Trustix Secure Linux 3.0

Installation Manual

Viper 1.0

Comodo Trustix Ltd.

Table of Contents

Introduction

1.1 Target Audience

This manual is aimed at both inexperienced and advanced users that want to install Trustix Secure Linux 3.0.

1.2 About This Manual

This Manual aims to guide the user through the installation procedure. It also tries to explain each feature of the Viper installer in depth, so that advanced users may take advantage of it's many new features.

1.3 About Viper

Viper is the Trustix Secure Linux (TSL) Installer. Development was started in 2004, with initial release with version 3.0 of TSL and is developed by a group of Comodo Trustix developers, focusing on ease of use and portability.

1.4 About Trustix Secure Linux

Trustix Secure Linux is a Linux distribution for servers, with focus on security and stability. The system is painlessly kept safe and up to date from day one using Swup, the automated software updater

1.5 About Comodo Group

Comodo is a leading Internet security specialist and provides next generation E-commerce Security Solutions - x.509 digital Certificate services, validation services, silicon security, crypto solutions and software security applications. Comodo provides secure Linux solutions through Trustix and also operates the world's only website identity assurance infrastructure.

1.6 Reporting Bugs

A bugzilla interface is available at https://bugs.trustix.org for reporting any bugs.

5-Step Quick Installation Guide

2.1 Welcome Screen

(Image 2.1)

The Welcome screen includes 3 buttons. These buttons or variations of them will be present in all the Installer screens.

Next

Move to the next step in the Installer.

Help

Enter the help text for the current step in the installer

Back

Return the the previously visited step in the installer

Cancel

Cancel installation. This will drop you to a shell.

2.2 Keyboard Configuration

(Image 2.2)

The Keyboard Configuration screen enables you to select what keyboard layout is to be used during installation and also to set the default keymap on the installed system.

Select the type of the layout from the given list as shown in image 2.2. You may navigate through the list using up arrow and down arrow keys. After selecting, press ENTER to get loaded with the selected keyboard type, or navigate to the Next button.

2.3 Root Password

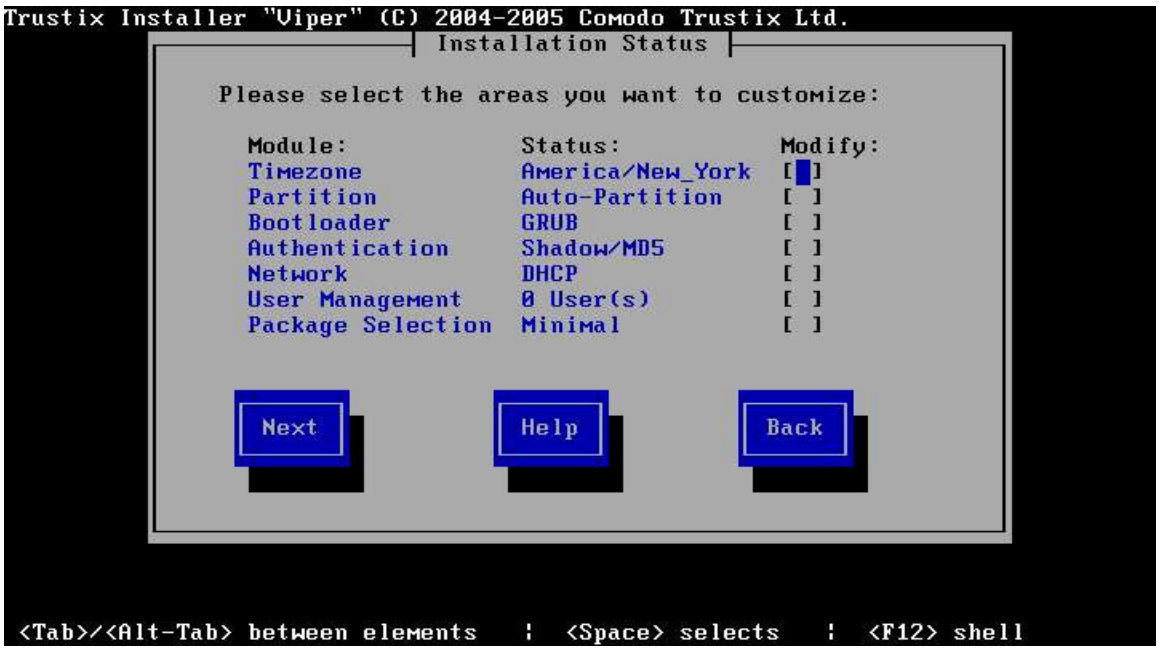
(Image 2.3)

The root user is the only truly mandatory user in a Linux system. Its user id (uid) is 0, and this user embodies every capability of the system. Most Linux distributions have other system users as well, most with specific tasks to preform and with various degrees of security level. This is also true with Trustix Secure Linux.

However, the root account is the only system user that is normally used for accessing the command line and the tools of the system. Normal root user actions is installing and removing software, performing upgrades, configuring the system, etc.

To be able to log into the system, a user needs a password. Viper provides a user interface to enter the root password for the installed Trustix Secure Linux system.

2.4 Installation Status Window

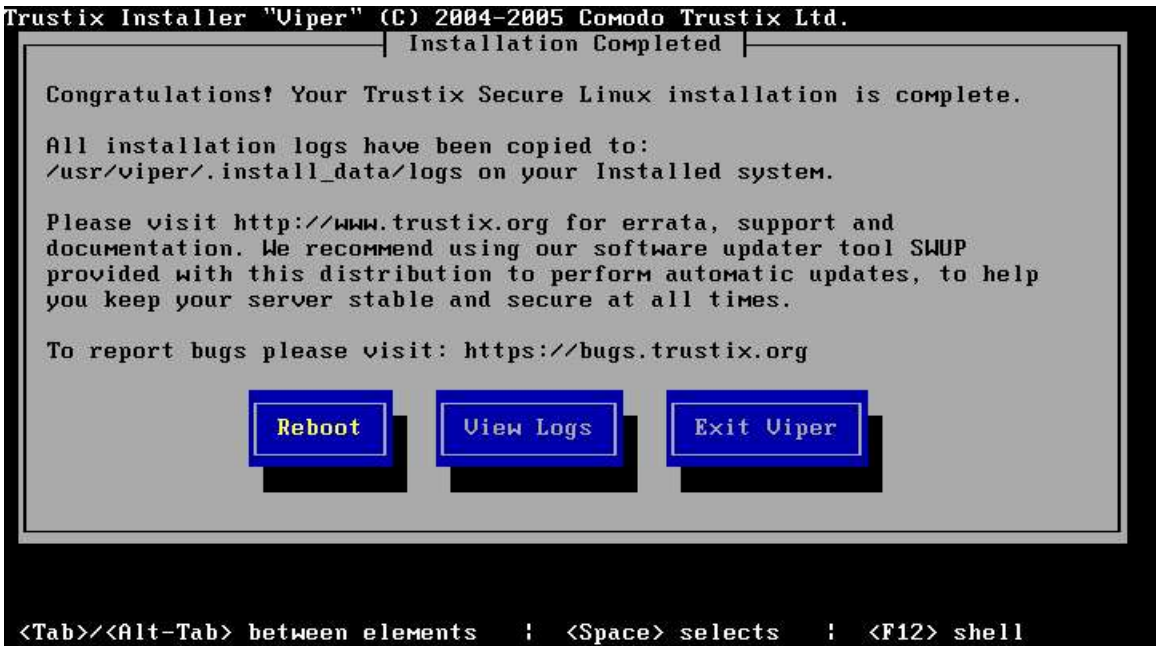


(Image 2.4)

One of the unique features of viper is its Installation Status window, which lists the settings which are to be used by the installer for a 5-step default installation of Trustix.

Hitting **Next** will make Viper proceed with the installation, using the default options.

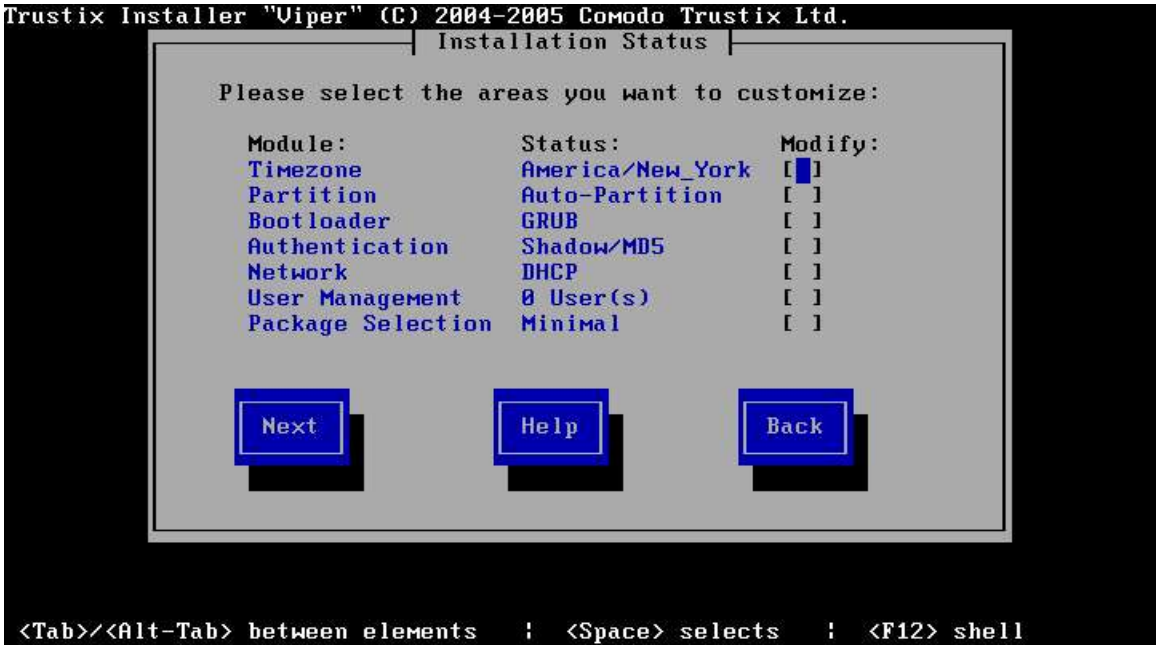
2.5 Finish Window



(Image 2.5)

The finish window displays options to reboot, view logs or exit viper to console. You can use terminal 2 (`Alt+F2`) to inspect contents of `/tmp/target` where your installation root is mounted which the finish window is still displayed, as soon as the finish window terminates all mounts are unmounted and finalized.

Advanced configuration from "Installation Status" window

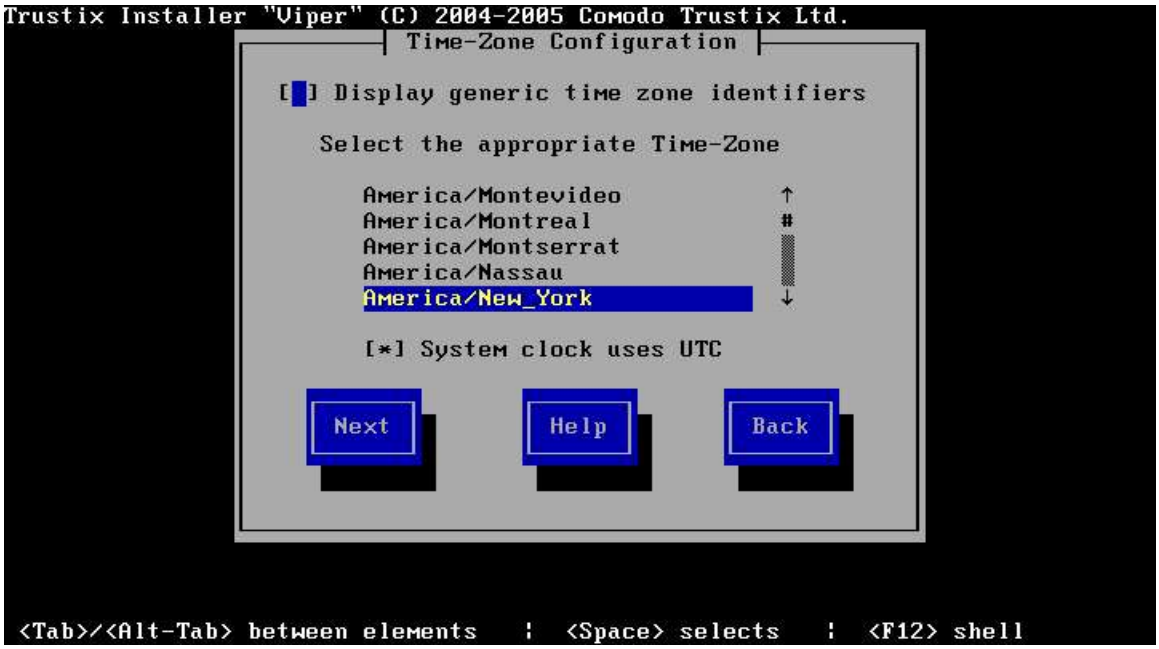


(Image 3.1)

If you wish to modify any of the settings displayed in the Installation Status window, you can simply select to modify it. If any Module is set to be modified, the configuration interface for that module will be displayed upon hitting **Next**. Only when no module is set to be modified, will the installer proceed with installation upon hitting **Next**.

After going through the configuration of the selected modules, the installer returns to this window. Note that the information about the modules that has been modified is updated and that the selection to modify will then be cleared, so that upon hitting **Next**, the installation will proceed.

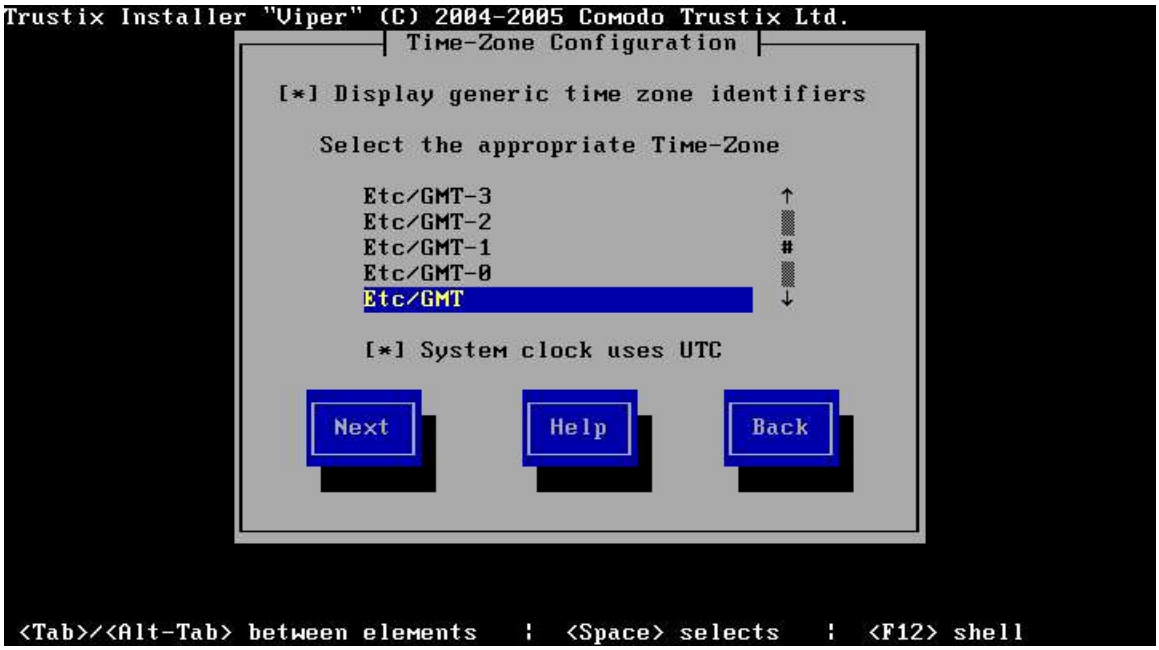
3.1 Time Zone Configuration



(Image 3.2)

Timezone configuration window displays a list of available timezones to use as system time configuration. You may select the appropriate timezone from the given list as shown in image 3.2.

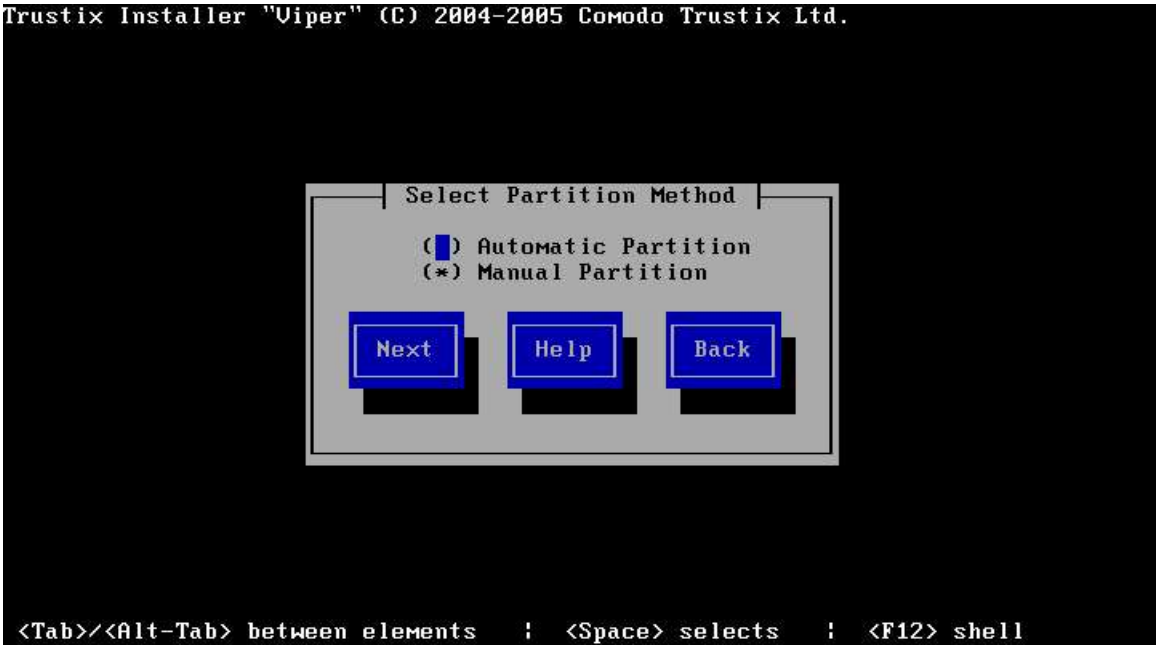
The bottom checkbox labeled “System time uses UTC” tells Linux that the hardware clock on the system is set to UTC (Universal Time Constant). Upon reboot the hardware clock is used to set the software clock. In most cases the hardware clock uses UTC, so this checkbox is enabled by default.



(Image 3.3)

You may also select the timezone from the list of generic timezone identifiers by selecting the checkbox on the top which shows the timezones with GMT. The list will then be updated to display the additional items as shown in image 3.3.

3.2 Partitioning



(Image 3.4)

This session deals with the partitioning of the hard disk(s). If you are not experienced with hard disk partitioning, selecting Automatic Partitioning is a safe bet.

Partitioning a hard disk means dividing it into partitions. This is often done to prevent normal users to fill the root partition with data, effectively a Denial of Service attack. It is also sometimes used to ensure proper booting of the system, or to enforce stricter permissions checking for parts of the system.

Each of the partitions needs a file system to be able to hold files. When partitioning a hard disk and creating new file systems on the partitions, old data is lost. Make sure you back up any important files on the existing system if not all!

Automatic Partitioning

If automatic partitioning is selected, Viper will automatically partition your hard drive. Creating partitions depends on the number of hard drives in the system and what partitions they already contain.

If the system has 1 hard drive, the installer will create boot, swap and root partitions and create file system on all three. These partitions will also be automatically mounted in the proper place:

Partition:	Size:	File system:	Mount point:
a.	130 MB	ext3	/boot
b.	2*size of RAM	swap	<special>
c.	all remaining space	ext3	/

If the system has two hard drives, It will create /boot, swap and root partition in first hard drive and a /home and a swap in another hard drive . File system will be created on all the 5 partitions. These partitions will also be automatically mounted in the proper place:

First hard disk:

Partition:	Size:	File system:	Mount point:
a.	130 MB	ext3	/boot
b.	1*size of RAM	swap	<special>
c.	all remaining space	ext3	/

Second hard disk:

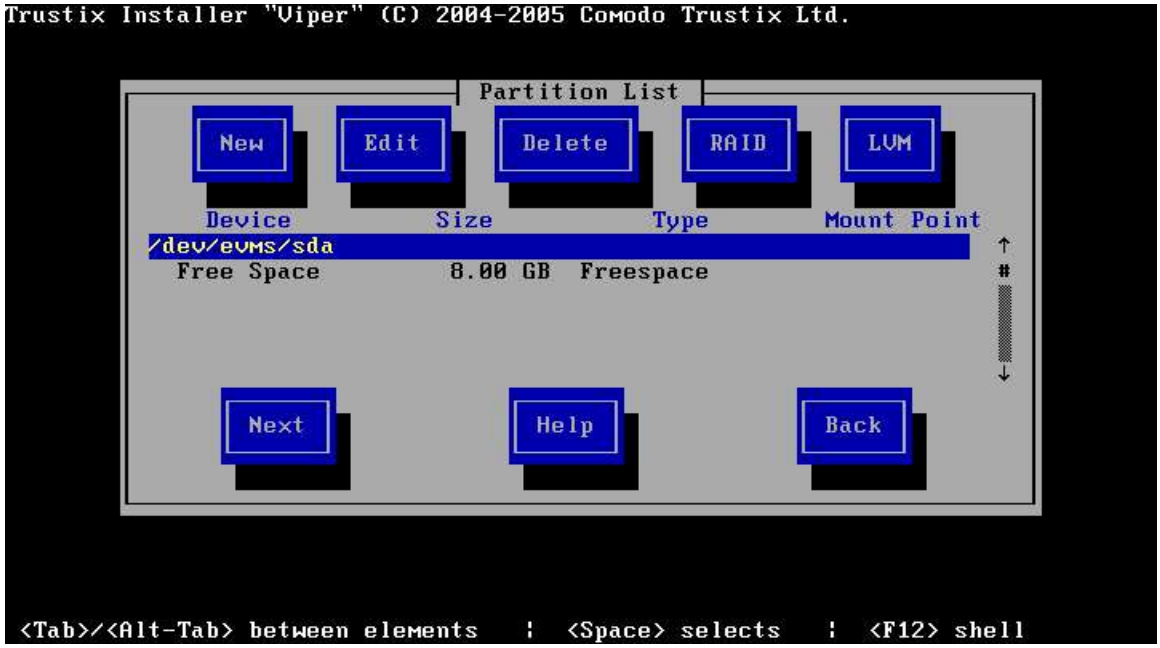
a.	1*size of RAM	swap	<special>
b.	all remaining space	ext3	/home

You can choose this option if you don't know much about hard drive partitions, but care must be taken to avoid data loss.

AUTO-PARTITION WILL ERASE ALL DATA ON THE
FIRST AND SECOND HARD DISKS.

If viper detects any existing partition, it will ask the user's confirmation to delete the existing partitions. If the system has more than two hard disks, only the first two hard disk will be partitioned and the remaining hard drives will remain untouched.

Manual Partitioning



(Image 3.5)

In manual partitioning, any pre-existing partitions will be shown with details. The user can create, edit and delete partitions. In addition to this RAID and LVM can also be configured.

The screen contains the following fields:

New

Request a new partition. Selecting this button causes a window appear containing the appropriate fields that must be filled in.

Edit

Modify the attributes of the partition currently highlighted in the partition list window. Selecting this button will cause a window to appear allowing you to change the attributes of the highlighted partition.

Delete

Delete the partition currently highlighted in the partition list window.
Selecting this button will cause a window to appear asking you to confirm the deletion.

RAID

Selecting this button causes a window to appear containing the relevant fields that must be filled in.

LVM

Selecting this button causes a window to appear containing fields that must be filled in order to create LVM volume group.

Next

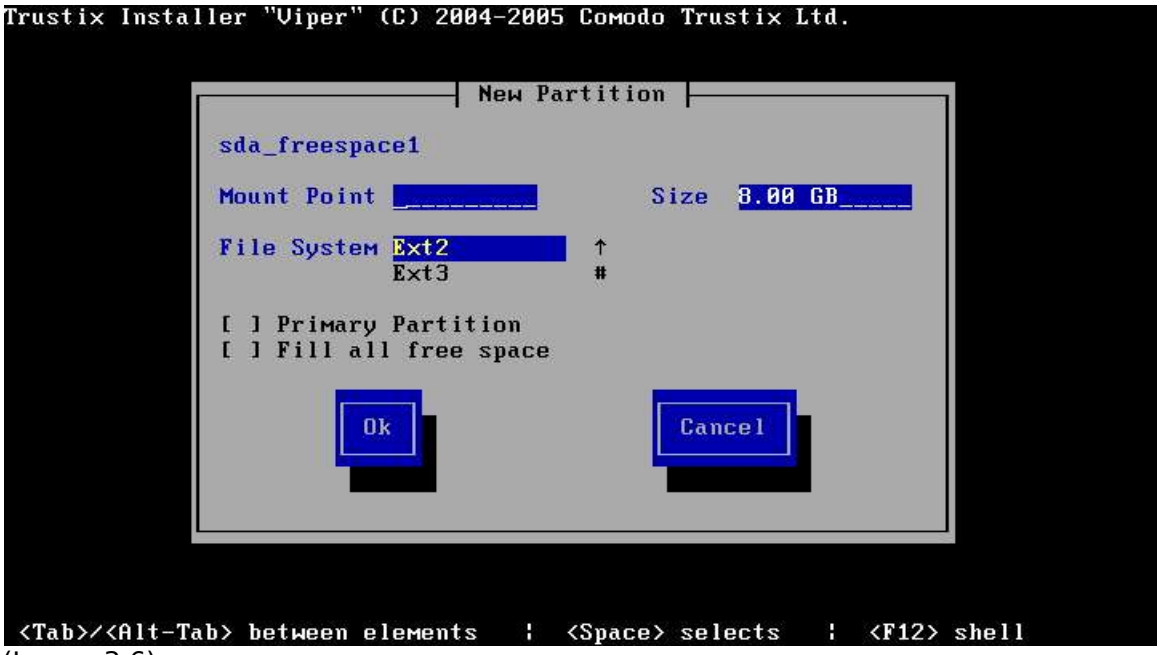
Confirm that changes made to your system's partitions, so that they may be written to disk.

Back

Abort without saving any changes you've made. When this button is selected, the installation program will take you back to the previous screen, so you can start over.

Create A New Partition

To create a new partition, Select a free space and hit **New**.



(Image 3.6)

The screen contains the following fields:

Mount Point

Select this field and enter the partition's mount point. Mount Point must begin with '`/`'. For example, '`/`' for root partition, '`/boot`' for boot partition.

Size

In this field, enter the size of the partition. Size must be given in MB or GB.

File System Type

This field contains a list of different file system types. Select the appropriate file system type by using the Up and Down arrow keys. Viper currently supports 9 file system types:

- ext2
- ext3
- XFS
- JFS
- reiserfs
- swapfs
- PPC PrepBoot
- Software RAID
- Logical Volume Member

Primary Partition

Creates primary partition on the selected hard disk's free space. Press the space bar key to select this checkbox.

Fill All Free Space

When this checkbox is selected, the partition will be created using the available free space on the drive

Edit Partition

(Image 3.7)

To edit a partition first select the partition to be edited and then press Edit button. The Edit partition window similar to the figure below will appear. In edit you can change mount point and file system of the selected partition.

The screen contains the following fields:

Mount Point

Select this field and enter the partition's mount point. Mount Point must begin with '`/`'. For example, '`/`' for root partition, '`/boot`' for boot partition.

File System Type

This field contains a list of different file system types. Select the appropriate file system type by using the Up and Down arrow keys. Viper currently supports 9 file system types. They are ext2, ext3, XFS, JFS, reiserfs, swapfs, sw RAID and LVM. PPC PrepBoot will be shown for primary partitions.

Swapon

When selected will change the status of swap to ON.

Swapoff

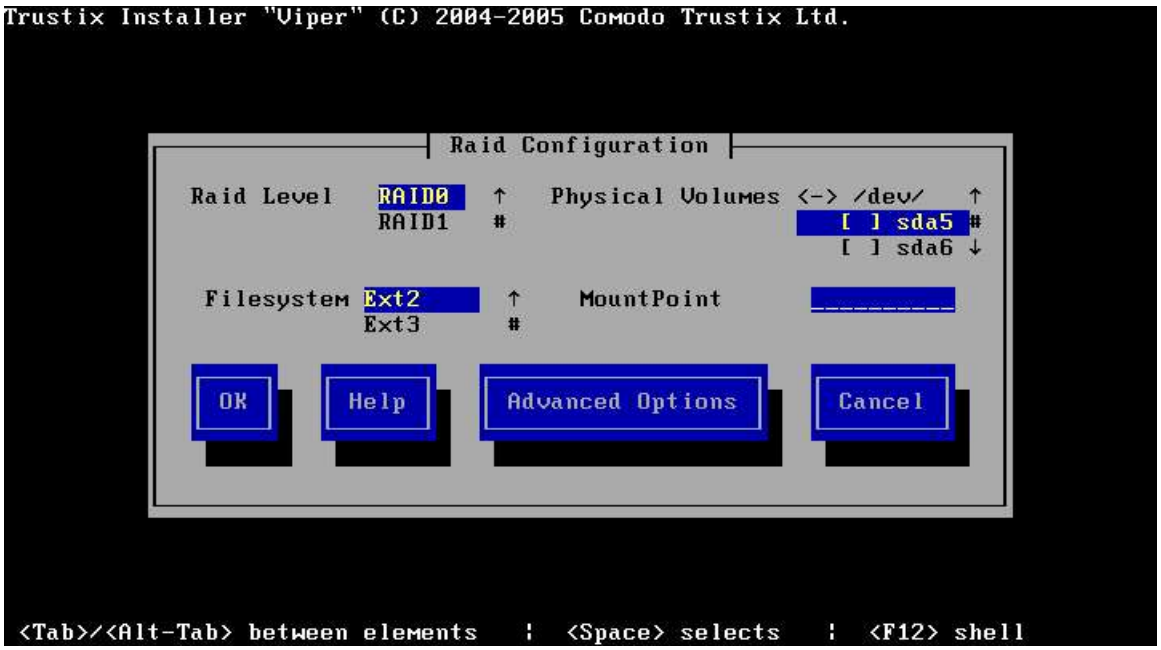
When selected will change the status of swap to OFF.

Delete Partition

(Image 3.8)

To delete, select the partition and hit Delete. You will be asked to confirm the deletion.

RAID



(Image 3.9)

To create a RAID device, you must first create software RAID partitions. Once you have created two or more software RAID partitions, select **RAID** and press Space bar or Enter to create.

Viper currently supports **RAID0**, **RAID1**, **RAID5** and **Linear** levels. The selected file system will be created and mounted at the given mount point. Advanced options will depend on selected RAID level. For Linear level there are no advanced options.

The screen contains the following fields:

RAID Level

Select the RAID level to be created.

Physical Volumes

Press space bar on the partitions to create RAID device.

File system Type

This field contains a list of different file system types. Select the appropriate file system type by using the Up and Down arrow keys. Displayed filesystems are ext2, ext3, XFS, JFS, reiserfs, swapfs and LVM.

Mount Point

Select this field and enter the partition's mount point. Mount Point must begin with '/'. For example, '/' for root partition, '/boot' for boot partition.

Advanced Options For RAID

Advanced options will vary depending on the RAID level selected. There is no advanced option for linear RAID level.

Chunk-size

The amount of data that is written to one child object before moving to the next object. If the option is not specified, the default chunk-size of 32 KB will be used. Option for RAID0 and RAID5.

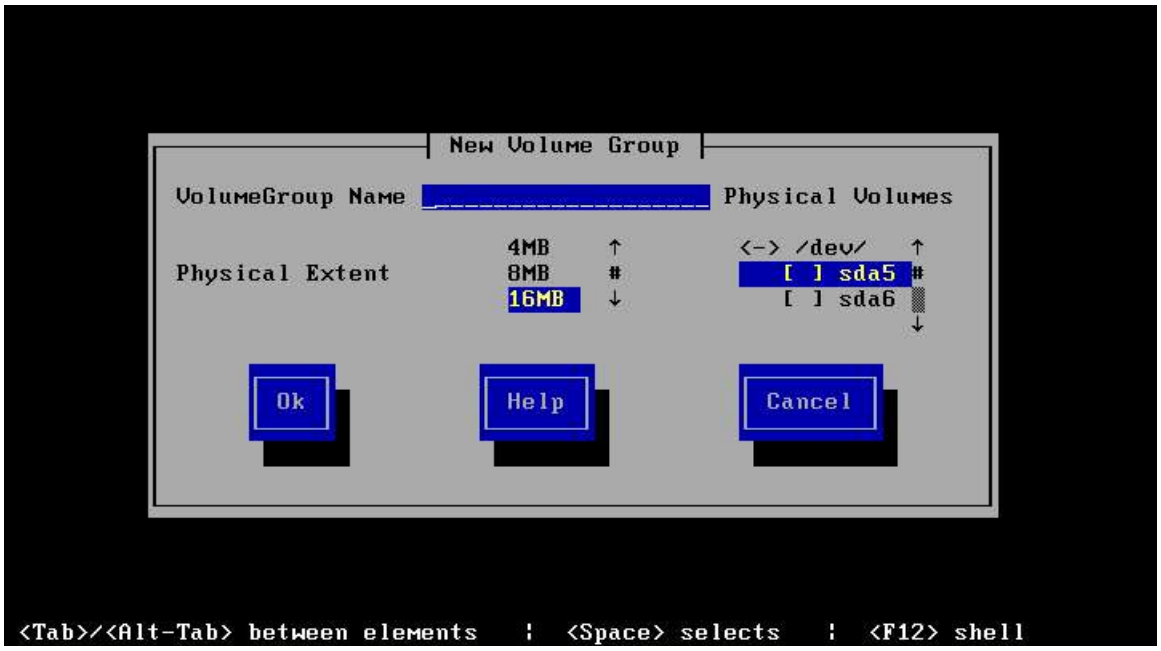
Spare-disk

The selected object will be used as a “hot-spare”. Unselected Software RAID partitions which are equal or greater in size of the smallest selected Physical Volume will be shown in spare disk list. By default, without any spare object will be created. Option for RAID1 and RAID5.

Algorithm

This the parity algorithm. Valid algorithms are “Left Symmetric”, "Right Symmetric," "Left Asymmetric, and "Right Asymmetric."By default “Left Symmetric” will be chosen. Only for RAID5.

LVM



(Image 3.10)

The **Logical Volume Manager** (LVM) enables you to resize your partitions without having to modify the partition tables on your hard disk.

To make an LVM Volume Group device, you must first create LVM partitions. Once you have created LVM partitions, select **LVM** to join the LVM partitions into a LVM Volume Group device.

Volume Group

LVM Volume Group will be created by selecting the Physical Volumes and by giving it a name. By default the Physical Extent Size is 16MB.

The screen contains the following fields:

Volume Group Name

Enter the name for the LVM volume group to be created. '/' is invalid character in the name field.

Physical Volumes

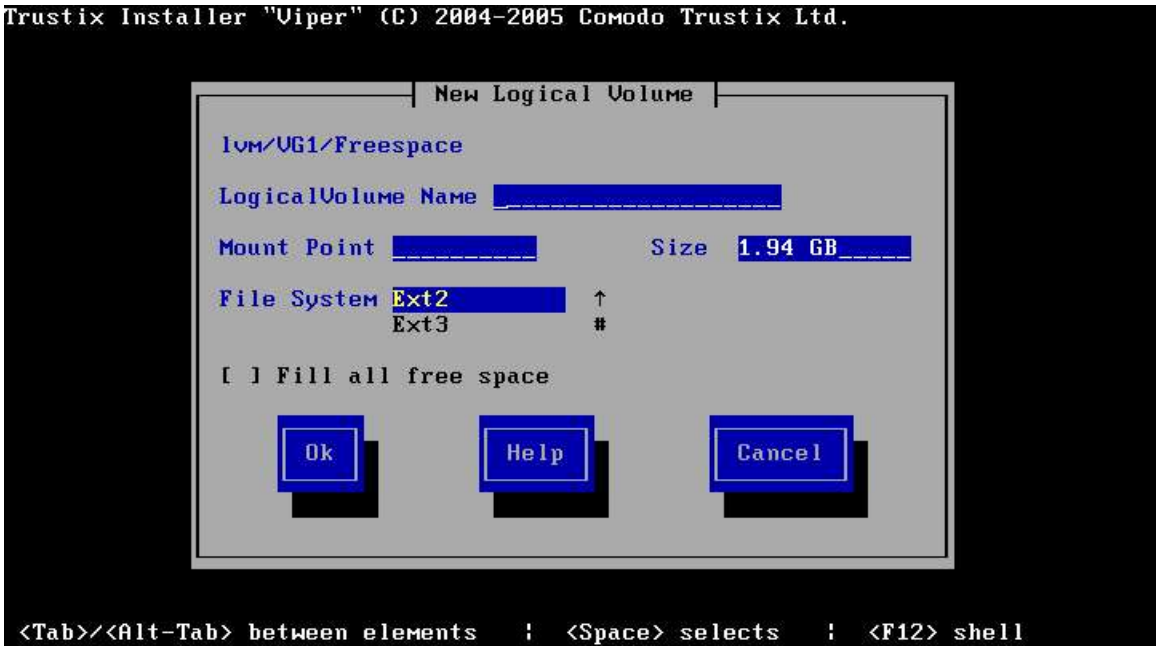
Select the partitions on which volume group is going to create. Press space bar on the partitions.

Physical Extent

Real disk partitions are divided into chunks of data called physical extents (PEs) when you add them to a logical volume.

Logical Volume

Logical Volume can be created with the volume group free space. Logical Volume will be created by giving the name, size, file system and mount point. It will be mounted to the specified mount point.



(Image 3.11)

Logical Volume Name

Enter the name to the logical volume. '/' is invalid character.

Mount Point

Select this field and enter the partition's mount point. Mount Point must begin with '/'. For example, '/' for root partition, '/boot' for boot partition.

Size

In this field, enter the size of the partition. Size must be given in MB or GB .

File System Type

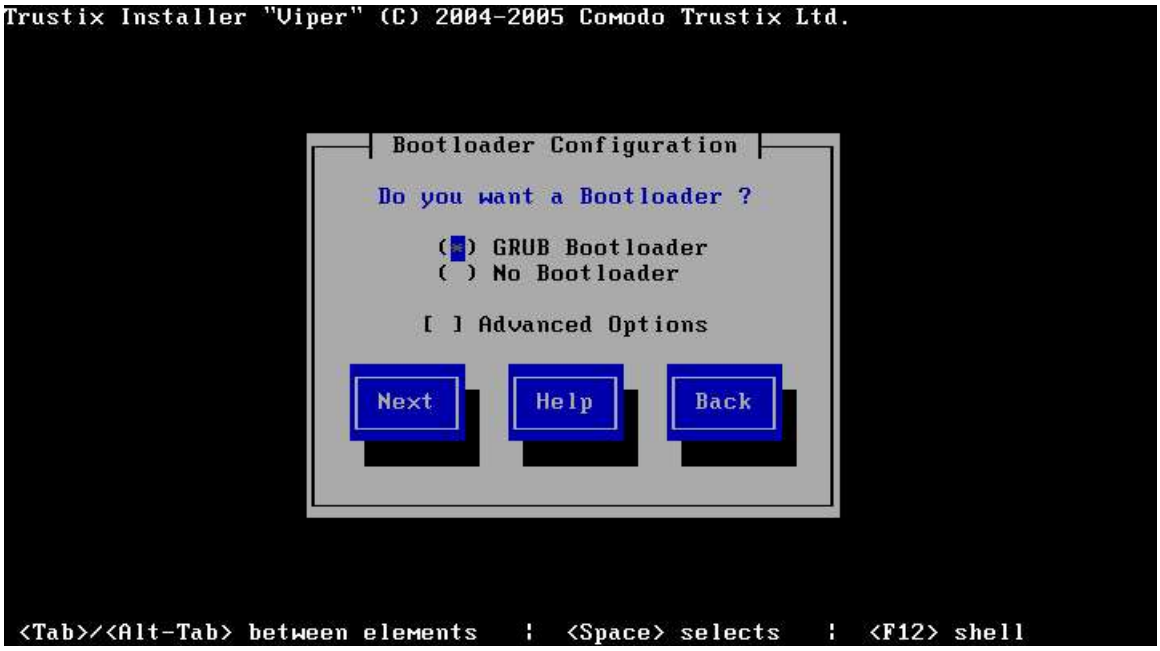
This field contains a list of different types of file system. Select the appropriate file system type by using the Up and Down arrow keys. Viper currently supports several file system types. They are ext2, ext3, XFS, JFS, reiserfs, swapfs.

Fill all free space

When this checkbox is selected, the Logical Volume will be created with all available free space.

When you are done with partition, press Next button to navigate next step in the installer.

3.3 Bootloader Configuration



(Image 3.12)

A bootloader is required in order to boot the system without a boot diskette. It helps to choose from multiple OS's or kernels. It is a bootloader that transfers control to the kernel which in turn starts the rest of the operating system. Trustix Secure Linux provides GRUB as the bootloader. GRUB is a very powerful bootloader that supports a lots of operating systems. It can also load another bootloader which in turn can load an operating system (chain-loader mechanism).

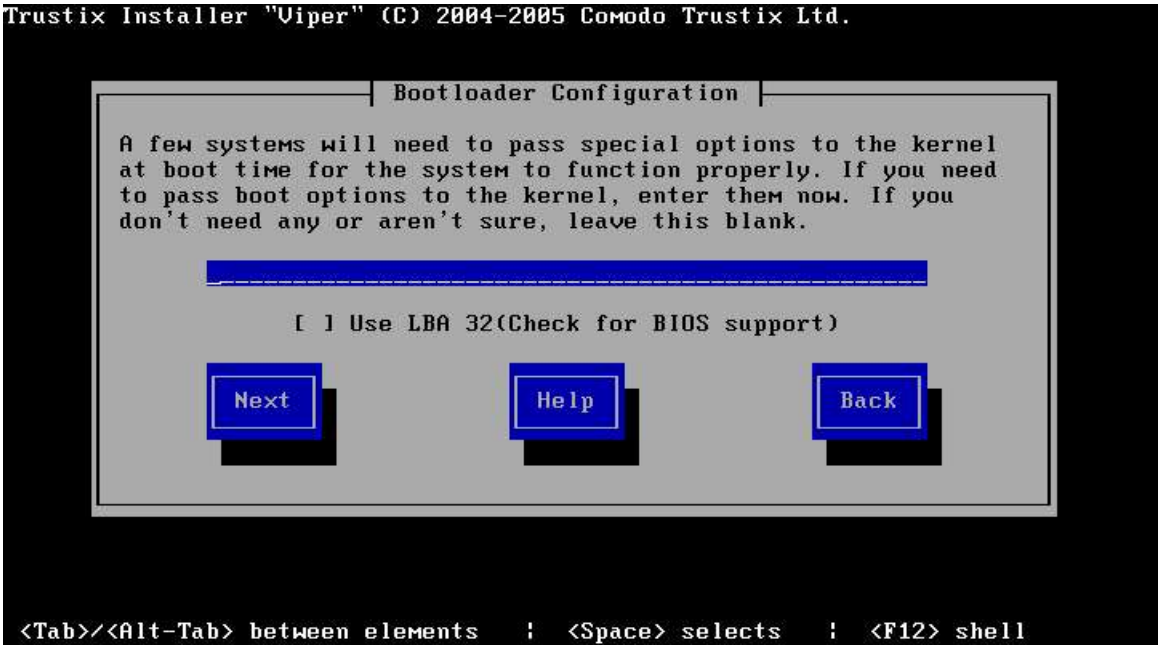
Bootloader Configuration helps in configuring the bootloader according to the required needs. By default Viper installs GRUB to the MBR (Master Boot Record) of the hard disk that contains the /boot partition (or '`/`' partition if there is no separate '`/boot`' partition). If you do not want to install a bootloader then choose the “No Bootloader” from the options. This would skip the installation of GRUB, and hence you will need a boot diskette to boot from unless you already have an existing bootloader installed.

The first window just asks user to choose from GRUB or No Bootloader. Clicking next without the advance options will finish the bootloader configuration and Viper will guess the location to install the bootloader, this is the recommended way. If the user wants further configuration to be done, check the advance options and then click next.

To configure GRUB you need to check the advance options and then click **Next**. The second window asks you where to install the bootloader. The bootloader can be

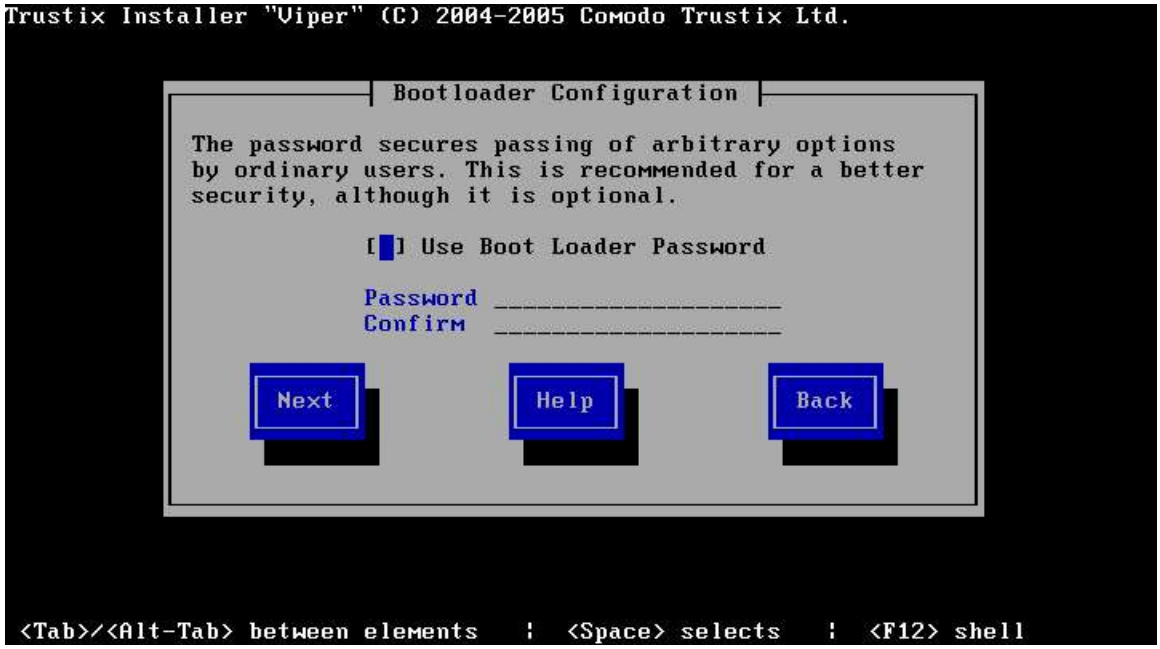
installed on an MBR or First Boot Sector of a partition. This can be multiple devices if the /boot or / is on a RAID devices. One must remember that the bootloader only supports RAID level 1 and hence the `/boot` (or `/` without separate `/boot`) should be on RAID Level 1 devices or else the bootloader installation will fail.

Next window asks for if the label for the Trustix entries in the booloader menu is to be changed or not. This is will be shown in the GRUB window during booting.



(Image 3.13)

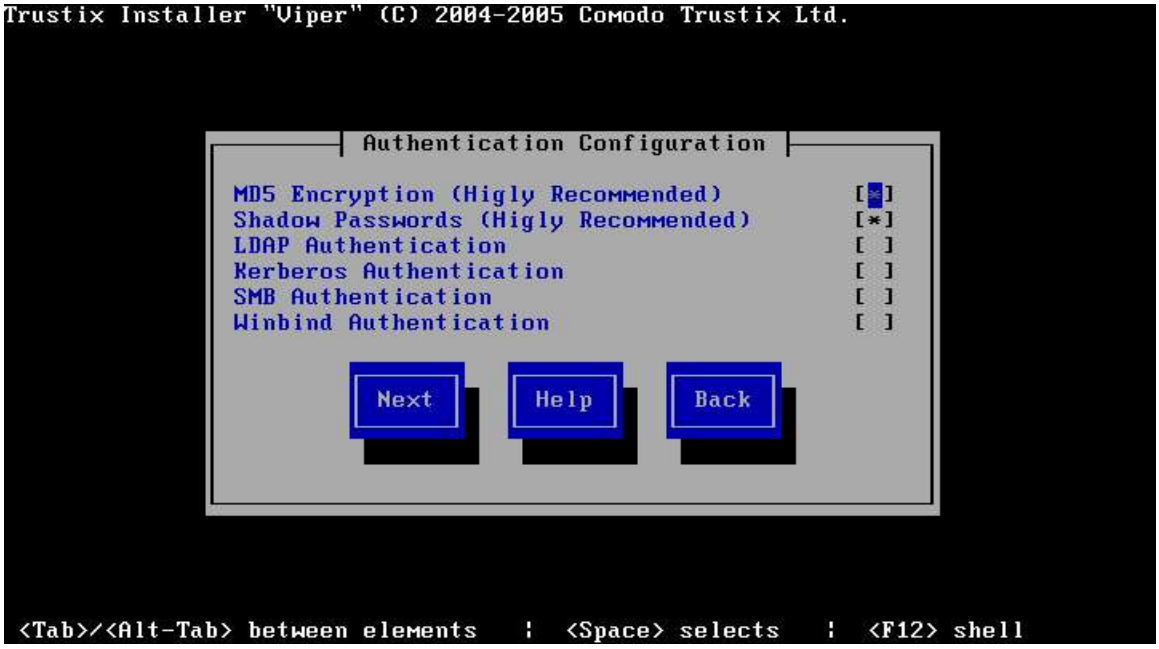
The next window (3.13) is an optional window asking if the user would like to pass any kernel parameters which will be used while booting. For example, if you have an IDE CD-ROM Writer, you can tell the kernel to use the SCSI emulation driver that must be loaded before by configuring hdd=ide-scsi as a kernel parameter (where hdd is the CD-ROM device). The Force use of LBA32 (not normally required) option allows you to exceed the 1024 cylinder limit for the /boot partition. If you have a system which supports the LBA32 extension for booting operating systems above the 1024 cylinder limit, and you want to place your /boot partition above cylinder 1024, you should select this option.



(Image 3.15)

The fifth and final window helps to set a password for protecting GRUB being edited by non privileged users. The password is always stored encrypted.

3.4 Authentication Configuration



(Image 3.16)

To login to Trustix Secure Linux requires the combination of a username and password, which must be authenticated as a valid user or not. This information to validate a user can be stored locally or remotely in a user database system. Authentication Configuration helps in the client side configuration of different authentication tools like MD5 password encryption, Shadow password system, LDAP, Kerberos, SMB, Winbind, Hesiod and NIS. The authentication system basically has to major aspects, user-information and method of authentication – PAM.

Linux-PAM (Pluggable Authentication Modules for Linux) is a suite of shared libraries that enable the local system administrator to choose how applications authenticate users. This may include the method of password encryption and verification (MD5 and Shadow) and also other methods of authentication like LDAP, Kerberos, SMB and Winbind.

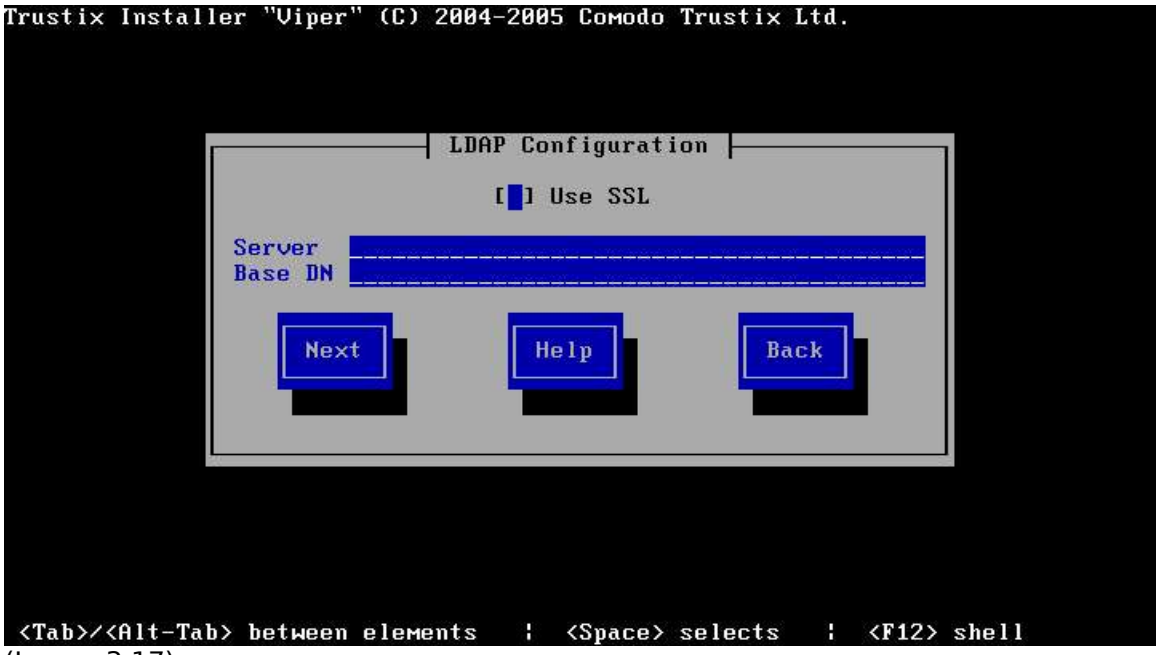
MD5 Encryption

MD5 Encryption is for encrypting passwords with the MD5 algorithm. This allows a long password to be used (up to 256 characters), instead of the standard eight letters or less. The MD5 algorithm is stronger than the older crypt function and encrypting the passwords using MD5 is highly recommended. This is enabled by default.

Shadow Password

Shadow Password provides a secure method for retaining passwords. This enables the storing of password in the /etc/shadow file rather than /etc/password, which is highly recommended and is default on any modern Linux system.

LDAP Authentication



(Image 3.17)

LDAP Authentication enables PAM enabled applications to use LDAP authentication. This tells your computer to use LDAP for authentication and consolidates certain types of information within your organization. For example, all of the different lists of users within your organization can be merged into one LDAP directory. You need an LDAP Authentication server on your network for this to work. If you do not have such a service available, leave this option. Configuring LDAP Authentication requires these information:

SSL

Use Transport Layer Security to encrypt passwords

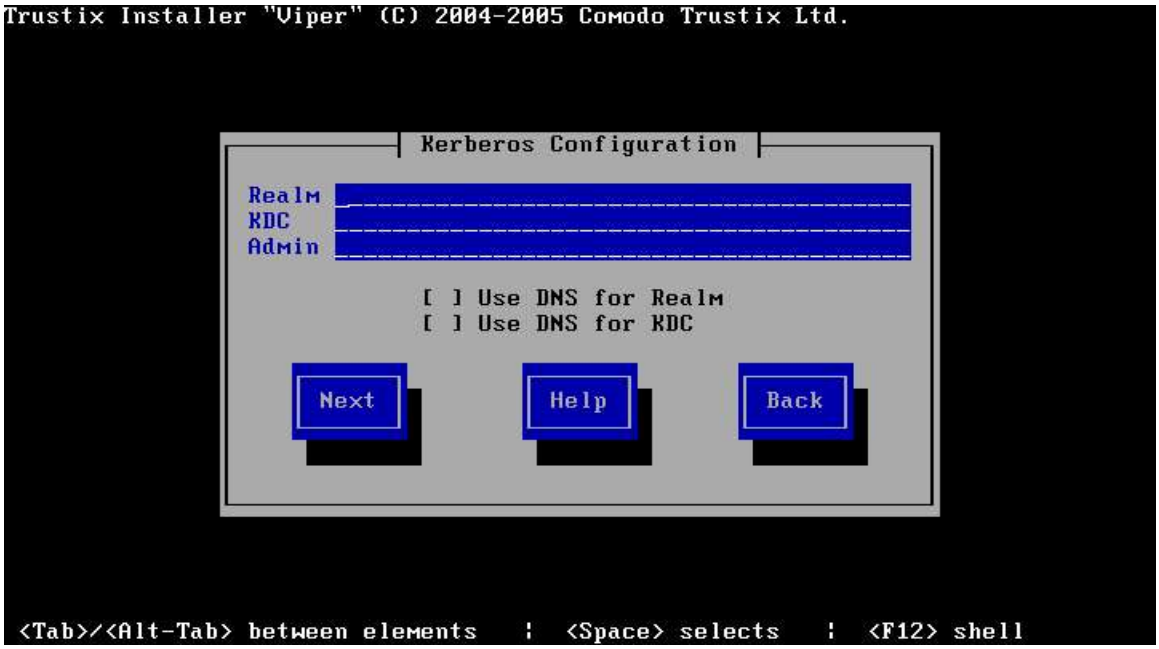
Server

Specify the IP address of the LDAP server.

Base DN

Retrieve user information by its Distinguished Name (DN)

Kerberos Authentication



(Image 3.18)

Kerberos Authentication enables PAM enabled applications to use Kerberos authentication. You need a Kerberos Authentication service on your network for this to work. If you do not have such a service available, leave this option unchecked.

Realm

Configure the realm for Kerberos server.

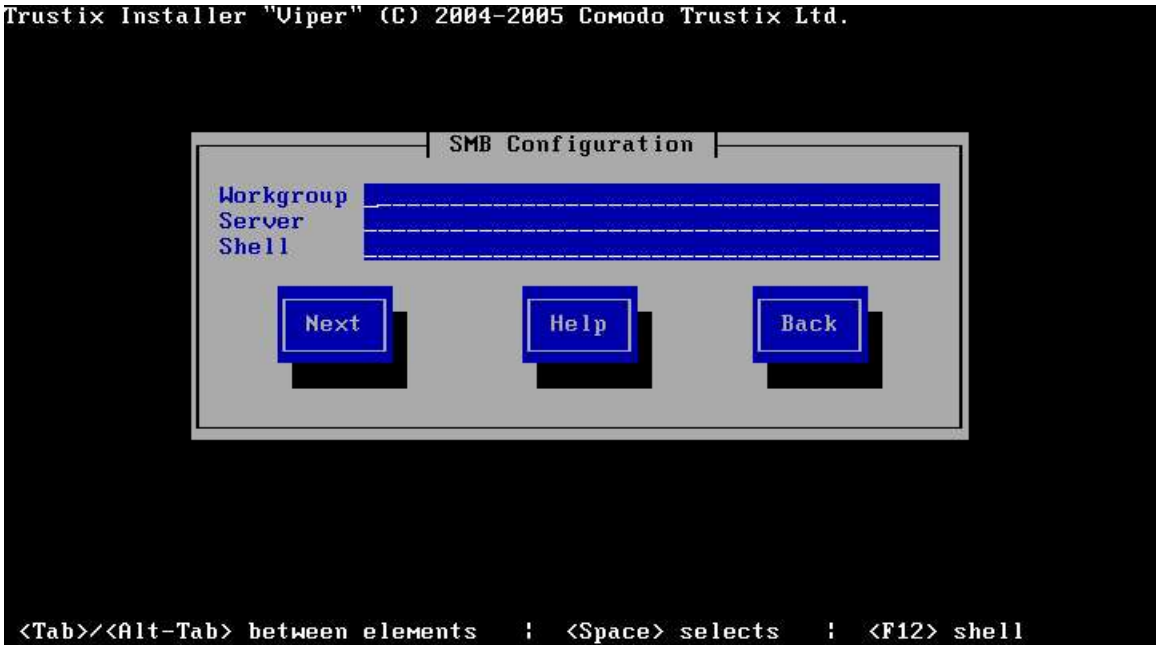
KDC

Key Distribution Center, the server that issues Tickets (sometimes called a Ticket Granting Server or TGS).

Admin Server

Specifies the admin server (server running kadmind)

Samba Authentication



(Image 3.19)

Samba Authentication enables PAM to use a SMB server for authentication. If you do not have such a service available, leave this option.

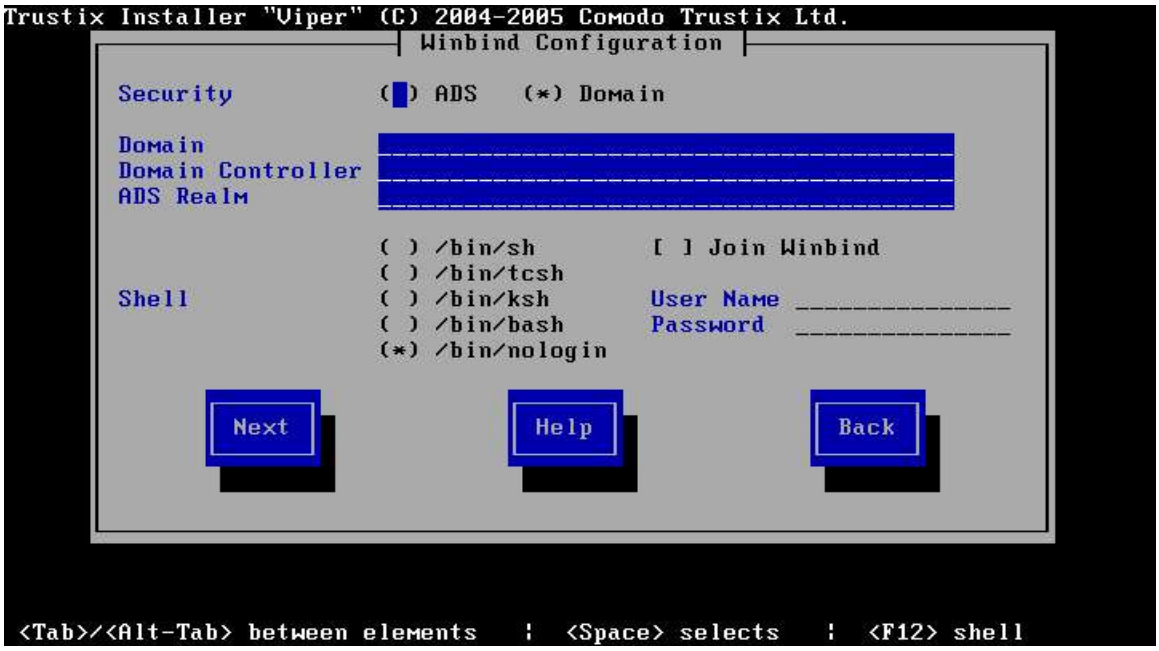
Workgroup

Indicates which workgroup the configured SMB servers are in.

Server

Indicates which SMB server you will connect to for authentication.

Winbind



(Image 3.20)

Winbind Authentication configures the system to connect to a Windows Active Directory or a Windows domain controller. Both the user information and the server authentication can be done. Winbind unifies UNIX and Windows NT account management by allowing a UNIX box to become a full member of an NT domain. Once this is done the UNIX box will see NT users and groups as if they were native UNIX users and groups, allowing the NT domain to be used in much the same manner that NIS+ is used within UNIX-only environments.

Domain

Workgroup for samba

Domain Controller

Samba Server

ADS Realm

Required if security is ADS

Shell

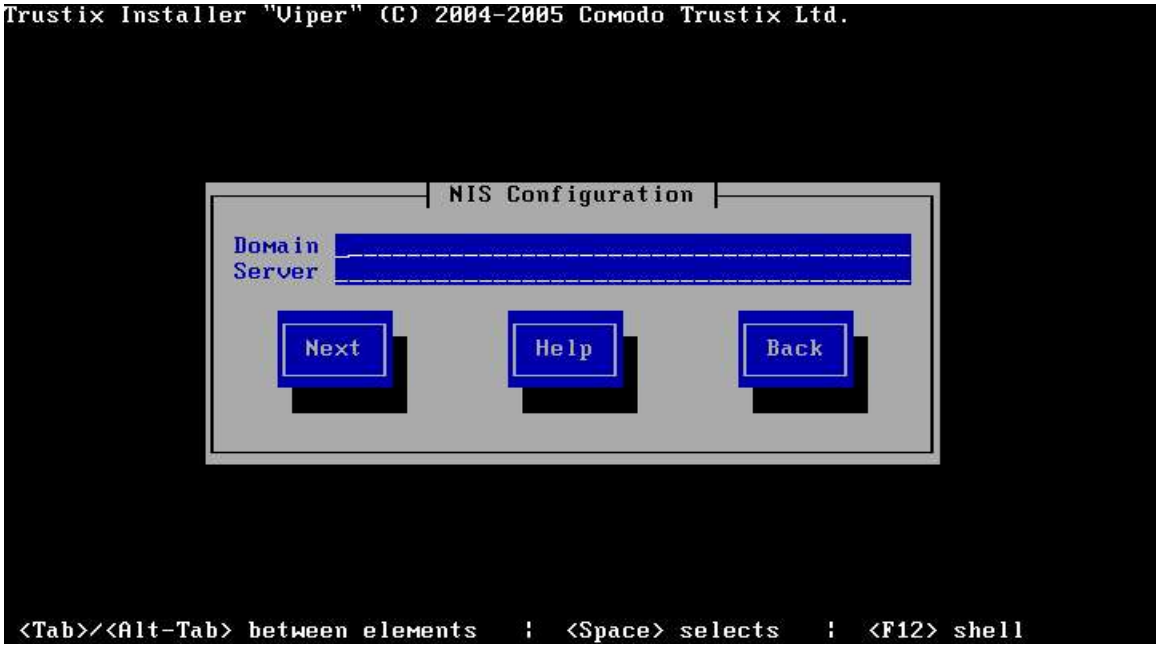
Provide the default shell required when logged in

As stated before, logging into a system is secured by verification of the username and password combination. This information, generally called user information, may be stored locally or remotely based on the interest and organization. Below are the methods of how user information is maintained and used.

NSCD

Cache User Information enables the name service cache daemon (nscd) and would start it at boot time.

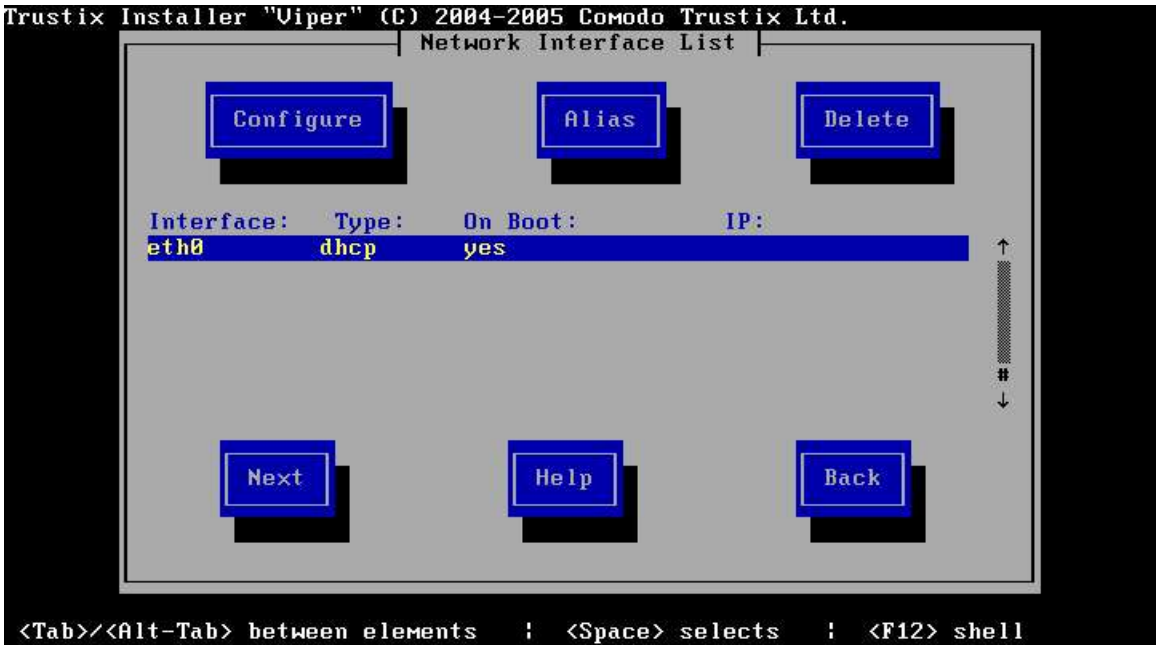
NIS



(Image 3.21)

NIS lookup configuration helps to authenticate user and password from an NIS server. This will start ypbind at boot time. The NIS server will be found via broadcast if NIS server is not specified.

3.5 Network Configuration



(Image 3.22)

The network configuration interface is used to configure the network devices.
Two different types of configurations are available:

- DHCP - Dynamic Host Configuration Protocol
- Static Configuration.

Network Interface List

Network interface list consists of all the real devices and aliases configured for the corresponding real devices.
By default all the devices will be configured as type as “DHCP” and on boot as “yes”

The screen contains the following fields:

Configure:

Configure the selected device or alias.

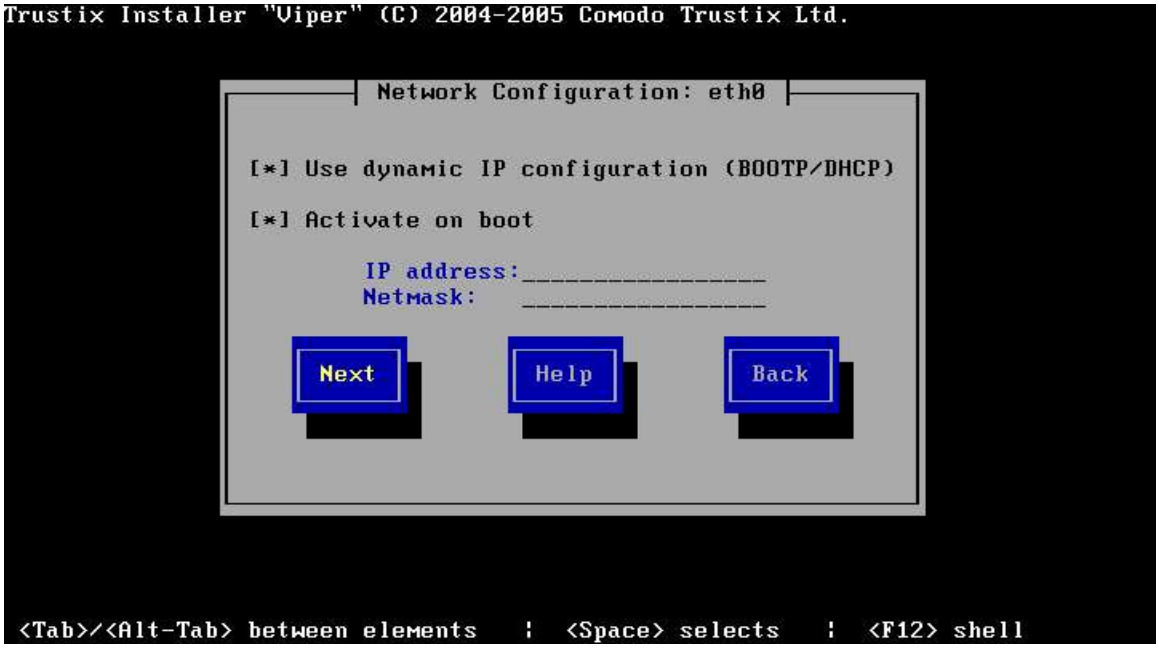
Alias:

Add an IP alias for the selected device.

Delete:

Delete the selected alias.

Network Configuration



(Image 3.23)

This interface lets the user enter configuration values for the selected network device. If the device has already been configured, the values will be prefilled, if not default values appear.

Dynamic IP configuration (BOOTP/DHCP)

Select the “Use dynamic IP configuration (BOOTP/DHCP)” and press space bar if the box is not already checked. (Pressing the space bar enables the check box.)

Enabling the check box will also disable the entry boxes “IP address” and “Netmask”, to make it impossible to edit these fields.

Static IP configuration

Deselect the “Use dynamic IP configuration (BOOTP/DHCP)” check box will configure the selected real device as STATIC device.
On disabling the check box will also enable the entry boxes “IP address” and “Netmask”, so the user can modify the values in these fields.

Activate on boot

Selecting the checkbox will activate the real device.

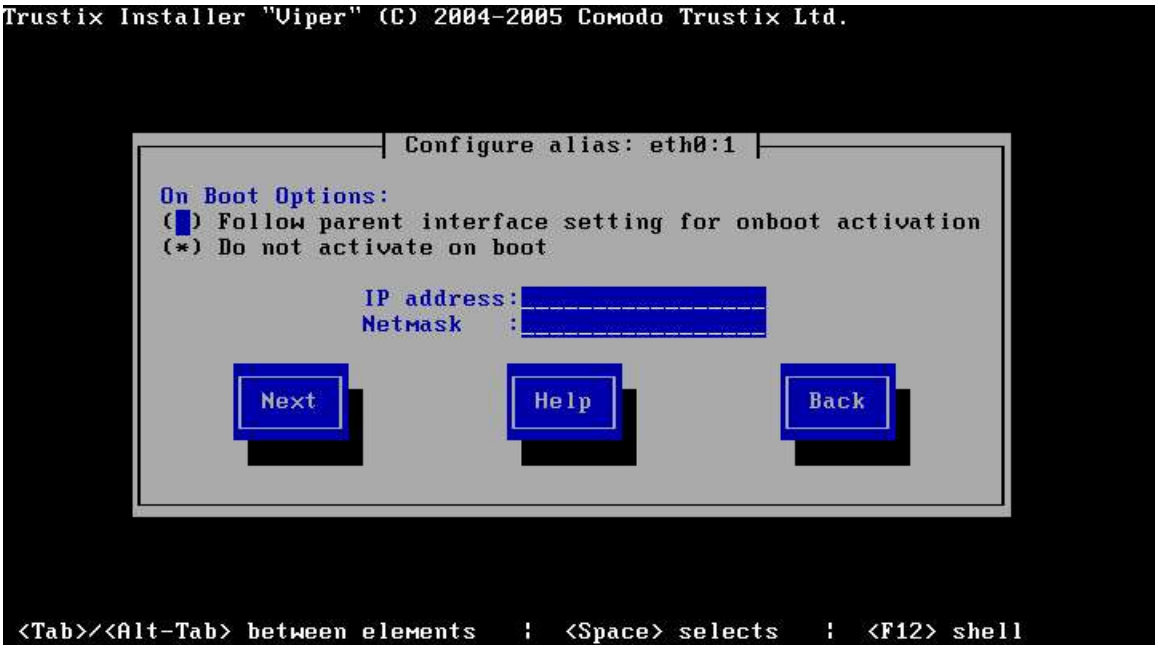
IP address

A valid IP address should be provided in the given entry to configure the real device with the corresponding address.

Netmask

The netmask entry is filled with the default subnet mask values. You can change the netmask entry value if required.

IP Alias Configuration



(Image 3.24)

Hitting the “Configure Alias” button in the network interface window shows a screen to configure the aliases for the selected device in the devices list. If the selected device is a real device, a window is shown to create a new alias. If it's an alias, the alias window shows the existing values for the alias configured already.

Boot Options

There are two boot options when configuring the alias:

Follow parent interface setting for onboot activation - use the boot options from the parent interface, and strictly follow any changes made on that interface.

Do not activate on boot - this option ensures that the alias is not activated when system is booted.

Gateway Configuration

(3.25)

The Configure gateway is displayed differently based on the number of interfaces and the network protocols used (static/DHCP).

Single Network Card

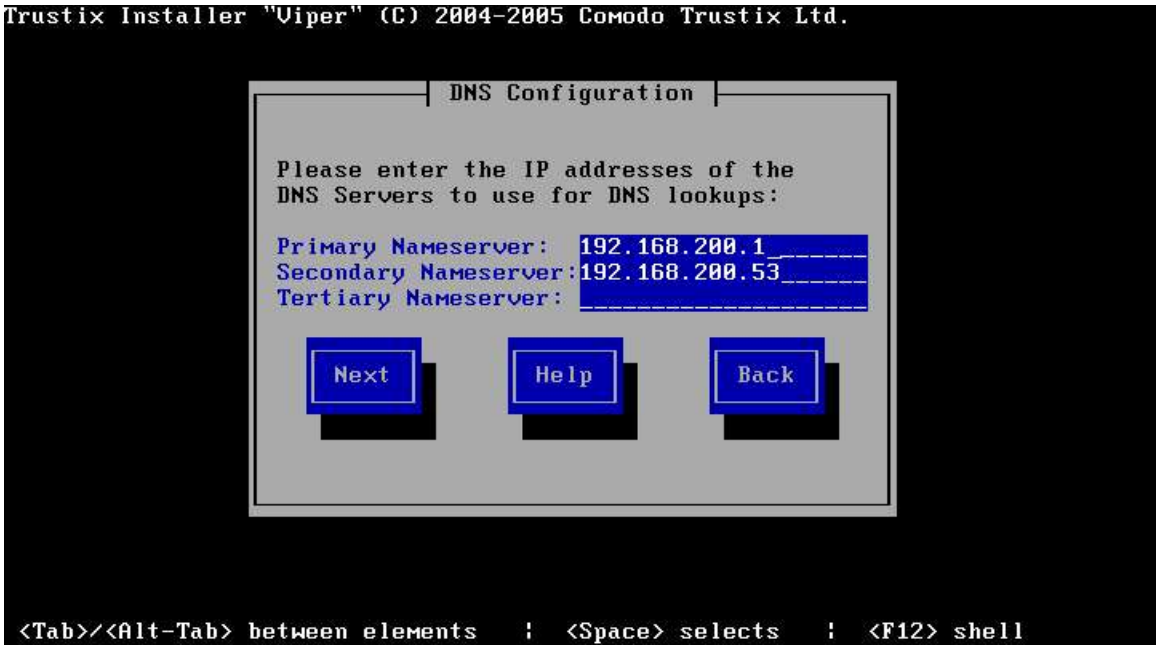
If there is only one network card and it is configured with DHCP, this window is skipped. If there is a single configured with static configuration, this window asks for a gateway value to be provided in the given entry (Image 3.25).

Multiple Network Cards

If there are multiple cards and they all are configured with DHCP, it shows a list of the real devices to which the gateway is to be set. If the mulitple cards have both the static and DHCP configurations, the gateway entry will be disabled for the DHCP

configured real devices whereas the user has to provide the gateway entry if a device configured is with a static configuration.

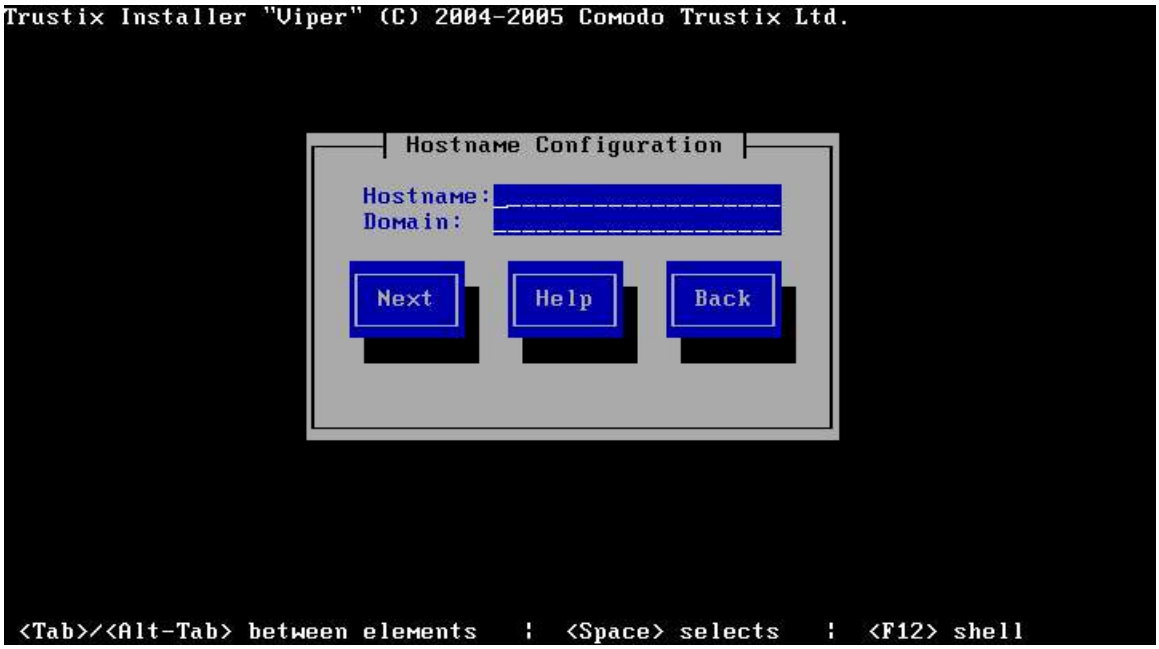
DNS Configuration



(Image 3.26)

DNS Configuration shows entries for providing the primary, secondary and tertiary name servers respectively. If the gateway device, i.e. the device to which the gateway is set is configured with DHCP, the the name server entries are fetched by default. If it is a statically configured device, only the primary name server is guessed based on the IP address.

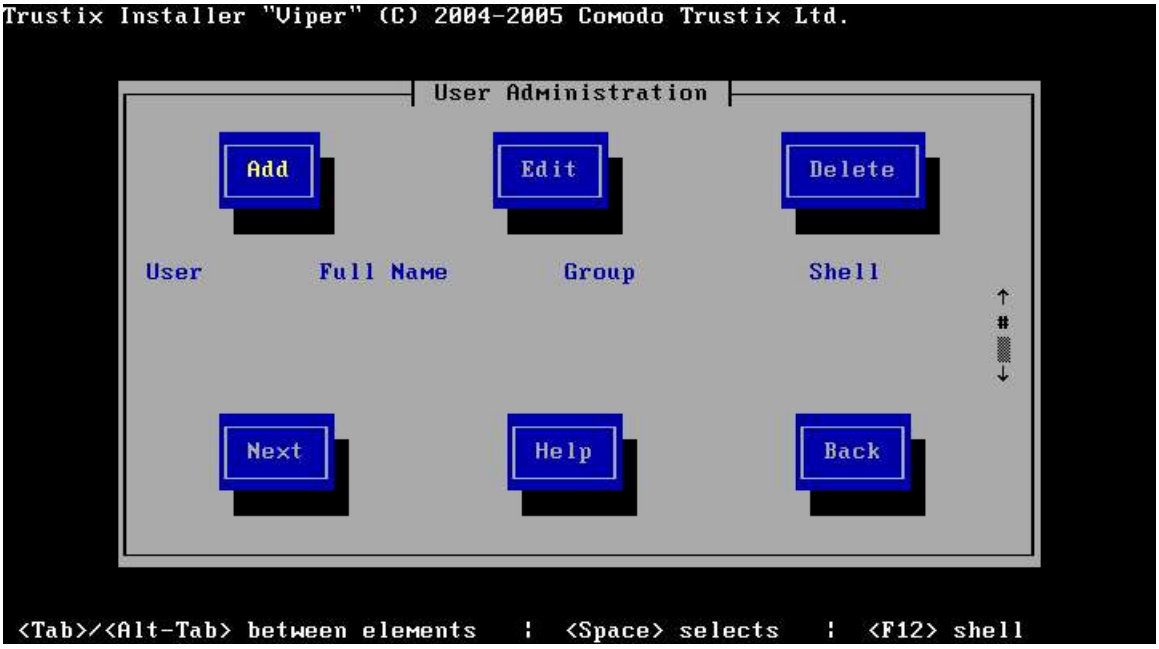
Hostname Configuration



(Image 3.27)

The Hostname configuration window shows the entries to provide the hostname and domain name for the system. The installer will try to autodetect the hostname and domain based on the information given when configuring the DNS servers. If the hostname is available from the given name servers, it is fetched along with the domain name.

3.6 User Administration

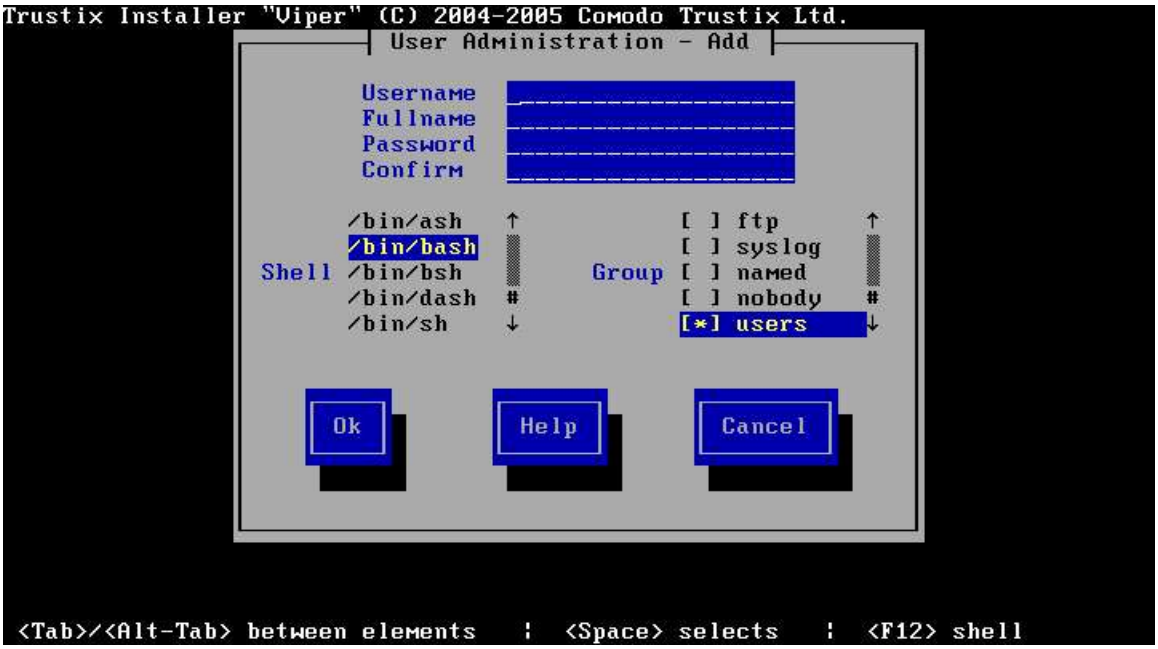


(Image 3.28)

It is always highly recommended to have a non-root user in the system. This ensures both safety and security as one may use a non-root user for normal system usage and use the root account only when it is required. Usually non root users are created after installation using the `useradd` command, but the installer provides a user administration utility as well.

The User Administration interface helps one to create, delete and also to edit non-root users. Remember that the root user, and several other system users, are always created by default and thus cannot be changed or edited. This utility provides for different aspects in the user creation and editing like the groups the user belongs to and the default shell that the user will use once he is logged in etc.

The first window shows up a list of added users and six buttons, three at the top and three at the bottom with the list in the middle. The list would be empty initially as there is no user created as of yet. The buttons at the top provides for the functionality of this utility and the buttons below is to navigate back or next, for help you can always click the help button.



(Image 3.29)

Clicking the Add button would show up the window shown in image 3.29. This window consists of the values required to create a user, out of which some are optional.

To create a user, the first thing required is the username (in fact this is the only one you need to provide apart from password, as all other values are either optional or have been provided by default). A username can be any alphanumeric value and can also consists of some characters like '-', but cannot have any whitespace (spaces, tabs etc.) as a character.

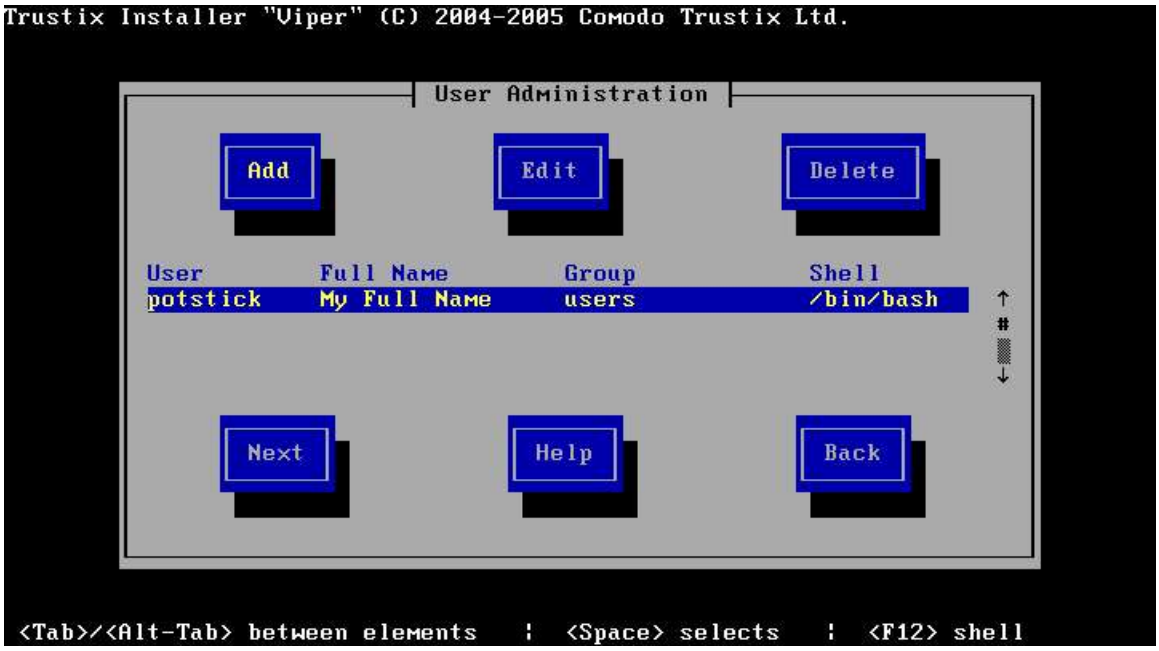
The full name field asks just for the actual name for the user that is going to be created and is optional.

The password fields are to be filled as a user cannot be logged into as long as the user doesn't have a valid password. For security reason Viper doesn't allow to create a password less than 6 characters and the password is also limited to 128 characters. Passwords can usually be of any character.

Any user that are going to log in needs a shell, Viper gives you the choice of what shell to be used for each user. By default the bash shell is chosen.

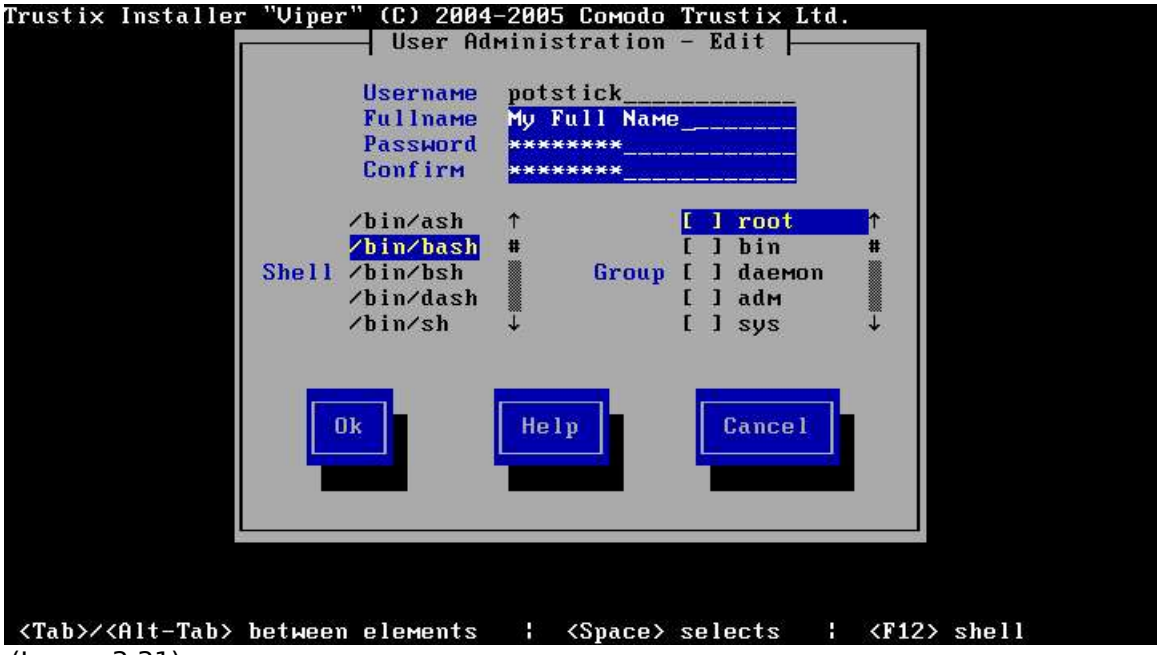
A user may belong to a group or groups, this is usually done to categorize users or to organize them. This also helps in providing group access to files or applications etc. By default Viper puts a user in the user group, but of course the user can change it or select multiple groups as required.

Once all the required fields are filled one can press next and the first window shows up with new user listed in it. In this way as many users as required can be created.



(Image 3.30)

To delete a user, one have to just select the desired user and press the delete button. This would immediately remove the user from the list.

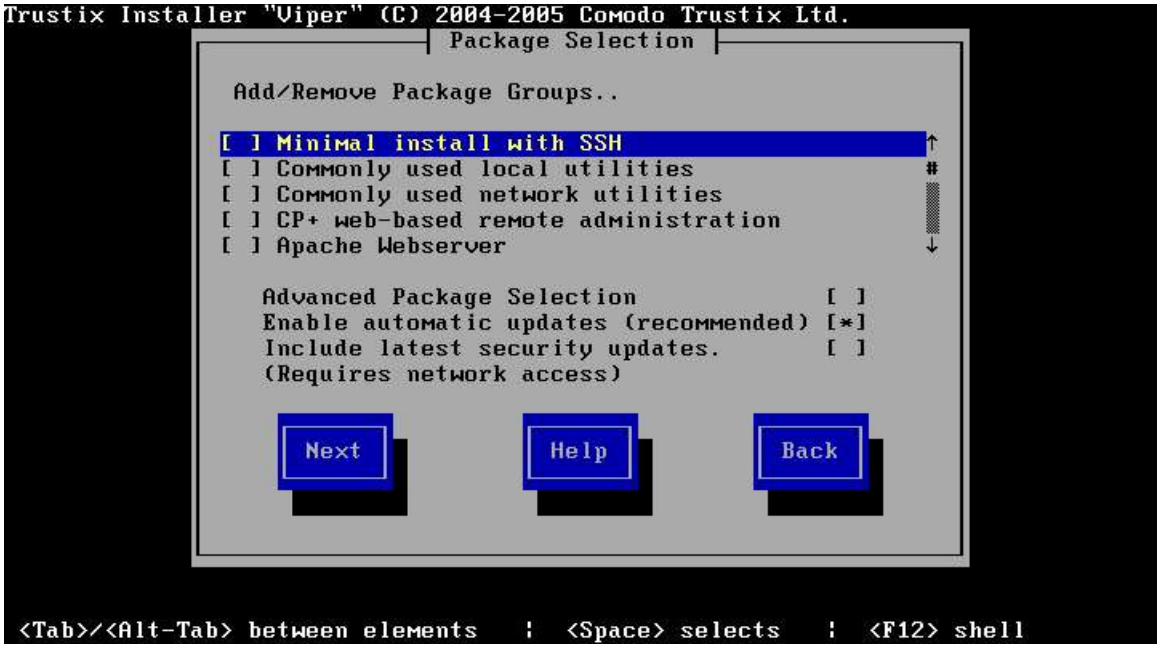


(Image 3.31)

To edit an existing user, One may select the desired user and click the edit button. This would show up a window similar to the add window except for the values filled in the corresponding locations.

One may edit almost anything except for the username, because editing the username is same as creating a new user. Once the editing is over the next button would take one to the first window. The user may then continue as required. The help button is provided in every window, which can be used if any confusion arises.

3.7 Package Selection



(Image 3.32)

The swup module has settings to install packages, select mirrors and use automatic updates.

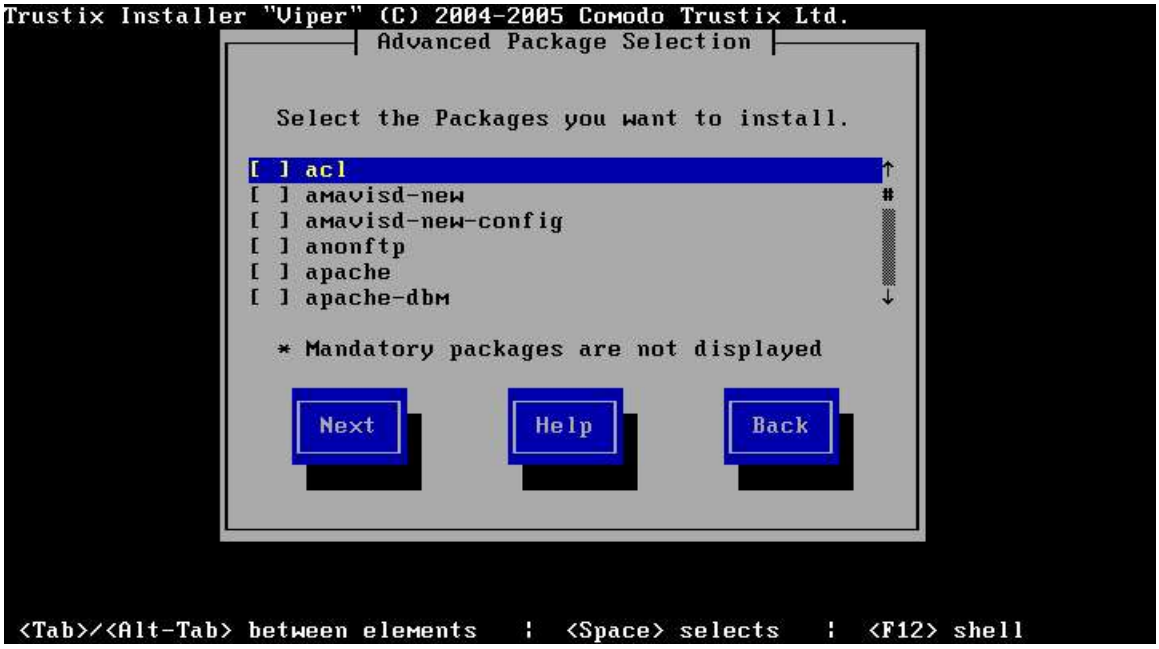
This window lists the available Trustix installation groups, you can select and deselect package groups with the space key.

You can also select packages individually using advanced package selection option.

The enable automatic updates checkbox adds the “swup-cron” package to your list of packages to install, this package adds a cron-job entry for swup to perform periodical automatic updates.

You can select “Include latest security updates” to install package updates from the network or internet. If packages are up to date on the primary installation media (usually the CDROM) they will be preferred, if the remote packages are of newer version, they will be downloaded over the network to produce an up to date system from day 0.

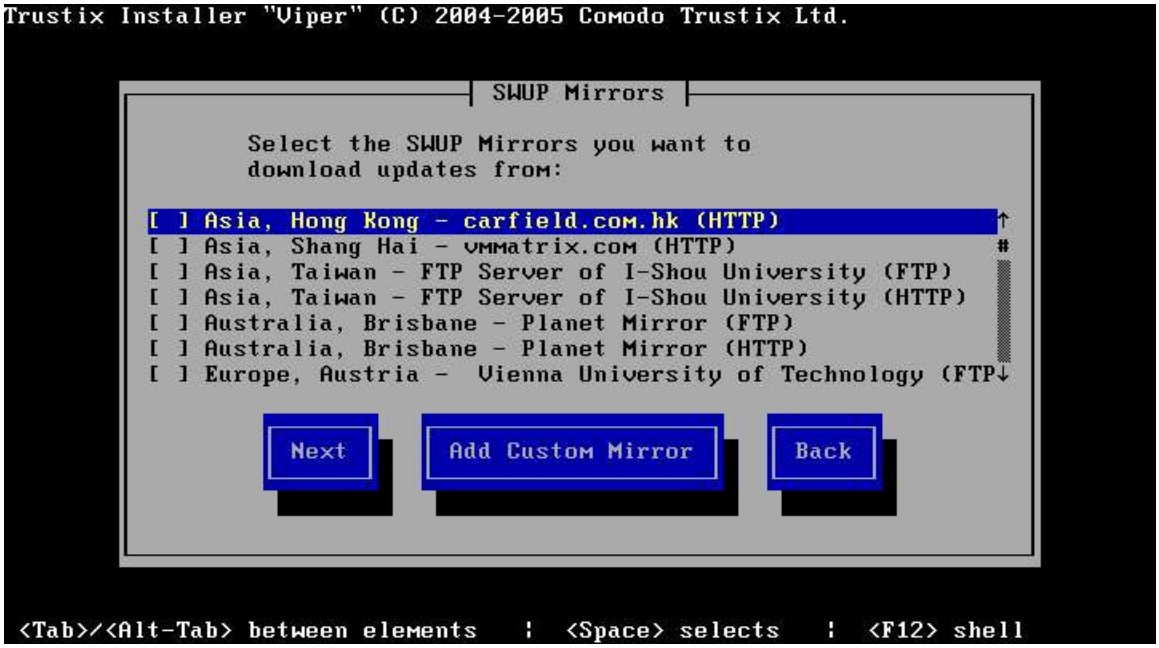
Advanced Package Selection



(Image 3.33)

You can select individual packages using this window.

Swup Mirror Selection



(Image 3.34)

This window lists the available swup mirrors fetched from trustix website from where you can perform a network install. you can also chose to add your own custom mirror which are not part of trustix list of known mirrors by using the “add custom mirror” option.

Custom Mirror

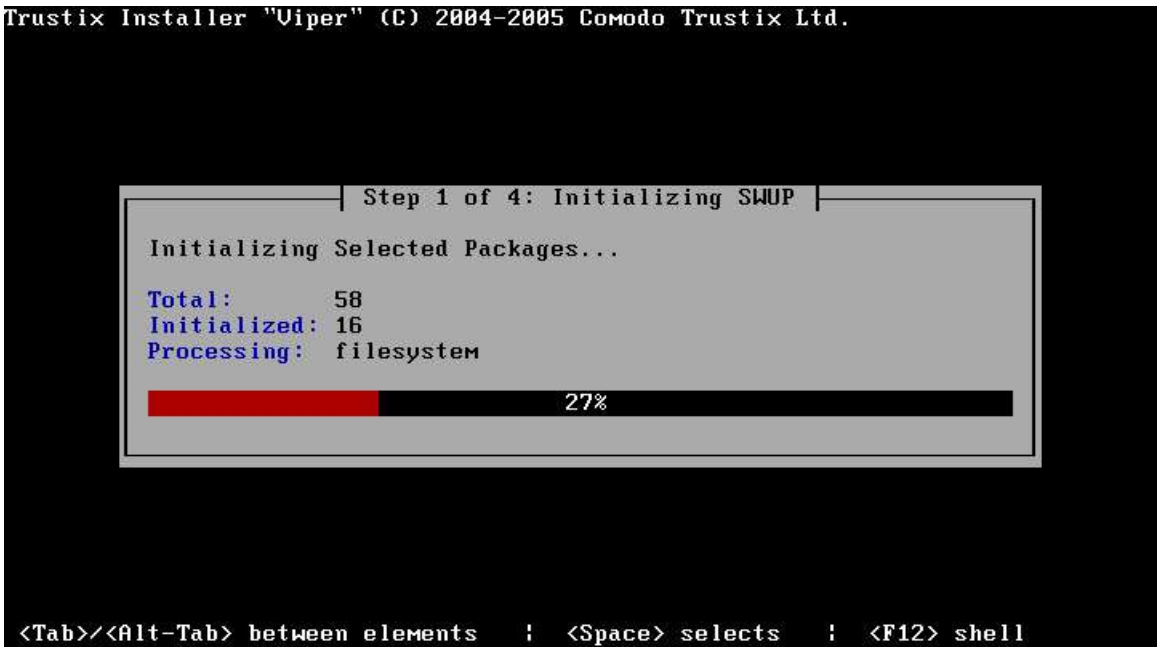
(Image 3.34)

Using the Custom mirror window, you can specify the mirror and it gets added to the list of mirrors to fetch packages from.

SWUP Installation Stages

The package installation is performed by SWUP, the secure software updater used in Trustix Secure Linux systems. The package installation is split into 4 steps:

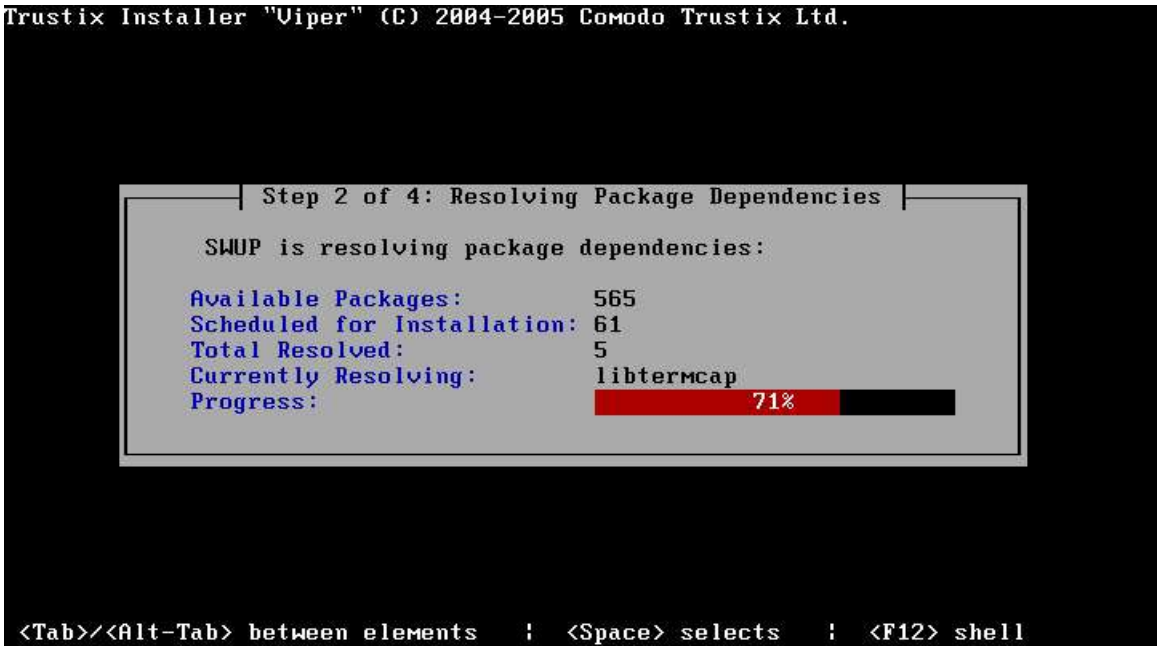
4.1 Initializing Selected Packages



(Image 4.1)

The first of the four steps of the package installation consists of grabbing information about the packages that are selected to be installed. Depending on the number of packages selected and the speed of any selected remote networked mirrors, this might take some time.

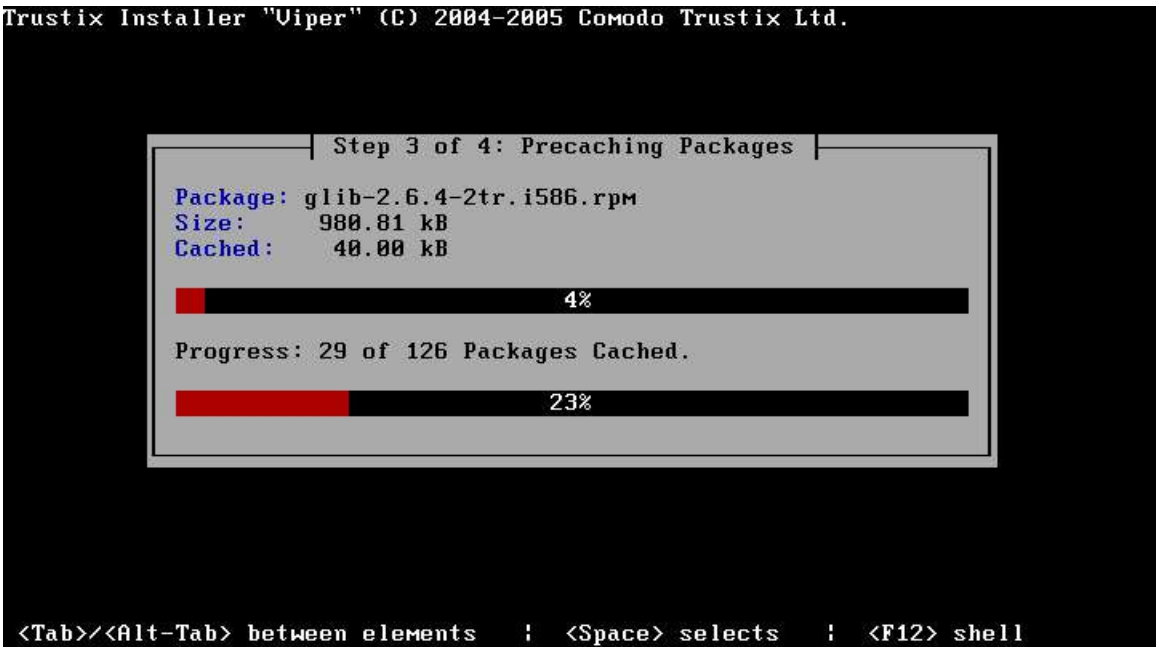
4.2 Resolving Dependencies



(Image 4.2)

The second step involves resolving any package dependencies. Each package may depend on 0 or many other packages, and these dependencies must be met for the package to install properly.

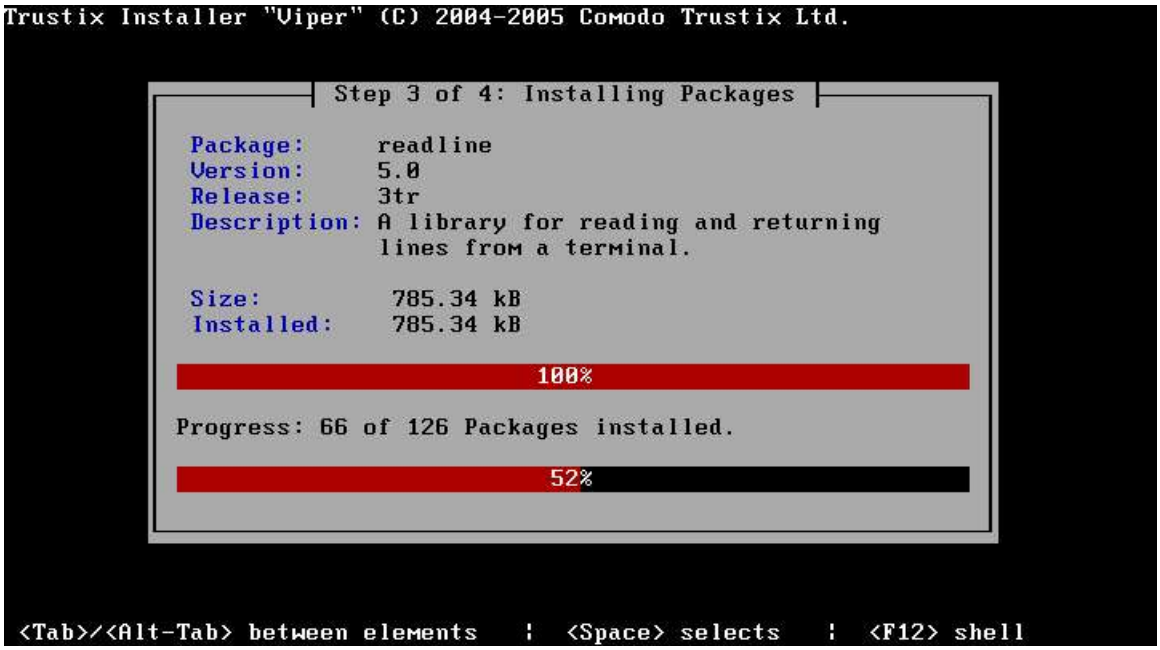
4.3 Precaching Packages



(Image 4.3)

The third step is to download packages from the network and the primary installation media to the filesystem. If not all packages are found on the primary installation media or on the network, one will be asked to insert additional CDs.

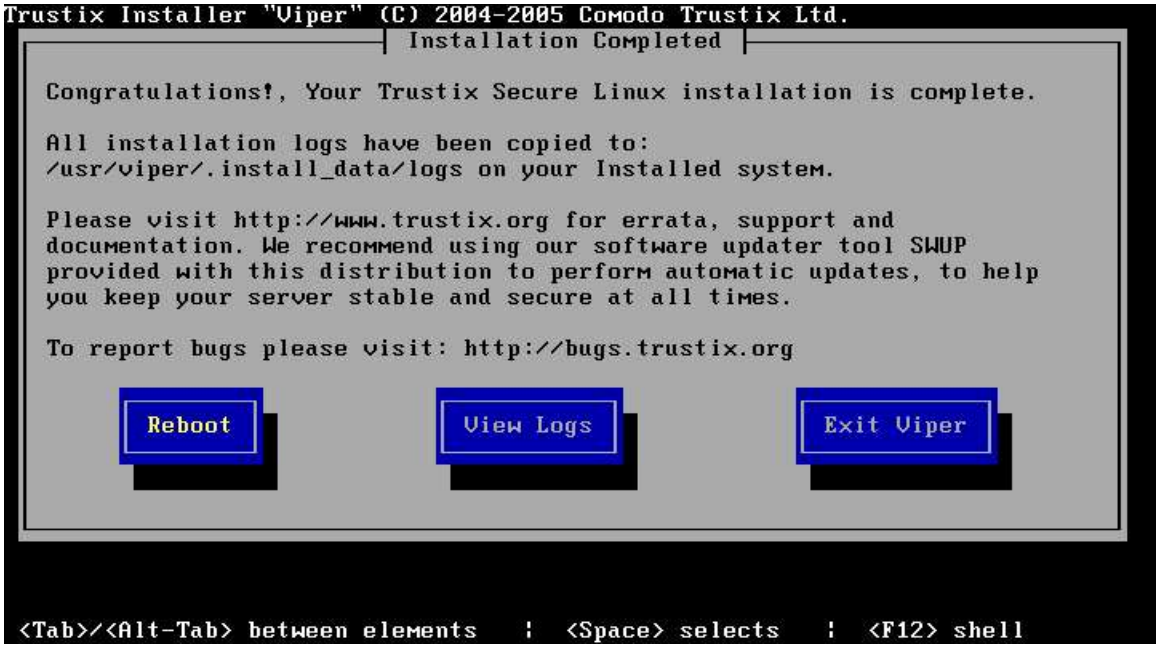
4.4 Installing Packages



(Image 4.4)

The last step of the Package Installation is actually installing the packages. Depending on the number of packages, this might take a while. Progress bars are provided for monitoring the process.

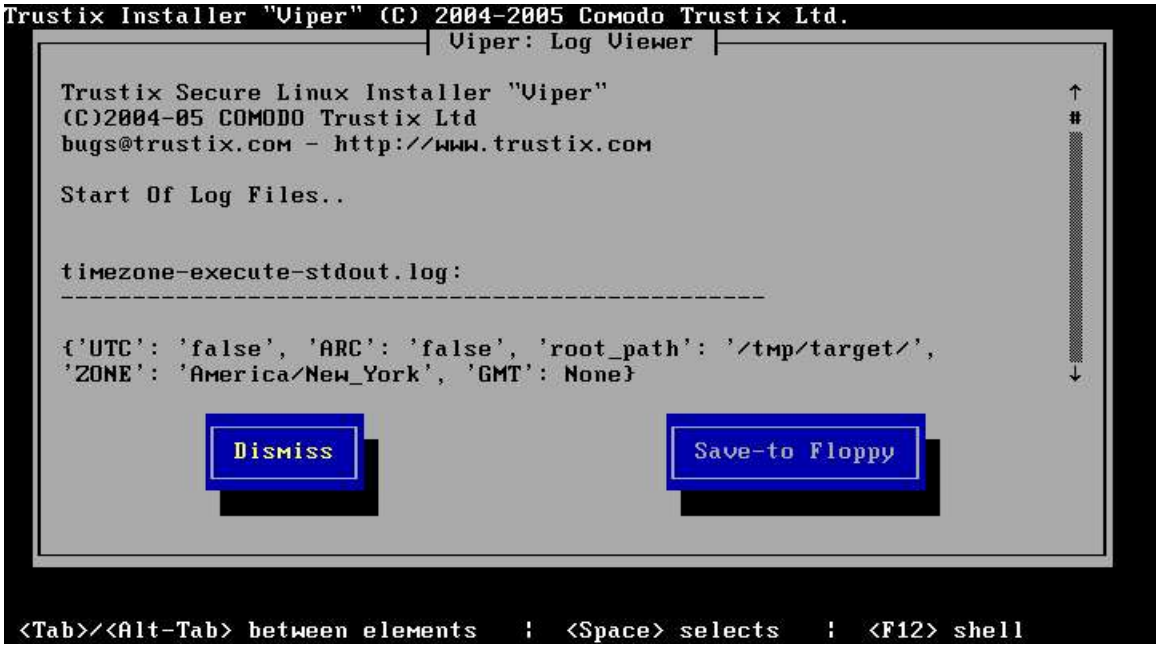
Finish Window



(Image 5.1)

The finish window displays options to reboot, view viper logs or exit viper to a console. You can use terminal 2 to inspect contents of /tmp/target where your installation root is mounted. As soon as you exit Viper, all mounts are unmounted and finalized.

5.1 Log window



(Image 5.2)

Using the log window you can view all the information about viper and other modules. You can also chose to save the logs to a floppy for reviewing your installation and settings

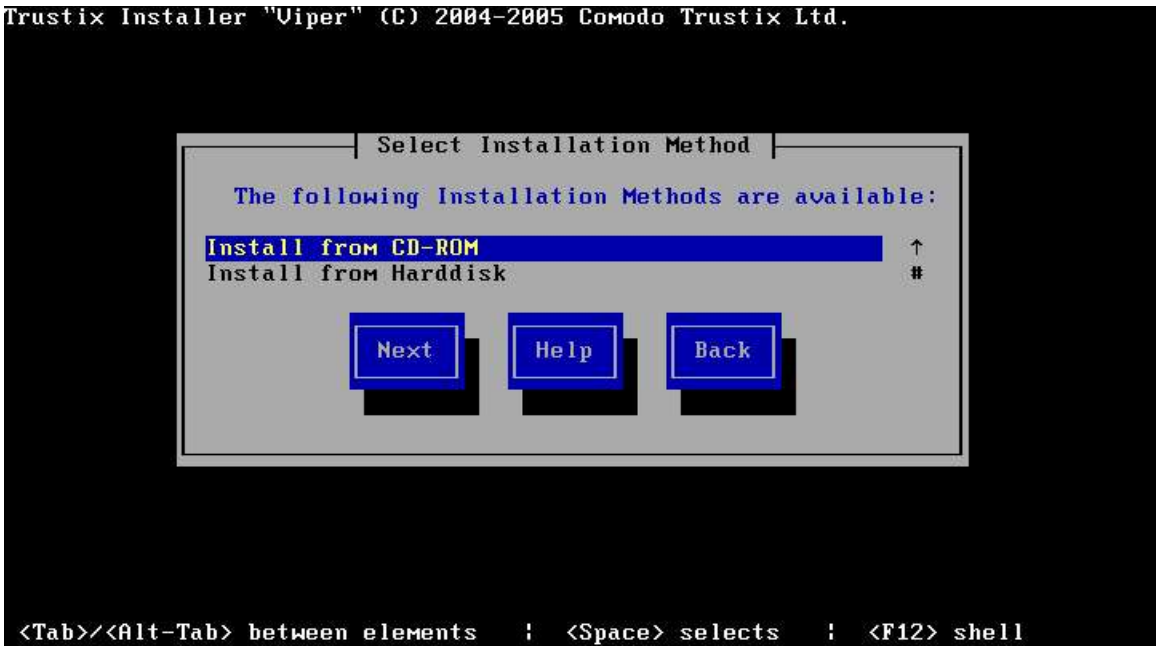
PXE, Hardware Detection, and Network install

(Image 6.1)

This window detects available hardware devices and prompts the user to load available kernel modules for the hardware to be detected.

If no CD-ROM or Network is found and no valid kernel modules are loaded, the installation media selection window is displayed.

6.1 Installation Media Selection (PXE-BOOT)



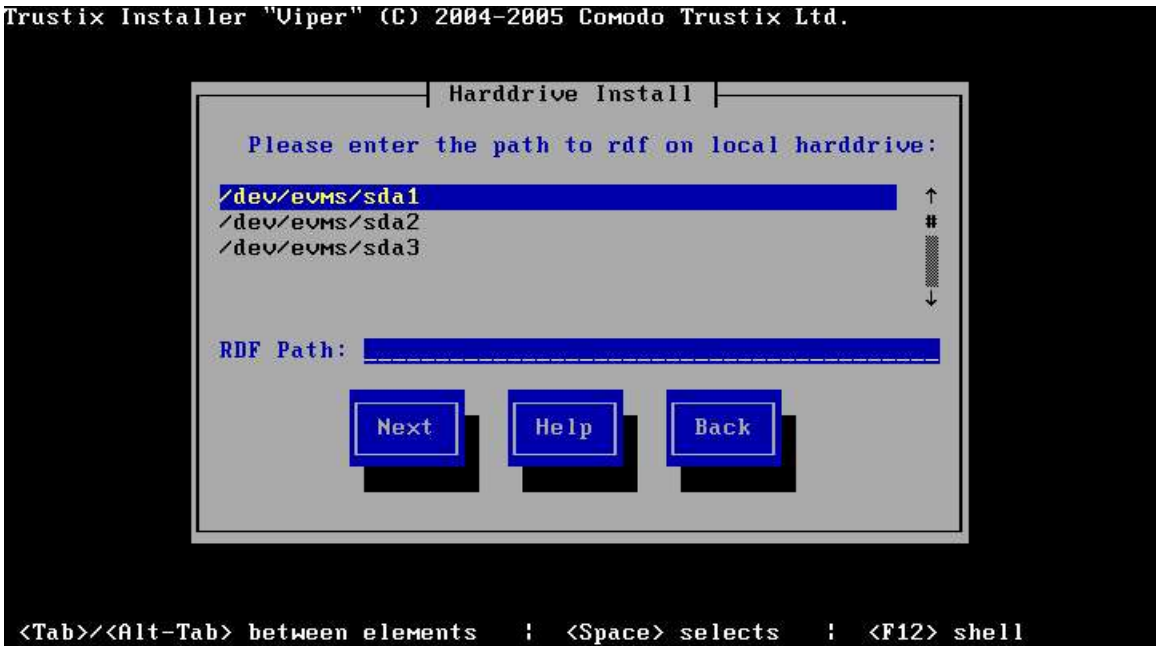
(Image 6.2)

This window pops up in case of a PXE boot without cd-rom or a computer which has no network interface.

This Window has the following options

List of installation methods available and navigation buttons.

6.2 Installation from hard-drive



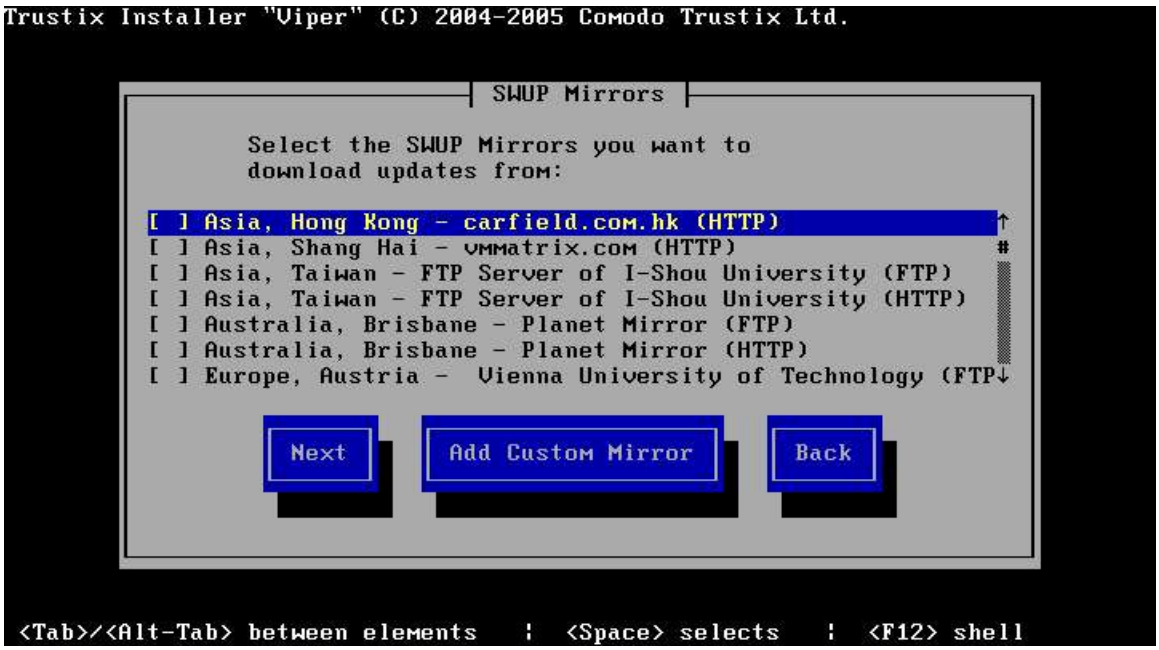
(Image 6.3)

This window pops-up on selecting the installation from harddrive option in the alternate installation media selection window.

You can select any one of the list of available partitions and the path where you have the rpm's and rdf's.

Warning: Care should be taken that you don't delete the partition which contains the rdf's and rpm's deleted during partitioning

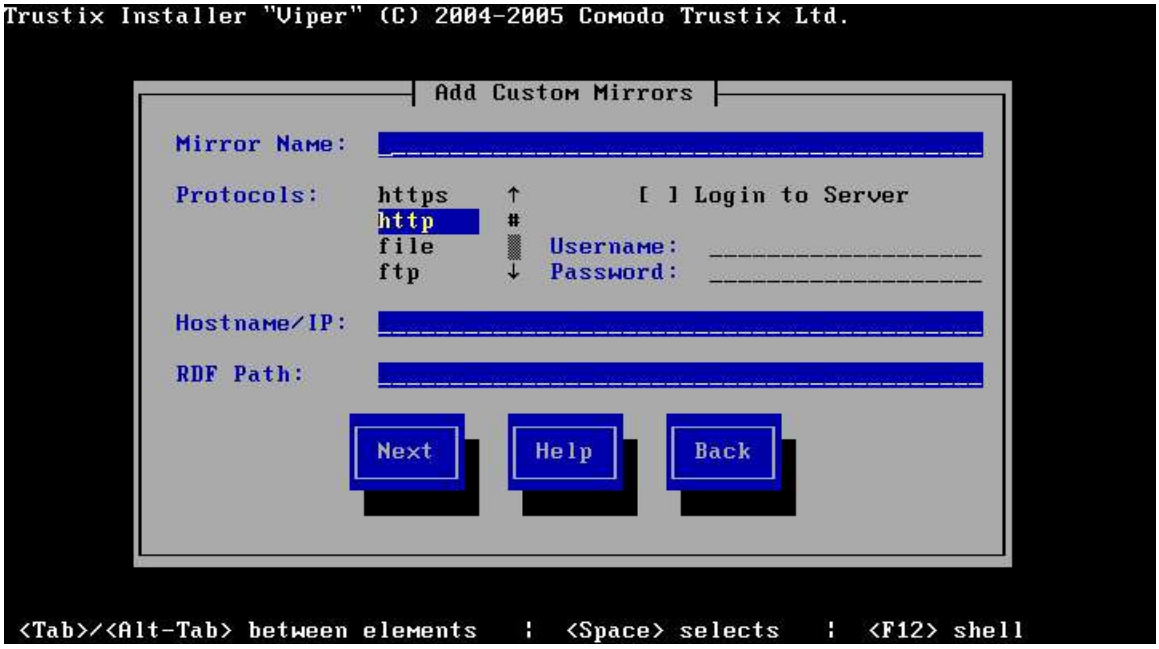
6.3 Network Installation + Swup Mirror Selection



(Image 6.4)

This window lists the available swup mirrors fetched from trustix website from where you can perform a network install. you can also chose to add your own custom mirror which are not part of trustix list of known mirrors by using the add custom mirror option.

Custom Mirror



(Image 6.5)

Using the Custom mirror window, you can specify the mirror and it gets added to the list of mirrors to fetch packages from. This is useful if you have several servers and want to save bandwidth by mirroring locally.

System Requirements

The following is the minimal system requirements for Trustix Secure Linux 3.0:

- Intel i586 compatible processor
- 64 MB RAM
- 2 * Size of RAM + 500MB HD

It is highly recommended that the system has a Network Interface Controller (NIC), although it will install and boot without it, provided a usable installation media is available.

It is also recommended that the system has a CDROM, since the CD is the primary installation media. However, several means if installation without CDROM exists and is supported.

Acknowledgement

Troubleshooting