Red Hat Enterprise Linux 7

Installation Guide

Installing Red Hat Enterprise Linux 7.4 on all architectures

Last Updated: 2017-11-23

Red Hat Enterprise Linux 7 Installation Guide

Installing Red Hat Enterprise Linux 7.4 on all architectures

Petr Bokoč
Red Hat Customer Content Services
pbokoc@redhat.com

Clayton Spicer
Red Hat Customer Content Services

Tomáš Čapek
Red Hat Customer Content Services

Barbora Ančincová
Red Hat Customer Content Services

Yoana Ruseva
Red Hat Customer Content Services

Brian Exelbierd
Red Hat Customer Content Services

Jack Reed
Red Hat Customer Content Services

Radek Bíba
Red Hat Customer Content Services

Zac Dover
Red Hat Customer Content Services

Legal Notice

Abstract

This manual explains how to boot the Red Hat Enterprise Linux 7.4 installation program (Anaconda) and how to install Red Hat Enterprise Linux 7.4 on AMD64 and Intel 64 systems, 64-bit IBM Power Systems servers, and IBM System z. It also covers advanced installation methods such as Kickstart installations, PXE installations, and installations over VNC. Finally, it describes common post-installation tasks and explains how to troubleshoot installation problems. Information on installing Red Hat Enterprise Linux Atomic Host can be found in the Red Hat Enterprise Linux Atomic Host Installation and Configuration Guide.

Table of Contents

CHAPTER 1. GETTING STARTED

You can install Red Hat Enterprise Linux with an installation utility called **Anaconda**. Most users can simply follow the procedure outlined in Section 4.1, “Interactive Installation” to install Red Hat Enterprise Linux using the graphical interface in **Anaconda**.

Users with advanced requirements can also use the graphical interface to configure many aspects of the installation, and install Red Hat Enterprise Linux on a wide variety of systems. On systems without a local interface, installation can be accessed entirely remotely. Installation can also be automated by using a **Kickstart** file, and performed with no interaction at all.

1.1. GRAPHICAL INSTALLATION

The Red Hat Enterprise Linux installer, **Anaconda**, provides a simple graphical method to install Red Hat Enterprise Linux. The graphical installation interface has a built-in help system which can guide you through most installations, even if you have never installed Linux before. However, **Anaconda** can also be used to configure advanced installation options if required.

Anaconda is different from most other operating system installation programs due to its parallel nature. Most installers follow a linear path; you must choose your language first, then you configure networking, and so on. There is usually only one way to proceed at any given time.

In the graphical interface in **Anaconda** you are at first only required to select your language and locale, and then you are presented with a central screen, where you can configure most aspects of the installation in any order you like. While certain parts require others to be completed before configuration - for example, when installing from a network location, you must configure networking before you can select which packages to install - most options in **Anaconda** can be configured in any order. If a background task, such as network initialization or disk detection, is blocking configuration of a certain option, you can configure unrelated options while waiting for it to complete.

Additional differences appear in certain screens; notably the custom partition process is very different from other Linux distributions. These differences are described in each screen's subsection.

Some screens will be automatically configured depending on your hardware and the type of media you used to start the installation. You can still change the detected settings in any screen. Screens which have not been automatically configured, and therefore require your attention before you begin the installation, are marked by an exclamation mark. You cannot start the actual installation process before you finish configuring these settings.

Installation can also be performed in text mode, however certain options, notably including custom partitioning, are unavailable. See Section 8.3, “Installing in Text Mode”, or if using an IBM Power system or IBM System z, see Section 13.3, “Installing in Text Mode”, or Section 17.4, “Installing in Text Mode”, respectively, for more information.

1.2. REMOTE INSTALLATION

You can use the graphical interface remotely to install Red Hat Enterprise Linux. For headless systems, **`Connect Mode`** can be used to perform a graphical installation completely remotely. For systems with a display and keyboard, but without the capacity to run the graphical interface, **`Direct Mode`** can instead be used to facilitate setup. For more information, see the Chapter 24, *Using VNC*.

1.3. AUTOMATED INSTALLATION

Anaconda installations can be automated through the use of a **Kickstart** file. **Kickstart** files can be used to configure any aspect of installation, allowing installation without user interaction, and can be used to easily automate installation of multiple instances of Red Hat Enterprise Linux.

In most situations, you can simply follow the procedure outlined in Section 4.2, “Automatic Installation” to create and configure a **Kickstart** file, which can be used to perform an arbitrary number of non-interactive installations of Red Hat Enterprise Linux.

Kickstart files can be automatically created based on choices made using the graphical interface, through the online *Kickstart Generator* tool, or written from scratch using any text editor. For more information, see Section 26.2.1, “Creating a Kickstart File”.

Kickstart files can be easily maintained and updated using various utilities in Red Hat Enterprise Linux. For more information, see Section 26.2.2, “Maintaining the Kickstart File”.

CHAPTER 2. DOWNLOADING RED HAT ENTERPRISE LINUX

If you have a Red Hat subscription, you can download *ISO image files* of the Red Hat Enterprise Linux 7 installation DVD from the Red Hat Customer Portal. If you do not have a subscription, either purchase one or obtain a free evaluation subscription from the Software & Download Center at https://access.redhat.com/downloads/.

There are two basic types of installation media available on the AMD64 and Intel 64 (x86_64) and IBM Power Systems (ppc64) architectures:

Binary DVD

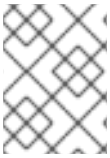
A full installation image which can be used to boot the installation program and perform an entire installation without additional package repositories.

boot.iso

A minimal boot image which can be used to boot the installation program, but requires access to additional package repositories from which software will be installed. Red Hat does not provide such a repository; you must create it using the full installation ISO image.

Supplementary DVD

An image containing additional packages, such as the IBM Java Runtime Environment, and additional virtualization drivers.



NOTE

Binary DVDs are also available for IBM System z. They can be used to boot the installation program using a SCSI DVD drive or as installation sources.

The following table indicates the types of boot and installation media available for different architectures and notes the image file that you need to produce the media.

Table 2.1. Boot and Installation Media

Architecture	Minimal boot image	Full installation image
AMD64 and Intel 64	**`rhel-variant-7.4-x86_64-boot.iso`**	**`rhel-variant-7.4-x86_64-dvd.iso`**
IBM Power Systems (big endian)	**`rhel-variant-7.4-ppc64-boot.iso`**	**`rhel-variant-7.4-ppc64-dvd.iso`**
IBM Power Systems (little endian)	**`rhel-variant-7.4-ppc64le-boot.iso`**	**`rhel-variant-7.4-ppc64le-dvd.iso`**
Replace *variant* with your chosen variant of Red Hat Enterprise Linux (for example, `server` or `workstation`).		

Architecture	Minimal boot image	Full installation image
IBM System z	Not available	**rhel-*variant*-7.4-s390x-dvd.iso**
Replace *variant* with your chosen variant of Red Hat Enterprise Linux (for example, `server` or `workstation`).		

If you have a subscription or evaluation subscription, follow these steps to obtain the Red Hat Enterprise Linux 7 ISO image files:

Procedure 2.1. Downloading Red Hat Enterprise Linux ISO Images

1. Visit the Customer Portal at https://access.redhat.com/home. If you are not logged in, click **LOG IN** on the right side of the page. Enter your account credentials when prompted.
2. Click **DOWNLOADS** at the top of the page.
3. Click **Red Hat Enterprise Linux**.
4. Ensure that you select the appropriate **Product Variant** and **Architecture** for your installation target. By default, **Red Hat Enterprise Linux Server** and **x86_64** are selected. If you are not sure which variant best suits your needs, see http://www.redhat.com/en/technologies/linux-platforms/enterprise-linux. Additionally, a list of packages available for every variant is available in the Red Hat Enterprise Linux 7 Package Manifest.
5. A list of available downloads is displayed; most notably, a minimal **Boot ISO** image and a full installation **Binary DVD** ISO image. These files are described above. Additional images can be available, such as preconfigured virtual machine images, which are beyond the scope of this document.
6. Choose the image file that you want to use. You have two ways to download it from the Customer Portal:
   - Click its name to begin downloading it to your computer using your web browser.
   - Right-click the name and then click **Copy Link Location** or a similar menu item, the exact wording of which depends on the browser that you are using. This action copies the URL of the file to your clipboard, which allows you to use an alternative application to download the file to your computer. This approach is especially useful if your Internet connection is unstable: in that case, you browser might fail to download the whole file, and an attempt to resume the interrupted download process fails because the download link contains an authentication key which is only valid for a short time. Specialized applications such as **curl** can, however, be used to resume interrupted download attempts from the Customer Portal, which means that you need not download the whole file again and thus you save your time and bandwidth consumption.

     Procedure 2.2. Using curl to Download Installation Media

     1. Make sure the curl package is installed by running the following command as root:

        ```
        # yum install curl
        ```

If your Linux distribution does not use **yum**, or if you do not use Linux at all, download the most appropriate software package from the curl web site.

2. Open a terminal window, enter a suitable directory, and type the following command:

```
$ curl -o filename.iso 'copied_link_location'
```

Replace *filename.iso* with the ISO image name as displayed in the Customer Portal, such as **rhel-server-7.0-x86_64-dvd.iso**. This is important because the download link in the Customer Portal contains extra characters which **curl** would otherwise use in the downloaded file name, too. Then, keep the single quotation mark in front of the next parameter, and replace *copied_link_location* with the link that you have copied from the Customer Portal; copy it again if you copied the commands above in the meantime. Note that in Linux, you can paste the content of the clipboard into the terminal window by middle-clicking anywhere in the window, or by pressing **Shift**+**Insert**. Finally, use another single quotation mark after the last parameter, and press **Enter** to run the command and start transferring the ISO image. The single quotation marks prevent the command line interpreter from misinterpreting any special characters that might be included in the download link.

Example 2.1. Downloading an ISO image with curl

The following is an example of a **curl** command line:

```
$ curl -o rhel-server-7.0-x86_64-dvd.iso
'https://access.cdn.redhat.com//content/origin/files/sha256/
85/85a...46c/rhel-server-7.0-x86_64-dvd.iso?
_auth_=141...7bf'
```

Note that the actual download link is much longer because it contains complicated identifiers.

3. If your Internet connection does drop before the transfer is complete, refresh the download page in the Customer Portal; log in again if necessary. Copy the new download link, use the same basic **curl** command line parameters as earlier but be sure to use the new download link, and add **-C -** to instruct **curl** to automatically determine where it should continue based on the size of the already downloaded file.

Example 2.2. Resuming an interrupted download attempt

The following is an example of a **curl** command line that you use if you have only partially downloaded the ISO image of your choice:

```
$ curl -o rhel-server-7.0-x86_64-dvd.iso
'https://access.cdn.redhat.com//content/origin/files/sha256/
85/85a...46c/rhel-server-7.0-x86_64-dvd.iso?
_auth_=141...963' -C -
```

7. Optionally, you can use a checksum utility such as **sha256sum** to verify the integrity of the image file after the download finishes. All downloads on the Download Red Hat Enterprise Linux page are provided with their checksums for reference:

```
$ sha256sum rhel-server-7.0-x86_64-dvd.iso
   85a...46c rhel-server-7.0-x86_64-dvd.iso
```

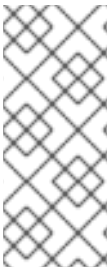
Similar tools are available for Microsoft Windows and Mac OS X. You can also use the installation program to verify the media when starting the installation; see Section 22.2.2, “Verifying Boot Media” for details.

After you have downloaded an ISO image file from the Customer Portal, you can:

- Burn it to a CD or DVD as described in Section 3.1, “Making an Installation CD or DVD”.
- Use it to create a bootable USB drive; see Section 3.2, “Making Installation USB Media”.
- Place it on a server to prepare for a network installation. For specific directions, see Section 3.3.3, “Installation Source on a Network”.
- Place it on a hard drive to use the drive as an installation source. For specific instructions, see Section 3.3.2, “Installation Source on a Hard Drive”.
- Use it to prepare a *Preboot Execution Environment* (PXE) server, which allows you to boot the installation system over a network. See Chapter 23, *Preparing for a Network Installation* for instructions.

CHAPTER 3. MAKING MEDIA

This chapter describes how to use ISO image files obtained by following the steps in Chapter 2, *Downloading Red Hat Enterprise Linux* to create bootable physical media, such as a DVD or a USB flash drive. You can then use these media to boot the installation program and start the installation. These steps only apply if you plan to install Red Hat Enterprise Linux on an AMD64 or Intel 64 system or an IBM Power Systems server using physical boot media. For information about installing Red Hat Enterprise Linux on an IBM System z server, see Chapter 16, *Booting the Installation on IBM System z*. For instructions on how to set up a *Preboot Execution Environment* (PXE) server to perform a PXE-based installation over a network, see Chapter 23, *Preparing for a Network Installation*.

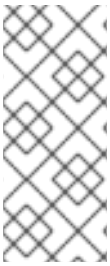


NOTE

By default, the **`inst.stage2=`** boot option is used on the installation media and set to a specific label (for example, **`inst.stage2=hd:LABEL=RHEL7\x20Server.x86_64`**). If you modify the default label of the file system containing the runtime image, or if using a customized procedure to boot the installation system, you must ensure this option is set to the correct value. See Specifying the Installation Source for details.

3.1. MAKING AN INSTALLATION CD OR DVD

You can make an installation CD or DVD using burning software on your computer and a CD/DVD burner. The exact series of steps that produces an optical disc from an ISO image file varies greatly from computer to computer, depending on the operating system and disc burning software installed. Consult your burning software's documentation for the exact steps needed to burn a CD or DVD from an ISO image file.



NOTE

It is possible to use optical discs (CDs and DVDs) to create both minimal boot media and full installation media. However, it is important to note that due to the large size of the full installation ISO image (between 4 and 4.5 GB), only a DVD can be used to create a full installation disc. Minimal boot ISO is roughly 300 MB, allowing it to be burned to either a CD or a DVD.

Make sure that your disc burning software is capable of burning discs from image files. Although this is true of most disc burning software, exceptions exist. In particular, note that the disc burning feature built into Windows XP and Windows Vista cannot burn DVDs; and that earlier Windows operating systems did not have any disc burning capability installed by default at all. Therefore, if your computer has a Windows operating system prior to Windows 7 installed on it, you need a separate piece of software for this task. Examples of popular disc burning software for Windows that you might already have on your computer include **Nero Burning ROM** and **Roxio Creator**. Most widely used disc burning software for Linux, such as **Brasero** and **K3b**, also has the built-in ability to burn discs from ISO image files.

On some computers, the option to burn a disc from an ISO file is integrated into a context menu in the file browser. For example, when you right-click an ISO file on a computer with a Linux or UNIX operating system which runs the **GNOME** desktop, the **Nautilus** file browser presents you with the option to **Write to disk**.

3.2. MAKING INSTALLATION USB MEDIA

You can use a USB drive instead of a CD or DVD to create bootable media for installing Red Hat Enterprise Linux on AMD64 and Intel 64 systems. The exact procedure varies depending on whether you

want to perform it on a Linux or Windows system. You can create minimal boot media and full installation media using the same procedure; the only limitation is the capacity of the USB drive - it must have enough space to fit the entire image, which means roughly 350 MB for minimal boot media and 4.5 GB for full installation media.

3.2.1. Making Installation USB Media on Linux

The following procedure assumes you are using a Linux system and that you have downloaded an appropriate ISO image as described in Chapter 2, *Downloading Red Hat Enterprise Linux*. On most Linux distributions, it will work without the need for installing any additional packages.

WARNING

This procedure is destructive. Any data on the USB flash drive will be destroyed with no warning. Make sure that you specify the correct drive, and make sure that this drive does not contain any data you want to preserve.

Many Linux distributions provide their own tools for creating live USB media: liveusb-creator on Fedora, usb-creator on Ubuntu, and others. Describing these tools is beyond the scope of this book; the following procedure will work on most Linux systems.

Procedure 3.1. Making USB Media on Linux

1. Connect a USB flash drive to the system and execute the **dmesg** command. A log detailing all recent events will be displayed. At the bottom of this log, you will see a set of messages caused by the USB flash drive you just connected. It will look like a set of lines similar to the following:

   ```
   [ 170.171135] sd 5:0:0:0: [sdb] Attached SCSI removable disk
   ```

   Note the name of the connected device - in the above example, it is **sdb**.

2. Log in as **root**:

   ```
   $ su -
   ```

   Provide your root password when prompted.

3. Make sure that the device is not mounted. First, use the **findmnt *device*** command and the device name you found in the earlier steps. For example, if the device name is **sdb**, use the following command:

   ```
   # findmnt /dev/sdb
   ```

   If the command displays no output, you can proceed with the next step. However, if the command does provide output, it means that the device was automatically mounted and you must unmount it before proceeding. A sample output will look similar to the following:

```
# findmnt /dev/sdb
TARGET   SOURCE   FSTYPE  OPTIONS
/mnt/iso /dev/sdb iso9660 ro,relatime
```

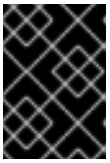
Note the **TARGET** column. Next, use the **umount *target*** command to unmount the device:

```
# umount /mnt/iso
```

4. Use the **dd** command to write the installation ISO image directly to the USB device:

```
# dd if=/image_directory/image.iso of=/dev/device bs=blocksize
```

Replace */image_directory/image.iso* with the full path to the ISO image file you downloaded, *device* with the device name as reported by the **dmesg** command earlier, and *blocksize* with a reasonable block size (for example, **512k**) to speed up the writing process. The **bs** parameter is optional, but it can speed up the process considerably.



IMPORTANT

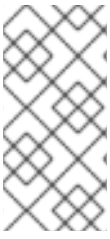
Make sure to specify the output as the device name (for example, **/dev/sda**), not as a name of a *partition* on the device (for example, **/dev/sda1**).

For example, if the ISO image is located in **/home/testuser/Downloads/rhel-server-7.4x86_64-boot.iso** and the detected device name is **sdb**, the command will look like the following:

```
# dd if=/home/testuser/Downloads/rhel-server-7.4x86_64-boot.iso
of=/dev/sdb bs=512k
```

5. Wait for **dd** to finish writing the image to the device. Note that no progress bar is displayed; the data transfer is finished when the # prompt appears again. After the prompt is displayed, log out from the **root** account and unplug the USB drive.

The USB drive is now ready to be used as a boot device. You can continue with Chapter 7, *Booting the Installation on AMD64 and Intel 64 Systems* on AMD64 and Intel 64 systems or Chapter 12, *Booting the Installation on IBM Power Systems* on IBM Power Systems servers.



NOTE

Non-virtualized installations (known as "bare metal" installations) on IBM Power Systems servers require that the **inst.stage2=** boot option is specified. Refer to Section 22.1, “Configuring the Installation System at the Boot Menu” for information about the **inst.stage2=** boot option.

3.2.2. Making Installation USB Media on Windows

The procedure of creating bootable USB media on Windows depends on which tool you use. There are many different utilities which allow you to write an ISO image to a USB drive. Red Hat recommends using the **Fedora Media Writer**, available for download at https://github.com/MartinBriza/MediaWriter/releases.

IMPORTANT

Transferring the ISO image file to the USB drive using Windows Explorer or a similar file manager will not work - you will not be able to boot from the device.

Procedure 3.2. Making USB Media on Windows

1. Download and install **Fedora Media Writer**.
2. Download the Red Hat Enterprise Linux ISO image you want to use to create the media. (See Chapter 2, *Downloading Red Hat Enterprise Linux* for instructions on obtaining ISO images.)
3. Plug in the USB drive you will be using to create bootable media.
4. Open **Fedora Media Writer**.
5. In the main window, click **`Custom Image`** and select the downloaded Red Hat Enterprise Linux ISO image.
6. From the drop-down menu, select the drive you want to use. If the drive does not appear, verify that the USB drive is connected and restart **Fedora Media Writer**.
7. Click **`Write to disk`**. The boot media creation process will begin. Do not unplug the drive until the operation completes. Depending on the size of the ISO image and the write speed of the USB drive, writing the image can take several minutes.

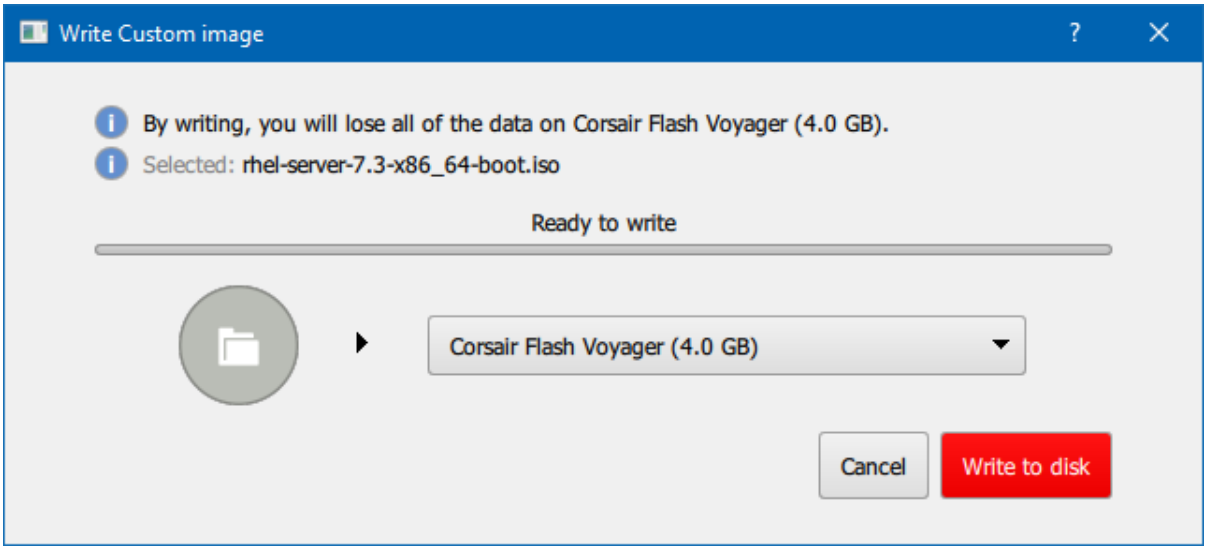


Figure 3.1. Fedora Media Writer

8. When the creation process finishes and the **`Complete!`** message appears, unmount the USB drive using the **`Safely remove hardware`** icon in the system's notification area.

The USB drive is now ready to be used as a boot device. You can continue with Chapter 7, *Booting the Installation on AMD64 and Intel 64 Systems* on AMD64 and Intel 64 systems or Chapter 12, *Booting the Installation on IBM Power Systems* on IBM Power Systems servers.

3.2.3. Making Installation USB Media on Mac OS X

This procedure involves using the **dd** command line tool to write the installation image to a USB flash drive. Note that some steps involve use of the **sudo** command, which is only available when logged in with an administrator account that requires a password.

WARNING

All data on the USB flash drive will be deleted by this procedure.

Procedure 3.3. Making USB Media on Mac OS X

1. Connect a USB flash drive to the system and identify the device path with the **`diskutil list`** command. The device path has the format of **`/dev/disk`*`number`***, where *number* is the number of the disk. The disks are numbered starting at zero (0). Disk 0 is likely to be the OS X recovery disk, and Disk 1 is likely to be your main OS X installation. In the following example, it is **`disk2`**:

```
$ diskutil list
/dev/disk0
#:                       TYPE NAME                    SIZE
IDENTIFIER
0:      GUID_partition_scheme                        *500.3 GB
disk0
1:                        EFI EFI                     209.7 MB
disk0s1
2:          Apple_CoreStorage                        400.0 GB
disk0s2
3:                 Apple_Boot Recovery HD            650.0 MB
disk0s3
4:          Apple_CoreStorage                        98.8 GB
disk0s4
5:                 Apple_Boot Recovery HD            650.0 MB
disk0s5
/dev/disk1
#:                       TYPE NAME                    SIZE
IDENTIFIER
0:                  Apple_HFS YosemiteHD             *399.6 GB
disk1
Logical Volume on disk0s1
8A142795-8036-48DF-9FC5-84506DFBB7B2
Unlocked Encrypted
/dev/disk2
#:                       TYPE NAME                    SIZE
IDENTIFIER
0:     FDisk_partition_scheme                        *8.0 GB
disk2
1:               Windows_NTFS SanDisk USB            8.0 GB
disk2s1
```

To identify your USB flash drive, compare the **`NAME`**, **`TYPE`** and **`SIZE`** columns to what you know about your flash drive. For example, the **`NAME`** should be the same as the title of the flash drive icon in the **Finder**. You can also compare these values to those in the flash drive's information

panel; right-click on the drive icon and select **Get Info**.

2. Use the **diskutil unmountDisk** command to unmount the flash drive's filesystem volumes:

```
$ diskutil unmountDisk /dev/disknumber
     Unmount of all volumes on disknumber was successful
```

When you do this, the icon for the flash drive disappears from your desktop. If it does not, you might have identified the wrong disk. If you attempt to unmount the system disk accidentally, you get a **failed to unmount** error.

3. Use the **dd** command as a parameter of the **sudo** command to write the ISO image to the flash drive:

```
$ sudo dd if=/path/to/image.iso of=/dev/rdisknumber bs=1m>
```

NOTE

Mac OS X provides both a block (**/dev/disk***) and character device (**/dev/rdisk***) file for each storage device. Writing an image to the **/dev/rdisk*number*** character device is faster than to the **/dev/disk*number*** block device.

Example 3.1. Writing an ISO Image to a Disk

To write the **/Users/*user_name*/Downloads/rhel-server-7.4x86_64-boot.iso** file to the **/dev/rdisk2** device:

```
$ sudo dd if=/Users/user_name/Downloads/rhel-server-7.4x86_64-
boot.iso of=/dev/rdisk2
```

4. Wait for the command to finish. Note that no progress bar is displayed; however, to check the status of the operation while it is still running, press **Ctrl**+**t** in the terminal:

```
load: 1.02  cmd: dd 3668 uninterruptible 0.00u 1.91s
112+0 records in
111+0 records out
116391936 bytes transferred in 114.834860 secs (1013559 bytes/sec)
```

5. The speed of the data transfer depends on the speed of your USB ports and the flash drive. After the prompt is displayed again, the data transfer is finished. You can then unplug the flash drive.

The flash drive is now ready to be used as a boot device. You can continue with Chapter 7, *Booting the Installation on AMD64 and Intel 64 Systems* on AMD64 and Intel 64 systems or Chapter 12, *Booting the Installation on IBM Power Systems* on IBM Power Systems servers.

3.3. PREPARING INSTALLATION SOURCES

As explained in Chapter 2, *Downloading Red Hat Enterprise Linux*, two basic types of media are available for Red Hat Enterprise Linux: a minimal boot image and a full installation image (also known as

a binary DVD). If you downloaded the binary DVD and created a boot DVD-ROM or USB drive from it, you can proceed with the installation immediately, as this image contains everything you need to install the system.

However, if you use the minimal boot image, you must also configure an additional source of the installation. This is because the minimal boot image only contains the installation program itself and tools needed to boot your system and start the installation; it does not include the software packages to be installed on your system.

The full installation DVD ISO image can be used as the source for the installation. If your system will require additional software not provided by Red Hat, you should configure additional repositories and install these packages *after* the installation is finished. For information about configuring additional **Yum** repositories on an installed system, see the Red Hat Enterprise Linux 7 System Administrator's Guide.

The installation source can be any of the following:

- **`DVD`**: You can burn the binary DVD ISO image onto a DVD and configure the installation program to install packages from this disk.
- **`Hard drive`**: You can place the binary DVD ISO image on a hard drive and install packages from it.
- **`Network location`**: You can copy the binary DVD ISO image or the *installation tree* (extracted contents of the binary DVD ISO image) to a network location accessible from the installation system and perform the installation over the network using the following protocols:
  - **`NFS`**: The binary DVD ISO image is placed into a *Network File System* (NFS) share.
  - **`HTTPS`**, **`HTTP`** or **`FTP`**: The installation tree is placed on a network location accessible over **`HTTP`**, **`HTTPS`**, or **`FTP`**.

When booting the installation from minimal boot media, you must always configure an additional installation source. When booting the installation from the full binary DVD, it is also possible to configure another installation source, but it is not necessary - the binary DVD ISO image itself contains all packages you need to install the system, and the installation program will automatically configure the binary DVD as the source.

You can specify an installation source in any of the following ways:

- In the installation program's graphical interface: After the graphical installation begins and you select your preferred language, the **`Installation Summary`** screen will appear. Navigate to the **`Installation Source`** screen and select the source you want to configure. For details, see:
  - Section 8.11, “Installation Source” for AMD64 and Intel 64 systems
  - Section 13.12, “Installation Source” for IBM Power Systems servers
  - Section 17.12, “Installation Source” for IBM System z
- Using a boot option: You can specify custom boot options to configure the installation program before it starts. One of these options allows you to specify the installation source to be used. See the **`inst.repo=`** option in Section 22.1, “Configuring the Installation System at the Boot Menu” for details.
- Using a Kickstart file: You can use the **`install`** command in a Kickstart file and specify an installation source. See Section 26.3.1, “Kickstart Commands and Options” for details on the

`install` Kickstart command, and Chapter 26, *Kickstart Installations* for information about Kickstart installations in general.

3.3.1. Installation Source on a DVD

You can burn the binary DVD ISO image onto a DVD and configure the installation program to install packages from this disk while booting the installation from another drive (for example, a minimal boot ISO on a USB flash drive). This procedure is the same as creating bootable optical media - see Section 3.1, “Making an Installation CD or DVD” for more information.

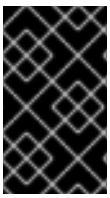
When using a DVD as an installation source, make sure the DVD is in the drive when the installation begins. The **Anaconda** installation program is not able to detect media inserted after the installation begins.

3.3.2. Installation Source on a Hard Drive

Hard drive installations use an ISO image of the binary installation DVD. To use a hard drive as the installation source, transfer the binary DVD ISO image to the drive and connect it to the installation system. Then, boot the **Anaconda** installation program.

You can use any type of hard drive accessible to the installation program, including USB flash drives. The binary ISO image can be in any directory of the hard drive, and it can have any name; however, if the ISO image is not in the top-level directory of the drive, or if there is more than one image in the top-level directory of the drive, you will be required to specify the image to be used. This can be done using a boot option, an entry in a Kickstart file, or manually in the **`Installation Source`** screen during a graphical installation.

A limitation of using a hard drive as the installation source is that the binary DVD ISO image on the hard drive must be on a partition with a file system which **Anaconda** can mount. These file systems are **`xfs`**, **`ext2`**, **`ext3`**, **`ext4`**, and **`vfat`** (**`FAT32`**). Note that on Microsoft Windows systems, the default file system used when formatting hard drives is **`NTFS`**, and the **`exFAT`** file system is also available; however, neither of these file systems can be mounted during the installation. If you are creating a hard drive or a USB drive to be used as an installation source on Microsoft Windows, make sure to format the drive as **`FAT32`**.



IMPORTANT

The **`FAT32`** file system does not support files larger than 4 GiB. Some Red Hat Enterprise Linux 7 installation media can be larger than that, which means you cannot copy them to a drive with this file system.

When using a hard drive or a USB flash drive as an installation source, make sure it is connected to the system when the installation begins. The installation program is not able to detect media inserted after the installation begins.

3.3.3. Installation Source on a Network

Placing the installation source on a network has the advantage of allowing you to install multiple systems from a single source, without having to connect and disconnect any physical media. Network-based installations can be especially useful when used together with a TFTP server, which allows you to boot the installation program from the network as well. This approach completely eliminates the need for creating physical media, allowing easy deployment of Red Hat Enterprise Linux on multiple systems at the same time. For further information about setting up a TFTP server, see Chapter 23, *Preparing for a Network Installation*.

3.3.3.1. Installation Source on an NFS Server

The **NFS** installation method uses an ISO image of the Red Hat Enterprise Linux binary DVD placed in a **Network File System** server's *exported directory*, which the installation system must be able to read. To perform an NFS-based installation, you will need another running system which will act as the NFS host.

For more information about NFS servers, see the Red Hat Enterprise Linux 7 Storage Administration Guide.

The following procedure is only meant as a basic outline of the process. The precise steps you must take to set up an NFS server will vary based on the system's architecture, operating system, package manager, service manager, and other factors. On Red Hat Enterprise Linux 7 systems, the procedure can be followed exactly as documented. For procedures describing the installation source creation process on earlier releases of Red Hat Enterprise Linux, see the appropriate *Installation Guide* for that release.

Procedure 3.4. Preparing for Installation Using NFS

1. Install the nfs-utils package by running the following command as **root**:

   ```
   # yum install nfs-utils
   ```

2. Copy the full Red Hat Enterprise Linux 7 binary DVD ISO image to a suitable directory on the NFS server. For example, you can create directory **/rhel7-install/** for this purpose and save the ISO image here.

3. Open the **/etc/exports** file using a text editor and add a line with the following syntax:

   ```
   /exported_directory/ clients
   ```

   Replace */exported_directory/* with the full path to the directory holding the ISO image. Instead of *clients*, use the host name or IP address of the computer which is to be installed from this NFS server, the subnetwork from which all computers are to have access the ISO image, or the asterisk sign (*****) if you want to allow any computer with network access to the NFS server to use the ISO image. See the **exports(5)** man page for detailed information about the format of this field.

   The following is a basic configuration which makes the **/rhel7-install/** directory available as read-only to all clients:

   ```
   /rhel7-install *
   ```

4. Save the **/etc/exports** file after finishing the configuration and exit the text editor.

5. Start the **nfs** service:

   ```
   # systemctl start nfs.service
   ```

   If the service was already running before you changed the **/etc/exports** file, enter the following command instead, in order for the running NFS server to reload its configuration:

   ```
   # systemctl reload nfs.service
   ```

After completing the procedure above, the ISO image is accessible over **NFS** and ready to be used as an installation source.

When configuring the installation source before or during the installation, use **nfs:** as the protocol, the server's host name or IP address, the colon sign (**:**), and the directory holding the ISO image. For example, if the server's host name is **myserver.example.com** and you have saved the ISO image in **/rhel7-install/**, specify **nfs:myserver.example.com:/rhel7-install/** as the installation source.

3.3.3.2. Installation Source on an HTTP, HTTPS or FTP Server

This installation method allows for a network-based installation using an installation tree, which is a directory containing extracted contents of the binary DVD ISO image and a valid **.treeinfo** file. The installation source is accessed over **HTTP**, **HTTPS**, or **FTP**.

For more information about HTTP and FTP servers, see the Red Hat Enterprise Linux 7 System Administrator's Guide.

The following procedure is only meant as a basic outline of the process. The precise steps you must take to set up an FTP server will vary based on the system's architecture, operating system, package manager, service manager, and other factors. On Red Hat Enterprise Linux 7 systems, the procedure can be followed exactly as documented. For procedures describing the installation source creation process on earlier releases of Red Hat Enterprise Linux, see the appropriate *Installation Guide* for that release.

Procedure 3.5. Preparing Installation Using HTTP or HTTPS

1. Install the httpd package by running the following command as **root**:

```
# yum install httpd
```

An **HTTPS** server needs additional configuration. For detailed information, see section Setting Up an SSL Server in the Red Hat Enterprise Linux 7 System Administrator's Guide. However, **HTTPS** is not necessary in most cases, because no sensitive data is sent between the installation source and the installer, and **HTTP** is sufficient.

WARNING

If your **Apache** web server configuration enables SSL security, make sure to only enable the **TLSv1** protocol, and disable **SSLv2** and **SSLv3**. This is due to the POODLE SSL vulnerability (CVE-2014-3566). See https://access.redhat.com/solutions/1232413 for details.

IMPORTANT

If you decide to use **HTTPS** and the server is using a self-signed certificate, you must boot the installer with the **noverifyssl** option.

2. Copy the full Red Hat Enterprise Linux 7 binary DVD ISO image to the HTTP(S) server.

3. Mount the binary DVD ISO image, using the **mount** command, to a suitable directory:

```
# mount -o loop,ro -t iso9660 /image_directory/image.iso
/mount_point/
```

   Replace */image_directory/image.iso* with the path to the binary DVD ISO image, and */mount_point/* with the path to the directory in which you want the content of the ISO image to appear. For example, you can create directory **/mnt/rhel7-install/** for this purpose and use that as the parameter of the **mount** command.

4. Copy the files from the mounted image to the HTTP server root.

```
# cp -r /mnt/rhel7-install/ /var/www/html/
```

   This command creates the **/var/www/html/rhel7-install/** directory with the content of the image.

5. Start the **httpd** service:

```
# systemctl start httpd.service
```

After completing the procedure above, the installation tree is accessible and ready to be used as the installation source.

When configuring the installation source before or during the installation, use **http://** or **https://** as the protocol, the server's host name or IP address, and the directory in which you have stored the files from the ISO image, relative to the HTTP server root. For example, if you are using **HTTP**, the server's host name is **myserver.example.com**, and you have copied the files from the image to **/var/www/html/rhel7-install/**, specify **http://myserver.example.com/rhel7-install/** as the installation source.

Procedure 3.6. Preparing for Installation Using FTP

1. Install the vsftpd package by running the following command as **root**:

```
# yum install vsftpd
```

2. Optionally, open the **/etc/vsftpd/vsftpd.conf** configuration file in a text editor, and edit any options you want to change. For available options, see the **vsftpd.conf(5)** man page. The rest of this procedure assumes that default options are used; notably, to follow the rest of the procedure, anonymous users of the FTP server must be permitted to download files.

WARNING

If you configured SSL/TLS security in your **vsftpd.conf** file, make sure to only enable the **TLSv1** protocol, and disable **SSLv2** and **SSLv3**. This is due to the POODLE SSL vulnerability (CVE-2014-3566). See https://access.redhat.com/solutions/1234773 for details.

3. Copy the full Red Hat Enterprise Linux 7 binary DVD ISO image to the FTP server.
4. Mount the binary DVD ISO image, using the **mount** command, to a suitable directory:

```
# mount -o loop,ro -t iso9660 /image_directory/image.iso
/mount_point
```

Replace */image_directory/image.iso* with the path to the binary DVD ISO image, and */mount_point* with the path to the directory in which you want the content of the ISO image to appear. For example, you can create directory **/mnt/rhel7-install/** for this purpose and use that as the parameter of the **mount** command.

5. Copy the files from the mounted image to the FTP server root:

```
# cp -r /mnt/rhel7-install/ /var/ftp/
```

This command creates the **/var/ftp/rhel7-install/** directory with the content of the image.

6. Start the **vsftpd** service:

```
# systemctl start vsftpd.service
```

If the service was already running before you changed the **/etc/vsftpd/vsftpd.conf** file, restart it to ensure the edited file is loaded. To restart, execute the following command:

```
# systemctl restart vsftpd.service
```

After completing the procedure above, the installation tree is accessible and ready to be used as the installation source.

When configuring the installation source before or during the installation, use **ftp://** as the protocol, the server's host name or IP address, and the directory in which you have stored the files from the ISO image, relative to the FTP server root. For example, if the server's host name is **myserver.example.com** and you have copied the files from the image to **/var/ftp/rhel7-install/**, specify **ftp://myserver.example.com/rhel7-install/** as the installation source.

3.3.3.3. Firewall Considerations for Network-based Installations

When using a network-based installation source, make sure that your firewall allows the server you are installing to access the remote installation source. The following table shows which ports must be open for each type of network-based installation

Table 3.1. Ports Used by Network Protocols

Protocol used	Ports to open
FTP	**21**
HTTP	**80**
HTTPS	**443**
NFS	**2049**, **111**, **20048**
TFTP	**69**

For information about opening specific firewall ports, see the Red Hat Enterprise Linux 7 Security Guide.

PART I. AMD64 AND INTEL 64 - INSTALLATION AND BOOTING

This part of the *Red Hat Enterprise Linux Installation Guide* discusses the installation of Red Hat Enterprise Linux 7 on 64-bit AMD and Intel systems as well as some basic troubleshooting. For advanced installation options, see Part IV, “Advanced Installation Options”.

CHAPTER 4. QUICK INSTALLATION GUIDE

4.1. INTERACTIVE INSTALLATION

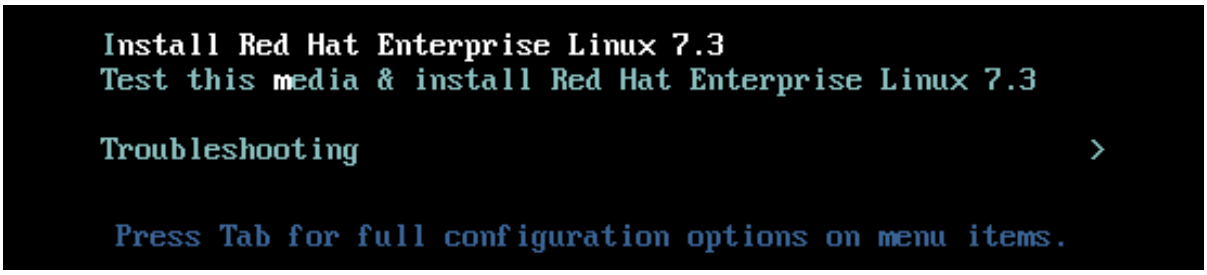
This section describes the simple procedure to install and register Red Hat Enterprise Linux after you have created and booted from an installation USB drive.

Prerequisites: Create an installation USB drive and boot it. For details, see:

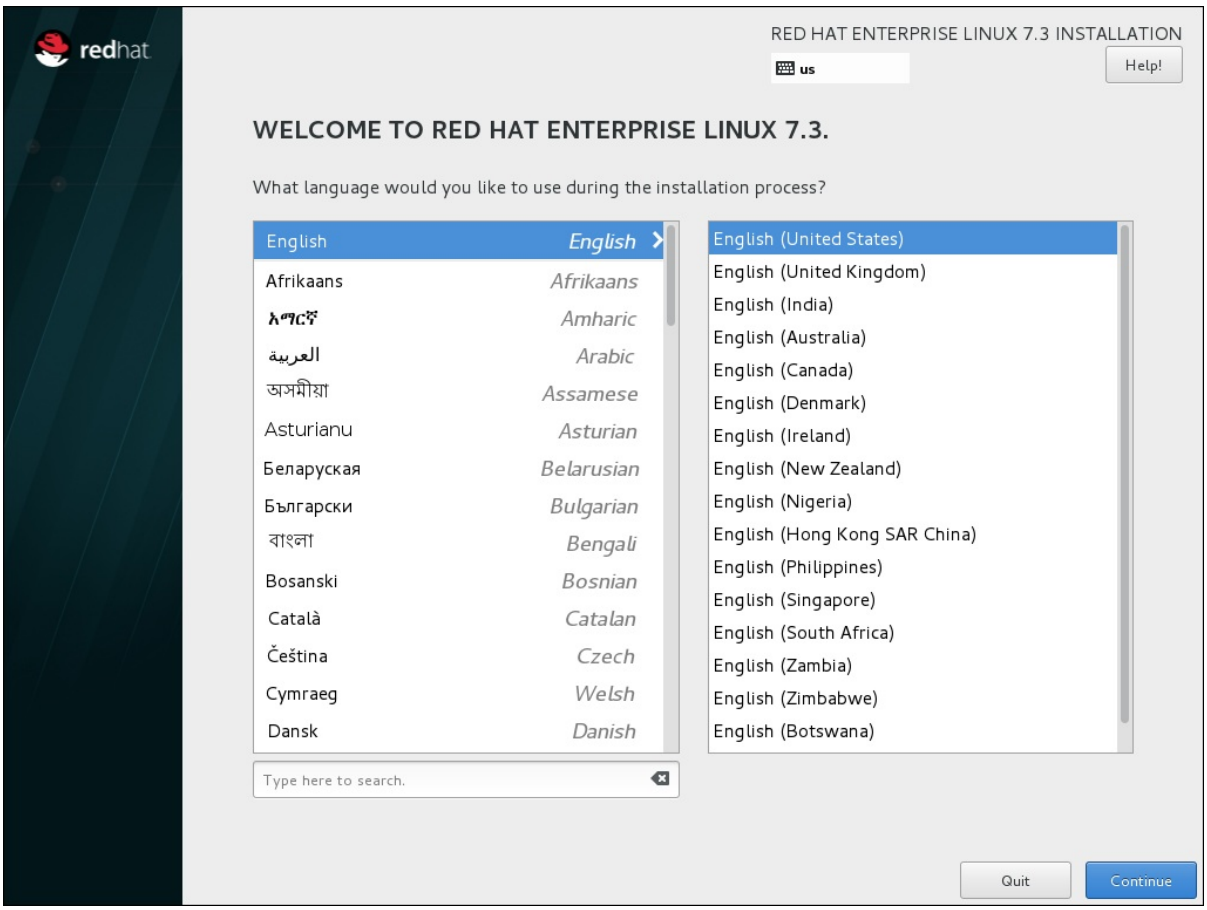
- Chapter 3, *Making Media*.
- Chapter 7, *Booting the Installation on AMD64 and Intel 64 Systems*.

After booting the installation USB drive:

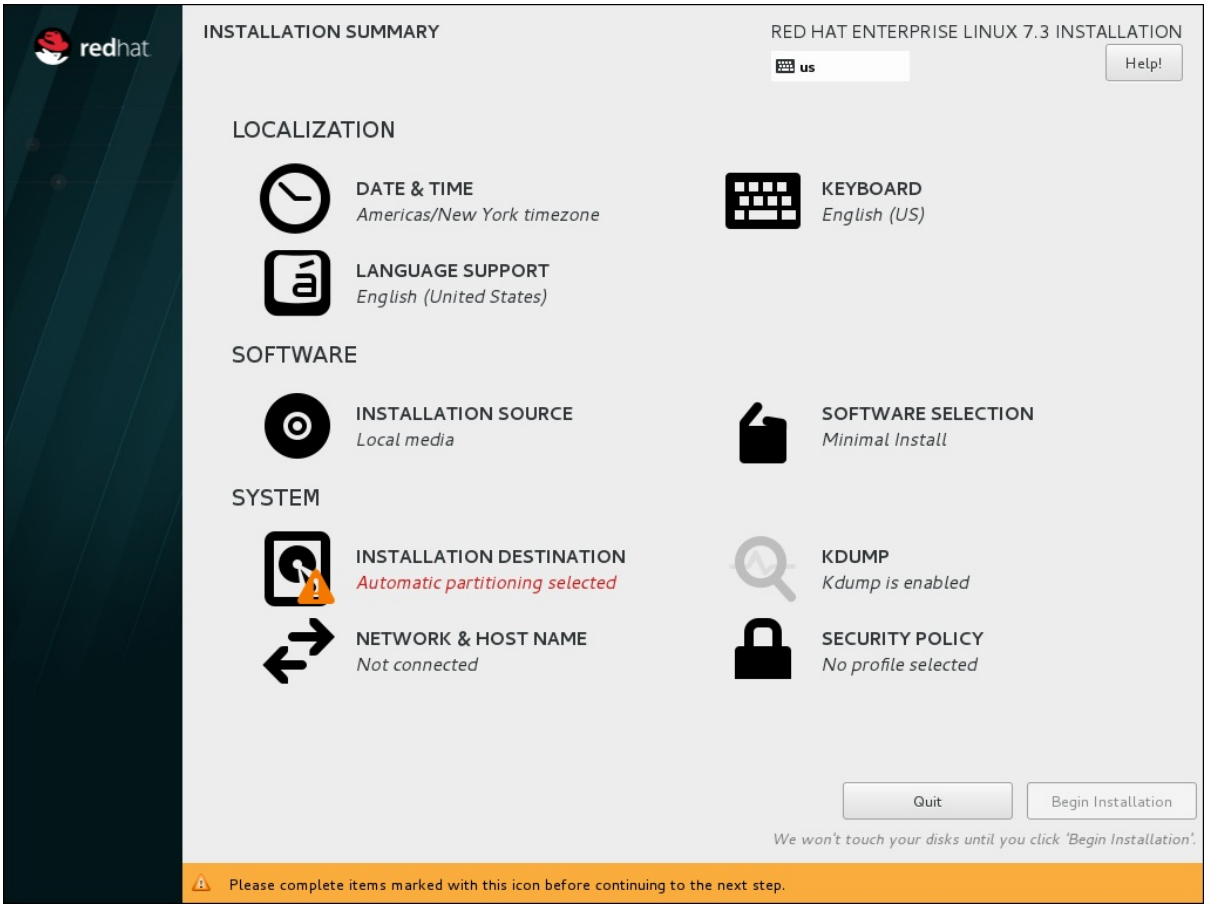
1. Select **`Install Red Hat Enterprise Linux`** in the boot menu and press **`Enter`**.



2. After **Anaconda**, the Red Hat Enterprise Linux installer, started, select your language and region, and click **`Continue`**.



3. The **`Installation Summary`** is the central screen to set configuration options:



You can display and modify the individual options in any order. If a configuration option was automatically configured correctly, no further action is required. However, if items are marked with an exclamation point icon, you must complete the configuration for these items before you can begin the installation.

NOTE

Nothing will be written to the disk until you click the **Begin Installation** button.

4. Select **Date & Time**:

   a. Set your region and the nearest city in your time zone.

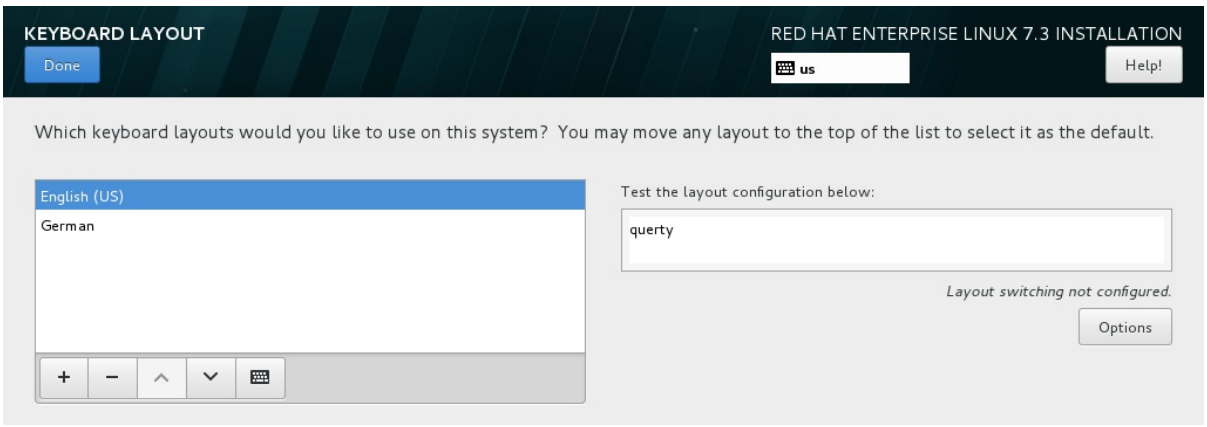
   b. Click **Done** to return to the **Installation Summary**.

5. Select **`Keyboard Layout`**:

   a. Use the **+** and **-** buttons to add and remove keyboard layouts.

   b. If you enable multiple keyboard layouts, move your preferred layout to the top of the list using the ↑ button to set it as default.

   c. Click **`Done`** to return to the **`Installation Summary`**.

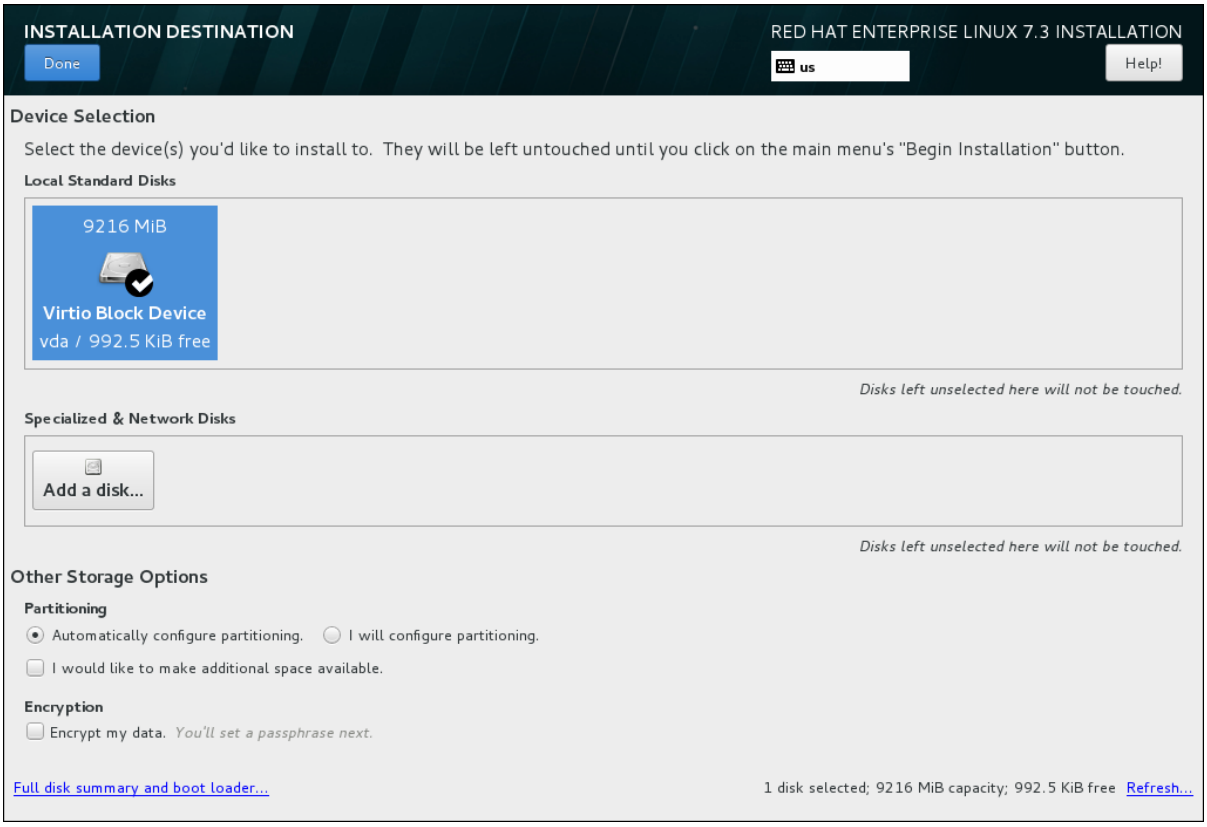


6. Select **`Installation Destination`**:

   a. Select the target disk. A check mark is displayed next to the selected target.

      The selected disk is partitioned automatically.

   b. Click **`Done`** to return to the **`Installation Summary`**.

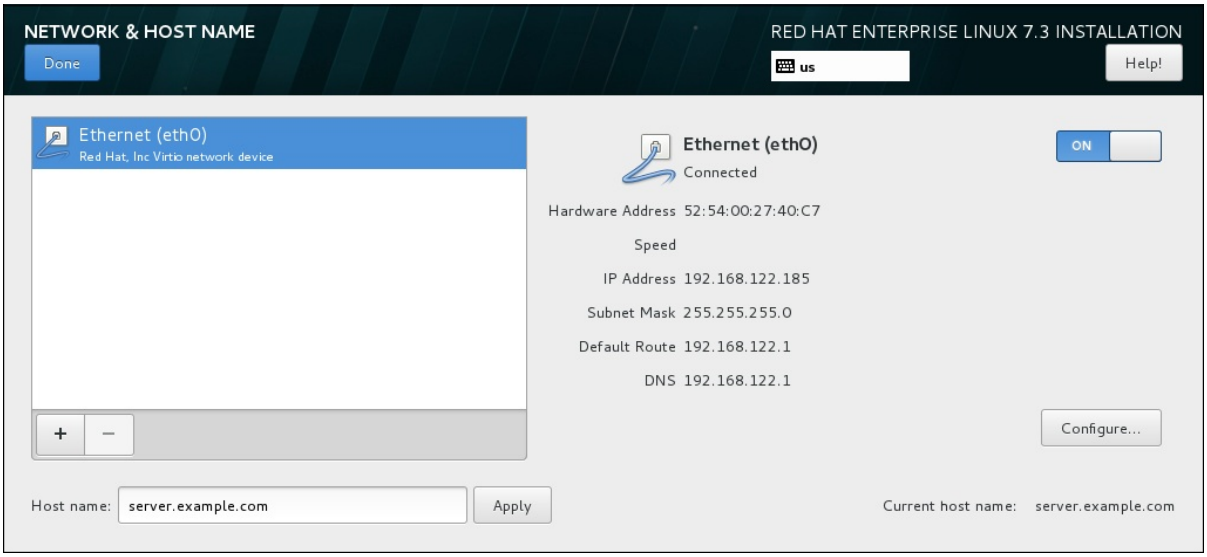


7. Select **`Network and Hostname`**:

   a. Click the **`Ethernet`** sliding switch in the top right corner to enable the network configuration.

   b. Optional, select the device and click **`Configure`** to update the network interface configuration.

   c. Click **`Done`** to return to the **`Installation Summary`**.

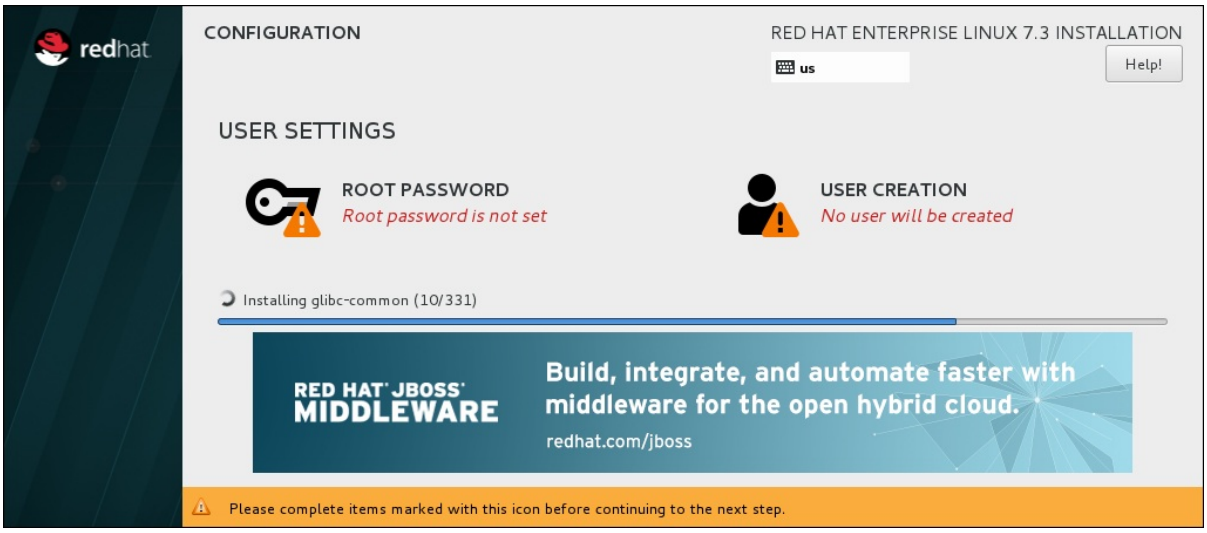


NOTE

Anaconda applies the network settings immediately. They are used during the setup and after the installation.

8. On the **`Installation Summary`** screen, click **`Begin Installation`**.

9. The installation starts and the **`Configuration`** screen is displayed:

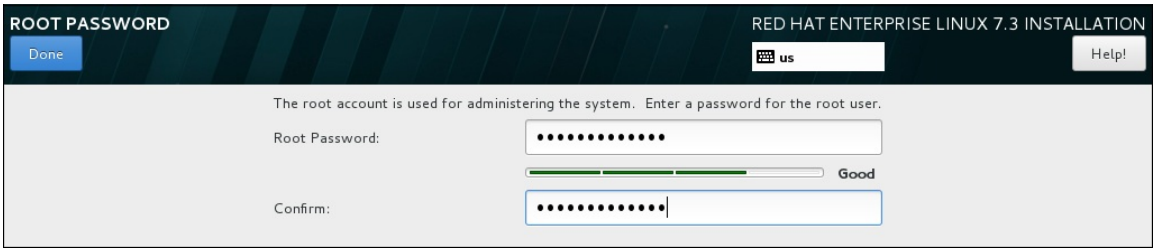


During the installation:

a. Select **`Root Password`**:

   i. Enter the password for the **`root`** user and confirm it.

   ii. Click **`Done`** to return to the **`Configuration`** screen.



b. Select **User Creation**:

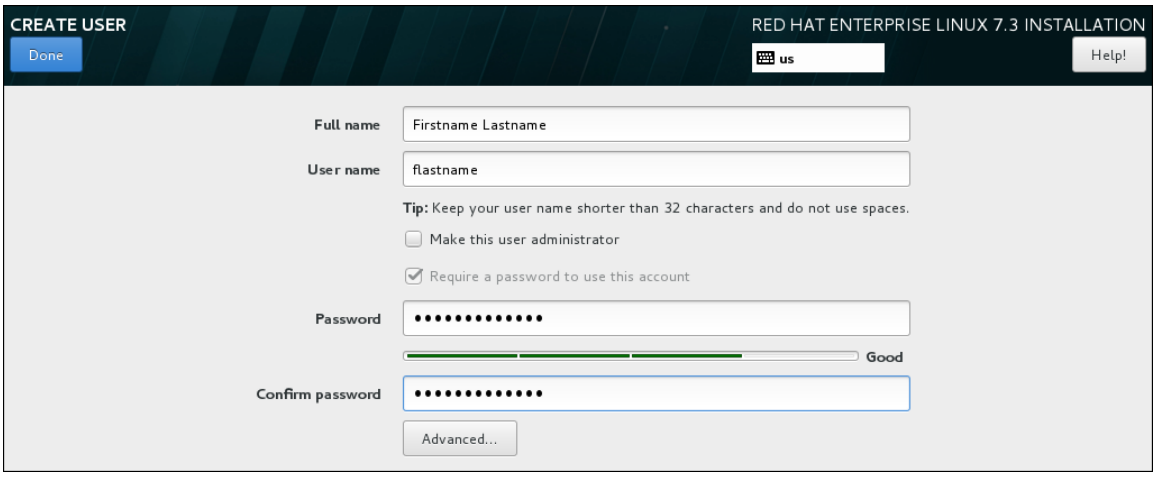
i. Enter the user's full name.

ii. Optionally, update the automatically generated user name.

iii. Set the password and confirm it.

iv. Optionally, check the **Make this user administrator** check box. This will add the user to the **wheel** group and allow this account to use **sudo** without any further configuration.

v. Click **Done** to return to the **Configuration** screen.



c. Wait until the installation completes and click **Reboot**.

10. After the installed system has been started:

- If you installed the server using the **Server with GUI** base environment, the **Initial Setup** application is started automatically:

  1. Accept the license agreement.
  2. Register the system.

  For details, see Chapter 29, *Initial Setup*.

- If you selected any other base environment during the installation:

  1. Log into the system as the **root** user.
  2. Register the system and automatically attach a subscription:

  ```
  # subscription-manager register --auto-attach \
  --username=user_name --password=password
  ```

4.2. AUTOMATIC INSTALLATION

This section describes a simple procedure on how to add a Kickstart file to the installation USB drive, which automatically installs and registers Red Hat Enterprise Linux. You can use this procedure to deploy Red Hat Enterprise Linux on multiple machines.

Generating the USB Boot Media

1. Record an installation in a Kickstart file:

   a. Manually install Red Hat Enterprise Linux once. For details see Section 4.1, “Interactive Installation”.

   b. Boot the installed system. During the installation, **Anaconda** created a Kickstart file with the settings in the **/root/anaconda-ks.cfg** file.

2. Download the Red Hat Enterprise Linux installation DVD ISO file to the **/tmp/** directory.

3. Mount the installation ISO file to the **/mnt/** directory. For example:

```
# mount -o loop /tmp/rhel-server-7.3-x86_64-dvd.iso /mnt/
```

4. Create a working directory and copy the DVD content to it. For example:

```
# mkdir /root/rhel-install/
# shopt -s dotglob
# cp -avRf /mnt/* /root/rhel-install/
```

5. Unmount the ISO file:

```
# umount /mnt/
```

6. Copy the Kickstart file generated during the installation to the working directory:

```
# cp /root/anaconda-ks.cfg /root/rhel-install/
```

7. To register Red Hat Enterprise Linux after the installation automatically and attach a subscription, append the following to the **/root/rhel-install/anaconda-ks.cfg** file:

```
%post
subscription-manager register --auto-attach --username=user_name --
password=password
%end
```

8. Display the installation DVD volume name:

```
# isoinfo -d -i rhel-server-7.3-x86_64-dvd.iso | grep "Volume id" |
\
sed -e 's/Volume id: //' -e 's/ /\\x20/g'
RHEL-7.3\x20Server.x86_64
```

9. Add a new menu entry to the boot **/root/rhel-install/isolinux/isolinux.cfg** file that uses the Kickstart file. For example:

```
#########################################
label kickstart
menu label ^Kickstart Installation of RHEL7.3
kernel vmlinuz
```

```
append initrd=initrd.img inst.stage2=hd:LABEL=RHEL-
7.3\x20Server.x86_64 inst.ks=cdrom:/anaconda-ks.cfg
########################################
```

NOTE

Set the **inst.stage2=hd:LABEL=** option to the DVD volume name retrieved in the previous step.

10. Create the **/root/rhel-ks.iso** file from the working directory:

```
# mkisofs -J -T -o /root/rhel-ks.iso -b isolinux/isolinux.bin \
-c isolinux/boot.cat -no-emul-boot -boot-load-size 4 -boot-info-
table \
-R -m TRANS.TBL -graft-points -V "RHEL-7.3 Server.x86_64" \
/root/rhel-install/
```

NOTE

Set the **-V** option to the DVD volume name retrieved in an earlier step and replace **\x20** in the string with a space.

11. Create an installation USB drive. For details, see Section 3.2.1, “Making Installation USB Media on Linux”.

Install Red Hat Enterprise Linux Using the Kickstart File

1. Boot the installation USB drive. See Chapter 7, *Booting the Installation on AMD64 and Intel 64 Systems*.

2. Select the entry, that contains the Kickstart configuration, you created in the section called “Generating the USB Boot Media”.

CHAPTER 5. PLANNING FOR INSTALLATION ON AMD64 AND INTEL 64 SYSTEMS

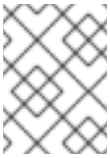
This chapter outlines the decisions and preparations you will need to make when deciding how to proceed with the installation.

5.1. UPGRADE OR INSTALL?

There are two procedures available for upgrading your current system to the next major version of Red Hat Enterprise Linux. To decide which procedure is the right one for your system, read the following descriptions:

Clean Install

A clean install is performed by backing up all data from the system, formatting disk partitions, performing an installation of Red Hat Enterprise Linux from installation media, and then restoring any user data.



NOTE

This is the recommended method for upgrading between major versions of Red Hat Enterprise Linux.

In-Place Upgrade

An in-place upgrade is a way of upgrading your system without removing the older version first. The procedure requires installing the migration utilities available for your system and running them as any other software. In Red Hat Enterprise Linux, the **Preupgrade Assistant** assesses your current system and identifies potential problems you might encounter during or after the upgrade. It also performs minor fixes and modifications to the system. The **Red Hat Upgrade Tool** utility downloads the packages and performs the actual upgrade. An in-place upgrade requires a lot of troubleshooting and planning and should only be done if there is no other choice. For more information on the **Preupgrade Assistant**, see Chapter 28, *Upgrading Your Current System*.

WARNING

Never perform an in-place upgrade on a production system without first testing it on a cloned backup copy of the system.

5.2. IS YOUR HARDWARE COMPATIBLE?

Red Hat Enterprise Linux 7 should be compatible with most hardware in systems that were factory built within the last two years. Hardware compatibility is a particularly important concern if you have an older or custom-built system. Because hardware specifications change almost daily, it is recommended that all systems be checked for compatibility.

The most recent list of supported hardware can be found in the *Red Hat Hardware Compatibility List*, available online at https://access.redhat.com/ecosystem/search/#/category/Server. Also see Red Hat Enterprise Linux technology capabilities and limits for general information about system requirements.

5.3. SUPPORTED INSTALLATION TARGETS

An installation target is a storage device that will store Red Hat Enterprise Linux and boot the system. Red Hat Enterprise Linux supports the following installation targets for AMD64 and Intel 64 systems:

- Storage connected by a standard internal interface, such as SCSI, SATA, or SAS
- BIOS/firmware RAID devices
- Fibre Channel Host Bus Adapters and multipath devices. Some can require vendor-provided drivers.
- Xen block devices on Intel processors in Xen virtual machines.
- VirtIO block devices on Intel processors in KVM virtual machines.

Red Hat does not support installation to USB drives or SD memory cards. For information about the support for third-party virtualization technologies, see the *Red Hat Hardware Compatibility List*, available online at https://hardware.redhat.com.

5.4. SYSTEM SPECIFICATIONS LIST

The installation program automatically detects and installs your computer's hardware and you do not usually need to supply the installation program with any specific details about your system. However, when performing certain types of installation, it is important to know specific details about your hardware. For this reason, it is recommended that you record the following system specifications for reference during the installation, depending on your installation type.

- If you plan to use a customized partition layout, record:
  - The model numbers, sizes, types, and interfaces of the hard drives attached to the system. For example, Seagate ST3320613AS 320 GB on SATA0, Western Digital WD7500AAKS 750 GB on SATA1. This will allow you to identify specific hard drives during the partitioning process.
- If you are installing Red Hat Enterprise Linux as an additional operating system on an existing system, record:
  - Information about the partitions used on the system. This information can include file system types, device node names, file system labels, and sizes. This will allow you to identify specific partitions during the partitioning process. Remember that different operating systems identify partitions and drives differently, therefore even if the other operating system is a Unix operating system, the device names can be reported by Red Hat Enterprise Linux differently. This information can usually be found by executing the equivalent of the **`mount`** command and **`blkid`** command and in the **`/etc/fstab`** file.

    If you have other operating systems already installed, the Red Hat Enterprise Linux 7 installation program attempts to automatically detect and configure to boot them. You can manually configure any additional operating systems if they are not detected properly. For more information, see Section 8.14.1, “Boot Loader Installation”.
- If you plan to install from an image on a local hard drive:

- The hard drive and directory that holds the image.

- If you plan to install from a network location:
  - The make and model numbers of the network adapters on your system. For example, Netgear GA311. This will allow you to identify adapters when manually configuring the network.
  - IP, DHCP, and BOOTP addresses
  - Netmask
  - Gateway IP address
  - One or more name server IP addresses (DNS)
  - The location of the installation source on an FTP server, HTTP (web) server, HTTPS (web) server, or NFS server.

  If any of these networking requirements or terms are unfamiliar to you, contact your network administrator for assistance.

- If you plan to install on an iSCSI target:
  - The location of the iSCSI target. Depending on your network, you might also need a CHAP user name and password, and perhaps a reverse CHAP user name and password.

- If your computer is part of a domain:
  - You should verify that the domain name will be supplied by the DHCP server. If not, you will need to input the domain name manually during installation.

5.5. DISK SPACE AND MEMORY REQUIREMENTS

Red Hat Enterprise Linux, like most modern operating systems, uses *disk partitions*. When you install Red Hat Enterprise Linux, you might have to work with disk partitions. For more information, see Appendix A, *An Introduction to Disk Partitions*.

If you have other operating systems installed on your system, the disk space they use must be separate from the disk space used by Red Hat Enterprise Linux.

NOTE

For AMD64 and Intel 64 systems, at least two partitions (`/` and **swap**) must be dedicated to Red Hat Enterprise Linux.

To install Red Hat Enterprise Linux, you must have a minimum of 10 GiB of space in either unpartitioned disk space or in partitions which can be deleted. For more information on partition and disk space recommendations, see the recommended partitioning sizes discussed in Section 8.14.4.4, “Recommended Partitioning Scheme”.

Red Hat Enterprise Linux requires minimum the following amount of RAM:

Installation type	Minimum required RAM
Local media installation (USB, DVD)	512 MiB
NFS network installation	512 MiB
HTTP, HTTPS, or FTP network installation	1 GiB

Installing Red Hat Enterprise Linux using a Kickstart file has the same minimum RAM requirements as a manual installation. However, if you use a Kickstart file that runs commands which require additional memory or write data to the RAM disk, additional RAM might be necessary.

For more information about the minimum requirements and technology limits of Red Hat Enterprise Linux 7, see the *Red Hat Enterprise Linux technology capabilities and limits* article on the Red Hat Customer Portal.

5.6. RAID AND OTHER DISK DEVICES

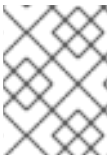
Some storage technology requires special consideration when using Red Hat Enterprise Linux. Generally, it is important to understand how these technologies are configured, visible to Red Hat Enterprise Linux, and how support for them might have changed between major versions.

5.6.1. Hardware RAID

RAID (Redundant Array of Independent Disks) allows a group, or array, of drives to act as a single device. Configure any RAID functions provided by the mainboard of your computer, or attached controller cards, before you begin the installation process. Each active RAID array appears as one drive within Red Hat Enterprise Linux.

5.6.2. Software RAID

On systems with more than one hard drive, you can use the Red Hat Enterprise Linux installation program to operate several of the drives as a Linux software RAID array. With a software RAID array, RAID functions are controlled by the operating system rather than dedicated hardware. These functions are explained in detail in Section 8.14.4, “Manual Partitioning”.



NOTE

When a pre-existing RAID array's member devices are all unpartitioned disks/drives, the installer will treat the array itself as a disk and will not provide a way to remove the array.

5.6.3. USB Disks

You can connect and configure external USB storage after installation. Most such devices are recognized by the kernel and available for use at that time.

Some USB drives might not be recognized by the installation program. If configuration of these disks at installation time is not vital, disconnect them to avoid potential problems.

5.6.4. Considerations for Intel BIOS RAID Sets

Red Hat Enterprise Linux 7 uses **mdraid** for installation onto Intel BIOS RAID sets. These sets are detected automatically during the boot process and their device node paths can change from boot to boot. For this reason, local modifications to `/etc/fstab`, `/etc/crypttab` or other configuration files which refer to devices by their device node paths might not work in Red Hat Enterprise Linux 7. Therefore, you should replace device node paths (such as `/dev/sda`) with file system labels or device UUIDs instead. You can find the file system labels and device UUIDs using the `blkid` command.

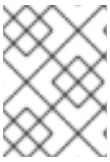
5.6.5. Considerations for Intel BIOS iSCSI Remote Boot

If you are installing using Intel iSCSI Remote Boot, all attached iSCSI storage devices must be disabled, otherwise the installation will succeed but the installed system will not boot.

5.7. CHOOSE AN INSTALLATION BOOT METHOD

You can use several methods to boot the Red Hat Enterprise Linux 7 installation program. The method you choose depends upon your installation media.

Your system's firmware (BIOS of UEFI) settings might need to be changed to allow booting from removable media such as a DVD or a USB flash drive. See Section 7.1.1, “Booting the Installation on AMD64 and Intel 64 Systems from Physical Media” for information.



NOTE

Installation media must remain mounted throughout installation, including during execution of the `%post` section of a kickstart file.

Full installation DVD or USB drive

You can create bootable media from the full installation DVD ISO image. In this case, a single DVD or USB drive can be used to complete the entire installation - it will serve both as a boot device and as an installation source for installing software packages. See Chapter 3, *Making Media* for instructions on how to make a full installation DVD or USB drive.

Minimal boot CD, DVD or USB Flash Drive

A minimal boot CD, DVD or USB flash drive is created using a small ISO image, which only contains data necessary to boot the system and start the installation. If you use this boot media, you will need an additional installation source from which packages will be installed. See Section 3.2, “Making Installation USB Media” for instructions on making boot CDs, DVDs and USB flash drives.

PXE Server

A *preboot execution environment* (PXE) server allows the installation program to boot over the network. After you boot the system, you complete the installation from a different installation source, such as a local hard drive or a location on a network. For more information on PXE servers, see Chapter 23, *Preparing for a Network Installation*.

5.8. AUTOMATING THE INSTALLATION WITH KICKSTART

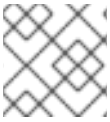
Red Hat Enterprise Linux 7 offers a way to partially or fully automate the installation process using a *Kickstart file*. Kickstart files contain answers to all questions normally asked by the installation program, such as what time zone do you want the system to use, how should the drives be partitioned or which packages should be installed. Providing a prepared Kickstart file at the beginning of the installation

therefore allows you to perform the entire installation (or parts of it) automatically, without need for any intervention from the user. This is especially useful when deploying Red Hat Enterprise Linux on a large number of systems at once.

In addition to allowing you to automate the installation, Kickstart files also provide more options regarding software selection. When installing Red Hat Enterprise Linux manually using the graphical installation interface, your software selection is limited to pre-defined environments and add-ons. A Kickstart file allows you to install or remove individual packages as well.

For instructions about creating a Kickstart file and using it to automate the installation, see Chapter 26, *Kickstart Installations*.

5.9. USING A BETA RELEASE WITH UEFI SECURE BOOT



NOTE

This section *only* concerns Beta releases of Red Hat Enterprise Linux 7.

The UEFI Secure Boot technology requires that the operating system kernel must be signed with a recognized private key in order to be able to boot. In every beta release of Red Hat Enterprise Linux 7, the kernel is signed with a Red Hat Beta-specific private key, which is different from the more common Red Hat key used to sign kernels in a General Availability (non-Beta) releases.

The Beta private key will likely not be recognized by your hardware, which means that any Beta release of Red Hat Enterprise Linux 7 will not be able to boot. In order to use a Beta release with UEFI Secure Boot enabled, you need to add the Red Hat Beta public key to your system using the *Machine Owner Key* (MOK) facility.

The procedure to add the Red Hat Beta key to your system is below.

Procedure 5.1. Adding a Custom Private Key for UEFI Secure Boot

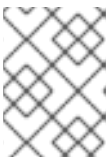
1. First, disable UEFI Secure Boot on the system, and install Red Hat Enterprise Linux 7 normally. The installation will not be able to proceed with Secure Boot enabled.

2. After the installation finishes, the system will reboot. Secure Boot should still be disabled at this point. Reboot the system, log in and, if applicable, go through the Initial Setup screens as described in Chapter 29, *Initial Setup*.

3. Open a terminal and log in as **root**. Then, execute the following command:

   ```
   # mokutil --import /lib/modules/$(uname -r)/kernel-signing-ca.cer
   ```

   Enter a password of your choosing when prompted.

   NOTE

   Make sure to remember the password. It will be required to finish this procedure as well as to remove the imported key when it is no longer needed.

4. Reboot the system again, and enable UEFI Secure Boot. Then, continue with the boot process; before the system starts, you will be prompted to confirm that you want to complete the pending key enrollment request. Select yes, and provide the password which you set earlier using the

mokutil command.

After finishing this procedure, the Red Hat Beta key will be added to your system. Any subsequent installations of Red Hat Enterprise Linux 7 Beta will *not* require you to perform this procedure again unless you manually remove the key.

WARNING

Remove the imported Beta public key when you no longer need it.

If you install a final (General Availability) release of Red Hat Enterprise Linux 7, or when you install a different operating system, you should remove the imported key. If you have *only* imported this public key, you can use the following command to reset the MOK:

```
# mokutil --reset
```

After the next reboot, you will be prompted for a confirmation and the password you created when importing the key. The key will be removed from the MOK after providing the correct password, and the system will revert to its original state.

CHAPTER 6. UPDATING DRIVERS DURING INSTALLATION ON AMD64 AND INTEL 64 SYSTEMS

In most cases, Red Hat Enterprise Linux already includes drivers for the devices that make up your system. However, if your system contains hardware that has been released very recently, drivers for this hardware might not yet be included. Sometimes, a driver update that provides support for a new device might be available from Red Hat or your hardware vendor on a *driver disc* that contains *RPM packages*. Typically, the driver disc is available for download as an *ISO image file*.

IMPORTANT

Driver updates should only be performed if a missing driver prevents you to complete the installation successfully. The drivers included in the kernel should always be preferred over drivers provided by other means.

Often, you do not need the new hardware during the installation process. For example, if you use a DVD to install to a local hard drive, the installation will succeed even if drivers for your network card are not available. In such a situation, complete the installation and add support for the new hardware afterward - see Red Hat Enterprise Linux 7 System Administrator's Guide for details of adding this support.

In other situations, you might want to add drivers for a device during the installation process to support a particular configuration. For example, you might want to install drivers for a network device or a storage adapter card to give the installation program access to the storage devices that your system uses. You can use a driver disc to add this support during installation in one of two ways:

1. place the ISO image file of the driver disc in a location accessible to the installation program, on a local hard drive, on a USB flash drive, or on a CD or DVD.

2. create a driver disc by extracting the image file onto a CD or a DVD, or a USB flash drive. See the instructions for making installation discs in Section 3.1, “Making an Installation CD or DVD” for more information on burning ISO image files to a CD or DVD, and Section 3.2, “Making Installation USB Media” for instructions on writing ISO images to USB drives.

If Red Hat, your hardware vendor, or a trusted third party told you that you will require a driver update during the installation process, choose a method to supply the update from the methods described in this chapter and test it before beginning the installation. Conversely, do not perform a driver update during installation unless you are certain that your system requires it. The presence of a driver on a system for which it was not intended can complicate support.

WARNING

Driver update disks sometimes disable conflicting kernel drivers, where necessary. In rare cases, unloading a kernel module in this way can cause installation errors.

6.1. LIMITATIONS OF DRIVER UPDATES DURING INSTALLATION

On UEFI systems with the Secure Boot technology enabled, all drivers being loaded must be signed with a valid certificate, otherwise the system will refuse them. All drivers provided by Red Hat are signed by one of Red Hat's private keys and authenticated by the corresponding Red Hat public key in the kernel. If

you load any other drivers (ones not provided on the Red Hat Enterprise Linux installation DVD), you must make sure that they are signed as well.

More information about signing custom drivers can be found in the Working with Kernel Modules chapter in the Red Hat Enterprise Linux 7 System Administrator's Guide.

6.2. PREPARING FOR A DRIVER UPDATE DURING INSTALLATION

If a driver update is necessary and available for your hardware, Red Hat, your hardware vendor, or another trusted third party will typically provide it in the form of an image file in ISO format. Once you obtain the ISO image, you must decide on the method you want to use to perform the driver update.

The available methods are:

Automatic driver update

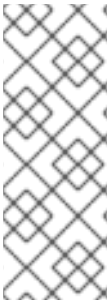
When starting the installation, the **Anaconda** installation program will attempt to detect all attached storage devices. If there is a storage device labeled **OEMDRV** present when the installation begins, **Anaconda** will always treat it like a driver update disc and attempt to load drivers present on it.

Assisted driver update

You can specify the **inst.dd** boot option when starting the installation. If you use this option without any parameters, **Anaconda** will display a list of all storage devices connected to the system, and it will prompt you to select a device which contains a driver update.

Manual driver update

You can specify the **inst.dd=*location*** boot option when starting the installation, where *location* is the path to a driver update disc or ISO image. When you specify this option, **Anaconda** will attempt to load any driver updates it finds at the specified location. With manual driver updates, you can specify either locally available storage devices, or a network location (an **HTTP**, **HTTPS** or **FTP** server).



NOTE

You can also use both **inst.dd=*location*** and **inst.dd** at the same time. However, what **Anaconda** does in this case depends on the type of *location* that you use. If it is a device, **Anaconda** prompts you to select drivers to update from the specified device and then it offers you additional devices. If *location* is a network location, **Anaconda** first prompts you to select a device containing a driver update and then it lets you update drivers from the specified network location.

If you want to use the automatic driver update method, you must create a storage device labeled **OEMDRV**, and it must be physically connected to the installation system. To use the assisted method, you can use any local storage device any label other than **OEMDRV**. To use the manual method, you can use any local storage with a different label, or a network location accessible from the installation system.

IMPORTANT

Make sure to initialize the network using the **ip=** option when loading a driver update from a network location. See Section 22.1, “Configuring the Installation System at the Boot Menu” for details.

6.2.1. Preparing to Use a Driver Update Image File on Local Storage

If you use a local storage device to provide the ISO file, such as a hard drive or USB flash drive, you can make the installation program to recognize it automatically by properly labeling the device. Only if it is not possible, install the update manually as described below.

- In order for the installation program to automatically recognize the driver disk, the volume label of the storage device must be **OEMDRV**. Also, you will need to extract the contents of the ISO image file to the root directory of the storage device rather than copy the ISO image itself. See Section 6.3.1, “Automatic Driver Update”. Note that installation of a driver from a device labeled **OEMDRV** is always recommended and preferable to the manual installation.

- For manual installation, simply copy the ISO image, as a single file, onto the storage device. You can rename the file if you find it helpful but you must not change the file name extension, which must remain **.iso**, for example **dd.iso**. See Section 6.3.3, “Manual Driver Update” to learn how to select the driver update manually during installation.

6.2.2. Preparing a Driver Disc

You can create a driver update disc on a CD or DVD. See Section 3.1, “Making an Installation CD or DVD” to learn more about burning discs from image files.

After you burn a driver update disc CD or DVD, verify that the disc was created successfully by inserting it into your system and browsing to it using the file manager. You should see a single file named **rhdd3**, which is a signature file that contains the driver disc's description, and a directory named **rpms**, which contains the RPM packages with the actual drivers for various architectures.

If you see only a single file ending in **.iso**, then you have not created the disc correctly and should try again. Ensure that you choose an option similar to **Burn from Image** if you use a Linux desktop other than **GNOME**, or if you use a different operating system.

6.3. PERFORMING A DRIVER UPDATE DURING INSTALLATION

At the very beginning of the installation process, you can perform a driver update in the following ways:

- let the installation program automatically find and offer a driver update for installation,

- let the installation program prompt you to locate a driver update,

- manually specify a path to a driver update image or an RPM package.

IMPORTANT

Always make sure to put your driver update discs on a standard disk partition. Advanced storage, such as RAID or LVM volumes, might not be accessible during the early stage of the installation when you perform driver updates.

6.3.1. Automatic Driver Update

To have the installation program automatically recognize a driver update disc, connect a block device with the **OEMDRV** volume label to your computer before starting the installation process.

NOTE

Starting with Red Hat Enterprise Linux 7.2, you can also use the **OEMDRV** block device to automatically load a Kickstart file. This file must be named **ks.cfg** and placed in the root of the device to be loaded. See Chapter 26, *Kickstart Installations* for more information about Kickstart installations.

When the installation begins, the installation program detects all available storage connected to the system. If it finds a storage device labeled **OEMDRV**, it will treat it as a driver update disc and attempt to load driver updates from this device. You will be prompted to select which drivers to load:

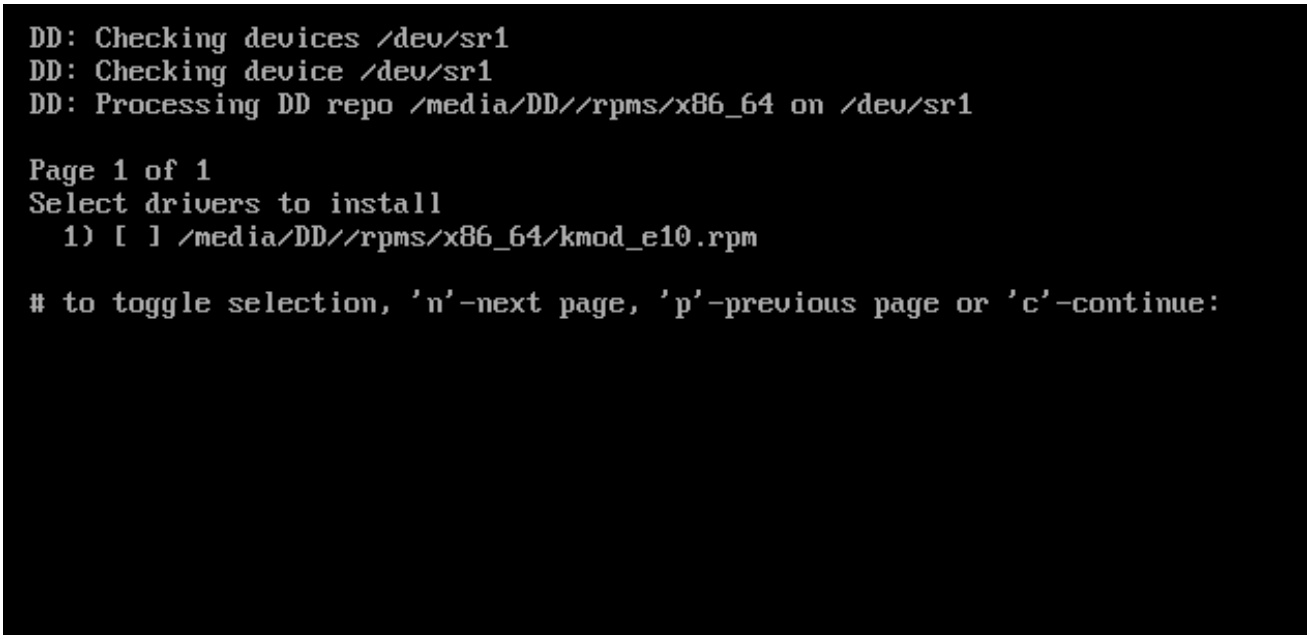


Figure 6.1. Selecting a Driver

Use number keys to toggle selection on individual drivers. When ready, press **c** to install the selected drivers and proceed to the **Anaconda** graphical user interface.

6.3.2. Assisted Driver Update

It is always recommended to have a block device with the **OEMDRV** volume label available to install a driver during installation. However, if no such device is detected and the **inst.dd** option was specified at the boot command line, the installation program lets you find the driver disk in interactive mode. In the first step, select a local disk partition from the list for **Anaconda** to scan for ISO files. Then, select one of the detected ISO files. Finally, select one or more available drivers. The image below demonstrates the process in the text user interface with individual steps highlighted.

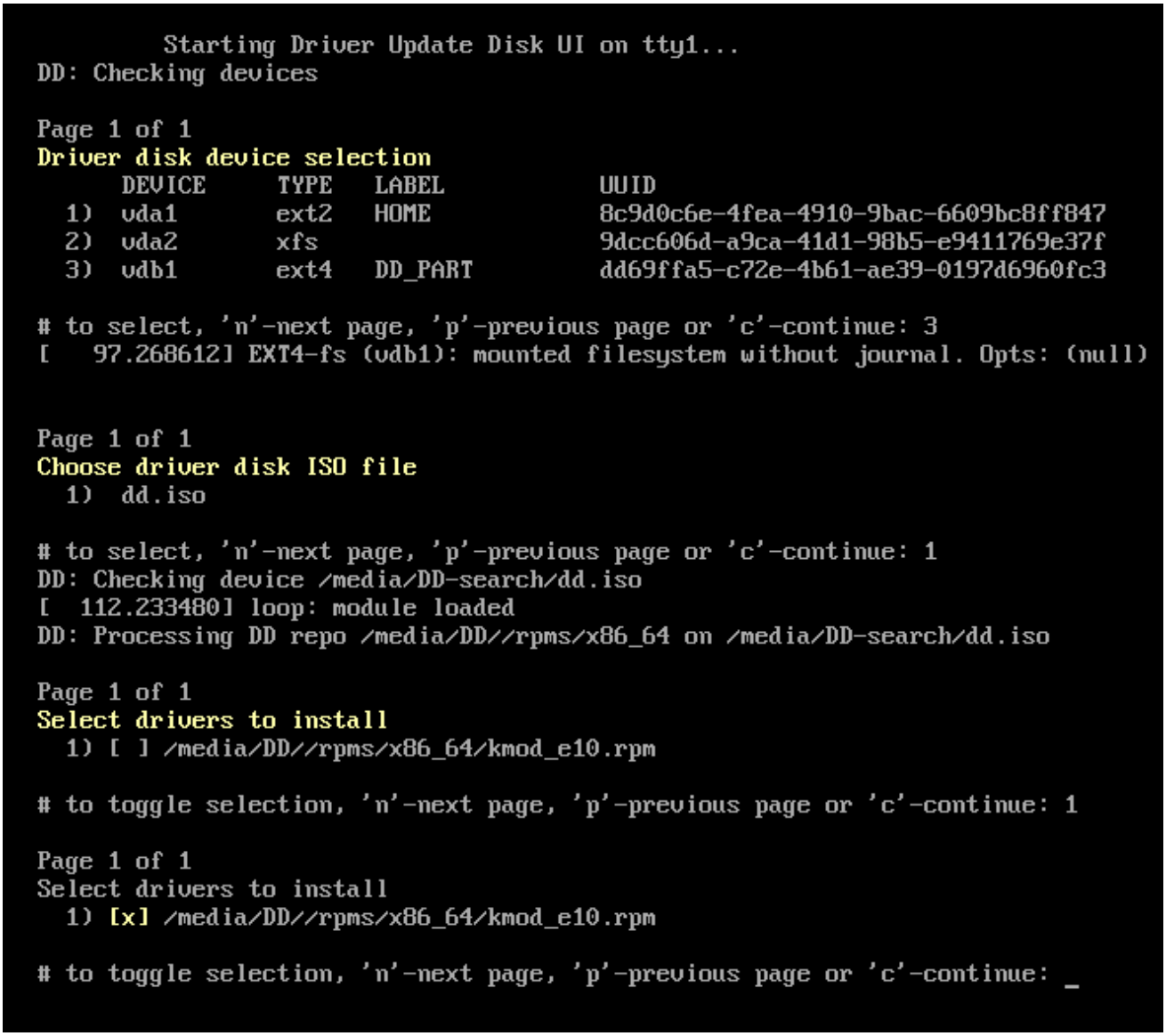


Figure 6.2. Selecting a Driver Interactively

NOTE

If you extracted your ISO image file and burned it on a CD or DVD but the media does not have the **OEMDRV** volume label, either use the **inst.dd** option with no arguments and use the menu to select the device, or use the following boot option for the installation program to scan the media for drivers:

```
inst.dd=/dev/sr0
```

Hit number keys to toggle selection on individual drivers. When ready, press **c** to install the selected drivers and proceed to the **Anaconda** graphical user interface.

6.3.3. Manual Driver Update

For manual driver installation, prepare an ISO image file containing your drivers to an accessible location, such a USB flash drive or a web server, and connect it to your computer. At the welcome screen, hit **Tab** to display the boot command line and append the **inst.dd=*location*** to it, where *location* is a path to the driver update disc:

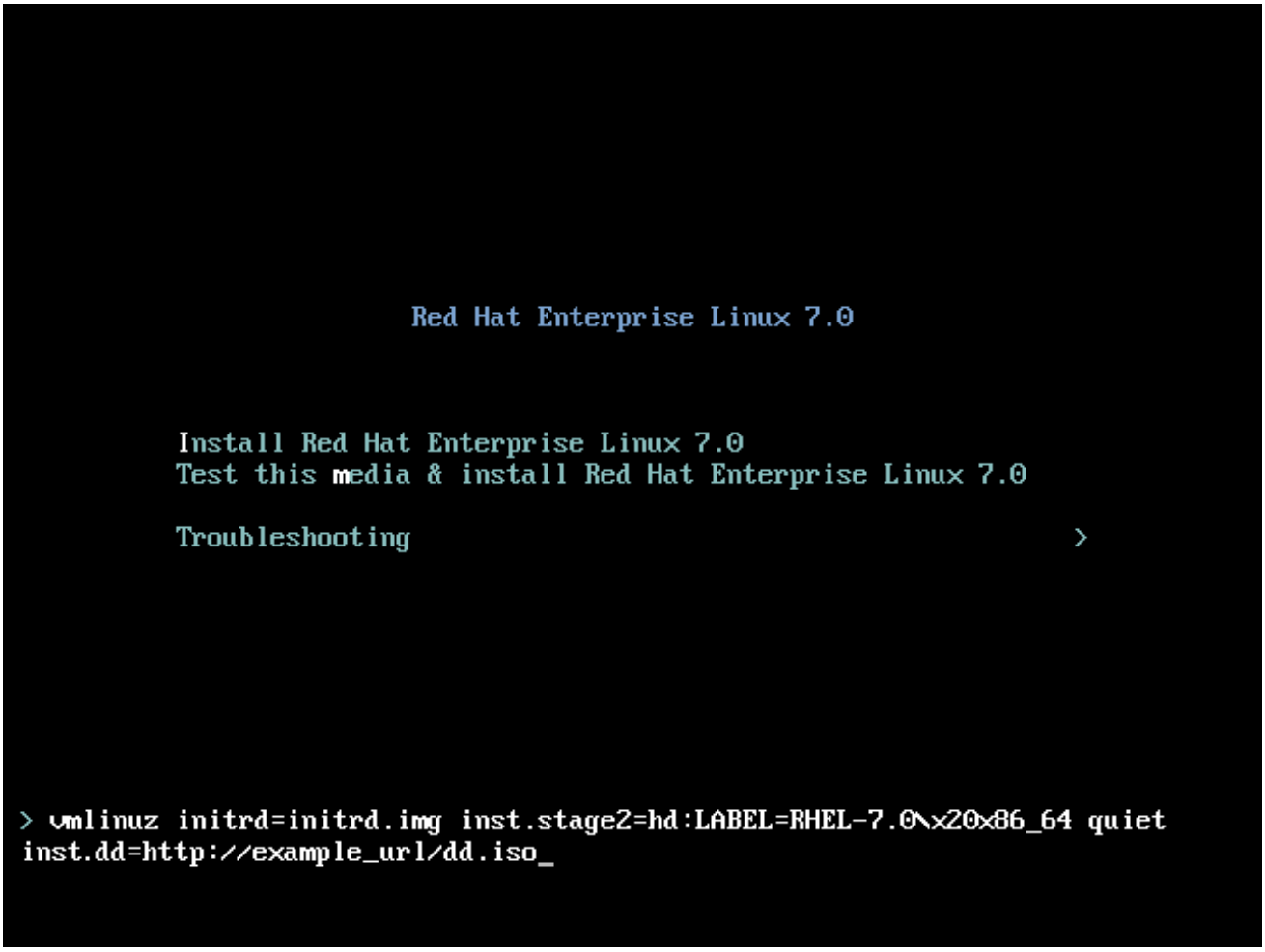


Figure 6.3. Specifying a Path to a Driver Update

Typically, the image file is located on a web server (for example, *http://server.example.com/dd.iso*) or on a USB flash drive (for example, */dev/sdb1*). It is also possible to specify an RPM package containing the driver update (for example *http://server.example.com/dd.rpm*).

When ready, hit **Enter** to execute the boot command. Then, your selected drivers will be loaded and the installation process will proceed normally.

6.3.4. Blacklisting a Driver

A malfunctioning driver can prevent a system from booting normally during installation. When this happens, you can disable (or blacklist) the driver by customizing the boot command line. At the boot menu, display the boot command line by hitting the **Tab** key. Then, append the **modprobe.blacklist=*driver_name*** option to it. Replace *driver_name* with names of a driver or drivers you want to disable, for example:

```
modprobe.blacklist=ahci
```

Note that the drivers blacklisted during installation using the **modprobe.blacklist=** boot option will remain disabled on the installed system and appear in the **/etc/modprobe.d/anaconda-blacklist.conf** file. See Chapter 22, *Boot Options* for more information about blacklisting drivers and other boot options.

CHAPTER 7. BOOTING THE INSTALLATION ON AMD64 AND INTEL 64 SYSTEMS

You can install Red Hat Enterprise Linux from the ISO images stored on hard disk, or from a network using **NFS**, **FTP**, **HTTP**, or **HTTPS** methods. Booting and installing from the full installation DVD is the easiest method to get started with. Other methods require some additional setup but provide different advantages that might suit your needs better. For example, when installing Red Hat Enterprise Linux on a large number of computers at the same time, the best approach is booting from a PXE server and installing from a source in a shared network location.

The following table summarizes the different boot methods and recommended installation methods to use with each:

Table 7.1. Boot Methods and Installation Sources

Boot method	Installation source
Full installation media (DVD or USB)	The boot media itself
Minimal boot media (CD or USB)	Full installation DVD ISO image or the installation tree extracted from this image, placed in a network location or on a hard drive
Network boot (PXE)	Full installation DVD ISO image or the installation tree extracted from this image, placed in a network location

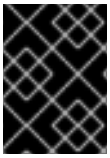
To create a boot CD-ROM or to prepare your USB flash drive for booting or installation, see Section 3.2, “Making Installation USB Media”.

This chapter covers the following topics:

- Section 7.1.1, “Booting the Installation on AMD64 and Intel 64 Systems from Physical Media” describes how to boot the installation program using physical media (Red Hat Enterprise Linux DVD, Boot CD-ROM, USB flash drive).
- Section 7.1.2, “Booting the Installation on AMD64 and Intel 64 Systems from the Network Using PXE” describes how to boot the installation program using PXE.
- Section 7.2, “The Boot Menu” contains information on the boot menu.

7.1. STARTING THE INSTALLATION PROGRAM

To start, first make sure that you have all necessary resources for the installation. If you have already read through Chapter 5, *Planning for Installation on AMD64 and Intel 64 Systems*, and followed the instructions, you should be ready to start the installation process. When you have verified that you are ready to begin, boot the installation program using the Red Hat Enterprise Linux DVD or any boot media that you have created.



IMPORTANT

Excessive input (for example, clicking the mouse repeatedly) during the boot sequence can cause the installer to ignore keyboard input later in the installation process.

NOTE

Occasionally, some hardware components require a *driver update* during the installation. A driver update adds support for hardware that is not otherwise supported by the installation program. See Chapter 6, *Updating Drivers During Installation on AMD64 and Intel 64 Systems* for more information.

7.1.1. Booting the Installation on AMD64 and Intel 64 Systems from Physical Media

To start the installation program from a Red Hat Enterprise Linux DVD or from minimal boot media, follow this procedure:

Procedure 7.1. Booting the Installation from Physical Media

1. Disconnect any drives which you do not need for the installation. See Section 5.6.3, “USB Disks” for more information.
2. Power on your computer system.
3. Insert the media in your computer.
4. Power off your computer with the boot media still inside.
5. Power on your computer system. Note that you might need to press a specific key or combination of keys to boot from the media or configure your system's *Basic Input/Output System* (BIOS) to boot from the media. For more information, see the documentation that came with your system.

After a short delay, the boot screen appears, which contains information on a variety of boot options. Installation program automatically begins if you take no action within the first minute. For a description of the options available on this screen, see Section 7.2, “The Boot Menu”.

7.1.2. Booting the Installation on AMD64 and Intel 64 Systems from the Network Using PXE

To boot with PXE, you need a properly configured TFTP server, and a network interface in your computer that supports PXE. For information on how to configure a PXE server, see Chapter 23, *Preparing for a Network Installation*.

Configure the computer to boot from the network interface. This option is in the BIOS, and can be labeled **`Network Boot`** or **`Boot Services`**. Also, ensure that the BIOS is configured to boot first from the correct network interface. Some BIOS systems specify the network interface as a possible boot device, but do not support the PXE standard. See your hardware's documentation for more information. Once you properly enable PXE booting, the computer can boot the Red Hat Enterprise Linux installation system without any other media.

Follow the procedure below to boot the installation program from a PXE server. Note that this procedure requires the use of a physical network connection, for example Ethernet. It will not work with a wireless connection.

Procedure 7.2. Booting the Installation from the Network Using PXE

1. Ensure that the network cable is attached. The link indicator light on the network socket should be lit, even if the computer is not switched on.

2. Switch on the computer.

3. Depending on your hardware, some network setup and diagnostic information can be displayed before your computer connects to a PXE server. Once it connects, a menu is displayed according to the configuration of the PXE server. Press the number key that corresponds to the desired option. If you are not sure of which option to select, ask your server administrator.

At this point, the installation program starts successfully and the boot screen appears, which contains information on a variety of boot options. Installation program automatically begins if you take no action within the first minute. For a description of the options available on this screen, see Section 7.2, “The Boot Menu”.

7.2. THE BOOT MENU

Once your system has completed loading the boot media, a boot menu is displayed using **GRUB2** (**GRand Unified Bootloader**, version 2). The boot menu provides several options in addition to launching the installation program. If no key is pressed within 60 seconds, the default boot option (the one highlighted in white) will be run. To choose the default, either wait for the timer to run out or press **Enter**.

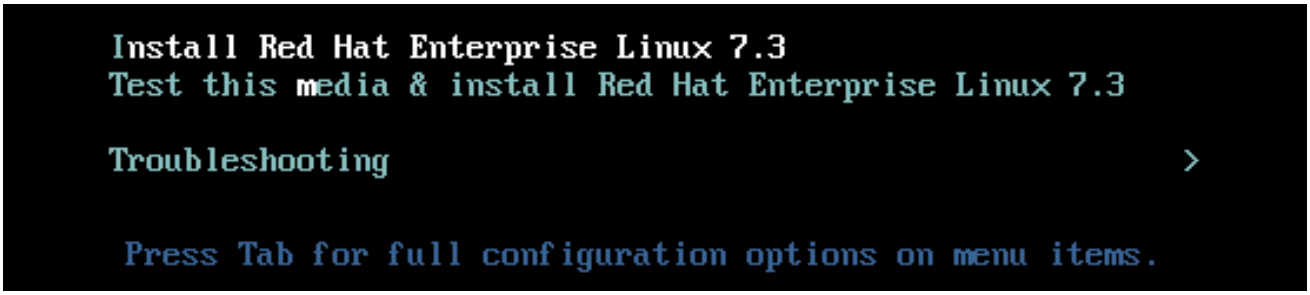


Figure 7.1. The Boot Screen

To select a different option than the default, use the arrow keys on your keyboard, and press **Enter** when the correct option is highlighted.

To customize the boot options for a particular menu entry:

- On BIOS-based systems, the preferred way is to press the **Tab** key and add custom boot options to the command line. You can also access the **boot:** prompt by pressing the **Esc** key but no required boot options will be preset in it. In that case, you must always specify the **linux** option before using any other boot options.

- On UEFI-based systems, press the **e** key and add custom boot options to the command line. When ready press **Ctrl**+**X** to boot the modified option.

See Chapter 22, *Boot Options* for more information about additional boot options.

The boot menu options are:

Install Red Hat Enterprise Linux 7.0

Choose this option to install Red Hat Enterprise Linux onto your computer system using the graphical installation program.

Test this media & install Red Hat Enterprise Linux 7.0

This option is the default. Prior to starting the installation program, a utility is launched to check the integrity of the installation media.

Troubleshooting >

This item is a separate menu containing options that help resolve various installation issues. When highlighted, press **Enter** to display its contents.

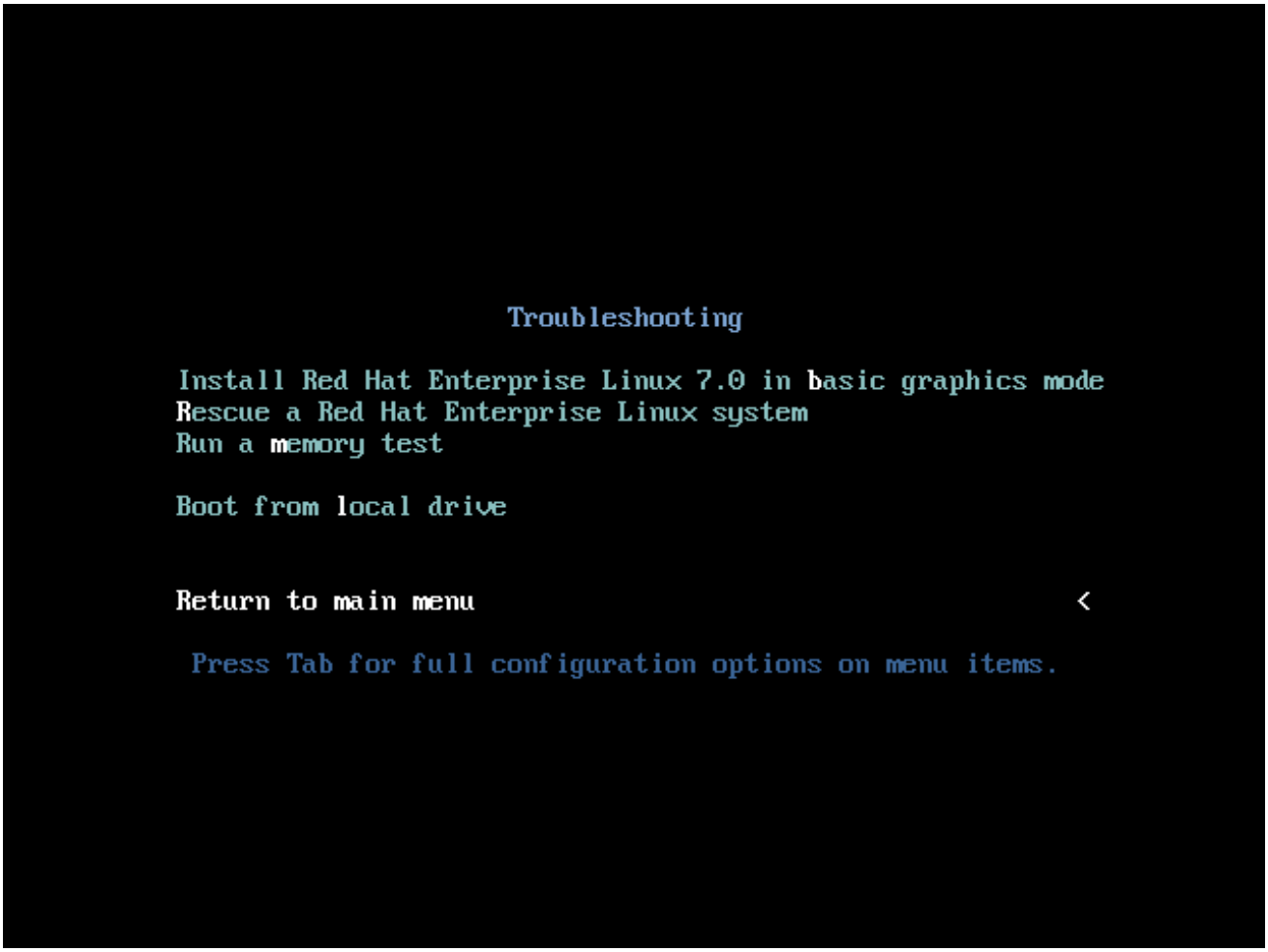


Figure 7.2. The Troubleshooting Menu

Install Red Hat Enterprise Linux 7.0 in basic graphics mode

This option allows you to install Red Hat Enterprise Linux in graphical mode even if the installation program is unable to load the correct driver for your video card. If your screen appears distorted or goes blank when using the **Install Red Hat Enterprise Linux 7.0** option, restart your computer and try this option instead.

Rescue a Red Hat Enterprise Linux system

Choose this option to repair a problem with your installed Red Hat Enterprise Linux system that prevents you from booting normally. The rescue environment contains utility programs that allow you fix a wide variety of these problems.

Run a memory test

This option runs a memory test on your system. For more information, see Section 22.2.1, “Loading the Memory (RAM) Testing Mode”.

Boot from local drive

This option boots the system from the first installed disk. If you booted this disc accidentally, use this option to boot from the hard disk immediately without starting the installation program.

CHAPTER 8. INSTALLING USING ANACONDA

This chapter provides step-by-step instructions for installing Red Hat Enterprise Linux using the **Anaconda** installer. The bulk of this chapter describes installation using the graphical user interface. A text mode is also available for systems with no graphical display, but this mode is limited in certain aspects (for example, custom partitioning is not possible in text mode).

If your system does not have the ability to use the graphical mode, you can:

- Use Kickstart to automate the installation as described in Chapter 26, *Kickstart Installations*
- Perform the graphical installation remotely by connecting to the installation system from another computer with a graphical display using the *VNC* (Virtual Network Computing) protocol - see Chapter 24, *Using VNC*

8.1. INTRODUCTION TO ANACONDA

The Red Hat Enterprise Linux installer, **Anaconda**, is different from most other operating system installation programs due to its parallel nature. Most installers follow a fixed path: you must choose your language first, then you configure network, then installation type, then partitioning, and so on. There is usually only one way to proceed at any given time.

In **Anaconda** you are only required to select your language and locale first, and then you are presented with a central screen, where you can configure most aspects of the installation in any order you like. This does not apply to all parts of the installation process, however - for example, when installing from a network location, you must configure the network before you can select which packages to install.

Some screens will be automatically configured depending on your hardware and the type of media you used to start the installation. You can still change the detected settings in any screen. Screens which have not been automatically configured, and therefore require your attention before you begin the installation, are marked by an exclamation mark. You cannot start the actual installation process before you finish configuring these settings.

Additional differences appear in certain screens; notably the custom partitioning process is very different from other Linux distributions. These differences are described in each screen's subsection.

8.2. CONSOLES AND LOGGING DURING THE INSTALLATION

The following sections describe how to access logs and an interactive shell during the installation. This is useful when troubleshooting problems, but should not be necessary in most cases.

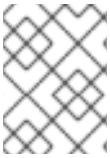
8.2.1. Accessing Consoles

The Red Hat Enterprise Linux installer uses the **tmux** terminal multiplexer to display and control several windows you can use in addition to the main interface. Each of these windows serves a different purpose - they display several different logs, which can be used to troubleshoot any issues during the installation, and one of the windows provides an interactive shell prompt with `root` privileges, unless this prompt was specifically disabled using a boot option or a Kickstart command.

NOTE

In general, there is no reason to leave the default graphical installation environment unless you need to diagnose an installation problem.

The terminal multiplexer is running in virtual console 1. To switch from the graphical installation environment to **tmux**, press **Ctrl+Alt+F1**. To go back to the main installation interface which runs in virtual console 6, press **Ctrl+Alt+F6**.



NOTE

If you choose text mode installation, you will start in virtual console 1 (**tmux**), and switching to console 6 will open a shell prompt instead of a graphical interface.

The console running **tmux** has 5 available windows; their contents are described in the table below, along with keyboard shortcuts used to access them. Note that the keyboard shortcuts are two-part: first press **Ctrl+b**, then release both keys, and press the number key for the window you want to use.

You can also use **Ctrl+b n** and **Ctrl+b p** to switch to the next or previous **tmux** window, respectively.

Table 8.1. Available tmux Windows

Shortcut	Contents
Ctrl+b 1	Main installation program window. Contains text-based prompts (during text mode installation or if you use VNC Direct Mode), and also some debugging information.
Ctrl+b 2	Interactive shell prompt with **root** privileges.
Ctrl+b 3	Installation log; displays messages stored in **/tmp/anaconda.log**.
Ctrl+b 4	Storage log; displays messages related storage devices from kernel and system services, stored in **/tmp/storage.log**.
Ctrl+b 5	Program log; displays messages from other system utilities, stored in **/tmp/program.log**.

In addition to displaying diagnostic information in **tmux** windows, **Anaconda** also generates several log files, which can be transferred from the installation system. These log files are described in Table 9.1, “Log Files Generated During the Installation”, and directions for transferring them from the installation system are available in Chapter 9, *Troubleshooting Installation on AMD64 and Intel 64 Systems*.

8.2.2. Saving Screenshots

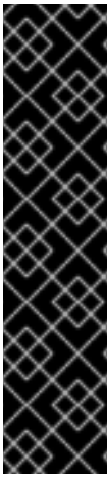
You can press **Shift+Print Screen** at any time during the graphical installation to capture the current screen. These screenshots are saved to **/tmp/anaconda-screenshots/**.

Additionally, you can use the **autostep --autoscreenshot** command in a Kickstart file to capture and save each step of the installation automatically. See Section 26.3.1, “Kickstart Commands and Options” for details.

8.3. INSTALLING IN TEXT MODE

Text mode installation offers an interactive, non-graphical interface for installing Red Hat Enterprise Linux. This can be useful on systems with no graphical capabilities; however, you should always consider the available alternatives before starting a text-based installation. Text mode is limited in

the amount of choices you can make during the installation.



IMPORTANT

Red Hat recommends that you install Red Hat Enterprise Linux using the graphical interface. If you are installing Red Hat Enterprise Linux on a system that lacks a graphical display, consider performing the installation over a VNC connection - see Chapter 24, *Using VNC*. The text mode installation program will prompt you to confirm the use of text mode if it detects that a VNC-based installation is possible.

If your system has a graphical display, but graphical installation fails, try booting with the **inst.xdriver=vesa** option - see Chapter 22, *Boot Options*.

Alternatively, consider a Kickstart installation. See Chapter 26, *Kickstart Installations* for more information.

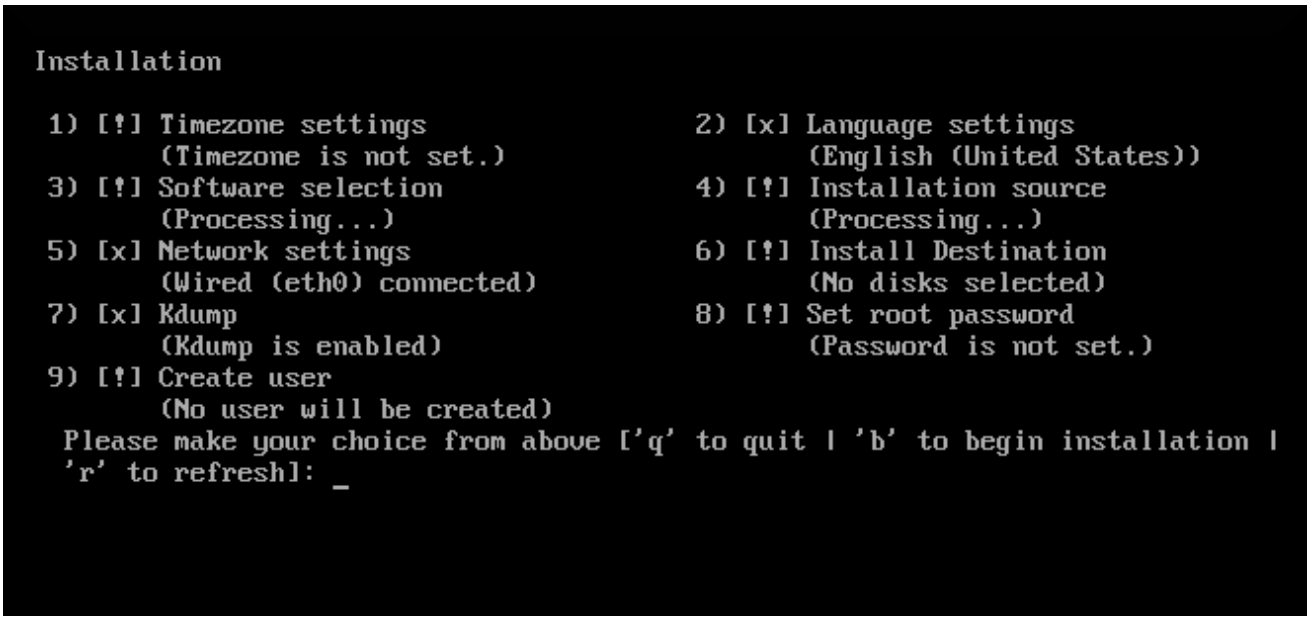
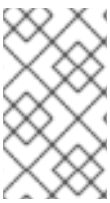


Figure 8.1. Text Mode Installation

Installation in text mode follows a pattern similar to the graphical installation: There is no single fixed progression; you can configure many settings in any order you want using the main status screen. Screens which have already been configured, either automatically or by you, are marked as **[x]**, and screens which require your attention before the installation can begin are marked with **[!]**. Available commands are displayed below the list of available options.



NOTE

When related background tasks are being run, certain menu items can be temporarily unavailable or display the **Processing...** label. To refresh to the current status of text menu items, use the **r** option at the text mode prompt.

At the bottom of the screen in text mode, a green bar is displayed showing five menu options. These options represent different screens in the **tmux** terminal multiplexer; by default you start in screen 1, and you can use keyboard shortcuts to switch to other screens which contain logs and an interactive command prompt. For information about available screens and shortcuts to switch to them, see Section 8.2.1, “Accessing Consoles”.

Limits of interactive text mode installation include:

- The installer will always use the English language and the US English keyboard layout. You can configure your language and keyboard settings, but these settings will only apply to the installed system, not to the installation.
- You cannot configure any advanced storage methods (LVM, software RAID, FCoE, zFCP and iSCSI).
- It is not possible to configure custom partitioning; you must use one of the automatic partitioning settings. You also cannot configure where the boot loader will be installed.
- You cannot select any package add-ons to be installed; they must be added after the installation finishes using the **Yum** package manager.

To start a text mode installation, boot the installation with the **`inst.text`** boot option used either at the boot command line in the boot menu, or in your PXE server configuration. See Chapter 7, *Booting the Installation on AMD64 and Intel 64 Systems* for information about booting and using boot options.

8.4. INSTALLING IN THE GRAPHICAL USER INTERFACE

The graphical installation interface is the preferred method of manually installing Red Hat Enterprise Linux. It allows you full control over all available settings, including custom partitioning and advanced storage configuration, and it is also localized to many languages other than English, allowing you to perform the entire installation in a different language. The graphical mode is used by default when you boot the system from local media (a CD, DVD or a USB flash drive).

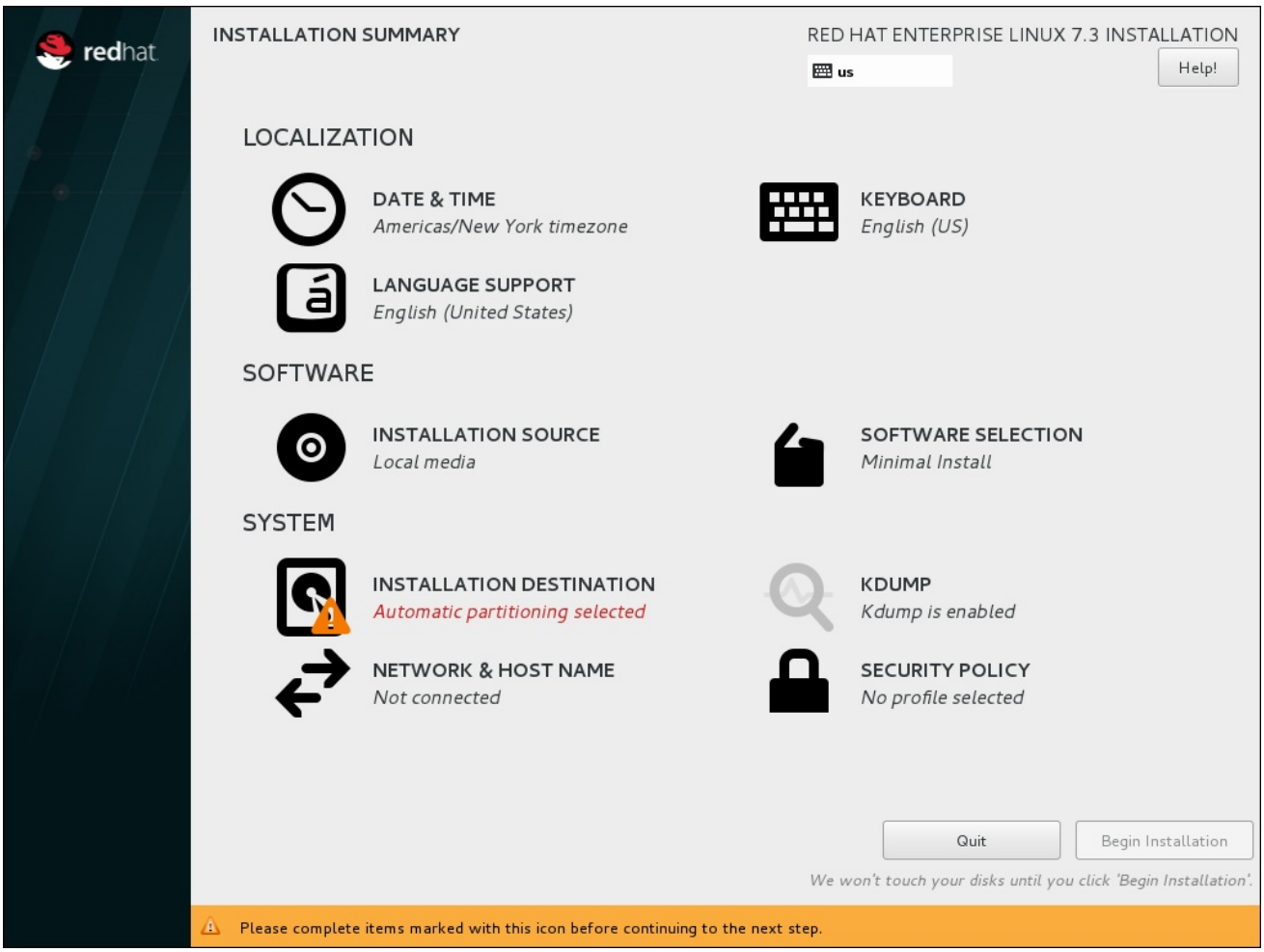


Figure 8.2. The `Installation Summary` Screen

The sections below discuss each screen available in the installation process. Note that due to the installer's parallel nature, most of the screens do not have to be completed in the order in which they are described here.

Each screen in the graphical interface contains a **Help** button. This button opens the **Yelp** help browser displaying the section of the *Red Hat Enterprise Linux Installation Guide* relevant to the current screen.

You can also control the graphical installer with your keyboard. Following table shows you the shortcuts you can use.

Table 8.2. Graphical installer keyboard shortcuts

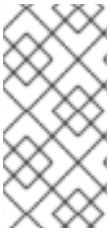
Shortcut keys	Usage
Tab and **Shift**+**Tab**	Cycle through active control elements (buttons, check boxes, and so on.) on the current screen
Up and **Down**	Scroll through lists
Left and **Right**	Scroll through horizontal toolbars and table entries
Space and **Enter**	Select or remove a highlighted item from selection and expand and collapse drop-down menus

Additionally, elements in each screen can be toggled using their respective shortcuts. These shortcuts are highlighted (underlined) when you hold down the **Alt** key; to toggle that element, press **Alt**+***X***, where *X* is the highlighted letter.

Your current keyboard layout is displayed in the top right hand corner. Only one layout is configured by default; if you configure more than layout in the **Keyboard Layout** screen (Section 8.9, “Keyboard Configuration”), you can switch between them by clicking the layout indicator.

8.5. WELCOME SCREEN AND LANGUAGE SELECTION

The first screen of the installation program is the **Welcome to Red Hat Enterprise Linux** screen. Here you select the language that **Anaconda** will use for the rest of the installation. This selection will also become the default for the installated system, unless changed later. In the left panel, select your language of choice, for example **English**. Then you can select a locale specific to your region in the right panel, for example **English (United States)**.



NOTE

One language is pre-selected by default on top of the list. If network access is configured at this point (for example, if you booted from a network server instead of local media), the pre-selected language will be determined based on automatic location detection using the **GeoIP** module.

Alternatively, type your preferred language into the search box as shown below.

Once you have made your selection, click the **Continue** button to proceed to the **Installation Summary** screen.

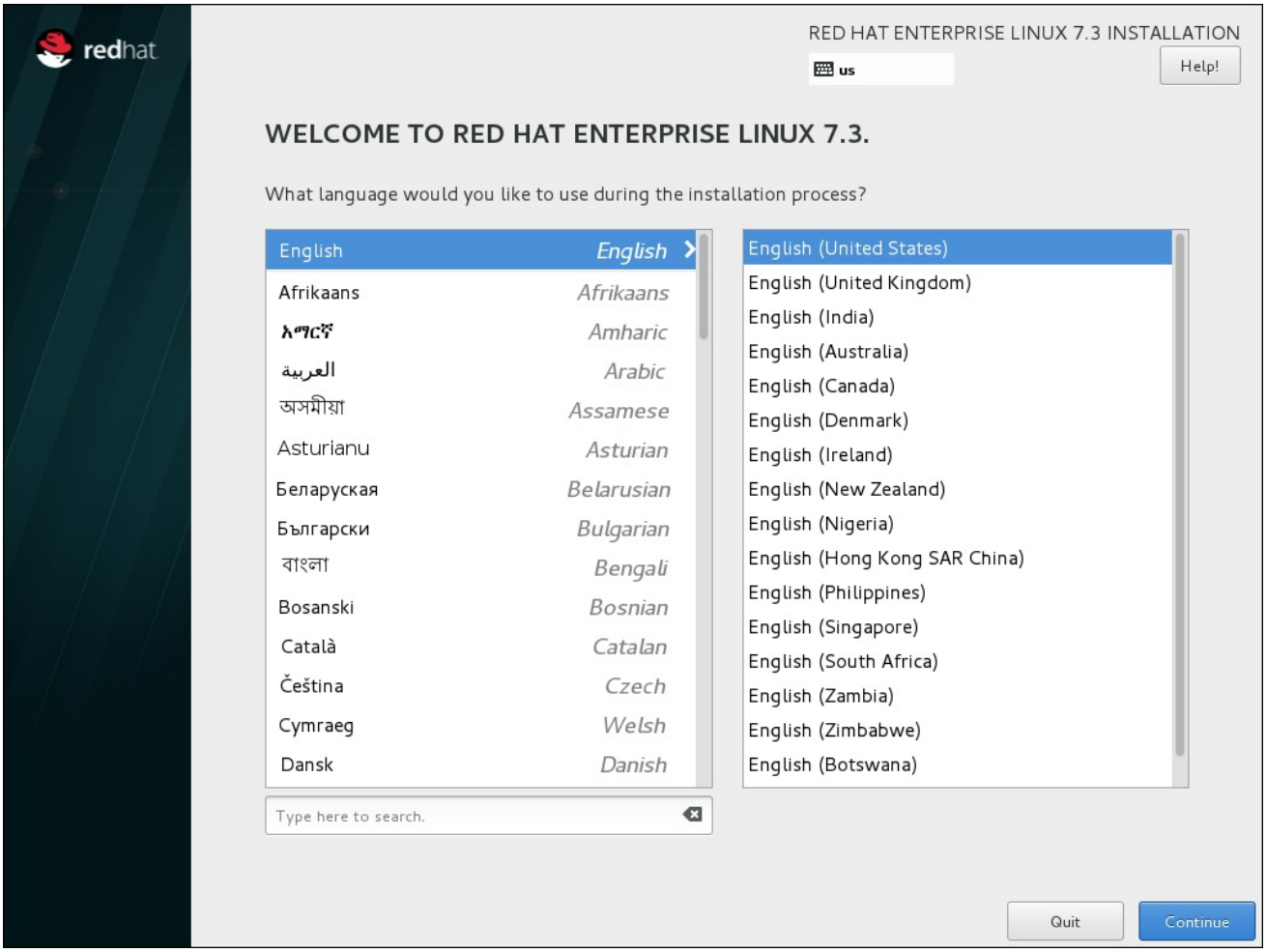


Figure 8.3. Language Configuration

After you click the **Continue** button, the unsupported hardware dialog may appear. This happens if you are using hardware that the kernel does not support.

8.6. THE INSTALLATION SUMMARY SCREEN

The **Installation Summary** screen is the central location for setting up an installation.

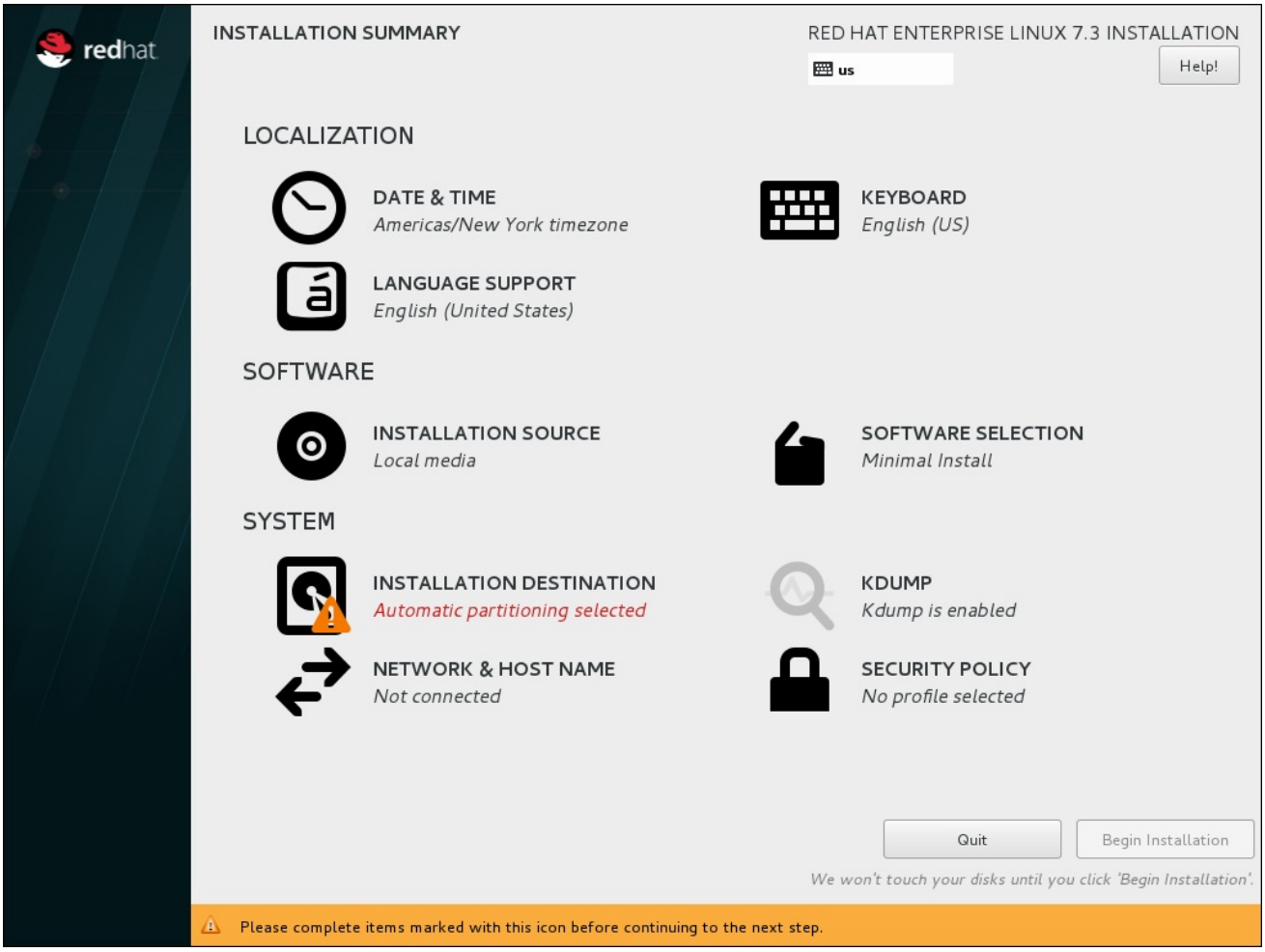


Figure 8.4. The `Installation Summary` Screen

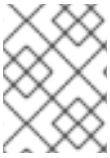
Instead of directing you through consecutive screens, the Red Hat Enterprise Linux installation program allows you to configure your installation in the order you choose.

Use your mouse to select a menu item to configure a section of the installation. When you have completed configuring a section, or if you would like to complete that section later, click the **Done** button located in the upper left corner of the screen.

Only sections marked with a warning symbol are mandatory. A note at the bottom of the screen warns you that these sections must be completed before the installation can begin. The remaining sections are optional. Beneath each section's title, the current configuration is summarized. Using this you can determine whether you need to visit the section to configure it further.

Once all required sections are complete, click the **`Begin Installation`** button. Also see Section 8.17, “Begin Installation”.

To cancel the installation, click the **`Quit`** button.



NOTE

When related background tasks are running, certain menu items might be temporarily unavailable.

If you used a Kickstart option or a boot command-line option to specify an installation repository on a network, but no network is available at the start of the installation, the installation program will display the configuration screen for you to set up a network connection prior to displaying the **`Installation`**

Summary screen.

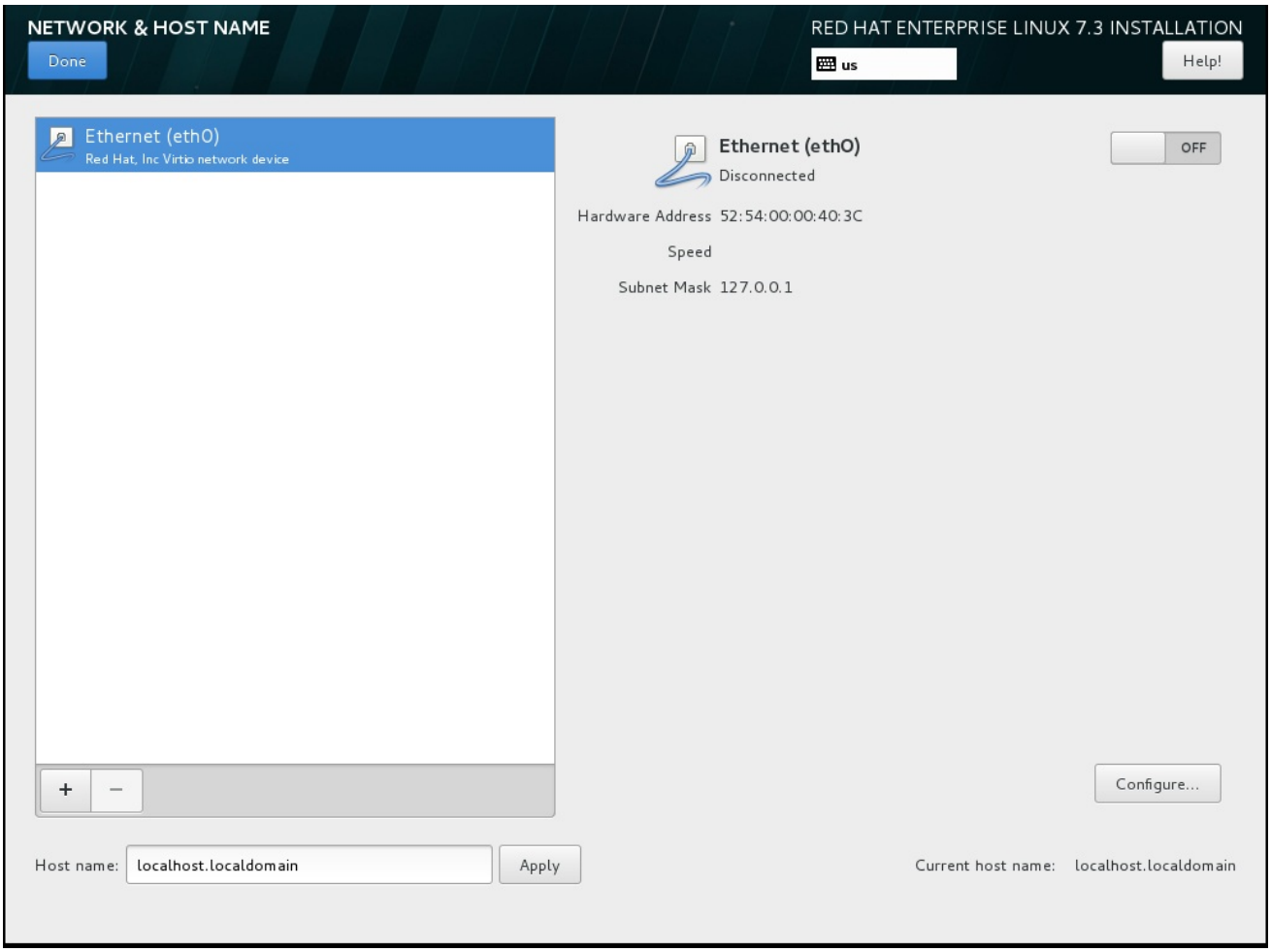


Figure 8.5. Network Configuration Screen When No Network Is Detected

You can skip this step if you are installing from an installation DVD or other locally accessible media, and you are certain you will not need network to finish the installation. However, network connectivity is necessary for network installations (see Section 8.11, “Installation Source”) or for setting up advanced storage devices (see Section 8.15, “Storage Devices”). For more details about configuring a network in the installation program, see Section 8.12, “Network & Hostname”.

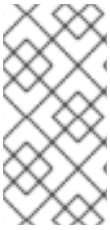
8.7. DATE & TIME

To configure time zone, date, and optionally settings for network time, select **Date & Time** at the **Installation Summary** screen.

There are three ways for you to select a time zone:

- Using your mouse, click on the interactive map to select a specific city. A red pin appears indicating your selection.
- You can also scroll through the **Region** and **City** drop-down menus at the top of the screen to select your time zone.
- Select **Etc** at the bottom of the **Region** drop-down menu, then select your time zone in the next menu adjusted to GMT/UTC, for example **GMT+1**.

If your city is not available on the map or in the drop-down menu, select the nearest major city in the same time zone.



NOTE

The list of available cities and regions comes from the Time Zone Database (tzdata) public domain, which is maintained by the Internet Assigned Numbers Authority (IANA). Red Hat cannot add cities or regions into this database. You can find more information at the official website, available at http://www.iana.org/time-zones.

Specify a time zone even if you plan to use NTP (Network Time Protocol) to maintain the accuracy of the system clock.

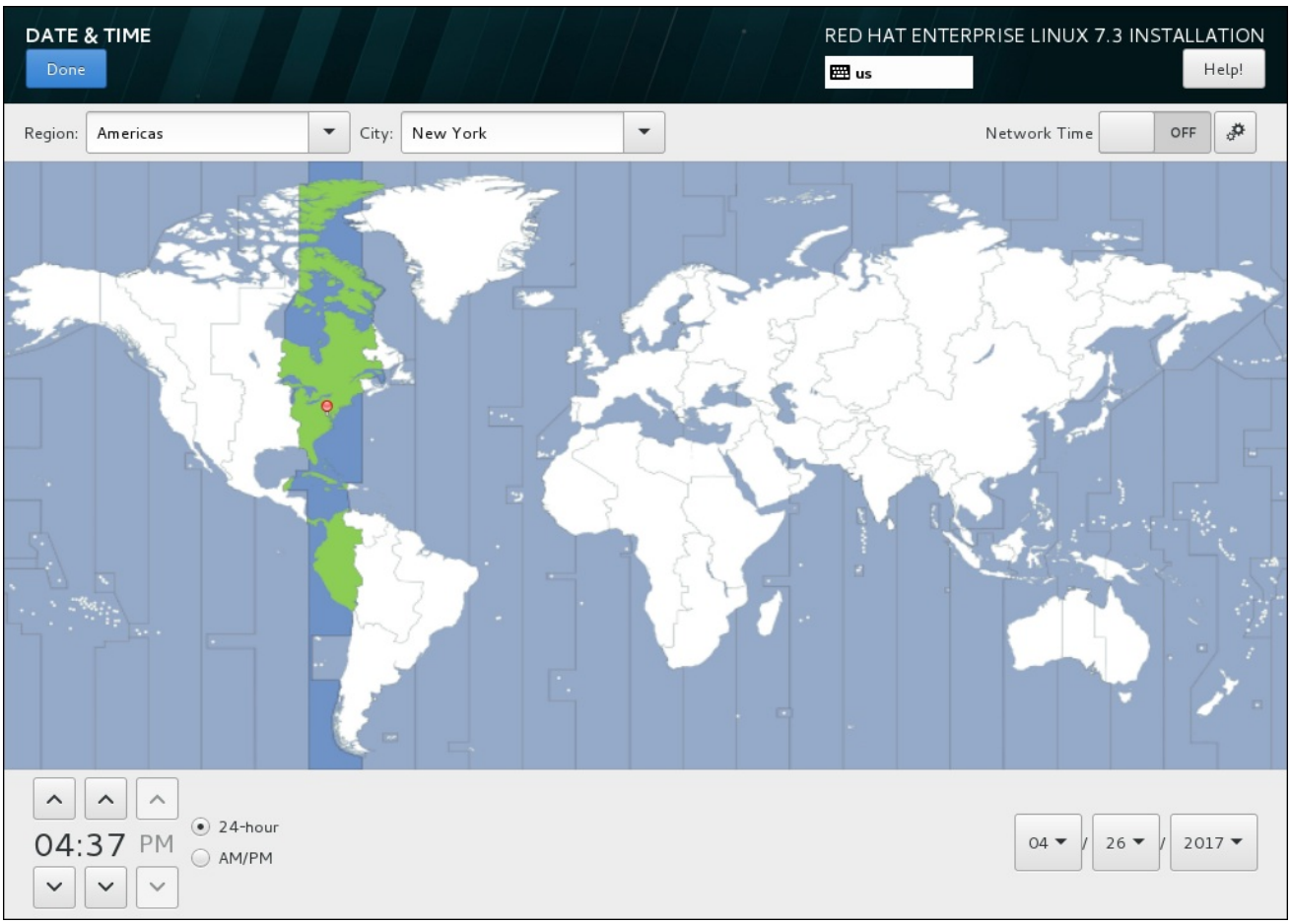


Figure 8.6. Time zone configuration screen

If you are connected to the network, the **Network Time** switch will be enabled. To set the date and time using NTP, leave the **Network Time** switch in the **ON** position and click the configuration icon to select which NTP servers Red Hat Enterprise Linux should use. To set the date and time manually, move the switch to the **OFF** position. The system clock should use your time zone selection to display the correct date and time at the bottom of the screen. If they are still incorrect, adjust them manually.

Note that NTP servers might be unavailable at the time of installation. In such a case, enabling them will not set the time automatically. When the servers become available, the date and time will update.

Once you have made your selection, click **Done** to return to the **Installation Summary** screen.

NOTE

To change your time zone configuration after you have completed the installation, visit the **Date & Time** section of the **Settings** dialog window.

8.8. LANGUAGE SUPPORT

To install support for additional locales and language dialects, select **Language Support** from the **Installation Summary** screen.

Use your mouse to select the language for which you would like to install support. In the left panel, select your language of choice, for example **Español**. Then you can select a locale specific to your region in the right panel, for example **Español (Costa Rica)**. You can select multiple languages and multiple locales. The selected languages are highlighted in bold in the left panel.

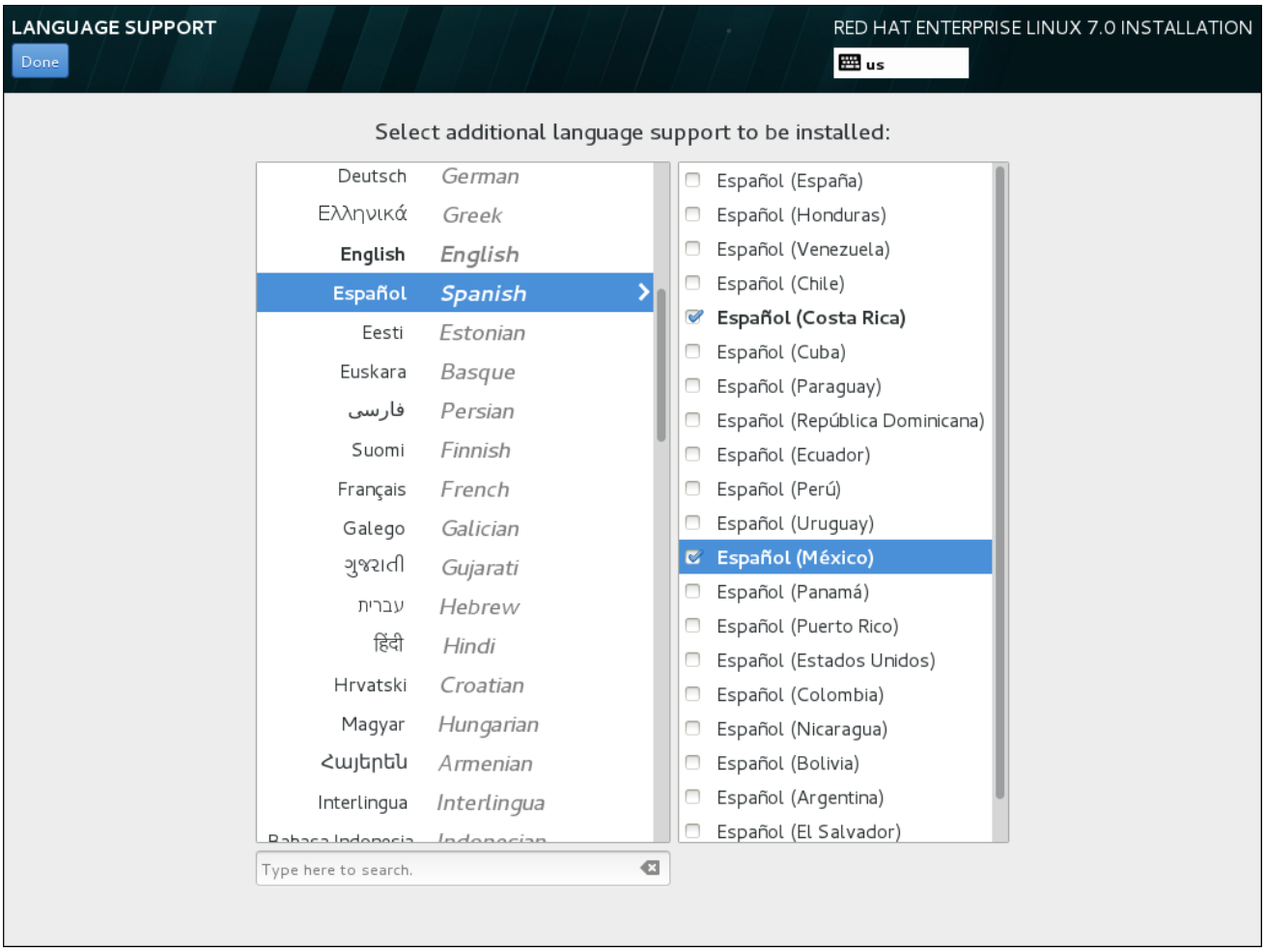
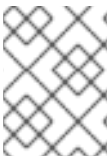


Figure 8.7. Configuring Language Support

Once you have made your selections, click **Done** to return to the **Installation Summary** screen.



NOTE

To change your language support configuration after you have completed the installation, visit the **Region & Language** section of the **Settings** dialog window.

8.9. KEYBOARD CONFIGURATION

To add multiple keyboard layouts to your system, select **Keyboard** from the **Installation Summary** screen. Upon saving, the keyboard layouts are immediately available in the installation program and you can switch between them by using the keyboard icon located at all times in the upper right corner of the screen.

Initially, only the language you selected in the welcome screen is listed as the keyboard layout in the left pane. You can either replace the initial layout or add more layouts. However, if your language does not use ASCII characters, you might need to add a keyboard layout that does, to be able to properly set a password for an encrypted disk partition or the root user, among other things.

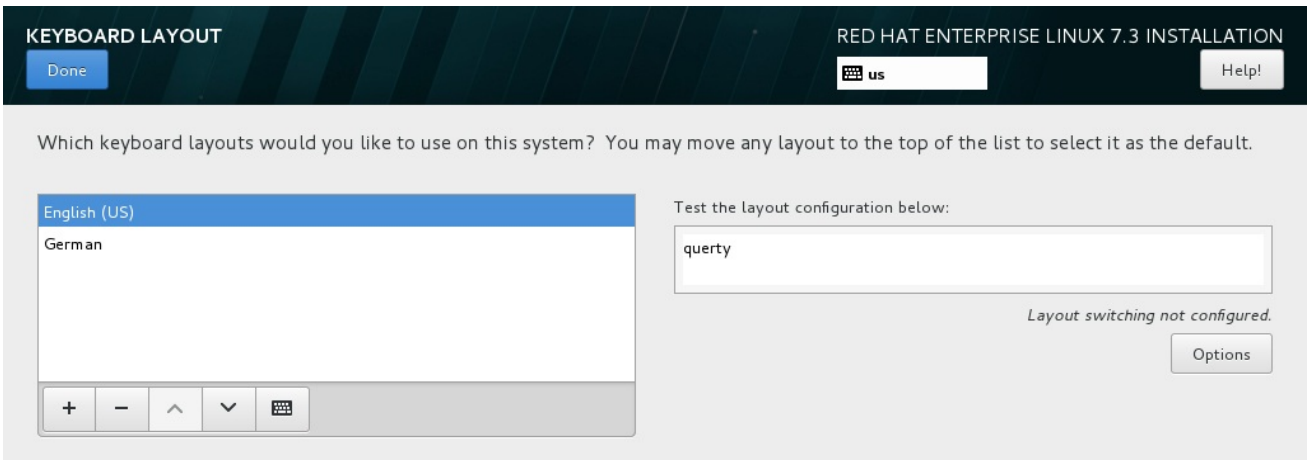


Figure 8.8. Keyboard Configuration

To add an additional layout, click the **+** button, select it from the list, and click **Add**. To delete a layout, select it and click the **-** button. Use the arrow buttons to arrange the layouts in order of preference. For a visual preview of the keyboard layout, select it and click the keyboard button.

To test a layout, use the mouse to click inside the text box on the right. Type some text to confirm that your selection functions correctly.

To test additional layouts, you can click the language selector at the top on the screen to switch them. However, it is recommended to set up a keyboard combination for switching layout. Click the **Options** button at the right to open the **Layout Switching Options** dialog and choose a combination from the list by selecting its check box. The combination will then be displayed above the **Options** button. This combination applies both during the installation and on the installed system, so you must configure a combination here in order to use one after installation. You can also select more than one combination to switch between layouts.

IMPORTANT

If you use a layout that cannot accept Latin characters, such as **Russian**, Red Hat recommends additionally adding the **English (United States)** layout and configuring a keyboard combination to switch between the two layouts. If you only select a layout without Latin characters, you might be unable to enter a valid root password and user credentials later in the installation process. This can prevent you from completing the installation.

Once you have made your selection, click **Done** to return to the **Installation Summary** screen.

NOTE

To change your keyboard configuration after you have completed the installation, visit the **Keyboard** section of the **Settings** dialogue window.

8.10. SECURITY POLICY

The **`Security Policy`** spoke allows you to configure the installed system following restrictions and recommendations (*compliance policies*) defined by the Security Content Automation Protocol (SCAP) standard. This functionality is provided by an add-on which has been enabled by default since Red Hat Enterprise Linux 7.2. When enabled, the packages necessary to provide this functionality will automatically be installed. However, by default, no policies are enforced, meaning that no checks are performed during or after installation unless specifically configured.

The Red Hat Enterprise Linux 7 Security Guide provides detailed information about security compliance including background information, practical examples, and additional resources.

IMPORTANT

Applying a security policy is not necessary on all systems. This screen should only be used when a specific policy is mandated by your organization rules or governemnt regulations.

If you apply a security policy to the system, it will be installed using restrictions and recommendations defined in the selected profile. The openscap-scanner package will also be added to your package selection, providing a preinstalled tool for compliance and vulnerability scanning. After the installation finishes, the system will be automatically scanned to verify compliance. The results of this scan will be saved to the **`/root/openscap_data`** directory on the installed system.

Pre-defined policies which are available in this screen are provided by **SCAP Security Guide**. See the OpenSCAP Portal for links to detailed information about each available profile.

You can also load additional profiles from an HTTP, HTTPS or FTP server.

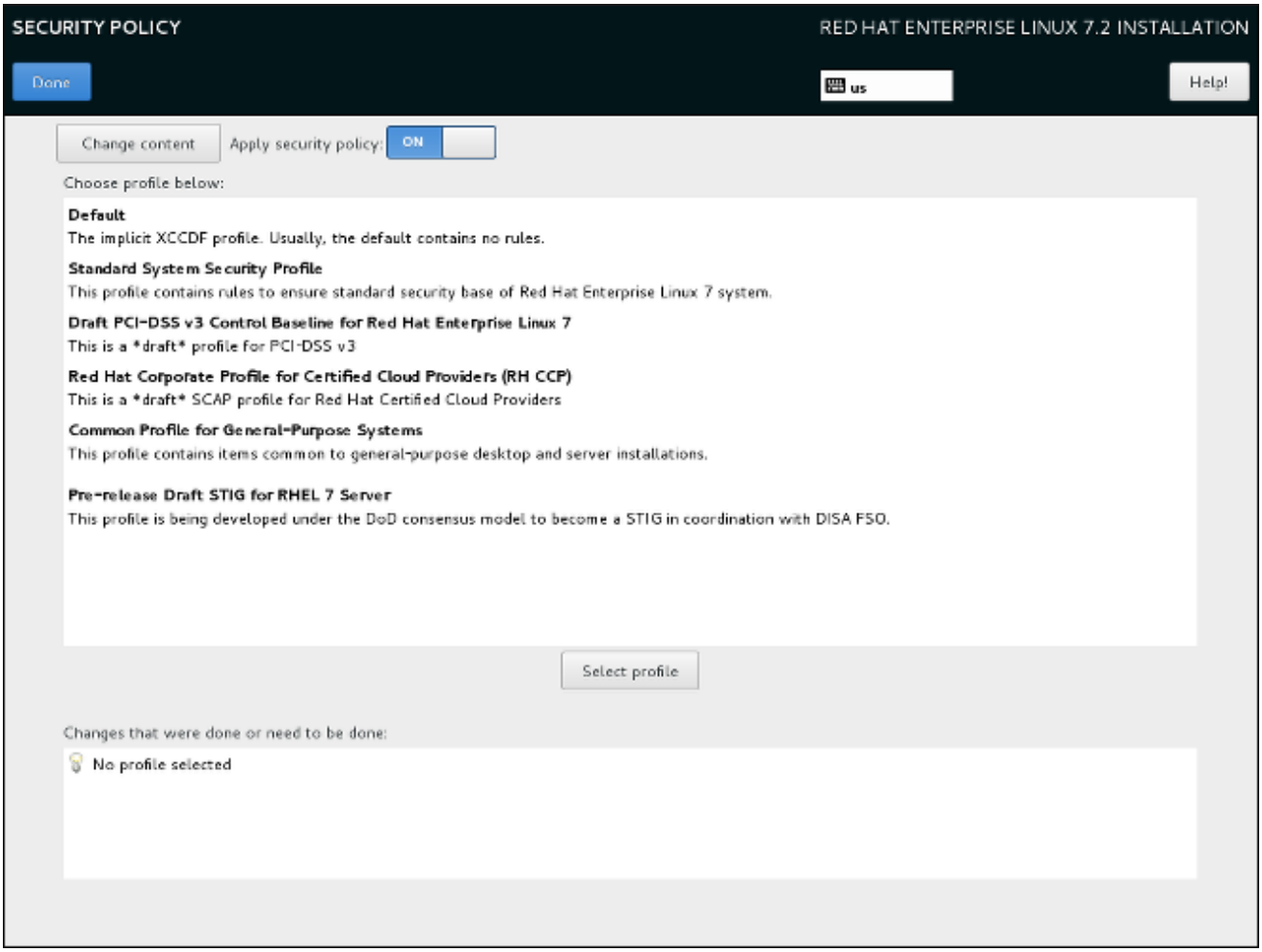
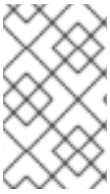


Figure 8.9. Security policy selection screen

To configure the use of security policies on the system, first enable configuration by setting the **Apply security policy** switch to **ON**. If the switch is in the **OFF** position, controls in the rest of this screen have no effect.

After enabling security policy configuration using the switch, select one of the profiles listed in the top window of the screen, and click the **Select profile** below. When a profile is selected, a green check mark will appear on the right side, and the bottom field will display whether any changes will be made before beginning the installation.



NOTE

None of the profiles available by default perform any changes before the installation begins. However, loading a custom profile as described below can require some pre-installation actions.

To use a custom profile, click the **Change content** button in the top left corner. This will open another screen where you can enter an URL of a valid security content. To go back to the default security content selection screen, click **Use SCAP Security Guide** in the top left corner.

Custom profiles can be loaded from an **HTTP**, **HTTPS** or **FTP** server. Use the full address of the content, including the protocol (such as **http://**). A network connection must be active (enabled in Section 8.12, “Network & Hostname”) before you can load a custom profile. The content type will be detected automatically by the installer.

After you select a profile, or if you want to leave the screen, click **Done** in the top left corner to return to

Section 8.6, “The Installation Summary Screen”.

8.11. INSTALLATION SOURCE

To specify a file or a location to install Red Hat Enterprise Linux from, select **Installation Source** from the **Installation Summary** screen. On this screen, you can choose between locally available installation media, such as a DVD or an ISO file, or a network location.

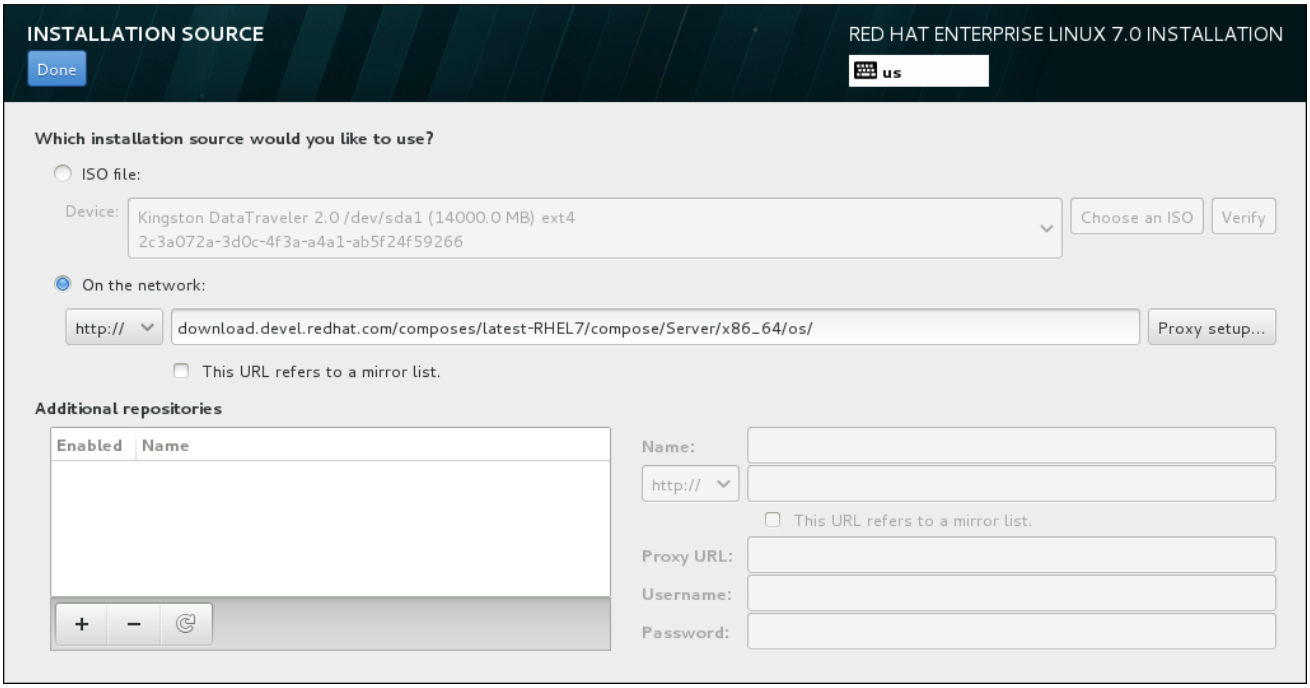


Figure 8.10. Installation Source Screen

Select one of the following options:

Auto-detected installation media

If you started the installation using the full installation DVD or USB drive, the installation program will detect it and display basic information under this option. Click the **Verify** button to ensure that the media is suitable for installation. This integrity test is the same as the one performed if you selected **Test this media & Install Red Hat Enterprise Linux** in the boot menu, or if you used the **rd.live.check** boot option.

ISO file

This option will appear if the installation program detected a partitioned hard drive with mountable file systems. Select this option, click the **Choose an ISO** button, and browse to the installation ISO file's location on your system. Then click **Verify** to ensure that the file is suitable for installation.

On the network

To specify a network location, select this option and choose from the following options in the drop-down menu:

- **http://**
- **https://**
- **ftp://**

- **nfs**

Using your selection as the start of the location URL, type the rest into the address box. If you choose NFS, another box will appear for you to specify any NFS mount options.

IMPORTANT

When selecting an NFS-based installation source, you must specify the address with a colon (**:**) character separating the host name from the path. For example:

```
server.example.com:/path/to/directory
```

To configure a proxy for an HTTP or HTTPS source, click the **Proxy setup** button. Check **Enable HTTP proxy** and type the URL into the **Proxy URL** box. If your proxy requires authentication, check **Use Authentication** and enter a user name and password. Click **Add**.

If your HTTP or HTTPS URL refers to a repository mirror list, mark the check box under the input field.

You can also specify additional repositories to gain access to more installation environments and software add-ons. See Section 8.13, “Software Selection” for more information.

To add a repository, click the **+** button. To delete a repository, click the **-** button. Click the arrow icon to revert to the previous list of repositories, that is, to replace current entries with those that were present at the time you entered the **Installation Source** screen. To activate or deactivate a repository, click the check box in the **Enabled** column at each entry in the list.

In the right part of the form, you can name your additional repository and configure it the same way as the primary repository on the network.

Once you have selected your installation source, click **Done** to return to the **Installation Summary** screen.

8.12. NETWORK & HOSTNAME

To configure essential networking features for your system, select **Network & Hostname** at the **Installation Summary** screen.

IMPORTANT

When the installation finishes and the system boots for the first time, any network interfaces which you configured during the installation will be activated. However, the installation does not prompt you to configure network interfaces on some common installation paths - for example, when you install Red Hat Enterprise Linux from a DVD to a local hard drive.

When you install Red Hat Enterprise Linux from a local installation source to a local storage device, be sure to configure at least one network interface manually if you require network access when the system boots for the first time. You will also need to set the connection to connect automatically after boot when editing the configuration.

Locally accessible interfaces are automatically detected by the installation program and cannot be

manually added or deleted. The detected interfaces are listed in the left pane. Click an interface in the list to display more details about in on the right. To activate or deactivate a network interface, move the switch in the top right corner of the screen to either **ON** or **OFF**.

NOTE

There are several types of network device naming standards used to identify network devices with persistent names such as **em1** or **wl3sp0**. For information about these standards, see the Red Hat Enterprise Linux 7 Networking Guide.

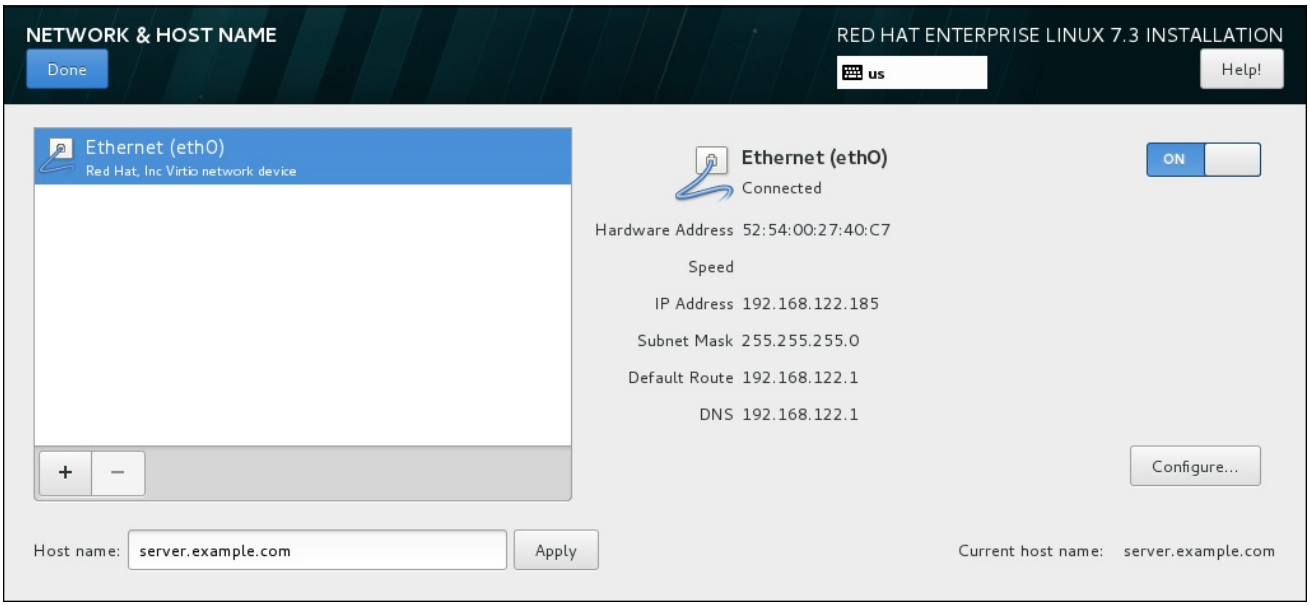


Figure 8.11. Network & Hostname Configuration Screen

Below the list of connections, enter a host name for this computer in the **Hostname** input field. The host name can be either a *fully-qualified domain name* (FQDN) in the format *hostname.domainname* or a *short host name* in the format *hostname*. Many networks have a *Dynamic Host Configuration Protocol* (DHCP) service that automatically supplies connected systems with a domain name. To allow the DHCP service to assign the domain name to this machine, only specify the short host name. The value **localhost.localdomain** means that no specific static host name for target system is configured, and the actual host name of installed system will be configured during process of network configuration (for example, by NetworkManager using DHCP or DNS).

IMPORTANT

If you want to manually assign the host name, make sure you do not use a domain name that is not delegated to you, as this can result in network resources becoming unavailable. For more information, see the recommended naming practices in the Red Hat Enterprise Linux 7 Networking Guide.

NOTE

You can use the **Network** section of the system **Settings** dialog to change your network configuration after you have completed the installation.

Once you have finished network configuration, click **Done** to return to the **Installation Summary** screen.

8.12.1. Edit Network Connections

This section only details the most important settings for a typical wired connection used during installation. Many of the available options do not have to be changed in most installation scenarios and are not carried over to the installed system. Configuration of other types of network is broadly similar, although the specific configuration parameters are necessarily different. To learn more about network configuration after installation, see the Red Hat Enterprise Linux 7 Networking Guide.

To configure a network connection manually, click the **Configure** button in the lower right corner of the screen. A dialog appears that allows you to configure the selected connection. The configuration options presented depends on whether the connection is wired, wireless, mobile broadband, VPN, or DSL. If required, see the *Networking Guide* for more detailed information on network settings.

The most useful network configuration options to consider during installation are:

- Mark the **Automatically connect to this network when it is available** check box if you want to use the connection every time the system boots. You can use more than one connection that will connect automatically. This setting will carry over to the installed system.

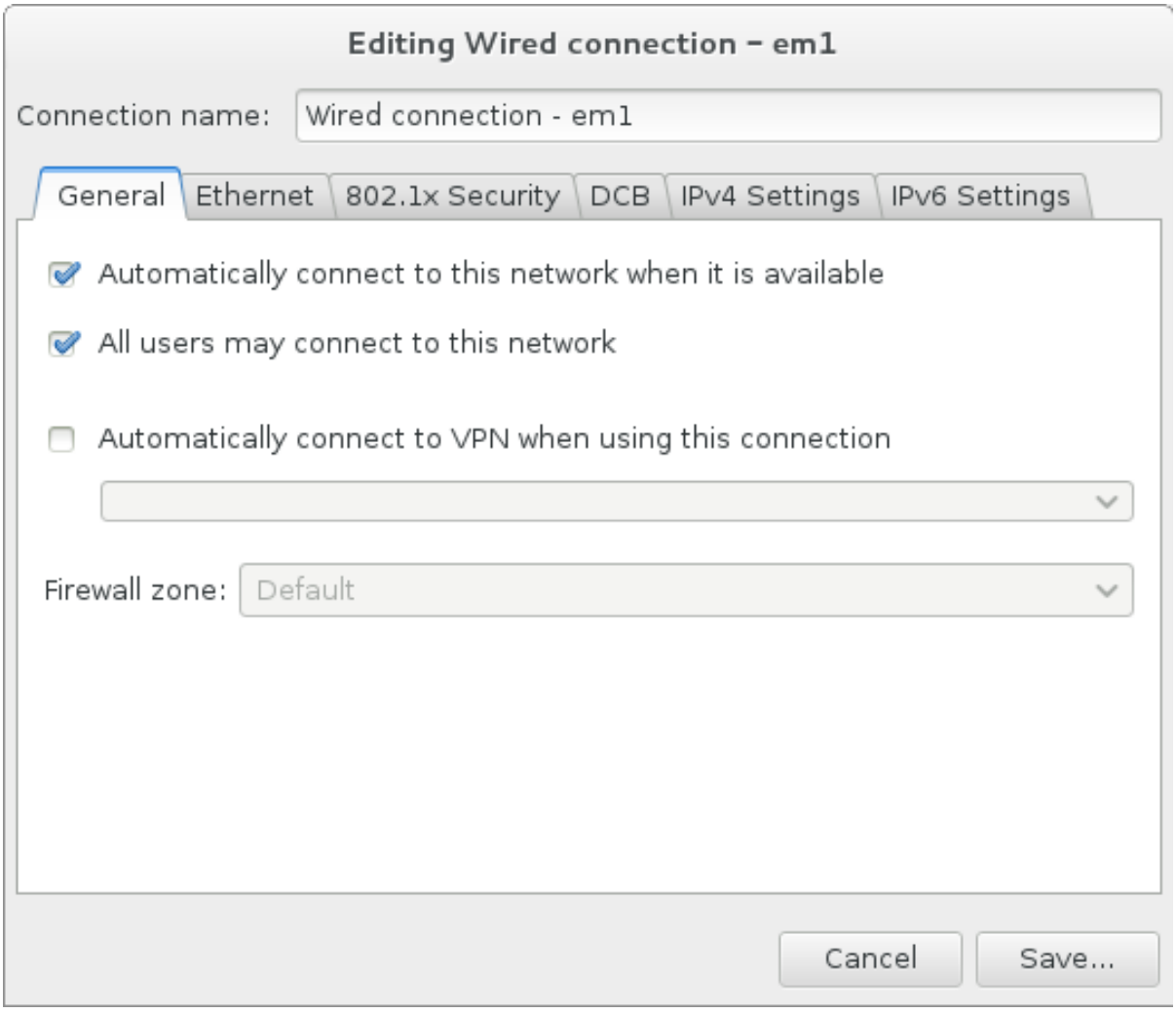


Figure 8.12. Network Auto-Connection Feature

- By default, IPv4 parameters are configured automatically by the DHCP service on the network. At the same time, the IPv6 configuration is set to the **Automatic** method. This combination is suitable for most installation scenarios and usually does not require any changes.

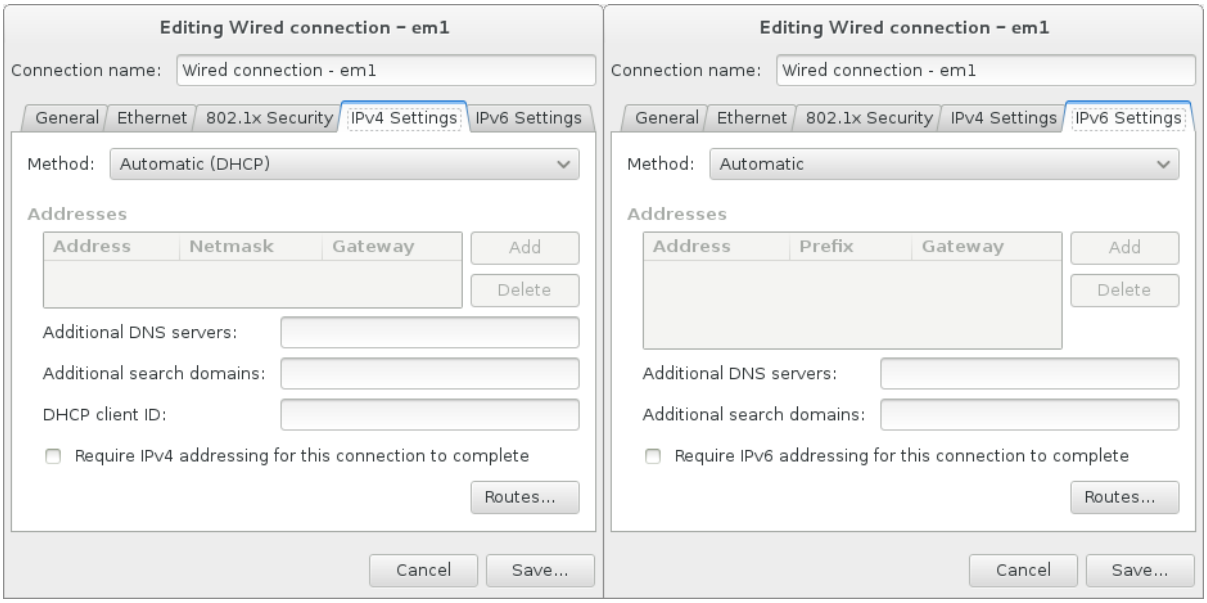


Figure 8.13. IP Protocol Settings

When you have finished editing network settings, click **Save** to save the new configuration. If you reconfigured a device that was already active during installation, you must restart the device in order to use the new configuration in the installation environment. Use the **ON/OFF** switch on the **Network & Host Name** screen to restart the device.

8.12.2. Advanced Network Interfaces

Advanced network interfaces are also available for installation. This includes virtual local area networks (VLANs) and three methods to use aggregated links. Detailed description of these interfaces is beyond the scope of this document; read the Red Hat Enterprise Linux 7 Networking Guide for more information.

To create an advanced network interface, click the **+** button in the lower left corner of the **Network & Hostname** screen.

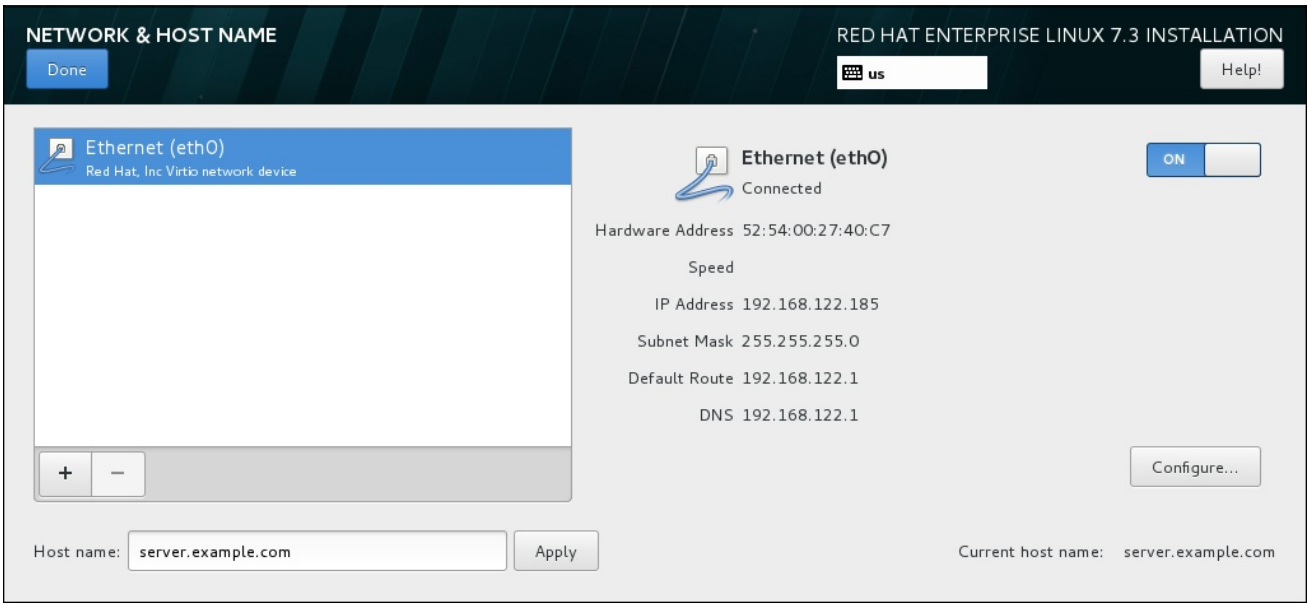


Figure 8.14. Network & Hostname Configuration Screen

A dialog appears with a drop-down menu with the following options:

- **Bond** - represents NIC (*Network Interface Controller*) Bonding, a method to bind multiple network interfaces together into a single, bonded, channel.
- **Bridge** - represents NIC Bridging, a method to connect multiple separate network into one aggregate network.
- **Team** - represents NIC Teaming, a new implementation to aggregate links, designed to provide a small kernel driver to implement the fast handling of packet flows, and various applications to do everything else in user space.
- **VLAN** - represents a method to create multiple distinct broadcast domains, which are mutually isolated.

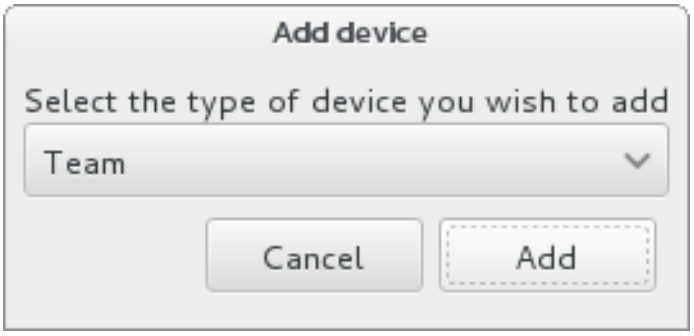
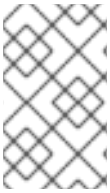


Figure 8.15. Advanced Network Interface Dialog



NOTE

Note that locally accessible interfaces, wired or wireless, are automatically detected by the installation program and cannot be manually added or deleted by using these controls.

Once you have selected an option and clicked the **Add** button, another dialog appears for you to configure the new interface. See the respective chapters in the Red Hat Enterprise Linux 7 Networking Guide for detailed instructions. To edit configuration on an existing advanced interface, click the **Configure** button in the lower right corner of the screen. You can also remove a manually-added interface by clicking the **-** button.

8.13. SOFTWARE SELECTION

To specify which packages will be installed, select **Software Selection** at the **Installation Summary** screen. The package groups are organized into *Base Environments*. These environments are pre-defined sets of packages with a specific purpose; for example, the **Virtualization Host** environment contains a set of software packages needed for running virtual machines on the system. Only one software environment can be selected at installation time.

For each environment, there are additional packages available in the form of *Add-ons*. Add-ons are presented in the right part of the screen and the list of them is refreshed when a new environment is selected. You can select multiple add-ons for your installation environment.

A horizontal line separates the list of add-ons into two areas:

- Add-ons listed *above* the horizontal line are specific to the environment you selected. If you select any add-ons in this part of the list and then select a different environment, your selection will be lost.

- Add-ons listed *below* the horizontal line are available for all environments. Selecting a different environment will not impact the selections made in this part of the list.

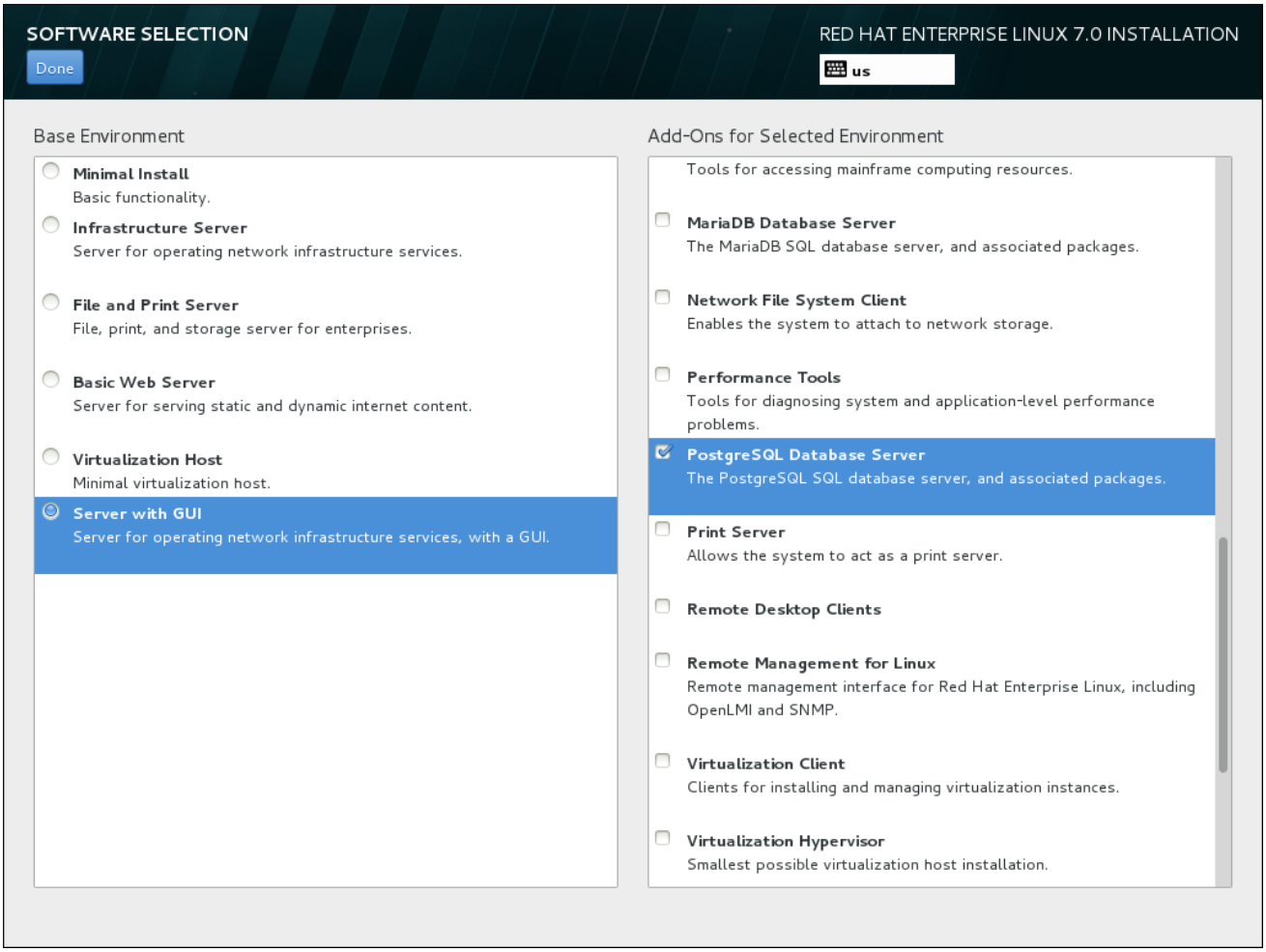


Figure 8.16. Example of a Software Selection for a Server Installation

The availability of base environments and add-ons depends on the variant of the installation ISO image which you are using as the installation source. For example, the **`server`** variant provides environments designed for servers, while the **`workstation`** variant has several choices for deployment as a developer workstation, and so on.

The installation program does not show which packages are contained in the available environments. To see which packages are contained in a specific environment or add-on, see the **`repodata/*-comps-`*`variant.architecture`*`.xml`** file on the Red Hat Enterprise Linux Installation DVD which you are using as the installation source. This file contains a structure describing available environments (marked by the **`<environment>`** tag) and add-ons (the **`<group>`** tag).

IMPORTANT

The pre-defined environments and add-ons allow you to customize your system, but in a manual installation, there is no way to select individual packages to install. If you are not sure what package should be installed, Red Hat recommends you to select the **Minimal Install** environment. **Minimal install** only installs a basic version of Red Hat Enterprise Linux with only a minimal amount of additional software. This will substantially reduce the chance of the system being affected by a vulnerability. After the system finishes installing and you log in for the first time, you can use the **Yum** package manager to install any additional software you need. For more details on **Minimal install**, see the Installing the Minimum Amount of Packages Required section of the Red Hat Enterprise Linux 7 Security Guide.

Alternatively, automating the installation with a Kickstart file allows for a much higher degree of control over installed packages. You can specify environments, groups and individual packages in the **%packages** section of the Kickstart file. See Section 26.3.2, “Package Selection” for instructions on selecting packages to install in a Kickstart file, and Chapter 26, *Kickstart Installations* for general information about automating the installation with Kickstart.

Once you have selected an environment and add-ons to be installed, click **Done** to return to the **Installation Summary** screen.

8.13.1. Core Network Services

All Red Hat Enterprise Linux installations include the following network services:

- centralized logging through the **rsyslog** service
- email through SMTP (Simple Mail Transfer Protocol)
- network file sharing through NFS (Network File System)
- remote access through SSH (Secure SHell)
- resource advertising through mDNS (multicast DNS)

Some automated processes on your Red Hat Enterprise Linux system use the email service to send reports and messages to the system administrator. By default, the email, logging, and printing services do not accept connections from other systems.

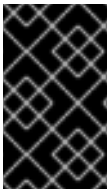
You can configure your Red Hat Enterprise Linux system after installation to offer email, file sharing, logging, printing, and remote desktop access services. The SSH service is enabled by default. You can also use NFS to access files on other systems without enabling the NFS sharing service.

8.14. INSTALLATION DESTINATION

To select the disks and partition the storage space on which you will install Red Hat Enterprise Linux, select **Installation Destination** in the **Installation Summary** screen. If you are unfamiliar with disk partitions, see Appendix A, *An Introduction to Disk Partitions* for more information.

WARNING

Red Hat recommends that you always back up any data that you have on your systems. For example, if you are upgrading or creating a dual-boot system, you should back up any data you want to keep on your storage devices. Unforeseen circumstances can result in loss of all your data.



IMPORTANT

If you install Red Hat Enterprise Linux in text mode, you can only use the default partitioning schemes described in this section. You cannot add or remove partitions or file systems beyond those that the installation program automatically adds or removes.

IMPORTANT

Special cases

- If you have a RAID card, be aware that some BIOS types do not support booting from the RAID card. In such a case, the **/boot** partition must be created on a partition outside of the RAID array, such as on a separate hard drive. It is necessary to use an internal hard drive for partition creation with problematic RAID cards. A **/boot** partition is also necessary for software RAID setups. If you have chosen to automatically partition your system, you should manually edit your **/boot** partition; see Section 8.14.4, “Manual Partitioning” for more details.

- To configure the Red Hat Enterprise Linux boot loader to *chain load* from a different boot loader, you must specify the boot drive manually by clicking the **Full disk summary and bootloader** link from the **Installation Destination** screen. See Section 8.14.1, “Boot Loader Installation” for instructions on specifying a boot drive.

- When you install Red Hat Enterprise Linux on a system with both multipath and non-multipath storage devices, the automatic partitioning layout in the installation program might create volume groups that contain a mix of multipath and non-multipath devices. This defeats the purpose of multipath storage. We advise that you select only multipath or only non-multipath devices on the **Installation Destination** screen. Alternatively, proceed to manual partitioning.

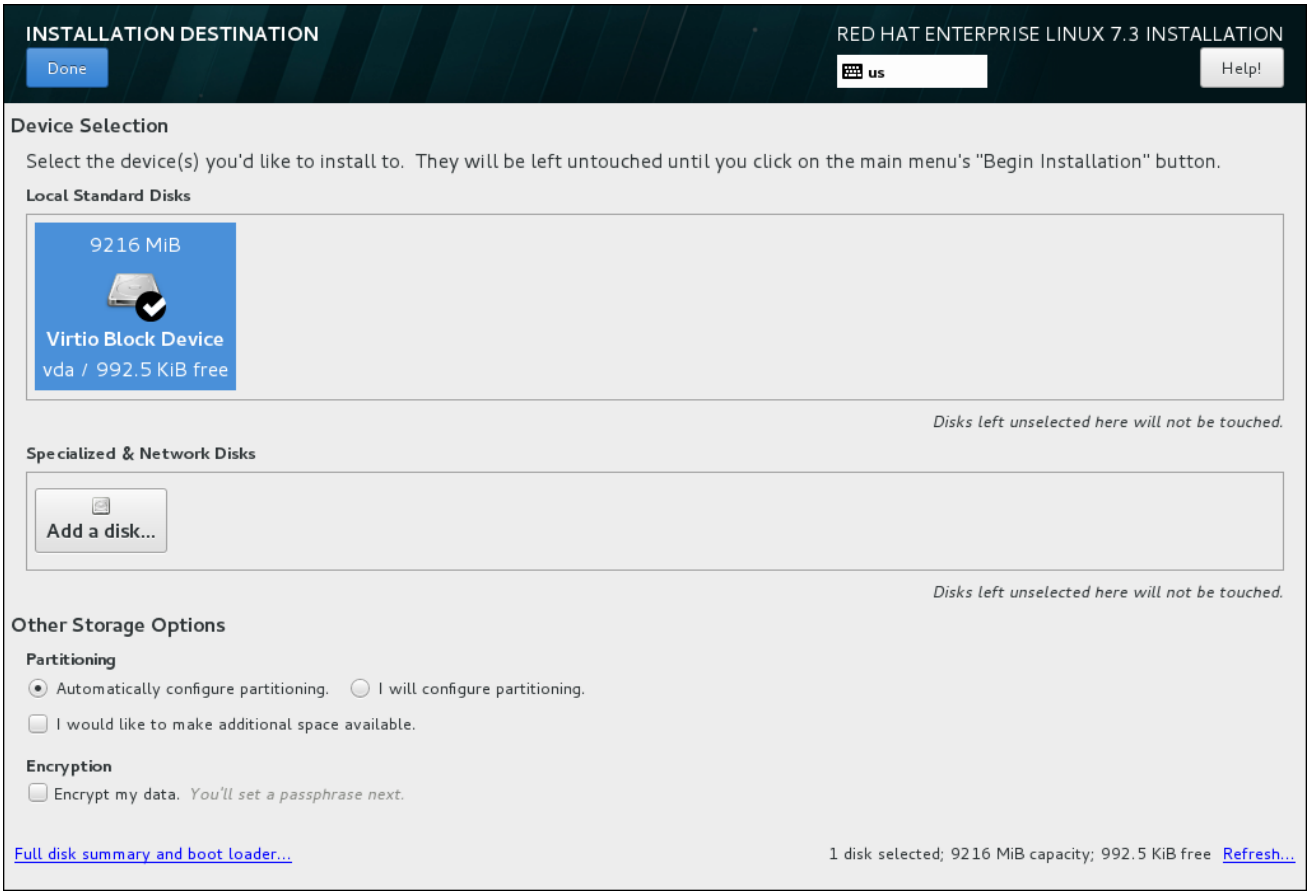


Figure 8.17. Storage Space Overview

On this screen, you can see storage devices available locally on your computer. You can also add additional specialized or network devices by clicking the **Add a disk** button. To learn more about these devices see Section 8.15, “Storage Devices”.

Choose the disks to install Red Hat Enterprise Linux on by clicking their icons in the pane at the top of the screen. Each disk is marked with its label, size, and available space. Disks left unselected on the screen will not be touched once the installation begins.

Below the panes for storage devices is a form of additional controls labeled **Other Storage Options**:

- In the **Partitioning** section, you can select how storage devices are partitioned and how volumes are created. You can configure the partitions, manually or allow the installation program to do it automatically.

  Automatic partitioning is recommended if you are doing a clean installation on previously unused storage or do not need to keep any data that might be present on the storage. To proceed this way, leave the default selection of the **Automatically configure partitioning** radio button, and the installation program will create the necessary partitions and volumes on the storage space for you.

  For automatic partitioning, you can also select the **I would like to make additional space available** check box to choose how to reassign space from other file systems to this installation. After you click **Done**, there are two dialogs that can appear. If you selected automatic partitioning but there is not enough storage space to complete the installation using the recommended partitioning configuration, a dialog will appear:

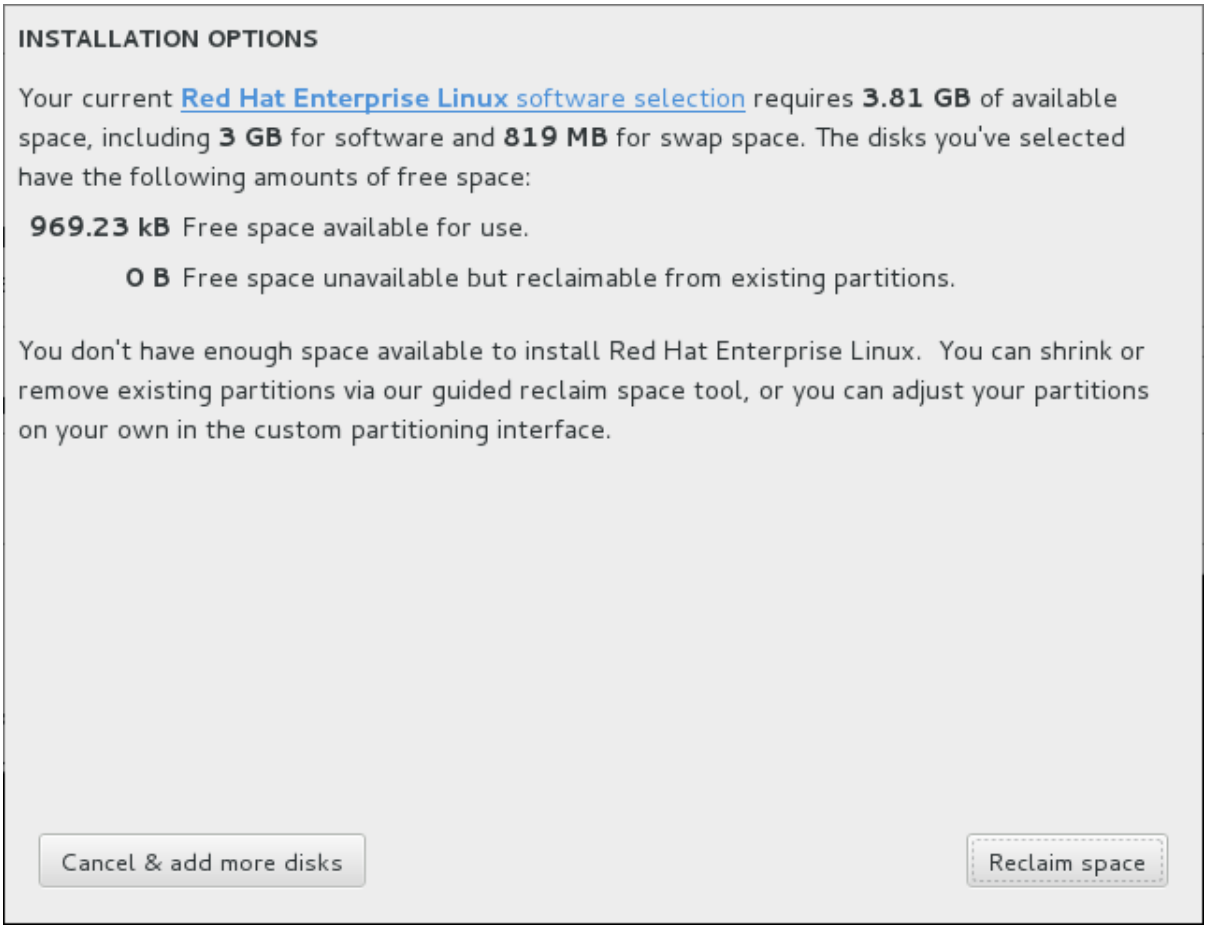


Figure 8.18. Installation Options Dialog with Option to Reclaim Space

You can click to the **Red Hat Enterprise Linux software selection** link. The link will navigate you to the **Software selection** section, where you can change what software you want to install, and free some aditional storage space.

Alternatively, you can click **Cancel & add more disks** to return to the **Installation Destination** screen, where it is possible to add more storage devices, or to choose to configure partitioning manually. Click **Reclaim space** to free some storage space from existing file systems. See Section 8.14.3, “Reclaim Disk Space” for details.

The second dialog appears if you cannot create enough free space. In this case, you have to add more disks on the initial storage screen or quit the installation.

If you select the **I will configure partitioning** radio button for manual setup, you will be brought to the **Manual Partitioning** screen after clicking **Done**. See Section 8.14.4, “Manual Partitioning” for details.

- In the **Encryption** section, you can select the **Encrypt my data** check box to encrypt all partitions except for the **/boot** partition. See the Red Hat Enterprise Linux 7 Security Guide for information on encryption.

At the bottom of the screen is the **Full disk summary and bootloader** button for you to configure a disk on which a boot loader will be installed.

See Section 8.14.1, “Boot Loader Installation” for more information.

Click the **Done** button once you have made your selections to either return to the **Installation Summary** screen or to proceed to the **Manual Partitioning** screen.

8.14.1. Boot Loader Installation

Red Hat Enterprise Linux uses GRUB2 (GRand Unified Bootloader version 2) as its boot loader. The boot loader is the first program that runs when the computer starts and is responsible for loading and transferring control to an operating system. GRUB2 can boot any compatible operating system and can also use *chain loading* to transfer control to other boot loaders for unsupported operating systems.

WARNING

Installing GRUB2 can overwrite your existing boot loader.

If you have other operating systems already installed, Red Hat Enterprise Linux attempts to automatically detect and configure GRUB2 to boot them. You can manually configure any additional operating systems if they are not detected properly.

To specify which device the boot loader should be installed on, click the **`Full disk summary and bootloader`** link at the bottom of the **`Installation Destination`** screen. The **`Selected Disks`** dialog will appear. If you are partitioning the drive manually, this dialog can be reached by clicking **`Storage device/s selected`** on the **`Manual Partitioning`** screen.

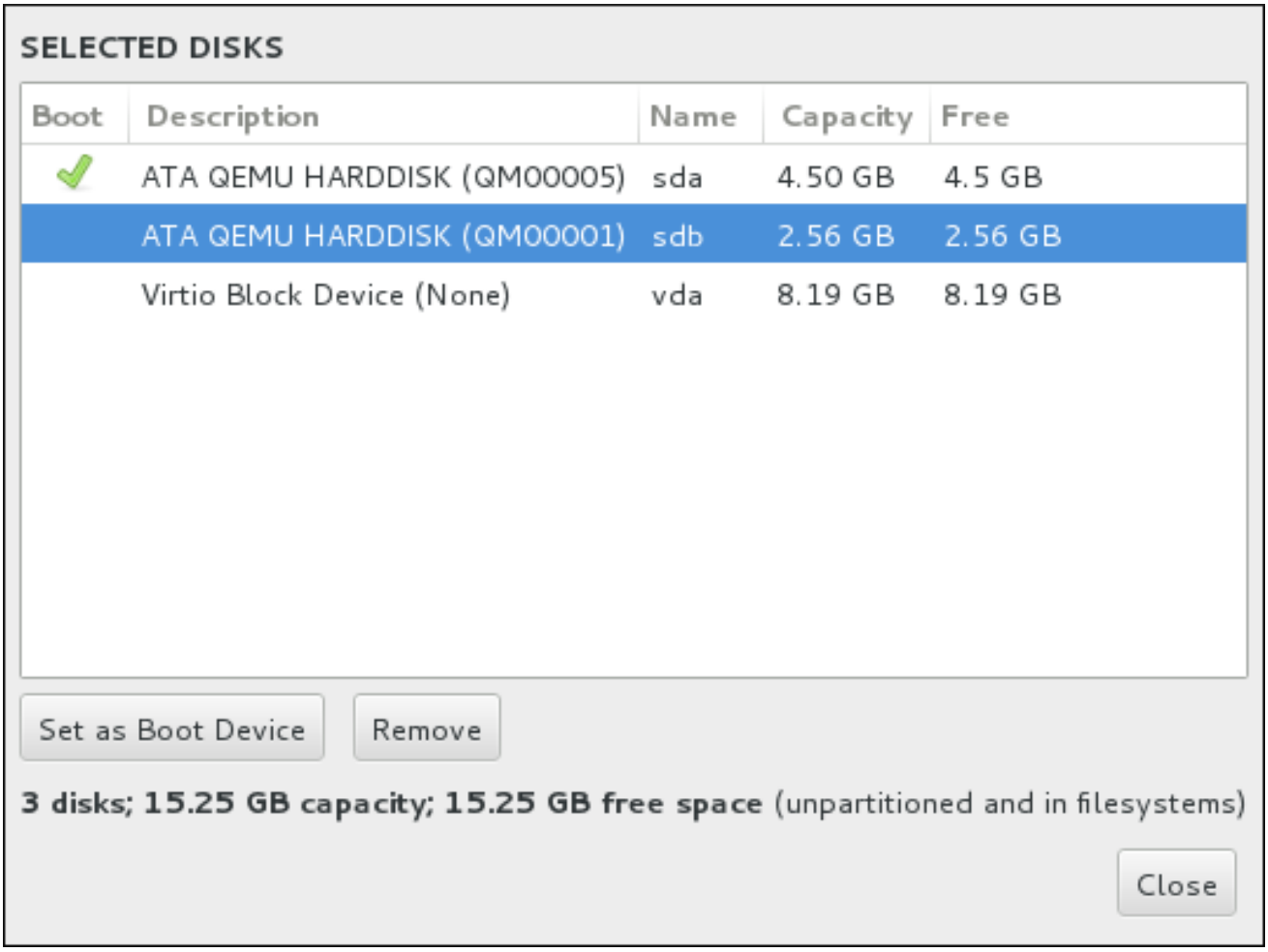


Figure 8.19. Summary of Selected Disks

In the **Boot** column, a green tick icon marks one of the devices as the intended boot device. To change the boot device, select a device from the list and click the **Set as Boot Device** button to install the boot loader there instead.

To decline installation of a new boot loader, select the marked device and click the **Do not install bootloader** button. This will remove the tick and ensure GRUB2 is not installed on any device.

WARNING

If you choose not to install a boot loader for any reason, you will not be able to boot the system directly, and you must use another boot method, such as a commercial boot loader application. Use this option only if you are sure you have another way to boot your system.

8.14.1.1. MBR and GPT Considerations

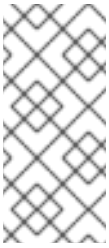
The installation program installs GRUB2 either in the *master boot record* (MBR) or the *GUID partition table* (GPT) of the device for the root file system. In order to determine which of these methods to use, the installation program considers the following variations:

BIOS systems, and UEFI systems in BIOS compatibility mode

If the disk is already formatted, the partitioning scheme is retained.

If the disk is not formatted, or the user erased all partitions from the disk, **Anaconda** will use:

- MBR if the disk has less than 2^{32} sectors. Most commonly, disks sectors are 512 bytes in size, in which case this would be equivalent to 2 TiB.
- GPT if the disk has 2^{32} sectors or more.



NOTE

Append the **inst.gpt** option to the boot command line to override the default behavior and use GPT on a disk of less than 2^{32} sectors in size. Note that you cannot manually override **Anaconda** to use MBR on a disk which is 2^{32} sectors in size or larger.

You need to create a BIOS Boot (*biosboot*) partition to install on a BIOS system where the disk containing the boot loader uses GPT. The **biosboot** partition should be 1 MiB in size. However, you do *not* need the **biosboot** partition if the disk containing the boot loader uses MBR.

UEFI systems

Only GPT is allowed on UEFI systems. In order to install on a formatted disk with a MBR, you must first reformat it.

You need to create an EFI System Partition (**/boot/efi**), regardless of the partitioning scheme. The **/boot/efi** partition should be at least 50 MiB in size; its recommended size is 200 MiB.

NOTE

Neither the **biosboot** nor **efi** partition can reside on an LVM volume. Use standard physical partitions for them.

8.14.2. Encrypt Partitions

If you selected the **Encrypt my data** option, when you click to proceed to the next screen the installation program will prompt you for a passphrase with which to encrypt the partitions on the system.

Partitions are encrypted using the *Linux Unified Key Setup* - see the Red Hat Enterprise Linux 7 Security Guide for more information.

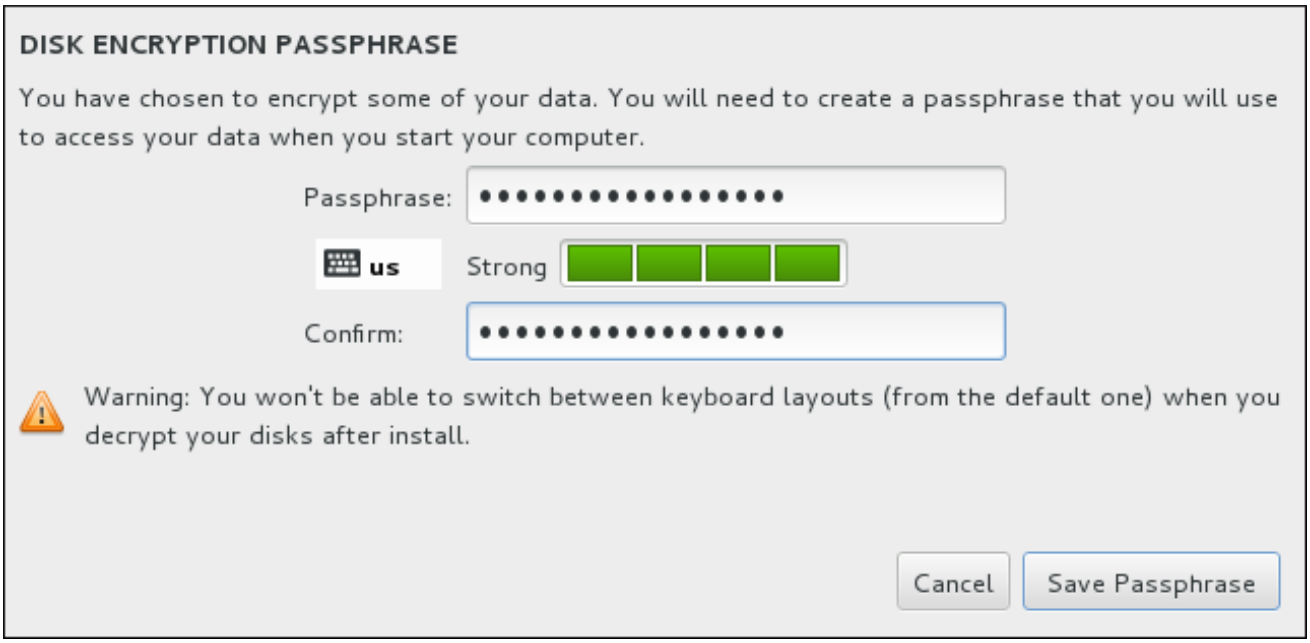


Figure 8.20. Enter Passphrase for an Encrypted Partition

Choose a passphrase and type it into each of the two fields in the dialog box. Note that you need to use the same keyboard layout for setting up this passphrase that you will use to unlock partitions later. Use the language layout icon to ensure the correct layout is selected. You must provide this passphrase every time that the system boots. Press **Tab** while in the **Passphrase** input field to retype it. If the passphrase is too weak, a warning icon appears in the field and you will not be allowed to type in the second field. Hover your mouse cursor over the warning icon to learn how to improve the passphrase.

WARNING

If you lose this passphrase, any encrypted partitions and the data on them will become completely inaccessible. There is no way to recover a lost passphrase.

Note that if you perform a Kickstart installation, you can save encryption passphrases and create backup encryption passphrases during installation. See the Red Hat Enterprise Linux 7 Security Guide for more information about disk encryption.

8.14.3. Reclaim Disk Space

If there is insufficient space to install Red Hat Enterprise Linux on the disks selected in **Installation Destination** and you selected **Reclaim Space** at the **Installation Options** dialog, the **Reclaim Disk Space** dialog appears.

WARNING

Unless you select to shrink a partition, reclaiming space on a partition involves deleting all the data on it and you should always verify that any data you need to keep was backed up.

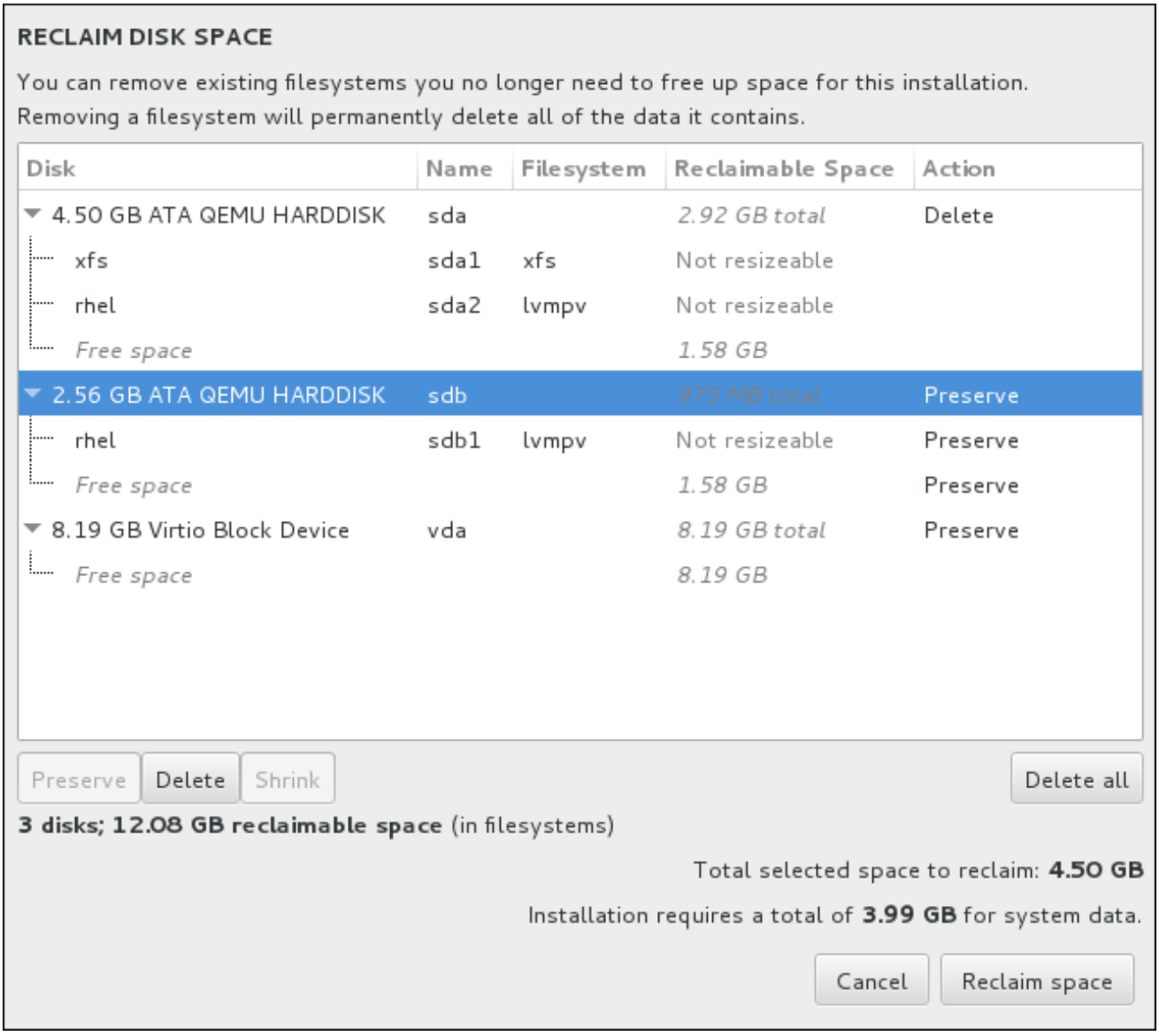


Figure 8.21. Reclaim Disk Space from Existing File Systems

The existing file systems Red Hat Enterprise Linux has detected are listed in a table as part of their respective disks. The **Reclaimable Space** column lists the space that could be reassigned to this installation. The **Action** column lists what action will be taken with the file system to reclaim space.

Beneath the table are four buttons:

- **Preserve** - leaves the file system untouched and no data will be deleted. This is the default action.
- **Delete** - removes the file system entirely. All the space it takes up on the disk will be made available for the installation.
- **Shrink** - recovers free space from the file system and makes it available for this installation. Use the slider to set a new size for the selected partition. Can only be used on resizable partitions where LVM or RAID is not used.
- **Delete all/Preserve all** - this button, located on the right, marks all file systems for deletion by default. Upon clicking, it changes the label and allows you to mark all file systems to be preserved again.

Select a file system or a whole disk in the table with your mouse and click one of the buttons. The label in the **Action** column will change to match your selection and the amount of **Total selected space to reclaim** displayed beneath the table will adjust accordingly. Beneath this value is the amount of space the installation requires based on the packages you have selected to install.

When enough space has been reclaimed for the installation to proceed, the **Reclaim Space** button will become available. Click this button to return to the Installation Summary screen and proceed with the installation.

8.14.4. Manual Partitioning

The **Manual Partitioning** screen is displayed when you click **Done** from Installation Destination if you selected the **I will configure partitioning** option. On this screen you configure your disk partitions and mount points. This defines the file system that Red Hat Enterprise Linux will be installed on.

WARNING

Red Hat recommends that you always back up any data that you have on your systems. For example, if you are upgrading or creating a dual-boot system, you should back up any data you want to keep on your storage devices. Unforeseen circumstances can result in loss of all your data.

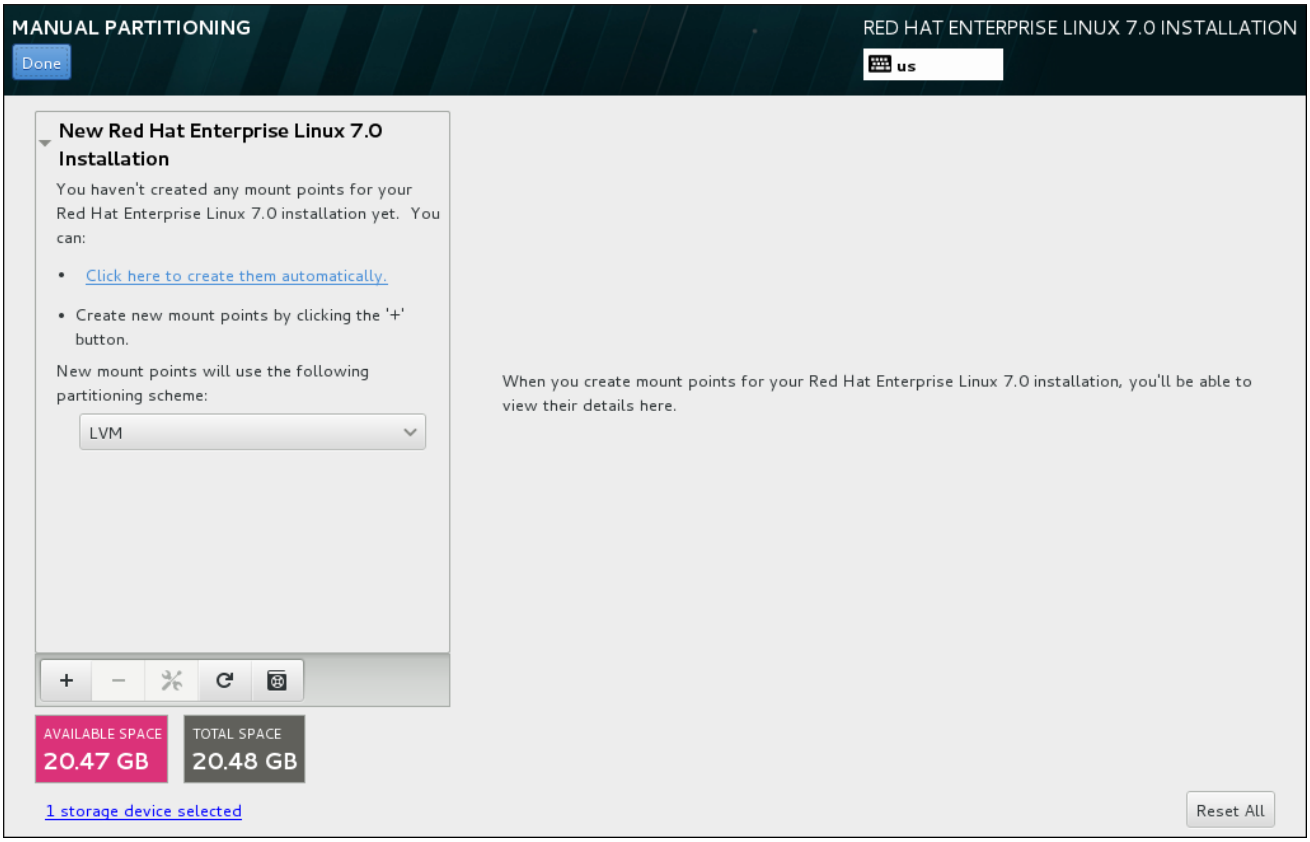


Figure 8.22. The Manual Partitioning Screen

The **`Manual Partitioning`** screen initially features a single pane on the left for the mount points. The pane is either empty except for information about creating mount points, or it displays existing mount points that the installation program has detected. These mount points are organized by detected operating system installations. Therefore, some file systems might be displayed multiple times if a partition is shared among several installations. The total space and available space on selected storage devices are displayed beneath this pane.

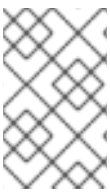
If your system contains existing file systems, ensure that enough space will be available for the installation. Use the `-` button to remove unneeded partitions.

NOTE

For recommendations and additional information about disk partitions, see Appendix A, *An Introduction to Disk Partitions* and Section 8.14.4.4, “Recommended Partitioning Scheme”. At a bare minimum, you need an appropriately sized root partition, and usually a swap partition appropriate to the amount of RAM you have on your system.

8.14.4.1. Adding File Systems and Configuring Partitions

An installation of Red Hat Enterprise Linux requires a minimum of one partition but Red Hat recommends using at least the following partitions or volumes: `/`, **`/home`**, **`/boot`**, and **`swap`**. You can also create additional partitions and volumes as you require. See Section 8.14.4.4, “Recommended Partitioning Scheme” for further details.



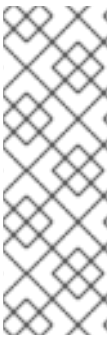
NOTE

If you have any specific requirements for some partitions (for example, requiring that a particular partition be on a specific disk) and less specific requirements for other partitions, create the partitions first which have more specific requirements.

Adding a file system is a two-step process. You first create a mount point in a certain partitioning scheme. The mount point appears in the left pane. Next, you can customize it using the options in the right pane, where you can change the mount point, capacity, the device type, file system type, label, and whether to encrypt or reformat the corresponding partition.

If you have no existing file systems and want the installation program to create the required file systems and their mount points for you, select your preferred partitioning scheme from the drop-down menu in the left pane (default for Red Hat Enterprise Linux is LVM), then click the link on top of the pane for creating mount points automatically. This will generate a **/boot** partition, a **/** (root) volume, and a swap volume proportionate to the size of the available storage. These are the recommended file systems for a typical installation, but you can add additional file systems and mount points if you need to.

Alternatively, create individual mount points using the **+** button at the bottom of the pane. The **Add a New Mount Point** dialog then opens. Either select one of the preset paths from the **Mount Point** drop-down menu or type your own; for example, select **/** for the root partition or **/boot** for the boot partition. Then enter the size of the file system in the **Desired Capacity** text field; for example, **2GiB**. If you leave the field empty or if you specify a size bigger than available space, all remaining free space is used instead. After entering these details, click the **Add mount point** button to create the partition.



NOTE

To avoid problems with space allocation, first create small partitions with known fixed sizes, such as **/boot**, and then create the rest of the partitions, letting the installation program allocate the remaining capacity to them.

Similarly, if you have multiple disks that the system is to reside on, they differ in size, and a particular partition must be created on the first disk detected by BIOS, be sure to start by creating such a partition.

For each new mount point you create manually, you can set its partitioning scheme from the drop-down menu located in the left pane. The available options are **Standard Partition**, **BTRFS**, **LVM**, and **LVM Thin Provisioning**. Note that the **/boot** partition will always be located on a standard partition, regardless of the value selected in this menu.

To change on which devices a single non-LVM mount point should be located, select the mount point and click the **Modify...** button in the right pane to open the **Configure Mount Point** dialog. Select one or more devices and click **Select**. After the dialog closes, note that you also need to confirm this setting by clicking the **Update Settings** button on the right side of the **Manual Partitioning** screen.

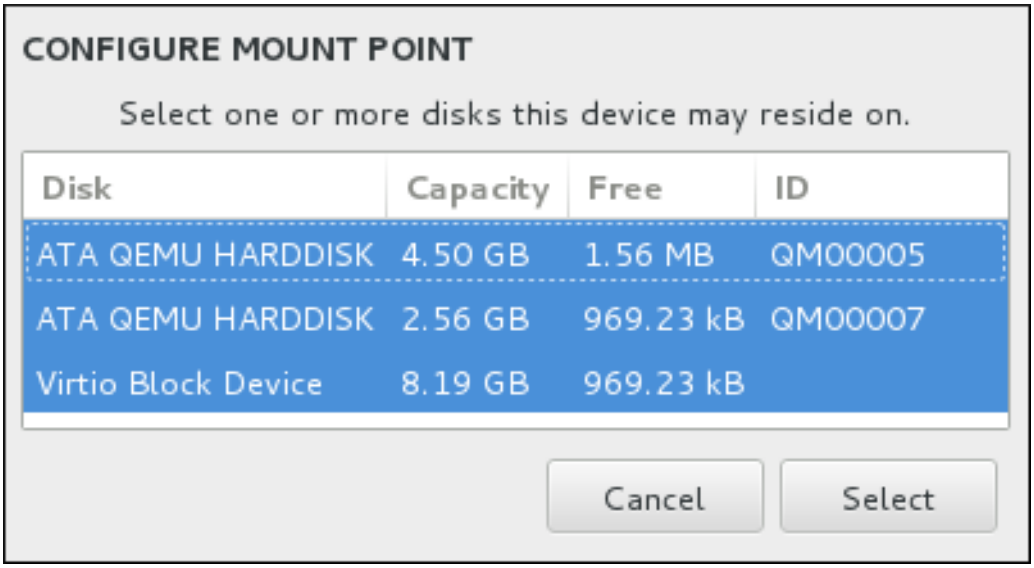


Figure 8.23. Configuring Mount Points

To refresh information about all local disks and partitions on them, click the **Rescan** button (with the circular arrow icon on it) in the toolbar. You only need to do this action after performing advanced partition configuration outside the installation program. Note that if you click the **Rescan Disks** button, all configuration changes you previously made in the installation program will be lost.

Figure 8.24. Rescanning Disks

At the bottom of the screen, a link states how many storage devices have been selected in **Installation Destination** (see Section 8.14, “Installation Destination”). Clicking on this link opens the **Selected Disks** dialog, where you review the information about the disks. See Section 8.14.1, “Boot Loader Installation” for more information.

To customize a partition or a volume, select its mount point in the left pane and the following customizable features then appear to the right:

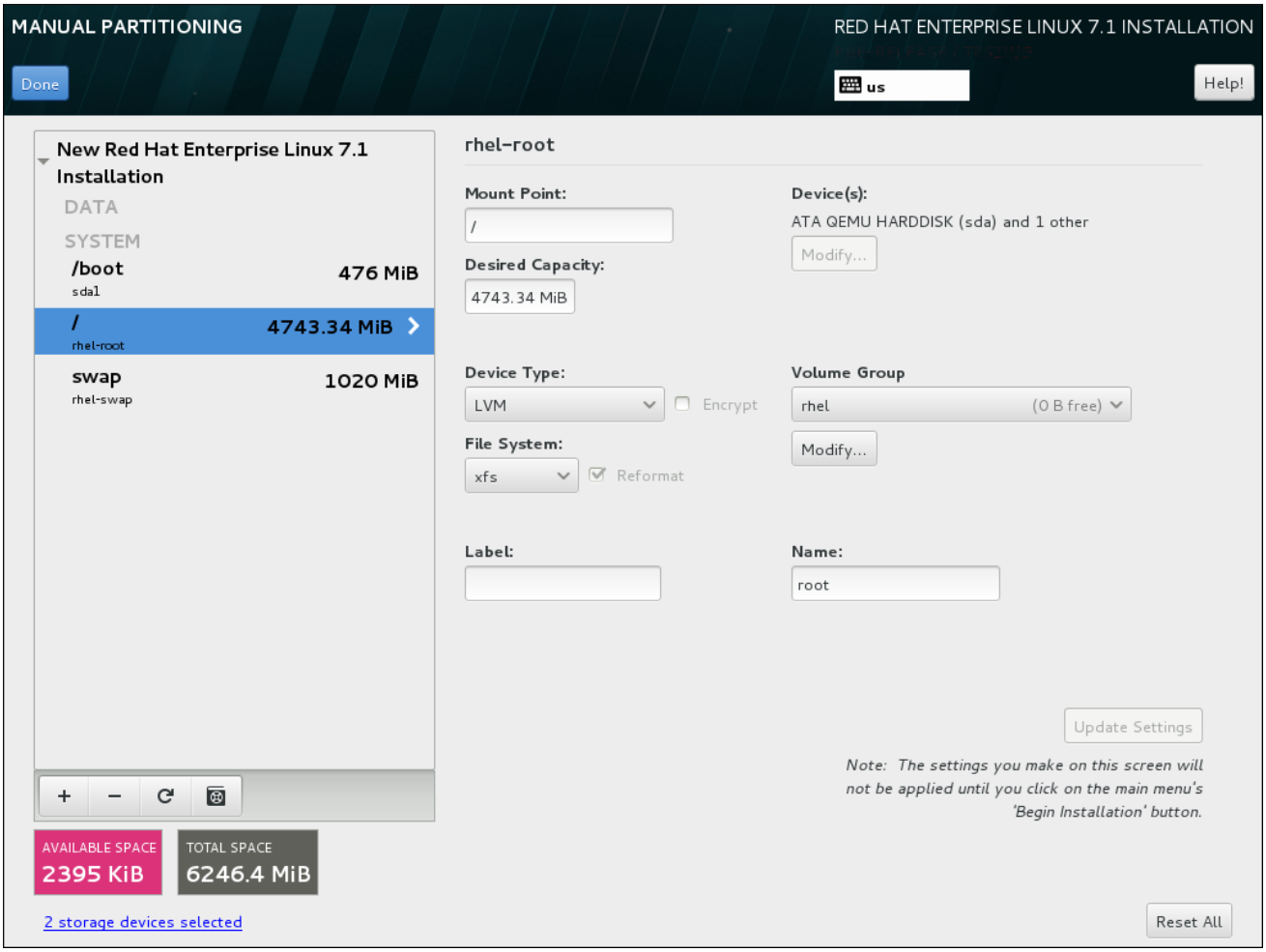


Figure 8.25. Customizing Partitions

- **Mount Point** - enter the file system's mount point. For example, if a file system should be the root file system, enter **/**; enter **/boot** for the **/boot** file system, and so on. For a swap file system, the mount point should not be set - setting the file system type to **swap** is sufficient.

- **Desired Capacity** - enter the desired size of the file system. You can use common size units such as KiB or GiB. The default is MiB if no other unit is specified.

- **Device type** - choose one of these types: **Standard Partition**, **LVM**, **RAID**, **LVM Thin Provisioning**, or **BTRFS**. Check the adjacent **Encrypt** box to encrypt the partition or volume. You will be prompted to set a password later. **RAID** is only available if two or more disks are selected for partitioning, and if you choose this type, you can also set the **RAID Level**. Similarly, if you select **LVM**, you can specify the **Volume Group**.

- **File system** - in the drop-down menu, select the appropriate file system type for this partition or volume. Check the adjacent **Reformat** box to format an existing partition, or leave it unchecked to retain your data. Note that newly created partitions and volumes must be reformatted, and the check box cannot be unchecked in this case.

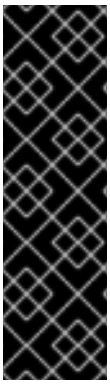
- **Label** - assign a label to the partition. Labels are used for you to easily recognize and address individual partitions.

- **Name** - assign a name to an LVM or Btrfs volume. Note that standard partitions are named automatically when they are created and their name cannot be edited, such as **/home** being assigned the name **sda1**.

See Section 8.14.4.1.1, “File System Types” for more information about file system and device types.

Click the **Update Settings** button to save your changes and select another partition to customize. Note that the changes will not be applied until you actually start the installation from the Installation summary page. Click the **Reset All** button to discard all changes to all partitions and start over.

When all file systems and mount points have been created and customized, click the **Done** button. If you chose to encrypt any file system, you will now be prompted to create a passphrase. Then, a dialog appears, showing a summary of all actions related to storage that the installation program will take. This includes creating, resizing, or deleting partitions and file systems. You can review all the changes and click **Cancel & Return to Custom Partitioning** to go back. To confirm your changes, click **Accept Changes** to return to the Installation Summary page. To partition additional devices, select them in the **Installation Destination** screen, return to the **Manual Partitioning** screen, repeat the steps outlined in this section for the additional devices.



IMPORTANT

If **/usr** or **/var** is partitioned separately from the rest of the root volume, the boot process becomes much more complex because these directories contain components critical to it. In some situations, such as when these directories are placed on an iSCSI drive or an FCoE location, the system can either be unable to boot, or hang with a **Device is busy** error when powering off or rebooting.

This limitation only applies to **/usr** or **/var**, not to directories below them. For example, a separate partition for **/var/www** will work without issues.

8.14.4.1.1. File System Types

Red Hat Enterprise Linux allows you to create different device types and file systems. The following is a brief description of the different device types and file systems available, and how they can be used.

Device Types

- **standard partition** - A standard partition can contain a file system or swap space, or it can provide a container for software RAID or an LVM physical volume.
- **logical volume (LVM)** - Creating an LVM partition automatically generates an LVM logical volume. LVM can improve performance when using physical disks. For information on how to create a logical volume, see Section 8.14.4.3, “Create LVM Logical Volume”. For more information regarding LVM, see the Red Hat Enterprise Linux 7 Logical Volume Manager Administration guide.
- **LVM thin provisioning** - Using thin provisioning, you can manage a storage pool of free space, known as a thin pool, which can be allocated to an arbitrary number of devices when needed by applications. The thin pool can be expanded dynamically when needed for cost-effective allocation of storage space. For more information regarding LVM, see the Red Hat Enterprise Linux 7 Logical Volume Manager Administration guide.

NOTE

The installer will automatically reserve 20% of any requested space for an LVM thin pool logical volume in the volume group containing it. This is a safety measure to ensure that you can extend either the metadata volume or the data volume of your thinly provisioned logical volume.

- **`software RAID`** - Creating two or more software RAID partitions allows you to create a RAID device. One RAID partition is assigned to each disk on the system. To create a RAID device, see Section 8.14.4.2, “Create Software RAID”. For more information regarding RAID, see the Red Hat Enterprise Linux 7 Storage Administration Guide.

File Systems

- **`xfs`** - XFS is a highly scalable, high-performance file system that supports file systems up to 16 EiB (approximately 16 billion GiB), files up to 8 EiB (approximately 8 billion GiB), and directory structures containing tens of millions of entries. XFS supports metadata journaling, which facilitates quicker crash recovery. The XFS file system can also be defragmented and resized while mounted and active. This file system is selected by default and is highly recommended. For information on how to translate common commands from previously used ext4 file system to XFS, see Appendix E, *Reference Table for ext4 and XFS Commands*.

  The maximum supported size of an XFS file system in Red Hat Enterprise Linux is currently *500 TiB*.

- **`ext4`** - The ext4 file system is based on the ext3 file system and features a number of improvements. These include support for larger file systems and larger files, faster and more efficient allocation of disk space, no limit on the number of subdirectories within a directory, faster file system checking, and more robust journaling.

  The maximum supported size of an ext4 file system in Red Hat Enterprise Linux is currently *50 TiB*.

- **`ext3`** - The ext3 file system is based on the ext2 file system and has one main advantage - journaling. Using a journaling file system reduces time spent recovering a file system after a crash as there is no need to check the file system for metadata consistency by running the **`fsck`** utility every time a crash occurs.

- **`ext2`** - An ext2 file system supports standard Unix file types, including regular files, directories, or symbolic links. It provides the ability to assign long file names, up to 255 characters.

- **`vfat`** - The VFAT file system is a Linux file system that is compatible with Microsoft Windows long file names on the FAT file system.

- **`swap`** - Swap partitions are used to support virtual memory. In other words, data is written to a swap partition when there is not enough RAM to store the data your system is processing.

- **`BIOS Boot`** - A very small partition required for booting a device with a GUID partition table (GPT) on a BIOS system. See Section 8.14.1, “Boot Loader Installation” for details.

- **`EFI System Partition`** - A small partition required for booting a device with a GUID partition table (GPT) on a UEFI system. See Section 8.14.1, “Boot Loader Installation” for details.

Each file system has different size limits for the file system itself as well as individual files contained within. For a list of maximum supported file and file system sizes, see the Red Hat Enterprise Linux technology capabilities and limits page, available on the Customer Portal at https://access.redhat.com/site/articles/rhel-limits.

8.14.4.2. Create Software RAID

Redundant arrays of independent disks (RAIDs) are constructed from multiple storage devices that are arranged to provide increased performance and, in some configurations, greater fault tolerance. See below for a description of different kinds of RAIDs.

A RAID device is created in one step and disks are added or removed as necessary. One RAID partition per physical disk is allowed for each device, so the number of disks available to the installation program determines which levels of RAID device are available to you. For example, if your system has two hard drives, the installation program will not allow you to create a RAID10 device, which requires 4 separate partitions.

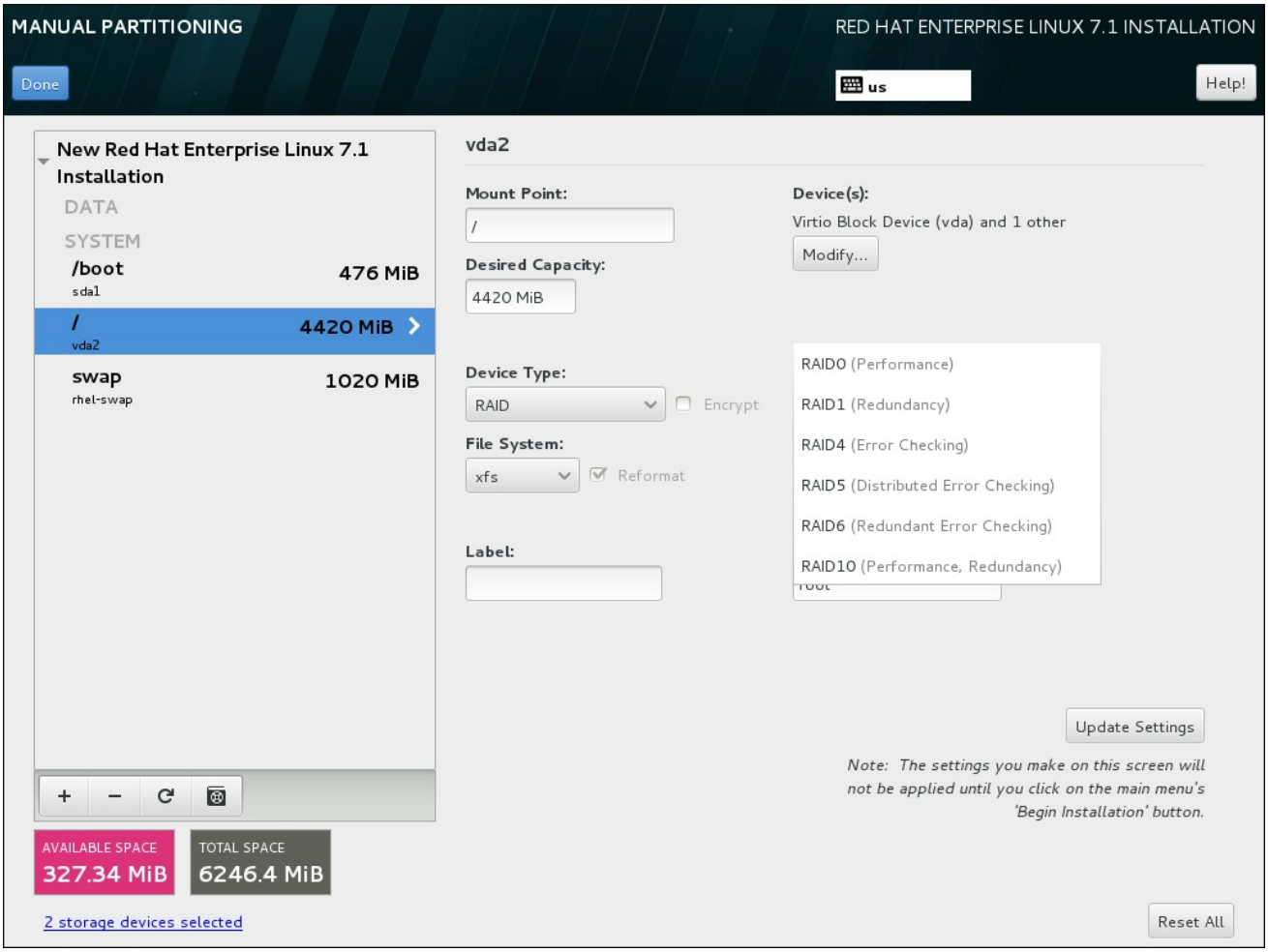


Figure 8.26. Creating a Software RAID Partition - the `Device Type` Menu Expanded

RAID configuration options are only visible if you have selected two or more disks for installation. At least two disks are required to create a RAID device.

To create a RAID device:

1. Create a mount point as described in Section 8.14.4.1, “Adding File Systems and Configuring Partitions”. By configuring this mount point, you configure the RAID device.

2. Keeping the partition selected in the left pane, select the configuration button below the pane to open the **`Configure Mount Point`** dialog. Select which disks will be included in the RAID device and click **`Select`**.

3. Click the **`Device Type`** drop-down menu and select **`RAID`**.

4. Click the **`File System`** drop-down menu and select your preferred file system type (see Section 8.14.4.1.1, “File System Types”.

5. Click the **`RAID Level`** drop-down menu and select your preferred level of RAID.

   The available RAID levels are:

RAID0 - `Optimized performance (stripe)`

Distributes data across multiple disks. Level 0 RAIDs offer increased performance over standard partitions, and can be used to pool the storage of multiple disks into one large virtual device. Note that Level 0 RAIDs offer no redundancy, and that the failure of one device in the array destroys data in the entire array. RAID 0 requires at least two RAID partitions.

RAID1 - `Redundancy (mirror)`

Mirrors all data on one disk onto one or more other disks. Additional devices in the array provide increasing levels of redundancy. RAID 1 requires at least two RAID partitions.

RAID4 - `Error detection (parity)`

Distributes data across multiple disks, and uses one disk in the array to store parity information that safeguards the array in case any disk within the array fails. Because all parity information is stored on one disk, access to this disk creates a bottleneck in the performance of the array. RAID 4 requires at least three RAID partitions.

RAID5 - `Distributed error detection`

Distributes data *and* parity information across multiple disks. Level 5 RAIDs therefore offer the performance advantages of distributing data across multiple disks, but do not share the performance bottleneck of level 4 RAIDs because the parity information is also distributed through the array. RAID 5 requires at least three RAID partitions.

RAID6 - `Redundant`

Level 6 RAIDs are similar to level 5 RAIDs, but instead of storing only one set of parity data, they store two sets. RAID 6 requires at least four RAID partitions.

RAID10 - `Redundancy (mirror)` and `Optimized performance (stripe)`

Level 10 RAIDs are *nested RAIDs* or *hybrid RAIDs*. They are constructed by distributing data over mirrored sets of disks. For example, a level 10 RAID array constructed from four RAID partitions consists of two mirrored pairs of striped partitions. RAID 10 requires at least four RAID partitions.

6. Click **`Update Settings`** to save your changes, and either continue with another partition or click **`Done`** to return to the **`Installation Summary`** screen.

If fewer disks are included than the specified RAID level requires, a message will be displayed at the bottom of the window, informing you how many disks are actually required for your selected configuration.

8.14.4.3. Create LVM Logical Volume

Logical Volume Management (LVM) presents a simple logical view of underlying physical storage space, such as hard drives or LUNs. Partitions on physical storage are represented as *physical volumes* that can be grouped together into *volume groups*. Each volume group can be divided into multiple *logical volumes*, each of which is analogous to a standard disk partition. Therefore, LVM logical volumes function as partitions that can span multiple physical disks.

To learn more about LVM, see Appendix C, *Understanding LVM* or read the Red Hat Enterprise Linux 7 Logical Volume Manager Administration guide. Note that LVM configuration is only available in the graphical installation program.

IMPORTANT

During text-mode installation, LVM configuration is not available. If you need to create an LVM configuration from scratch, press **Ctrl+Alt+F2** to use a different virtual console, and run the **lvm** command. To return to the text-mode installation, press **Ctrl+Alt+F1**.

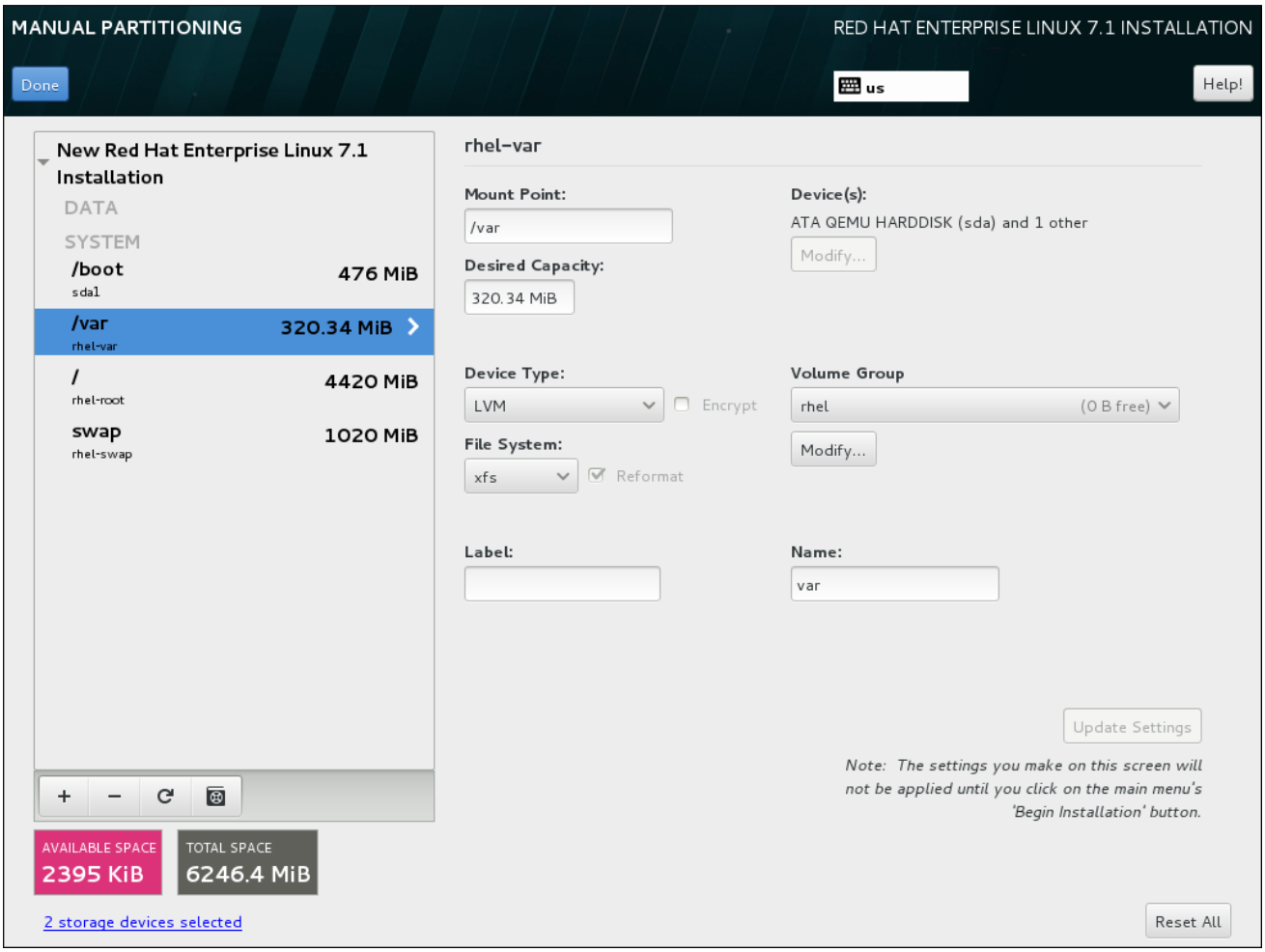


Figure 8.27. Configuring a Logical Volume

To create a logical volume and add it to a new or existing volume group:

1. Create a mount point for the LVM volume as described in Section 8.14.4.1, “Adding File Systems and Configuring Partitions”.

2. Click the **Device Type** drop-down menu and select **LVM**. The **Volume Group** drop-down menu appears and displays the newly-created volume group name.

3. Optionally, either click the menu and select **Create a new volume group** or click **Modify** to configure the newly-created volume group, if you need to. Both the **Create a new volume group** option and the **Modify** button lead to the **Configure Volume Group** dialog, where you can rename the logical volume group and select which disks will be included.

NOTE

The configuration dialog does not allow you to specify the size of the volume group's physical extents. The size will always be set to the default value of 4 MiB. If you want to create a volume group with different physical extents, create it manually by switching to an interactive shell and using the **vgcreate** command, or use a Kickstart file with the **volgroup --pesize=*size*** command.

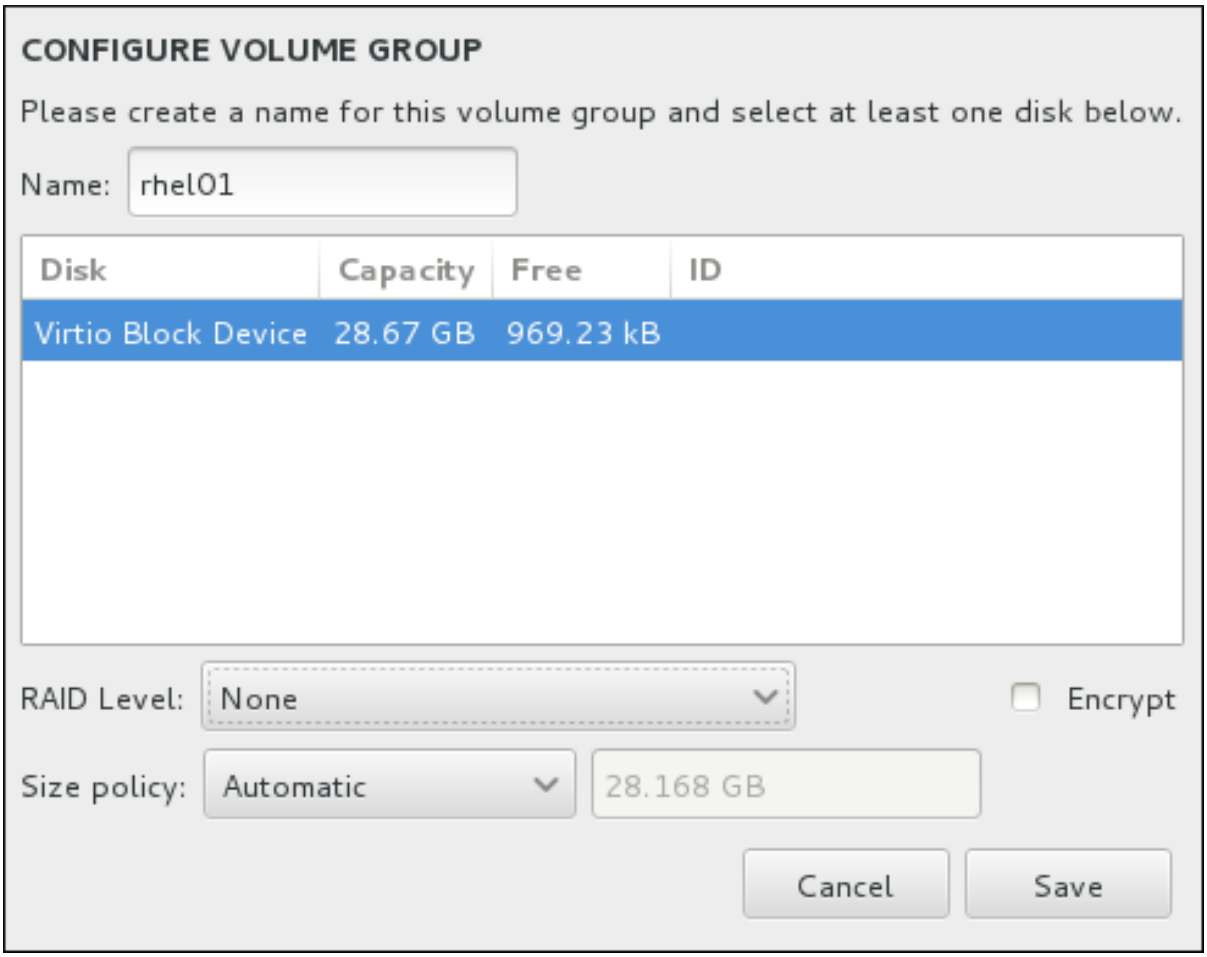


Figure 8.28. Customizing an LVM Volume Group

The available RAID levels are the same as with actual RAID devices. See Section 8.14.4.2, “Create Software RAID” for more information. You can also mark the volume group for encryption and set the size policy for it. The available policy options are:

- **Automatic** - the size of the volume group is set automatically so that it is just large enough to contain the configured logical volumes. This is optimal if you do not need free space within the volume group.
- **As large as possible** - the volume group is created with maximum size, regardless of the size of the configured logical volumes it contains. This is optimal if you plan to keep most of your data on LVM and later need to increase the size of some existing logical volumes, or if you need to create additional logical volumes within this group.
- **Fixed** - with this option, you can set an exact size of the volume group. Any configured logical volumes must then fit within this fixed size. This is useful if you know exactly how large you would like the volume group to be.

Click **Save** when the group is configured.

4. Click **Update Settings** to save your changes, and either continue with another partition or click **Done** to return to the **Installation Summary** screen.

WARNING

Placing the **/boot** partition on an LVM volume is not supported.

8.14.4.4. Recommended Partitioning Scheme

Red Hat recommends that you create separate file systems at the following mount points on AMD64 and Intel 64 systems:

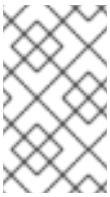
- **/boot**
- **/** (root)
- **/home**
- **swap**

/boot partition - recommended size at least 1 GiB

The partition mounted on **/boot** contains the operating system kernel, which allows your system to boot Red Hat Enterprise Linux, along with files used during the bootstrap process. Due to the limitations of most firmwares, creating a small partition to hold these is recommended. In most scenarios, a 1 GiB boot partition is adequate. Unlike other mount points, using an LVM volume for **/boot** is not possible - **/boot** must be located on a separate disk partition.

WARNING

Normally, the **/boot** partition is created automatically by the installation program. However, if the **/** (root) partition is larger than 2 TiB and (U)EFI is used for booting, you need to create a separate **/boot** partition that is smaller than 2 TiB to boot the machine successfully.



NOTE

If you have a RAID card, be aware that some BIOS types do not support booting from the RAID card. In such a case, the **/boot** partition must be created on a partition outside of the RAID array, such as on a separate hard drive.

root - recommended size of 10 GiB

This is where "/", or the root directory, is located. The root directory is the top-level of the directory structure. By default, all files are written to this file system unless a different file system is mounted in the path being written to (for example, **/boot** or **/home**).

While a 5 GiB root file system allows you to install a minimal installation, it is recommended to allocate at least 10 GiB so that you can install as many package groups as you want.

IMPORTANT

Do not confuse the / directory with the **/root** directory. The **/root** directory is the home directory of the root user. The **/root** directory is sometimes referred to as *slash root* to distinguish it from the root directory.

/home - recommended size at least 1 GiB

To store user data separately from system data, create a dedicated file system for the **/home** directory. This file system should be sized based on the amount of data that will be stored locally, number of users, and so on. This will enable you to upgrade or reinstall Red Hat Enterprise Linux without erasing user data files. If you select automatic partitioning, it is recommended to have at least 55GiB of disk space available for the installation, to ensure that the **/home** file system is created.

swap partition - recommended size at least 1 GB

Swap file systems support virtual memory; data is written to a swap file system when there is not enough RAM to store the data your system is processing. Swap size is a function of system memory workload, not total system memory and therefore is not equal to the total system memory size. Therefore, it is important to analyze what applications a system will be running and the load those applications will serve in order to determine the system memory workload. Application providers and developers should be able to provide some guidance.

When the system runs out of swap space, the kernel terminates processes as the system RAM memory is exhausted. Configuring too much swap space results in storage devices being allocated but idle and is a poor use of resources. Too much swap space can also hide memory leaks. The maximum size for a swap partition and other additional information can be found in the **mkswap(8)** manual page.

The following table provides the recommended size of a swap partition depending on the amount of RAM in your system and whether you want sufficient memory for your system to hibernate. If you let the installation program partition your system automatically, the swap partition size will be established using these guidelines. Automatic partitioning setup assumes hibernation is not in use. The maximum size of the swap partition is limited to 10% of the total size of the hard drive, and the installer cannot create swap partitions more than 128GB in size. If you want to set up enough swap space to allow for hibernation, or if you want to set the swap partition size to more than 10% of the system's storage space, or more than 128GB, you must edit the partitioning layout manually.

Table 8.3. Recommended System Swap Space

Amount of RAM in the system	Recommended swap space	Recommended swap space if allowing for hibernation
less than 2 GB	2 times the amount of RAM	3 times the amount of RAM
2 GB - 8 GB	Equal to the amount of RAM	2 times the amount of RAM

Amount of RAM in the system	Recommended swap space	Recommended swap space if allowing for hibernation
8 GB - 64 GB	4GB to 0.5 times the amount of RAM	1.5 times the amount of RAM
more than 64 GB	workload dependent (at least 4GB)	hibernation not recommended

At the border between each range listed above (for example, a system with 2 GB, 8 GB, or 64 GB of system RAM), discretion can be exercised with regard to chosen swap space and hibernation support. If your system resources allow for it, increasing the swap space can lead to better performance.

Distributing swap space over multiple storage devices - particularly on systems with fast drives, controllers and interfaces - also improves swap space performance.

Many systems have more partitions and volumes than the minimum listed above. Choose partitions based on your particular system needs. See Section 8.14.4.4.1, “Advice on Partitions” for more information.

NOTE

Only assign storage capacity to those partitions you require immediately. You can allocate free space at any time, to meet needs as they occur. To learn about a more flexible method for storage management, see Appendix C, *Understanding LVM*.

If you are not sure how best to configure the partitions for your computer, accept the automatic default partition layout provided by the installation program.

8.14.4.4.1. Advice on Partitions

Optimal partition setup depends on the usage for the Linux system in question. Use these tips to decide how to configure your disk space.

- Consider encrypting any partitions that might contain sensitive data. Encryption prevents unauthorized people from accessing the data on the partitions, even if they have access to the physical storage device. In most cases, you should at least encrypt the **/home** partition.
- Each kernel installed on your system requires approximately 20 MiB on the **/boot** partition. The default partition size of 1 GiB for **/boot** should suffice for most common uses; increase the size of this partition if you plan to keep many kernels installed at the same time.
- The **/var** directory holds content for a number of applications, including the **Apache** web server. It also is used to store downloaded update packages on a temporary basis. Ensure that the partition containing the **/var** directory has enough space to download pending updates and hold your other content.
- The **PackageKit** update software downloads updated packages to **/var/cache/yum/** by default. If you create a separate partition or volume for **/var**, ensure that it is at least 3GB in size to accommodate downloaded package updates.

- The **/usr** directory holds the majority of software content on a Red Hat Enterprise Linux system. For an installation of the default set of software, allocate at least 5 GB of space. If the system will be used as a software development workstation, allocate at least 10GB.

- If **/usr** or **/var** is partitioned separately from the rest of the root volume, the boot process becomes much more complex because these directories contain components critical to it. In some situations, such as when these directories are placed on an iSCSI drive or an FCoE location, the system can either be unable to boot, or it can hang with a **Device is busy** error when powering off or rebooting.

  This limitation only applies to **/usr** or **/var**, not to directories below them. For example, a separate partition for **/var/www** will work without issues.

- Consider leaving a portion of the space in an LVM volume group unallocated. This unallocated space gives you flexibility if your space requirements change but you do not want to remove data from other partitions to reallocate storage. You can also select the **Thin provisioning** device type for the partition to have the unused space handled automatically by the volume.

- If you separate subdirectories into partitions, you can retain content in those subdirectories if you decide to install a new version of Red Hat Enterprise Linux over your current system. For instance, if you intend to run a **MySQL** database in **/var/lib/mysql/**, make a separate partition for that directory in case you need to reinstall later.

- On a BIOS system with its boot loader using GPT (GUID partition table), you need to create the **biosboot** partition of 1 MiB in size. See Section 8.14.1, “Boot Loader Installation” for more details.

- UEFI systems need to contain a small partition with a mount point of **/boot/efi/** containing an EFI System Partition file system. Its recommended size is 200 MiB, which is also the default value for automatic partitioning.

8.15. STORAGE DEVICES

You can install Red Hat Enterprise Linux on a large variety of storage devices. You can see basic, locally accessible, storage devices in the **Installation Destination** page, as described in Section 8.14, “Installation Destination”. To add a specialized storage device, click the **Add a disk** button in the **Specialized & Network Disks** section of the screen.

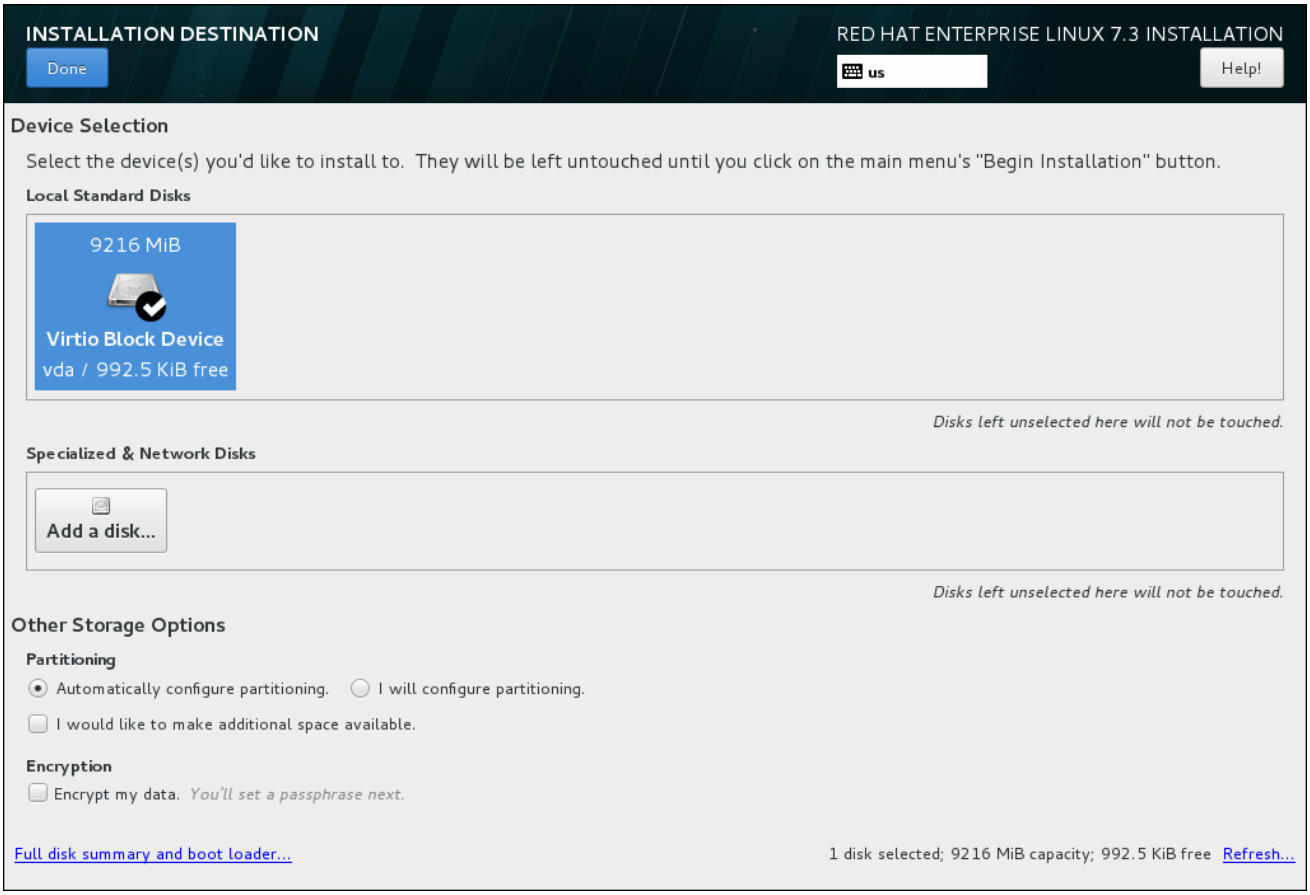


Figure 8.29. Storage Space Overview

NOTE

Monitoring of LVM and software RAID devices by the **`dmeventd`** daemon is not performed during installation.

8.15.1. The Storage Devices Selection Screen

The storage device selection screen displays all storage devices to which the **Anaconda** installation program has access.

The devices are grouped under the following tabs:

Multipath Devices

Storage devices accessible through more than one path, such as through multiple SCSI controllers or Fiber Channel ports on the same system.

The installation program only detects multipath storage devices with serial numbers that are 16 or 32 characters long.

Other SAN Devices

Devices available on a Storage Area Network (SAN).

Firmware RAID

Storage devices attached to a firmware RAID controller.

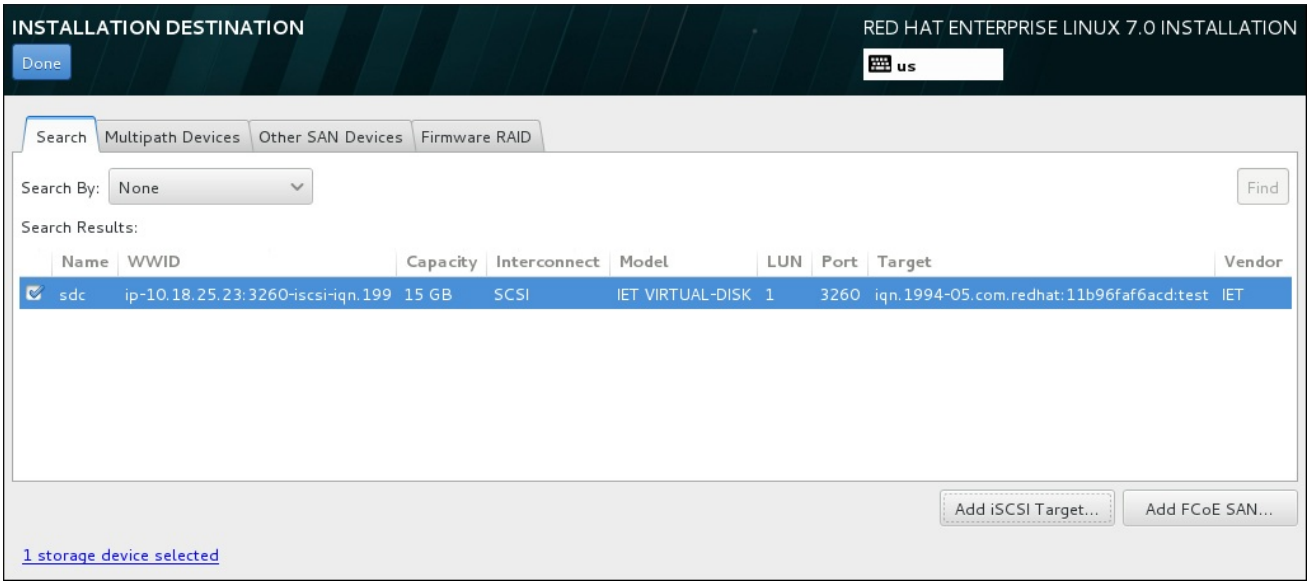


Figure 8.30. Tabbed Overview of Specialized Storage Devices

A set of buttons is available in the bottom right corner of the screen. Use these buttons to add additional storage devices. The available buttons are:

- **`Add iSCSI Target`** - use to attach iSCSI devices; continue with Section 8.15.1.1.1, “Configuring iSCSI Parameters”
- **`Add FCoE SAN`** - use to configure a Fibre Channel Over Internet storage device; continue with Section 8.15.1.1.2, “Configuring FCoE Parameters”

The overview page also contains the **`Search`** tab that allows you to filter storage devices either by their *World Wide Identifier* (WWID) or by the port, target, or *logical unit number* (LUN) at which they are accessed.

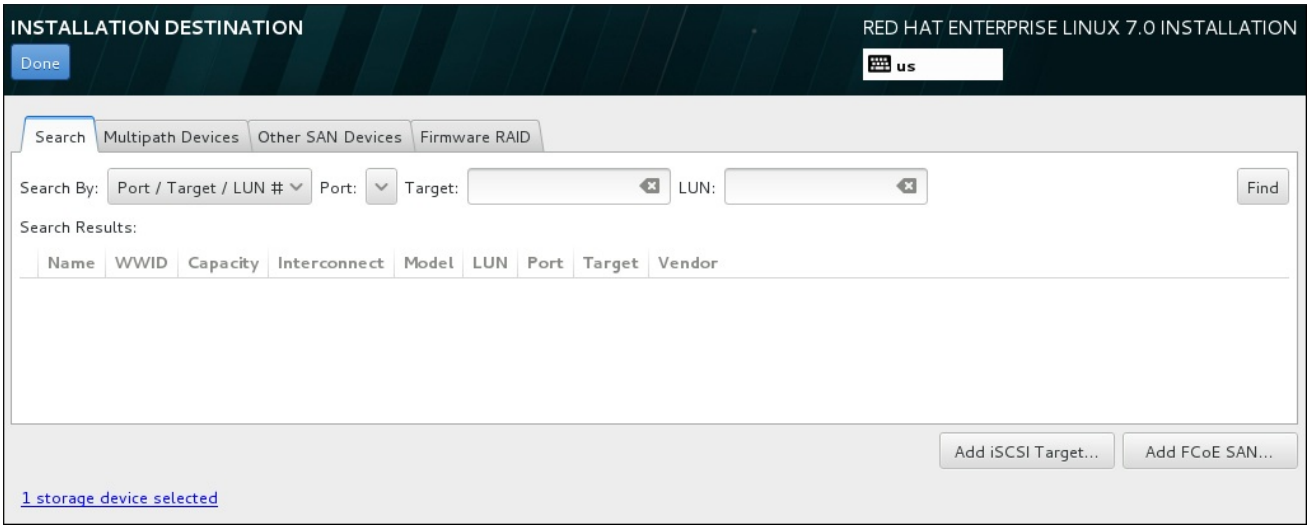


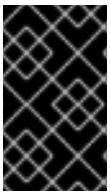
Figure 8.31. The Storage Devices Search Tab

The Search tab contains the **`Search By`** drop-down menu to select searching by port, target, LUN, or WWID. Searching by WWID or LUN requires additional values in the corresponding input text fields. Click the **`Find`** button to start the search.

Each device is presented on a separate row, with a check box to its left. Click the check box to make the device available during the installation process. Later in the installation process, you can choose to

install Red Hat Enterprise Linux onto any of the devices selected here, and can choose to automatically mount any of the other devices selected here as part of the installed system.

Note that the devices that you select here are not automatically erased by the installation process. Selecting a device on this screen does not, in itself, place data stored on the device at risk. Also note that any devices that you do not select here to form part of the installed system can be added to the system after installation by modifying the **/etc/fstab** file.



IMPORTANT

Any storage devices that you do not select on this screen are hidden from **Anaconda** entirely. To *chain load* the Red Hat Enterprise Linux boot loader from a different boot loader, select all the devices presented in this screen.

When you have selected the storage devices to make available during installation, click **Done** to return to the Installation Destination screen.

8.15.1.1. Advanced Storage Options

To use an advanced storage device, you can configure an *iSCSI* (SCSI over TCP/IP) target or *FCoE* (Fibre Channel over Ethernet) *SAN* (Storage Area Network) by clicking the appropriate button in the lower right corner of the Installation Destination screen. See Appendix B, *iSCSI Disks* for an introduction to iSCSI.

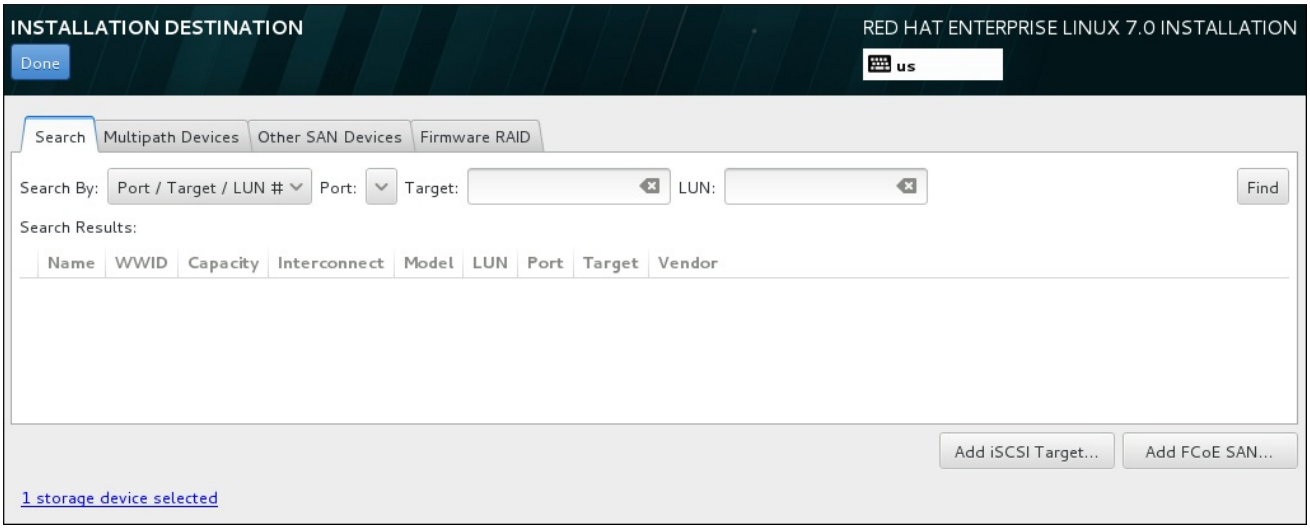


Figure 8.32. Advanced Storage Options

8.15.1.1.1. Configuring iSCSI Parameters

When you have clicked the **Add iSCSI target...** button, the **Add iSCSI Storage Target** dialog appears.

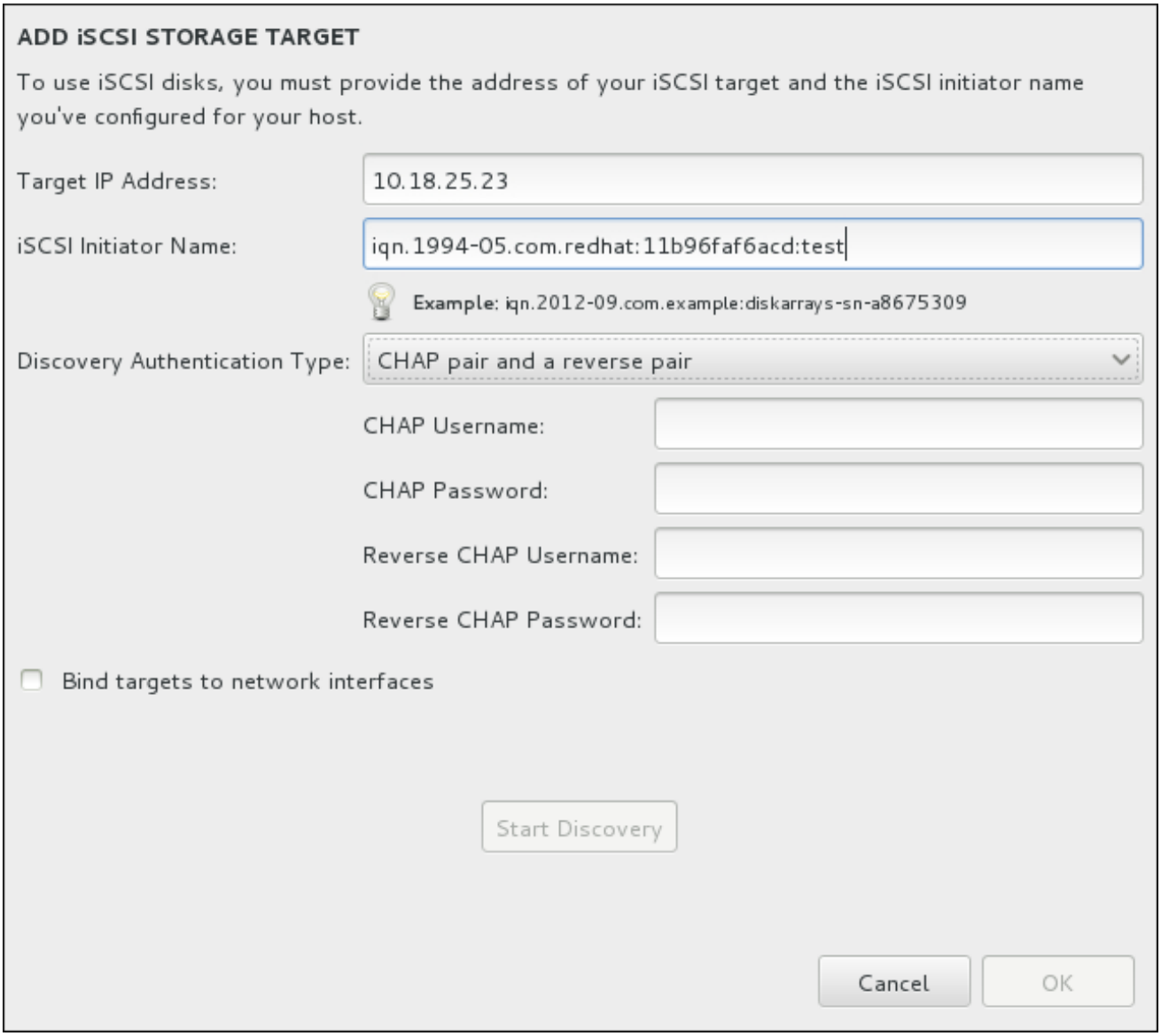


Figure 8.33. The iSCSI Discovery Details Dialog

To use iSCSI storage devices for the installation, **Anaconda** must be able to *discover* them as iSCSI targets and be able to create an iSCSI *session* to access them. Each of these steps might require a user name and password for *CHAP* (Challenge Handshake Authentication Protocol) authentication. Additionally, you can configure an iSCSI target to authenticate the iSCSI initiator on the system to which the target is attached (*reverse CHAP*), both for discovery and for the session. Used together, CHAP and reverse CHAP are called *mutual CHAP* or *two-way CHAP*. Mutual CHAP provides the greatest level of security for iSCSI connections, particularly if the user name and password are different for CHAP authentication and reverse CHAP authentication.

NOTE

Repeat the iSCSI discovery and iSCSI login steps as many times as necessary to add all required iSCSI storage. However, you cannot change the name of the iSCSI initiator after you attempt discovery for the first time. To change the iSCSI initiator name, you must restart the installation.

Procedure 8.1. iSCSI Discovery and Starting an iSCSI Session

Use the **`Add iSCSI Storage Target`** dialog to provide **Anaconda** with the information necessary to discover the iSCSI target.

1. Enter the IP address of the iSCSI target in the **Target IP Address** field.

2. Provide a name in the **iSCSI Initiator Name** field for the iSCSI initiator in *iSCSI qualified name* (IQN) format. A valid IQN entry contains:

   - the string **iqn.** (note the period)
   - a date code that specifies the year and month in which your organization's Internet domain or subdomain name was registered, represented as four digits for the year, a dash, and two digits for the month, followed by a period. For example, represent September 2010 as **2010-09.**
   - your organization's Internet domain or subdomain name, presented in reverse order with the top-level domain first. For example, represent the subdomain **storage.example.com** as **com.example.storage**
   - a colon followed by a string that uniquely identifies this particular iSCSI initiator within your domain or subdomain. For example, **:diskarrays-sn-a8675309**

   A complete IQN can therefore look as follows: **iqn.2010-09.storage.example.com:diskarrays-sn-a8675309** . **Anaconda** prepopulates the **iSCSI Initiator Name** field with a name in this format to help you with the structure.

   For more information on IQNs , see *3.2.6. iSCSI Names* in *RFC 3720 - Internet Small Computer Systems Interface (iSCSI)* available from http://tools.ietf.org/html/rfc3720#section-3.2.6 and *1. iSCSI Names and Addresses* in *RFC 3721 - Internet Small Computer Systems Interface (iSCSI) Naming and Discovery* available from http://tools.ietf.org/html/rfc3721#section-1.

3. Use the **Discovery Authentication Type** drop-down menu to specify the type of authentication to use for iSCSI discovery. The following options are available:

   - no credentials
   - CHAP pair
   - CHAP pair and a reverse pair

4. - If you selected **CHAP pair** as the authentication type, provide the user name and password for the iSCSI target in the **CHAP Username** and **CHAP Password** fields.
   - If you selected **CHAP pair and a reverse pair** as the authentication type, provide the user name and password for the iSCSI target in the **CHAP Username** and **CHAP Password** field and the user name and password for the iSCSI initiator in the **Reverse CHAP Username** and **Reverse CHAP Password** fields.

5. Optionally check the box labeled **Bind targets to network interfaces**.

6. Click the **Start Discovery** button. **Anaconda** attempts to discover an iSCSI target based on the information that you provided. If discovery succeeds, the dialog displays a list of all iSCSI nodes discovered on the target.

7. Each node is presented with a check box beside it. Click the check boxes to select the nodes to use for installation.

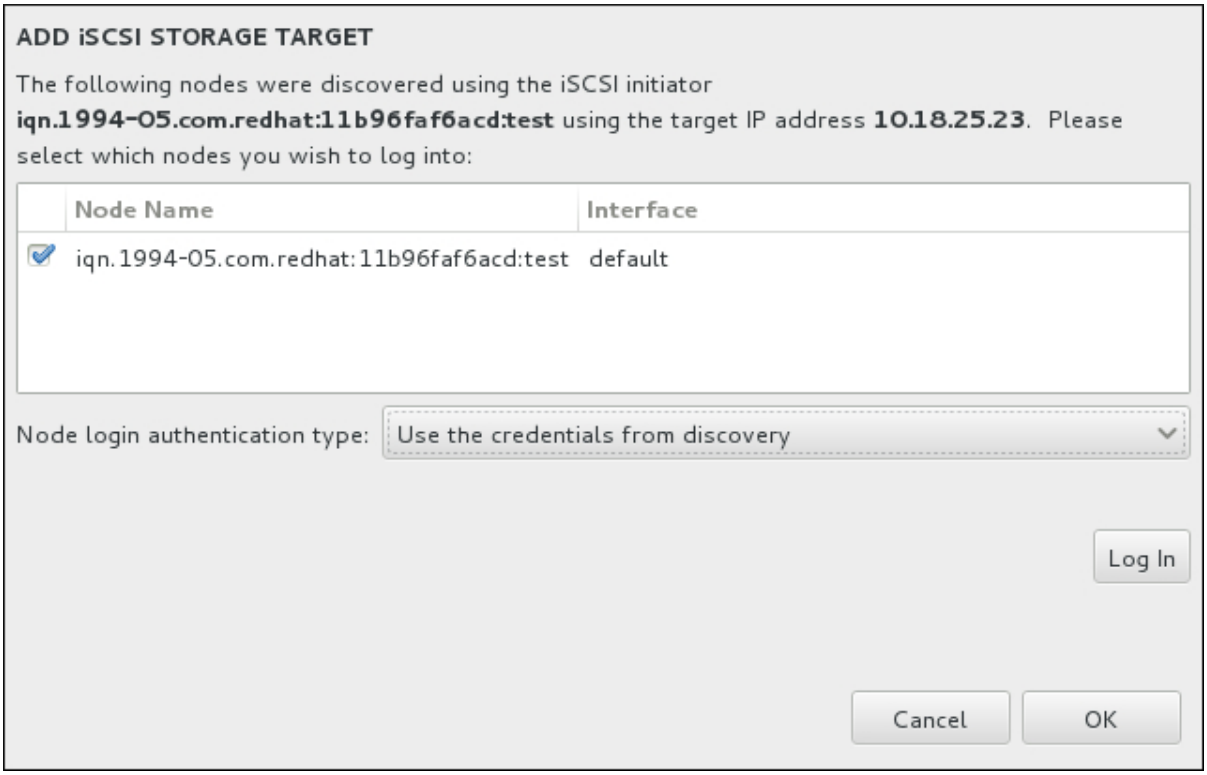


Figure 8.34. The Dialog of Discovered iSCSI Nodes

8. The **Node login authentication type** menu provides the same options as the **Discovery Authentication Type** menu described in step 3. However, if you needed credentials for discovery authentication, it is typical to use the same credentials to log into a discovered node. To do that, use the additional **Use the credentials from discovery** option from the menu. When the proper credentials have been provided, the **Log In** button becomes available.

9. Click **Log In** to initiate an iSCSI session.

8.15.1.1.2. Configuring FCoE Parameters

When you have clicked the **Add FCoE SAN...** button, a dialog appears for you to configure network interfaces for discovering FCoE storage devices.

First, select a network interface that is connected to a FCoE switch in the **NIC** drop-down menu and click the **Add FCoE disk(s)** button to scan the network for SAN devices.

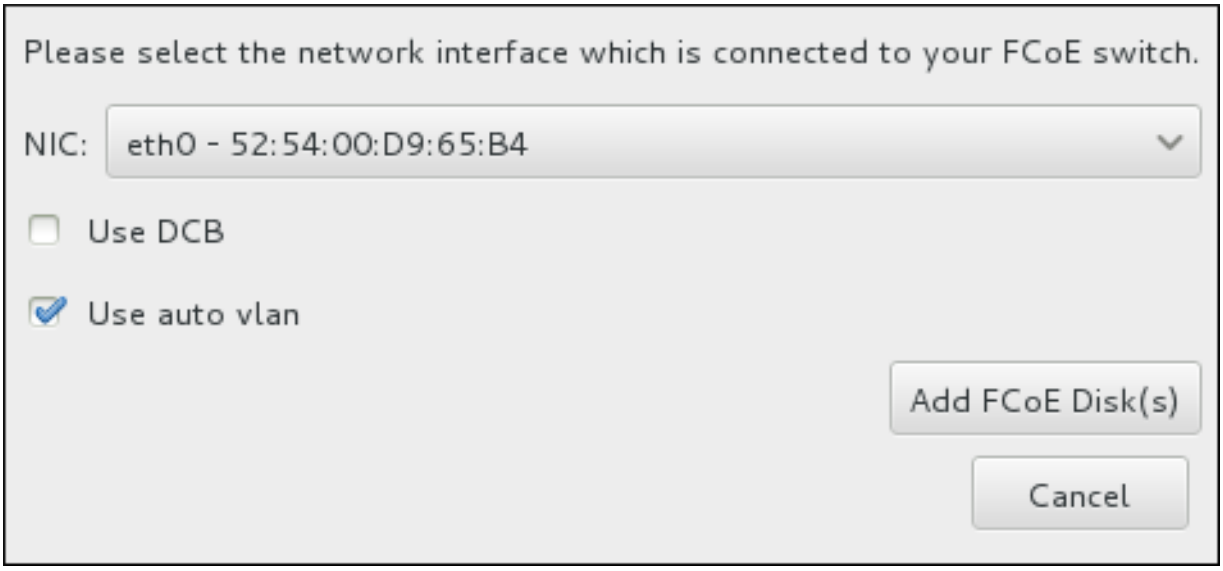


Figure 8.35. Configure FCoE Parameters

There are check boxes with additional options to consider:

Use DCB

Data Center Bridging (DCB) is a set of enhancements to the Ethernet protocols designed to increase the efficiency of Ethernet connections in storage networks and clusters. Enable or disable the installation program's awareness of DCB with the check box in this dialog. This option should only be enabled for network interfaces that require a host-based DCBX client. Configurations on interfaces that implement a hardware DCBX client should leave this check box empty.

Use auto vlan

Auto VLAN indicates whether VLAN discovery should be performed. If this box is checked, then the FIP (FCoE Initiation Protocol) VLAN discovery protocol will run on the Ethernet interface once the link configuration has been validated. If they are not already configured, network interfaces for any discovered FCoE VLANs will be automatically created and FCoE instances will be created on the VLAN interfaces. This option is enabled by default.

Discovered FCoE devices will be displayed under the **`Other SAN Devices`** tab in the Installation Destination screen.

8.16. KDUMP

Use this screen to select whether or not to use **Kdump** on this system. **Kdump** is a kernel crash dumping mechanism which, in the event of a system crash, captures information that can be invaluable in determining the cause of the crash.

Note that if you enable **Kdump**, you must reserve a certain amount of system memory for it. As a result, less memory is available for your processes.

If you do not want to use **Kdump** on this system, uncheck **`Enable kdump`**. Otherwise, set the amount of memory to reserve for **Kdump**. You can let the installer reserve a reasonable amount automatically, or you can set any amount manually. When your are satisfied with the settings, click **Done** to save the configuration and return to the previous screen.

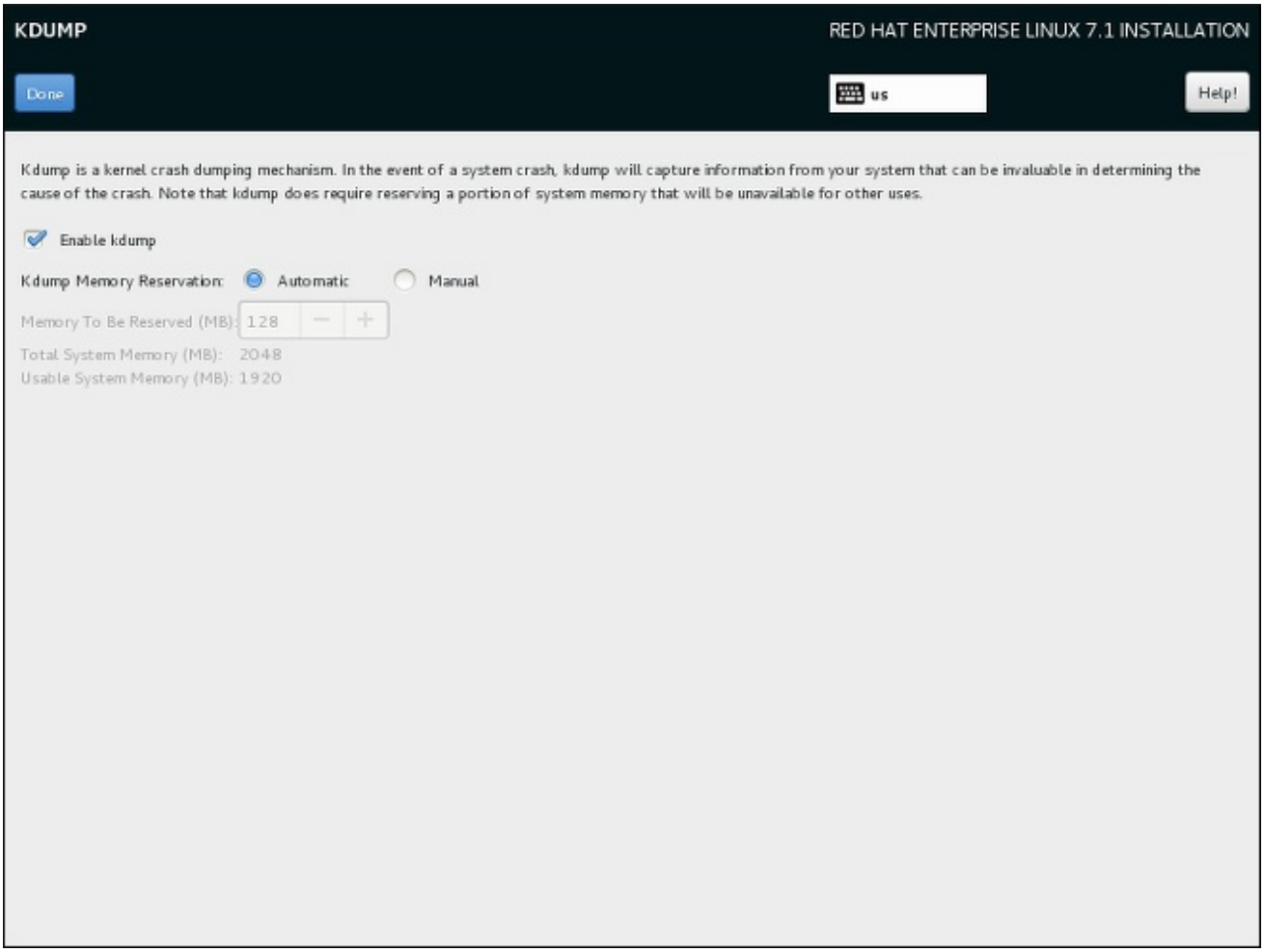


Figure 8.36. Kdump Enablement and Configuration

8.17. BEGIN INSTALLATION

When all required sections of the **`Installation Summary`** screen have been completed, the admonition at the bottom of the menu screen disappears and the **`Begin Installation`** button becomes available.

Figure 8.37. Ready to Install

WARNING

Up to this point in the installation process, no lasting changes have been made on your computer. When you click **Begin Installation**, the installation program will allocate space on your hard drive and start to transfer Red Hat Enterprise Linux into this space. Depending on the partitioning option that you chose, this process might include erasing data that already exists on your computer.

To revise any of the choices that you made up to this point, return to the relevant section of the **Installation Summary** screen. To cancel installation completely, click **Quit** or switch off your computer. To switch off most computers at this stage, press the power button and hold it down for a few seconds.

If you have finished customizing your installation and are certain that you want to proceed, click **Begin Installation**.

After you click **Begin Installation**, allow the installation process to complete. If the process is interrupted, for example, by you switching off or resetting the computer, or by a power outage, you will probably not be able to use your computer until you restart and complete the Red Hat Enterprise Linux installation process, or install a different operating system.

8.18. THE CONFIGURATION MENU AND PROGRESS SCREEN

Once you click **Begin Installation** at the **Installation Summary** screen, the progress screen appears. Red Hat Enterprise Linux reports the installation progress on the screen as it writes the selected packages to your system.

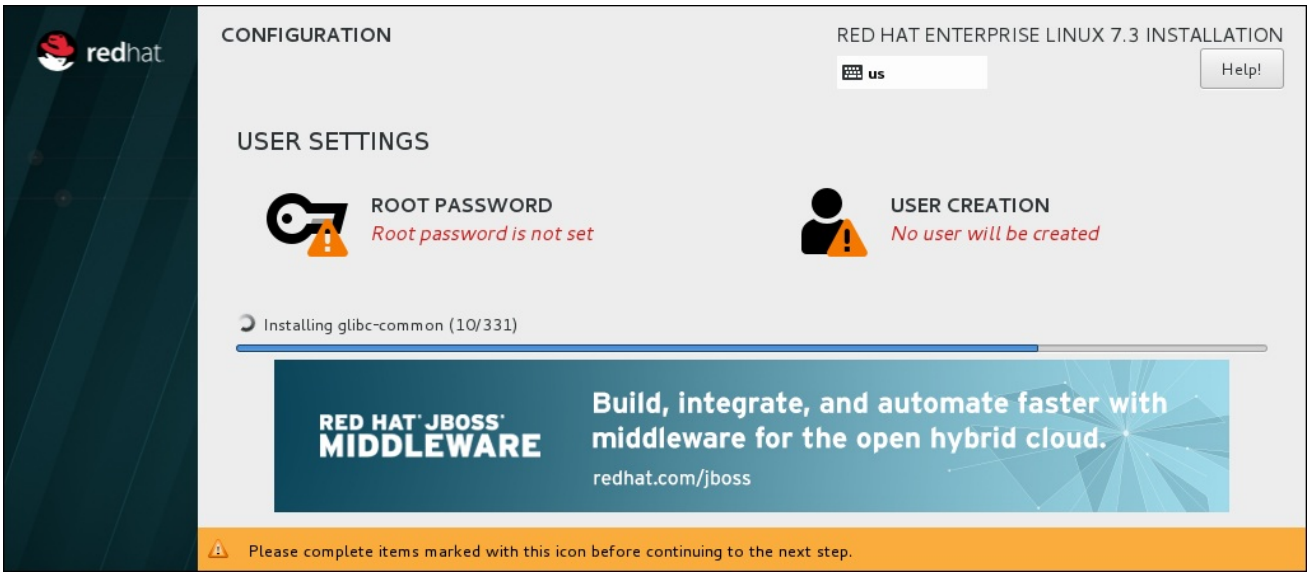


Figure 8.38. Installing Packages

For your reference, a complete log of your installation can be found in the **/var/log/anaconda/anaconda.packaging.log** file, once you reboot your system.

If you chose to encrypt one or more partitions during partitioning setup, a dialog window with a progress bar will be displayed during the early stage of the installation process. This window informs that the installer is attempting to gather enough entropy (random data) to ensure that the encryption is secure. This window will disappear after 256 bits of entropy are gathered, or after 10 minutes. You can speed up the gathering process by moving your mouse or randomly typing on the keyboard. After the window disappears, the installation process will continue.

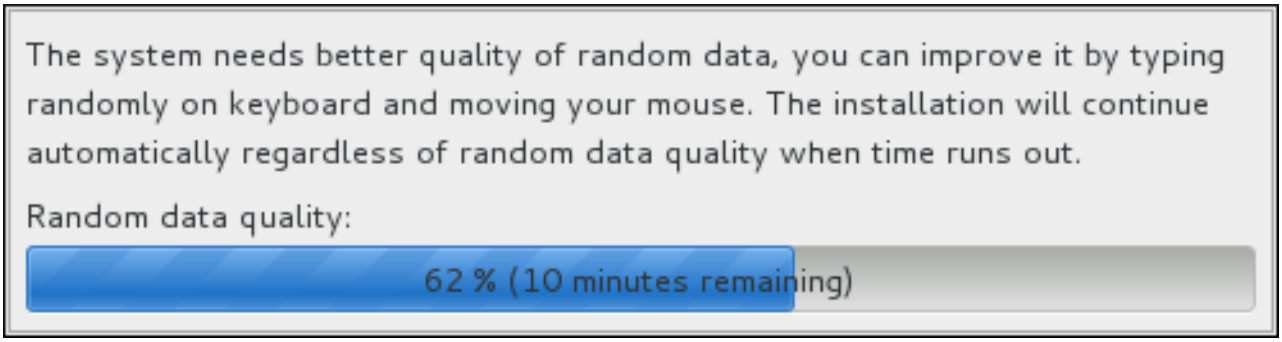


Figure 8.39. Gathering Entropy for Encryption

While the packages are being installed, more configuration is required. Above the installation progress bar are the **Root Password** and **User Creation** menu items.

The **Root Password** screen is used to configure the system's **root** account. This account can be used to perform critical system management and administration tasks. The same tasks can also be performed with a user account with the **wheel** group membership; if such an user account is created during installation, setting up a **root** password is not mandatory.

Creating a user account is optional and can be done after installation, but it is recommended to do it on this screen. A user account is used for normal work and to access the system. Best practice suggests that you always access the system through a user account, not the root account.

It is possible to disable access to the **Root Password** or **Create User** screens. To do so, use a Kickstart file which includes the **rootpw --lock** or **user --lock** commands. See Section 26.3.1, "Kickstart Commands and Options" for more information these commands.

8.18.1. Set the Root Password

Setting up a root account and password is an important step during your installation. The root account (also known as the superuser) is used to install packages, upgrade RPM packages, and perform most system maintenance. The root account gives you complete control over your system. For this reason, the root account is best used *only* to perform system maintenance or administration. See the Red Hat Enterprise Linux 7 System Administrator's Guide for more information about becoming root.

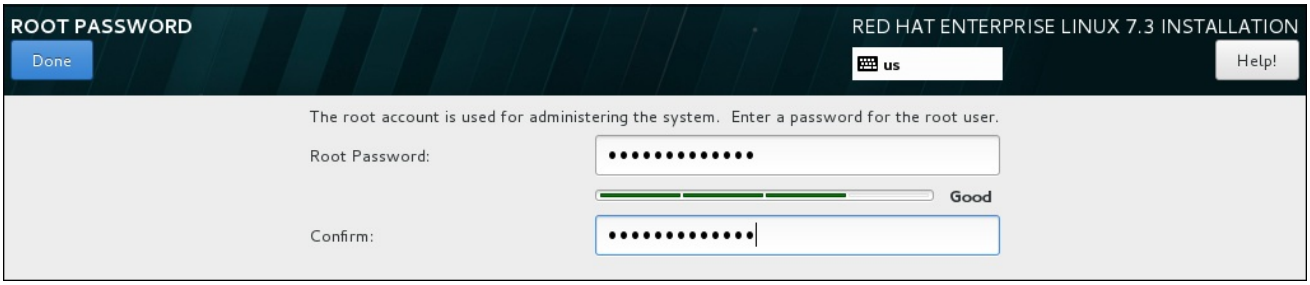


Figure 8.40. Root Password Screen

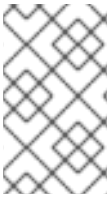
NOTE

You must always set up at least one way to gain root privileges to the installed system: either using a **root** account, or by creating a user account with administrative privileges (member of the **wheel** group), or both.

Click the **Root Password** menu item and enter your new password into the **Root Password** field. Red Hat Enterprise Linux displays the characters as asterisks for security. Type the same password into the **Confirm** field to ensure it is set correctly. After you set the root password, click **Done** to return to the User Settings screen.

The following are the requirements and recommendations for creating a strong root password:

- *must* be at least eight characters long
- may contain numbers, letters (upper and lower case) and symbols
- is case-sensitive and should contain a mix of cases
- something you can remember but that is not easily guessed
- should not be a word, abbreviation, or number associated with you, your organization, or found in a dictionary (including foreign languages)
- should not be written down; if you must write it down keep it secure



NOTE

To change your root password after you have completed the installation, run the **passwd** command as **root**. If you forget the root password, see Section 31.1.3, "Resetting the Root Password" for instructions on how to use the rescue mode to set a new one.

8.18.2. Create a User Account

To create a regular (non-root) user account during the installation, click **User Settings** on the progress screen. The **Create User** screen appears, allowing you to set up the regular user account and configure its parameters. Though recommended to do during installation, this step is optional and can be performed after the installation is complete.

NOTE

You must always set up at least one way to gain root privileges to the installed system: either using a **root** account, or by creating a user account with administrative privileges (member of the **wheel** group), or both.

To leave the user creation screen after you have entered it, without creating a user, leave all the fields empty and click **Done**.

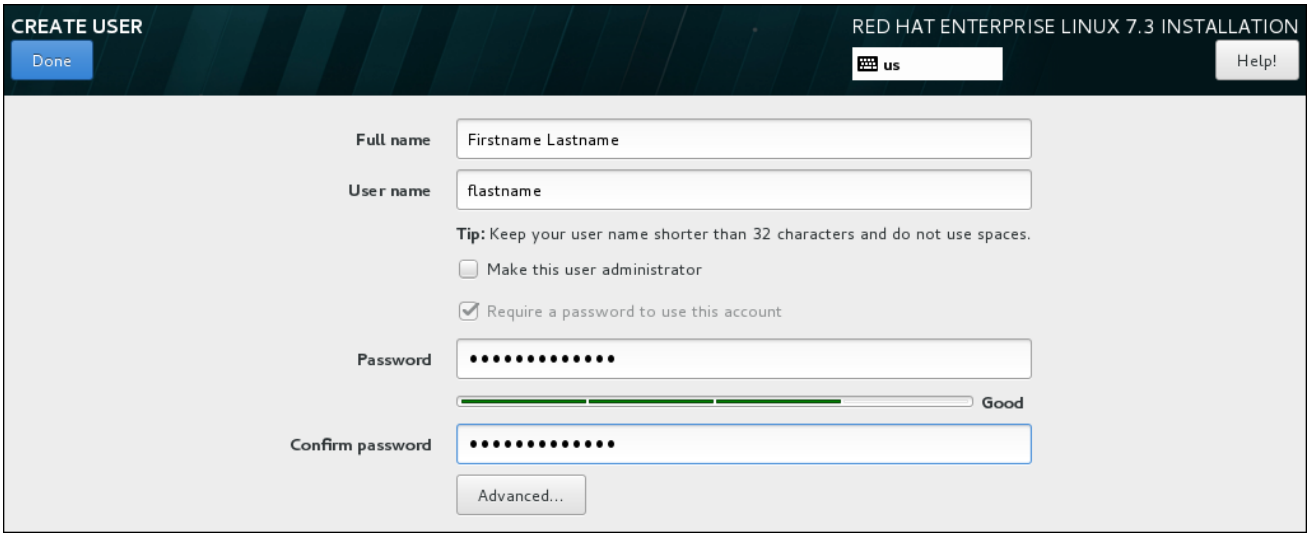


Figure 8.41. User Account Configuration Screen

Enter the full name and the user name in their respective fields. Note that the system user name must be shorter than 32 characters and cannot contain spaces. It is highly recommended to set up a password for the new account.

When setting up a strong password even for a non-root user, follow the guidelines described in Section 8.18.1, “Set the Root Password”.

Click the **Advanced** button to open a new dialog with additional settings.

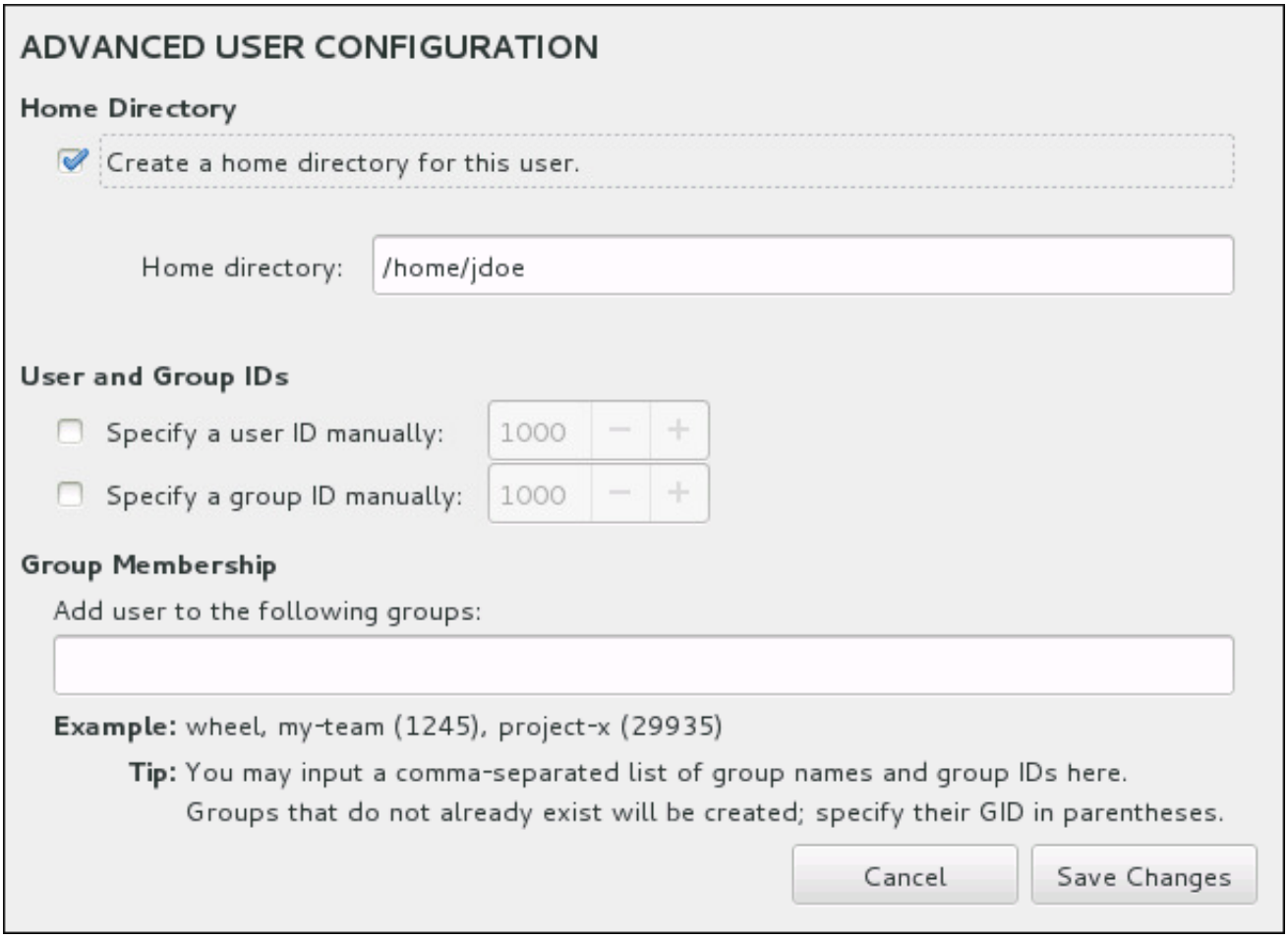


Figure 8.42. Advanced User Account Configuration

By default, each user gets a home directory corresponding to their user name. In most scenarios, there is no need to change this setting.

You can also manually define a system identification number for the new user and their default group by selecting the check boxes. The range for regular user IDs starts at the number **1000**. At the bottom of the dialog, you can enter the comma-separated list of additional groups, to which the new user shall belong. The new groups will be created in the system. To customize group IDs, specify the numbers in parenthesis.

NOTE

Consider setting IDs of regular users and their default groups at range starting at **5000** instead of **1000**. That is because the range reserved for system users and groups, **0**-**999**, might increase in the future and thus overlap with IDs of regular users.

For creating users with custom IDs using kickstart, see **user** (optional) .

For changing the minimum UID and GID limits after the installation, which ensures that your chosen UID and GID ranges are applied automatically on user creation, see the Users and Groups chapter of the System Administrator's Guide.

Once you have customized the user account, click **Save Changes** to return to the **User Settings** screen.

8.19. INSTALLATION COMPLETE

Congratulations! Your Red Hat Enterprise Linux installation is now complete!

Click the **Reboot** button to reboot your system and begin using Red Hat Enterprise Linux. Remember to remove any installation media if it is not ejected automatically upon reboot.

After your computer's normal power-up sequence has completed, Red Hat Enterprise Linux loads and starts. By default, the start process is hidden behind a graphical screen that displays a progress bar. Eventually, a GUI login screen (or if the X Window System is not installed, a **login:** prompt) appears.

If your system was installed with the X Window System during this installation process, the first time you start your Red Hat Enterprise Linux system, applications to set up your system are launched. These applications guide you through initial configuration of Red Hat Enterprise Linux and allow you to set your system time and date, register your machine with Red Hat Network, and more.

See Chapter 29, *Initial Setup* for information about the configuration process. For instructions on post-installation procedures, configuration and updates for Red Hat Enterprise Linux Atomic Host, see the Getting Started withRed Hat Enterprise Linux Atomic Host document.

CHAPTER 9. TROUBLESHOOTING INSTALLATION ON AMD64 AND INTEL 64 SYSTEMS

This chapter discusses some common installation problems and their solutions.

For debugging purposes, **Anaconda** logs installation actions into files in the **/tmp** directory. These files are listed in the following table.

Table 9.1. Log Files Generated During the Installation

Log file	Contents
/tmp/anaconda.log	general **Anaconda** messages
/tmp/program.log	all external programs run during the installation
/tmp/storage.log	extensive storage module information
/tmp/packaging.log	**yum** and **rpm** package installation messages
/tmp/syslog	hardware-related system messages

If the installation fails, the messages from these files are consolidated into **/tmp/anaconda-tb-*identifier***, where *identifier* is a random string.

After successful installation, by default, these files will be copied to the installed system under the directory **/var/log/anaconda/**. However, if installation is unsuccessful, or if the **inst.nosave=all** or **inst.nosave=logs** options are used when booting the installation system, these logs will only exist in the installation program's RAM disk. This means they are not saved permanently and will be lost once the system is powered down. To store them permanently, copy those files to another system on the network by using **scp** on the system running the installation program, or copy them to a mounted storage device (such as an USB flash drive). Details on how to transfer the log files over the network are below. Note that if you use an USB flash drive or other removable media, you should make sure to back up any data on it before starting the procedure.

Procedure 9.1. Transferring Log Files Onto a USB Drive

1. On the system you are installing, press **Ctrl**+**Alt**+**F2** to access a shell prompt. You will be logged into a root account and you will have access to the installation program's temporary file system.

2. Connect a USB flash drive to the system and execute the **dmesg** command. A log detailing all recent events will be displayed. At the bottom of this log, you will see a set of messages caused by the USB flash drive you just connected. It will look like a set of lines similar to the following:

   ```
   [ 170.171135] sd 5:0:0:0: [sdb] Attached SCSI removable disk
   ```

   Note the name of the connected device - in the above example, it is **sdb**.

3. Go to the **/mnt** directory and once there, create new directory which will serve as the mount target for the USB drive. The name of the directory does not matter; this example uses the name **usb**.

```
# mkdir usb
```

4. Mount the USB flash drive onto the newly created directory. Note that in most cases, you do not want to mount the whole drive, but a partition on it. Therefore, do not use the name **sdb** - use the name of the partition you want to write the log files to. In this example, the name **sdb1** is used.

```
# mount /dev/sdb1 /mnt/usb
```

   You can now verify that you mounted the correct device and partition by accessing it and listing its contents - the list should match what you expect to be on the drive.

```
# cd /mnt/usb
```

```
# ls
```

5. Copy the log files to the mounted device.

```
# cp /tmp/*log /mnt/usb
```

6. Unmount the USB flash drive. If you get an error message saying that the target is busy, change your working directory to outside the mount (for example, **/**).

```
# umount /mnt/usb
```

The log files from the installation are now saved on the USB flash drive.

Procedure 9.2. Transferring Log Files Over the Network

1. On the system you are installing, press **Ctrl**+**Alt**+**F2** to access a shell prompt. You will be logged into a root account and you will have access to the installation program's temporary file system.

2. Switch to the **/tmp** directory where the log files are located:

```
# cd /tmp
```

3. Copy the log files onto another system on the network using the **scp** command:

```
# scp *log user@address:path
```

   Replace *user* with a valid user name on the target system, *address* with the target system's address or host name, and *path* with the path to the directory you want to save the log files into. For example, if you want to log in as **john** to a system with an IP address of **192.168.0.122** and place the log files into the **/home/john/logs/** directory on that system, the command will have the following form:

```
# scp *log john@192.168.0.122:/home/john/logs/
```

When connecting to the target system for the first time, the SSH client asks you to confirm that the fingerprint of the remote system is correct and that you want to continue:

```
The authenticity of host '192.168.0.122 (192.168.0.122)' can't be
established.
ECDSA key fingerprint is
a4:60:76:eb:b2:d0:aa:23:af:3d:59:5c:de:bb:c4:42.
Are you sure you want to continue connecting (yes/no)?
```

Type **yes** and press **Enter** to continue. Then, provide a valid password when prompted. The files will start transferring to the specified directory on the target system.

The log files from the installation are now permanently saved on the target system and available for review.

9.1. TROUBLE BEGINNING THE INSTALLATION

9.1.1. System Does Not Boot When UEFI Secure Boot Is Enabled

Beta releases of Red Hat Enterprise Linux 7 have their kernels signed with a special public key which is not recognized by standard UEFI Secure Boot implementations. This prevents the system from booting when the Secure Boot technology is enabled.

To fix this issue, you must disable UEFI Secure Boot, install the system, and then import the Beta public key using the *Machine Owner Key* facility. See Section 5.9, “Using a Beta Release with UEFI Secure Boot” for instructions.

9.1.2. Problems with Booting into the Graphical Installation

Systems with some video cards have trouble booting into the graphical installation program. If the installation program does not run using its default settings, it attempts to run in a lower resolution mode. If that still fails, the installation program attempts to run in text mode.

There are several possible solutions to display issues, most of which involve specifying custom boot options. For more information, see Section 22.1, “Configuring the Installation System at the Boot Menu”.

Use the basic graphics mode

You can attempt to perform the installation using the basic graphics driver. To do this, either select **Troubleshooting** > **Install Red Hat Enterprise Linux in basic graphics mode** in the boot menu, or edit the installation program's boot options and append **inst.xdriver=vesa** at the end of the command line.

Specify the display resolution manually

If the installation program fails to detect your screen resolution, you can override the automatic detection and specify it manually. To do this, append the **inst.resolution=*x*** option at the boot menu, where *x* is your display's resolution (for example, **1024x768**).

Use an alternate video driver

You can also attempt to specify a custom video driver, overriding the installation program's automatic detection. To specify a driver, use the **inst.xdriver=*x*** option, where *x* is the device driver you want to use (for example, **nouveau**).

NOTE

If specifying a custom video driver solves your problem, you should report it as a bug at https://bugzilla.redhat.com under the **anaconda** component. **Anaconda** should be able to detect your hardware automatically and use the appropriate driver without your intervention.

Perform the installation using VNC

If the above options fail, you can use a separate system to access the graphical installation over the network, using the *Virtual Network Computing* (VNC) protocol. For details on installing using VNC, see Chapter 24, *Using VNC*.

9.1.3. Serial Console Not Detected

In some cases, attempting to install in text mode using a serial console will result in no output on the console. This happens on systems which have a graphics card, but no monitor connected. If **Anaconda** detects a graphics card, it will attempt to use it for a display, even if no display is connected.

If you want to perform a text-based installation on a serial console, use the **inst.text** and **console=** boot options. See Chapter 22, *Boot Options* for more details.

9.2. TROUBLE DURING THE INSTALLATION

9.2.1. No Disks Detected

In the **Installation Destination** screen, the following error message can appear at the bottom: **No disks detected. Please shut down the computer, connect at least one disk, and restart to complete installation**.

The message indicates that **Anaconda** did not find any writable storage devices to install to. In that case, first make sure that your system does have at least one storage device attached.

If your system uses a hardware RAID controller, verify that the controller is properly configured and working. See your controller's documentation for instructions.

If you are installing into one or more iSCSI devices and there is no local storage present on the system, make sure that all required LUNs (*Logical Unit Numbers*) are being presented to the appropriate HBA (*Host Bus Adapter*). For additional information about iSCSI, see Appendix B, *iSCSI Disks*.

If you made sure you have a connected and properly configured storage device and the message still appears after you reboot the system and start the installation again, it means that the installation program failed to detect the storage. In most cases this message appears when you attempt to install on an SCSI device which has not been recognized by the installation program.

In that case, you will have to perform a driver update before starting the installation. Check your hardware vendor's website to determine if a driver update is available that fixes your problem. For more general information on driver updates, see Chapter 6, *Updating Drivers During Installation on AMD64 and Intel 64 Systems*.

You can also consult the *Red Hat Hardware Compatibility List*, available online at https://hardware.redhat.com.

9.2.2. Reporting Traceback Messages

If the graphical installation program encounters an error, it presents you with a crash reporting dialog box. You can then choose to send information about the problem you encountered to Red Hat. To send a crash report, you will need to enter your Customer Portal credentials. If you do not have a Customer Portal account, you can register at https://www.redhat.com/wapps/ugc/register.html. Automated crash reporting also requires a working network connection.

Figure 9.1. The Crash Reporting Dialog Box

When the dialog appears, select **Report Bug** to report the problem, or **Quit** to exit the installation.

Optionally, click **More Info** to display detailed output that can help determine the cause of the error. If you are familiar with debugging, click **Debug**. This will take you to virtual terminal **tty1**, where you can request more precise information that will enhance the bug report. To return to the graphical interface from **tty1**, use the **continue** command.

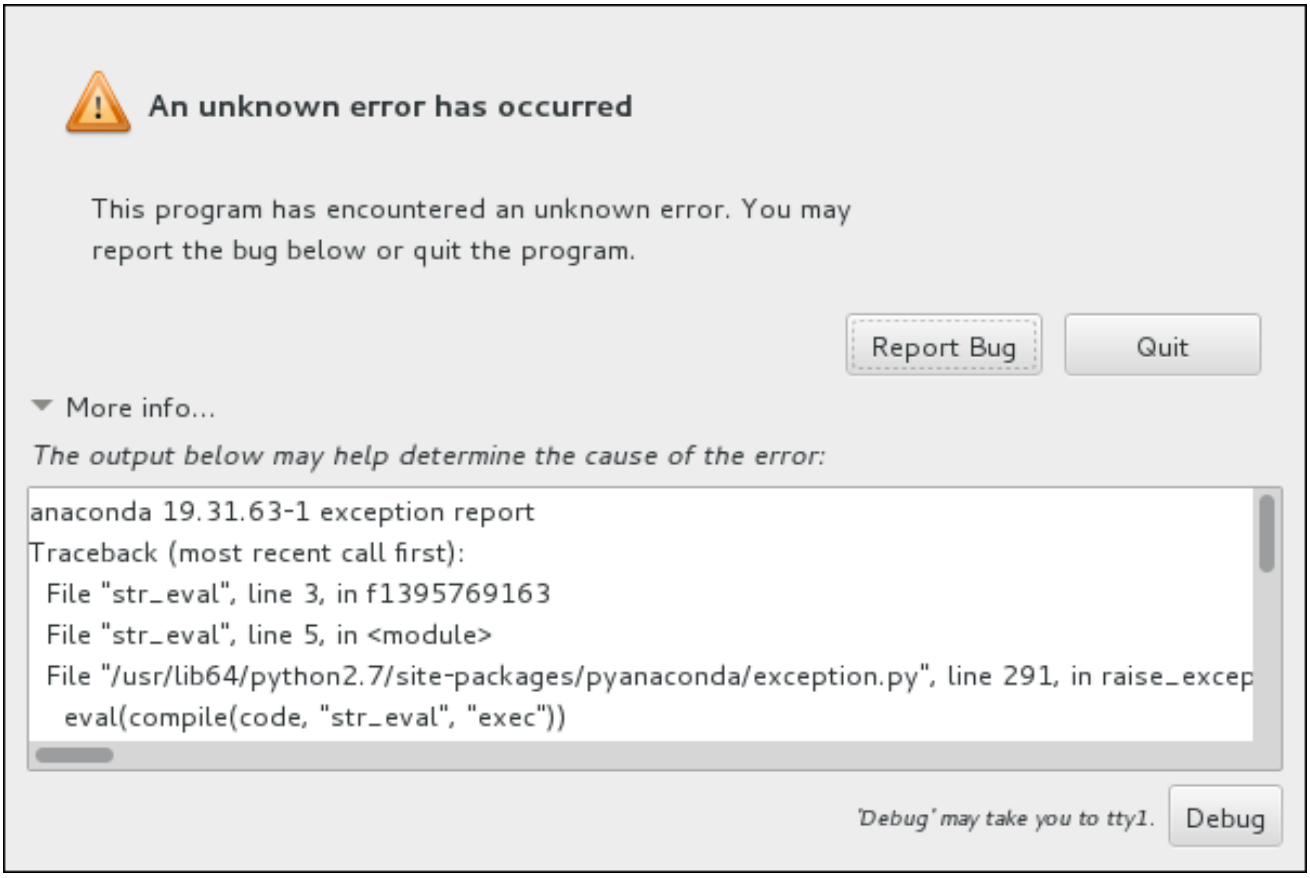


Figure 9.2. The Expanded Crash Reporting Dialog Box

If you want to report the bug to the customer portal, follow the procedure below.

Procedure 9.3. Reporting Errors to Red Hat Customer Support

1. In the menu that appears, select **`Report a bug to Red Hat Customer Portal`**.
2. To report the bug to Red Hat, you first need to provide your Customer Portal credentials. Click **`Configure Red Hat Customer Support`**.

Figure 9.3. Customer Portal Credentials

3. A new window is now open, prompting you to enter your Customer Portal user name and password. Enter your Red Hat Customer Portal credentials.

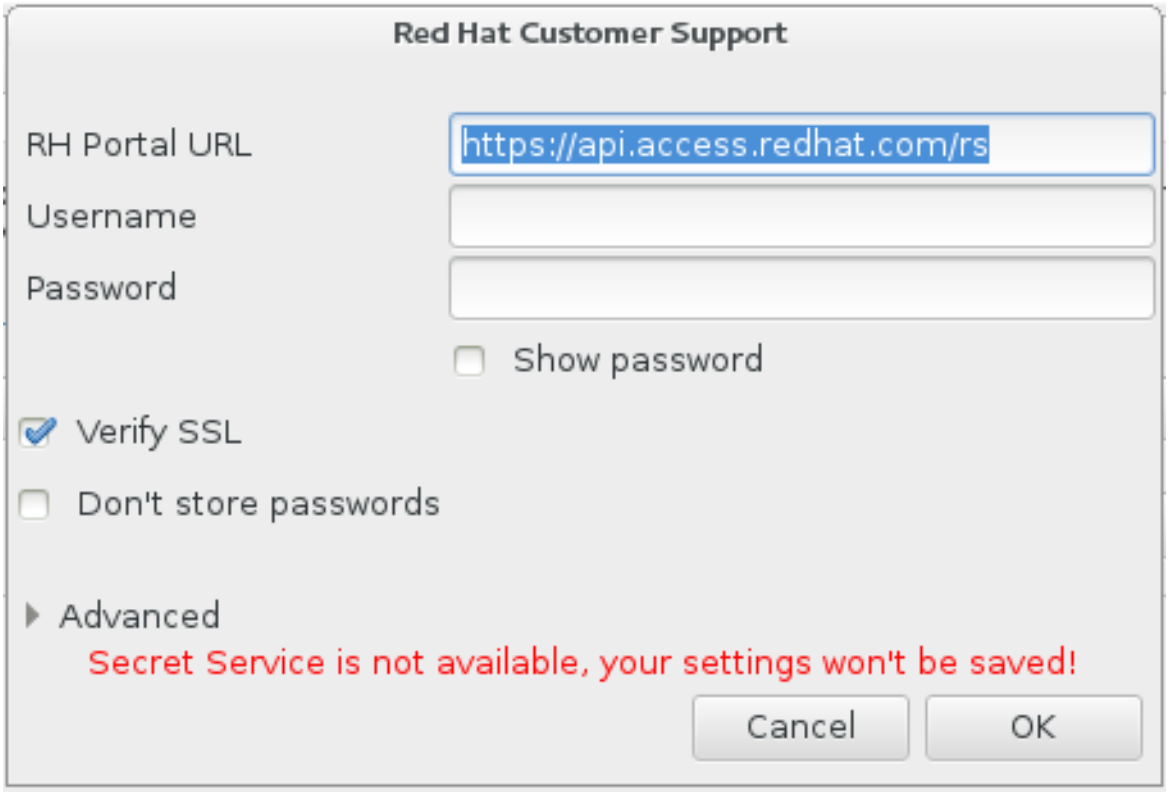


Figure 9.4. Configure Red Hat Customer Support

If your network settings require you to use a **HTTP** or **HTTPS** proxy, you can configure it by expanding the **Advanced** menu and entering the address of the proxy server.

When you put in all required credentials, click **OK** to proceed.

4. A new window appears, containing a text field. Write down any useful information and comments here. Describe how the error can be reproduced by explaining each step you took before the crash reporting dialog appeared. Provide as much relevant detail as possible, including any information you acquired when debugging. Be aware that the information you provide here can become publicly visible on the Customer Portal.

   If you do not know what caused the error, check the box labeled **I don't know what caused this problem** at the bottom of the dialog.

   Then, click **Forward**.

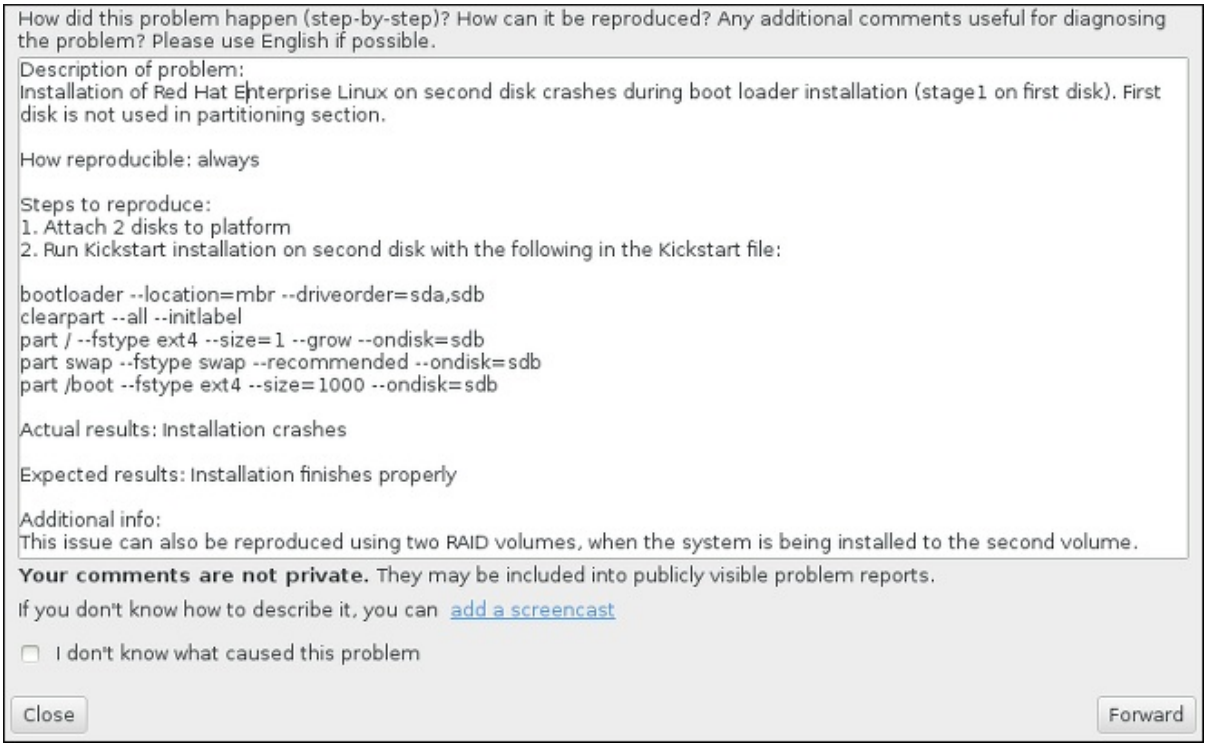


Figure 9.5. Describe the Problem

5. Next, review the information that will be sent to the Customer Portal. The explanation you provided is in the **comment** tab. Other tabs include such information as your system's host name and other details about the installation environment. You can remove any items you do not want sent to Red Hat, but be aware that providing less detail can affect the investigation of the issue.

   Click **Forward** when you finish reviewing the information to be sent.

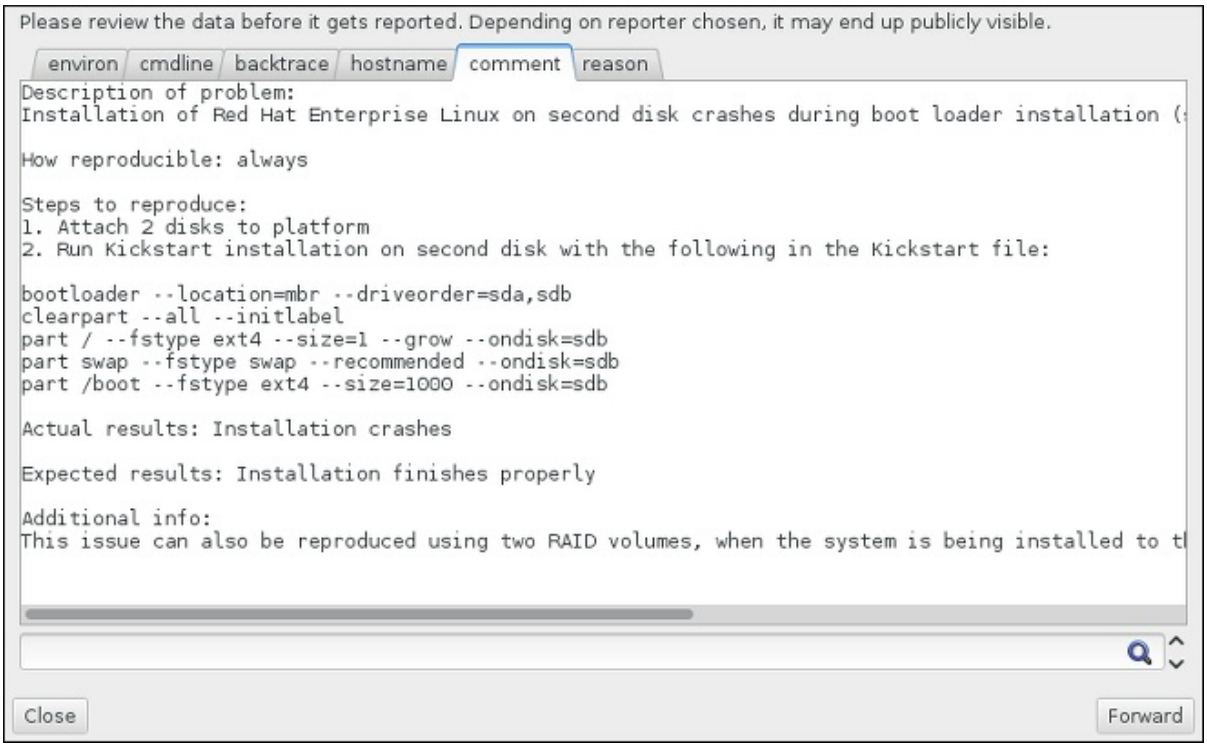


Figure 9.6. Review the Data to Be Sent

6. Review the list of files that will be sent and included in the bug report as individual attachments. These files provide system information that will assist the investigation. If you do not want to

send certain files, uncheck the box next to each one. To provide additional files that can help find the problem, click **Attach a file**.

Once you have reviewed the files to be sent, check the box labeled **I have reviewed the data and agree with submitting it**. Then, click **Forward** to send the report and attachments to the Customer Portal.

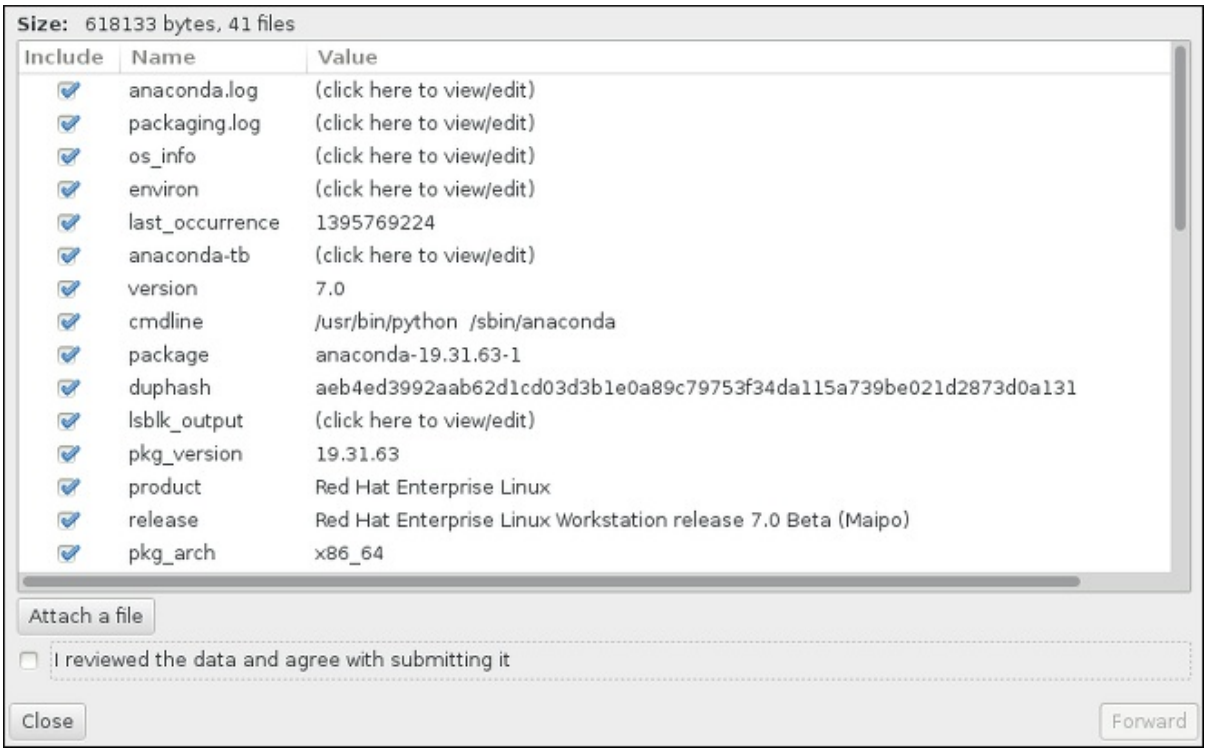


Figure 9.7. Review the Files to Be Sent

7. When the dialog reports that processing has finished, you can click **Show log** to view details of the reporting process or **Close** to return to the initial crash reporting dialog box. There, click **Quit** to exit the installation.

9.2.3. Creating Pre-installation Log Files

To debug installation problems you can set the **inst.debug** option to create log files from the environment before the installation starts. These log files contain, for example, the current storage configuration.

To set the option in the Red Hat Enterprise Linux installation boot menu:

1. Select the **Install Red Hat Enterprise Linux 7.3** entry.
2. Press the **Tab** key to edit the boot options.
3. Append **inst.debug** to the options. For example:

```
> vmlinuz ... inst.debug
```

   For further details, see Chapter 22, *Boot Options*.

4. Press **Enter** to start the setup.

The system stores the pre-installation log files in the **/tmp/pre-anaconda-logs/** directory before Anaconda starts. To access the log files:

1. Switch to the console. See Section 8.2.1, “Accessing Consoles”.
2. Change into the **/tmp/pre-anaconda-logs/** directory:

```
# cd /tmp/pre-anaconda-logs/
```

9.3. PROBLEMS AFTER INSTALLATION

9.3.1. Are You Unable to Boot With Your RAID Card?

If you have performed an installation and cannot boot your system properly, you might need to reinstall and partition your system's storage differently.

Some BIOS types do not support booting from RAID cards. After you finish the installation and reboot the system for the first time, a text-based screen showing the boot loader prompt (for example, **grub>**) and a flashing cursor might be all that appears. If this is the case, you must repartition your system and move your **/boot** partition and the boot loader outside the RAID array. The **/boot** partition and the boot loader must be on the same drive.

Once these changes have been made, you should be able to finish your installation and boot the system properly. For more information about partitioning, see Section 8.14, “Installation Destination”.

9.3.2. Trouble With the Graphical Boot Sequence

After you finish the installation and reboot your system for the first time, it is possible that the system stops responding during the graphical boot sequence, requiring a reset. In this case, the boot loader is displayed successfully, but selecting any entry and attempting to boot the system results in a halt. This usually means a problem with the graphical boot sequence; to solve this issue, you must disable graphical boot. To do this, temporarily alter the setting at boot time before changing it permanently.

Procedure 9.4. Disabling Graphical Boot Temporarily

1. Start your computer and wait until the boot loader menu appears. If you set your boot loader timeout period to 0, hold down the **Esc** key to access it.
2. When the boot loader menu appears, use your cursor keys to highlight the entry you want to boot and press the **e** key to edit this entry's options.
3. In the list of options, find the kernel line - that is, the line beginning with the keyword **linux** (or, in some cases, **linux16** or **linuxefi**). On this line, locate the **rhgb** option and delete it. The option might not be immediately visible; use the cursor keys to scroll up and down.
4. Press **F10** or **Ctrl**+**X** to boot your system with the edited options.

If the system started successfully, you can log in normally. Then you will need to disable the graphical boot permanently - otherwise you will have to perform the previous procedure every time the system boots. To permanently change boot options, do the following.

Procedure 9.5. Disabling Graphical Boot Permanently

1. Log in to the **root** account using the **su -** command:

```
$ su -
```

2. Use the **grubby** tool to find the default **GRUB2** kernel:

```
# grubby --default-kernel
/boot/vmlinuz-3.10.0-229.4.2.el7.x86_64
```

3. Use the **grubby** tool to remove the **rhgb** boot option from the default kernel, identified in the last step, in your **GRUB2** configuration. For example:

```
# grubby --remove-args="rhgb" --update-kernel /boot/vmlinuz-3.10.0-
229.4.2.el7.x86_64
```

After you finish this procedure, you can reboot your computer. Red Hat Enterprise Linux will not use the graphical boot sequence any more. If you want to enable graphical boot in the future, follow the same procedure, replacing the **--remove-args="rhgb"** parameter with the **--args="rhgb"** paramter. This will restore the **rhgb** boot option to the default kernel in your **GRUB2** configuration.

See the Red Hat Enterprise Linux 7 System Administrator's Guide for more information about working with the **GRUB2** boot loader.

9.3.3. Booting into a Graphical Environment

If you have installed the **X Window System** but are not seeing a graphical desktop environment once you log into your system, you can start it manually using the **startx** command. Note, however, that this is just a one-time fix and does not change the log in process for future log ins.

To set up your system so that you can log in at a graphical login screen, you must change the default **systemd** target to **graphical.target**. When you are finished, reboot the computer. You will presented with a graphical login prompt after the system restarts.

Procedure 9.6. Setting Graphical Login as Default

1. Open a shell prompt. If you are in your user account, become root by typing the **su -** command.
2. Change the default target to **graphical.target**. To do this, execute the following command:

```
# systemctl set-default graphical.target
```

Graphical login is now enabled by default - you will be presented with a graphical login prompt after the next reboot. If you want to reverse this change and keep using the text-based login prompt, execute the following command as **root**:

```
# systemctl set-default multi-user.target
```

For more information about targets in **systemd**, see the Red Hat Enterprise Linux 7 System Administrator's Guide.

9.3.4. No Graphical User Interface Present

If you are having trouble getting **X** (the **X Window System**) to start, it is possible that it has not been installed. Some of the preset base environments you can select during the installation, such as **Minimal install** or **Web Server**, do not include a graphical interface - it has to be installed manually.

If you want **X**, you can install the necessary packages afterwards. See the Knowledgebase article at https://access.redhat.com/site/solutions/5238 for information on installing a graphical desktop environment.

9.3.5. X Server Crashing After User Logs In

If you are having trouble with the **X** server crashing when a user logs in, one or more of your file systems can be full or nearly full. To verify that this is the problem you are experiencing, execute the following command:

```
$ df -h
```

The output will help you diagnose which partition is full - in most cases, the problem will be on the **/home** partition. The following is a sample output of the **df** command:

```
Filesystem                                Size  Used Avail Use%
Mounted on
/dev/mapper/vg_rhel-root                   20G  6.0G   13G  32% /
devtmpfs                                  1.8G     0  1.8G   0% /dev
tmpfs                                     1.8G  2.7M  1.8G   1%
/dev/shm
tmpfs                                     1.8G 1012K  1.8G   1% /run
tmpfs                                     1.8G     0  1.8G   0%
/sys/fs/cgroup
tmpfs                                     1.8G  2.6M  1.8G   1% /tmp
/dev/sda1                                 976M  150M  760M  17% /boot
/dev/dm-4                                  90G   90G     0 100% /home
```

In the above example, you can see that the **/home** partition is full, which causes the crash. You can make some room on the partition by removing unneeded files. After you free up some disk space, start **X** using the **startx** command.

For additional information about **df** and an explanation of the options available (such as the **-h** option used in this example), see the **df(1)** man page.

9.3.6. Is Your RAM Not Being Recognized?

In some cases the kernel does not recognize all of your memory (RAM), which causes the system to use less memory than is installed. You can find out how much RAM is being utilized using the **free -m** command. If the displayed total amount of memory does not match your expectations, it is likely that at least one of your memory modules is faulty. On BIOS-based systems, you can use the **Memtest86+** utility to test your system's memory - see Section 22.2.1, “Loading the Memory (RAM) Testing Mode” for details.

NOTE

Some hardware configurations have a part of the system's RAM reserved and unavailable to the main system. Notably, laptop computers with integrated graphics cards will reserve some memory for the GPU. For example, a laptop with 4 GiB of RAM and an integrated Intel graphics card will show only roughly 3.7 GiB of available memory.

Additionally, the **kdump** crash kernel dumping mechanism, which is enabled by default on most Red Hat Enterprise Linux systems, reserves some memory for the secondary kernel used in case of the primary kernel crashing. This reserved memory will also not be displayed as available when using the **free** command. For details about **kdump** and its memory requirements, see the Red Hat Enterprise Linux 7 Kernel Crash Dump Guide.

If you made sure that your memory does not have any issues, you can try and set the amount of memory manually using the **mem=** kernel option.

Procedure 9.7. Configuring the Memory Manually

1. Start your computer and wait until the boot loader menu appears. If you set your boot loader timeout period to 0, hold down the **Esc** key to access it.

2. When the boot loader menu appears, use your cursor keys to highlight the entry you want to boot and press the **e** key to edit this entry's options.

3. In the list of options, find the kernel line - that is, the line beginning with the keyword **linux** (or, in some cases, **linux16**). Append the following option to the end of this line:

   ```
   mem=xxM
   ```

   Replace *xx* with the amount of RAM you have in MiB.

4. Press **F10** or **Ctrl**+**X** to boot your system with the edited options.

5. Wait for the system to boot and log in. Then, open a command line and execute the **free -m** command again. If total amount of RAM displayed by the command matches your expectations, append the following to the line beginning with **GRUB_CMDLINE_LINUX** in the **/etc/default/grub** file to make the change permanent:

   ```
   mem=xxM
   ```

   Replace *xx* with the amount of RAM you have in MiB.

6. After you updated the file and saved it, refresh the boot loader configuration so that the change will take effect. Run the following command with root privileges:

   ```
   # grub2-mkconfig --output=/boot/grub2/grub.cfg
   ```

In **/etc/default/grub**, the above example would look similar to the following:

```
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR="$(sed 's, release.*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
```

```
GRUB_TERMINAL_OUTPUT="console"
GRUB_CMDLINE_LINUX="rd.lvm.lv=rhel/root vconsole.font=latarcyrheb-sun16
rd.lvm.lv=rhel/swap $([ -x /usr/sbin/rhcrashkernel.param ] &&
/usr/sbin/rhcrashkernel-param || :) vconsole.keymap=us rhgb quiet
mem=1024M"
GRUB_DISABLE_RECOVERY="true"
```

See the Red Hat Enterprise Linux 7 System Administrator's Guide for more information about working with the **GRUB2** boot loader.

9.3.7. Is Your System Displaying Signal 11 Errors?

A signal 11 error, commonly known as a *segmentation fault*, means that a program accessed a memory location that was not assigned to it. A signal 11 error can occur due to a bug in one of the software programs that is installed, or faulty hardware.

If you receive a fatal signal 11 error during the installation, first make sure you are using the most recent installation images, and let **Anaconda** verify them to make sure they are not corrupted. Bad installation media (such as an improperly burned or scratched optical disk) are a common cause of signal 11 errors. Verifying the integrity of the installation media is recommended before every installation.

For information about obtaining the most recent installation media, see Chapter 2, *Downloading Red Hat Enterprise Linux*. To perform a media check before the installation starts, append the **`rd.live.check`** boot option at the boot menu. See Section 22.2.2, “Verifying Boot Media” for details.

If you performed a media check without any errors and you still have issues with segmentation faults, it usually means that your system encountered a hardware error. In this case, the problem is most likely in the system's memory (RAM). This can be a problem even if you previously used a different operating system on the same computer without any errors. On BIOS-based systems, you can use the **Memtest86+** memory testing module included on the installation media to perform a thorough test of your system's memory. See Section 22.2.1, “Loading the Memory (RAM) Testing Mode” for details.

Other possible causes are beyond this document's scope. Consult your hardware manufacturer's documentation and also see the *Red Hat Hardware Compatibility List*, available online at https://hardware.redhat.com.