and partition names, such as **/dev/sda** (first SCSI disk) and **/dev/hdc3** (third partition on the third IDE disk) whenever possible. If you attempt to perform a **System Backup** with SBAdmin and are informed that the root filesystem, or any other filesystem, is either not found or not mounted, then SBAdmin may have been unable to determine the devfs names, and you probably need to put the classic names in the **/etc/fstab** file.

Boot Loaders

SBAdmin will attempt to determine which boot loader the system is currently using when performing a system backup. If the backup process is unable to determine the boot loader used, the backup will fail.

Initial Ramdisk (initrd/initramfs) Support

One of the most difficult issues with any system recovery product is trying to figure out how to make the system bootable. The configuration files restored from the backup may no longer be applicable if changes to the hardware or storage configuration have been made. After a SBAdmin System Installation is completed, the boot loader is configured to make the system bootable based on that kernel and the root filesystem. This is often not enough information to make everything available at system startup that is required. For example, if your root filesystem resides on a SCSI disk, and the SCSI adapter support is not built into your kernel, then your system probably loads an **Initial Ram Disk (initrd/initramfs)** containing the SCSI adapter support, which allows the adapter to be configured before attempting to mount the root filesystem. SBAdmin will determine if an initrd is necessary and create one automatically. If not required, SBAdmin will configure the system to boot from your kernel without an initrd image. If your kernel has built-in support for any devices or filesystems required to mount your root filesystem, you should have no problems. If an initrd image is required, you are given the opportunity at the end of the system recovery process to configure your own boot loader, or modify the boot loader configuration file to handle any potential problems. Note that SBAdmin does not support systems using monolithic kernels (no loadable kernel modules).

More specific information creating an [Initial Ramdisk Image](#) is provided later in this document.

2. Creating System Recovery Boot Media

The SBAAdmin User Interface (either Xwindows GUI or Web Interface) provides a very simple procedure for creating boot media, which is described in this section. This interface may be used to create bootable **tapes**, boot **CDROM** images, **network boot** images, or can configure a local **hard disk** to boot to the system recovery process. This interface may create any of the boot media types. Also refer to the **stmakeboot** command in the [Commands Reference](#), which may be run on any client to make bootable media directly from that system. All media types will boot the target system into the same recovery menus.

When to Create Boot Media

It is generally a good idea to create bootable media for each individual system that is backed up using SBAAdmin. This is because most systems do not run under the same Linux kernel level, have the same device support installed and configured, and have the same software level of various device support and other applications installed.

If you attempt to boot from media created using one Linux kernel version (i.e. "2.4"), then attempt to install the system from a backup that was running under a version 2.6 kernel, you may run into problems during or after the installation completes. This is because the devices and filesystems created during the system recovery will be later accessed by a different Linux kernel version that may not be compatible or provide the proper support. For this reason, the SBAAdmin Installation process provides strong warnings if you boot from a different kernel than was running at the time the backup was created. The installation process also verifies that your boot media contains the device and filesystem support that is required to install the system, based on those devices or filesystems that were in use at the time of the backup. If the support is not provided by the bootable media, you will be required to remove or change those devices or filesystems that are not supported.

If you have multiple systems, all running the same kernel level (but not necessary the exact same kernel), it is generally safe to use the same boot media to boot and install different systems. Because the boot media is *probably the most important boot media you will ever need*, it is a good idea to keep at least one spare or create boot media of different types.

When You Should Create New Boot Media

1. Any time you update your operating system or compile/install a new kernel. Even if the kernel version does not change, support for built-in devices or filesystems may have been added or removed, and device or filesystem modules may also have been added or removed.
2. Any time you install a new *release level* of **SBAAdmin**. Although we try to maintain compatibility between current and past versions, there may be times when a new feature supported by the backup software also adds new support to the system recovery process. Since the system recovery programs are written to your boot media, you will need to remake the boot media to make sure you are using the latest installation programs.

Creating System Installation Boot Media

To create the boot media, select **Utilities->Create/Manage Boot Media->(CDROM, Network, Hard Disk or Tape Boot Images)** from the menu bar in the administrator main menu. If using a **Network Administrator**, you will be prompted to select the server on which the boot media will be stored, the name of the image to create/update, and the client on which the boot media should be created. Note that the boot media is created on the selected **client**, but may be used to boot other clients of similar system type and operating system release levels.

When selecting A **Linux** client, a screen similar to the following will appear:

Boot Server Name	woody	▼
CDROM Boot Image Name	sles112_x64	▼
Client System Information		
Client Name	stitch	Linux
Kernel Release Level	3.0.13-0.27-default	
Platform Type	i386	x86_64
UEFI Boot Support	<input checked="" type="radio"/> Yes <input type="radio"/> No	
User Description	SLES 11.2 x86_64 boot media	Clear
Kernel Modules to Load Automatically		
Select SCSI Modules		Select Network Modules
System Installation Mode		
<input type="radio"/> No-Prompt <input type="radio"/> Menus (set defaults) <input checked="" type="radio"/> Menus (no defaults)		
Create/Update	Remove	✖

Remember to use the [QuickHelp](#) (right mouse button) on any button or entry field for details on the use and options for each when using the Graphical User Interface (GUI). When using the Web Interface, utilize the Roll-Over Help for details.

Creation of each media type is described separately:

CDROM image

This process will make a CDROM ISO image, but will not actually burn the image to the CDROM. This image may be copied to any system where your CD/RW device resides where you can use any software or program you choose to copy the image to the CDROM. If using the *Network Administrator* you can make the CDROM image for any client you have configured.

To create a bootable CDROM, select [Utilities](#)→[Create/Manage Boot Media](#)→[CDROM Boot Images](#).

Boot Server Name	woody	▼
CDROM Boot Image Name	sles112_x64	▼
Client System Information		
Client Name	stitch	Linux
Kernel Release Level	3.0.13-0.27-default	
Platform Type	i386	x86_64
UEFI Boot Support	<input checked="" type="radio"/> Yes <input type="radio"/> No	
User Description	SLES 11.2 x86_64 boot media	Clear
Kernel Modules to Load Automatically		
Select SCSI Modules		Select Network Modules
System Installation Mode		
<input type="radio"/> No-Prompt <input type="radio"/> Menus (set defaults) <input checked="" type="radio"/> Menus (no defaults)		
Create/Update	Remove	✖



NOTE When using Workstation Edition, you will not be prompted for the Client and Boot Server Name.

Using *Network Administrator* a minimum of three fields are required [Boot Server name](#), [CDROM Boot Image Name](#), and [Client Name](#).

The [Boot Server name](#) is the name of the server the boot media will be stored on. Use the drop down arrow to select a configured server. The boot media will be created using the selected client, but will be copied to "Client Directory for CDROM & Network Boot Images" directory as configured on the selected boot server. You may also select "Store On Client" to keep the image on the client rather than send it to a server.

The [CDROM Boot Image Name](#) is the name of the image as it will be stored on the filesystem. For clarity you may choose to name the image to reflect the hostname or operating system level of the client. Further details about the image can be saved in the [User Description](#) field and can be viewed when managing boot media through the SBAAdmin interface.

The [Client Name](#) is selected with the drop down menu to the right of the field. This is the client used to create the boot media. The client's [Kernel Release Level](#) and [Platform Type](#) will automatically be populated into the appropriate fields.

The [UEFI Boot Support](#) will be enabled if the client has [support for UEFI](#). The boot media will always support booting from BIOS firmware. However, if you wish to create the CDROM boot media with support for booting from both BIOS and UEFI firmware, then select "Yes".

Boot media is not specific to this client, and can be used to perform recovery from backups of similar systems running the same Linux distribution and update level.

When this process is complete, you may copy this image to a system containing the CD writer device, if there is no CD burner on the Boot Server.

Tape

A bootable tape may be created for any hardware platform that supports tape boot. Currently, only the *IBM PowerLinux (POWER, System p) and System i systems* are capable of booting from a tape drive. To create the boot tape, you need only insert the tape into the drive, and the boot images will be written to the start of the tape. Note that any other data on the tape will not be readable after making the tape bootable.

To create a bootable tape, select [Utilities](#)→[Create System Installation Boot Media](#)→[Tape Boot Media](#).

Tape Server Name	woody	
Tape Drive Name	st0	
Client System Information		
Client Name	grumpy	
Kernel Release Level	2.6.16.21-0.8-ppc64	
Platform Type	ppc	
Kernel Modules to Load Automatically		
Select SCSI Modules	Select Network Modules	
System Installation Mode		
<input type="radio"/> No-Prompt	<input type="radio"/> Menus (set defaults)	<input checked="" type="radio"/> Menus (no defaults)
Create/Update		X

For systems which support booting from tape, the tape will automatically be made bootable when you create a [System Backup](#) to the start of the tape. You can stack additional System Backups to the tape, but no further boot images will be written since they must be at the start of the tape.

If using a *Network Administrator*, select the [Server Name](#), the [Tape Drive Name](#), and the [Client Name](#).

To boot from the tape, you must have the tape in the drive, and select to boot from the tape device within the system firmware (*OpenFirmware* on *IBM System p and System i* hardware). After booting from a

bootable system backup, the tape will be the default install device, and you can continue the system installation from the same tape without a need to select any other options.

Hard Disk

If you configured a disk as a **Local System Backup Disk** (see [SBAdmin User Guide](#)), then this disk (or disks) can also be made bootable to boot directly to the system recovery process. This allows you to perform your system backups to a local (or SAN-attached/portable) disk, then boot and reinstall the system from that same disk with no need for other backup media.



Using this option will not change how the system boots by default. After configuring a disk to boot to the SBAdmin System Install process, you must select to boot from that disk from within your system firmware boot menus.

To create a bootable disk, select [Utilities→Create System Installation Boot Media→Hard Disk Boot Media](#).

The screenshot shows a configuration window for creating a bootable disk. At the top, there are two dropdown menus: 'Client Name' with the value 'stitch' and 'Hard Disk Name' with the value 'sdc'. Below these are three sections with red headers: 'Client System Information' containing 'Kernel Release Level' (3.0.13-0.27-default), 'Platform Type' (i386), and 'UEFI Boot Support' (radio buttons for Yes and No, with 'Yes' selected); 'Kernel Modules to Load Automatically' containing two buttons: 'Select SCSI Modules' and 'Select Network Modules'; and 'System Installation Mode' containing three radio buttons: 'No-Prompt', 'Menus (set defaults)', and 'Menus (no defaults)', with 'Menus (no defaults)' selected. At the bottom left is a 'Create/Update' button, and at the bottom right is a red 'X' icon.

Select the [Client Name](#) to configure using the drop down arrow to the right. Next, select the disk to configure in the [Hard Disk Name](#) field by using the arrow to the right of the entry field. When pressing the arrow, the system will be queried to find one or more disks that were configured as a **Local System Backup Disk**. If no disks are listed, then none were configured for system backup/recovery. The [UEFI Boot Support](#) option will be selected based on how the disk was originally configured and cannot be changed.

Network

Use this option to create a **network boot image** to be used with various *network boot loaders* to boot a client system over the network from a *network boot server*.

To create a network boot image on any configured client or server and save the image on the boot server, select either:

[Configure→Network Boot/Install→Create/Update a Network Boot Image](#) or
[Utilities→Create System Installation Boot Media→Network Boot Images](#)

Select the [Boot Server Name](#). This is the server on which the network boot image will be stored after it is created. The network boot server may be the same system from which the network boot image is created.

Next, type the name of the boot image in the [Network Boot Image Name](#) field or select the name of an existing image to overwrite by pressing the arrow button to the right of the entry field. If you enter a unique name, a new image will be created using that name. Note that the network boot “*image*” actually consists of several files on disk, but will always be referred to within the application as a single image by a unique **boot image name**. The files are copied into the directory specified as the **Client Directory for CDROM & Network Boot Images** directory when the server was configured. You may also use the select button to the right to choose an existing name. The named image will be overwritten.


Finally, select the [Client name](#) for which boot media is to be created using the drop down arrow to the right of the [Client Name](#) field. **Kernel Release Level** and **Platform Type** will be automatically populated with the appropriate information from the client. The [UEFI Boot Support](#) will be enabled if the client has [support for UEFI](#). The boot media will always support booting from BIOS firmware. However, if you wish to create the Network boot images capable of booting from both BIOS and UEFI firmware, then select “Yes”.

Upon successful completion, the network boot image will be created and transferred to the boot server. It will now be possible to configure any client to boot from this image using the option “[Enable/Disable Network Installation of a Client](#)” below.

When all selections are complete, press the [Create/Update](#) button. A new window will appear with the output of the command to create the media and any error message if they should occur, such as in the following example:

```
Creating CDROM Boot Image boot media on host stitch ...
Checking system requirements ...
Generating cdrom boot media for release 3.0.13-0.27-default ...
Using kernel file: /boot/efi/efi/SuSE/vmlinuz-3.0.13-0.27-default
Supported boot firmware: BIOS UEFI
Creating filelist ...
Creating initramfs image ...
Verifying contents of initramfs image ...
Configuring ELILO bootloader ...
Configuring GRUB bootloader ...
Creating CDROM ISO image ...
Verifying contents of CDROM ISO image ...
Moving CDROM ISO to server woody.storix ...

Bootable CDROM ISO image "sles112_x64.iso" has been created successfully and
moved to the /backups/netboot directory on server "woody.storix". You may now
use a CD writing program such as "cdrrecord" to burn the image to CDROM media.
```

Print/Send 

Customizing the Boot Media

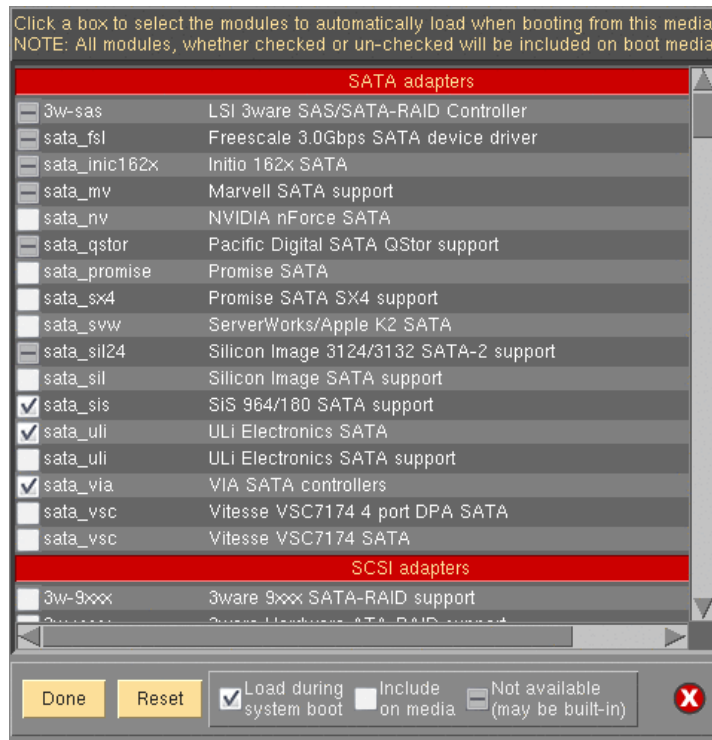
There are a number of options when configuring boot media, which may be used to boot the system on different systems and allow it to recognize different types of devices. Refer to the [Create Linux System Installation Boot Media](#) screen. The options specific to each boot media type are defined above. Each option for customizing the boot media is described below:

Select SCSI Modules

SBAAdmin boot media created from most 2.6 kernel distributions should be able to detect and automatically load all necessary modules/drivers to perform the recovery to the same or dissimilar hardware. However, in those instances where the detection is not possible you may select which specific SCSI adapter or Fibre Channel Host Bus Adapter (HBA) support should be automatically loaded when booting from the media. If there are devices (i.e. disk or tape) attached to an adapter of a selected type, those devices will be made available automatically.

All SCSI and HBA support (if included) will be available on the boot media. Therefore, even if the desired adapter support is not loaded automatically when booting from the media, it may be loaded at a later time from the [System Installation Menus](#) (see [Loading Additional Device Support](#)).

To select which SCSI or HBA modules will be automatically loaded on system boot, press the **Select SCSI Modules** button. By default, SBAAdmin will automatically load only the modules which are currently loaded on the client system. Those adapters, if any, will be automatically selected on the screen which appears, similar to the following:



Modules with a **dash** are defined in the configuration file, but do not exist on the system, and therefore cannot be selected or de-selected. Those with a **checkmark** are currently selected and will be loaded on system boot. Lines with an **empty box** indicate those available on the system that will be included on the boot media, but not automatically loaded on boot. To select or de-select a module, move the cursor over the box and press the left mouse button.

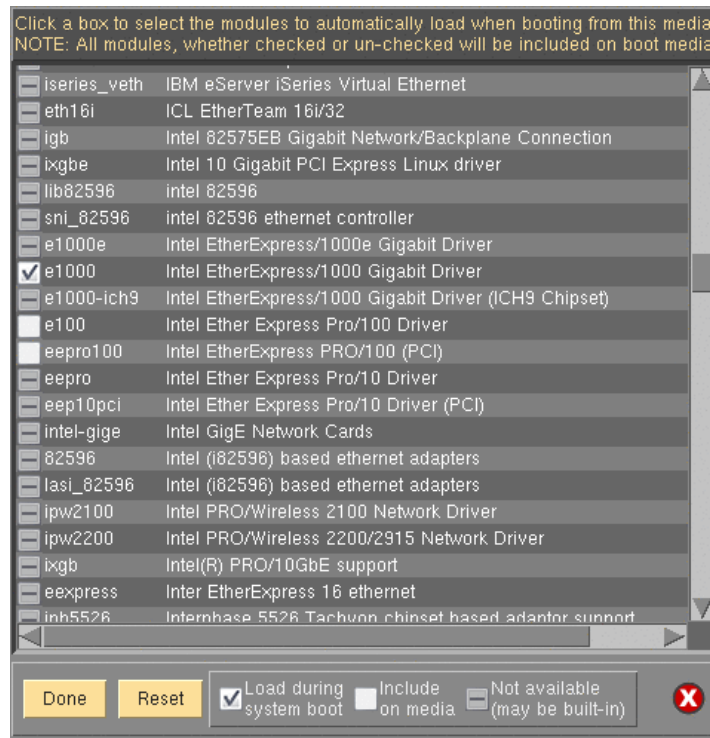
When finished with selections, press the **Done** button. The **Reset** button may be used if you wish to revert back to the original configuration file distributed with the software. If you wish to cancel only the changes made in this session, press the **Cancel** button on the far right.

Network Modules

SBAAdmin boot media created from most 2.6 kernel distributions should be able to detect and automatically load all necessary modules/drivers to perform the recovery to the same or dissimilar hardware. However, in those instances where the detection is not possible, you may wish to manually select the network module support to automatically load on the boot media. Select or de-select them by pressing the **Select Network Modules** button. By default, SBAAdmin will include all network modules available for the selected kernel release level. Only modules that are selected will be loaded automatically. It is not recommended to automatically load all network module support as some modules may conflict when they are loaded (often causing the boot process to hang). If a network adapter is detected by one of the loaded modules, a network device will be automatically created.

Again, all network modules on the system the boot media is created from will be available on the boot media. Therefore, even if the desired network adapter support is not loaded automatically when booting from the media, it may be loaded at a later time from the [System Installation Menu](#) (see [Loading Additional Device Support](#)).

To select which network adapter modules will be automatically loaded on system boot, press the **Select Network Modules** button. By default, SBAAdmin will automatically load only the network modules which are currently loaded on the system. Those adapters, if any, will be automatically selected on the screen which appears, similar to the following:



Modules with a **dash** are defined in the configuration file, but do not exist on the system, and therefore cannot be selected or de-selected. Those with a **checkmark** are currently selected and will be loaded on system boot. Lines with an **empty box** indicate those available on the system that will be included on the boot media, but not automatically loaded on boot. To select or de-select a module, move the cursor over the circle and press the left mouse button.

When finished with selections, press the **Done** button. The **Reset** button may be used if you wish to revert back to the original configuration file distributed with the software. If you wish to cancel only the changes made in this session, press the **Cancel** button on the far right.

Boot console device

By default, SBAdmin will create boot media to be displayed on a graphical display directly attached to the system (**tty0**). If you will be using a console other than **tty0**, it is necessary to define the type of console device that will be used.

To define the boot console device you must select either **No-Prompt** or **Menus (set defaults)** as the **Installation Mode**. Use the arrow next to the **Console Device Type** field to list and select a device name. Note the description of each device name.

When using a serial console attached to a serial port, select **ttyS0**. Other types may include **ttyUSB0** (for USB-attached console devices), etc.



The boot media can only be created to boot a particular console type. If you select the wrong type, the boot process will complete, but you may not see the Installation Menus on the screen.

If booting from a serial terminal, the terminal must be connected to the first serial port (S1 or COM1) and must be set to 9600 baud, 8 bits, 1 stop bit and no parity (9600,8,1,NONE).

Kernel Release Level

Your system may be configured with multiple kernels and associated modules. This is typical of a system that is being tested or in the process of upgrading. This process will automatically display the name of the kernel (as provided by the “`uname -r`” command) that the client is currently running under in the [Kernel release level](#) field.

If you wish to create boot media using a kernel release level other than the currently running level, you may do so by using the `stmakeboot` command on the client. Documentation for this command may be found in the [Commands Reference Guide](#).

When you boot from this media, the kernel and modules you will be running under will match those displayed here. Keep in mind that the kernel release level and modules level should also match the level of the [backup that you will be restoring](#).

No-prompt Installation

CDROM and **Network** boot media may be created with the default installation options set, also allowing the system to be installed as soon as a system is booted from this media. This allows an installation to take place simply by booting from a network boot image, for instance, with no operator intervention required.

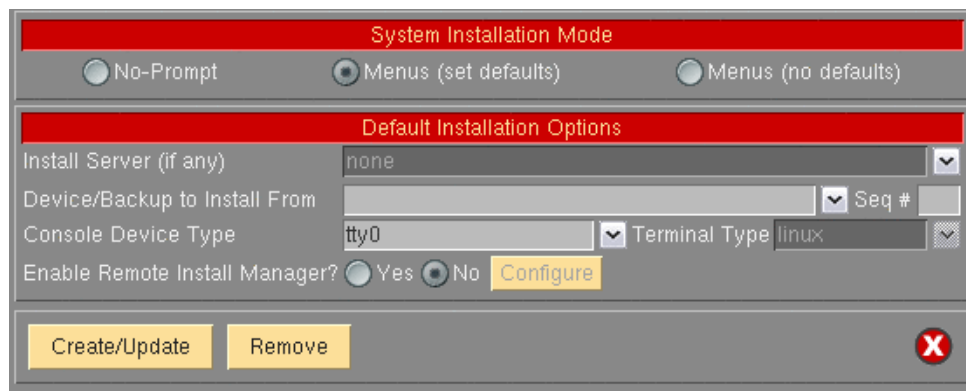
NOTE

Be careful not to leave the CDROM in the drive with the system firmware set to boot from CDROM first, as a no-prompt installation could occur without any user intervention.

Be very careful when using this option, as the user will not have the option of intervening in the system recovery process if the boot media was created for no-prompt installation. The exception, however, is if the defaults are not valid (such as an installation device not being available), or if the backup data will not fit onto the new system’s hardware without some re-configuration. In this case, the installation menus will be presented to allow the user to make the necessary changes.

When creating **CDROM** boot media, the following options are available when using the option to [Create System Installation Media](#). For **Network** boot media, the options are available when selecting to [Enable Network Installation of a Client](#). The reason is that, when creating network boot media, a single network boot image may be used for different client systems, and each client system can be configured with different defaults. Refer to each corresponding section for additional details.

If you select either “**No-prompt**” or “**Menus (set defaults)**” for the [Installation Mode](#), additional information will appear within the window, such as in the following example:



The [Install Server](#) is available only if using a *Network Edition* or *TSM Edition* license. If the client will install from a backup on a local device (ie. Tape or local system backup device), leave this field set to “**none**”. If the system will be installed from a remote server, use the arrow button to the right of this field to select a server name.

When selecting an [Install Server](#) name when [Enabling a Client for Network Boot/Install](#) and the install server differ from the boot server, more information will appear on the screen below this field:

The screenshot shows a window titled "System Installation Mode" with three radio buttons: "No-Prompt", "Menus (set defaults)" (which is selected), and "Menus (no defaults)". Below this is a section titled "Client Default Installation Options". It contains several fields and options: "Server to Install From" is a dropdown menu with "donald" selected; "Alternate Install Server Network" is a dropdown menu with "none" selected; "Gateway Address (optional)" is a text input field; "If boot and install network adapters differ:" is a label; "Client Network Adapter Name" is a dropdown menu; "Client IP Address" is a text input field; "Subnet Mask (optional)" is a text input field; "Device/Backup to Install From" is a dropdown menu with "Seq #" to its right; "Console Device Type" is a dropdown menu with "tty0" selected; "Terminal Type" is a dropdown menu with "linux" selected; "Apply Network Settings to Installed System?" has two radio buttons, "Yes" and "No", with "No" selected; "Enable Remote Install Manager?" has two radio buttons, "Yes" and "No", with "No" selected, and a yellow "Configure" button to its right; "Disable Network Boot After Install?" has two radio buttons, "Yes" and "No", with "No" selected. At the bottom of the window are two yellow buttons: "Enable/Update" and "Disable", and a red "X" button in the bottom right corner.

For the client to be installed from a remote server, you must select the name of the client to be installed (which must be a configured client). Also, the network adapter name (of the client) will be required. Other fields are optional, but may be required for the client to contact the server.

Select the [Alternate Server Network](#) if the server was configured with an alternate server network. In this case, the client will retrieve the backup data from the server using this alternate network. Be sure to select the correct adapter name the client will use to contact the server via its alternate adapter.

Enabling Remote Installation Manager

This feature will allow connection to the SBAAdmin *System Installation Process* from any remote system. With proper authority, a remote user can perform all of the tasks in recovering a system as if they were at the locally attached console. This process may be started from the SBAAdmin interface on a Network Administrator system, or from any SSH client application. Therefore, installation of even a *Workstation Edition* system may be managed remotely.

The remote user will be required to enter a password to access the system installation process. This password may have been defined when the boot media was created or may be defined in the system installation menus after booting from the media.

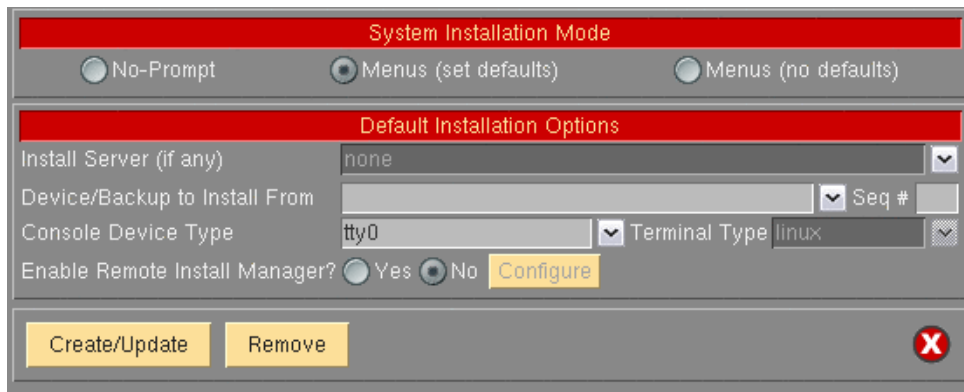
The Remote Install Manager (RIM) may be configured and started in one of two ways:

Configuring RIM when Creating Boot Media

To start RIM automatically when booting a system from SBAAdmin boot media:

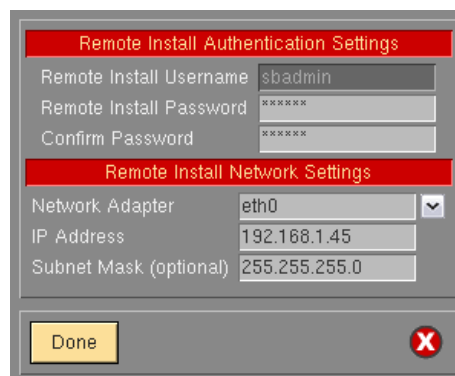
[Utilities](#)→[Create System Installation Media](#)

Select either **Menus (set defaults)** or **No prompt** for the installation mode. The screen will expand to include the following options:



Select "Yes" for **Enable Remote Install Manager**

Select the **Configure** button to the right to configure the settings. You will be presented with the following window:



The **Remote Install Username** is set to "sbadmin" and may not be changed. Enter a password in the **Remote Install Password** field. The password will be necessary to login to the remote install client.

Select the **Network Adapter** that should be configured to connect to the remote install client. If performing a network boot, then you may select **UseBootAdapter** to use the adapter that was used to perform the network boot. If you configured the **Client Network Adapter** on the previous screen, you can select **UseInstallAdapter** to use the same adapter configured for network installation.

Enter the **IP Address** used to configure the network adapter. This field will be disabled if you selected to use either the boot or install adapter, which will already be configured.

Enter the **Subnet Mask** used (if necessary) when configuring the network adapter. This field will be disabled if you select to use either the boot or install adapter.

After pressing **Done**, the settings will be saved in the boot configuration. The adapter will be enabled, and a remote connection (with appropriate password) will be accepted when booting from this media.

Configuring RIM after Booting from the Boot Media

From within the [System Installation Menus](#) select [System Recovery Utilities](#). Then select [Configure Remote Install Manager](#), and follow the instructions for [Configuring Remote Install Manager](#) in the Utilities section.

Connecting to the Remote Install Process

To connect to the remote install client use one of the following:

- a. **SSH** client program (i.e. "**ssh sbadmin@192.168.1.121**"): Note that you will always use the user id "sbadmin" and the password you selected in the previous step. If you do not have an SSH client program, you can use the one installed on the SBAdmin Administrator System. This program is called strimsh (i.e. "**/opt/storix/bin/strimsh sbadmin@192.168.1.121**").

or

Select [Utilities](#)→[Start Remote Install Manager](#) from the *SBAdmin Interface*. A window will appear where you must enter the remote install password:



Select the **Remote Install Client Name** from the drop-down list. The primary IP address of the client will be shown in the **Remote Install Client IP** field. You may change this IP address if you are connecting using a different adapter.

When you press the **Connect** button, a new terminal window will display, and the [System Installation Menus](#) will appear. You can, from this window, perform all system installation and maintenance tasks for the remote client.

3. Network Boot/Install Configuration

The information provided in this section will prepare a client system for network boot and installation from a backup server.

Understanding Network Boot and Network Installation

Any client system defined to the [admin system](#) may be installed or reinstalled from a [System Backup](#). That System Backup will typically reside on the disk or on a tape device attached to a backup server. In order for the client to restore from this backup data, it must first be *booted* over the network from a [boot server](#), and then installed from an [install server](#).

- The **boot server** is used solely to deliver the boot images to the target client. The boot images will provide a basic operating system with which the client will run the remainder of the installation process.
- The **install server** is used only to provide access to the data to be restored. If the backup is on tape, the install server will be the system on which the tape drive is attached. Likewise, if the backup is a disk image file, the disk will be attached to the install server.

Although the boot server and install server are typically the same system, this is not a requirement. If, for instance, there are several systems on which tape drives are attached, the client may be installed from any tape on any system, even though the client is always booted from the same boot server.

The first step is to create a network boot image from the client or any other system running the same level of Linux that you will be installing. The system from which the network boot image is created must also have installed and selected the device support necessary for the target network adapter. To create a network boot image on any system and copy the boot image to the boot server, refer to "[Create System Installation Boot Media - Network](#)".

Enable/Disable Client for Network Boot/Install

This section provides details on configuring a client to be booted and installed from a network **boot server** and/or network **install server**. Although the basic settings are simple, there are optional settings which may be used for more flexibility, such as configuring a [no-prompt installation](#) of the client, or installing (reading the backup data) from a different network adapter than the one the client was booted from.

To setup the client, select the option [Configure→Network Boot/Install→Enable/Disable Network Installation of a Client](#) from the menu bar. You will be prompted for the client to configure. Select the client and press the [Continue](#) button. A screen similar to the following will appear:

Options may appear or disappear from this screen depending on your selections. The screen is broken into two main sections; one for configuring the [Client network boot options](#) and one for configuring the [Client network install options](#). The setting for the **System Installation Mode** towards the bottom of the screen determines whether or not the **Client network install options** section will appear.

The following fields are used to configure the client to boot from a [boot server](#):

1. **Server to Boot From:** If the server in this field is incorrect, use the arrow button to list and select a different server from which to boot from. By default, the boot server is assumed to be the install server as well. However, the [install server](#) may be changed as described later. If updating an image and you choose to change the boot server, the image on the old boot server will be automatically disabled.

If the boot server has been configured with an [Alternate Server Network](#) and you wish to perform the network boot over that network, select the network from the drop-down list.

2. **Boot Image Name:** Use the arrow button to the right of the entry field to select from a list of boot images previously created using the [Create Bootable Installation Media \(Network\)](#) option. The boot image name selected will determine the operating system, platform and network type that will be used to install the client.
3. **Gateway Address:** If the client must go through a gateway to reach the boot server, enter the IP address of the gateway machine.
4. **Subnet Mask:** If the client is on a subnet, enter the subnet mask.
5. **Network Adapter Hardware Address:** The process for network booting a Linux system is referred to as a **broadcast boot**. It is required that the client and server are on the same network (no gateway between them). The broadcast is initiated from the client network adapter using the client's network adapter hardware address. This is also referred to as the **MAC address**. Having the MAC address available on the server allows the client system to be booted without knowing the server or client IP address, as this information is obtained from the server. Refer to the section **Boot a Client for Installation from a System Backup** for details on [determining the client hardware adapter address](#). Because the MAC address is required, you will need to enter the target client's hardware address when configuring a client for network boot.
6. **Boot on UEFI Firmware:** To perform a network boot of the client on UEFI firmware select "Yes" to this option. Otherwise, the client will be enabled to boot from BIOS. This option is only selectable for boot images that were created with support for booting from UEFI firmware.

7. **System Installation Mode:** You must select here whether you want to perform a no-prompt or menu-driven installation:
 - a. By selecting **No-prompt**, the client will be installed without entering any information on the client. This is referred to as a [no-prompt install](#). If selected, all of the remaining prompts must be filled in.
 - b. If **Menus (set defaults)** is selected, you will be provided the additional prompts now, all of which are optional. The information you provide will appear as defaults on the client after it is booted, but those options may also be changed on the client.
 - c. If **Menus (no-defaults)** is selected, it is assumed that all install options will be selected from the client install menus once it is booted. When selected, all remaining options will disappear from the screen as they no longer apply.
8. **Server to install from:** This field will, by default, contain the name of the [boot server](#). If the backup data will be restored from a different server than you booted from, select a different [install server](#) in this field. If the install server differs from the boot server, additional fields will appear on the screen, which are described in the section [Using a Different Install Server than the Boot Server](#) below.

If you wish to install the client using the server's alternate network, select the network from the [Alternate Server Network](#) drop-down list. If selected, additional fields will appear as described in the section [Using a Different Install Server than the Boot Server](#) below, since the client may need to use a different adapter to reach this alternate network on the install server.
9. **Device or File to install from:** Use the arrow button to list and select the device from which the backup data will be restored. If a directory device is selected, you will be prompted for the specific [System Backup](#) from which to install. After selecting the backup, the backup ID of the backup image will be placed in this field, and the **Backup Sequence Number** field will be automatically filled in with the sequence number of the client backup selected. If you select a tape device for this field, the device name will be placed in the field, but the backup will not be read at this time, since the backup may not be in the drive at the moment.
10. **Backup Sequence Number:** If the client will be installed from a tape device, you must manually select the backup sequence number on the tape media to install from. If there is only one [System Backup](#) on the tape, the backup sequence number will be 1 (default). If there is more than one, you must enter the appropriate backup sequence number. If you are unsure as to the correct sequence number to use, view the backup label and use the backup sequence number that corresponds to the desired backup.
11. **Console Device Name:** Select the name of the console device that will be used on the client. If the client is using a graphical display, this is likely **"tty0"**.
12. **Console terminal type:** If the console device selected was a graphical device, the terminal type will be set to **linux**. Otherwise, an [ASCII terminal](#) is assumed and you must list and select the specific terminal type. Using the arrow key, you can list the terminal types that are available during the installation process and select one from the list.
13. **Disable Network Boot After Install:** Select **"yes"** if you wish to have the client automatically disabled for network boot following a successful system recovery. The default is **"no"**.
14. **Apply Network Settings to Installed System:** When performing a recovery over the network or from a local NFS share, if the network configuration used to perform the recovery is different than the network configuration of the original backup client then the network configuration will be migrated to the configuration used for the recovery. This is done to prevent multiple systems configured with the same IP, which may cause conflicts and network problems. Select **"no"** to this option if you do not want this network migration to take place.

When all selections have been made, select the [Enable/Update](#) button at the bottom of the screen. The client boot information will be saved and the client will be ready to boot and install. If you have changed the boot

server, the image on the old boot server will be disabled automatically. Refer to the section [Boot a Client for Installation from a System Backup](#) to initiate the installation process.

Disable a Network Install Client

It may be desirable to disable the network install for a client once the installation of the client is complete. If the client should inadvertently boot over the network and the client is configured for a [no-prompt install](#), the client may end up being reinstalled automatically.

To unconfigure the client, simply select the option [Configure→Network Boot/Install→Enable/Disable Network Installation of a Client](#) from the menu bar. Select the client to disable. The client network install configuration will appear. Simply press the **Disable** button at the bottom of the screen to unconfigure the network install.

Unconfiguring the network install client will prevent the client from booting over the network. Although the network install will be disabled, the information for the network install will be retained and will be automatically used as defaults should the same client be configured for network install again in the future.

Using an Alternate Network to Restore the Data

Even though the boot and install server may be the same, it may be desirable to perform the network install (actual restoration of the data) using a different network than was used to perform the network boot. For instance, the client may boot from the server using the *ent0* (ethernet) network, but may want to restore the data from the same server using the *tok0* (token-ring) network instead. This is commonly done in order to redirect the restore data traffic onto a different network than that which is in use by other applications.

To install using an alternate server network, a drop-down list is provided on the [Network Boot/Install Configuration Screen](#) labeled "**Alternate Install Server Network**". If you want the alternate server network connection to be used for network install, select the appropriate network. If no option is selected, the default network connection used by the client to reach the server (as defined by the server hostname and network routing information on the client) will be used.

Note that this option will not be available if there was no [Alternate Server Networks](#) configured on the install server. To set the Alternate Server Networks for a server, refer to the [server configuration](#) options.

If you select this button, additional options will appear which will be required only if you are using a different network adapter on the client system to contact the install server than was used to boot the client. Refer to the section [Using a Different Install Server Than the Boot Server](#) below for additional instructions.

Using a Different Install Server than the Boot Server

If the **Server to install from** (install server) is not the same as the **Server to boot from** (boot server), or if you selected to use an alternate server network, additional fields will appear on the screen allowing you to configure the network differently for contacting the [install server](#):

1. **Gateway Address:** If the client must go through a gateway to reach the install server, enter the gateway IP address in this field.
2. **Subnet Mask:** If the network the client uses to reach the install server uses a subnet mask, enter the subnet mask here.
3. **Client Network adapter name:** If the client will use a different network adapter to reach the install server than was used to reach the boot server, use the arrow button to select an adapter name from the list. If you select a different adapter, you must also fill in the additional field as well:
 - a. **Client IP Address:** Enter the IP address associated with the adapter selected. If you are using a different install server than the boot server, the install server must recognize the client by this IP address and the hostname associated with this IP address must have been used to configure the client in the administrator application. If you are using the same server but an alternate server network, you must enter the client IP address that will be used to contact the server using the server's alternate network. Refer to the [Configure Servers](#) option for information on using an [Alternate Server Network](#).

Using the Same Boot Server to Install Different Linux Versions

The same boot server may be used to boot clients of any platform, network type and Linux version. The boot server does not need to have any device support installed to support the client's hardware and does not need to run the same level of Linux as the client. If every system is different, you may create a separate boot image for each client. Or, you may create a single boot image for all clients of similar hardware type and Linux version.

SBAAdmin will create a network boot image from any client, and then copies that boot image to the boot server. Each boot image is saved under a different name (of your choosing) and may be separately selected when you configure a client to network boot. This allows a single boot image to be used to install different client systems.

This 2-step process is described above in this section. First, [Create a Network Boot Image](#) (which also copies the boot image to the boot server), then [Enable the Network Install of a Client](#) by selecting the boot image on the server you previously created.

Updating Network Boot Images

If you have updated the operating system or installed new *base system hardware support* (network devices, disk drives, platform types or display adapters) onto a system that you previously created a network boot image from, you will need to recreate that network boot image before the new device support will be accessible to the clients booting from that image.

After installing the new device support, simply follow the instructions for [Create/Update a Network Boot Image](#) to recreate the boot image and copy to the boot server. If you recreate the boot image for the same platform, network and Linux version/release level, it will not be necessary to reconfigure the clients for network boot/install since the clients using the previous boot image will automatically begin using the newly created boot image.

4. Booting to the System Installation Process

Booting the Various System Types

This section will provide general guidelines for booting a system to the [Installation and Maintenance Menu](#), used to install a system from a [System Backup](#). Note that the steps differ widely between systems. Because new systems are being introduced frequently, this is not intended to be a complete guide for all systems. The following guidelines represent those systems most commonly found in our test and customer environments. If you are not familiar with the process of booting your system from different media, you should refer to your system documentation for detailed instructions.

To begin the system recovery process, the client system must be booted from [SBAdmin Boot Media](#). This may be a local bootable cdrom, tape, hard disk, or a network boot image stored on a boot server. In any case, the remainder of the installation process will be the same.

The instructions for booting the system vary for each boot type and also differ greatly depending on the type of the machine to be booted. SBAdmin supports *Intel-based 32 and 64-bit* systems which use *BIOS* firmware, and all *IBM POWER (System p) and System i* systems which use *OpenFirmware*. The exact details of how to boot each can vary with each model of hardware and version of firmware.

Although specific instructions on booting the systems from the installation media are not described here, here are some hints to help get you started:

Booting to the System Installation Process

CDROM or Tape

If your system uses BIOS or UEFI, it must be configured to allow booting from CDROM. Currently only the *IBM POWER (System p) and System i* systems (using OpenFirmware) support booting from tape. If your firmware (BIOS/UEFI/SMS) attempts to boot from a hard disk before booting from CDROM or Tape, you will need to change this in case there is already a bootable hard disk in the system.

Typically the BIOS can be accessed on most *Intel*-based (x86) systems by pressing the **Delete** key immediately after the display messages begin to appear. Once your BIOS is setup to boot from the correct media, just exit the BIOS menu or reset the system.

64-bit Intel-based systems (x86_64) with UEFI firmware will configure the device boot order using the EFI Boot Manager. In most cases, the default option to boot from CDROM will allow you to boot SBAdmin boot media directly from the UEFI firmware. However, it may be necessary for you to select "Boot From File" in the EFI Boot Manager to boot from the media in UEFI-mode. This will allow you to traverse the boot filesystem tree, where you would select the file "elilo.efi" to boot from.

For other firmware types, which will scan the system for bootable devices, you will normally receive a firmware prompt where you can select the specific device to boot from.

Hard Disk

To install from a hard disk configured as a system recovery boot disk, you must select to boot from the disk within the *BIOS*, *UEFI*, or *SMS* menus.

Assuming your firmware is setup to boot by default from the correct media, just turn on or reset the system. The remainder of the boot process will complete without further interaction.

Network Boot

To network boot an *Intel-based* system with [BIOS/UEFI](#):

Most BIOS or UEFI-based systems are not, themselves, network boot capable. However, if you have a network adapter card with network boot capabilities, you can have the system boot to the firmware on the network card. Therefore, the network card will be used to provide the network boot capabilities the system firmware does not.

Initiating a network boot will vary depending on your version of the firmware installed on the system. On most systems with BIOS or UEFI, there will be an option to boot from the network during POST by selecting a specific function key (i.e. F12). Others may require you to set the network adapter as the first boot device in the boot order.

It may also be necessary to select the Network Boot Protocol to use. If this option is provided, select “**PXE**”, unless you have manually configured a different boot protocol on the *boot server*.

Depending on the firmware of your network adapter, you may be provided the option of entering the client and server IP address (and optional gateway address). If your boot server is configured with your *network adapter hardware (MAC) address*, you may perform a *broadcast boot* without entering the IP addresses. If not, you will need to enter this information. If you are booting across a gateway, you must enter the client, server and gateway addresses (in which case a broadcast boot is not possible).

If you follow the instructions provided here, and/or on the screen, and the boot process does not work (or no network boot option is provided), then neither the system nor your network adapter are boot-capable. You will need to use a network adapter that includes the **PXE network boot protocol**.

To network boot *IBM POWER (System) p and System i* (CHRP) systems from the [OpenFirmware](#) prompt:

1. CHRP systems network boot directly from OpenFirmware (OF) without a boot loader. You must specify the OF device name to boot from as well as all necessary kernel command-line options at the OF prompt. For network devices, there is often an alias established in OF that points to the OF device name. This is because the OF device name is rather lengthy and complicated. To illustrate, in the example we will use below, the OF device name is:
`is:/pci@8000000200000002/pci@2,2/ethernet@1`

The alias for this device is “*network*”. If you perform network installs often, you may want to set up this alias. To determine the OF device name of the network device:

Select “**Select Boot Options**” from the SMS “*Main Menu*”

Select, “**Select Install/Boot Device**” from the “Multiboot menu”

Select, “**List all Devices**” from the “*Select Device Type*” menu

Select the “**Device Number**” of the network device.

Select “**Information**” for the task to perform.

This will present an information screen that will provide details about the ethernet device, including the OpenFirmware device name.

```
SMS 1.6 (c) Copyright IBM Corp. 2000,2005 All rights reserved.
```

```
-----  
Device Information  
IBM,FW-ADAPTER-NAME: IBM 10/100/1000 Base-TX PCI-X Adapter
```

```

        /pci@800000020000002/pci@2,2/ethernet@1
                : (Bootable)
DEVICE        : Ethernet
        ( loc=U7879.001.DQDZHXCX-P1-C4-T1 )
NAME          : ethernet
DEVICE-TYPE   : network
SUPPORTED-NETWORK-TYPES:
                : ethernet,auto,rj45,auto   <==  chosen
                : ethernet,10,rj45,half
                : ethernet,10,rj45,full
                : ethernet,100,rj45,half
                : ethernet,100,rj45,full
                : ethernet,1000,rj45,full
MAC-ADDRESS   : 000255d33813
-----
Navigation keys:
M = return to Main Menu      N = Next page of list
ESC key = return to previous screen      X = eXit System Management Services
-----
Type menu item number and press Enter or select Navigation key:

```

In this example the OF device name is `/pci@800000020000002/pci@2,2/ethernet@1`. This procedure is ONLY to get the OF device name. Do not select to boot from this device. You must enter this device name manually (or use an alias) at the OF prompt.

2. Initiate OpenFirmware (OF) by pressing `F8` (graphical display) or the “8” key (ASCII terminal) when the system configuration icons or messages begin to appear on the screen. After the system configuration completes, the OpenFirmware prompt will appear
3. From the OF prompt, enter the following line to boot from the network adapter.

```

ok> boot network_adapter_device_name console=hvc0 load_ramdisk=1
      init=/init ramdisk_size=65536 rw selinux=0 devfs=nomount
      raid=noautodetect

```

- a. For the **network_adapter_device_name**, use the OpenFirmware (OF) device name of the network adapter you wish to boot from.

You may also use a device alias for **network_adapter_device_name**. To determine if an alias is already set up for your device type:

```
ok> devalias
```

To create a device alias called “**network**” using the OF device name obtained from SMS type:

```
ok> devalias network network_adapter_device_name
```

To create a device alias that is retained across reboots, you should use the **nvalias** command:

```
ok> nvalias network network_adapter_device_name
```

You can then use the “**network**” alias you created in place of the **network_adapter_device_name** in the command above.

- b. For the **console** option, use **tty0** for a display attached to a graphics adapter, or **ttyS0** for a directly attached serial (ASCII) terminal. If installing onto an LPAR system, use **hvc0** (virtual console).
- c. The **selinux** option is needed only on systems with Security Enhanced Linux support, but will be ignored otherwise.
- d. The **devfs** option is needed only on systems with DEVFS support, but will be ignored otherwise.

- e. The **raid** option is needed only on systems with disks previously containing software RAID devices, but will be ignored otherwise.

Depending on the firmware of your network adapter, you may be provided the option of entering the client and server IP address (and optional gateway address). If your boot server is configured with your *network adapter hardware (MAC) address*, you may perform a *broadcast boot* without entering the IP addresses. If not, you will need to enter this information. If you are booting across a gateway, you must enter the client, server and gateway addresses (in which case a broadcast boot is not possible).

Tape Boot

Tape boot **IBM POWER (System p) and System i** (CHRP) systems from the [Open Firmware](#) prompt:

1. CHRP systems initiate a boot from tape directly from OpenFirmware (OF) without a boot loader. You must specify the OF device name to boot from as well as all necessary kernel command-line options at the OF prompt. For some devices (like disk and network), there often is an alias established in OF that points to the OF device name. This is because the OF device name is rather lengthy and complicated and the device can be referred to as “*disk*” or “*network*”. To illustrate, in the example we will use below, the OF device name for the tape device is:

```
/pci@80000002000000b/pci@2,2/pci1069,b166@1/scsi@0/st@2,0
```

Unfortunately, our experience shows that tape drives rarely have an alias set up. The alias for the tape drive in our example will be “*tape*”. If you perform tape boots often, you may want to set up this alias. To determine the OF device name of the tape drive:

Select “**Select Boot Options**” from the SMS “*Main Menu*”

Select, “**Select Install/Boot Device**” from the “*Multiboot menu*”

Select, “**List all Devices**” from the “*Select Device Type*” menu

Select the “**Device Number**” of the tape drive.

Select “**Information**” for the task to perform.

This will present an information screen that will provide details about the tape drive, including the OpenFirmware device name.

```
SMS 1.6 (c) Copyright IBM Corp. 2000,2005 All rights reserved.
-----
Device Information
  /pci@80000002000000b/pci@2,2/pci1069,b166@1/scsi@0/st@2,0
      : (Bootable)
DEVICE      : SCSI Tape
  ( loc=U7879.001.DQDHZDC-P1-C4-T1-L2-L0 )
NAME        : st
DEVICE-TYPE : byte

Parent Information
IBM,FW-ADAPTER-NAME: Dual Ultra-320
NAME         : scsi
DEVICE-TYPE  : scsi-2

-----
Navigation keys:
M = return to Main Menu
ESC key = return to previous screen      X = eXit System Management Services
-----
Type menu item number and press Enter or select Navigation key:
```

In this example the OF device name is:


```
/pci@80000002000000b/pci@2,2/pci1069,b166@1/scsi@0/st@2,0
```

This procedure is ONLY to get the OF device name. Do not select to boot from this device. You must enter this device name manually (or use an alias) at the OF prompt.

2. Initiate OpenFirmware (OF) by pressing F8 (graphical display) or the “8” key (ASCII terminal) when the system configuration icons or messages begin to appear on the screen. After the system configuration completes, the OpenFirmware prompt will appear
3. From the OF prompt, enter the following line to boot from the tape drive.

```
ok> boot tape_drive_device_name console=hvc0 load_ramdisk=1 init=/init  
ramdisk_size=65536 rw selinux=0 devfs=nomount raid=noautodetect
```

- (1) For the **tape_drive_device_name**, use the OpenFirmware (OF) device name of the tape drive you wish to boot from.

You may also use a device alias for **tape_drive_device_name**. To determine if an alias is already set up for your device type:

```
ok> devalias
```

To create a device alias called “**tape**” using the OF device name obtained from SMS type:

```
ok> devalias tape tape_drive_device_name
```

To create a device alias that is retained across reboots, you should use the *nvalias* command:

```
ok> nvalias tape tape_drive_device_name
```

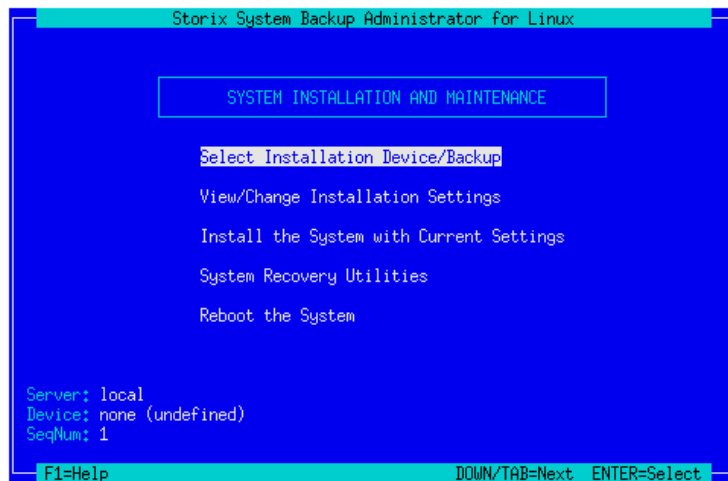
You can then use the “**tape**” alias you created in place of the **tape_drive_device_name** in the command above.

- (2) For the **console** option, use **tty0** for a display attached to a graphics adapter, or **ttyS0** for a directly attached serial (ASCII) terminal. If installing onto an LPAR system, use **hvc0** (virtual console).
- (3) The **selinux** option is needed only on systems with Security Enhanced Linux support, but will be ignored otherwise.
- (4) The **devfs** option is needed only on systems with DEVFS support, but will be ignored otherwise.
- (5) The **raid** option is needed only on systems with disks previously containing software RAID devices, but will be ignored otherwise.

Completing the Boot Process

If the installation mode of the boot media was configured for [no-prompt install](#), the installation will proceed without any user prompts. This assumes that a console and restore device was pre-determined and the storage configuration information on the backup media is compatible with the system being installed. Refer to the section [Enable Client for Network Installation](#) for details on the configuration of a no-prompt install.

If not performing a [no-prompt install](#) (or problems were detected with a no-prompt install), the following **Installation and Maintenance** screen will appear:



The detailed instructions for using the options on this menu are provided in the sections [Reinstall a System from a Backup](#) and [View/Change Installation Settings](#).

Troubleshooting a Network Boot

To boot from the network, a server must have first been configured to provide a network boot image to this client. Those steps are outlined in the section [Network Boot/Install Configuration](#).

To perform a network boot, SBAAdmin uses a standard network process called “**BOOTP**”. BOOTP is initiated from the client and communicates with a BOOTP daemon on the boot server, who in turn provides the client with information needed to obtain and execute a network boot image.

If you are able to initiate the BOOTP process, but the client still fails to get to the SBAAdmin Installation and Maintenance process, there may have been an error in network communication between the client and server or an error in the network boot configuration. Be sure to check the following:

1. Check that the settings in the [Enable Network Installation of a Client](#) process are configured properly. Specifically be sure that the client gateway, subnet mask, platform and adapter type are correct.
2. If you are booting an IBM System p or System I system, and trying to perform a **broadcast BOOTP** (by leaving the client and server IP address fields blank), try filling out the client and server addresses instead. Note that a broadcast BOOTP cannot be performed if a gateway is used between the client and server. Also, BIOS and EFI-based systems will only support broadcast boot, so entering IP addresses is not an option.
3. Be sure that the **bootpd** or **dhcpcd** daemons, as well as the **tftpd** daemons are enabled on the boot server. Specifics for checking for the availability and enabling the daemons differ with each Linux distribution, so details cannot be provided here.
4. Check that the server's IP address is correct, and that you specified the correct gateway and subnet mask (if needed). Keep in mind that the gateway address should be the gateway the client uses to connect to the server, not the other way around.
5. The **SMS** and many **PXE** boot menus have options to “ping” the boot server. This is handy to determine if the TCP/IP communication is valid between the systems, rather than a BOOTP configuration issue.
6. If you are entering a gateway address in the network boot screen on the client, be sure to enter the gateway address the client uses to reach the server, not the gateway address found on the server.

7. If you are attempting a *broadcast boot* and the boot fails, return to the network boot menu (if any) and make sure there are no IP addresses entered in the network boot settings. Remove any entries if they exist. If any entries are found, they will be used instead of a broadcast boot.

Determining the Network Adapter Hardware Address

Some systems require that the adapter hardware address, also referred to as the **MAC address**, be used to network boot a client. The MAC address is used to initiate a **broadcast boot**. In other words, the boot request is *broadcast* on the network, and each server running the **bootpd** or **dhcpd** daemon will examine the request to see if it is configured to respond to that MAC address.

A non-broadcast boot requires you enter the IP address of the server and the IP address assigned to the client you are booting. Since this request is sent directly to the server, and the server responds to the client IP, there is no need to know the MAC address.

Performing a broadcast boot, therefore, does not require that you enter the server or client IP addresses into the network boot screen (and for some systems this is not an option). The broadcast boot, however, requires that the MAC address be entered when [setting up the client for network installation](#). The steps to obtain the network adapter hardware address of the client differ widely depending on the platform and system model. If you do not know how to determine the adapter hardware address, you can usually find this information on the screen when initiating a network boot operation (even if the boot is unsuccessful) or when displaying the available network adapters to boot from.

5. Reinstall from a System Backup

A [System Backup](#) may be used to reinstall either the original system or a different system with either the same or different hardware configuration. To initiate the installation, you must first boot the client from CDROM, network boot server, local (internal, or external/portable) disk, or from the local tape using the instructions found in the section [Booting to the System Installation Process](#).

To setup a client system to be installed from a System Backup on a network install server, you must first configure it using the process described in the section [Enable/Disable Network Installation of a Client](#).

Cloning Systems

"Cloning" a system means to install a system from a backup originating on another system. The system from which the backup was made may be identical or completely different than the system you are installing.

If the system to be installed is identical in hardware type and configuration to the one the backup was made from, the installation may be performed with no customization required. However, if the systems differ, there may be changes required. For instance, if the disk configuration on which the volume groups were placed is not available on the new system, messages will be displayed that the original disks are not available and you must select new physical volumes into which the volume groups will be placed. See [View/Change Installation Settings](#).

Installing onto UEFI-Based Firmware Systems

In order to perform a system installation which will subsequently boot from UEFI firmware, you must first boot the system from UEFI using SBAAdmin boot media. Then you must perform the recovery using a backup that is also [supported on UEFI](#).

Most UEFI-based systems are capable of booting from both UEFI and BIOS (often referred to as *Legacy*). In the event you are unable to boot from UEFI firmware, the SBAAdmin boot media, backup, and system installation process will always be supported when booting from BIOS or Legacy mode.

No-Prompt Installation

If the system is set to [no-prompt installation](#), the [Installation and Maintenance Menu](#) will not appear (as described in the following section), but the installation will proceed without any input from the user. If your boot media was created for a no-prompt installation, a banner will display as follows:

```
=====
                !!!! NO-PROMPT INSTALLATION !!!!
=====
The installation process was set to no-prompt mode. The installation
will continue in  seconds with no prompts unless a problem
occurs requiring user-interaction.

    You may enter one of the following options or the
    installation process will continue in 60 seconds:
        1) Continue the installation
        2) Go to installation menu
        3) Halt the system
```

As indicated, you will have 60 seconds to turn off the system to prevent the system recovery process from continuing (and possibly overwriting all data on the system).

However, if any error occurs, such as an install server or device not being available, or if the backup data read from the installation media cannot be installed onto the detected hardware without user intervention, an error message will occur and the [System Installation Menu](#) will appear.

Refer to [Creating Boot Media](#) and [Enable/Disable Network Installation of a Client](#) for information how to pre-answer any questions normally asked during the install process which are required for a no-prompt installation. If configured for no-prompt installation, the installation process will proceed automatically as follows:

1. The defined install server and device will be checked to ensure they are available and readable
2. The selected backup will be read and the installation information will be extracted
3. The configuration information from the backup will be compared against the current system configuration to ensure the storage configuration may be created according to the backup data. If there are non-fatal problems which can be corrected, they will be corrected automatically.
4. If there are any fatal problems, such as no disks on the new system that match the original system, or if the disks on the new system are not large enough to contain the original data, the system will enter prompted mode and the installation menus will appear in order for the user to make changes to correct the problems before continuing.

Installing from an Encrypted Backup

If the backup to be restored from was encrypted during the backup process, it will be necessary to decrypt the data during the restore. Unlike restoring data on a live system, where the encryption keys are available on the backup system, the encryption key must be entered manually during the system installation. The encryption keys are not stored in the boot media or the backup information as this might be penetrable to hackers.



As warned during the backup process, an encrypted backup **cannot** be restored without the proper *encryption key*. This key may not be retrieved from the backup, nor can SBAAdmin assist in providing the correct key. If you do not have the proper encryption key needed to decrypt this backup, you will **not** restore this data!

The encryption key is a value that the user defined prior to performing the backup. If the encryption key is not known, you will not be able to restore the system from this backup. However, to make encryption keys easier to remember and/or enter, it may be entered either as a hexadecimal number or an ASCII text equivalent (if this was the form used to create the original key).

When selecting to install from an encrypted backup, the following message will appear:

```
=====
                        BACKUP DATA IS ENCRYPTED
=====
To read the backup data, an encryption key is required. You may supply
a 32-byte HEX key to decrypt the data. If you used a 16-byte
ASCII (text) key to generate the HEX key, you may also enter it here.

Select one of the following:
  1) Enter a HEX key
  2) Enter an ASCII (text) key
  3) Start a shell
==> 
```

Select the appropriate option for entering either a HEX or ASCII encryption key. The third option may be used to start a shell to type commands at the command line should you need to perform system tasks without reading the backup data.

Enter a HEX Key

The length of the key will depend on the number of bits of encryption. For 128-bit encryption, a 32-byte hexadecimal number is required. For 192-bit encryption, a 48-byte number is needed, and for 256-bit encryption, a 64-byte hex number is needed. Select option 1 from the list above, then when prompted to "Enter your 32-byte HEX key (or press Enter to reselect key type)", enter they key, or press Enter to return to the options above.

Enter an ASCII (text) Key

The length of the key will depend on the number of bits of encryption. For 128-bit encryption, a 16-byte ASCII string is required. For 192-bit encryption, a 24-byte string is needed, and for 256-bit encryption, a 32-byte string is needed. Select option 1 from the list above, then when prompted to "Enter your 16-byte ASCII (text) key (or press Enter to reselect key type)", enter they key, or press Enter to return to the options above.

The key you enter will be converted to an appropriate hexadecimal number and used to decrypt the data, just as if you entered the hex key yourself.

Upon entry of a valid key, the restoration of the data will continue. If an invalid key is entered, you will be informed so, and returned to the above menu of options.

System Installation Process

After booting from a network boot server

When the system is booted from the network, the client network installation options will also be copied from the boot server to the client. Any installation options setup when the client was configured for network boot (see [Enable/Disable Network Installation of a Client](#)) will be used by default for the installation. These pre-set defaults may include the install server and device, the console device and terminal type, the backup sequence number, or anything else required for the installation to proceed with no required input from the user. If the user selected a no-prompt installation (see [No-Prompt Installation](#) above), the installation will continue automatically. Otherwise, the installation menus will appear and the user may manually change any prior defaults, add any settings that were not pre-configured, or continue the installation process with the current settings.

Verifying the hardware configuration

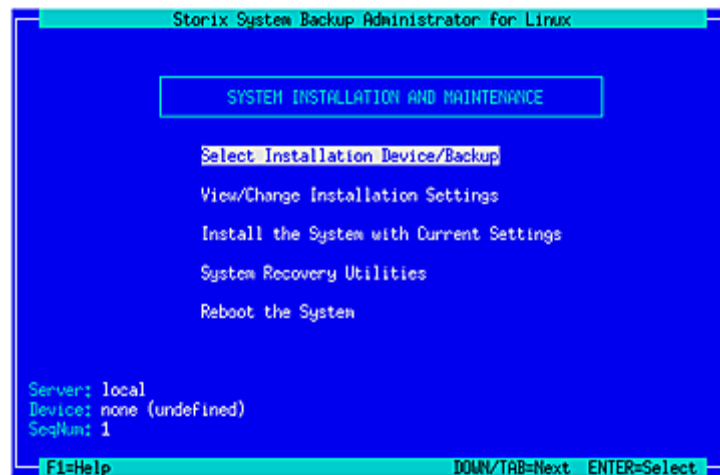
Once the backup media is selected, and you chose to either continue the installation with the current settings or to change the storage configuration, the following will occur:

1. The disks defined on the backup are compared against the current system's hardware configuration. If there are problems that would prevent the backup from being installed onto the system, such as missing disks or disks that are too small to contain the backup data, a list of messages indicating the problems will be displayed and the user will be required to either make changes manually or may select to **automatically fix** any problems that are non-fatal.
2. Non-fatal errors are those that require changes to the configuration in order to allow the data to be restored, although some settings may differ from those of the original system. If such non-fatal errors occur when checking the system information, you will be provided the option of automatically fixing the errors. You may also change the storage configuration manually to either add more disk space or change other attributes manually that would allow it to fit on the new hardware.

More details of the verification that takes place are described later in [Verification Process](#).

The System Installation and Maintenance Menu

When the boot process has completed, the **System Installation and Maintenance Menu** will appear:

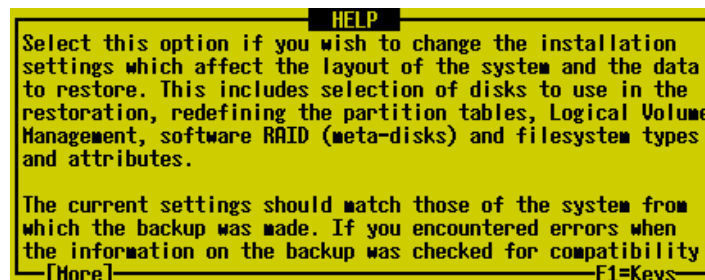


Using Keys and Getting Help

Because these menus are designed to appear on both graphic and serial (ASCII), the menus are provided in a form viewable on **ASCII terminals**. The use of the mouse is not available. Most keyboards will support arrow keys while others do not. Also, some keyboards have page up and page down keys, help keys, etc, that others do not. For this reason, there is a variety of methods which may be used to traverse the menus and options in the installation screens:

- To move between fields, use the **Up-arrow** and **Down-arrow** keys on the keyboard.
- To make a selection, press the **Enter** key, and
- To return to a previous screen, use the **F3** or **ESC** (escape) key
- For pop-up lists, help screens and other messages, you may use the arrow keys to move up and down the list or to scroll the text. You may also use the **Page-up** and **Page-down** keys, if available, or use **CTRL-N** for 'next page' and **CTRL-P** for 'previous page' if not.

Help Windows: The **F1** or **“!”** key (shift/1) may be pressed at any field or menu item to obtain help instructions, detailing the use and options for the corresponding item. A help window will appear in the center of the screen as in the following example:



If the help information is lengthy for a particular option (indicated by **[more]** at the bottom), it may be necessary to page the message using the page or control keys described above. To remove the help window and return to the previous entry, press the **F3** or **ESC** key.

Pop-up List Options: Pop-up lists are available for many entry options. When supported, “List=F4” will appear at the bottom of the screen. At that field, you may press the **F4** or “\$” key (shift/4) to list the available options for the corresponding field and select an option from the list. To select an option, use the arrow keys to highlight the desired option and press **Enter**. The selected option will be placed in the entry field and the pop-up window will disappear.

Select Installation Device/Backup

The installation server and device, if any, will be displayed at the bottom of the screen. If the system was booted from the network, the install server will default to the boot server unless a different install server was defined when the client was configured for network boot. If the system was booted from a local tape, the server is assumed to be “local” (or none) and the installation device is assumed to be the tape drive the system was booted from.

Select the **Select Installation Device/Backup** option if you wish to change the server on which the backup media is attached, or the remote or local installation device. You will only be able to select a remote server when using the *Network Edition* license. After selecting this option, you are presented with one of the following additional option screens:

NOTE

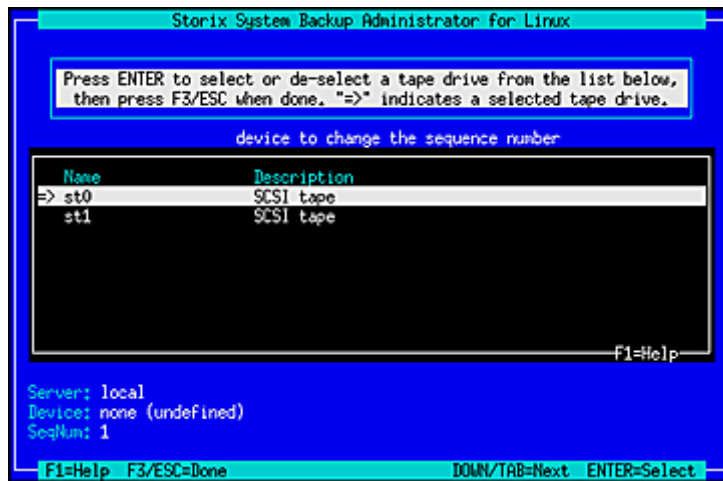
The following menu options appear if you did not have TSM support installed onto the client from which the backup media was created. Refer to the TSM Configuration section below for information and examples.

```
Storix System Backup Administrator for Linux
Select Installation Device/Backup
NOTE: Select the device to change the sequence number
Install from LOCAL Device:
  Select Local Tape Drive(s)
  Select Local Disk Backup
Install from LOCAL NFS Mount:
  Set or Change NFS Mount Configuration
  Select NFS Mount Backup
Install from REMOTE Device:
  Set or Change Network Configuration
  Select Remote Tape Device
  Select Remote Disk Backup
Server: local
Device: none (undefined)
SeqNum: 1
F1=Help F3/ESC=Done DOWN/TAB=Next ENTER=Select
```

Highlight the option you wish to select using the up and down arrow keys on the keyboard. Each option is described in detail below:

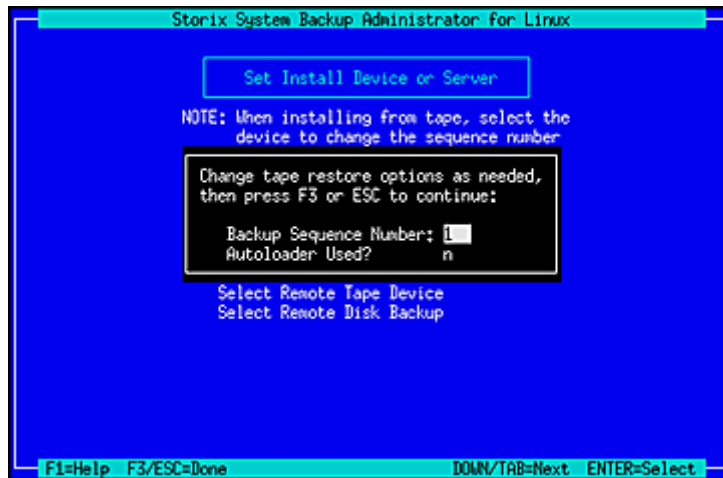
Select Local Tape Device Drives(s)

Regardless of the type of SBAdmin boot media used to boot the target system, you may change the installation settings to allow installation from a local tape drive, even a different drive than was booted from. When selecting this option, a list of local tape devices will be displayed.



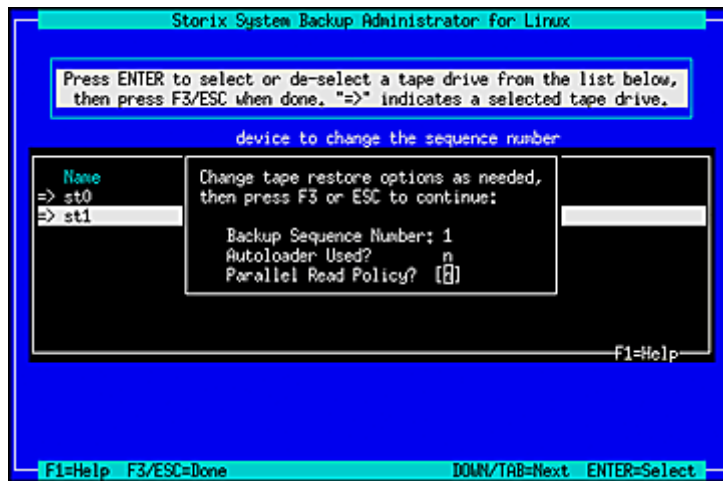
If you are restoring from a *parallel tape device*, then you should select all tape drives that make up that device. Otherwise you should only select a single tape drive.

After selecting the tape drive, press **F3** or **ESC** and the following window will pop-up on the screen:



If the backup you wish to install from is not the first backup on the media, type the [backup sequence number](#) in the **Backup Sequence Number** field. Refer to the backup sequence number in the backup label if you do not know the correct backup sequence number to use. If an [Autoloader](#) is used with the device, select "y" in the **Autoloader used?** field. Refer to [Virtual Devices](#) for more information on the use of sequential autoloaders. Once you have selected the desired options, press **F3** or **ESC** to return to the [Change Installation Server or Device menu](#).

When selecting multiple tape drives, the following window will pop-up on the screen:



The **Backup Sequence Number** and **Autoloader used?** options are the same as previously described. However, there is a **Parallel Read Policy** which should be set to “y” if the backup was created using a **Parallel Tape Device**.

If the backup was created using a **Parallel Tape Device**, you must select all tape drives that make up this device and enter “y” for *Parallel Read Policy*. The devices previously configured on the system are not known when booting in installation mode, so this option provides you a method of defining a parallel tape device on the local system. You must select at least two drives from the list. To do so, highlight the desired entry and press Enter. An arrow (=>) will appear next to each option selected.



Important: You must select the same number of devices used to create the backup and you must select them in the same order as they were previously configured

You may also use sequential tape devices to restore from the backup if the backup spans multiple tapes and you want the installation to automatically span the tapes inserted in different devices. This option is identical to the use of a **Sequential Tape Device**. The devices previously configured on the system are not known when booting in installation mode, so this option provides you a method of defining sequential devices on the local system.

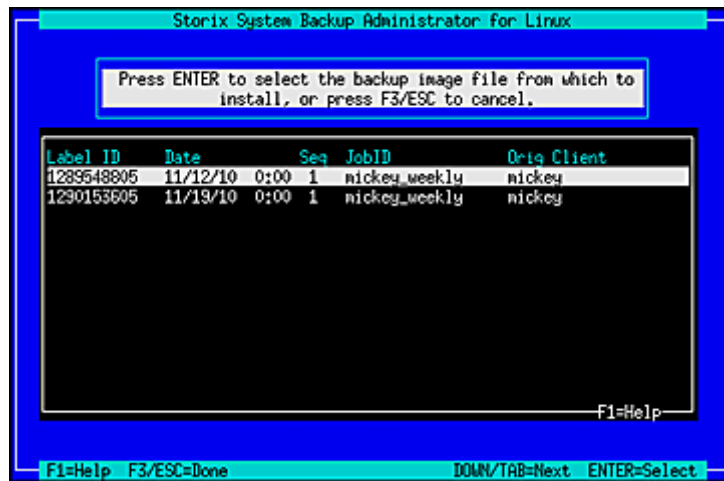
You must select at least two drives from the list. To do so, highlight the desired entry and press Enter. An arrow (=>) will appear next to each option selected.



Important: You must select the devices in the same order in which they will be read.

Select Local Disk Backup

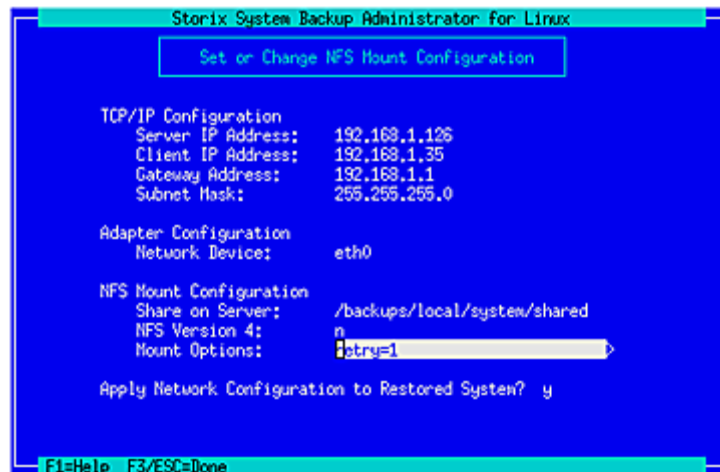
If you configured a locally-attached (or SAN-attached) disk for system backup/recovery (refer to **SBAdmin User Guide**), and you performed the System Backup to a configured **local system backup disk**, you may reinstall the system using that backup. If you select this option, the system will be scanned for one or more system backup disks, and then the disks will be queried for available system backups. If any are found, a screen similar to the following will appear, from which you may select the backup to restore:



Select a backup by highlighting the desired line and pressing **ENTER**, or press **F3** or **ESC** key to cancel the selection. After making your selection, you are returned to the [Change Installation Server or Device menu](#).

Install From Local NFS Mount

If the system backup you wish to use for the recovery is located on a remote NFS share, you may use this option to get access to the backup by performing a NFS mount of the share to the local system. Performing recovery from local NFS mount is supported with **Network Edition** and **Workstation Edition** licenses only. You must first select the [Set or Change NFS Mount Configuration](#) option which will display a screen similar to the following:



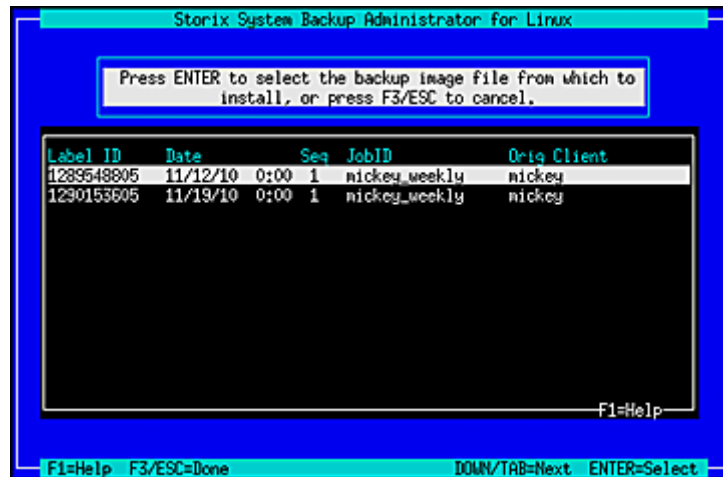
To restore from a NFS mounted backup the **Server IP Address**, the **Client IP Address**, the **Network Device**, and the **Share on Server** fields must be filled in. If the client requires a gateway to reach the NFS server enter the **Gateway Address**. When selecting the network device, use the **F4** key to list the adapters available on the system. The option to **Apply Network Configuration to Restored System** indicates whether you wish to migrate the above client network settings to the restored system.



If you receive a message that no network devices are found, then you probably need to [Load Additional Network Device Modules](#).

You should enter "y" in the **NFS Version 4** option if the share you will be accessing is to be mounted using NFS v4 (NFS v2, v3, and v4 are supported). The **Mount Options** field allows you to enter any *mount* command "-o" options necessary to mount the remote share. Press **F3** or **ESC** to save the options and configure the network.

After entering the above NFS mount configuration options, select the **Select NFS Mount Backup** option. Selecting this option will mount the remote share locally and list all system backups found in the share. Only backups of type **FULL SYSTEM** will be listed. If any are found a screen similar to the following will be shown:



NFS Considerations

SBAAdmin in no way configures the remote NFS server. It must be configured to allow the client IP you are using read access to the files in the share.

The share is mounted using the options you provided and the `mount` command as follows:

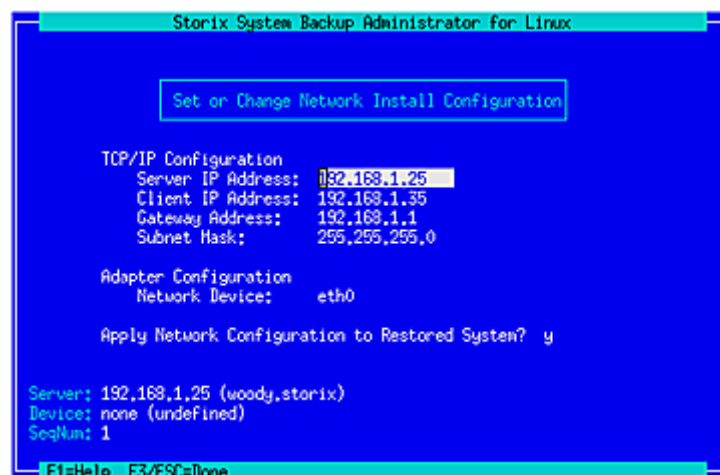
```
mount -t nfs -o MOUNTOPTIONS SERVERIP:NFS SHARE /images
```

NOTE

The system recovery process does not support mounting NFS shares that require any type of authentication (ie Kerberos).

Set or Change Network Configuration

When performing recovery from a remote SBAAdmin server, you may set or change the [network install server](#) from which to obtain the backup. The backup itself may be on a tape attached to the server or on the server's disk drive. Upon selecting this option, a screen similar to the following will be displayed:



To use a network install server, the **Server IP Address**, **Client IP Address** and **Network Device** fields must be filled in. If a gateway is required for the client to reach the install server, enter the gateway the client must use in the **Gateway Address** field. Under Adapter Configuration, press **F4** to list the devices available on the system. The option to **Apply Network Configuration to Restored System** indicates whether you wish to migrate the above client network settings to the restored system.

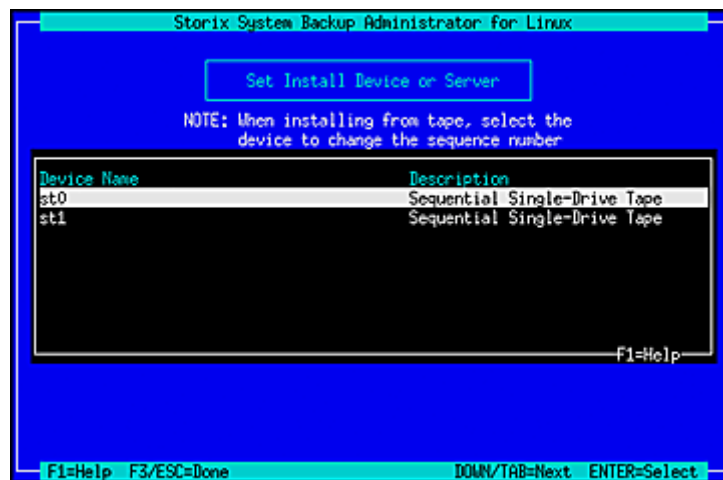
NOTE

If you receive a message that no network devices are found, then you probably need to [Load Additional Network Device Modules](#).

Press the **F3** or **ESC** key to end and return to the [Change Installation Server or Device menu](#) once you have finished your selection. When you do so, the network will be configured according to the settings you chose, and the new server will be displayed at the bottom of the screen. If the server has changed, any previous device selection will be removed and you will be required to select a new installation device.

Select Remote Tape Device

If a [network install server](#) is selected and available (indicated by the **Server** at the bottom of the screen), you may select to install from a backup in a tape drive attached to the remote server. Note that you may select a remote server and device regardless of the type of boot media used. When selecting this option, a list of tape devices on the server will be displayed and you may select a tape device from the list.

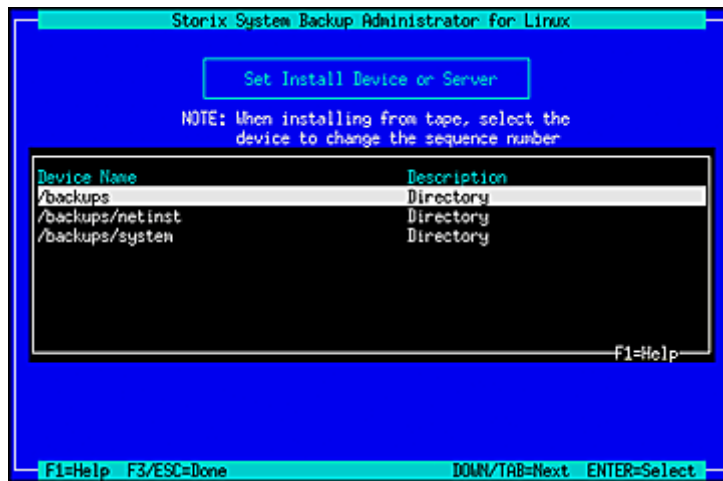


Once you have made your selection, the drive will be checked to ensure that it is available and the name of the device will be displayed at the bottom of the screen, and you will be returned to the [Change Installation Server or Device menu](#).

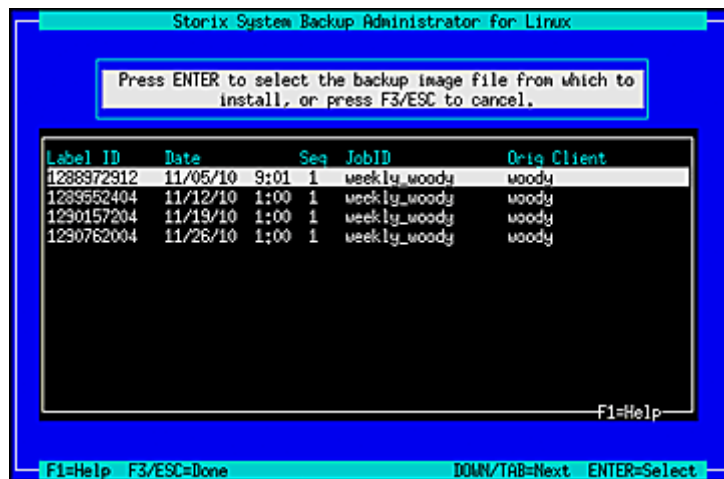
Select Remote Disk Backup

If a [network install server](#) is selected and available (indicated by the **Server** field at the bottom of the screen), you may select to install from a disk file backup available on the server. Note that you may select to install from a remote server and device regardless of the type of boot media used.

When selecting this option, a list of directory devices will be displayed. This list will only include those directory devices that are configured for System Backups. Refer to [Configuring Backup Servers and Devices](#) for more information on configuring devices for system backups.



After selecting the directory device, a list of System Backup images on the server will be displayed which you may select. The list will also display the client from which the backup was originally made, the date and backup job ID.



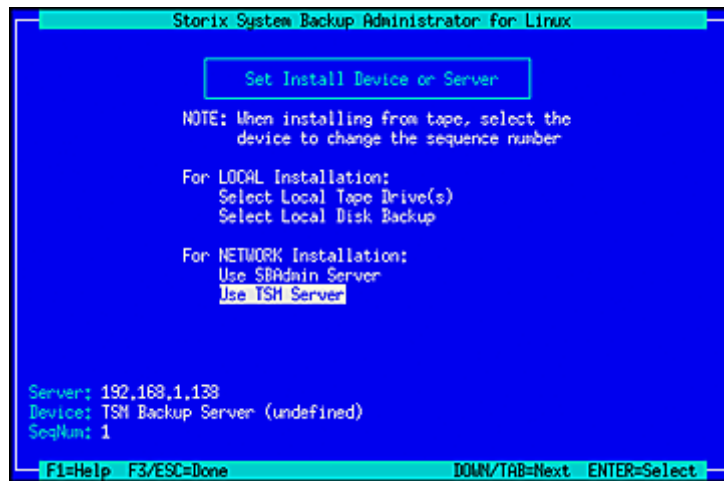
If you expect a backup image to appear in the list that does not, it may be that the backup was written with permission for only the original client to read it. If the client to install is not the same as the original client (or the client is installing from a different network adapter and therefore has a different hostname), you must change the backup image to allow clients other than the originating client to read it. Refer to [Change Access Permission of a Disk Backup](#) for details. Only backups of type **FULL SYSTEM** will appear in the list.

Once you have made your selection, the **Backup ID** of the backup file will be displayed in the **Device** field at the bottom of the screen, and you will be returned to the [Change Installation Server or Device menu](#).

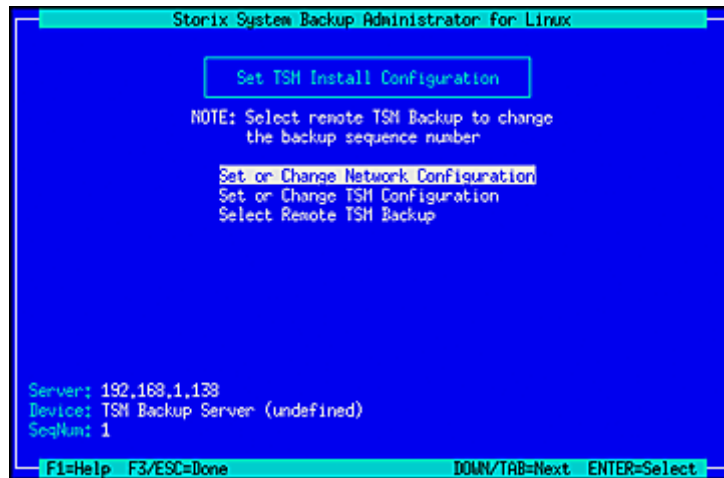
Once the installation server and/or device have been selected, press the **F3** or **ESC** key to return to the [Installation and Maintenance Menu](#).

TSM Configuration

When selecting the [Change Installation Server or Device](#) option from the main menu and **TSM support** was enabled on the client from whom you created the boot media, the [Set Install Device or Server](#) menu will look a bit different as shown below:



If you wish to install from a TSM server, select **Use TSM Server** from the list above. The following screen will appear:



You will need to enter additional information used to contact the TSM server on the screen below:



TSM Client Configuration

You are required to enter the **NODENAME** of the TSM client you are installing. Note that this is not necessarily the same node from which the backup was originally created. If you know the node's password, enter it in the **NODE Password** field. If you do not know the node password, then you will be required to supply the TSM Administrator username and password in the fields below.

Note that, when logging onto the server using the nodename and password, you will have access to backups created by this node, as well as any backups of other nodes for which the backup read permission was set to allow access to any client. If you need access to all client backups on the server, you will need to log on using the administrative username and password as described below.

TSM Server Configuration

The required field in this section is the **TCPServeraddress**. You must use the TCP address, not the hostname, since host name services are not available when booting from the installation media. The remainder of the fields may typically use the defaults shown. Use the **F1** key to display detailed help information for any screens.

TSM Administrator Configuration

The TSM administrative user information need only be entered if you do not know the **NODE Password**. Also, by logging onto the server as the administrative user, instead of using the node password, you will have access to all backups on the server, even those for which the permission was set to only allow owner access in the backup profile.

Once you have entered all of the required TSM information, press the **F3** or **ESC** key to return to the previous menu.

Change the Installation Settings

The sizes, locations and all other attributes for [disks](#), [partitions](#), [volume groups](#), [logical volumes](#), [meta-disks](#), [swap spaces](#) and [filesystems](#) as defined on the backup may be changed using this option. If the backup settings have not been previously read from the backup, the backup will be read and the settings, according to the original system, will be extracted from the backup. The settings will then be verified to ensure they are compatible with the current system's hardware configuration. If the verification fails, you will be required to fix the information to accommodate installation of the backup onto the current system. This may be done either automatically or by changing the setting manually as described in the section [Verify the hardware configuration](#) above.

Upon selection of this option, a set of menus will appear that allow you to customize virtually any attribute of a partition, volume group, logical volume, meta-disk or filesystem defined on the backup. You may also choose to exclude certain elements from being created or restored, or you may select to create them without actually restoring the data. These menus and options are numerous, and are described in detail in the chapter [View/Change Installation Settings](#).

Once you have completed all changes, press the **F3** or **ESC** key to return to the [Installation and Maintenance Menu](#).

Install the System with Current Settings

When you have completed all steps necessary prior to installing the system, such as changing the installation server, device or volume group information, you may select this option to begin the installation of the system using the current settings.

The backup settings will again be verified to ensure consistency with the current hardware configuration as described in the [Verification Process](#). If any problems are found, you will be returned to the [Installation and Maintenance Menu](#).

If no problems in the system configuration were found that prevent the installation from proceeding, a confirmation screen will appear, showing you the disks that will be overwritten by the installation. You will be required to press Enter to continue. A final warning will appear and you must then press "y" to continue the installation or "n" to return to the Installation and Maintenance Menu.

Once you have selected to continue, the installation will proceed with no further user input. The partition tables, volume groups, logical volumes, meta-disks and filesystems will be created and restored from the backup as defined in the backup information and as previously customized.

More details on the complete installation process are found in the [Install the System](#) chapter below.

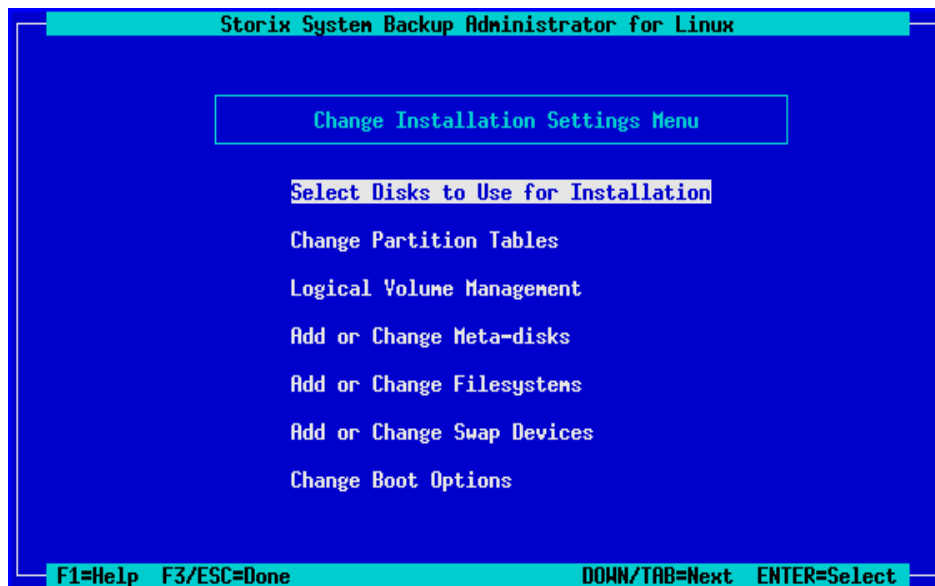
6. View/Change Installation Settings

From the **Main Menu**, select **View/Change Installation Settings**. The first time you enter this option, the backup information will be read from the installation media and compared with the system and disk configuration to ensure there is adequate space on the available disks to perform the installation. Checks will also be made to ensure you booted from boot media that supports all of the devices you will be restoring from the backup. If there are any inconsistencies, you will be required to make changes within these menus to correct the problem.

Note

It is important to note that any options or changes made in these selections have **NO AFFECT** on the actual disks or their contents until **AFTER** you begin the installation. If you change your mind at any time, you can cancel or change information without worry as to the state of the data on the disks!

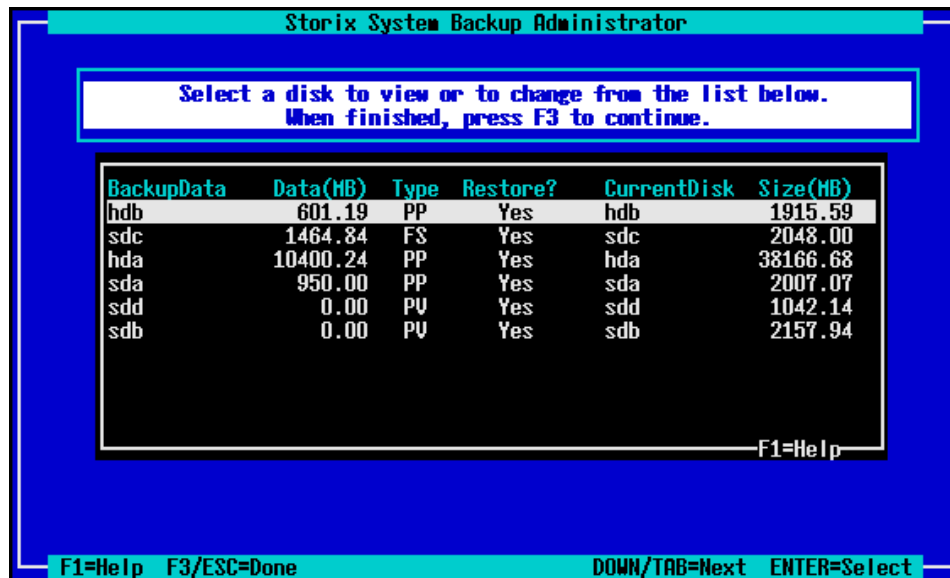
The following is the **Change Installation Settings Menu**:



At times, you may be required to make changes throughout these menus to correct problems that would prevent the devices from being created or the data from being restored. Only after returning to the [Main Menu](#) by pressing **F3** or **ESC**, and selecting to begin the installation, will the data be checked again for consistency and additional changes may be required.

Select Disks to Use for Installation

If the disks detected on the system do not exactly match those described on the backup, this option will appear automatically. Otherwise, you can select this option from the [Settings Menu](#) to display a screen similar to the following. We will refer to this as the **Disk Table Menu**.



Many options are available from this screen for moving data between disks. This is necessary when the disks currently available don't match those defined on the backup, or if you simply want to reorganize the data on the disks for better performance or implement RAID striping or Logical Volume Management (all described later).

To return to the [Settings Menu](#), press **F3** or **ESC**. The backup data will again be checked to ensure you have enough room on the disks for the partitions or other data as you have defined them. If not, you will be warned, but can make changes in this or other settings to fix the problem before the installation is actually performed.

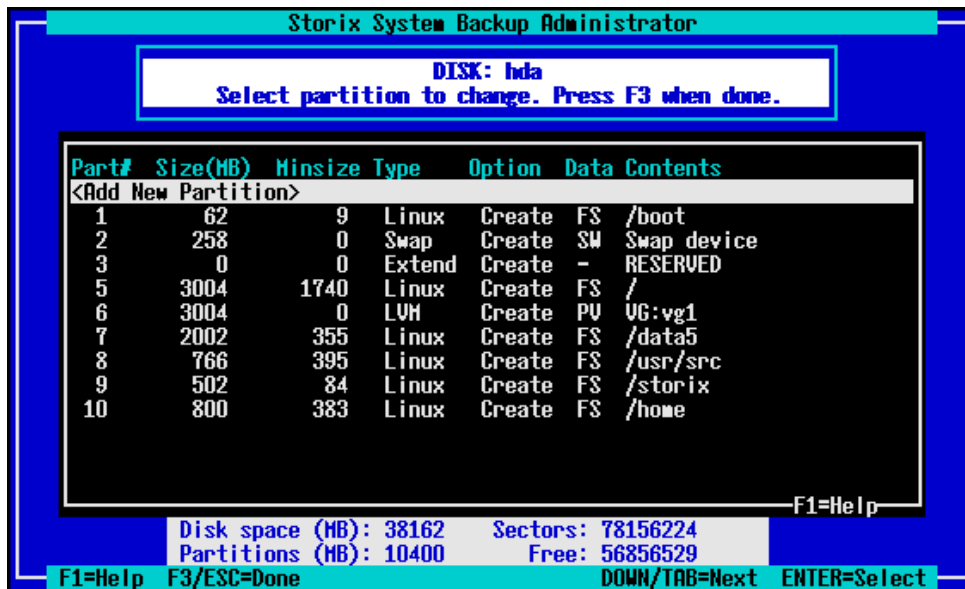
The above screen shows you the original disk the data resided on and the new disk that is assigned that data. There may be previous disks that are not assigned to a new disk, or even additional detected disks that have no data currently assigned to them. By selecting one of the lines on the screen, you are provided several options as shown below:



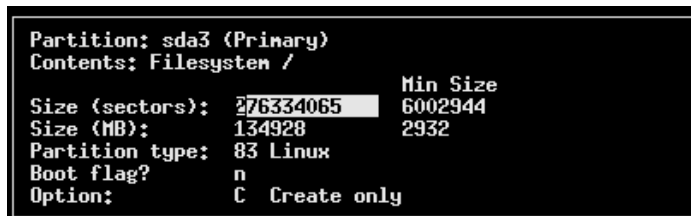
Note that the options for displaying or migrating partitions only appear if the selected disk was previously partitioned or you have chosen to create partitions on it. Each option is described below:

View/Change Partition Table

When selecting this option the partitions on the disk will be displayed as in this example:



You may select to add a new partition by pressing Enter at the highlighted line at the top, or move the highlighted line over the partition you wish to change. When adding a new partition you will be prompted where to insert the partition within the table. Then, when either adding or changing a partition, a window similar to the following will be displayed:



The above screen allows editing of partitions for *MSDOS partition tables*. Most systems only support these partition table types. If you are using an Intel IA/64 system which uses *GPT partition tables*, the options will differ slightly as follows:



You may change any of the options shown. The **Size** of the partition can be set by either entering the number of sectors (512-bytes each) or by entering the number of megabytes. In either case, the other will be adjusted accordingly. You normally will not need to change the **Partition type** or **Partition flag**, even if creating a RAID or LVM device on the partition because the software will automatically do that for you. The **Boot flag** is not used by the software, and need only be changed if the partition contains a non-Linux operating system that requires it. If your backup contains raw partition data, the **Option** will show **Create/Restore**. If you do not want to restore that data, change this to **Create only**.

When finished with your selections, press F3 or ESC to return to the [Change/View Partition Table](#) options.

Assign All Contents of a Disk to a Different Disk

Select this option only if you want to move all of the previously defined backup contents to a different disk. You will then be asked which disk to assign the data to. If you select a disk that is currently assigned other data, you'll be given the option of making the other data unassigned so that you can either move it to a different disk or choose not to restore it.

Migrate a Partition to a Different Disk

If you select this option, the [partition table](#) will be displayed where you can select a partition to be moved to a different disk. You will then be prompted for the location on the new disk to place the partition. If the disk you are moving to currently has no partitions assigned to it, you can select to make the new partition either a physical (partitions 1-3) or logical (partitions 5-16). Note that partition 4 is always reserved for the extended partition, on which all logical partitions are created.

Select Not to Restore Data to a Disk

By selecting this option, you are choosing not to restore the data that is assigned to the selected disk. By doing so, all previous contents will become undefined, and the disk will not be used when installing the system. Any data that actually resides on the disk at this time will not be overwritten.

If selecting not to restore a disk's contents causes any problems which would prevent the installation from being performed (for instance, removing one partition of a striped meta-disk), you will be informed so and required to make additional changes before continuing the installation.

When you have finished all changes press **F3** or **ESC** to return to the [Disk Table Menu](#) and **F3** or **ESC** again to return to the [Settings Menu](#).

Change Partition Tables

This option on the menu is really just a shortcut into the same options available when selecting disks to use for installation. You have the same options of changing partition information or adding new partitions to a disk, but must use the [Select Disks to Use for Installation](#) option to move partitions or other data between disks.

If your system supports both **MSDOS** and **GPT** partition tables, you will be provided the following option:



Select the first option to view or change the existing partition table. Refer to [View/Change Partition Table](#) for additional information. If you select to change the partition table type, you will be asked whether you want the partition table to be MSDOS or GPT format.

GPT partition tables have only one partition format, but MSDOS tables have *Primary* and *Logical* partitions (logical partitions are contained within an *Extended* partition).

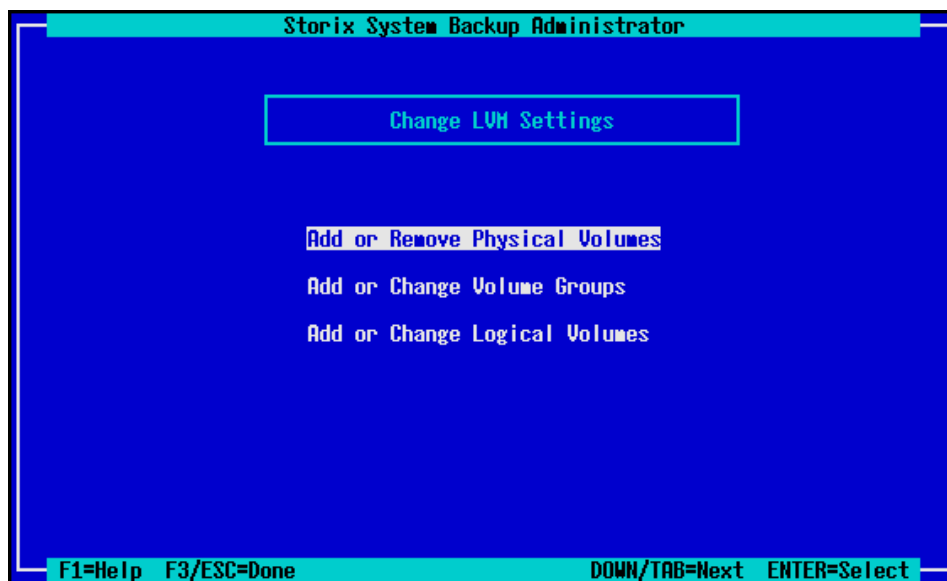
When changing from MSDOS to GPT, the Extended partition (only used in MSDOS tables) is removed and all partitions are changed to a "primary" type. When changing from GPT to MSDOS, the first 3 partitions are converted to a Primary partition, an Extended partition is created as partition 4 (if needed) and additional partitions are created as Logical. After the conversion takes place, the new partition table is displayed where you may change the partition information. Refer to [View/Change Partition Table](#) for additional information.

Logical Volume Management

The **Logical Volume Manager (LVM)** support, included with many distributions, provides the flexibility of logically managing multiple physical disks as one large logical disk. This allows, for instance, a filesystem to be spread sequentially across multiple disks, striped across disks, and the filesystem (contained in a logical volume) does not have to use contiguous segments of disk space. Therefore, you can expand and reduce the size of these containers even if there is not contiguous disk space available. Since LVM support in SBAdmin is quite extensive, we'll provide a quick lesson in LVM terminology, but you should refer to your LVM documentation and the "man" pages for the LVM commands for details:

- **Physical Volumes (PVs):** In most cases, this is the physical disk assigned to LVM, but may also be other types of block devices, including partitions, meta-disks, and other logical volumes. PVs are assigned to volume groups to group them into a single large "logical" disk.
- **Volume Groups (VGs):** This is basically the logical view of a disk, which actually contains one or more physical volumes. A volume group may then be split into smaller units which may be used for storing raw data or filesystems.
- **Logical Volumes (LVs):** Volume groups are broken down into logical volumes, which is similar to a disk "partition". The difference is that the segments making up the logical volumes may actually exist on different disks and do not need to be contiguous. A logical volume may also be "striped", providing added I/O performance by making use of multiple physical volumes concurrently.
- **Physical Extents (PEs):** This is a unit a physical volume is divided into, each in size. A PE may be from 1 Kbyte up to 128 megabytes in size, and is the smallest unit of allocation for logical volumes. A logical volume might be made up of PEs existing on different physical volumes.
- **Logical Extents (LEs):** A logical volume is actually made up of LEs, which at this time is the same as a PE. We refer to PEs when talking of the physical units of allocation and LEs when talking of the logical units of allocation. The reason for the differentiation is for future support of mirrored logical volumes, where a 100 megabyte logical volume, made up of 25 4 megabyte LEs actually takes up 50 PEs (since every LE will be mirrored onto 2 PEs).

When selecting this option from the menu, you will be provided another list of options:

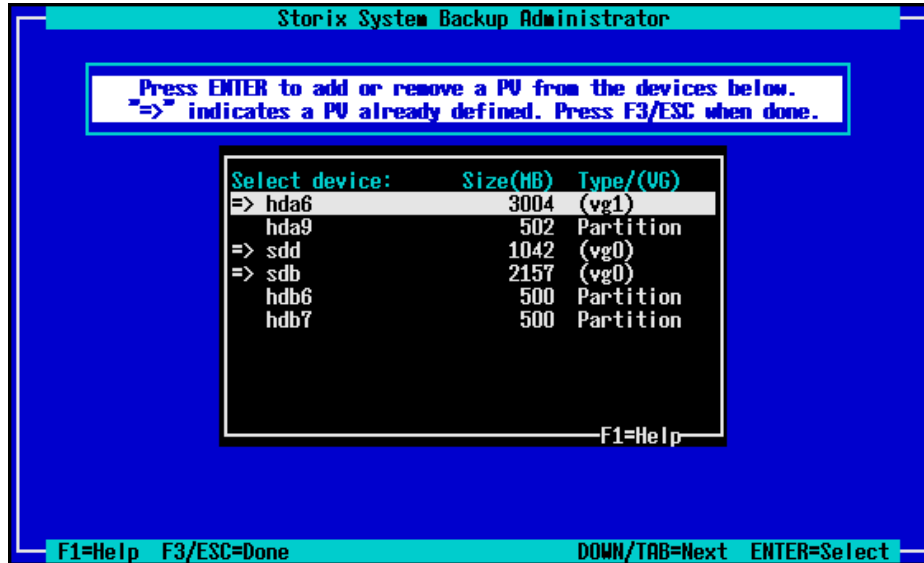


You will note that these options may not only be used to change settings of existing LVM definitions, but also for creating new PVs, VGs and LVs. After refining new logical volumes, you will be able to later either create a new filesystem in the logical volume or even move a filesystem previously residing on a disk partition into a logical volume!

You will also find that physical volumes may be created on meta-disks and meta-disks can be created from logical volumes. This will allow a

Add or Remove Physical Volumes

This option is used to define a block device as a physical volume for use with LVM. When selecting this option a list of potential physical volume devices as well as those currently defined is displayed:

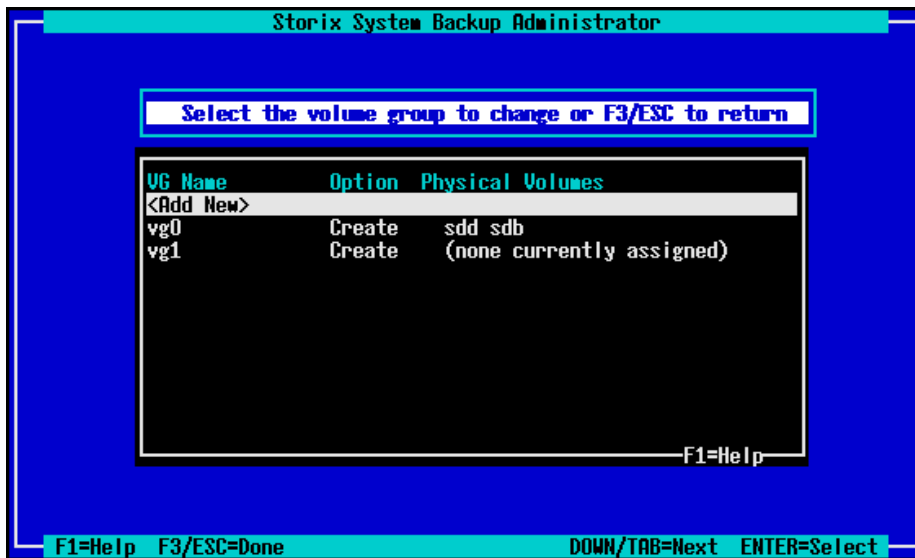


This list will only contain devices, such as *disks*, *partitions* or *meta-disks*, that do not already have other data assigned to them. Those indicated with => are currently physical volumes. You may select any line to either define or un-define this as a physical volume. The **Type/(VG)** column will display either the type of device (it not currently a physical volume), or the volume group name (or none) the physical volume currently is assigned to.

When finished with your selections, press **F3** or **ESC** to return to the [LVM Settings Menu](#).

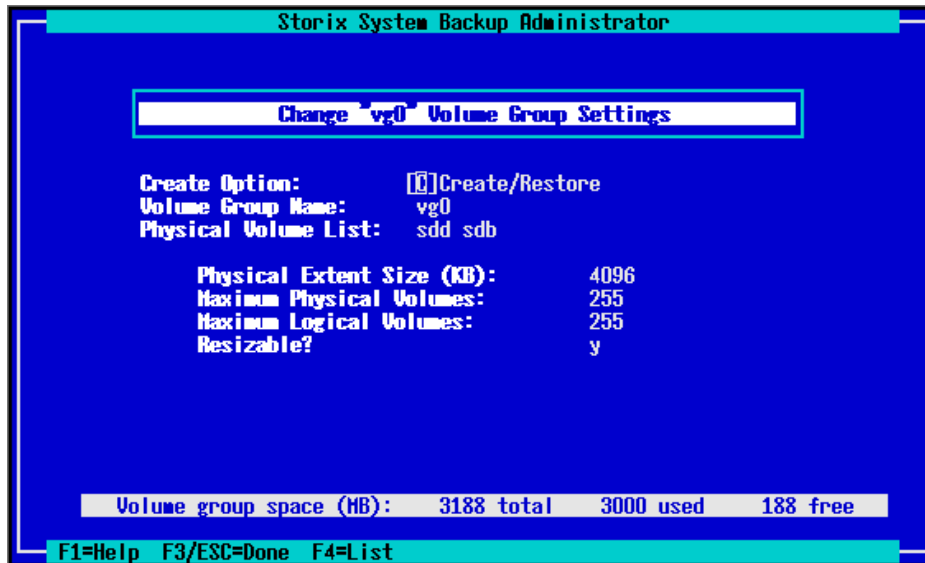
Add or Change Volume Groups

Use this option to change the attributes of a volume group, delete a volume group or to add a new volume group. When selecting this option, a screen similar to the following will first appear:



This will show the currently defined volume groups, if any. If you select the **<Add New>** option at the top, you can define a new volume group. You will be required in this case to have first defined at least one physical volume to assign to the volume group.

After making your selection, the following screen will be displayed:



Remember to press **F1** at any time for detailed help on a particular field. Use **F4** in most fields to display a list of available choices. From this screen you can change the VG name, the physical volumes assigned to the VG, the PE size and other options.

Notice that the amount of space available in the volume group is shown at the bottom, as well as the amount of space used by current logical volumes.

The **Create Option** may be changed to either **"C"** (create) or **"D"** (delete). If you change the option to **Delete**, you will be given warning, and the volume group and any logical volumes assigned to it will be removed. Any physical volumes assigned to it will become available to assign to other volume groups, if any.

If you change the **PE size**, any logical volumes currently assigned to the volume groups will be adjusted to fit. The number of LEs assigned to each LV will change, and in some cases, the LV size may change slightly in order to round up to the new PE size.

To select physical volumes for the VG, press **F4** in the Physical Volume List field. A pop-up window will display similar to the following will be shown:

PVname	VGname	Total MB
sdd	vg0	1042
sdb	vg0	2157
hda6	(free)	3004

F1=Help

You may only select a physical volume that is either currently assigned to this VG (in order to un-assign it), or a physical volume listed as “free”, indicating that it does not belong to a volume group. By selecting the line, the list will refresh showing the PV either assigned or unassigned. Press **F3** to return to the [Change Volume Group](#) screen.

Add or Change Logical Volumes

Select this option to add, delete or change logical volumes. When selecting this option, a screen containing the currently defined LVs is shown:

Storix System Backup Administrator

Select the logical volume to change or F3/ESC to return

LV Name	Size (MB)	MinSize	Contents
<Add New>			
vg0/lvol1	800	12	/data1
vg0/lvol2	200	0	md2
vg0/lvol3	2000	0	md2
vg1/lvol1	800	177	/data2
vg1/lvol2	2000	1978	/data3

F1=Help

F1=Help
F3/ESC=Done
DOWN/TAB=Next
ENTER=Select

Select **<Add New>** to create a new logical volume or select a line containing a current logical volume to change or remove it. The logical volume settings can then be changed on the following screen:



Use the **F1** key for help on any field or the **F4** key to list current choices.

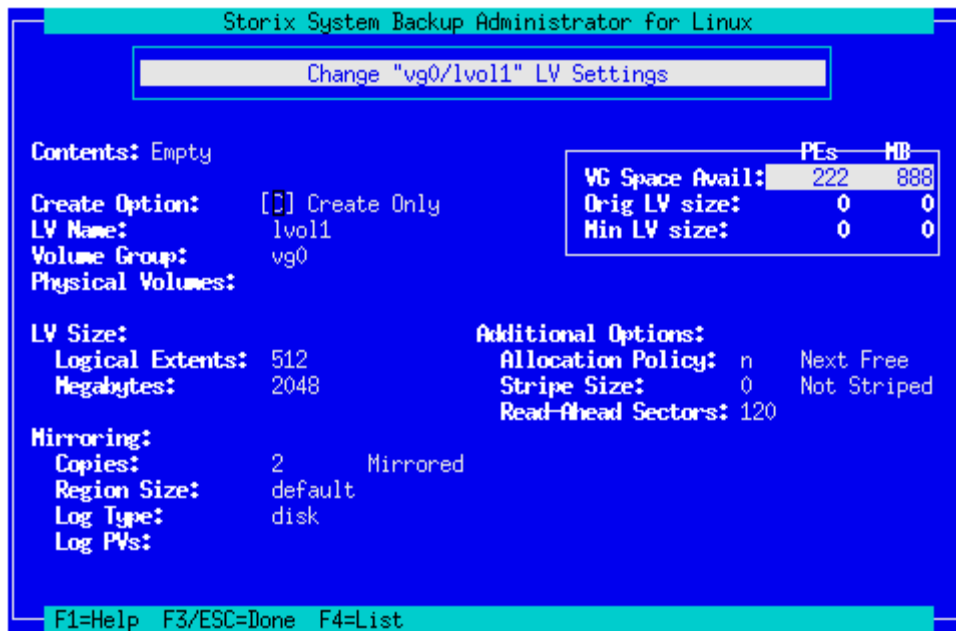
The amount of space available in the volume group, and the minimum LV size (if the LV previously contained data) is shown at the bottom of the screen. These numbers will be adjusted as you change the size of the LV, which may be specified in either LEs or megabytes.

You may also change the name of the volume group the LV is assigned to. Note that this will change the actual LV device name, since the name of the logical volume device is actually `"/dev/VGname/LVname"` (but we of course don't bother you with the `/dev` prefix).

To select the specific physical volumes within the volume group where you want this LV placed, move to the **Physical Volumes** field and press **F4**. It is not necessary to assign PVs to the LV unless you plan to stripe the LV or you have a desire to specify its location (you may want 2 LVs that perform different I/O workloads located on different PVs, for example). A window will pop up showing the physical volumes currently assigned to the volume group, and you can select or deselect PVs from the list.

Note that you must select at least 2 PVs when you choose to stripe the logical volume data across PVs (by setting the **Stripe Size** value to any non-zero value).

If you select to have more than 1 **Copies** then you are utilizing **LVM mirroring** and additional options will become selectable as follows:



When finished with your selections, press **F3** or **ESC** to return to the list of LVs, and F3 or ESC again to return the [Change LVM Settings](#) menu.

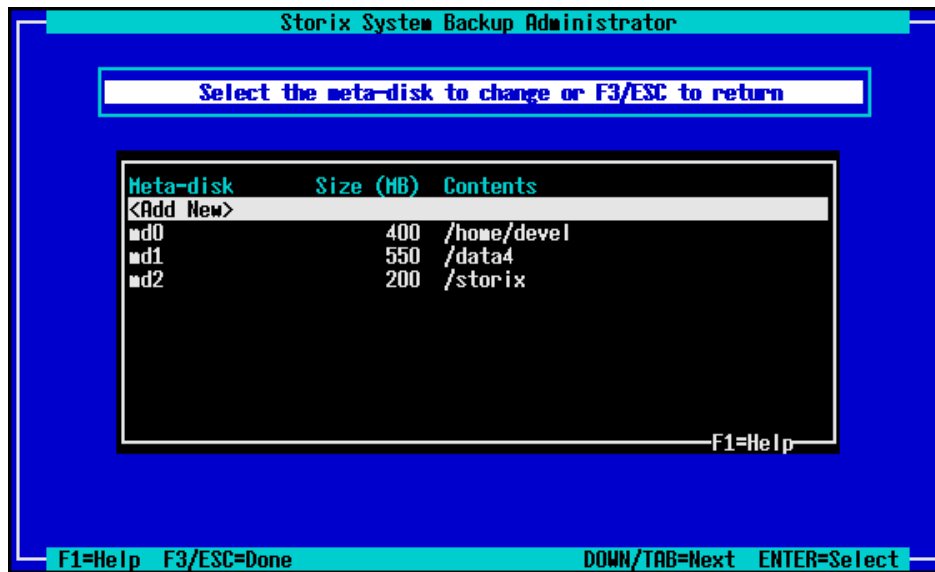
Add or Change Meta-disks

Use this option to add a new meta-disk (software RAID device) or to remove an existing meta-disk or change its attributes. Details on the use of meta-disks can be found throughout the Linux documentation as well as in the **mkraid** and **raidstart** command *man* pages. A brief description is provided here.

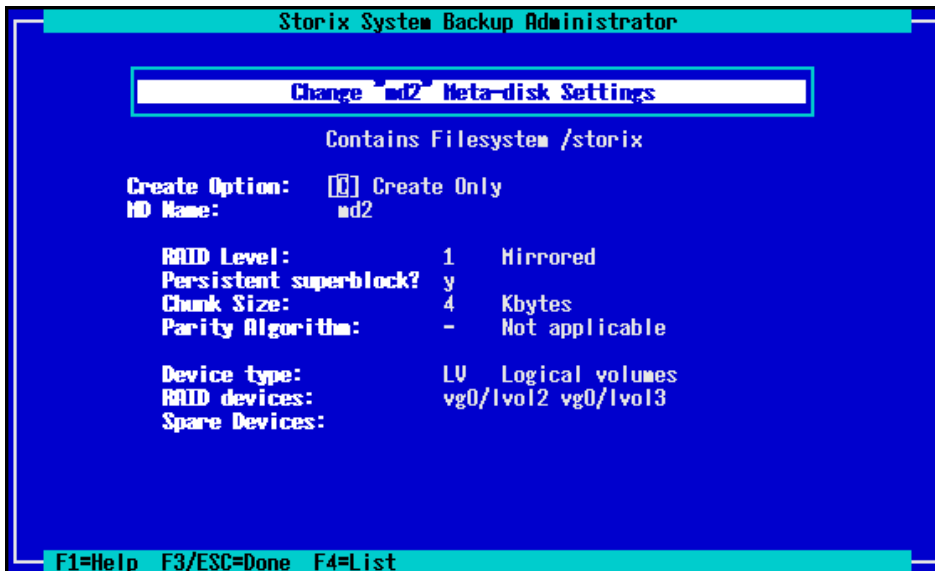
A meta-disk provides various levels of software RAID, otherwise referred to as "RAID levels". The levels are defined as follows:

- 0 (Striping)** Data is striped across 2 or more physical devices for better performance.
- 1 (Mirroring)** Identical copies of the data is stored on two or more physical devices.
- 5 (Striping/parity)** Data is striped across 2 or more physical volumes, and an additional disk is used to contain parity information, which itself is striped across the disks.
- 9 (Linear)** OK, "9" was of our own choosing since we wanted to use a number for consistency. Linear means that there is no striping or mirroring, but multiple devices can be combined sequentially to provide a single larger-sized device.

When selecting this option you are first provided a list of meta-disks currently defined, if any, and an option to **<Add New>** meta-disks:



In any case, your next selection will take you the screen for adding, changing or removing meta-disk definitions as follows:



From this screen you can choose to **Create**, **Create and Restore**, or **Delete** a meta-disk. The option to **Create/Restore** is only available if this is a meta-disk whose raw data contents were included on the system backup. The **MD Name** must begin with "md" and is followed by a number between 0 and 31.

Specify the **RAID Level** as described above, keeping in mind the minimum number of devices that must be assigned to this meta-disk to accommodate the RAID level.

Information on the other options may be displayed by pressing the **F1** (help) key. For a list of selections for a particular field, press the **F4** key.

The **Device type** may be one of **DISK** (for whole disks), **PP** (for partitions), **LV** (for logical volumes) or **MD** (to build the meta-disk on other meta-disks). The **RAID devices** field may only be filled in with devices of the type. Press **F4** in the **RAID devices** field to list the devices available (of the type specified in the **Device type** field) and select from the list as shown:

Device name	Size (MB)
=> vg0/lvol2	200
=> vg0/lvol3	2000

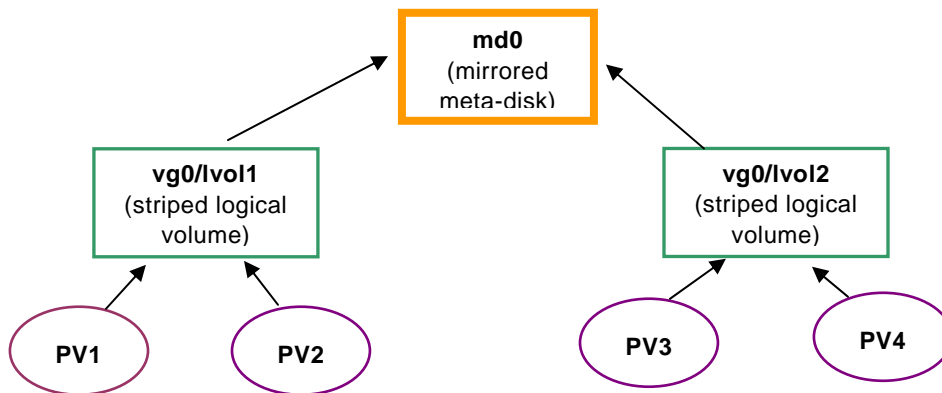
F1=Help

The example above shows logical volumes to be assigned. Note that the LVs shown are of varying sizes, which is not recommended for striped or mirrored meta-disks, since the maximum amount of space available would be that of the smallest disk (times the number of disks). This will work fine for linear meta-disks, however.

When finished with your selections, press **F3** or **ESC** to return to the [meta-disk list](#), and **F3** or **ESC** again to return to the [Change Settings](#) menu.

RAID 0+1

RAID 0+1 is both striping and mirrored. It means building a mirrored RAID device from striped RAID devices. Since mirroring usually causes I/O performance degradation, this design is typically used to get normal disk I/O performance while still having mirrored (redundant) data. Since both **Logical Volumes** and **meta-disks** can stripe data, and they are both block devices, they can both be used to build a mirrored meta-disk! Here's an example:



The **logical volumes** are striped across multiple physical volumes (PV) and then your striped logical volumes are combined into a mirrored meta-disk. This means that as data is written to the meta-disk (**md0**), an identical copy is written to both logical volumes **vg0/lvol1** and **vg0/lvol2**. Those logical volumes each stripe the data across 2 of the 4 physical volumes assigned to them, alleviating much of the performance hit taken by mirroring in the first place.

Refer to the [LVM Settings](#) section for more information on **logical volumes**.

Add or Change Filesystems

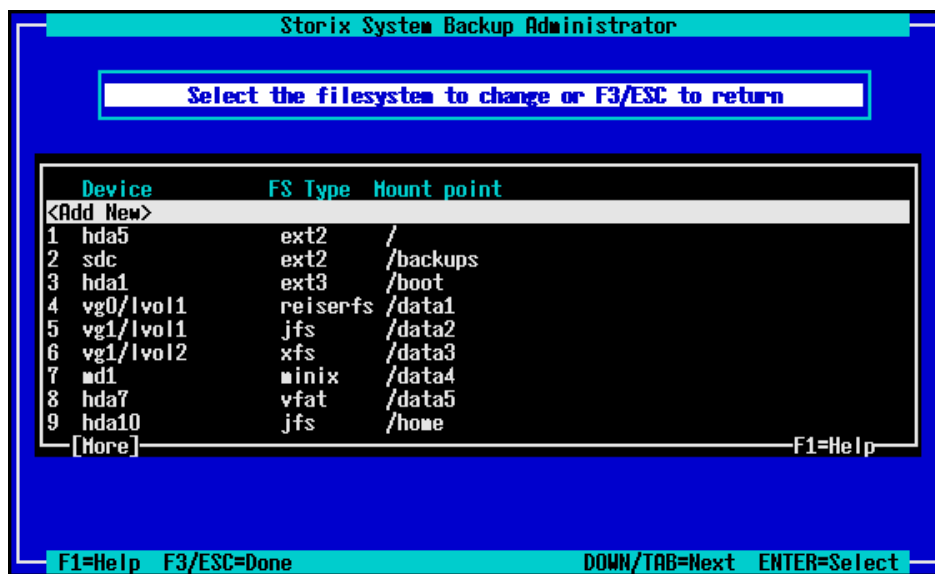
This option may be used to change any of the settings for the filesystems, which vary depending on the filesystem type. SBAAdmin supports the following most popular filesystem types at this time:

- ext2** Linux Second Extended
- ext3** Linux Journalled Third Extended
- ext4** Linux Journalled Fourth Extended

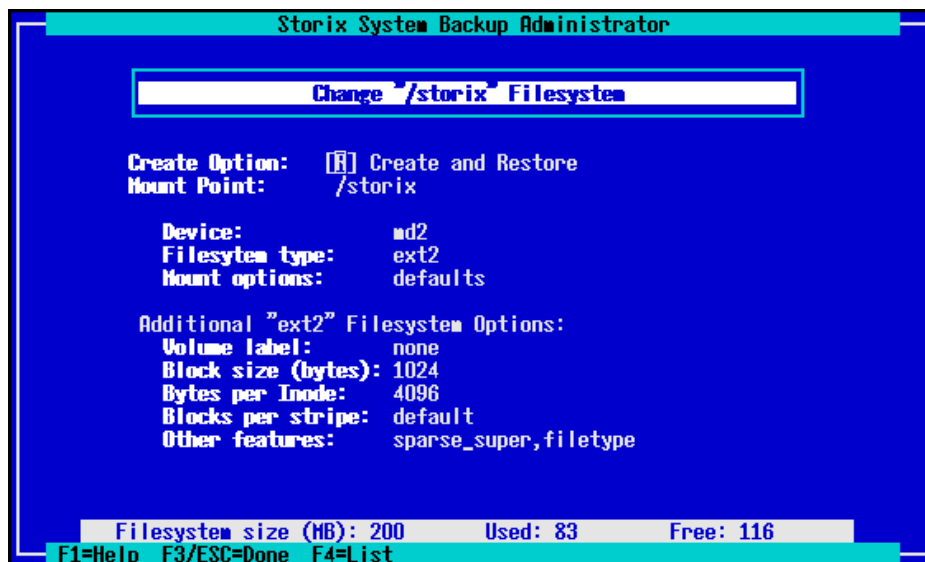
reiserfs	Reiser Filesystem
btrfs	Btrfs Filesystem
jfs	IBM Journaled Filesystem
xfs	SGI Extended Filesystem
vfat	MSDOS/Windows FAT Filesystem
minix	Old Linux Filesystem
msdos	MS/DOS FAT12 Filesystem

Virtually any of the attributes which are available for the filesystems above can be set or changed from the menus. Since some filesystems provide advanced features and performance not previously available on, for instance, an **ext2** filesystem, you can simply change the type of the filesystem to take advantage of the new features. You can even select external devices to use for journaling **ext3**, **ext4** and **xfs** data, adding performance by placing the journal on a separate disk than the filesystem.

When you select this option you will receive a list of filesystems currently defined:



Select **<Add New>** to add a new filesystem. You will be required to specify the new mount point, or directory, for this new filesystem. Then, the following options screen will appear:



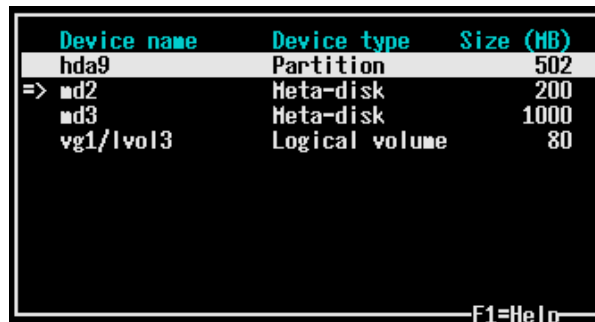
The options displayed here are for an “ext2” filesystem. If you change to a different filesystem type, the options will change as well. We won’t describe the options in detail since you have much information available with the F1 (help) key. Also use the F4 key to show lists of available options.

The options common to all filesystems are:

Create Option – Here you can specify to **Create the filesystem only**, **Create it and restore the data**, or **Delete** it. Although the filesystem data may be on the backup, you can choose to create the filesystem without actually restoring the data into it.

Mount point – You can change the directory where the filesystem will be mounted. The data is restored relative to this directory, so the contents, if any will not change. You cannot change the mount point of the root (/), /boot or /usr (if any) filesystems.

Device – Here you can select a new device where the filesystem should be created and/or restored. Possible filesystem devices are whole disks, partitions, mate-disks and logical volumes. When pressing F4 at this field, you will get a list of any devices that are not already assigned data as follows:



Device name	Device type	Size (MB)
hda9	Partition	502
=> md2	Meta-disk	200
md3	Meta-disk	1000
vg1/lvol3	Logical volume	80

Filesystem type – Here’s where you can select the type of filesystem to create. Only the filesystem types supported by BOTH the boot media and the backup to be restored will be selectable within this field. Changing this field will change the options while appear in the **Additional options** section below.

NOTE

Only filesystems supported by the boot loader will be available for the *root* filesystem UNLESS you have a */boot* or */yaboot* filesystem. In that case, the */boot* or */yaboot* filesystem will be limited to filesystem types supported by the boot loader.

Mount options – Pressing **F4** at this field will display a lengthy list of mount options which apply to all filesystems as well as additional mount options specific to the selected filesystem type. You can combine them in most cases, and some options, when selected, will prompt you for additional input. In most cases, you can use “default”. Don’t change these unless you know what you’re doing.

Additional Options – Various options such as *block size*, *fragment size*, *external journal device*, *label id*, etc, will appear, based on the **filesystem type** selected. The options vary for each filesystem, and the list of available selections under each option will also vary depending on both the filesystem type and the other options selected.

External Journals

Some filesystem types provide the ability to use external journals. In this case, you can select another device (same type as the filesystem itself) where the filesystem metadata will be journaled. Since journaling the metadata can be a bit of a performance hit, this allows you to keep the journal on a separate disk than the filesystem itself to ease the I/O workload.

Minimum Filesystem Size versus Device Size

The minimum filesystem size displayed in various places in the menus is the size of the data in the original filesystem that was backed up. The size of the device may have to be quite a bit larger depending on the amount of space the filesystem metadata and journaling requires.

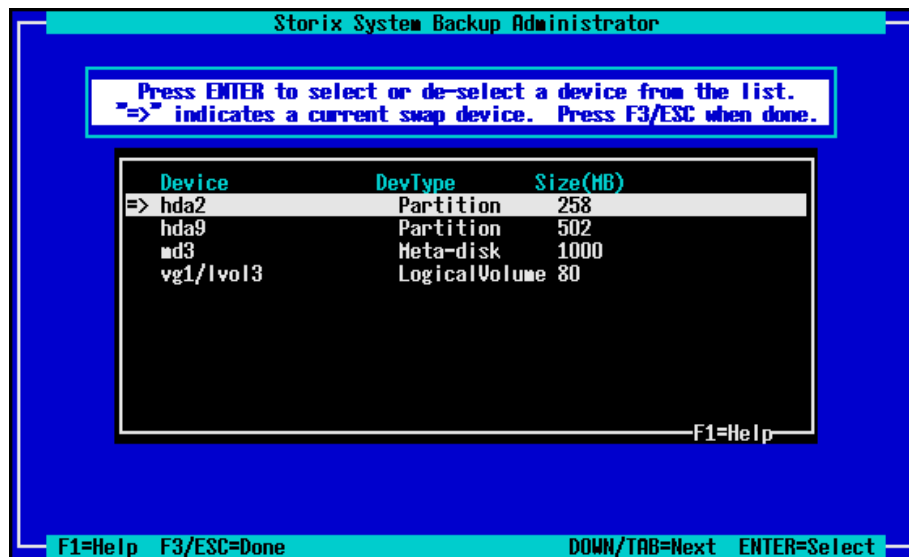
The journal size can be specified in some cases. We generally recommend using the default size, which varies by filesystem type. If you change the journal size, more or less room in the device itself will be taken up by the journal. The size of the journal also varies in most cases based on the size of the filesystem.

SBAAdmin tries to keep track of the minimum size of the device based on the amount of data to be restored, and this calculation varies based on the filesystem type, the journal size, and many other options that are configurable here. If you change any of the options, such as the **number of inodes** in a filesystem, be sure you have plenty of free space available (based on the size of the device) in case the change requires more space than the filesystem previously needed.

After you have finished making changes, press **F3** or **ESC** to return to the [filesystem selection screen](#). Press **F3** or **ESC** again to return to the [Change Settings](#) menu.

Add or Change Swap Devices

Use this option to select the device or devices which should be used as swap devices (also known as *swap space* and *paging space*) on the system. Any raw device, including *partitions*, *logical volumes*, or *meta-disks* may be used for swap. When selecting this option, a screen similar to the following will appear:



If an arrow (=>) appears next to a device, then that device is currently configured as a swap device. To select a device, highlight the desired line and press **Enter**. If you do not want to use that device for swap, press **Enter** and the arrow will disappear. This device will not be used, and may be instead used for other features, such as filesystem data.

After you've completed your selections, press **F3** or **ESC** to return to the [Change Settings](#) menu.

Change Boot Options

This option will allow you to select or change the boot loader that will be used to boot the system after the installation completes. By default, the boot loader used on the original system when the backup was made will be used (if it could be determined at the time of the backup). Refer to [Boot loaders](#) for additional information.

When selecting this option, a screen similar to the following will appear:



Each option is described below:

Boot loader – Press **F4** to select the boot loader to use. The only options provided are those available on the system and appropriate for the system type. The **LILLO** boot loader will always be available for *Intel 32-bit-based* systems, **ELILO** for *Intel-based* systems that boot from UEFI, and the **Yaboot** boot loader will be the only available option for *IBM System p and System i* systems.

Boot device – Press **F4** to list and select the name of the boot disk. For **LILLO** and **Yaboot**, this will always be the disk containing the boot filesystem. For **GRUB**, it can be any disk on the system (and need not contain the [boot filesystem](#)). The boot disk must be a disk containing a **partition table**. The boot device (disk) is the device you must later set your system firmware to boot from after the installation completes.

Kernel options – This field will display the kernel options used to boot the system when the backup was made. Some options specific to the boot process that do not apply will be removed after restoration of the system. You may change the options that are passed to the kernel from the boot loader by editing this field. Anything you enter in this field will be available to the kernel and the system boot process, whether valid or not.

Console type – This field indicates if the system console will be a *graphical* display or a *serial* (ASCII/text) terminal. This field is filled in with the console type you booted from.

Console device – This field indicates the name of the device to use as the system console. The default will be the console device you booted from if known, “tty0” for graphical displays or “ttyS0” for serial terminals.

Terminal type – If using a serial terminal, you should specify the terminal type in this field. If you booted from a serial terminal you were asked to select a terminal type during the boot process, and this terminal type will be the default. You may set this to the terminal type that should use used after logging into the system console after system startup.

Also, refer to The [Boot loader](#) in **Making the System Bootable**. When you've completed your selections, press **F3** or **ESC** to return to the [Change Settings](#) menu.

7. Install the System

To install the system from the [SBAdmin System Backup](#), you first must have selected the [Installation Device](#) (which may be located on a local or remote host). You then have the option [View/Change the Installation Settings](#), where you can make any changes to the backup information stored on the backup media. If you used that option, then the backup information was already restored from the backup, verified and modified as needed to ensure the installation can be started.

Verification Process

If you select the option **Install the System with Current Settings**, this backup data will be checked (again if necessary) to ensure the defined devices and filesystems can be created successfully. Here are a few things that are checked:

1. The devices and filesystems defined on the backup are checked to ensure the kernel and modules available from the boot media are adequate to create them. This includes ensuring that LVM and the various RAID levels are available if required.
2. Ensures any backup data previously residing on a disk is assigned to a new disk unless the user explicitly chose not to restore data.
3. Verifies that all devices assigned to meta-disks are valid and that there are enough devices assigned for the appropriate RAID level.
4. Verifies that the physical volumes assigned to both volume groups and logical volumes are valid.
5. Checks that volume groups are large enough to hold the logical volumes defined.
6. Verifies physical volumes assigned to logical volumes are adequate for striping, if defined.
7. Validates the partition table and automatically adds an extended partition if needed to allow future expansion into logical partitions. This is important also since the backup may be installed onto larger disks, and using all primary partitions would prevent the ability to expand onto them.
8. Verifies that partitions will fit onto their respective disks and that primary partition sizes are defined at disk track boundaries (in case the disk geometry has changed).
9. Checks that all filesystems are being created on devices large enough to restore the data. Even if a device has not changed, the requirements may change if, for instance, the filesystem type was changed to one which requires more space for filesystem metadata than was previously needed.
10. Verifies that the root filesystem is being restored and the device on which it is defined is still valid.
11. Verifies that the configuration conforms to boot loader requirements of the specific system type.

If any problems are detected, you will be informed of the problem and a recommended solution. In some cases the process will offer to fix the problem for you. If problems persist, you will need to return to the [Change Settings](#) menu to make any changes required to restore the data.

Starting the Installation

If all checks out, you are given one final warning:

```
!! YOU HAVE SELETED TO INSTALL THE SYSTEM !!

If you continue, all disks selected for the
installation will be overwritten!

Are you sure you want to continue with the system
installation? (y/n) 
```

Press “y” to continue the installation or “n” to return to the [Main Menu](#).

If you choose to continue the install, the system will begin by reading additional information from the backup media, then creating the devices and filesystems that are defined. Devices are created in the correct order so that meta-disks created on logical volumes, for instance, are created after those logical volumes they depend on, etc. After the devices are created, all filesystems are created and mounted.

If the backup was *encrypted* when it was created, you will be asked to enter the *encryption key* to decrypt the data during the installation. If the correct key is not entered, you will not be able to continue the installation. Refer to [Installing from an Encrypted Backup](#) for more information.

As the data is restored from the backup, a progress indicator will appear showing the status of the restore including the estimated amount of data and time to completion. When all data for included on the backup is restored, the system will perform some cleanup and post-installation processing and attempt to make the system bootable.

Configuration Files

During the installation, a copy of any former configuration files that were modified by the installation will be saved into the **STXPATH/temp/storix_install** directory (where STXPATH is the Storix data directory of the target system). This will include system files modified during the installation process, such as the */etc/fstab*, */etc/raidtab* and */etc/lilo.conf* files (if used). You should examine these files and compare to the modified files to verify the changes.

Making the System Bootable

When all data is restored and the installation processing is complete, the final, and very important step, is to make sure the system will now reboot successfully.

The Boot Loader

SBAAdmin uses one of the following as the **boot loader** to configure the system for boot-up, depending on the system type:

1. For *Intel-based* systems, SBAAdmin uses either:

GRUB – If the system previously had GRUB configured, a copy of the original GRUB configuration files **grub.conf**, **menu.lst**, and **device.map** will be copied into the **STXPATH/temp/storix_install** directory (where STXPATH is the Storix data directory). The **grub.conf** file will be modified to add the new boot configuration as the default system to boot from.

GRUB2 – If the system previously had GRUB2 configured, a copy of the original GRUB configuration files */etc/default/grub*, */etc/grub.d/01_** will be copied into the **STXPATH/temp/storix_install**

directory (where STXPATH is the Storix data directory). A new GRUB2 boot option configuration file `/etc/grub.d/01_storix` will be created.

LILO – If GRUB or GRUB2 are not being used, LILO will be used instead. If there was a previous configuration in the `/etc/lilo.conf` file, that configuration is saved to the `STXPATH/temp/storix_install` directory (where STXPATH is the Storix data directory). A new stanza with the boot configuration will be added to the prior `lilo.conf` file, if any, or if the previous file was invalid (or unused) a new file will be created with only one stanza used to boot the system. If a previous file existed, the original copy will be saved in the `STXPATH/temp/storix_install` directory (where STXPATH is the Storix data directory).

ELILO – Systems that boot from UEFI firmware with use the ELILO boot loader. The boot loader configuration file used by ELILO is `elilo.conf` and will be found in the VFAT filesystem used as the boot filesystem (typically `/boot/efi` or a subdirectory of `/boot/efi`). If the system previously used ELILO, the original version will be copied to `STXPATH/storix/storix_install` (where STXPATH is the Storix data directory) before it is changed.

2. For IBM POWER (System p) and System i systems

Yaboot - SBAAdmin does not use the utilities that accompany this boot loader, as they differ greatly between distributions. Instead, SBAAdmin creates its own `/etc/yaboot.conf` file, then copies the yaboot boot loader (`yaboot.chrp`) to the **PREP Boot or FAT16 partition**. If a previous `yaboot.conf` file existed, it will be copied to the `STXPATH/temp/storix_install` directory (where STXPATH is the Storix data directory) before being changed.

Refer also to the [Boot loader](#) section.

Initial Ramdisk Image

SBAAdmin will attempt to determine if any device support is required to mount the root filesystem that is not already built into your kernel. This may include various filesystem support, LVM commands and modules, or software RAID commands and modules. If it is determined that required device support is not built into the kernel, then an Initial Ramdisk Image (`initrd/initramfs`) is automatically created.

The `initrd/initramfs` image will contain the device support modules and programs, and a script for loading and initializing the modules. The `initrd` is loaded by the kernel prior to mounting the root filesystem. Therefore, the `initrd` will initialize any support needed to mount the root filesystem

The /boot filesystem

Boot loaders must be able to access information restored to the system during startup. This information is contained in the **/boot directory** (or sometimes `/yaboot` or `/boot/efi`) of a filesystem. The `/boot` directory may be in the **root (/)** filesystem or may be its own filesystem. We'll just refer to it as the "boot" filesystem here.



The system recovery process will verify that your system configuration, boot loader and boot device are valid and will require you to make changes as necessary in the installation menus. In the installation menus, you will only be able to make selections that are valid, based on your system type, boot filesystem type, and support available on your system. The menus will also recommend creating a separate `/boot` filesystem when necessary.

The boot filesystem must be of a type that the boot loader recognizes. **LILO**, for instance, must map the physical disk blocks that make up the boot configuration files, kernel and `initrd` image. To do so, it must know the filesystem format. **Yaboot** and **GRUB** boot loaders must be able to mount the boot filesystem in order to find the configuration file, kernel and `initrd`. In any case, the boot filesystem must be a filesystem type that the boot loader supports. **ELILO** must be on a VFAT type filesystem and the partition must be marked with the boot flag.

Intel 32-bit (BIOS) systems using LILO or GRUB: In addition, the boot filesystem must be in a **primary disk partition (1-4)**, not in an **LVM logical volume** or a **striped software RAID (meta-disk)** device.

Intel 64-bit (UEFI) systems using ELILO: In addition, the boot filesystem (/boot/efi) must be a VFAT filesystem on a partition with the boot flag set. This may be either GPT or MSDOS partition table, but it is recommended that the boot filesystem is on the first partition of the boot disk.

IBM System p and System i using Yaboot: These systems require that you have a **PRéP boot** (type 41) or FAT16 partition on the boot disk, into which the **yaboot** boot loader is copied. When using a PRéP partition, be careful to make this partition small (< 10 MB) since the entire partition is read into memory. The boot filesystem must also be in a primary (1-4) partition on the same disk, and contain an ext2, ext3, reiserfs or xfs filesystem.

It is sometimes advantageous to have the **root (/)** filesystem in a striped logical volume or software RAID, or be a **Reiserfs** filesystem, for instance. For this to be possible, you cannot use the root filesystem as the boot filesystem. Therefore, you can create a **/boot** (or **/yaboot** or **/boot/efi**) filesystem in addition to the root filesystem. This will become the boot filesystem, and may be of a size only large enough to contain the boot configuration files, kernel and initrd images. Since the root filesystem is no longer part of the boot process, there are no limitations on the type of container (LVM, RAID, partition, etc) of the root filesystem, or its filesystem type.

If these conditions are met, SBAAdmin will create this filesystem during the system install process and use it to store the boot configuration files, kernel and initrd image required to mount the "real" root filesystem. With all of the information and files required by the boot loader existing in this filesystem there are no longer ANY limitations on what device or filesystem the root filesystem can be created on!

Refer to the [Boot loader](#) section for additional information on each boot loader's requirements.

Doing it yourself

In some cases, SBAAdmin may not be able to determine what device support is required or already built into the kernel. Therefore, at the end of the installation process, you are placed in a prompt (assuming this is not a **no-prompt installation**), where you can use your own commands for configuring a different boot loader as needed. At this point, you are given a message similar to the following:

```
=====
                THE SYSTEM HAS BEEN RESTORED SUCCESSFULLY!
=====
LILO has been configured as the boot loader. If you want to use a
different boot loader or require additional configuration prior to
rebooting the system, you may do so now.

The LILO boot configuration file is /etc/lilo.conf. Your original
lilo.conf, if any, has been saved as /storix/temp/storix_install/lilo.conf.
-----
Please remove any boot media and be sure the
system firmware is configured to boot from "sda".
-----

=====
When done, type "exit" to complete the installation process and reboot.
sh>
```

At this point, if no change is required, just type "exit" to allow the system to reboot. If you want to make changes, you can manually update your boot loader configuration or install a different boot loader. This will override the boot loader configuration that SBAAdmin applied. If you want to revert back to the original boot loader configuration that was overwritten by SBAAdmin, the original copies of the config files are located in the **/storix/temp/storix_install** directory (assuming /storix is the data directory on client). Be warned however that the SBAAdmin configuration has taken into account any changes to the system to ensure it will boot after the restore. **The previous configuration may no longer be valid.**

Only when you are sure you have correctly applied the boot configuration should you type “exit”. Once you do so the system will be rebooted normally.

Installation Errors

If any error occurs in creating the devices, creating or mounting the filesystems, or restoring the data, you will be provided a message containing the details and the failing command and asked to correct the process manually before continuing the installation. At this point you are placed at a shell prompts where you can diagnose and correct the problem. The command which failed must be completed before the installation can continue successfully. When the problem is corrected, type “**exit**” to exit the shell and continue the installation.

System Boot Problems

The SBAAdmin installation process does its best to prevent you from making any changes that might prevent the system from booting. For example, you are not allowed to put the /boot filesystem on a logical volume since boot loaders can’t read the boot configuration or kernel from a logical volume.

The most common boot problem after an install is simply that your system firmware is trying to boot from the wrong device. First remove any removable boot media from the system and try again. If you changed the disk containing the /boot (or root if no /boot) filesystem, you may need to tell your firmware to boot from the new disk. Each firmware used has different menu options and even names the disks differently, so you will have to refer to your system documentation for details.

SBAAdmin takes care of ensuring that all devices, LVM and/or software RAID are running if they’re needed to access the root filesystem. Once the root filesystem is available, control is turned over to the normal system initialization procedures. Any errors that occur at this point will not usually render the system unusable, but may require additional customization (beyond the scope of SBAAdmin) to restart all system processes in the correct order.

Should all else fail, at least we know that the system has been configured and restored successfully, so we just need to figure out how to get it to boot. Your SBAAdmin Boot CDROM can help. You can boot from the CDROM, and when the menus appear, select “[Enter a Maintenance Shell](#)”. At this time, you can attempt to mount your root filesystem manually. Once you have successfully mounted the root filesystem, you can chroot to that filesystem and attempt to correct your boot configuration.

Should any system, even when changing the disk configuration, not startup at the end of the installation process the same as the original system, you should report the problem to Storix immediately. With the vast number of Linux distributions changing daily, it’s virtually impossible for Storix to test every scenario. However, we will do our best to ensure that your system gets up and running!

Network Re-configuration (avoiding conflicts)

If the system is reinstalled from a remote install serve or from local NFS mount (except Workstation Edition), you entered the client IP address when either booting the system, or when selecting to restore from a remote server. In either case, the client IP address entered will be used to reconfigure the network adapter information restored from the backup. In addition, any additional network adapter configurations restored from the backup will be disabled on reboot.



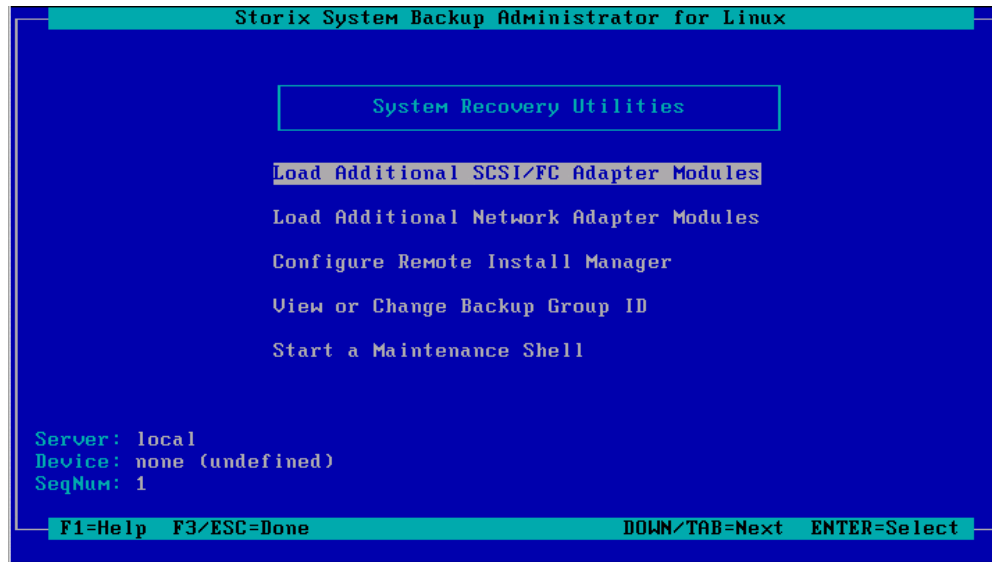
This behavior may be prevented by selecting to not apply the network configuration to the restored system when configuring the network settings.

This is handy when a single backup is used to reinstall multiple clients, as each client will then reboot with its own customized network configuration, regardless of what was on the backup. Network adapters not used during the installation are disabled on reboot to prevent any duplicate IP addresses (i.e. this system and that of the original client the backup was taken from).

If, however, you installed the system from local boot media (CDROM, tape or hard disk), the new network configuration, if different, is not known. It is assumed that the backup being restored came from the same system, and the network configuration is unchanged. Therefore, when the system reboots at the end of the install, it the network will configure with the original settings restored from the backup. If the backup contains IP addresses used by another system on the network, you should unplug the system from the network to prevent IP address conflicts until you have changed the network settings on the newly restored system.

8. System Recovery Utilities

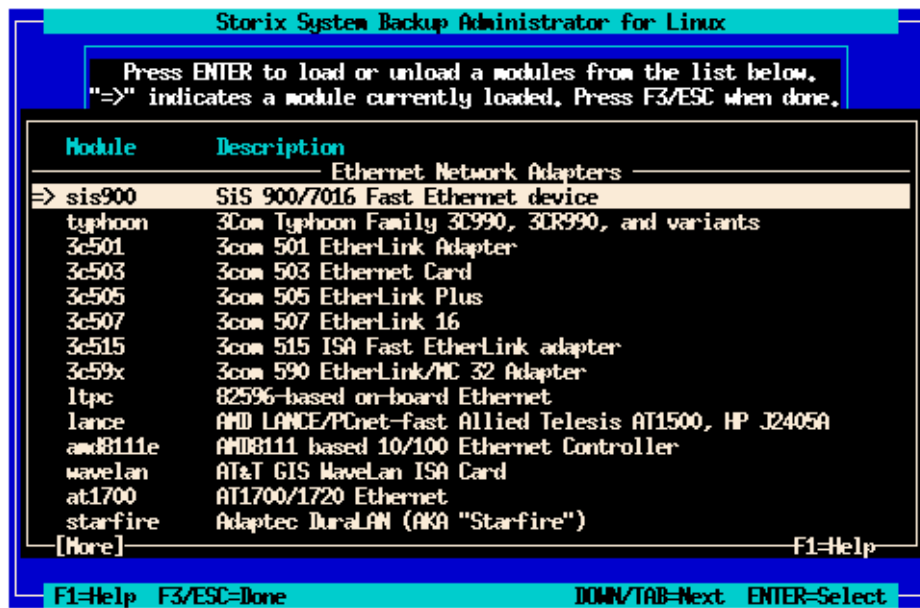
From the [System Installation and Maintenance Main Menu](#), select **System Recovery Utilities** to display the following options:



Load Additional Device Adapter Modules

This option is used to load *SCSI*, *Fibre-channel* or *Network* adapter modules that were not automatically loaded when the system was booted from the media. While most necessary modules will be detected and automatically loaded, if you are installing onto a different system with different adapters, it may be necessary to load additional modules before all devices are detected.

For SCSI and Fibre-channel storage adapters, select **Load Additional SCSI/FC Adapter Modules**. For networks, select **Load Additional Network Adapter Modules**. As with the following (Network) example, a list of available modules and their descriptions will appear:



An arrow (=>) will appear next to the device modules that are currently loaded on the system. If you highlight and select a line for a module that is not currently loaded, a message will appear indicating that the module is being loaded. If the module is loaded successfully and new devices (or adapters) are detected, a message will appear showing you the names of the configured devices. If no new devices are detected, the module will be unloaded automatically and a message to that affect will appear on the screen.

If you highlight a line containing an arrow and press enter, you will be informed that the module is currently loaded and asked if you want to unload the module. Note that unloading a module may cause devices currently configured to become unavailable (i.e. disk or tape drives), and some modules may not be unloaded if they are currently in use (i.e. network adapters for active networks).

When you have finished your selections, press **ESC** or **F3** to return to the [System Recovery Utilities menu](#).

Start a Maintenance Shell

Select this option to start a maintenance shell where you may perform various operations for performing system maintenance or recovery such as mounting and repairing disk filesystems, or reconfiguring the disk boot loader.

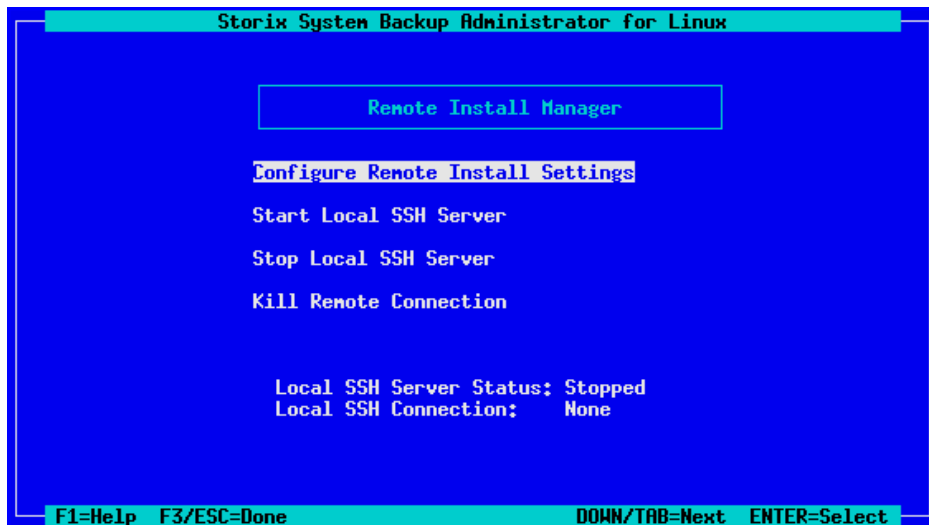
When entering the shell, no disk filesystems will be loaded, and only the command set available on the boot media for system recovery are available. The user will need to perform the manual tasks needed to mount the root (/) or other filesystems if access to the data stored on the disks is desired. The commands and options for doing this vary much too widely to be discussed here, as some filesystems reside in LVM, others are made from RAID devices, etc.

When you have finished the system maintenance tasks, you may reboot the system from the command line, or, if you wish to return to the system installation process, you may type **"exit"** at the prompt to return to the menus.

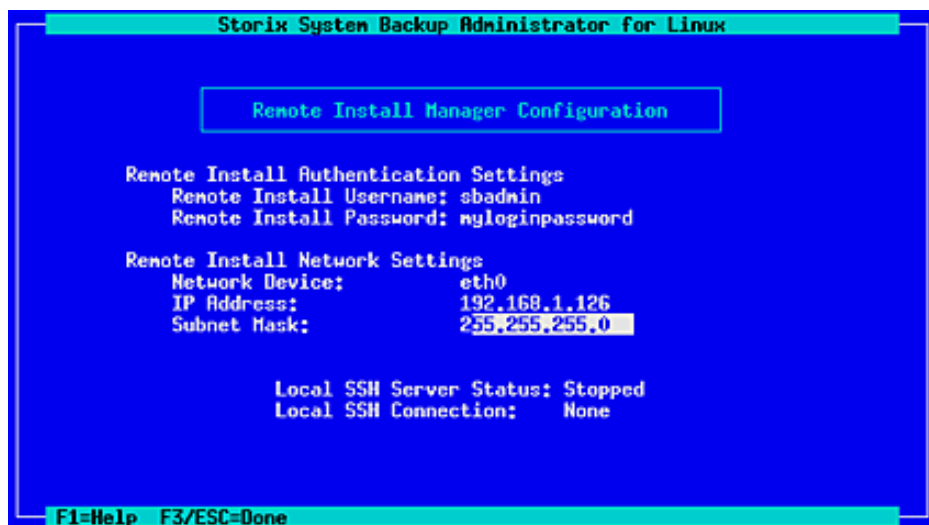
Note: There is no job control in the maintenance shell. Therefore using CTRL-C to end a process will not work. This is important to note if you are attempting to use the "ping" command to diagnose network issues. Any command you run should exit by itself. For example, if you are using the "ping" command, add an argument to limit the number of tries (normally the **-c** flag) so that the command will exit on its own.

Configure Remote Install Manager

If you configured RIM at the time you created the boot media, it will be automatically enabled and it will not be necessary to configure in this option. If, however you did not pre-configure RIM, or if you need to change the RIM configuration, you make changes from within the *system Installation menus* after booting from the SBAAdmin boot media. To do so, select the **System Recovery Utilities** option from the main menu to display the following:



Select **Configure Remote Install Manager**. The following screen will display:



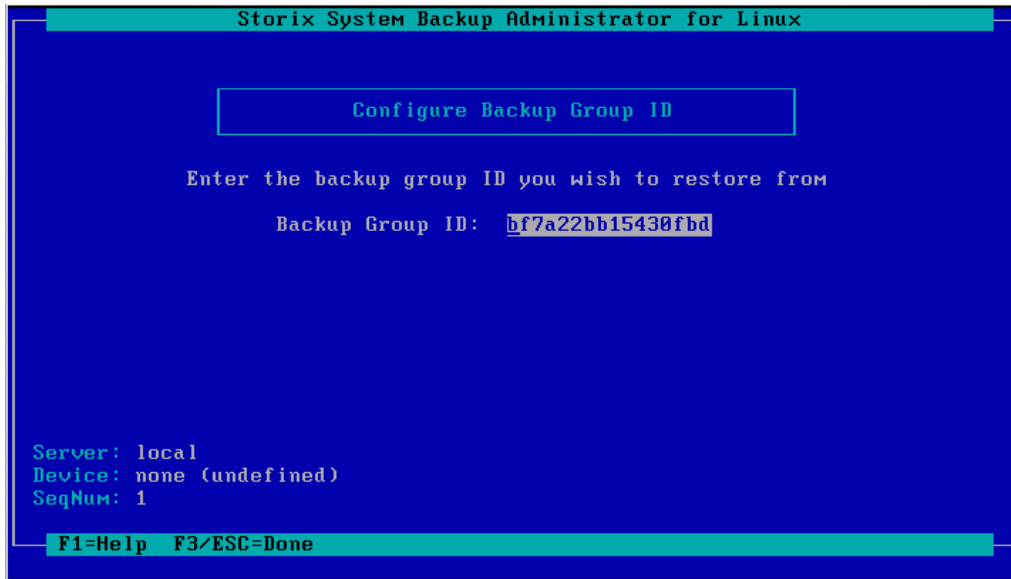
1. The **Remote Install Username** is set to “sbadmin” and may not be changed. Enter a password in the **Remote Install Password** field. The password will be necessary to login to the remote install client.
2. Select the **Network Device** (adapter) that should be configured to connect to the remote install client.
3. Enter the **IP Address** used to configure the network adapter. Note that, if the selected adapter is already configured (as a boot or install device) and you enter a different IP address than the adapter is currently using, you will be provided a warning and allowed to continue. If you do so, however, the previous settings will no longer apply, and the adapter will be reconfigured under the new IP address.
4. Enter the **Subnet Mask** (if necessary) used when configuring the network adapter. As with the IP Address, if the adapter is currently configured under a different subnet mask, you will be warned and allowed to reconfigure the adapter under the new subnet mask.

When you have finished your selections, press **ESC** or to return to the [RIM Menu](#). Then select **Start Local SSH Server**. The network adapter will be configured with these settings and the RIM server will be started. You can see the current status of the RIM server by looking at the **Local SSH** settings which appear on the screen.

Configure Backup Group ID

This option is used if you have configured a server with an “Optional client with access to all groups”. For further information about configuring the server this way please see the [SBAdmin User Guide](#).

If a backup has been copied to a shared server, the new group id will not match the group id of the original client backup. When restoring from the shared server, you will need to ensure a client is configured with access to all groups, and you have the appropriate group ID.



To change the groups ID simply begin typing and it will replace the old group id. Press the escape key to save the new setting and return to the previous menu.

Index

A

ascii
 encryption key, 38

B

backup sequence number, 41
 network install, 25
boot
 booting to install process, 29
 console, 18
 making system bootable, 67
 problems, 70
boot loader, 8
 definition, 7
boot media
 cdrom, 12
 creating, 11–28
 disk, 14
 kernel level, 19
 network, 14
 network adapter support, 17
 when to make, 11
boot server. *See* network boot server
booting, 29, *See also* network boot
bootloader, 10, 67
 boot filesystem, 68
 configure or change, 65
 ELILO, 68
 GRUB, 67, 68
 GRUB2, 67
 initrd support, 10
 Intel-based systems, 67
 LILO, 68
 pSeries systems, 68
 yaboot, 68
bootloader, 68
BOOTP, 34
bootpd, 34
broadcast boot, 24, 30, 32, 34, 35

C

cdrecord, 9
cdrom
 create ISO image, 12
 writer programs, 9
client
 booting for system installation, 29
 network installation, 23
cloning systems, 36
configure
 network boot/install, 23
 network boot/install client, 24
console

boot type, 18
 serial settings, 18

D

decrypt. *See* encryption
devfs, 9
device filesystem. *See* devfs
dhcpd, 34
disk
 configure boot disk, 14
disk backup file
 local install device, 42
disks
 selecting for installation, 50–53

E

EFI Boot Manager, 29
ELILO, 65, 68
encryption, 38, 67
 installing, 37
 software, 3

F

filesystem
 changing install settings, 48
filesystems
 adding/changing, 61
 definition, 8
 types, 61
firmware, 7
 definition, 7

G

GPT
 partitions, 52, 53
GRUB, 65, 67, 68
GRUB2, 67

H

hard disk. *See* boot media: disk
help, 39
 system installation menu, 39
hex
 encryption key, 38

I

initial ramdisk. *See* initrd
initrd, 8, 10
install
 from system backup. *See* system installation
install device
 parallel virtual device, 42
 sequential virtual device, 42

install server. *See* network install server
installation. *See* system installation
ISO. *See* boot media: cdrom

J

journals
external, 63

K

kernel
boot options, 65
boot release level, 19
definition, 7
modules. *See* modules
release level, 19
support requirements, 8
keys. *See* encryption

L

LILO, 65, 68
linear
meta-disks, 59
logical extents', 54
logical volume
changing install settings, 48
Logical Volume Management. *See* LVM
logical volumes, 54, 57
loopback device, 9
LVM, 54–59
definition, 8

M

MAC address, 24, 35
menu
system installation and maintenance, 33
metadisks, 59
definition, 8
metadisks, 69
mirroring
logical volumes, 58
meta-disks, 59
mkisofs, 9
modules
kernel modules
definition, 7
loading/unloading adapters support, 72
selecting network adapter support, 17
selecting scsi adapter support, 16
MSDOS
filesystem, 8, 62
partitions, 52, 53

N

network, 23
adapter hardware address, 24, 35
alternate install server, 25

re-configuration after system install, 71
selecting adapter modules, 17
network adapter
hardware address, 30, 32
remote installation manager, 21, 74
network boot server, 15, 23, 24, 26, 27, 38
network boot/install, **23**
alternate install server, 26
boot image
creating, 14
updating, 28
boot loaders, 14
boot server, 14, 23, *See* network boot server
install device, 25
install server. *See* network install server
installing different Linux levels, 27
troubleshooting network boot, 34
unconfigure install client, 26
using alternate network, 26
using different boot and install servers, 26
network install device
tape, 45
network install server, 23, 25, 26, 27, 45
changing during install, 40
nfs mount backup file
local install device, 43
no-prompt install, 19
no-prompt install, 25
no-prompt install, 33
no-prompt install, 36

O

OpenFirmware, 8
device name
network, 30
tape, 32
prompt, 31, 33

P

paging space. *See* swap devices
partition
boot device, 65
bootloader, 69
migrating, 53
partition table
changing, 51, 53
PE size, 57
physical extents, 54
physical volumes, 54, 55

R

RAID. *See also* metadisks
level 0+1, 61
levels, 59
recovery. *See* system installation
remote install manager
configuring from install menus, 74

remote installation manager, 20
RIM. *See* remote installation manager

S

SCSI
 selecting modules, 16
shell
 maintenance, 73
software RAID. *See* metadisks
ssh program, 22
strimsh program, 22
striping
 logical volumes, 58
 meta-disks, 59
support for UEFI, 13, 15
swap devices, 64
system backup
 network install, 23
 system installation, 36
system backup disk
 local install device, 42
system backup nfs
 local install device, 43
system installation
 booting, 29
 booting in installation mode, 29
 changing LVM and filesystem settings, 48
 cloning systems, 36
 device, 40
 errors, 70
 install device
 changing, 40
 selecting a remote device, 45
 installing the system, 66
 main menu, 34
 mode, 25
 network install server
 changing, 40, 44
 no-prompt install, 19, 36
 settings, 64, 65
 starting, 67
 UEFI, 36
 verification, 66

system recovery. *See* system installation

T

tape
 autoloader, 41
 network install device, 45
tape boot, 32
tape drive
 remote, 45
text
 encryption key, 38
tftpd, 34
Tivoli. *See* TSM
TSM
 administrative user, 48
 client, 48
 configuration, 46
 server, 48

U

UEFI firmware boot, 29
UEFI support, 9
utilities. *See* system recovery utilities
 configure remote install manager, 74
 loading/unloading adapters support, 72
 maintenance shell, 73

V

verify
 hardware configuration, 38
virtual devices
 parallel, 42
 sequential, 42
volume group
 changing install settings, 48
volume groups, 54, 55

Y

yaboot, 65, 68