Red Hat

Red Hat Enterprise Linux 8

Performing a standard RHEL installation

Installing Red Hat Enterprise Linux 8 using the graphical user interface

Last Updated: 2019-05-07

Red Hat Enterprise Linux 8 Performing a standard RHEL installation

Installing Red Hat Enterprise Linux 8 using the graphical user interface

Legal Notice

Abstract

This document is for users who want to perform a standard Red Hat Enterprise Linux 8 installation using the graphical user interface.

Table of Contents

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your input on our documentation. Please let us know how we could make it better. To do so:

- For simple comments on specific passages, make sure you are viewing the documentation in the Multi-page HTML format. Highlight the part of text that you want to comment on. Then, click the **Add Feedback** pop-up that appears below the highlighted text, and follow the displayed instructions.

- For submitting more complex feedback, create a Bugzilla ticket:

  1. Go to the Bugzilla website.

  2. As the Component, use **Documentation**.

  3. Fill in the **Description** field with your suggestion for improvement. Include a link to the relevant part(s) of documentation.

  4. Click **Submit Bug**.

CHAPTER 1. INTRODUCTION

Red Hat Enterprise Linux 8 delivers a stable, secure, consistent foundation across hybrid cloud deployments with the tools needed to deliver workloads faster with less effort. It can be deployed as a guest on supported hypervisors and Cloud provider environments as well as deployed on physical infrastructure, so your applications can take advantage of innovations in the leading hardware architecture platforms.

1.1. SUPPORTED ARCHITECTURES

Red Hat Enterprise Linux supports the following architectures:

- AMD and Intel 64-bit architectures
- The 64-bit ARM architecture
- IBM Power Systems, Little Endian
- IBM Z

1.2. INSTALLATION TERMINOLOGY

This section describes Red Hat Enterprise Linux installation terminology. Different terminology can be used for the same concepts, depending on its upstream or downstream origin.

Anaconda: The operating system installer used in Fedora, Red Hat Enterprise Linux, and their derivatives. Anaconda is a set of Python modules and scripts with additional files like Gtk widgets (written in C), systemd units, and dracut libraries. Together, they form a tool that allows users to set parameters of the resulting (target) system. In this document, the term **installation program** refers to the installation aspect of **Anaconda**.

CHAPTER 2. INSTALLATION METHODS

You can install Red Hat Enterprise Linux using one of the following methods:

Quick install

Install Red Hat Enterprise Linux on AMD64, Intel 64, and 64-bit ARM architectures using the graphical user interface. The quick installation assumes that you are familiar with Red Hat Enterprise Linux and your environment, and that you can accept the default settings provided by the installation program.

Graphical install

Install Red Hat Enterprise Linux using the graphical user interface and customize the graphical settings for your specific requirements.

Automated install

Install Red Hat Enterprise Linux using Kickstart. The automated installation allows you to perform unattended operating system installation tasks.

Additional resources

- To perform a graphical installation on AMD64, Intel 64, and 64-bit ARM architectures using the graphical user interface, see Chapter 3, *Installation workflow*.
- To perform an installation on IBM Power System LC servers, see Section 8.1, “Overview”.
- To perform an installation on IBM Power System AC servers, see Section 9.1, “Overview”.
- To perform an installation on IBM Power System L servers, see Section 10.1, “Overview”.
- To perform an installation on IBM Z, see Section 11.1, “Overview of the IBM Z installation process”.
- To perform an automated install using Kickstart, see the *Performing an advanced RHEL installation* document.

2.1. PERFORMING A QUICK INSTALL ON AMD64, INTEL 64, AND 64-BIT ARM

Follow this procedure to perform a quick installation on AMD64, Intel 64, and 64-bit ARM architectures using the graphical user interface. To complete this procedure you must be familiar with Red Hat Enterprise Linux and your environment, and you must be able to accept the default settings provided by the installation program.

Prerequisites

- You have downloaded the required ISO image file. See Section 4.5, “Downloading the installation ISO image” for more information.
- You have created bootable installation media. See Section 4.6, “Creating installation media” for more information.
- You have booted the installation program and the boot menu is displayed. See Chapter 5, *Booting the installation* for more information.

Procedure

1. From the boot menu, select **Install Red Hat Enterprise Linux 8.0**

2. Press the **Enter** key on your keyboard.

3. From the **Welcome to Red Hat Enterprise Linux 8.0**window, select your language and location.

4. Click **Continue** to proceed to the **Installation Summary** window.

    NOTE

    The **Installation Summary** window is the central hub that you can use to configure the Red Hat Enterprise Linux graphical user interface. The default settings assigned by the installation program are displayed under each category.

5. From the **Installation Summary** window, accept the default **Localization** and **Software** options.

6. Select **System > Installation Destination**.

    a. From the **Local Standard Disks** pane, select the target disk.

    b. Click **Done** to accept the selection and the default setting of automatic partitioning, and return to the **Installation Summary** window.

7. Select **Network & Host Name**.

    a. Toggle the **Ethernet** switch to **ON** to enable network configuration.

        i. Optional: Select a network device and click **Configure** to update the network interface configuration.

    b. Click **Done** to accept the changes and return to the **Installation Summary** window.

8. Optional: Select **Security Policy**.

    a. Select the profile that you require, and click **Select profile**.

    b. Click **Done** to accept the changes and return to the **Installation Summary** window.

9. Optional: Select **System Purpose**.

    a. Select the role, service level agreement, and usage.

    b. Click **Done** to accept the changes and return to the **Installation Summary** window.

10. Click **Begin Installation** to start the installation.

11. From the **Configuration** window, configure a root password and create a user account.

12. When the installation process is complete, click **Reboot** to restart the system.

13. From the **Initial Setup** window, accept the licensing agreement and register your system.

Additional resources

- To learn more about how to prepare for your installation, see Chapter 4, *Preparing for your installation*.

- To learn more about installing Red Hat Enterprise Linux using the graphical user interface, and customizing the interface settings, see Section 6.1, “Graphical installation workflow”.

- To learn more about how to register your system, see Chapter 7, *Completing post-installation tasks*.

PART I. PERFORMING A GRAPHICAL INSTALL ON AMD64, INTEL 64, AND 64-BIT ARM

This section describes how to install Red Hat Enterprise Linux on AMD64, Intel 64, and 64-bit ARM architectures using the graphical user interface.

CHAPTER 3. INSTALLATION WORKFLOW

This installation workflow contains the high-level steps for installing Red Hat Enterprise Linux on AMD64, Intel 64, and 64-bit ARM architectures using the graphical user interface.

Procedure

1. Prepare for your installation by checking your system and hardware requirements, downloading an installation image file, and creating bootable installation media.

2. Boot the installation program and install Red Hat Enterprise Linux using the graphical user interface.

3. Complete post-installation tasks such as initial setup and system registration.

Additional resources

- For more information about preparing for your installation, see Chapter 4, *Preparing for your installation*.

- For more information about booting the installation program, see Chapter 5, *Booting the installation*.

- For more information about installing Red Hat Enterprise Linux using the graphical user interface, see Chapter 6, *Installing RHEL using the Graphical User Interface*

- For more information about completing post-installation tasks, see Chapter 7, *Completing post-installation tasks*.

CHAPTER 4. PREPARING FOR YOUR INSTALLATION

If you are new to Red Hat Enterprise Linux, it is important to prepare for your installation by reviewing system requirements, downloading the required installation image, and creating installation media.

4.1. RECOMMENDED STEPS

Preparing for your installation consists of several steps.

NOTE

- If you are new to Red Hat Enterprise Linux, complete steps 1 to 5.
- If you are familiar with Red Hat Enterprise Linux, complete steps 3 to 5.

Procedure

1. Check system requirements.
2. Choose an installation boot method.
3. Select and download the installation image.
4. Create bootable installation media.
5. Prepare the installation source*

*Only required for the Boot ISO (minimal install) image.

4.2. CHECK SYSTEM REQUIREMENTS

If this is a first-time installation of Red Hat Enterprise Linux it is recommended that you review the guidelines provided for system, hardware, security, memory, and RAID before installing. See Appendix A, *System requirements reference* for more information.

Additional resources

For more information about securing Red Hat Enterprise Linux, see the *Security hardening* document.

4.3. CHOOSE AN INSTALLATION BOOT METHOD

There are several methods to boot the Red Hat Enterprise Linux installation program. The method you choose depends on your installation media.

Full installation DVD or USB flash drive

Create a full installation DVD or USB flash drive using the **Binary DVD ISO** image. The DVD or USB flash drive can be used as a boot device and as an installation source for installing software packages. Due to the size of the Binary DVD ISO image, a DVD or USB flash drive are the recommended media types.

Minimal installation DVD, CD, or USB flash drive

Create a minimal installation CD, DVD, or USB flash drive using the **Boot ISO** image, which contains only the minimum files necessary to boot the system and start the installation program. The **Boot ISO** image requires an installation source that contains the required software packages.

PXE Server

A *preboot execution environment* (PXE) server allows the installation program to boot over the network. After a system boot, you must complete the installation from a different installation source, such as a local hard drive or a network location.

Additional Resources

- For instructions on how to create an installation DVD or USB flash drive, see Section 4.6, “Creating installation media” for more information.
- For instructions on how to create a bootable DVD, CD, and USB flash drive, see Section 4.7, “Preparing an installation source” for more information.
- For more information about PXE servers, see the *Performing an advanced RHEL installation* document.

4.4. SELECT THE REQUIRED INSTALLATION IMAGE

Two Red Hat Enterprise Linux 8 installation images are available from the Red Hat Customer Portal.

Binary DVD ISO image file

A full installation program that contains the BaseOS and AppStream repositories and allows you to complete the installation without additional repositories. Installing Red Hat Enterprise Linux from the Binary DVD ISO is the easiest and the recommended method of performing a standard RHEL installation.

IMPORTANT

- It is **recommended** that you use the Binary DVD ISO image file to install Red Hat Enterprise Linux 8.
- You can use a Binary DVD for IBM Z to boot the installation program using a SCSI DVD drive, or as an installation source.

Boot ISO image file

The Boot ISO image is a minimal installation that requires access to the BaseOS and AppStream repositories to install software packages. The repositories are part of the Binary DVD ISO image that is available for download from https://access.redhat.com/home. Download and unpack the Binary DVD ISO image to access the repositories.

The following table contains information about the images that are available for the supported architectures.

Table 4.1. Boot and Installation Images

Architecture	Installation DVD	Boot DVD
AMD64 and Intel 64	x86_64 Binary DVD ISO image file	x86_64 Boot ISO image file
ARM 64	AArch64 Binary DVD ISO image file	AArch64 Boot ISO image file

Architecture	Installation DVD	Boot DVD
IBM POWER	ppc64le Binary DVD ISO image file	ppc64le Boot ISO image file
IBM Z	s390x Binary DVD ISO image file	s390x Boot ISO image file

Additional Resources

- For instructions on how to access the Binary DVD ISO image repositories, see Section 4.7, “Preparing an installation source” for more information.

4.5. DOWNLOADING THE INSTALLATION ISO IMAGE

This section contains instructions about downloading a Red Hat Enterprise Linux installation image from the Red Hat Customer Portal or by using the **curl** command.

4.5.1. Downloading an ISO image from the Customer Portal

Follow this procedure to download a Red Hat Enterprise Linux 8 ISO image from the Red Hat Customer Portal.

NOTE

- Red Hat recommends using the Binary DVD ISO image to install Red Hat Enterprise Linux 8 as it contains all repositories and software packages, and does not require any additional configuration.
- If you download the Boot ISO image file, you must configure an installation source to obtain the repositories and software packages. See Section 4.7, “Preparing an installation source” for more information.

Prerequisites

- You have an active Red Hat subscription.
- You are logged in to the **Product Downloads** section of the Red Hat Customer Portal at https://access.redhat.com/downloads.

Procedure

1. From the **Product Downloads** page, select the **By Category** tab.
2. Click the **Red Hat Enterprise Linux 8** link.
   The **Download Red Hat Enterprise Linux**web page opens.
3. From the **Product Variant** drop-down menu, select the variant that you require, for example **Red Hat Enterprise Linux for x86_64**

NOTE

If you are unsure of the variant for your requirements, see http://www.redhat.com/en/technologies/linux-platforms/enterprise-linux.

4. The **Version** drop-down menu defaults to 8.0.

5. The **Architecture** drop-down menu defaults to x86_64.
   The **Product Software** tab displays the images, which include:

   - **Red Hat Enterprise Linux 8.0 Binary DVD**image.

   - **Red Hat Enterprise Linux 8.0 Boot ISO**image.

   Additional images may be available, for example, preconfigured virtual machine images, but they are beyond the scope of this document.

6. Click **Download Now** beside the ISO image that you require.

4.5.2. Downloading an ISO image using curl

Use the **curl** command to download installation images directly from a specific URL.

Prerequisites

- Verify the curl package is installed:

  - If your distribution uses the **yum** package manager:

    ```
    # yum install curl
    ```

  - If your distribution uses the **dnf** package manager:

    ```
    # dnf install curl
    ```

  - If your distribution uses the **apt** package manager:

    ```
    # apt update
    # apt install curl
    ```

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

- You have navigated to the **Product Downloads** section of the Red Hat Customer Portal at https://access.redhat.com/downloads, and selected the variant, version, and architecture that you require. You have right-clicked on the required ISO image file, and selected **Copy Link Location** to copy the URL of the ISO image file to your clipboard.

Procedure

1. On the command line, enter a suitable directory, and run the following command to download the file:

   ```
   $ curl --output directory-path/filename.iso 'copied_link_location'
   ```

Replace *directory-path* with a path to the location where you want to save the file; replace *filename.iso* with the ISO image name as displayed in the Customer Portal; replace *copied_link_location* with the link that you have copied from the Customer Portal.

4.6. CREATING INSTALLATION MEDIA

This section contains information about using the ISO image file that you downloaded in Section 4.5, “Downloading the installation ISO image” to create bootable physical installation media, such as a USB, DVD, or CD.

NOTE

By default, the **inst.stage2=** boot option is used on the installation media and is set to a specific label, for example, **inst.stage2=hd:LABEL=RHEL8\x86_64**. If you modify the default label of the file system containing the runtime image, or if you use a customized procedure to boot the installation system, you must verify that the label is set to the correct value.

4.6.1. Creating a bootable DVD or CD

You can create a bootable installation DVD or CD using burning software and a CD/DVD burner. The exact steps to produce a DVD or CD from an ISO image file vary greatly, depending on the operating system and disc burning software installed. Consult your system’s burning software documentation for the exact steps to burn a CD or DVD from an ISO image file.

WARNING

You can create a bootable DVD or CD using either the Binary DVD ISO image (full install), or the Boot ISO image (minimal install). However, the Binary DVD ISO image is larger than 4.7 GB, and as a result, it might not fit on a single-layer DVD. A dual-layer DVD or USB key is recommended when using the Binary DVD ISO image to create bootable installation media.

4.6.2. Creating a bootable USB device on Linux

Follow this procedure to create a bootable USB device on a Linux system.

Prerequisites

- You have downloaded an installation ISO image as described in Section 4.5, “Downloading the installation ISO image”.

- The **Binary DVD** ISO image is larger than 4.7 GB, so you must have a USB flash drive that is large enough to hold the ISO image.

Procedure

NOTE

This procedure is destructive and data on the USB flash drive is destroyed without a warning.

1. Connect the USB flash drive to the system.

2. Open a terminal window and run the **dmesg** command:

   ```
   $ dmesg|tail
   ```

   The **dmesg** command returns a log that details all recent events. Messages resulting from the attached USB flash drive are displayed at the bottom of the log. Record the name of the connected device.

3. Switch to user root:

   ```
   $ su -
   ```

4. Enter your root password when prompted.

5. Find the device node assigned to the drive. In this example, the drive name is **sdd**.

   ```
   # dmesg|tail
   [288954.686557] usb 2-1.8: New USB device strings: Mfr=0, Product=1, SerialNumber=2
   [288954.686559] usb 2-1.8: Product: USB Storage
   [288954.686562] usb 2-1.8: SerialNumber: 000000009225
   [288954.712590] usb-storage 2-1.8:1.0: USB Mass Storage device detected
   [288954.712687] scsi host6: usb-storage 2-1.8:1.0
   [288954.712809] usbcore: registered new interface driver usb-storage
   [288954.716682] usbcore: registered new interface driver uas
   [288955.717140] scsi 6:0:0:0: Direct-Access     Generic  STORAGE DEVICE   9228 PQ: 0
   ANSI: 0
   [288955.717745] sd 6:0:0:0: Attached scsi generic sg4 type 0
   [288961.876382] sd 6:0:0:0: sdd Attached SCSI removable disk
   ```

6. Run the **dd** command to write the ISO image directly to the USB device.

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

   Replace */image_directory/image.iso* with the full path to the ISO image file that you downloaded, and replace *device* with the device name that you retrieved with the **dmesg** command. In this example, the full path to the ISO image is **/home/testuser/Downloads/rhel-8-x86_64-boot.iso**, and the device name is **sdd**:

   ```
   # dd if=/home/testuser/Downloads/rhel-8-x86_64-boot.iso of=/dev/sdd
   ```

   NOTE

   Ensure that you use the correct device name, and not the name of a partition on the device. Partition names are usually device names with a numerical suffix. For example, **sdd** is a device name, and **sdd1** is the name of a partition on the device **sdd**.

7. Wait for the **dd** command to finish writing the image to the device. The data transfer is complete when the **#** prompt appears. When the prompt is displayed, log out of the root account and unplug the USB drive. The USB drive is now ready to be used as a boot device.

4.6.3. Creating a bootable USB device on Windows

Follow the steps in this procedure to create a bootable USB device on a Windows system. The procedure varies depending on the tool. Red Hat recommends using Fedora Media Writer, available for download at https://github.com/FedoraQt/MediaWriter/releases.

> **NOTE**
>
> Fedora Media Writer is a community product and is not supported by Red Hat. You can report any issues with the tool at https://github.com/FedoraQt/MediaWriter/issues.

Prerequisites

- You have downloaded an installation ISO image as described in Section 4.5, "Downloading the installation ISO image".
- The **Binary DVD** ISO image is larger than 4.7 GB, so you must have a USB flash drive that is large enough to hold the ISO image.

Procedure

> **NOTE**
>
> This procedure is destructive and data on the USB flash drive is destroyed without a warning.

1. Download and install Fedora Media Writer from https://github.com/FedoraQt/MediaWriter/releases.

   > **NOTE**
   >
   > To install Fedora Media Writer on Red Hat Enterprise Linux, use the pre-built Flatpak package. You can obtain the package from the official Flatpak repository Flathub.org at https://flathub.org/apps/details/org.fedoraproject.MediaWriter.

2. Connect the USB flash drive to the system.
3. Open Fedora Media Writer.
4. From the main window, click **Custom Image** and select the previously downloaded Red Hat Enterprise Linux ISO image.
5. From **Write Custom Image** window, select the drive that you want to use.
6. Click **Write to disk**. The boot media creation process starts. Do not unplug the drive until the operation completes. The operation may take several minutes, depending on the size of the ISO image, and the write speed of the USB drive.
7. When the operation completes, unmount the USB drive. The USB drive is now ready to be used as a boot device.

4.6.4. Creating a bootable USB device on Mac OS X

Follow the steps in this procedure to create a bootable USB device on a Mac OS X system.

Prerequisites

- You have downloaded an installation ISO image as described in Section 4.5, "Downloading the installation ISO image".
- The **Binary DVD** ISO image is larger than 4.7 GB, so you must have a USB flash drive that is large enough to hold the ISO image.

Procedure

> **NOTE**
>
> This procedure is destructive and data on the USB flash drive is destroyed without a warning.

1. Connect the USB flash drive to the system.
2. Identify the device path with the **diskutil list** command. The device path has the format of */dev/disknumber*, where number is the number of the disk. The disks are numbered starting at zero (0). Typically, Disk 0 is the OS X recovery disk, and Disk 1 is the main OS X installation. In the following example, the USB device 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
```

3. To identify your USB flash drive, compare the NAME, TYPE and SIZE columns to your flash drive. For example, the NAME should be the title of the flash drive icon in the **Finder** tool. You can also compare these values to those in the information panel of the flash drive.
4. 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 the command completes, the icon for the flash drive disappears from your desktop. If the icon does not disappear, you may have selected the wrong disk. Attempting to unmount the system disk accidentally returns a **failed to unmount** error.

5. Log in as root:

```
$ su -
```

6. Enter your root password when prompted.

7. 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/rdisknumber character device is faster than writing to the /dev/disknumber block device.

8. To write the */Users/user_name/Downloads/rhel-8-x86_64-boot.iso* file to the */dev/rdisk2* device, run the following command:

```
# sudo dd if=/Users/user_name/Downloads/rhel-8-x86_64-boot.iso of=/dev/rdisk2
```

9. Wait for the **dd** command to finish writing the image to the device. The data transfer is complete when the **#** prompt appears. When the prompt is displayed, log out of the root account and unplug the USB drive. The USB drive is now ready to be used as a boot device.

4.7. PREPARING AN INSTALLATION SOURCE

The Boot ISO image file does not include any repositories or software packages; it contains only the installation program and the tools required to boot the system and start the installation. This section contains information about creating an installation source for the Boot ISO image using the Binary DVD ISO image that contains the required repositories and software packages.

IMPORTANT

Creating an installation source is required only for the Boot ISO image. Red Hat recommends the **Binary DVD** ISO image as the preferred method to install Red Hat Enterprise Linux.

4.7.1. Types of installation source

You can use one of the following installation sources for minimal boot images:

- **DVD:** Burn the Binary DVD ISO image to DVD and configure the installation program to install the software packages.

- **Hard drive or USB drive:** Copy the Binary DVD ISO image to the drive and configure the installation program to install the software packages from the drive. If you use a USB drive, verify that it is connected to the system before the installation begins. The installation program cannot detect media after the installation begins.

- **Hard drive limitation**: The Binary DVD ISO image on the hard drive must be on a partition with a file system that the installation program can mount. The supported file systems are **xfs**, **ext2**, **ext3**, **ext4**, and **vfat (FAT32)**.

WARNING

On Microsoft Windows systems, the default file system used when formatting hard drives is NTFS; 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 as an installation source on Microsoft Windows, verify that you formatted the drive as FAT32, however, the FAT32 file system cannot store files larger than 4 GiB.

In Red Hat Enterprise Linux 8 you can enable installation from a repository on a local hard drive. To do so, you need to copy the content of DVD ISO image to a directory on a hard drive and then specify the directory as installation source instead of the ISO image. For example: **inst.repo=hd:<device>:<path to the repository>**

- **Network location:** Copy the Binary DVD ISO image or the installation tree (extracted contents of the Binary DVD ISO image) to a network location and perform the installation over the network using the following protocols:
  - **NFS:** The Binary DVD ISO image is in a Network File System (NFS) share.
  - **HTTPS or HTTP:** The installation tree is on a network location that is accessible over HTTP or HTTPS.

4.7.2. Specify the installation source

You can specify the installation source using any of the following methods:

- **Graphical installation:** Select the installation source in the **Installation Source** window of the graphical installation. See Section 6.5.1, “Configuring installation source” for more information.
- **Boot option:** Configure a custom boot option to specify the installation source. See Section 5.3, “Boot options” for more information.
- **Kickstart file:** Use the install command in a Kickstart file to specify the installation source. See the *Performing an advanced RHEL installation* document for more information.

4.7.3. Ports for network-based installation

The following table lists the ports that must be open on the server providing the files for each type of network-based installation.

Table 4.2. Ports for network-based installation

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

Additional resources

- See the *Securing networks* document for more information.

4.7.4. Creating an installation source on an NFS server

Follow the steps in this procedure to place the installation source on an NFS server. Use this installation method to install multiple systems from a single source, without having to connect to physical media. A network-based installation is convenient when used with a TFTP server, as it enables you to boot the installation from the network. This approach eliminates the need to create physical media and simultaneously deploys Red Hat Enterprise Linux on multiple systems.

Prerequisites

- You have downloaded a Binary DVD ISO image. See Section 4.5, “Downloading the installation ISO image” for more information.

- You have created a bootable CD, DVD, or USB device from the image file. See Section 4.6, “Creating installation media” for more information.

- You have verified that your firewall allows the server you are installing to access the remote installation source. See Section 4.7.3, “Ports for network-based installation” for more information.

Procedure

NOTE

The NFS installation method uses the Binary DVD ISO image in a Network File System server’s exported directory, which the system must be able to read. To perform an NFS-based installation, another system must act as the NFS host. The steps to configure an NFS server vary depending on the system architecture, operating system, package manager, and service manager. This procedure contains a basic outline of the process.

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

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

2. Copy the Binary DVD ISO image to a directory on the NFS server.

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

```
/exported_directory/ clients
```

4. Replace */exported_directory/* with the full path to the directory with the ISO image. Replace *clients* with the host name or IP address of the target system, the subnetwork that all target systems can use to access the ISO image, or the asterisk sign (*) if you want to allow any system 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.
   A basic configuration that makes the **/rhel8-install/** directory available as read-only to all clients is:

   ```
   /rhel8-install *
   ```

5. Save the **/etc/exports** file and exit the text editor.

6. Start the nfs service:

   ```
   # systemctl start nfs-server.service
   ```

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

   ```
   # systemctl reload nfs-server.service
   ```

   The ISO image is now accessible over NFS and ready to be used as an installation source.

NOTE

When configuring the installation source, use **nfs:** as the protocol, the server host name or IP address, the colon sign **(:)**, and the directory holding the ISO image. For example, if the server host name is **myserver.example.com** and you have saved the ISO image in **/rhel8-install/**, specify **nfs:myserver.example.com:/rhel8-install/** as the installation source.

4.7.5. Creating an installation source using HTTP or HTTPS

Follow the steps in this procedure to create an installation source 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 or HTTPS.

Prerequisites

- You have downloaded a Binary DVD ISO image. See Section 4.5, “Downloading the installation ISO image” for more information.

- You have created a bootable CD, DVD, or USB device from the image file. See Section 4.6, “Creating installation media” for more information.

- You have verified that your firewall allows the server you are installing to access the remote installation source. See Section 4.7.3, “Ports for network-based installation” for more information.

Procedure

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

```
# yum install httpd
```

WARNING

If your Apache web server configuration enables SSL security, verify that you enable only 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 use an HTTPS server with a self-signed certificate, you must boot the installation program with the **noverifyssl** option.

2. Copy the 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.
- Replace */mount_point/* with the path to the directory where you want to locate the contents of the ISO image.

4. Copy the files from the mounted image to the HTTP(S) server root. This command creates the **/var/www/html/rhel8-install/** directory with the contents of the image.

```
# cp -r /mnt/rhel8-install/ /var/www/html/
```

5. Start the **httpd** service:

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

The installation tree is now accessible and ready to be used as the installation source.

NOTE

When configuring the installation source, use **http://** or **https://** as the protocol, the server host name or IP address, and the directory that contains the files from the ISO image, relative to the HTTP server root. For example, if you are using HTTP, the server host name is **myserver.example.com**, and you have copied the files from the image to **/var/www/html/rhel8-install/**, specify **http://myserver.example.com/rhel8-install/** as the installation source.

Additional resources

- For more information about HTTP servers, see the *Deploying different types of servers* document.

CHAPTER 5. BOOTING THE INSTALLATION

Installing Red Hat Enterprise Linux from the Binary DVD ISO is the easiest and the recommended method of performing a standard RHEL installation. Other installation methods require additional setup and configuration. For example, when installing Red Hat Enterprise Linux on a large number of systems simultaneously, the best approach is to boot from a PXE server and install from a source in a shared network location.

After you have created a bootable USB, DVD, or CD you are ready to boot the Red Hat Enterprise Linux installation.

5.1. BOOTING THE INSTALLATION FROM A USB, CD, OR DVD

Follow the steps in this procedure to boot the Red Hat Enterprise Linux installation using a USB, CD, or DVD. The following steps are generic. Consult your hardware manufacturer's documentation for specific instructions.

Prerequisite

You have created bootable installation media (USB, CD or DVD). See Section 4.6, "Creating installation media" for more information.

Procedure

1. Power off the system to which you are installing Red Hat Enterprise Linux.
2. Disconnect any drives from the system.
3. Power on the system.
4. Insert the bootable installation media (USB, DVD, or CD).
5. Power off the system but do not remove the boot media.
6. Power on the system.

   NOTE

   You might need to press a specific key or combination of keys to boot from the media or configure the Basic Input/Output System (BIOS) of your system to boot from the media. For more information, see the documentation that came with your system.

7. The **Red Hat Enterprise Linux boot** window opens and displays information about a variety of available boot options.
8. Use the arrow keys on your keyboard to select the boot option that you require, and press **Enter** to select the boot option. The **Welcome to Red Hat Enterprise Linux**window opens and you can install Red Hat Enterprise Linux using the graphical user interface.

   NOTE

   The installation program automatically begins if no action is performed in the boot window within 60 seconds.

9. Optional: For UEFI-based systems, press **E** to edit the available boot options. For BIOS-based systems, press the **Tab** key on your keyboard to edit the available boot options. The boot window enters edit mode and you can change the predefined command line to add or remove boot options.

    a. Press **Enter** to confirm your choice.

Additional Resources

- For more information about installing Red Hat Enterprise Linux using the Graphical User Interface, see Chapter 6, *Installing RHEL using the Graphical User Interface* .
- For more information about the list of available boot options you can use on the boot command line, see Section 5.3, "Boot options".

5.2. BOOTING THE INSTALLATION FROM A NETWORK USING PXE

Follow the steps in this procedure to boot the Red Hat Enterprise Linux installation from a network using PXE.

Prerequisites

- You have configured a TFTP server, and there is a network interface in your system that supports PXE. See **Additional resources** for more information.
- You have configured your system to boot from the network interface. This option is in the BIOS, and can be labeled **Network Boot** or **Boot Services**.
- You have verified that the BIOS is configured to boot from the specified 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. When you have properly enabled PXE booting, the system can boot the Red Hat Enterprise Linux installation program without any other media.

Procedure

NOTE

To boot the installation process from a network using PXE, you must use a physical network connection, for example, Ethernet. You cannot boot the installation process with a wireless connection.

1. Verify 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 system.
   Depending on your hardware, some network setup and diagnostic information can be displayed before your system connects to a PXE server. When connected, a menu is displayed according to the PXE server configuration.
3. Press the number key that corresponds to the option that you require.

> NOTE
>
> In some instances, boot options are not displayed. If this occurs, press the **Enter** key on your keyboard or wait until the boot window opens.

The **Red Hat Enterprise Linux boot** window opens and displays information about a variety of available boot options.

4. Use the arrow keys on your keyboard to select the boot option that you require, and press **Enter** to select the boot option. The **Welcome to Red Hat Enterprise Linux**window opens and you can install Red Hat Enterprise Linux using the graphical user interface.

> NOTE
>
> The installation program automatically begins if no action is performed in the boot window within 60 seconds.

5. Optional: For UEFI-based systems, press **E** to edit the available boot options. For BIOS-based systems, press the **Tab** key on your keyboard to edit the available boot options. The boot window enters edit mode and you can change the predefined command line to add or remove boot options.
   a. Press **Enter** to confirm your choice.

Additional Resources

- For information about installing Red Hat Enterprise Linux using the Graphical User Interface, see Chapter 6, *Installing RHEL using the Graphical User Interface* .
- For information about how to prepare to install Red Hat Enterprise Linux from the network using PXE, see the *Performing an advanced RHEL installation* document.
- For more information about the list of available boot options you can use on the boot command line, see Section 5.3, “Boot options”.

5.3. BOOT OPTIONS

This section contains information about some of the boot options that you can use to modify the default behavior of the installation program. For a full list of boot options, see the upstream boot option content. For Kickstart and advanced boot options, see the *Performing an advanced RHEL installation* document.

5.3.1. Types of boot options

There are two types of boot options; those with an equals "=" sign, and those without an equals "=" sign. Boot options are appended to the boot command line and multiple options must be separated by a single space. Boot options that are specific to the installation program always start with **inst**.

Options with an equals "=" sign

You must specify a value for boot options that use the **=** symbol. For example, the **inst.vncpassword=** option must contain a value, in this case, a password. The correct syntax for this example is **inst.vncpassword=password**.

Options without an equals "=" sign

This boot option does not accept any values or parameters. For example, the **rd.live.check** option forces the installation program to verify the installation media before starting the installation. If this boot option is present, the verification is performed; if the boot option is not present, the verification is skipped.

5.3.2. Editing boot options

This section contains information about the different ways that you can edit boot options from the boot menu. The boot menu opens after you boot the installation media.

Editing the boot: prompt

When using the **boot:** prompt, the first option must always specify the installation program image file that you want to load. In most cases, you can specify the image using the keyword. You can specify additional options according to your requirements.

Prerequisites

- You have created bootable installation media (USB, CD or DVD).
- You have booted the installation from the media, and the installation boot menu is open.

Procedure

1. With the boot menu open, press the **Esc** key on your keyboard.
2. The **boot:** prompt is now accessible.
3. Press the **Tab** key on your keyboard to display the help commands.
4. Press the **Enter** key on your keyboard to start the installation with your options. To return from the **boot:** prompt to the boot menu, restart the system and boot from the installation media again.

NOTE

The **boot:** prompt also accepts **dracut** kernel options. A list of options is available in the **dracut.cmdline(7)** man page.

Editing the > prompt

You can use the **>** prompt to edit predefined boot options. For example, select **Test this media and install Red Hat Enterprise Linux 8.0.0** from the boot menu to display a full set of options.

NOTE

This procedure is for BIOS-based AMD64 and Intel 64 systems.

Prerequisites

- You have created bootable installation media (USB, CD or DVD).
- You have booted the installation from the media, and the installation boot menu is open.

Procedure

1. From the boot menu, select an option and press the **Tab** key on your keyboard. The **>** prompt is accessible and displays the available options.
2. Append the options that you require to the **>** prompt.
3. Press the **Enter** key on your keyboard to start the installation.
4. Press the **Esc** key on your keyboard to cancel editing and return to the boot menu.

Editing the GRUB2 menu
The GRUB2 menu is available on UEFI-based AMD64, Intel 64, and 64-bit ARM systems.

Prerequisites

- You have created bootable installation media (USB, CD or DVD).
- You have booted the installation from the media, and the installation boot menu is open.

Procedure

1. From the boot menu window, select an option and press the **e** key on your keyboard.
2. When you finish editing, press **F10** or **Ctrl+X** on your keyboard to start the installation using the specified options.

5.3.3. Installation source boot options

This section contains information about the various installation source boot options.

inst.repo=

The **inst.repo=** boot option specifies the installation source, that is, the location of images and packages. For example: **inst.repo=cdrom**. The target of the **inst.repo=** option must be one of the following installation media:

- an installable tree, which is a directory structure containing the installation program images, packages, and repository data as well as a valid **.treeinfo** file
- a DVD (a physical disk present in the system DVD drive)
- an ISO image of the full Red Hat Enterprise Linux installation DVD, placed on a hard drive or a network location accessible to the system.
  You can use the **inst.repo=** boot option to configure different installation methods using different formats. The following table contains details of the **inst.repo=** boot option syntax:

Table 5.1. Installation source boot options

Installation source	Boot option format
Any CD/DVD drive	**inst.repo=cdrom**
Specific CD/DVD drive	**inst.repo=cdrom:device**
Hard Drive	**inst.repo=hd:device:/path**

Installation source	Boot option format
HMC	**inst.repo=hmc**
HTTP Server	**inst.repo=http://host/path**
HTTPS Server	**inst.repo=https://host/path**
NFS Server	**inst.repo=nfs:[options:]server:/path**

NOTE

The NFS Server option uses NFS protocol version 3 by default. To use a different version, add **+nfsvers=X** to the option.

You can set disk device names with the following formats:

- Kernel device name, for example **/dev/sda1** or **sdb2**
- File system label, for example **LABEL=Flash** or **LABEL=RHEL8**
- File system UUID, for example **UUID=8176c7bf-04ff-403a-a832-9557f94e61db**
  Non-alphanumeric characters must be represented as **\xNN**, where *NN* is the hexadecimal representation of the character. For example, **\x20** is a white space **(" ")**.

inst.stage2=

The **inst.stage2=** boot option specifies the location of the installation program runtime image. This option expects a path to a directory containing a valid **.treeinfo** file. The location of the runtime image is read from the **.treeinfo** file. If the **.treeinfo** file is not available, the installation program attempts to load the image from **LiveOS/squashfs.img**.
You can use the **inst.stage2=** boot option multiple times to specify multiple HTTP or HTTPS sources. For example:

```
inst.stage2=host1/install.img inst.stage2=host2/install.img
inst.stage2=host3/install.img
```

NOTE

By default, the **inst.stage2=** boot option is used on the installation media and is set to a specific label, for example, **inst.stage2=hd:LABEL=RHEL-8-0-0-BaseOS-x86_64**. If you modify the default label of the file system containing the runtime image, or if you use a customized procedure to boot the installation system, you must verify that the **inst.stage2=** boot option is set to the correct value.

inst.dd=

The **inst.dd=** boot option is used to perform a driver update during the installation. See the *Performing an advanced RHEL installation* document for information on how to update drivers during installation.

inst.repo=hmc

When booting from a Binary DVD, the installation program prompts you to enter additional kernel parameters. To set the DVD as an installation source, append **inst.repo=hmc** to the kernel parameters. The installation program then enables **SE** and **HMC** file access, fetches the images for stage2 from the DVD, and provides access to the packages on the DVD for software selection. This option eliminates the requirement of an external network setup and expands the installation options.

Additional resources

- For a full list of boot options, see the upstream boot option content.

5.3.4. Network boot options

This section contains information about commonly used network boot options.

NOTE

Initial network initialization is handled by **dracut**. For a complete list, see the **dracut.cmdline(7)** man page.

ip=

Use the **ip=** boot option to configure one or more network interfaces. To configure multiple interfaces, you can use the **ip** option multiple times - once for each interface. If you configure multiple interfaces, you must specify a primary boot interface using the **bootdev** option. Alternatively, you can use the **ip** option once, and then use Kickstart to set up further interfaces. This option accepts several different formats. The following tables contain information about the most common options.

NOTE

In the following tables:

- The **ip** parameter specifies the client IP address. You can specify IPv6 addresses in square brackets, for example, [2001:DB8::1].
- The **gateway** parameter is the default gateway. IPv6 addresses are also accepted.
- The **netmask** parameter is the netmask to be used. This can be either a full netmask (for example, 255.255.255.0) or a prefix (for example, 64).
- The **hostname** parameter is the host name of the client system. This parameter is optional.

Table 5.2. Network interface configuration boot option formats

Configuration method	Boot option format
Automatic configuration of any interface	**ip=method**
Automatic configuration of a specific interface	**ip=interface:method**
Static configuration	**ip=ip::gateway:netmask:hostname:interface:none**

Configuration method	Boot option format
Automatic configuration of a specific interface with an override	**ip=ip::gateway:netmask:hostname:interface:method:mtu**

NOTE

The method **automatic configuration of a specific interface with an override** brings up the interface using the specified method of automatic configuration, such as **dhcp**, but overrides the automatically-obtained IP address, gateway, netmask, host name or other specified parameters. All parameters are optional, so specify only the parameters that you want to override.

The **method** parameter can be any of the following:

Table 5.3. Automatic interface configuration methods

Automatic configuration method	Value
DHCP	**dhcp**
IPv6 DHCP	**dhcp6**
IPv6 automatic configuration	**auto6**
iSCSI Boot Firmware Table (iBFT)	**ibft**

NOTE

- If you use a boot option that requires network access, such as **inst.ks=http://host:/path**, without specifying the ip option, the installation program uses **ip=dhcp**.
- To connect to an iSCSI target automatically, you must activate a network device for accessing the target. The recommended way to activate a network is to use the **ip=ibft** boot option.

nameserver=

The **nameserver=** option specifies the address of the name server. You can use this option multiple times.

rd.neednet=

Typically, **ip=** options are applied only if the network is required by the installation (based on any other boot options that are used). You can use **rd.neednet=1** to explicitly force the application of **ip=** options.

bootdev=

The **bootdev=** option specifies the boot interface. This option is mandatory if you use more than one **ip** option.

ifname=

The **ifname=** options assigns an interface name to a network device with a given MAC address. You can use this option multiple times. The syntax is **ifname=interface:MAC**. For example:

```
ifname=eth0:01:23:45:67:89:ab
```

NOTE

The **ifname=** option is the only supported way to set custom network interface names during installation.

inst.dhcpclass=

The **inst.dhcpclass=** option specifies the DHCP vendor class identifier. The **dhcpd** service sees this value as **vendor-class-identifier**. The default value is **anaconda-$(uname -srm)**.

inst.waitfornet=

Using the **inst.waitfornet=SECONDS** boot option causes the installation system to wait for network connectivity before installation. The value given in the **SECONDS** argument specifies the maximum amount of time to wait for network connectivity before timing out and continuing the installation process even if network connectivity is not present.

vlan=

Use the **vlan=** option to configure a Virtual LAN (VLAN) device on a specified interface with a given name. The syntax is **vlan=name:interface**. For example:

```
vlan=vlan5:em1
```

This configures a VLAN device named **vlan5** on the em1 interface. The name can take the following forms:

Table 5.4. VLAN device naming conventions

Naming scheme	Example
VLAN_PLUS_VID	**vlan0005**
VLAN_PLUS_VID_NO_PAD	**vlan5**
DEV_PLUS_VID	**em1.0005**
DEV_PLUS_VID_NO_PAD	**em1.5**

bond=

Use the **bond=** option to configure a bonding device with the following syntax: **bond=name[:slaves][:options]**. Replace *name* with the bonding device name, *slaves* with a comma-separated list of physical (ethernet) interfaces, and *options* with a comma-separated list of bonding options. For example:

```
bond=bond0:em1,em2:mode=active-backup,tx_queues=32,downdelay=5000
```

For a list of available options, execute the **modinfo** bonding command. Using this option without any parameters assumes **bond=bond0:eth0,eth1:mode=balance-rr**.

team=

Use the **team=** option to configure a team device with the following syntax: **team=master:slaves**. Replace *master* with the name of the master team device and *slaves* with a comma-separated list of physical (ethernet) devices to be used as slaves in the team device. For example:

```
team=team0:em1,em2
```

Additional resources

- For a full list of boot options, see the upstream boot option content.
- For more information about networking, see the *Configuring and managing networking* document.

5.3.5. Console boot options

This section contains information about configuring boot options for your console, monitor display, and keyboard.

console=

Use the **console=** option to specify a device that you want to use as the primary console. For example, to use a console on the first serial port, use **console=ttyS0**. Use this option in conjunction with the **inst.text** option. You can use the **console=** option multiple times. If you do, the boot message is displayed on all specified consoles, but only the last one is used by the installation program. For example, if you specify **console=ttyS0 console=ttyS1**, the installation program uses **ttyS1**.

noshell

Use the **noshell** option to disable access to the root shell during installation. This is useful with Kickstart installations.

inst.lang=

Use the **inst.lang=** option to set the language that you want to use during the installation. **locale -a** or **localectl list-locales** returns a list of locales.

inst.geoloc=

Use the **inst.geoloc=** option to configure geolocation usage in the installation program. Geolocation is used to preset the language and time zone, and uses the following syntax: **inst.geoloc=value**. The **value** can be any of the following parameters:

Table 5.5. Values for the inst.geoloc boot option

Value	Boot option format
Disable geolocation	**inst.geoloc=0**
Use the Fedora GeoIP API	**inst.geoloc=provider_fedora_geoip**

Value	Boot option format
Use the Hostip.info GeoIP API	**inst.geoloc=provider_hostip**

If you do not specify the **inst.geoloc=** option, the installation program uses **provider_fedora_geoip**.

inst.keymap=

Use the **inst.keymap=** option to specify the keyboard layout that you want to use for the installation.

inst.text

Use the **inst.text** option to force the installation program to run in text mode instead of graphical mode.

inst.cmdline

Use the **inst.cmdline** option to force the installation program to run in command-line mode. This mode does not allow any interaction, and you must specify all options in a Kickstart file or on the command line.

inst.graphical

Use the **inst.graphical** option to force the installation program to run in graphical mode. This mode is the default.

inst.resolution=

Use the **inst.resolution=** option to specify the screen resolution in graphical mode. The format is **NxM**, where *N* is the screen width and *M* is the screen height (in pixels). The lowest supported resolution is 800x600.

inst.xdriver=

Use the **inst.xdriver=** option to specify the name of the X driver that you want to use both during installation and on the installed system.

inst.usefbx

Use the **inst.usefbx** option to prompt the installation program to use the frame buffer X driver instead of a hardware-specific driver. This option is equivalent to **inst.xdriver=fbdev**.

modprobe.blacklist=

Use the **modprobe.blacklist=** option to blacklist or completely disable one or more drivers. Drivers (mods) that you disable using this option cannot load when the installation starts, and after the installation finishes, the installed system retains these settings. You can find a list of the blacklisted drivers in the **/etc/modprobe.d/** directory. Use a comma-separated list to disable multiple drivers. For example:

```
modprobe.blacklist=ahci,firewire_ohci
```

inst.sshd=0

By default, the **sshd** option is automatically started only on the IBM Z architecture. On other architectures, **sshd** is not started unless you use the **inst.sshd** option. Use the **inst.sshd=0** option to prevent **sshd** from starting automatically on IBM Z.

inst.sshd

Use the **inst.sshd** option to start the **sshd** service during installation, so that you can connect to the system during the installation using SSH, and monitor the installation progress. For more information about SSH, see the **ssh(1)** man page. By default, the **sshd** option is automatically started only on the IBM Z architecture. On other architectures, **sshd** is not started unless you use the **inst.sshd** option.

NOTE

During installation, the root account has no password by default. You can set a root password during installation with the **sshpw** Kickstart command.

inst.kdump_addon=

Use the **inst.kdump_addon=** option to enable or disable the Kdump configuration screen (add-on) in the installation program. This screen is enabled by default; use **inst.kdump_addon=off** to disable it. Disabling the add-on disables the Kdump screens in both the graphical and text-based interface as well as the **%addon com_redhat_kdump** Kickstart command.

Additional resources

- For a full list of boot options, see the upstream boot option content.

5.3.6. Debug boot options

This section contains information about the options that you can use when debugging issues.

inst.rescue=

Use the **inst.rescue=** option to run the rescue environment. The option is useful for trying to diagnose and fix systems.

inst.updates=

Use the **inst.updates=** option to specify the location of the **updates.img** file that you want to apply during installation. There are a number of sources for the updates.

Updates from a network

The easiest way to use **inst.updates=** is to specify the network location of **updates.img**. This does not require any modification to the installation tree. To use this method, edit the kernel command line to include **inst.updates**, for example:

```
inst.updates=http://some.website.com/path/to/updates.img
```

Updates from a disk image

You can also save an **updates.img** on a floppy drive or a USB key. This can be done only with an **ext2** filesystem type of **updates.img**. To save the contents of the image on your floppy drive, insert the floppy disc and run the following command:

```
dd if=updates.img of=/dev/fd0 bs=72k count=20
```

To use a USB key or flash media, replace **/dev/fd0** with the device name of your USB key.

Updates from an installation tree

If you are using a CD, hard drive, or HTTP install, you can save the **updates.img** in the installation tree so that all installations can detect the .img. Save the file in the **images/** directory. The file name must be **updates.img**.

For NFS installs, there are two options: You can either save the image in the **images/** directory, or in the **RHupdates/** directory in the installation tree.

inst.loglevel=

Use the **inst.loglevel=** option to specify the minimum level of messages logged on a terminal. This concerns only terminal logging; log files always contain messages of all levels. Possible values for this option from the lowest to highest level are: **debug**, **info**, **warning**, **error** and **critical**. The default value is **info**, which means that by default, the logging terminal displays messages ranging from **info** to **critical**.

inst.syslog=

When installation starts, the **inst.syslog=** option sends log messages to the **syslog** process on the specified host. The remote **syslog** process must be configured to accept incoming connections.

inst.virtiolog=

Use the **inst.virtiolog=** option to specify the virtio port (a character device at **/dev/virtio-ports/name**) that you want to use for forwarding logs. The default value is **org.fedoraproject.anaconda.log.0**; if this port is present, it is used.

inst.nokill

The **inst.nokill** option is a debugging option that prevents the installation program from rebooting when a fatal error occurs, or at the end of the installation process. Use the **inst.nokill** option to capture installation logs which would be lost upon reboot.

Additional resources

- For a full list of boot options, see the upstream boot option content.

CHAPTER 6. INSTALLING RHEL USING THE GRAPHICAL USER INTERFACE

This section contains information about installing Red Hat Enterprise Linux using the Graphical User Interface (GUI). The GUI is the preferred method of installing Red Hat Enterprise Linux when you boot the system from a CD, DVD, or USB flash drive, or from a network using PXE.

NOTE

There may be some variance between the online help and the content that is published on the Customer Portal. For the latest updates, see the installation content on the Customer Portal.

6.1. GRAPHICAL INSTALLATION WORKFLOW

Complete the following steps to install Red Hat Enterprise Linux using the graphical user interface:

Steps

1. Configure language and location settings. See Section 6.2, “Configuring language and location settings” for more information.

2. Configure localization settings. See Section 6.4, “Configuring localization options” for more information.

3. Select the installation source and software packages that you require. See Section 6.5, “Configuring software options” for more information.

4. Configure installation destination, KDUMP, network, security policy, and system purpose. See Section 6.6, “Configuring system options” for more information.

5. Configure storage. See Section 6.7, “Configuring storage devices” for more information.

6. Start the installation and create a user account and password. See Section 6.9, “Starting the installation program” for more information.

7. Complete the graphical installation. See Section 6.9.4, “Graphical installation complete” for more information.

NOTE

When installing from a network location, you must configure the network before you can select the software packages that you want to install.

6.2. CONFIGURING LANGUAGE AND LOCATION SETTINGS

The installation program uses the language that you select during installation, and on the installed system.

Prerequisites

1. You created installation media. See Section 4.6, “Creating installation media” for more information.

2. You specified an installation source if you are using the Boot ISO image file. See Section 4.7, “Preparing an installation source” for more information.

3. You booted the installation. See Chapter 5, *Booting the installation* for more information.

Procedure

1. From the left-hand pane of the **Welcome to Red Hat Enterprise Linux**window, select a language. Alternatively, type your preferred language into the **Search** field.

   #### NOTE

   A language is pre-selected by default. If network access is configured, that is, if you booted from a network server instead of local media, the pre-selected language is determined by the automatic location detection feature of the **GeoIP** module. If you used the **inst.lang=** option on the boot command line or in your PXE server configuration, then the language that you define with the boot option is selected.

2. From the right-hand pane of the **Welcome to Red Hat Enterprise Linux**window, select a location specific to your region.

3. Click **Continue** to proceed to the Section 6.3, “The Installation Summary window” window.

   #### IMPORTANT

   If you are installing a pre-release version of Red Hat Enterprise Linux, a warning message is displayed about the pre-release status of the installation media. Click **I want to proceed**to continue with the installation, or **I want to exit**to quit the installation and reboot the system.

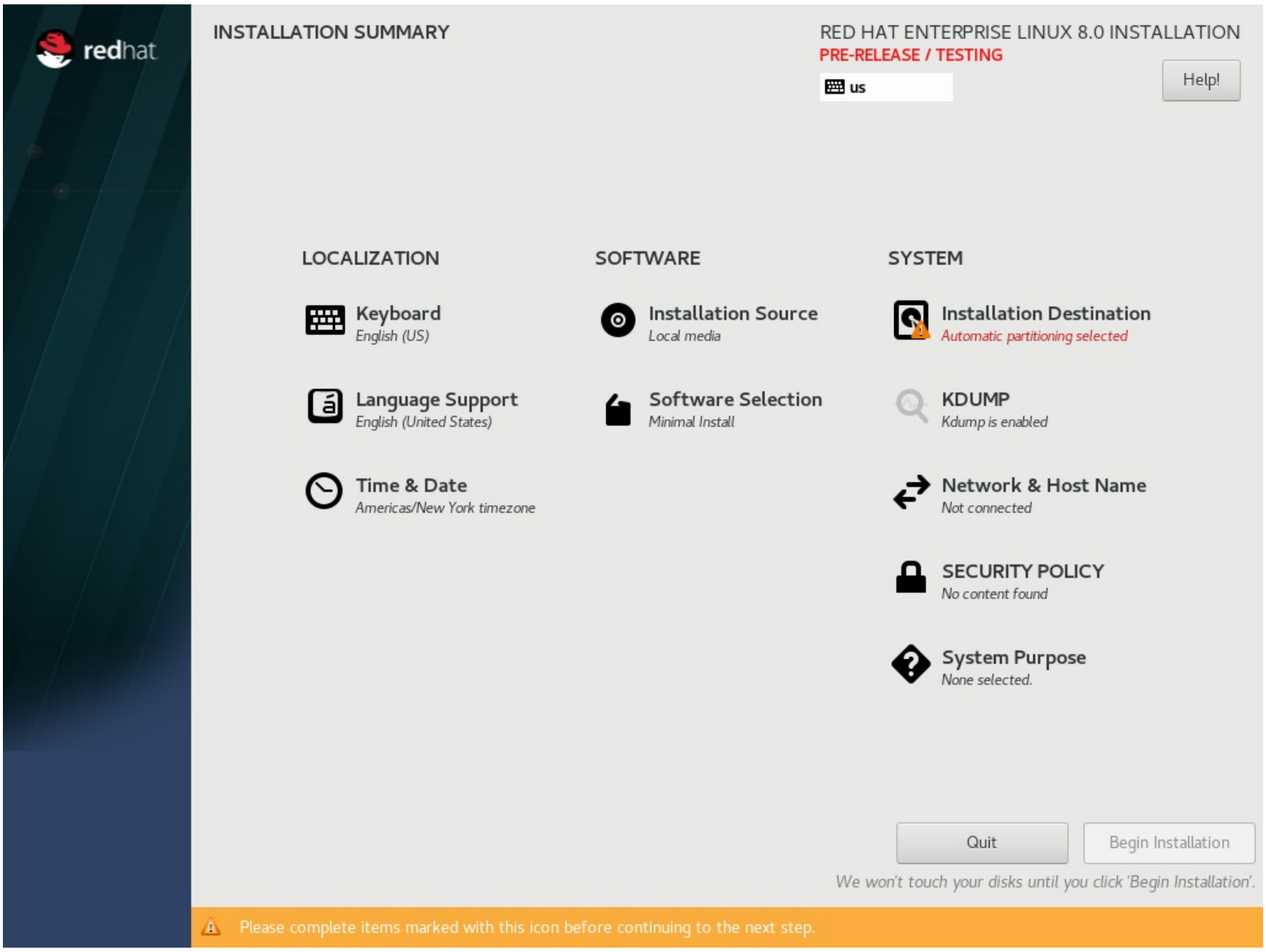
Additional resources

For information about how to change language and location settings during the installation program, see Section 6.4, “Configuring localization options”

6.3. THE INSTALLATION SUMMARY WINDOW

The **Installation Summary** window is the central location for the Red Hat Enterprise Linux 8 installation program.

Figure 6.1. Installation summary



INSTALLATION SUMMARY

RED HAT ENTERPRISE LINUX 8.0 INSTALLATION

PRE-RELEASE / TESTING

us

LOCALIZATION

Keyboard
English (US)

Language Support
English (United States)

Time & Date
Americas/New York timezone

SOFTWARE

Installation Source
Local media

Software Selection
Minimal Install

SYSTEM

Installation Destination
Automatic partitioning selected

KDUMP
Kdump is enabled

Network & Host Name
Not connected

SECURITY POLICY
No content found

System Purpose
None selected.

We won't touch your disks until you click 'Begin Installation'.

Please complete items marked with this icon before continuing to the next step.

The **Installation Summary** window contains three categories:

- **LOCALIZATION**: You can configure Keyboard, Language Support, and Time and Date.
- **SOFTWARE**: You can configure Installation Source and Software Selection.
- **SYSTEM**: You can configure Installation Destination, KDUMP, Network and Host Name, Security Policy, and System Purpose.

A category can have a different status depending on where it is in the installation program.

Table 6.1. Category status

Category status	Status	Description
Warning symbol type 1	Yellow triangle with an exclamation mark and red text	Requires attention before installation. For example, **Installation Destination** requires attention as you must confirm the default automatic partitioning variant.

Category status	Status	Description
Warning symbol type 2	Grayed out and with a warning symbol (yellow triangle with an exclamation mark)	The installation program is configuring a category and you must wait for it to finish before accessing the window.

NOTE

A warning message is displayed at the bottom of the **Installation Summary** window and the **Begin Installation** button is disabled until you configure all of the required categories.

Additional resources

- For information about how to configure Localization settings, see Section 6.4, "Configuring localization options"
- For information about how to configure Software settings, see Section 6.5, "Configuring software options"
- For information about how to configure System settings, see Section 6.6, "Configuring system options"

6.4. CONFIGURING LOCALIZATION OPTIONS

This section contains information about configuring your keyboard, language support, and time and date settings.

IMPORTANT

If you use a layout that cannot accept Latin characters, such as **Russian**, add the **English (United States)** layout and configure a keyboard combination to switch between the two layouts. If you select only a layout that does not have 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.

6.4.1. Configuring keyboard, language, and time and date settings

NOTE

Keyboard, Language, and Time and Date Settings are configured by default as part of Section 6.2, "Configuring language and location settings". To change any of the settings, complete the following steps, otherwise proceed to Section 6.5, "Configuring software options".

Procedure: Configuring keyboard settings

1. From the **Installation Summary** window, click **Keyboard**. The default layout depends on the option selected in Section 6.2, "Configuring language and location settings".
   a. Click **+** to open the **Add a Keyboard Layout** window and change to a different layout.

b. Select a layout by browsing the list or use the **Search** field.

c. Select the required layout and click **Add**. The new layout appears under the default layout.

d. Click **Options** to optionally configure a keyboard switch that you can use to cycle between available layouts. The **Layout Switching Options** window opens.

e. To configure key combinations for switching, select one or more key combinations and click **OK** to confirm your selection.

NOTE

When you select a layout, click the **Keyboard** button to open a new dialog box that displays a visual representation of the selected layout.

f. Click **Done** to apply the settings and return to Section 6.3, "The Installation Summary window".

Procedure: Configuring language settings

1. From the **Installation Summary** window, click **Language Support**. The **Language Support** window opens. The left pane lists the available language groups. If at least one language from a group is configured, a check mark is displayed and the supported language is highlighted.

    a. From the left pane, click a group to select additional languages, and from the right pane, select regional options. Repeat this process for languages that you require.

    b. Click **Done** to apply the changes and return to Section 6.3, "The Installation Summary window".

Procedure: Configuring time and date settings

1. From the **Installation Summary** window, click **Time & Date**. The **Time & Date** window opens.

    NOTE

    The **Time & Date** settings are configured by default based on the settings you selected in Section 6.2, "Configuring language and location settings".

    The list of cities and regions come from the Time Zone Database (**tzdata**) public domain that is maintained by the Internet Assigned Numbers Authority (IANA). Red Hat can not add cities or regions to this database. You can find more information at the IANA official website.

    a. From the **Region** drop-down menu, select a region.

    NOTE

    Select **Etc** as your region to configure a time zone relative to Greenwich Mean Time (GMT) without setting your location to a specific region.

    b. From the **City** drop-down menu, select the city, or the city closest to your location in the same time zone.

c. Toggle the **Network Time** switch to enable or disable network time synchronization using the Network Time Protocol (NTP).

> NOTE
>
> Enabling the Network Time switch keeps your system time correct as long as the system can access the internet. By default, one NTP pool is configured; you can add a new option, or disable or remove the default options by clicking the gear wheel button next to the **Network Time** switch.

d. Click **Done** to apply the changes and return to Section 6.3, "The Installation Summary window".

> NOTE
>
> If you disable network time synchronization, the controls at the bottom of the window become active, allowing you to set the time and date manually.

6.5. CONFIGURING SOFTWARE OPTIONS

This section contains information about configuring your installation source and software selection settings, and activating a repository.

6.5.1. Configuring installation source

Follow the steps in this procedure to configure the Binary DVD ISO image as the installation source, which is the **recommended** method of installing Red Hat Enterprise Linux.

Prerequisites

- You have downloaded the Binary DVD ISO image as detailed in Section 4.5, "Downloading the installation ISO image".
- You have created bootable installation media as detailed in Section 4.6, "Creating installation media".
- The **Installation Summary** window is open.

> NOTE
>
> When the **Installation Summary** window first opens, the installation program attempts to configure an installation source based on the type of media that was used to boot the system. The full Red Hat Enterprise Linux Server DVD configures the source as local media.

Procedure

1. From the **Installation Summary** window, click **Installation Source**. The **Installation Source** window opens.

   a. Review the **Auto-detected installation** section to verify the details. This option is selected by default if you started the installation program from media containing an installation source, for example, a DVD.

b. Click **Verify** to check the media integrity.

c. Review the **Additional repositories** section and note that the **Appstream** checkbox is selected by default.

IMPORTANT

- **No additional configuration is necessary as the BaseOS and Appstream repositories are installed as part of the full installation image.**
- **Do not disable the Appstream repository check box if you want a full Red Hat Enterprise Linux 8 installation.**

2. Select the **On the network** option to download and install packages from a network location instead of local media.

NOTE

- If you do not want to download and install additional repositories from a network location, proceed to Section 6.5.2, "Configuring software selection".
- This option is available only when a network connection is active. See Section 6.6.3, "Configuring network and host name options" for information about how to configure network connections in the GUI.

a. Select the **On the network** drop-down menu to specify the protocol for downloading packages. This setting depends on the server that you want to use.

WARNING

The Appstream repository check box is disabled if you select **On the network** and then decide to revert to **Auto-detected installation**. You must select the Appstream check box to enable the Appstream repository.

b. Type the server address (without the protocol) into the address field. If you choose NFS, a second input field opens where you can specify custom **NFS mount options**. This field accepts options listed in the **nfs(5)** man page.

IMPORTANT

When selecting an NFS 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
```

NOTE

The following steps are optional and are only required if you use a proxy for network access.

c. Click **Proxy setup...** to configure a proxy for an HTTP or HTTPS source.

d. Select the **Enable HTTP proxy** check box and type the URL into the **Proxy Host** field.

e. Select the **Use Authentication** check box if the proxy server requires authentication.

f. Type in your user name and password.

g. Click **OK** to finish the configuration and exit the **Proxy Setup...** dialog box.

NOTE

If your HTTP or HTTPS URL refers to a repository mirror menu, select the required option from the **URL type** drop-down list. All environments and add-ons are available for selection when you finish configuring the sources.

3. Click **+** to add a repository.

4. Click **–** to delete a repository.

5. Click the arrow icon to revert the current entries to the setting when you opened the **Installation Source** window.

6. To activate or deactivate a repository, click the check box in the **Enabled** column for each entry in the list.

NOTE

You can name and configure your additional repository in the same way as the primary repository on the network.

7. Click **Done** to apply the settings and return to the **Installation Summary** window.

6.5.2. Configuring software selection

Use the **Software Selection** window to select the software packages that you require. The packages are organized by Base Environments and Add-Ons.

- **Base Environments** are predefined packages. You can select only one base environment, and availability is dependent on the installation ISO image used as the installation source.

- **Add-Ons** are additional packages for the base environment. You can select multiple add-ons.

Use the predefined environments and add-ons to customize your system, but in a standard installation, you cannot select individual packages to install. To view the packages contained in a specific environment or add-on, see the ***repository*/repodata/*-comps-*repository*.*architecture*.xml** file on your installation source media (DVD, CD, USB). The XML file contains details of the packages installed as part of a base environment or add-on. Available environments are marked by the **<environment>** tag, and add-ons are marked by the **<group>** tag.

If you are unsure about which packages to install, Red Hat recommends that you select the **Minimal Install** base environment. Minimal install installs a basic version of Red Hat Enterprise Linux with only a minimal amount of additional software. After the system finishes installing and you log in for the first time, you can use the **Yum package manager** to install additional software. For more information about Yum package manager, see the *Configuring basic system settings* document.

NOTE

- The **yum group list** command lists all package groups from yum repositories. See the *Configuring basic system settings* document for more information.
- If you need to control which packages are installed, you can use a Kickstart file and define the packages in the **%packages** section. See the *Performing an advanced RHEL installation* document for information about installing Red Hat Enterprise Linux using Kickstart.

Prerequisites

- You have configured the installation source.
- The installation program downloaded package metadata.
- The **Installation Summary** window is open.

Procedure

1. From the **Installation Summary** window, click **Software Selection**. The **Software Selection** window opens.
2. From the **Base Environment** pane, select a base environment. You can select only one base environment.

   NOTE

   The **Server with GUI** base environment is the default base environment and it launches the **Initial Setup** application after the installation completes and you restart the system.

3. From the **Add-Ons for Selected Environment** pane, select one or more add-ons.
4. Click **Done** to apply the settings and return to Section 6.3, “The Installation Summary window”.

6.6. CONFIGURING SYSTEM OPTIONS

This section contains information about configuring Installation Destination, KDUMP, Network and Host Name, Security Policy, and System Purpose.

6.6.1. Configuring installation destination

Use the **Installation Destination** window to configure the storage options, for example, the disks that you want to use as the installation target for your Red Hat Enterprise Linux installation. You must select at least one disk.

WARNING

Back up your data if you plan to use a disk that already contains data. For example, if you want to shrink an existing Microsoft Windows partition and install Red Hat Enterprise Linux as a second system, or if you are upgrading a previous release of Red Hat Enterprise Linux. Manipulating partitions always carries a risk. For example, if the process is interrupted or fails for any reason data on the disk can be lost.

IMPORTANT

- Some BIOS types do not support booting from a RAID card. In these instances, 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 choose to partition your system automatically, you should manually edit your /**boot** partition.

- 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** window.

- 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 creates volume groups that contain a mix of multipath and non-multipath devices. This defeats the purpose of multipath storage. It is recommended that you select either multipath or non-multipath devices on the **Installation Destination** window. Alternatively, proceed to manual partitioning.

Prerequisite

The **Installation Summary** window is open.

Procedure

1. From the **Installation Summary** window, click **Installation Destination**. The **Installation Destination** window opens.

    a. From the **Local Standard Disks** section, select the storage device that you require; a white check mark indicates your selection. Disks without a white check mark are not used during the installation process; they are ignored if you choose automatic partitioning, and they are not available in manual partitioning.

    NOTE

    All locally available storage devices (SATA, IDE and SCSI hard drives, USB flash and external disks) are displayed under **Local Standard Disks**. Any storage devices connected after the installation program has started are not detected. If you use a removable drive to install Red Hat Enterprise Linux, your system is unusable if you remove the device.

b. Optional: Click the **Refresh** link in the lower right-hand side of the window if you want to configure additional local storage devices to connect new hard drives. The **Rescan Disks** dialog box opens.

> **NOTE**
>
> All storage changes that you make during the installation are lost when you click **Rescan Disks**.

i. Click **Rescan Disks** and wait until the scanning process completes.

ii. Click **OK** to return to the **Installation Destination** window. All detected disks including any new ones are displayed under the **Local Standard Disks** section.

2. Optional: To add a specialized storage device, click **Add a disk…**.
The **Storage Device Selection** window opens and lists all storage devices that the installation program has access to. For information about how to add a specialized disk, see Section 6.7.3, “Using advanced storage options”.

3. Optional: Under **Storage Configuration**, select the **Automatic** radio button.

> **IMPORTANT**
>
> Automatic partitioning is the **recommended** method of partitioning your storage. You can also configure custom partitioning, for more details see Section 6.8, “Configuring manual partitioning”

4. Optional: To reclaim space from an existing partitioning layout, select the **I would like to make additional space available** check box. For example, if a disk you want to use already contains a different operating system and you want to make this system’s partitions smaller to allow more room for Red Hat Enterprise Linux.

5. Optional: Select **Encrypt my data** to encrypt all partitions except the ones needed to boot the system (such as **/boot**) using *Linux Unified Key Setup* (LUKS). Encrypting your hard drive is recommended.

a. If you selected **Encrypt my data** the **Disk Encryption Passphrase** dialog box opens.

i. Type your passphrase in the **Passphrase** and **Confirm** fields.

ii. Click **Save Passphrase** to complete disk encryption.

> **WARNING**
>
> If you lose the LUKS passphrase, any encrypted partitions and their data is completely inaccessible. There is no way to recover a lost passphrase. However, if you perform a Kickstart installation, you can save encryption passphrases and create backup encryption passphrases during the installation. See the *Performing an advanced RHEL installation* document for information.

6. Optional: Click the **Full disk summary and bootloader** link in the lower left-hand side of the window to select which storage device contains the boot loader. For more information, see Section 6.6.1.1, "Configuring boot loader".

    NOTE

    In most cases it is sufficient to leave the boot loader in the default location. Some configurations, for example, systems that require chain loading from another boot loader require the boot drive to be specified manually.

7. Click **Done**.

    a. If you selected **automatic partitioning** and **I would like to make additional space available**, or if there is not enough free space on your selected hard drives to install Red Hat Enterprise Linux, the **Reclaim Disk Space** dialog box opens when you click **Done**, and lists all configured disk devices and all partitions on those devices. The dialog box displays information about how much space the system needs for a minimal installation and how much space you have reclaimed.

        WARNING

        If you **delete** a partition, all data on that partition is lost. If you want to preserve your data, use the **Shrink** option, not the **Delete** option.

    b. Review the displayed list of available storage devices. The **Reclaimable Space** column shows how much space can be reclaimed from each entry.

    c. To reclaim space, select a disk or partition, and click either the **Delete** button to delete that partition, or all partitions on a selected disk, or click **Shrink** to use free space on a partition while preserving the existing data.

        NOTE

        Alternatively, you can click **Delete all**, this deletes all existing partitions on all disks and makes this space available to Red Hat Enterprise Linux. Existing data on all disks is lost.

    d. Click **Reclaim space** to apply the changes and return to Section 6.3, "The Installation Summary window".

IMPORTANT

No disk changes are made until you click **Begin Installation** on the **Installation Summary** window. The **Reclaim Space** dialog only marks partitions for resizing or deletion; no action is performed.

6.6.1.1. Configuring boot loader

Red Hat Enterprise Linux uses GRand Unified Bootloader version 2 (**GRUB2**) as the boot loader for AMD64 and Intel 64, IBM Power Systems, and ARM. For IBM Z, the **zipl** boot loader is used.

The boot loader is the first program that runs when the system starts and is responsible for loading and transferring control to an operating system. **GRUB2** can boot any compatible operating system (including Microsoft Windows) and can also use chain loading to transfer control to other boot loaders for unsupported operating systems.

WARNING

Installing **GRUB2** may overwrite your existing boot loader.

If an operating system is already installed, the Red Hat Enterprise Linux installation program attempts to automatically detect and configure the boot loader to start the other operating system. If the boot loader is not detected, you can manually configure any additional operating systems after you finish the installation.

If you are installing a Red Hat Enterprise Linux system with more than one disk, you might want to manually specify the disk where you want to install the boot loader.

Procedure

1. From the **Installation Destination** window, click the **Full disk summary and bootloader** link. The **Selected Disks** dialog box opens.
   The boot loader is installed on the device of your choice, or on a UEFI system; the **EFI system partition** is created on the target device during guided partitioning.

2. To change the boot device, select a device from the list and click **Set as Boot Device**. You can set only one device as the boot device.

3. To disable a new boot loader installation, select the device currently marked for boot and click **Do not install boot loader**. This ensures **GRUB2** is not installed on any device.

WARNING

If you choose not to install a boot loader, you cannot boot the system directly and you must use another boot method, such as a standalone commercial boot loader application. Use this option only if you have another way to boot your system.

The boot loader may also require a special partition to be created, depending on if your system uses BIOS or UEFI firmware, or if the boot drive has a *GUID Partition Table* (GPT) or a **Master Boot Record** (MBR, also known as **msdos**) label. If you use automatic partitioning, the installation program creates the partition.

6.6.2. Configuring Kdump

Kdump is a kernel crash-dumping mechanism. In the event of a system crash, **Kdump** captures the contents of the system memory at the moment of failure. This captured memory can be analyzed to find the cause of the crash. If **Kdump** is enabled, it must have a small portion of the system's memory (RAM) reserved to itself. This reserved memory is not accessible to the main kernel.

Procedure

1. From the **Installation Summary** window, click **Kdump**. The **Kdump** window opens.
2. Select the **Enable kdump** check box.
3. Select either the **Automatic** or **Manual** memory reservation setting.
    a. If you select **Manual**, enter the amount of memory (in megabytes) that you want to reserve in the **Memory to be reserved**field using the **+** and **-** buttons. The **Usable System Memory** readout below the reservation input field shows how much memory is accessible to your main system after reserving the amount of RAM that you select.
4. Click **Done** to apply the settings and return to Section 6.3, "The Installation Summary window".

NOTE

The amount of memory that you reserve is determined by your system architecture (AMD64 and Intel 64 have different requirements than IBM Power) as well as the total amount of system memory. In most cases, automatic reservation is satisfactory.

IMPORTANT

Additional settings, such as the location where kernel crash dumps will be saved, can only be configured after the installation using either the **system-config-kdump** graphical interface, or manually in the **/etc/kdump.conf** configuration file.

6.6.3. Configuring network and host name options

Use the **Network and Host name** window to configure network interfaces. Options that you select here are available both during the installation for tasks such as downloading packages from a remote location, and on the installed system.

6.6.3.1. Configuring network and host name

Follow the steps in this procedure to configure your network and host name.

Procedure

1. From the **Installation Summary** window, click **Network and Host Name**.
2. From the list in the left-hand pane, select an interface. The details are displayed in the right-hand pane.
3. Toggle the **ON/OFF** switch to enable or disable the selected interface.

    NOTE

    Locally accessible interfaces are automatically detected by the installation program and cannot be manually added or deleted.

4. Click **+** to add a virtual network interface, which can be either: Team, Bond, Bridge, or VLAN.

5. Click **-** to remove a virtual interface.

6. Click **Configure** to change settings such as IP addresses, DNS servers, or routing configuration for an existing interface (both virtual and physical).

7. Type a host name for your system in the **Host Name** field.

   NOTE

   - There are several types of network device naming standards used to identify network devices with persistent names, for example, **em1** and **wl3sp0**. For information about these standards, see the *Configuring and managing networking* document.

   - The host name can be either a fully-qualified domain name (FQDN) in the format hostname.domainname, or a short host name with no domain name. 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, specify only the short host name. The value **localhost.localdomain** means that no specific static host name for the target system is configured, and the actual host name of the installed system is configured during the processing of the network configuration, for example, by NetworkManager using DHCP or DNS.

8. Click **Apply** to apply the host name to the environment.

6.6.3.2. Adding a virtual network interface

Follow the steps in this procedure to add a virtual network interface.

Procedure

1. From the **Network & Host name**window, click the **+** button to add a virtual network interface. The **Add a device** dialog opens.

2. Select one of the four available types of virtual interfaces:

   - **Bond**: NIC (*Network Interface Controller*) Bonding, a method to bind multiple physical network interfaces together into a single bonded channel.

   - **Bridge**: Represents NIC Bridging, a method to connect multiple separate networks into one aggregate network.

   - **Team**: 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** (*Virtual LAN*): A method to create multiple distinct broadcast domains which are mutually isolated.

3. Select the interface type and click **Add**. An editing interface dialog box opens, allowing you to edit any available settings for your chosen interface type. For more information see Section 6.6.3.3, “Editing network interface configuration” .

4. Click **Save** to confirm the virtual interface settings and return to the **Network & Host name** window.

> **NOTE**
>
> If you need to change the settings of a virtual interface, select the interface and click **Configure**.

6.6.3.3. Editing network interface configuration

This section contains information about the most important settings for a typical wired connection used during installation. Configuration of other types of networks is broadly similar, although the specific configuration parameters might be different.

> **NOTE**
>
> On IBM Z, you cannot add a new connection as the network subchannels need to be grouped and set online beforehand, and this is currently done only in the booting phase.

Procedure

1. To configure a network connection manually, select the interface from the **Network and Host name** window and click **Configure**.
   An editing dialog specific to the selected interface opens.

> **NOTE**
>
> The options present depend on the connection type - the available options are slightly different depending on whether the connection type is a physical interface (wired or wireless network interface controller) or a virtual interface (Bond, Bridge, Team, or Vlan) that was previously configured in Section 6.6.3.2, “Adding a virtual network interface” .

The following sections contain information about the three most common and useful options in the editing dialog:

6.6.3.4. Enabling or Disabling the Interface Connection

Follow the steps in this procedure to enable or disable an interface connection.

Procedure

1. Click the **General** tab.

2. Select the **Automatically connect to this network when it is available** check box to enable connection by default.

NOTE

- When enabled on a wired connection, the system typically connects during startup (unless you unplug the network cable). On a wireless connection, the interface attempts to connect to any known wireless networks in range.
- You can enable or disable all users on the system from connecting to this network using the **All users may connect to this network**option. If you disable this option, only **root** will be able to connect to this network.
- It is not possible to only allow a specific user other than **root** to use this interface, as no other users are created at this point during the installation. If you need a connection for a different user, you must configure it after the installation.

3. Click **Save** to apply the changes and return to the **Network and Host name**window.

6.6.3.5. Setting up Static IPv4 or IPv6 Settings

By default, both IPv4 and IPv6 are set to automatic configuration depending on current network settings. This means that addresses such as the local IP address, DNS address, and other settings will be detected automatically when the interface connects to a network. In many cases, this is sufficient, but you can also provide static configuration in the **IPv4 Settings** and **IPv6 Settings** tabs. Complete the following steps to configure IPv4 or IPv6 settings:

Procedure

1. To set static network configuration, navigate to one of the IPv Settings tabs and from the **Method** drop-down menu, select a method other than **Automatic**, for example, **Manual**. The **Addresses** pane is enabled.

   NOTE

   In the **IPv6 Settings** tab, you can also set the method to **Ignore** to disable IPv6 on this interface.

2. Click **Add** and enter your address settings.
3. Type the IP addresses in the **Additional DNS servers** field; it accepts one or more IP addresses of DNS servers, for example, **10.0.0.1,10.0.0.8**.
4. Select the **Require IPv*X* addressing for this connection to complete**check box.

   NOTE

   Select this option in the **IPv4 Settings** or **IPv6 Settings** tabs to allow this connection only if IPv4 or IPv6 was successful. If this option remains disabled for both IPv4 and IPv6, the interface is able to connect if configuration succeeds on either IP protocol.

5. Click **Save** to apply the changes and return to the **Network & Host name**window.

6.6.3.6. Configuring Routes

Complete the following steps to configure routes.

Procedure

1. In the **IPv4 Settings** and **IPv6 Settings** tabs, click **Routes** to configure routing settings for a specific IP protocol on an interface. An editing routes dialog specific to the interface opens.
2. Click **Add** to add a route.
3. Select the **Ignore automatically obtained routes** check box to configure at least one static route and to disable all routes not specifically configured.
4. Select the **Use this connection only for resources on its network** check box to prevent the connection from becoming the default route.

   > NOTE
   >
   > This option can be selected even if you did not configure any static routes. This route is used only to access certain resources, such as intranet pages that require a local or VPN connection. Another (default) route is used for publicly available resources. Unlike the additional routes configured, this setting is transferred to the installed system. This option is useful only when you configure more than one interface.

5. Click **OK** to save your settings and return to the editing routes dialog that is specific to the interface.
6. Click **Save** to apply the settings and return to the **Network and Host Name** window.

Additional resources

- To learn more about network configuration after installation, see the *Configuring and managing networking* document.

6.6.4. Configuring security policy

This section contains information about the Red Hat Enterprise Linux 8 security policy add-on and how to configure it for use on your system.

6.6.4.1. About security policy

The Red Hat Enterprise Linux security policy adheres to restrictions and recommendations (compliance policies) defined by the Security Content Automation Protocol (SCAP) standard. The packages are automatically installed. However, by default, no policies are enforced and therefore no checks are performed during or after installation unless specifically configured.

Applying a security policy is not a mandatory feature of the installation program. If you apply a security policy to the system, it is installed using restrictions and recommendations defined in the profile that you selected. The **openscap-scanner** package is added to your package selection, providing a preinstalled tool for compliance and vulnerability scanning. After the installation finishes, the system is automatically scanned to verify compliance. The results of this scan are saved to the **/root/openscap_data** directory on the installed system. You can also load additional profiles from an HTTP or HTTPS server.

6.6.4.2. Configuring a security policy

Complete the following steps to configure a security policy.

Prerequisite

The **Installation Summary** window is open.

Procedure

1. From the **Installation Summary** window, click **Security Policy**. The **Security Policy** window opens.

2. To enable security policies on the system, toggle the **Apply security policy** switch to **ON**.

3. Select one of the profiles listed in the top pane.

4. Click **Select profile**.
   Profile changes that you must apply before installation appear in the bottom pane.

   > **NOTE**
   >
   > The default profiles do not require changes before installation. However, loading a custom profile can require pre-installation tasks.

5. Click **Change content** to use a custom profile. A separate window opens allowing you to enter a URL for valid security content.

   a. Click **Fetch** to retrieve the URL.

   b. Click **Use SCAP Security Guide** to return to the **Security Policy** window.

   > **NOTE**
   >
   > You can load custom profiles from an **HTTP** or **HTTPS** server. Use the full address of the content including the protocol, such as **http://**. A network connection must be active before you can load a custom profile. The installation program detects the content type automatically.

6. Click **Done** to apply the settings and return to the **Installation Summary** window.

6.6.4.3. Related information

- **scap-security-guide(8)** - The manual page for the **scap-security-guide** project contains information about SCAP security profiles, including examples on how to utilize the provided benchmarks using the OpenSCAP utility.

- Red Hat Enterprise Linux security compliance information is available in the *Security hardening* document.

6.6.5. Configuring system purpose

System administrators use System Purpose to record the intended use of a Red Hat Enterprise Linux 8 system by the organization. When you set system purpose, the entitlement server receives information that helps to auto-attach a subscription that satisfies the intended use of the system. This section contains information about configuring System Purpose using either the graphical user interface, or the **syspurpose** command-line tool.

6.6.5.1. Overview

You can enter System Purpose data in the following ways:

- During image creation.
- During installation using the graphical user interface.
- Using Kickstart automation scripts.
- Using the **syspurpose** command-line tool.

You can configure the following components:

- **Role**:
  - Red Hat Enterprise Linux Server
  - Red Hat Enterprise Linux Workstation
  - Red Hat Enterprise Linux Compute Node
- **Service Level Agreement**
  - Premium
  - Standard
  - Self-Support
- **Usage**:
  - Production
  - Disaster Recovery
  - Development/Test

Benefits include:

- In-depth system-level information for system administrators and business operations.
- Reduced overhead when determining why a system was procured and its intended purpose.
- Improved customer experience of Subscription Manager auto-attach as well as automated discovery and reconciliation of system usage.

Additional resources

- For more information about Image Builder, see the *Composing a customized RHEL system image* document.
- For more information about Kickstart, see the *Performing an advanced RHEL installation* document.
- For more information about Subscription Manager, see the *Using and Configuring Red Hat Subscription Manager* document.

6.6.5.2. Configuring system purpose using the graphical user interface

Follow the steps in this procedure to configure System Purpose using the graphical user interface.

> **NOTE**
>
> While it is strongly recommended that you configure System Purpose, it is an optional feature of the Red Hat Enterprise Linux installation program. If you want to enable System Purpose after the installation completes, you can do so using the **syspurpose** command-line tool.

Prerequisites

- The **Installation Summary** window is open.

Procedure

1. From the **Installation Summary** window, click **System Purpose**. The **System Purpose** window opens.
2. Select the system role that you require from the **Role** pane.
3. Select the service level agreement that you require from the **Red Hat Service Level Agreement** pane.
4. Select the usage type that you require from the **Usage** pane.
5. Click **Done** to apply the settings and return to the **Installation Summary** window.

The System Purpose data is now available for Subscription Manager to auto-attach to the system.

6.6.5.3. Configuring System Purpose using the syspurpose command-line tool

Follow the steps in this procedure to configure System Purpose after installation using the **syspurpose** command-line tool.

Prerequisites

- You have installed and registered your Red Hat Enterprise Linux 8 system.
- You are logged in as a **root** user.

Procedure

Follow the steps in this procedure to set and unset System Purpose options using the **syspurpose** command-line tool.

1. From a terminal window, run the following command to set the intended role of the system:

   ```
   # syspurpose set-role "VALUE"
   ```

   Replace **VALUE** with the role that you want to assign:

   - **Red Hat Enterprise Linux Server**
   - **Red Hat Enterprise Linux Workstation**

- **Red Hat Enterprise Linux Compute Node**

For example:

```
# syspurpose set-role "Red Hat Enterprise Linux Server"
```

Run the following command to unset the role:

```
# syspurpose unset-role
```

2. Run the following command to set the intended sla of the system:

```
# syspurpose set-sla "VALUE"
```

Replace **VALUE** with the sla that you want to assign:

- **Premium**
- **Standard**
- **Self-Support**

For example:

```
# syspurpose set-sla "Standard"
```

Run the following command to unset the sla:

```
# syspurpose unset-sla
```

3. Run the following command to set the intended usage of the system:

```
# syspurpose set-usage "VALUE"
```

Replace **VALUE** with the usage that you want to assign:

- **Production**
- **Disaster Recovery**
- **Development/Test**
  For example:

  ```
  # syspurpose set-usage "Production"
  ```

  Run the following command to unset the usage:

  ```
  # syspurpose unset-usage
  ```

4. Run the following command to show the current system purpose properties:

```
# syspurpose show
```

Run the following command to access the **syspurpose** man page:

```
# man syspurpose
```

NOTE

Using the **syspurpose** command-line tool to set the role, sla, and usage influences the subscriptions that are auto-attached to the system. If your system is registered and has subscriptions that do not satisfy the required system purpose, you can run the **subscription-manager remove --all** command to remove attached subscriptions. You can then use the **syspurpose** command-line tool to set the system purpose that you require, and run **subscription-manager attach --auto** to entitle the system with the updated system purpose attributes.

6.6.5.4. Related information

- For information on configuring System Purpose using Kickstart, see the *Performing an advanced RHEL installation* document.

6.7. CONFIGURING STORAGE DEVICES

You can install Red Hat Enterprise Linux on a large variety of storage devices. You can configure basic, locally accessible, storage devices in the **Installation Destination** window. Basic storage devices directly connected to the local system, such as hard disk drives and solid-state drives, are displayed in the **Local Standard Disks** section of the window. On IBM Z, this section contains activated Direct Access Storage Devices (DASDs).

WARNING

A known issue prevents DASDs configured as HyperPAV aliases from being automatically attached to the system after the installation is complete. These storage devices are available during the installation, but are not immediately accessible after you finish installing and reboot. To attach HyperPAV alias devices, add them manually to the **/etc/dasd.conf** configuration file of the system.

6.7.1. Storage device selection

The storage device selection window lists all storage devices that the installation program can access. Depending on your system and available hardware, some tabs might not be displayed. 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.

IMPORTANT

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.

NVDIMM Devices

Under specific circumstances, Red Hat Enterprise Linux 8 can boot and run from (NVDIMM) devices in sector mode on the Intel 64 and AMD64 architectures.

System z Devices

Storage devices, or Logical Units (LUNs), attached through the zSeries Linux FCP (Fiber Channel Protocol) driver.

6.7.2. Filtering storage devices

In the storage device selection window you can filter storage devices either by their World Wide Identifier (WWID) or by the port, target, or logical unit number (LUN).

Prerequisite

The **Installation Summary** window is open.

Procedure

1. From the **Installation Summary** window, click **Installation Destination**. The **Installation Destination** window opens, listing all available drives.

2. Under the **Specialized & Network Diskss**ection, click **Add a disk…**. The storage devices selection window opens.

3. Click the **Search by** tab to search by port, target, LUN, or WWID.
   Searching by WWID or LUN requires additional values in the corresponding input text fields.

4. Select the option that you require from the **Search** drop-down menu.

5. Click **Find** to start the search. Each device is presented on a separate row with a corresponding check box.

6. Select the check box to enable the device that you require during the installation process.
   Later in the installation process you can choose to install Red Hat Enterprise Linux on any of the selected devices, and you can choose to mount any of the other selected devices as part of the installed system automatically.

   NOTE

   - Selected devices are not automatically erased by the installation process and selecting a device does not put the data stored on the device at risk.

   - You can add devices to the system after installation by modifying the **/etc/fstab** file.

7. Click **Done** to return to the **Installation Destination** window.

IMPORTANT

Any storage devices that you do not select are hidden from the installation program entirely. To chain load the boot loader from a different boot loader, select all the devices present.

6.7.3. Using 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).

To use iSCSI storage devices for the installation, the installation program 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 Challenge Handshake Authentication Protocol (CHAP) 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 to add all required iSCSI storage. 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.

6.7.3.1. Discovering and starting an iSCSI session

Complete the following steps to discover and start an iSCSI session.

Prerequisites

- The **Installation Summary** window is open.

Procedure

1. From the **Installation Summary** window, click **Installation Destination**. The **Installation Destination** window opens, listing all available drives.

2. Under the **Specialized & Network Disks**section, click **Add a disk…** The storage devices selection window opens.

3. Click **Add iSCSI target…** The **Add iSCSI Storage Target**window opens.

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

5. Type a name in the **iSCSI Initiator Name** field for the iSCSI initiator in iSCSI qualified name (IQN) format. A valid IQN entry contains the following information:

    - 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 is as follows: **iqn.2010-09.storage.example.com:diskarrays-sn-a8675309**. The installation program prepopulates the **iSCSI Initiator Name** field with a name in this format to help you with the structure. For more information about IQNs, see *3.2.6. iSCSI Names* in *RFC 3720 - Internet Small Computer Systems Interface (iSCSI)* available from tools.ietf.org and *1. iSCSI Names and Addresses* in *RFC 3721 - Internet Small Computer Systems Interface (iSCSI) Naming and Discovery* available from tools.ietf.org.

6. Select 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

7. a. If you selected **CHAP pair** as the authentication type, enter the user name and password for the iSCSI target in the **CHAP Username** and **CHAP Password** fields.

   b. If you selected **CHAP pair and a reverse pair** as the authentication type, enter 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.

8. Optionally, select the **Bind targets to network interfaces** check box.

9. Click **Start Discovery**.
   The installation program attempts to discover an iSCSI target based on the information provided. If discovery succeeds, the **Add iSCSI Storage Target** window displays a list of all iSCSI nodes discovered on the target.

10. Select the check boxes for the node that you want to use for installation.

> NOTE
>
> The **Node login authentication type** menu contains the same options as the **Discovery Authentication Type** menu. However, if you need credentials for discovery authentication, use the same credentials to log in to a discovered node.

11. Click the additional **Use the credentials from discovery** drop-down menu. When you provide the proper credentials, the **Log In** button becomes available.

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

6.7.3.2. Configuring FCoE parameters

Complete the following steps to configure FCoE parameters.

Prerequisite

The **Installation Summary** window is open.

Procedure

1. From the **Installation Summary** window, click **Installation Destination**. The **Installation Destination** window opens, listing all available drives.

2. Under the **Specialized & Network Disks**section, click **Add a disk…**. The storage devices selection window opens.

3. Click **dd FCoE SAN…** A dialog box opens for you to configure network interfaces for discovering FCoE storage devices.

4. Select a network interface that is connected to an FCoE switch in the **NIC** drop-down menu.

5. Click **Add FCoE disk(s)** to scan the network for SAN devices.

6. Select the required check boxes:

   - **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. Select the check box to enable or disable the installation program's awareness of DCB. Enable this option only for network interfaces that require a host-based DCBX client. For configurations on interfaces that use a hardware DCBX client, disable the check box.

   - **Use auto vlan:***Auto VLAN* is enabled by default and indicates whether VLAN discovery should be performed. If this check box is enabled, then the FIP (FCoE Initiation Protocol) VLAN discovery protocol runs on the Ethernet interface when the link configuration has been validated. If they are not already configured, network interfaces for any discovered FCoE VLANs are automatically created and FCoE instances are created on the VLAN interfaces.

7. Discovered FCoE devices are displayed under the **Other SAN Devices** tab in the **Installation Destination** window.

6.7.3.3. Configuring DASD storage devices

Complete the following steps to configure DASD storage devices.

Prerequisite

The **Installation Summary** window is open.

Procedure

1. From the **Installation Summary** window, click **Installation Destination**. The **Installation Destination** window opens, listing all available drives.

2. Under the **Specialized & Network Disks**section, click **Add a disk…**. The storage devices selection window opens.

3. Click **Add DASD**. The **Add DASD Storage Target**dialog box opens and prompts you to specify a device number, such as **0.0.0204**, and attach additional DASDs that were not detected when the installation started.

4. Type the device number of the DASD that you want to attach in the **Device number** field.

5. Click **Start Discovery**.

NOTE

- If a DASD with the specified device number is found and if it is not already attached, the dialog box closes and the newly-discovered drives appear in the list of drives. You can then select the check boxes for the required devices and click **Done**. The new DASDs are available for selection (marked as **DASD device 0.0.*xxxx***) in the **Local Standard Disks** section of the **Installation Destination** window.

- If you entered an invalid device number, or if the DASD with the specified device number is already attached to the system, an error message appears in the dialog box, explaining the error and prompting you to try again with a different device number.

6.7.3.4. Configuring FCP devices

FCP devices enable IBM Z to use SCSI devices rather than, or in addition to, Direct Access Storage Device (DASD) devices. FCP devices provide a switched fabric topology that enables IBM Z systems to use SCSI LUNs as disk devices in addition to traditional DASD devices.

Prerequisites

- The **Installation Summary** window is open.

- For an FCP-only installation, remove the **DASD=** option from the CMS configuration file or the **rd.dasd=** option from the parameter file to indicate that no DASD is present.

Procedure

1. From the **Installation Summary** window, click **Installation Destination**. The **Installation Destination** window opens, listing all available drives.

2. Under the **Specialized & Network Disks**section, click **Add a disk…**. The storage devices selection window opens.

3. Click **Add ZFCP LUN**. The **Add zFCP Storage Target**dialog box opens allowing you to add a FCP (Fibre Channel Protocol) storage device.
   IBM Z requires that you enter any FCP device manually so that the installation program can activate FCP LUNs. You can enter FCP devices either in the graphical installation, or as a unique parameter entry in the parameter or CMS configuration file. The values that you enter must be unique to each site that you configure.

4. Type the 4 digit hexadecimal device number in the **Device number** field.

5. Type the 16 digit hexadecimal World Wide Port Number (WWPN) in the **WWPN** field.

6. Type the 16 digit hexadecimal FCP LUN identifier in the **LUN** field.

7. Click **Start Discovery** to connect to the FCP device.

The newly-added devices are displayed in the **System z Devices**tab of the **Installation Destination** window.

NOTE

- Interactive creation of an FCP device is only possible in graphical mode. It is not possible to configure an FCP device interactively in text mode installation.
- Use only lower-case letters in hex values. If you enter an incorrect value and click **Start Discovery**, the installation program displays a warning. You can edit the configuration information and retry the discovery attempt.
- For more information about these values, consult the hardware documentation and check with your system administrator.

6.7.4. Installing to an NVDIMM device

Non-Volatile Dual In-line Memory Module (NVDIMM) devices combine the performance of RAM with disk-like data persistence when no power is supplied. Under specific circumstances, Red Hat Enterprise Linux 8 can boot and run from NVDIMM devices.

6.7.4.1. Criteria for using an NVDIMM device as an installation target

You can install Red Hat Enterprise Linux 8 to Non-Volatile Dual In-line Memory Module (NVDIMM) devices in sector mode on the Intel 64 and AMD64 architectures, supported by the **nd_pmem** driver.

Conditions for using an NVDIMM device as storage

To use an NVDIMM device as storage, the following conditions must be satisfied:

- The architecture of the system is Intel 64 or AMD64.
- The NVDIMM device is configured to sector mode. The installation program can reconfigure NVDIMM devices to this mode.
- The NVDIMM device must be supported by the **nd_pmem** driver.

Conditions for booting from an NVDIMM Device

Booting from an NVDIMM device is possible under the following conditions:

- All conditions for using the NVDIMM device as storage are satisfied.
- The system uses UEFI.
- The NVDIMM device must be supported by firmware available on the system, or by an UEFI driver. The UEFI driver may be loaded from an option ROM of the device itself.
- The NVDIMM device must be made available under a namespace.

Utilize the high performance of NVDIMM devices during booting, place the **/boot** and **/boot/efi** directories on the device. The Execute-in-place (XIP) feature of NVDIMM devices is not supported during booting and the kernel is loaded into conventional memory.

6.7.4.2. Configuring an NVDIMM device using the graphical installation mode

A Non-Volatile Dual In-line Memory Module (NVDIMM) device must be properly configured for use by Red Hat Enterprise Linux 8 using the graphical installation.

> **WARNING**
>
> Reconfiguration of a NVDIMM device process destroys any data stored on the device.

Prerequisites

- A NVDIMM device is present on the system and satisfies all the other conditions for usage as an installation target.
- The installation has booted and the **Installation Summary** window is open.

Procedure

1. From the **Installation Summary** window, click **Installation Destination**. The **Installation Destination** window opens, listing all available drives.
2. Under the **Specialized & Network Disks**section, click **Add a disk...**. The storage devices selection window opens.
3. Click the **NVDIMM Devices** tab.
4. To reconfigure a device, select it from the list.
   If a device is not listed, it is not in sector mode.
5. Click **Reconfigure NVDIMM...**. A reconfiguration dialog opens.
6. Enter the sector size that you require and click **Start Reconfiguration**.
   The supported sector sizes are 512 and 4096 bytes.
7. When reconfiguration completes click **OK**.
8. Select the device check box.
9. Click **Done** to return to the **Installation Destination** window.
   The NVDIMM device that you reconfigured is displayed in the **Specialized & Network Disks** section.
10. Click **Done** to return to the **Installation Summary** window.

The NVDIMM device is now available for you to select as an installation target. Additionally, if the device meets the requirements for booting, you can set the device as a boot device.

6.8. CONFIGURING MANUAL PARTITIONING

You can use manual partitioning to configure your disk partitions and mount points and define the file system that Red Hat Enterprise Linux is installed on.

NOTE

Before installation, you should consider whether you want to use partitioned or unpartitioned disk devices. For more information, see the Knowledgebase article at https://access.redhat.com/solutions/163853.

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: **PReP**, /, /**home**, /**boot**, and **swap**. You can also create additional partitions and volumes as you require.

NOTE

An installation of Red Hat Enterprise Linux on IBM Power Systems servers requires a **PReP** boot partition.

WARNING

To prevent data loss it is recommended that you back up your data before proceeding. If you are upgrading or creating a dual-boot system, you should back up any data you want to keep on your storage devices.

6.8.1. Starting manual partitioning

Prerequisites

- The **Installation Summary** screen is currently displayed.
- All disks are available to the installation program.

Procedure

1. Select disks for installation:
   a. Click **Installation Destination** to open the **Installation Destination** window.
   b. Select the disks that you require for installation by clicking the corresponding icon. A selected disk has a check-mark displayed on it.
   c. Under **Storage Configuration**, select the **Custom** radio-button.
   d. Optional: To enable storage encryption with LUKS, select the **Encrypt my data** check box.
   e. Click **Done**.
2. If you selected to encrypt the storage, a dialog box for entering a disk encryption passphrase opens. Type in the LUKS passphrase:
   a. Enter the passphrase in the two text fields. To switch keyboard layout, use the keyboard icon.

> **WARNING**
>
> In the dialog box for entering the passphrase, you cannot change the keyboard layout. Select the English keyboard layout to enter the passphrase in the installation program.

b. Click **Save Passphrase**. The **Manual Partitioning** window opens.

3. Deleted Mount points are listed in the left-hand pane. The mount points are organized by detected operating system installations. As a result, some file systems may be displayed multiple times if a partition is shared among several installations.

    a. Select the mount points in the left pane; the options that can be customized are displayed in the right pane.

    > **NOTE**
    >
    > - If your system contains existing file systems, ensure that enough space is available for the installation. To remove any partitions, select them in the list and click the **-** button.
    >   The dialog has a check box that you can use to remove all other partitions used by the system to which the deleted partition belongs.
    > - If there are no existing partitions and you want to create the recommended set of partitions as a starting point, select your preferred partitioning scheme from the left pane (default for Red Hat Enterprise Linux is LVM) and click the **Click here to create them automatically** link.
    >   A /**boot** partition, a / (root) volume, and a **swap** volume proportionate to the size of the available storage are created and listed in the left pane. These are the recommended file systems for a typical installation, but you can add additional file systems and mount points.

    b. Click **Done** to confirm any changes and return to the **Installation Summary** window.

Continue with adding mount points, configuring the individual mount points, and configuring the underlying partitions or volumes.

6.8.2. Adding a mount point file system

Complete the following steps to add multiple mount point file systems.

Prerequisites

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

- If you want to install the system on multiple disks, or if your disks differ in size and a particular partition must be created on the first disk detected by BIOS, then create these partitions first.

Procedure

1. Click **+** to create a new mount point file system. The **Add a New Mount Point** dialog opens.

2. 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.

3. Enter the size of the file system in to the **Desired Capacity** field; for example, **2GiB**.

   WARNING

   If you do not specify a value in the Desired Capacity field, or if you specify a size bigger than available space, then all remaining free space is used.

4. Click **Add mount point** to create the partition and return to the **Manual Partitioning** window.

6.8.3. Configuring a mount point file system

This procedure describes how to set the partitioning scheme for each mount point that was created manually. The available options are **Standard Partition**, **LVM**, and **LVM Thin Provisioning**.

NOTE

- BTRFS support has been deprecated in Red Hat Enterprise Linux 8.
- The **/boot** partition is always located on a standard partition, regardless of the value selected.

Procedure

1. To change the devices that a single non-LVM mount point should be located on, select the required mount point from the left-hand pane.

2. Under the **Device(s)** heading, click **Modify…**. The **Configure Mount Point** dialog opens.

3. Select one or more devices and click **Select** to confirm your selection and return to the **Manual Partitioning** window.

4. Click **Update Settings** to apply the changes.

   NOTE

   Click the **Rescan** button (circular arrow button) to refresh all local disks and partitions; this is only required after performing advanced partition configuration outside the installation program. Clicking the **Rescan Disks** button resets all configuration changes made in the installation program.

5. In the lower left-hand side of the **Manual Partitioning** window, click the **storage device selected** link to open the **Selected Disks** dialog and review disk information.

6.8.4. Customizing a partition or volume

You can customize a partition or volume if you want to set specific settings.

IMPORTANT

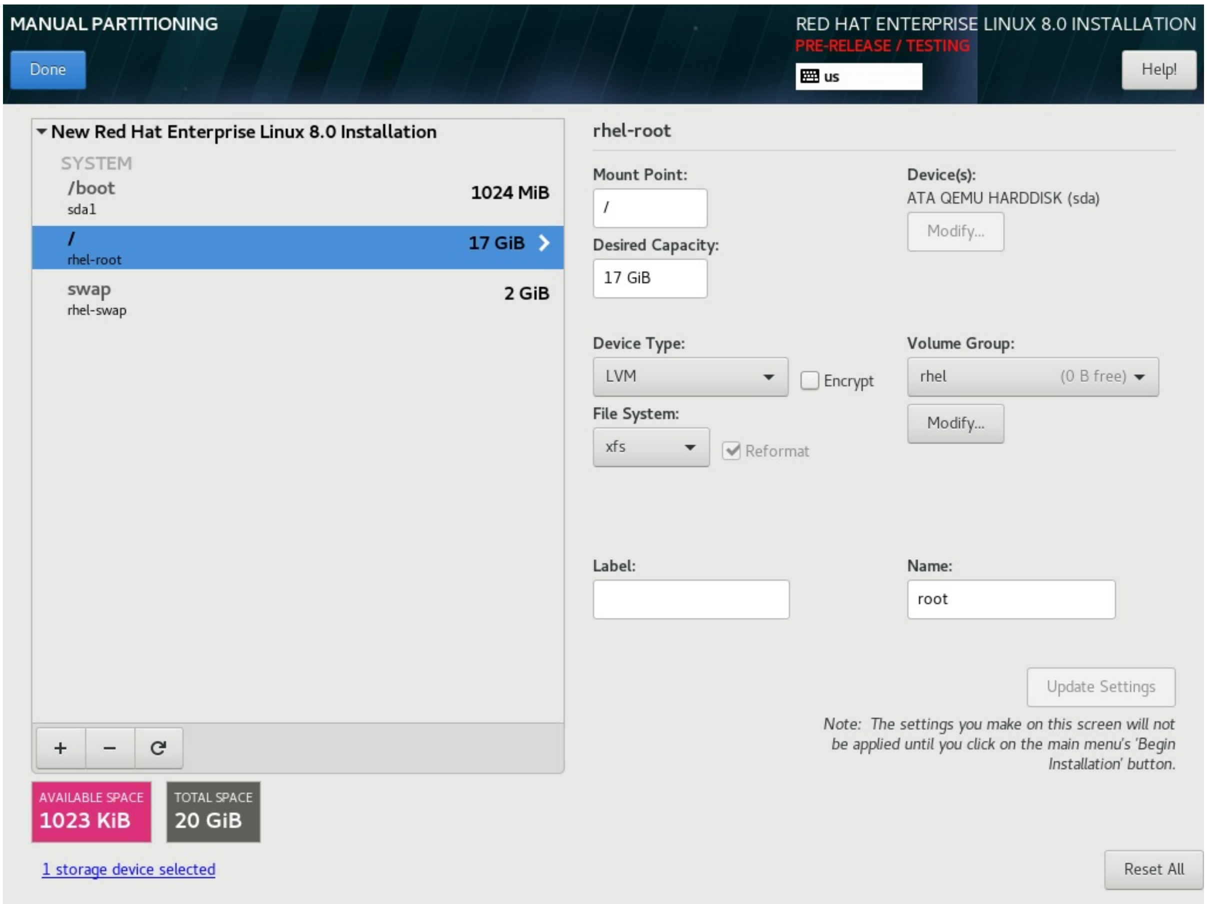
If **/usr** or **/var** is partitioned separately from the rest of the root volume, the boot process becomes much more complex as these directories contain critical components. In some situations, such as when these directories are placed on an iSCSI drive or an FCoE location, the system is unable to boot, or hangs 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** works successfully.

Procedure

1. From the left pane, select the mount point.

Figure 6.2. Customizing Partitions



MANUAL PARTITIONING

RED HAT ENTERPRISE LINUX 8.0 INSTALLATION

PRE-RELEASE / TESTING

New Red Hat Enterprise Linux 8.0 Installation

SYSTEM

/boot sda1	1024 MiB
/ rhel-root	17 GiB
swap rhel-swap	2 GiB

rhel-root

Mount Point: /

Desired Capacity: 17 GiB

Device(s): ATA QEMU HARDDISK (sda)

Device Type: LVM

□ Encrypt

File System: xfs

☑ Reformat

Volume Group: rhel (0 B free)

Label:

Name: root

Note: The settings you make on this screen will not be applied until you click on the main menu's 'Begin Installation' button.

AVAILABLE SPACE 1023 KiB

TOTAL SPACE 20 GiB

1 storage device selected

2. From the right-hand pane, you can customize the following options:

    a. Enter the file system mount point into the **Mount Point** field. For example, if a file system is the root file system, enter /; enter /**boot** for the /**boot** file system, and so on. For a swap file system, do not set the mount point as setting the file system type to **swap** is sufficient.

b. Enter the size of the file system in the **Desired Capacity** field. You can use common size units such as KiB or GiB. The default is MiB if you do not set any other unit.

c. Select the device type that you require from the drop-down **Device Type** menu: **Standard Partition**, **LVM**, or **LVM Thin Provisioning**.

> NOTE
>
> **RAID** is available only if two or more disks are selected for partitioning. If you choose **RAID**, you can also set the **RAID Level**. Similarly, if you select **LVM**, you can specify the **Volume Group**.

d. Select the **Encrypt** check box to encrypt the partition or volume. You must set a password later in the installation program. The **LUKS Version** drop-down menu is displayed.

e. Select the LUKS version that you require from the drop-down menu.

f. Select the appropriate file system type for this partition or volume from the **File system** drop-down menu.

g. Select the **Reformat** check box to format an existing partition, or deselect the **Reformat** check box to retain your data. The newly-created partitions and volumes must be reformatted, and the check box cannot be deselected.

h. Type a label for the partition in the **Label** field. Use labels to easily recognize and address individual partitions.

i. Type a name in the **Name** field.

> NOTE
>
> Note that standard partitions are named automatically when they are created and you cannot edit the names of standard partitions. For example, you cannot edit the /**boot** name **sda1**.

3. Click **Update Settings** to apply your changes and if required, select another partition to customize. Changes are not applied until you click **Begin Installation** from the **Installation Summary** window.

> NOTE
>
> Click **Reset All** to discard your partition changes.

4. Click **Done** when you have created and customized all file systems and mount points. If you choose to encrypt a file system, you are prompted to create a passphrase.
   A **Summary of Changes** dialog box opens, displaying a summary of all storage actions for the installation program.

5. Click **Accept Changes** to apply the changes and return to the **Installation Summary** window.

6.8.5. Creating software RAID

Follow the steps in this procedure to create a Redundant Arrays of Independent Disks (RAID) device. RAID devices are constructed from multiple storage devices that are arranged to provide increased performance and, in some configurations, greater fault tolerance.

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

NOTE

On IBM Z, the storage subsystem uses RAID transparently. There is no need to configure a software RAID manually.

Prerequisites

- You have selected two or more disks for installation before RAID configuration options are visible. At least two disks are required to create a RAID device.
- You have created a mount point. By configuring a mount point, you configure the RAID device.
- You have selected the **Custom** radio button on the **Installation Destination** window.

Procedure

1. From the left pane of the **Manual Partitioning** window, select the required partition.
2. Under the **Device(s)** section, click **Modify**. The **Configure Mount Point** dialog box opens.
3. Select the disks that you want to include in the RAID device and click **Select**.
4. Click the **Device Type** drop-down menu and select **RAID**.
5. Click the **File System** drop-down menu and select your preferred file system type.
6. Click the **RAID Level** drop-down menu and select your preferred level of RAID.
7. Click **Update Settings** to save your changes.
8. Click **Done** to apply the settings and return to the **Installation Summary** window.

A message is displayed at the bottom of the window if the specified RAID level requires more disks.

6.8.6. Creating an 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 you can group together into volume groups. You can divide each volume group 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.

NOTE

LVM configuration is available only in the graphical installation program.

IMPORTANT

During text-mode installation, LVM configuration is not available. To create an LVM configuration, 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**.

Procedure

1. From the left-hand pane of the **Manual Partitioning** window, select the mount point.
2. Click the **Device Type** drop-down menu and select **LVM**. The **Volume Group** drop-down menu is displayed with the newly-created volume group name.

   NOTE

   You cannot specify the size of the volume group's physical extents in the configuration dialog. The size is always set to the default value of 4 MiB. If you want to create a volume group with different physical extents, you must 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. See the *Performing an advanced RHEL installation* document for more information about Kickstart.

Additional resources

- For more information about LVM, see the *Configuring and managing logical volumes* document.

6.8.7. Configuring an LVM logical volume

Follow the steps in this procedure to configure a newly-created LVM logical volume.

WARNING

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

Procedure

1. From the left-hand pane of the **Manual Partitioning** window, select the mount point.
2. Click the **Device Type** drop-down menu and select **LVM**. The **Volume Group** drop-down menu is displayed with the newly-created volume group name.
3. Click **Modify** to configure the newly-created volume group.
   The **Configure Volume Group** dialog box opens.

NOTE

You cannot specify the size of the volume group's physical extents in the configuration dialog. The size is always set to the default value of 4 MiB. If you want to create a volume group with different physical extents, you must 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. See the *Performing an advanced RHEL installation* document for more information about Kickstart.

4. From the **RAID Level** drop-down menu, select the RAID level that you require. The available RAID levels are the same as with actual RAID devices.

5. Select the **Encrypt** check box to mark the volume group for encryption.

6. From the **Size policy** drop-down menu, select the size policy for the volume group. The available policy options are:

   - **Automatic**: The size of the volume group is set automatically so that it is 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**: 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 need the volume group to be.

7. Click **Save** to apply the settings and return to the **Manual Partitioning** window.

8. Click **Update Settings** to save your changes

9. Click **Done** to return to the **Installation Summary** window.

6.9. STARTING THE INSTALLATION PROGRAM

Before you start the installation program, you must configure your root password and user settings.

6.9.1. Beginning installation

When the installation process has started, it is not possible to return to the **Installation Summary** window and change any settings. To change settings, you must wait for the installation process to finish, reboot your system, log in, and change your settings on the installed system.

Prerequisites

- You have completed all configuration steps in Section 6.3, "The Installation Summary window".

- The **Installation Summary** window is open.

Procedure

1. From the **Installation Summary** window, click **Begin Installation**. The **Configuration** window opens and the installation process starts.
   Two user setting options, **Root Password** (mandatory) and **User Creation** (optional) are available.

IMPORTANT

Before you finish the installation and reboot, either remove the media (CD, DVD, or a USB drive) used to start the installation, or verify that your system tries to boot from the hard drive before attempting removable media. Otherwise, your system starts the installation program again, instead of the installed system.

6.9.2. Configuring a root password

You must configure a **root** password to finish the installation process and to log in to the administrator (also known as superuser or root) account that is used for system administration tasks. These tasks include installing and updating software packages and changing system-wide configuration such as network and firewall settings, storage options, and adding or modifying users, groups and file permissions.

IMPORTANT

- Use one or both of the following ways to gain root privileges to the installed system:
  - Use a root account
  - Create a user account with administrative privileges (member of the wheel group). The **root** account is always created during the installation. Switch to the administrator account only when you need to perform a task that requires administrator access.

WARNING

The **root** account has complete control over the system. If unauthorized personnel gain access to the account, they can access or delete users' personal files.

Procedure

1. From the **Configuration** window, click **Root Password**. The **Root Password** window opens.
2. Type your password in the **Root Password** field.
   The requirements and recommendations for creating a strong root password are:
   - *Must* be at least eight characters long
   - May contain numbers, letters (upper and lower case) and symbols
   - Is case-sensitive
3. Type the same password in the **Confirm** field.

4. Click **Done** to confirm your root password and return to Section 6.9.1, “Beginning installation”.

   NOTE

   If you proceeded with a weak password, you must click **Done** twice.

6.9.3. Creating a user account

It is recommended that you create a user account to finish the installation. If you do not create a user account, you must log in to the system as **root** directly, which is **not** recommended.

Procedure

1. From the **Configuration** window, click **User Creation**. The **Create User** window opens.
2. Type the user account name in to the **Full name** field, for example: John Smith.
3. Type the username in to the **User name** field, for example: jsmith.

   NOTE

   The **User name** is used to log in from a command line; if you install a graphical environment, then your graphical login manager uses the **Full name**.

4. Select the **Make this user administrator** check box if the user requires administrative rights (the installation program adds the user to the **wheel** group).

   IMPORTANT

   An administrator user can use the **sudo** command to perform tasks that are only available to **root** using the user password, instead of the **root** password. This may be more convenient, but it can also cause a security risk.

5. Select the **Require a password to use this account**check box.

   WARNING

   If you give administrator privileges to a user, verify that the account is password protected. Never give a user administrator privileges without assigning a password to the account.

6. Type a password into the **Password** field.
7. Type the same password into the **Confirm password** field.
8. **Save Changes** to apply the changes and return to the **Configuration** window.
9. When the installation process is complete, click **Reboot** to reboot and log in to your Red Hat Enterprise Linux 8 system.

6.9.3.1. Editing advanced user settings

Follow the steps in this procedure to edit the default settings for the user account in the **Advanced User Configuration** dialog box.

Procedure

1. Edit the details in the **Home directory** field, if required. The field is populated by default with **/home/*username*** .

2. In the **User and Groups IDs**section you can:

    a. Select the **Specify a user ID manually**check box and use the **+** or **-** to enter the required value.

    > **NOTE**
    >
    > The default value is 1000. User IDs (UIDs) 0-999 are reserved by the system so they cannot be assigned to a user.

    b. Select the **Specify a group ID manually** check box and use the **+** or **-** to enter the required value.

    > **NOTE**
    >
    > The default group name is the same as the user name, and the default Group ID (GID) is 1000. GIDs 0-999 are reserved by the system so they can not be assigned to a user group.

3. Specify additional groups as a comma-separated list in the **Group Membership** field. Groups that do not already exist are created; you can specify custom GIDs for additional groups in parentheses. If you do not specify a custom GID for a new group, the new group receives a GID automatically.

    > **NOTE**
    >
    > The user account created always has one default group membership (the user's default group with an ID set in the **Specify a group ID manually** field).

4. Click **Save Changes** to apply the updates and return to the **Configuration** window.

6.9.4. Graphical installation complete

Remove any installation media if it is not ejected automatically upon reboot.

Red Hat Enterprise Linux 8 starts after your system's normal power-up sequence is complete. If your system was installed on a workstation with the X Window System, applications to configure your system are launched. These applications guide you through initial configuration and you can set your system time and date, register your system with Red Hat, and more. If the X Window System is not installed, a **login:** prompt is displayed.

To learn how to complete initial setup, register, and secure your system, see Chapter 7, *Completing post-installation tasks*.

CHAPTER 7. COMPLETING POST-INSTALLATION TASKS

This section describes how to complete the following post-installation tasks:

- Completing initial setup
- Registering your system
- Securing your system

7.1. COMPLETING INITIAL SETUP

This section contains information about how to complete initial setup on a Red Hat Enterprise Linux 8 system.

IMPORTANT

If you selected the **Server with GUI** base environment during installation, the **Initial Setup** window opens the first time you reboot your system after the installation process is complete.

The information displayed in the **Initial Setup** window might vary depending on what was configured during installation. At a minimum, the **Licensing** and **Subscription Manager** options are displayed.

Prerequisite

- You have completed the graphical installation according to the recommended workflow described on Section 6.1, “Graphical installation workflow”.
- You have an active, non-evaluation Red Hat Enterprise Linux subscription.

Procedure

1. From the **Initial Setup** window, select **Licensing Information**.
   The **License Agreement** window opens and displays the licensing terms for Red Hat Enterprise Linux.

2. Review the license agreement and select the **I accept the license agreement** checkbox.

   #### NOTE

   You must accept the license agreement. Exiting **Initial Setup** without completing this step causes a system restart. When the restart process is complete, you are prompted to accept the license agreement again.

3. Click **Done** to apply the settings and return to the **Initial Setup** window.

> **NOTE**
>
> If you did not configure network settings, you cannot register your system immediately. In this case, click **Finish Configuration**. Red Hat Enterprise Linux 8 starts and you can login, activate access to the network, and register your system. See Section 7.3, "Registering your system using the Subscription Manager User Interface" for more information. If you configured network settings, as described in Section 6.6.3, "Configuring network and host name options" , you can register your system immediately, as shown in the following steps:

4. From the **Initial Setup** window, select **Subscription Manager**.
5. The **Subscription Manager** graphical interface opens and displays the option you are going to register, which is: ***subscription.rhsm.redhat.com***.
6. Click **Next**.
7. Enter your **Login** and **Password** details and click **Register**.
8. Confirm the Subscription details and click **Attach**. You must receive the following confirmation message: **Registration with Red Hat Subscription Management is Done!**
9. Click **Done**. The **Initial Setup** window opens.
10. Click **Finish Configuration**. The login window opens.
11. Configure your system. See the *Configuring basic system settings* document for more information.

Additional resources

There are four methods to register your system:

- During installation using Initial Setup.
- After installation using the command line. See Section 7.2, "Registering your system using the command line" for more information.
- After installation using the Subscription Manager user interface. See Section 7.3, "Registering your system using the Subscription Manager User Interface" for more information.
- After installation using Registration Assistant. Registration Assistant is designed to help you choose the most suitable registration option for your Red Hat Enterprise Linux environment. See https://access.redhat.com/labs/registrationassistant/ for more information.

7.2. REGISTERING YOUR SYSTEM USING THE COMMAND LINE

This section contains information about how to register your Red Hat Enterprise Linux 8 system using the command line.

> **NOTE**
>
> When auto-attaching a system, the subscription service checks if the system is physical or virtual, as well as how many sockets are on the system. A physical system usually consumes two entitlements, a virtual system usually consumes one. One entitlement is consumed per two sockets on a system.

Prerequisites

- You have an active, non-evaluation Red Hat Enterprise Linux subscription.
- Your Red Hat subscription status is verified.
- You have not previously received a Red Hat Enterprise Linux 8 subscription.
- You have activated your subscription before attempting to download entitlements from the Customer Portal. You need an entitlement for each instance that you plan to use. Red Hat Customer Service is available if you need help activating your subscription.
- You have successfully installed Red Hat Enterprise Linux 8 and logged into the system.

Procedure

1. Open a terminal window and run the following command to register a subscription:

```
# subscription-manager register
```

2. Enter your **Customer Portal** credentials:

```
# Registering to: subscription.rhsm.redhat.com:443/subscription
# Username: USERNAME
# Password: PASSWORD
```

3. When the subscription is successfully registered, you should see an output similar to the following example:

```
# The system has been registered with ID: 123456abcdef
# The registered system name is: localhost.localdomain
```

4. Set the role for the intended use of the system:

NOTE

Available roles depend on the subscriptions that have been purchased by the organization and the architecture of the RHEL 8 system. You can set one of the following roles: **Red Hat Enterprise Linux Server**, **Red Hat Enterprise Linux Workstation**, or **Red Hat Enterprise Linux Compute Node**.

```
# subscription-manager role --set="Red Hat Enterprise Linux Server"
```

5. Attach the system to an entitlement that matches the host system architecture:

```
# subscription-manager attach
```

6. When the subscription is successfully attached, you should see an output similar to the following example:

```
Installed Product Current Status:
Product Name: Red Hat Enterprise Linux for x86_64
Status: Subscribed
```

NOTE

You can also register Red Hat Enterprise Linux 8 by logging in to the system as a **root** user and using the Subscription Manager graphical user interface.

7.3. REGISTERING YOUR SYSTEM USING THE SUBSCRIPTION MANAGER USER INTERFACE

This section contains information about how to register your Red Hat Enterprise Linux 8 system using the Subscription Manager User Interface to receive updates and access package repositories.

Prerequisites

- You have completed the graphical installation as per the recommended workflow described on Section 6.1, "Graphical installation workflow".
- You have an active, non-evaluation Red Hat Enterprise Linux subscription.
- Your Red Hat subscription status is verified.

Procedure

1. Log in to your system.
2. From the top left-hand side of the window, click **Activities**.
3. From the menu options, click the **Show Applications** icon.
4. Click the **Red Hat Subscription Manager** icon, or enter **Red Hat Subscription Manager** in the search.
5. Enter your administrator password in the **Authentication Required** dialog box.

   NOTE

   Authentication is required to perform privileged tasks on the system.

6. The **Subscriptions** window opens, displaying the current status of Subscriptions, System Purpose, and installed products. Unregistered products display a red X.
7. Click the **Register** button.
8. The **Register System** dialog box opens. Enter your **Customer Portal** credentials and click the **Register** button.

The **Register** button in the **Subscriptions** window changes to **Unregister** and installed products display a green X. You can troubleshoot an unsuccessful registration using the **subscription-manager status** command.

Additional resources

- For more information about Subscription Manager, see the *Using and Configuring Red Hat Subscription Manager* document.

7.4. REGISTRATION ASSISTANT

Registration Assistant is designed to help you choose the most suitable registration option for your Red Hat Enterprise Linux environment. See https://access.redhat.com/labs/registrationassistant/ for more information.

7.5. SECURING YOUR SYSTEM

Complete the following security-related steps immediately after you install Red Hat Enterprise Linux.

Prerequisites

- You have completed the graphical installation according to the recommended workflow described in Section 6.1, “Graphical installation workflow”.

Procedure

1. To update your system, run the following command as root:

   ```
   # yum update
   ```

2. Even though the firewall service, **firewalld**, is automatically enabled with the installation of Red Hat Enterprise Linux, there are scenarios where it might be explicitly disabled, for example in a Kickstart configuration. In that scenario, it is recommended that you re-enable the firewall. To start **firewalld**, run the following commands as root:

   ```
   # systemctl start firewalld
   # systemctl enable firewalld
   ```

3. To enhance security, disable services that you do not need. For example, if your system has no printers installed, disable the cups service using the following command:

   ```
   # systemctl mask cups
   ```

   To review active services, run the following command:

   ```
   $ systemctl list-units | grep service
   ```

APPENDIX A. SYSTEM REQUIREMENTS REFERENCE

This section provides information and guidelines for hardware, installation target, system, memory, and RAID when installing Red Hat Enterprise Linux.

A.1. HARDWARE COMPATIBILITY

Red Hat works closely with hardware vendors on supported hardware.

- To verify that your hardware is supported, see the Red Hat Hardware Compatibility List, available at https://access.redhat.com/ecosystem/search/#/category/Server.
- To view supported memory sizes or CPU counts, see https://access.redhat.com/articles/rhel-limits for information.

A.2. SUPPORTED INSTALLATION TARGETS

An installation target is a storage device that stores Red Hat Enterprise Linux and boots the system. Red Hat Enterprise Linux supports the following installation targets for AMD64, Intel 64, and 64-bit ARM systems:

- Storage connected by a standard internal interface, such as SCSI, SATA, or SAS
- BIOS/firmware RAID devices
- NVDIMM devices in sector mode on the Intel64 and AMD64 architectures, supported by the nd_pmem driver.
- 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 support for third-party virtualization technologies, see the Red Hat Hardware Compatibility List .

A.3. SYSTEM SPECIFICATIONS

The Red Hat Enterprise Linux installation program automatically detects and installs your system's hardware, so you should not have to supply any specific system information. However, for certain Red Hat Enterprise Linux installation scenarios, it is recommended that you record system specifications for future reference. These scenarios include:

Installing RHEL with 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.

Installing RHEL as an additional operating system on an existing system

Record: Partitions used on the system. This information can include file system types, device node names, file system labels, and sizes, and allows you to identify specific partitions during the partitioning process. If one of the operating systems is a Unix operating system, Red Hat Enterprise Linux may report the device names differently. Additional information can be found by executing the equivalent of the **mount** command and the **blkid** command, and in the **/etc/fstab** file.

If multiple operating systems are installed, the Red Hat Enterprise Linux installation program attempts to automatically detect them, and to configure boot loader to boot them. You can manually configure additional operating systems if they are not detected automatically. See *Configuring boot loader* in Section 6.5, "Configuring software options" for more information.

Installing RHEL from an image on a local hard drive

Record: The hard drive and directory that holds the image.

Installing RHEL from a network location

If the network has to be configured manually, that is, DHCP is not used.

Record:

- IP address
- Netmask
- Gateway IP address
- Server IP addresses, if required

Contact your network administrator if you need assistance with networking requirements.

Installing RHEL on an iSCSI target

Record: The location of the iSCSI target. Depending on your network, you may need a CHAP user name and password, and a reverse CHAP user name and password.

Installing RHEL if the system is part of a domain

Verify that the domain name is supplied by the DHCP server. If it is not, enter the domain name during installation.

A.4. DISK AND MEMORY REQUIREMENTS

If several operating systems are installed, it is important that you verify that the allocated disk space is separate from the disk space required by Red Hat Enterprise Linux.

NOTE

- For AMD64, Intel 64, and 64-bit ARM, at least two partitions (/ and **swap**) must be dedicated to Red Hat Enterprise Linux.
- For IBM Power Systems servers, at least three partitions (/, **swap**, and a **PReP** boot partition) must be dedicated to Red Hat Enterprise Linux.

You must have a minimum of 10 GiB of available disk space. See Appendix B, *Partitioning reference* for more information.

To install Red Hat Enterprise Linux, you must have a minimum of 10 GiB of space in either unpartitioned disk space or in partitions that can be deleted. See Appendix B, *Partitioning reference* for more information.

Table A.1. Minimum RAM requirements

Installation type	Recommended minimum RAM
Local media installation (USB, DVD)	768 MiB
NFS network installation	768 MiB
HTTP or HTTPS network installation	1.5 GiB

NOTE

It is possible to complete the installation with less memory than the recommended minimum requirements. The exact requirements depend on your environment and installation path. It is recommended that you test various configurations to determine the minimum required RAM for your environment. Installing Red Hat Enterprise Linux using a Kickstart file has the same recommended minimum RAM requirements as a standard installation. However, additional RAM may be required if your Kickstart file includes commands that require additional memory, or write data to the RAM disk. See the *Performing an advanced RHEL installation* document for more information.

A.5. RAID REQUIREMENTS

It is important to understand how storage technologies are configured and how support for them may have changed between major versions of Red Hat Enterprise Linux.

Hardware RAID

Any RAID functions provided by the mainboard of your computer, or attached controller cards, need to be configured before you begin the installation process. Each active RAID array appears as one drive within Red Hat Enterprise Linux.

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 the dedicated hardware.

NOTE

When a pre-existing RAID array's member devices are all unpartitioned disks/drives, the installation program treats the array as a disk and there is no method to remove the array.

USB Disks

You can connect and configure external USB storage after installation. Most devices are recognized by the kernel, but some devices may not be recognized. If it is not a requirement to configure these disks during installation, disconnect them to avoid potential problems.

NVDIMM devices

To use a Non-Volatile Dual In-line Memory Module (NVDIMM) device as storage, the following conditions must be satisfied:

- Version of Red Hat Enterprise Linux is 7.6 or later.
- The architecture of the system is Intel 64 or AMD64.
- The device is configured to sector mode. Anaconda can reconfigure NVDIMM devices to this mode.
- The device must be supported by the nd_pmem driver.

Booting from an NVDIMM device is possible under the following additional conditions:

- The system uses UEFI.
- The device must be supported by firmware available on the system, or by a UEFI driver. The UEFI driver may be loaded from an option ROM of the device itself.
- The device must be made available under a namespace.

To take advantage of the high performance of NVDIMM devices during booting, place the **/boot** and **/boot/efi** directories on the device.

NOTE

The Execute-in-place (XIP) feature of NVDIMM devices is not supported during booting and the kernel is loaded into conventional memory.

Considerations for Intel BIOS RAID Sets

Red Hat Enterprise Linux uses **mdraid** for installing on Intel BIOS RAID sets. These sets are automatically detected during the boot process and their device node paths can change across several booting processes. For this reason, local modifications to the **/etc/fstab**, **/etc/crypttab** or other configuration files that refer to the devices by their device node paths may not work in Red Hat Enterprise Linux. It is recommended that you replace device node paths (such as **/dev/sda**) with file system labels or device UUIDs. You can find the file system labels and device UUIDs using the **blkid** command.

APPENDIX B. PARTITIONING REFERENCE

B.1. SUPPORTED DEVICE TYPES

Standard partition

A standard partition can contain a file system or swap space. Standard partitions are most commonly used for **/boot** and the **BIOS Boot** and **EFI System partitions**. LVM logical volumes are recommended for most other uses.

LVM

Choosing **LVM** (or Logical Volume Management) as the device type creates an LVM logical volume. If no LVM volume group currently exists, one is automatically created to contain the new volume; if an LVM volume group already exists, the volume is assigned. LVM can improve performance when using physical disks, and it allows for advanced setups such as using multiple physical disks for one mount point, and setting up software RAID for increased performance, reliability, or both.

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. You can dynamically expand the pool when needed for cost-effective allocation of storage space.

B.2. SUPPORTED FILE SYSTEMS

This section describes the file systems available in Red Hat Enterprise Linux.

xfs

XFS is a highly scalable, high-performance file system that supports file systems up to 16 exabytes (approximately 16 million terabytes), files up to 8 exabytes (approximately 8 million terabytes), and directory structures containing tens of millions of entries. **XFS** also supports metadata journaling, which facilitates quicker crash recovery. The maximum supported size of a single XFS file system is 500 TB. **XFS** is the default and recommended file system on Red Hat Enterprise Linux.

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 a single **ext4** file system is 50 TB.

ext3

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

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.

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.

vfat

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

BIOS Boot

A very small partition required for booting from a device with a GUID partition table (GPT) on BIOS systems and UEFI systems in BIOS compatibility mode.

EFI System Partition

A small partition required for booting a device with a GUID partition table (GPT) on a UEFI system.

PReP

This small boot partition is located on the first partition of the hard drive. The **PReP** boot partition contains the GRUB2 boot loader, which allows other IBM Power Systems servers to boot Red Hat Enterprise Linux.

B.3. SUPPORTED RAID TYPES

RAID stands for Redundant Array of Independent Disks, a technology which allows you to combine multiple physical disks into logical units. Some setups are designed to enhance performance at the cost of reliability, while others will improve reliability at the cost of requiring more disks for the same amount of available space.

This section describes supported software RAID types which you can use with LVM and LVM Thin Provisioning to set up storage on the installed system.

None

No RAID array will be set up.

RAID0

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

RAID1

Redundancy: Mirrors all data from one partition onto one or more other disks. Additional devices in the array provide increasing levels of redundancy. RAID 1 requires at least two disks.

RAID4

Error checking: Distributes data across multiple disks and uses one disk in the array to store parity information which safeguards the array in case any disk in the array fails. As all parity information is stored on one disk, access to this disk creates a "bottleneck" in the array’s performance. RAID 4 requires at least three disks.

RAID5

Distributed error checking: Distributes data and parity information across multiple disks. RAID 5 offers the performance advantages of distributing data across multiple disks, but does not share the performance bottleneck of RAID 4 as the parity information is also distributed through the array. RAID 5 requires at least three disks.

RAID6

Redundant error checking: RAID 6 is similar to RAID 5, but instead of storing only one set of parity data, it stores two sets. RAID 6 requires at least four disks.

RAID10

Performance and redundancy: RAID 10 is nested or hybrid RAID. It is constructed by distributing data over mirrored sets of disks. For example, a RAID 10 array constructed from four RAID partitions consists of two mirrored pairs of striped partitions. RAID 10 requires at least four disks.

B.4. RECOMMENDED PARTITIONING SCHEME

Red Hat recommends that you create separate file systems at the following mount points:

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

/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 8, 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. Base the file system size on the amount of data that is stored locally, number of users, and so on. You can upgrade or reinstall Red Hat Enterprise Linux 8 without erasing user data files. If you select automatic partitioning, it is recommended to have at least 55 GiB 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. 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 can provide 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 if you want sufficient memory for your system to hibernate. If you let the installation program partition your system automatically, the swap partition size is established using these guidelines. Automatic partitioning setup assumes hibernation is not in use. The maximum size of the swap partition is limited to 10 percent of the total size of the hard drive, and the installation program cannot create swap partitions more than 128 GB in size. To set up enough swap space to allow for hibernation, or if you want to set the swap partition size to more than 10 percent of the system's storage space, or more than 128 GB, you must edit the partitioning layout manually.

/boot/efi partition - recommended size of 200 MiB

UEFI-based AMD64, Intel 64, and 64-bit ARM require a 200 MiB EFI system partition. The recommended minimum size is 200 MiB, the default size is 600 MiB, and the maximum size is 600 MiB. BIOS systems do not require an EFI system partition.

Table B.1. 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
8 GB - 64 GB	4 GB to 0.5 times the amount of RAM	1.5 times the amount of RAM

Amount of RAM in the system	Recommended swap space	Recommended swap space if allowing for hibernation
More than 64 GB	Workload dependent (at least 4GB)	Hibernation not recommended

At the border between each range, 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 required. Choose partitions based on your particular system needs.

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.
- If you are unsure about how to configure partitions, accept the automatic default partition layout provided by the installation program.

PReP boot partition - recommended size of 4 to 8 MiB

When installing Red Hat Enterprise Linux on IBM Power System servers, the first partition of the hard drive should include a **PReP** boot partition. This contains the GRUB2 boot loader, which allows other IBM Power Systems servers to boot Red Hat Enterprise Linux.

B.5. ADVICE ON PARTITIONS

There is no best way to partition every system; the optimal setup depends on how you plan to use the system being installed. However, the following tips may help you find the optimal layout for your needs:

- Create partitions that have specific requirements first, for example, if a particular partition must be on a specific disk.
- Consider encrypting any partitions and volumes which 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, which contains user data.
- In some cases, creating separate mount points for directories other than /, **/boot** and **/home** may be useful; for example, on a server running a **MySQL** database, having a separate mount point for **/var/lib/mysql** will allow you to preserve the database during a reinstallation without having to restore it from backup afterwards. However, having unnecessary separate mount points will make storage administration more difficult.
- Some special restrictions apply to certain directories with regards on which partitioning layouts can they be placed. Notably, the **/boot** directory must always be on a physical partition (not on an LVM volume).

- If you are new to Linux, consider reviewing the *Linux Filesystem Hierarchy Standard* at http://refspecs.linuxfoundation.org/FHS_2.3/fhs-2.3.html for information about various system directories and their contents.

- Each kernel installed on your system requires approximately 20 MB on the /**boot** partition. The default partition size of 1 GB 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, and is used by the **DNF** package manager to temporarily store downloaded package updates. Make sure that the partition or volume containing /**var** has at least 3 GB.

- The contents of the /**var** directory usually change very often. This may cause problems with older solid state drives (SSDs), as they can handle a lower number of read/write cycles before becoming unusable. If your system root is on an SSD, consider creating a separate mount point for /**var** on a classic (platter) HDD.

- The /**usr** directory holds the majority of software on a typical Red Hat Enterprise Linux installation. The partition or volume containing this directory should therefore be at least 5 GB for minimal installations, and at least 10 GB for installations with a graphical environment.

- 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 boot-critical components. In some situations, such as when these directories are placed on an iSCSI drive or an FCoE location, the system may either be unable to boot, or it may 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 wish to remove data from other volumes. You can also select the **LVM Thin Provisioning** device type for the partition to have the unused space handled automatically by the volume.

- The size of an XFS file system can not be reduced - if you need to make a partition or volume with this file system smaller, you must back up your data, destroy the file system, and create a new, smaller one in its place. Therefore, if you expect needing to manipulate your partitioning layout later, you should use the ext4 file system instead.

- Use Logical Volume Management (LVM) if you anticipate expanding your storage by adding more hard drives or expanding virtual machine hard drives after the installation. With LVM, you can create physical volumes on the new drives, and then assign them to any volume group and logical volume as you see fit - for example, you can easily expand your system's /**home** (or any other directory residing on a logical volume).

- Creating a BIOS Boot partition or an EFI System Partition may be necessary, depending on your system's firmware, boot drive size, and boot drive disk label. See Section B.4, "Recommended partitioning scheme" for information about these partitions. Note that graphical installation will not let you create a BIOS Boot or EFI System Partition if your system does **not** require one - in that case, they will be hidden from the menu.

- If you need to make any changes to your storage configuration after the installation, Red Hat Enterprise Linux repositories offer several different tools which can help you do this. If you prefer a command line tool, try **system-storage-manager**.

APPENDIX C. TROUBLESHOOTING

The following sections cover various troubleshooting information which may be helpful when diagnosing installation issues.

C.1. CONSOLES AND LOGGING DURING INSTALLATION

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 actual 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 C.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**.

Shortcut	Contents
Ctrl+**b 5**	Program log; displays messages from other system utilities, stored in **/tmp/program.log**.

C.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**.

C.3. RESUMING AN INTERRUPTED DOWNLOAD ATTEMPT

You can resume an interrupted download using the **curl** command.

Prerequisite

You have navigated to the **Product Downloads** section of the Red Hat Customer Portal at https://access.redhat.com/downloads, and selected the required variant, version, and architecture. You have right-clicked on the required ISO file, and selected **Copy Link Location** to copy the URL of the ISO image file to your clipboard.

Procedure

1. Download the ISO image from the new link. Add the **--continue-at -** option to automatically resume the download:

```
$ curl --output directory-path/filename.iso 'new_copied_link_location' --continue-at -
```

2. Use a checksum utility such as **sha256sum** to verify the integrity of the image file after the download finishes:

```
$ sha256sum rhel-8.0-x86_64-dvd.iso
  `85a...46c rhel-8.0-x86_64-dvd.iso`
```

Compare the output with reference checksums provided on the Red Hat Enterprise Linux **Product Download** web page.

> **Example C.1. Resuming an interrupted download attempt**
>
> The following is an example of a **curl** command for a partially downloaded ISO image:
>
> ```
> $ curl --output _rhel-8.0-x86_64-dvd.iso
> 'https://access.cdn.redhat.com//content/origin/files/sha256/85/85a...46c/rhel-8.0-x86_64-dvd.iso?
> _auth=141...963' --continue-at -
> ```

PART II. INSTALLING RED HAT ENTERPRISE LINUX ON IBM POWER SYSTEM LC SERVERS

This section describes how to install Red Hat Enterprise Linux on the IBM Power Systems LC server.

CHAPTER 8. INSTALLING RED HAT ENTERPRISE LINUX ON IBM POWER SYSTEM LC SERVERS

This guide helps you install Red Hat Enterprise Linux on a Linux on Power Systems LC server. Use these instructions for the following IBM Power System servers:

- 8335-GCA (IBM Power System S822LC)
- 8335-GTA (IBM Power System S822LC)
- 8335-GTB (IBM Power System S822LC)
- 8001-12C (IBM Power System S821LC)
- 8001-22C (IBM Power System S822LC for Big Data)
- 9006-12P (IBM Power System LC921)
- 9006-22P (IBM Power System LC922)

8.1. OVERVIEW

Use this information to install Red Hat Enterprise Linux 8 on a non-virtualized or bare metal IBM Power System LC server. This procedure follows these general steps:

- Create a bootable USB device
- Connect to the BMC firmware to set up network connection
- Connect to the BMC firmware with IPMI
- Choose your installation method:
  - Install Red Hat Enterprise Linux from USB device
  - Install Red Hat Enterprise Linux with virtual media Download your ISO file from the Red Hat Enterprise Linux website.

Additional Resources

- For a list of virtualization options, see Supported Linux distributions and virtualization options for POWER8 and POWER9 Linux on Power systems.

8.1.1. Creating a bootable USB device on Linux

Follow this procedure to create a bootable USB device on a Linux system.

Prerequisites

- You have downloaded an installation ISO image as described in Section 4.5, “Downloading the installation ISO image”.
- The **Binary DVD** ISO image is larger than 4.7 GB, so you must have a USB flash drive that is large enough to hold the ISO image.

Procedure

NOTE

This procedure is destructive and data on the USB flash drive is destroyed without a warning.

1. Connect the USB flash drive to the system.
2. Open a terminal window and run the **dmesg** command:

   ```
   $ dmesg|tail
   ```

   The **dmesg** command returns a log that details all recent events. Messages resulting from the attached USB flash drive are displayed at the bottom of the log. Record the name of the connected device.

3. Switch to user root:

   ```
   $ su -
   ```

4. Enter your root password when prompted.
5. Find the device node assigned to the drive. In this example, the drive name is **sdd**.

   ```
   # dmesg|tail
   [288954.686557] usb 2-1.8: New USB device strings: Mfr=0, Product=1, SerialNumber=2
   [288954.686559] usb 2-1.8: Product: USB Storage
   [288954.686562] usb 2-1.8: SerialNumber: 000000009225
   [288954.712590] usb-storage 2-1.8:1.0: USB Mass Storage device detected
   [288954.712687] scsi host6: usb-storage 2-1.8:1.0
   [288954.712809] usbcore: registered new interface driver usb-storage
   [288954.716682] usbcore: registered new interface driver uas
   [288955.717140] scsi 6:0:0:0: Direct-Access     Generic  STORAGE DEVICE   9228 PQ: 0
   ANSI: 0
   [288955.717745] sd 6:0:0:0: Attached scsi generic sg4 type 0
   [288961.876382] sd 6:0:0:0: sdd Attached SCSI removable disk
   ```

6. Run the **dd** command to write the ISO image directly to the USB device.

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

   Replace */image_directory/image.iso* with the full path to the ISO image file that you downloaded, and replace *device* with the device name that you retrieved with the **dmesg** command. In this example, the full path to the ISO image is **/home/testuser/Downloads/rhel-8-x86_64-boot.iso**, and the device name is **sdd**:

   ```
   # dd if=/home/testuser/Downloads/rhel-8-x86_64-boot.iso of=/dev/sdd
   ```

   NOTE

   Ensure that you use the correct device name, and not the name of a partition on the device. Partition names are usually device names with a numerical suffix. For example, **sdd** is a device name, and **sdd1** is the name of a partition on the device **sdd**.

7. Wait for the **dd** command to finish writing the image to the device. The data transfer is complete when the **#** prompt appears. When the prompt is displayed, log out of the root account and unplug the USB drive. The USB drive is now ready to be used as a boot device.

8.1.2. Creating a bootable USB device on Windows

Follow the steps in this procedure to create a bootable USB device on a Windows system. The procedure varies depending on the tool. Red Hat recommends using Fedora Media Writer, available for download at https://github.com/FedoraQt/MediaWriter/releases.

> **NOTE**
>
> Fedora Media Writer is a community product and is not supported by Red Hat. You can report any issues with the tool at https://github.com/FedoraQt/MediaWriter/issues.

Prerequisites

- You have downloaded an installation ISO image as described in Section 4.5, "Downloading the installation ISO image".
- The **Binary DVD** ISO image is larger than 4.7 GB, so you must have a USB flash drive that is large enough to hold the ISO image.

Procedure

> **NOTE**
>
> This procedure is destructive and data on the USB flash drive is destroyed without a warning.

1. Download and install Fedora Media Writer from https://github.com/FedoraQt/MediaWriter/releases.

   > **NOTE**
   >
   > To install Fedora Media Writer on Red Hat Enterprise Linux, use the pre-built Flatpak package. You can obtain the package from the official Flatpak repository Flathub.org at https://flathub.org/apps/details/org.fedoraproject.MediaWriter.

2. Connect the USB flash drive to the system.
3. Open Fedora Media Writer.
4. From the main window, click **Custom Image** and select the previously downloaded Red Hat Enterprise Linux ISO image.
5. From **Write Custom Image** window, select the drive that you want to use.
6. Click **Write to disk**. The boot media creation process starts. Do not unplug the drive until the operation completes. The operation may take several minutes, depending on the size of the ISO image, and the write speed of the USB drive.
7. When the operation completes, unmount the USB drive. The USB drive is now ready to be used as a boot device.

8.1.3. Creating a bootable USB device on Mac OS X

Follow the steps in this procedure to create a bootable USB device on a Mac OS X system.

Prerequisites

- You have downloaded an installation ISO image as described in Section 4.5, “Downloading the installation ISO image”.
- The **Binary DVD** ISO image is larger than 4.7 GB, so you must have a USB flash drive that is large enough to hold the ISO image.

Procedure

> **NOTE**
>
> This procedure is destructive and data on the USB flash drive is destroyed without a warning.

1. Connect the USB flash drive to the system.
2. Identify the device path with the **diskutil list** command. The device path has the format of */dev/disknumber*, where number is the number of the disk. The disks are numbered starting at zero (0). Typically, Disk 0 is the OS X recovery disk, and Disk 1 is the main OS X installation. In the following example, the USB device 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
```

3. To identify your USB flash drive, compare the NAME, TYPE and SIZE columns to your flash drive. For example, the NAME should be the title of the flash drive icon in the **Finder** tool. You can also compare these values to those in the information panel of the flash drive.
4. 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 the command completes, the icon for the flash drive disappears from your desktop. If the icon does not disappear, you may have selected the wrong disk. Attempting to unmount the system disk accidentally returns a **failed to unmount** error.

5. Log in as root:

   ```
   $ su -
   ```

6. Enter your root password when prompted.

7. 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/rdisknumber character device is faster than writing to the /dev/disknumber block device.

8. To write the */Users/user_name/Downloads/rhel-8-x86_64-boot.iso* file to the */dev/rdisk2* device, run the following command:

   ```
   # sudo dd if=/Users/user_name/Downloads/rhel-8-x86_64-boot.iso of=/dev/rdisk2
   ```

9. Wait for the **dd** command to finish writing the image to the device. The data transfer is complete when the **#** prompt appears. When the prompt is displayed, log out of the root account and unplug the USB drive. The USB drive is now ready to be used as a boot device.

8.2. COMPLETING THE PREREQUISITES AND BOOTING YOUR FIRMWARE

Before you power on the system, ensure that you have the following items:

- Ethernet cable
- VGA monitor. The VGA resolution must be set to 1024x768-60Hz.
- USB Keyboard
- Power cords and outlet for your system.
  - PC or notebook that has IPMItool level 1.8.15 or greater. (Verifying this piece of info)
  - Bootable USB device

Complete these steps:

1. If your system belongs in a rack, install your system into that rack. For instructions, see IBM Power Systems information at https://www.ibm.com/support/knowledgecenter/.

2. Connect an Ethernet cable to the embedded Ethernet port next to the serial port on the back of your system. Connect the other end to your network.

3. Connect your VGA monitor to the VGA port on back of system.
4. Connect your USB keyboard to an available USB port.
5. Connect the power cords to the system and plug them into the outlets.

At this point, your firmware is booting. Wait for the green LED on the power button to start flashing, indicating that it is ready to use. If your system does not have a green LED indicator light, then wait 1 to 2 minutes.

8.3. CONFIGURING THE IP ADDRESS IBM POWER

To set up or enable your network connection to the baseboard management controller (BMC) firmware, use the Petitboot bootloader interface. Follow these steps:

1. Power on your server using the power button on the front of your system. Your system will power on to the Petitboot bootloader menu. This process takes about 1 - 2 minutes to complete. Do not walk away from your system! When Petitboot loads, your monitor will become active and you will need to push any key in order to interrupt the boot process.
2. At the Petitboot bootloader main menu, select Exit to Shell.
3. Run **ipmitool lan print 1**. If this command returns an IP address, verify that is correct and continue. To set a static IP address, follow these steps:
    a. Set the mode to static by running this command: **ipmitool lan set 1 ipsrc static**
    b. Set your IP address by running this command: **ipmitool lan set 1 ipaddr *ip_address*** where *ip_address* is the static IP address that you are assigning to this system.
    c. Set your netmask by running this command: **ipmitool lan set 1 netmask *netmask_address*** where *netmask_address* is the netmask for the system.
    d. Set your gateway server by running this command: **ipmitool lan set 1 defgw ipaddr *gateway_server*** where gateway_server is the gateway for this system.
    e. Confirm the IP address by running the command i`pmitool lan print 1` again.
    This network interface is not active until after you perform the following steps:
4. To reset your firmware, run the following command: **ipmitool mc reset cold**.
    This command must complete before continuing the process; however, it does not return any information. To verify that this command has completed, ping your system BMC address (the same IP address used in your IPMItool command). When the ping returns successfully, continue to the next step.
    a. If your ping does not return successfully within a reasonable amount of time (2 - 3 minutes), try these additional steps:
        i. Power your system off with this command: **ipmitool power off**.
        ii. Unplug the power cords from the back of the system. Wait 30 seconds and then apply power to boot BMC.

8.4. POWERING ON YOUR SERVER WITH IPMI

Intelligent Platform Management Interface (IPMI) is the default console to use when connecting to the OPAL firmware.

Use the default values for IPMI:

- Default user: **ADMIN**
- Default password: **admin**

NOTE

After your system powers on, the Petitboot interface loads. If you do not interrupt the boot process by pressing any key within 10 seconds, Petitboot automatically boots the first option. To power on your server from a PC or notebook that is running Linux, follow these steps:

1. Open a terminal program on your PC or notebook.
2. To power on your server, run the following command:

   ```
   ipmitool -I lanplus -H server_ip_address -U ipmi_user -P ipmi_password chassis power on
   ```

   where *server_ip_ipaddress* is the IP address of the Power system and *ipmi_password* is the password set up for IPMI.

   NOTE

   If your system is already powered on, continue to activate your IPMI console.

3. Activate your IPMI console by running this command

   ```
   ipmitool -I lanplus -H server_ip_address -U ipmi_user -P ipmi_password sol activate
   ```

NOTE

Use your keyboard up arrow to display the previous **ipmitool** command. You can edit previous commands to avoid typing the entire command again. If you need to power off or reboot your system, deactivate the console by running this command:

```
ipmitool -I lanplus -H server_ip_address -U user-name -P ipmi_password
sol deactivate
```

To reboot the system, run this command:

```
ipmitool -I lanplus -H server_ip_address -U user-name -P ipmi_password chassis
power reset
```

8.5. CHOOSE YOUR INSTALLATION METHOD ON IBM LC SERVERS

You can either install Red Hat Enterprise Linux from a USB device or through virtual media.

8.5.1. Configuring Petitboot for installation with USB device

After the system powers on, the Petitboot bootloader scans local boot devices and network interfaces to find boot options that are available to the system. For information about creating a bootable USB device, see Section 8.1.1, "Creating a bootable USB device on Linux" .

Use one of the following USB devices:

- USB attached DVD player with a single USB cable to stay under 1.0 Amps
- 8 GB 2.0 USB flash drive

Follow these steps to configure Petitboot:

1. Insert your bootable USB device into the front USB port. Petitboot displays the following option:

   ```
   [USB: sdb1 / 2015-10-30-11-05-03-00]
      Rescue a Red Hat Enterprise Linux system (64-bit kernel)
      Test this media & install Red Hat Enterprise Linux 8.0  (64-bit kernel)
    *  Install Red Hat Enterprise Linux 8.0 (64-bit kernel)
   ```

   NOTE

   Select Rescan devices if the USB device does not appear. If your device is not detected, you may have to try a different type.

2. Record the UUID of the USB device. For example, the UUID of the USB device in the above example is 2015-10-30-11-05-03-00.

3. Select Install Red Hat Enterprise Linux 8.0 (64-bit kernel) and press e (Edit) to open the Petitboot Option Editor window.

4. Move the cursor to the Boot arguments section and add the following information:

   ```
   inst.stage2=hd:UUID=your_UUID
   where your_UUID is the UUID that you recorded.
   Petitboot Option Editor
   qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
   qqq

     Device:    ( ) sda2 [f8437496-78b8-4b11-9847-bb2d8b9f7cbd]
                (*) sdb1 [2015-10-30-11-05-03-00]
                ( ) Specify paths/URLs manually

                     Kernel:         /ppc/ppc64/vmlinuz
                     Initrd:         /ppc/ppc64/initrd.img
                     Device tree:
                     Boot arguments: ro inst.stage2=hd:UUID=2015-10-30-11-05-03-00

                       [    OK    ] [   Help   ] [  Cancel  ]
   ```

5. Select OK to save your options and return to the Main menu.

6. Verify that Install Red Hat Enterprise Linux 8.x (64-bit kernel) is selected and then press Enter to begin your installation.

8.5.2. Access BMC Advanced System Management interface to configure virtual media

Baseboard Management Controller (BMC) Advanced Systems Management is a remote management controller used to access system information, status, and other process for your server. You can use the BMC Advanced Systems Management to set up your installation and provide the CD image as virtual media to the Power System. However, the actual installation requires a serial-over-LAN (SOL) connection through IPMI.

To access the BMC Advanced Systems Management, open a web browser to **http://*ip_address*** where *ip_address* is the IP address for the BMC. Log in using these default values:

- Default user name: ADMIN
- Default password: admin

In order to fully use the BMC Advanced Systems Management, you need to add the IP address of the BMC firmware to the Exceptions list in the Java Control Panel of your laptop or PC. On a Windows system, this is usually located by selecting Control Panel > Control Panel for Java.

On a Linux system, this is usually located by selecting the Control Center and then selecting the Java web browser plugin.

After accessing the Control Panel for Java, select Security tab. Then add the IP address of the BMC firmware to the Exceptions list, by clicking Edit Site List and then clicking Add. Enter the IP address and click OK.

To create a virtual CD/DVD, follow these steps:

1. Log into the BMC Advanced Systems Management interface from a PC or notebook using the default user name and password.
2. **Select** Remote Control > Console Redirection.
3. **Select** Java Console. As the console opens, you might need to direct your browser to open the **jviewer.jnlp** file by selecting to Open with Java Web Start and click OK. Accept the warning and click Run.
4. In the Console Redirection window, **select** Media > Virtual Media wizard from the menu.
5. In the Virtual Media wizard, **select** CD/DVD Media:1.
6. **Select** CD Image and the path to the Linux distribution ISO file. For example, **/tmp/RHEL-7.2-20151030.0-Server-ppc64el-dvd1.iso**. Click Connect CD/DVD. If the connection is successful, the message Device redirected in Read Only Mode is displayed.
7. Verify that CD/DVD is shown as an option in Petitboot as **sr0**:

```
CD/DVD: sr0
        Install
        Repair
```

NOTE

Select Rescan devices if CD/DVD does not appear.

8. **Select** Install. Ater selecting Install, your remote console may become inactive. Open or reactivate your IPMI console to complete the installation.

NOTE

Be patient! It can sometimes take a couple minutes for the installation to begin.

8.6. COMPLETING YOUR LC SERVER INSTALLATION

After you select to boot the Red Hat Enterprise Linux 8 (RHEL) installer, the installer wizard walks you through the steps.

1. Follow the installation wizard for RHEL to set up disk options, your user name and password, time zones, and so on. The last step is to restart your system.

   NOTE

   While your system is restarting, remove the USB device.

2. After the system restarts, Petitboot displays the option to boot Red Hat Enterprise Linux 8. **Select** this option and press Enter.

PART III. INSTALLING RED HAT ENTERPRISE LINUX ON IBM POWER SYSTEM AC SERVERS

This section describes how to install Red Hat Enterprise Linux on the IBM Power Systems accelerated server.

CHAPTER 9. INSTALLING RED HAT ENTERPRISE LINUX ON IBM POWER SYSTEM ACCELERATED SERVERS

This guide helps you install Red Hat Enterprise Linux on an IBM Power Systems accelerated server (AC). Use these instructions for the following IBM Power System servers:

- 8335-GTG (IBM Power System AC922)
- 8335-GTH (IBM Power System AC922)
- 8335-GTX (IBM Power System AC922)

9.1. OVERVIEW

Use this information to install Red Hat Enterprise Linux on a non-virtualized, or bare metal IBM Power System accelerated server. This procedure follows these general steps:

- Connect to the BMC firmware to set up network connection
- Choose your installation method:
  - Install Red Hat Enterprise Linux from USB device
  - Install Red Hat Enterprise Linux from network
- Install Red Hat Enterprise Linux

Additional resources

- For a list of supported Red Hat Enterprise Linux versions, see Supported Linux distributions for POWER8 and POWER9 Linux on Power systems.

9.2. COMPLETING THE PREREQUISITES AND BOOTING YOUR FIRMWARE

Before you power on the system, ensure that you have the following items:

- Ethernet cable
- VGA monitor. The VGA resolution must be set to 1024x768-60Hz.
- USB Keyboard
- Power cords and outlet for your system

These instructions require that you have a network server set up with Red Hat Enterprise Linux 7.x. Download Red Hat Enterprise Linux 7.x LE ALT at https://access.redhat.com/products/red-hat-enterprise-linux/#addl-arch.

1. Take the link for **Downloads for Red Hat Enterprise Linux for Power, little endian**
2. Log into your Red Hat account (if you have not already done so). Select **Red Hat Enterprise Linux for Power 9** from the Product Variant list.

3. Look for the Red Hat Enterprise Linux for Power 9 (v. 7.x for ppc64le) ISO file. The downloaded ISO file will include ***rhel-alt......iso*** rather than ***rhel....iso*** in the path name.

Complete these steps:

- If your system belongs in a rack, install your system into that rack. For instructions, see IBM Power Systems information at https://www.ibm.com/support/knowledgecenter/POWER9/p9hdx/POWER9welcome.htm.
- Connect an Ethernet cable to the embedded Ethernet port next to the serial port on the back of your system. Connect the other end to your network.
- Connect your VGA monitor to the VGA port on back of system.
- Connect your USB keyboard to an available USB port.
- Connect the power cords to the system and plug them into the outlets.

At this point, your firmware is booting. Wait for the green LED on the power button to start flashing, indicating that it is ready to use. If your system does not have a green LED indicator light, then wait 1 to 2 minutes.

9.3. CONFIGURING THE FIRMWARE IP ADDRESS

To set up or enable your network connection to the BMC firmware, use the Petitboot bootloader interface. Follow these steps:

1. Power on your server using the power button on the front of your system. Your system will power on to the Petitboot bootloader menu. This process usually takes about 1 - 2 minutes to complete, but may take 5 - 10 minutes on the first boot or after a firmware update. Do not walk away from your system! When Petitboot loads, your monitor will become active and you will need to push any key in order to interrupt the boot process.
2. At the Petitboot bootloader main menu, select Exit to Shell.
3. Run **ipmitool lan print 1**. If this command returns an IP address, verify that is correct and continue to step 4. If no IP addresses are returned, follow these steps:
    a. Set the mode to static by running this command:

    ```
    ipmitool lan set 1 ipsrc static
    ```

    b. Set your IP address by running this command:

    ```
    ipmitool lan set 1 ipaddr _ip_address_
    ```

    Where *ip_address* is the static IP address that you are assigning to this system.

    c. Set your netmask by running this command:

    ```
    ipmitool lan set 1 netmask _netmask_address_
    ```

    Where netmask_address is the netmask for the system.

    d. Set your gateway server by running this command:

```
ipmitool lan set 1 defgw ipaddr _gateway_server_
```

```
Where gateway_server is the gateway for this system.
```

e. Confirm the IP address by running the command **ipmitool lan print 1** again.

NOTE

This interface is not active until after you perform the following steps.

f. To reset your firmware, run the following command:

```
ipmitool raw 0x06 0x40.
```

This command must complete before continuing the process; however, it does not return any information. To verify that this command has completed, ping your system BMC address (the same IP address used in your IPMItool command). When the ping returns successfully, continue to the next step.

NOTE

Note: If your ping does not return successfully within a reasonable amount of time (2 - 3 minutes), try these additional steps

g. Power your system off with this command: **poweroff.h.**

h. Unplug the power cords from the back of the system. Wait 30 seconds and then apply power to boot BMC.

9.4. POWERING ON YOUR SERVER WITH OPENBMC COMMANDS

NOTE

After your system powers on, the Petitboot interface loads. If you do not interrupt the boot process by pressing any key within 10 seconds, Petitboot automatically boots the first option.

To power on your server from a PC or notebook that is running Linux, follow these steps:

- Default user name: **root**
- Default password: **0penBmc** (where, 0penBMC is using a zero and not a capital O)

1. Open a terminal program on your PC or notebook.
2. Log in to the BMC by running the following commands.

```
ssh root@<BMC server_ip_address>
root@<BMC server password>
```

Where *BMC server_ip_address* is the IP address of the BMC and *BMC server password* is the password to authenticate.

3. To power on your server, run the following command:

```
$ root@witherspoon:~# obmcutil poweron
```

4. Connect to OS console and use the default password **0penBmc**.

```
ssh -p 2200 root@<BMC server_ip_address> root@
```

Where *BMC server_ip_address* is the IP address of the BMC and *BMC server password* is the password to authenticate.

9.5. CHOOSE YOUR INSTALLATION METHOD ON IBM ACCELERATED SERVERS

You can either install Red Hat Enterprise Linux from a USB device or through the network.

9.6. CONFIGURING PETITBOOT FOR NETWORK INSTALLATION

After the system powers on, the Petitboot bootloader scans local boot devices and network interfaces to find boot options that are available to the system. To install Red Hat Enterprise Linux from a network server, you need to set up a network interface (that is not the BMC network interface).

Set up a network connection and provide the network boot detail to Petitboot by following these steps:

a. Connect an Ethernet cable to the second Ethernet port on the back of your system. Connect the other end to your network.

b. On the Petitboot main screen, select c to configure your system options.

c. In the Network field of the configuration screen, enter your network information:

   i. Select your network type

   ii. Select your network device (remember the interface name and mac address)

   iii. Specify your IP/mask, Gateway, and DNS server (remember these setting as you will need them in the next step)

   iv. Select OK to return to the main menu.

d. Back on the Petitboot main screen, select **n** to create new options.

e. Choose your boot device or select to Specify paths/URLs manually and then enter your boot options:

   i. In the Kernel field, enter the path to the kernel. This field is mandatory. Enter a URL similar to this one for a network:

   ```
   http://&lt;http_server_ip&gt;/ppc/ppc64/vmlinuz
   ```

   ii. In the Initrd field, enter the path to the init ramdisk. Enter a URL similar to this one for a network:

   ```
   http://&lt;http_server_ip&gt;/ppc/ppc64/initrd.gz
   ```

iii. In the Boot parameter field, set up the set up the repository path and the IP address of the server where the operating system is installed. For example:

```
append repo=http://<http_server_ip>/
root=live:http://<http_server_ip>/os/LiveOS/squashfs.img ipv6.disable=1 ifname=
<ethernet_interface_name>:<mac_addr> ip=<os ip>::<gateway>:<2 digit mask>:
<hostname>:<ethernet_interface_name>:none nameserver=<anem_server> inst.text
```

You can accept the defaults for the rest of the fields.

f. After you set your netboot options, select OK and press Enter.

g. On the Petitboot main window, select User Item 1 as your boot option and press Enter.

9.7. CONFIGURING PETITBOOT FOR INSTALLATION WITH USB DEVICE ON ACCELERATED SERVERS

After the system powers on, the Petitboot bootloader scans local boot devices and network interfaces to find boot options that are available to the system. For information about creating a bootable USB device, see Section 8.1.1, "Creating a bootable USB device on Linux" .

Use one of the following USB devices:

- USB attached DVD player with a single USB cable to stay under 1.0 Amps
- 8 GB 2.0 USB flash drive

Follow these steps to configure Petitboot:

1. Insert your bootable USB device into the front USB port. Petitboot displays the following:

```
[USB: sdb1 / 2015-10-30-11-05-03-00]

   Rescue a Red Hat Enterprise Linux system (64-bit kernel)
   Test this media & install Red Hat Enterprise Linux 8.x  (64-bit kernel)

 *  Install Red Hat Enterprise Linux 8.x (64-bit kernel)
```

NOTE

Select Rescan devices if the USB device does not appear. If your device is not detected, you may have to try a different type.

2. Record the UUID of the USB device. For example, the UUID of the USB device in the above example is 2015-10-30-11-05-03-00.

3. Select Install Red Hat Enterprise Linux 8.x (64-bit kernel) and press e (Edit) to open the Petitboot Option Editor window.

4. Move the cursor to the Boot arguments section and add the following information:

```
    inst.text inst.stage2=hd:UUID=your_UUID
    where your_UUID is the UUID that you recorded.
    Petitboot Option Editor
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
qqqqqq

            Device:   ( ) sda2 [f8437496-78b8-4b11-9847-bb2d8b9f7cbd]
                      (*) sdb1 [2015-10-30-11-05-03-00]
                      ( ) Specify paths/URLs manually

            Kernel:      /ppc/ppc64/vmlinuz
            Initrd:      /ppc/ppc64/initrd.img
            Device tree:
            Boot arguments: ro inst.text inst.stage2=hd:UUID=2015-10-30-11-05-03-00

              [    OK    ]  [   Help   ]  [  Cancel  ]
```

5. **Select** OK to save your options and return to the Main menu.

6. Verify that Install Red Hat Enterprise Linux 8.x (64-bit kernel) is selected and then **press** Enter to begin your installation.

9.8. COMPLETING YOUR ACCELERATED SERVER INSTALLATION

After you select to boot the Red Hat Enterprise Linux 8.x installer, the installer wizard walks you through the steps.

a. Follow the installation wizard for Red Hat Enterprise Linux to set up disk options, your user name and password, time zones, and so on. The last step is to restart your system.

> **NOTE**
>
> While your system is restarting, remove the USB device.

b. After the system restarts, Petitboot displays the option to boot Red Hat Enterprise Linux 8.x. Select this option and press Enter.

PART IV. INSTALLING RED HAT ENTERPRISE LINUX ON IBM POWER SYSTEM L SERVERS

This section describes how to install Red Hat Enterprise Linux on the IBM L servers.

CHAPTER 10. INSTALLING RED HAT ENTERPRISE LINUX ON IBM POWER SYSTEM L SERVER

This guide helps you install Red Hat Enterprise Linux on an IBM Power System L server. Use these instructions for the following IBM Power System servers:

- 88247-22L (IBM Power System S822L)
- 8247-21L (IBM Power System S812L)
- 8247-42L (IBM Power System S824L)

For a list of supported distributions, see Supported Linux distributions for POWER8 and POWER9 Linux on Power systems.

10.1. OVERVIEW

Use this information to install Red Hat Enterprise Linux on a non-virtualized or bare metal IBM Power System L server. This procedure follows these general steps:

- Complete prerequisites
- Connecting to the ASMI
  - Connect using DHCP
  - Connect using Static IP
- Enabling IPMI
- Powering on your server with IPMI
  - Connecting from Linux notebook
  - Connecting from Windows notebook
- Configuring Petitboot and installing Red Hat Enterprise Linux

10.2. COMPLETING THE PREREQUISITES AND BOOTING YOUR FIRMWARE ON L SERVER

Before you install Red Hat Enterprise Linux, ensure that you have the following items:

- Ethernet cable
- VGA monitor. The VGA resolution must be set to 1024x768-60Hz.
- USB Keyboard
- Power cords and outlet for your system

Before you power on the system, follow these steps:

- If your system belongs in a rack, install your system into that rack. For instructions, see IBM Power Systems information at https://www.ibm.com/support/knowledgecenter/.

- Remove the shipping brackets from the power supplies. Ensure that the power supplies are fully seated in the system
- Access the server control panel.
- Connect the power cords to the system and plug them into the outlets.

At this point, your firmware is booting. Wait for the green power LED on the control panel to start flashing, indicating that it is ready to use, and for the prompt 01 N OPAL T to appear on the display.

10.3. CONNECTING TO ASMI WITH DHCP

To connect to the Advanced System Management Interface (ASMI) you need to set up your network connection. You can set up DHCP or static IP.

Use this type of connection if you are using DHCP. Use these steps to find the IP address of the service processor and then connect with the ASMI web interface. If you know what IP address that your server is using, complete step 1 and then skip to Step 5: Enabling

1. Connect an Ethernet cable to the HMC1 or HMC2 port on the back of your Power system to your DHCP network.
2. Access the control panel for your server.
3. Scroll to function 02 using Increment **(↑)** or Decrement **(↓)** buttons (up and down arrows) and then press Enter.
4. Move the cursor to the N by pressing Enter. The display looks like this example: **02 A N< T**
5. Change N to M to start manual mode using the Increment **(↑)** or Decrement **(↓)** buttons. The display looks like this example: **02 A M< T**
6. Press Enter two times to exit the mode menu.
7. Scroll to function 30 using Increment or Decrement buttons
8. Press Enter to enter subfunction. The display looks like this example: **30****
9. Use the Increment **(↑)** or Decrement **(↓)** buttons to select a network device. 3000 displays the IP address that is assigned to ETH0 (HMC1). 3001 displays the IP address that is assigned to ETH1 (HMC2)
10. Press Enter to display the selected IP address. Be sure to record this IP address.
11. Use the Increment **(↑)** or Decrement **(↓)** buttons to select subfunction exit (30**).
12. Press Enter to exit subfunction mode.
13. Scroll to 02 using Increment **(↑)** or Decrement **(↓)** buttons and press Enter.
14. Change the mode to N. The display looks like this example: **02 A N< T**

10.4. CONNECTING TO ASMI WITH STATIC IP ADDRESS

Use this type of connection if you are using a static IP address. This connection configures a console interface to the ASMI.

1. Connect an Ethernet cable from the PC or notebook to the Ethernet port labeled HMC1 on the back of the managed system.

2. Set your IP address on your PC or notebook to match the default values on your Power system. IP address on PC or notebook:

```
169.254.2.140 Subnet mask: 255.255.255.0
The default IP address of HMC1: 169.254.2.147
```

NOTE

The default values of HMC1 are already set and you do not need to change them. If you want to verify the IP address, follow the steps in Connecting to ASMI with DHCP to find the IP addresses with the control panel.

If you are running Linux on your PC or notebook, set your IP address by following these steps:

1. Log in as root.

2. Start a terminal session.

3. Run the follow command: ifconfig -a. Record these values so that you can reset your network connection later.

4. Type **ifconfig *ethx* 169.254.2.140 netmask 255.255.255.0**. Replace *ethx* with either eth0 or eth1, depending on what your PC or notepad is using.

If you are running Windows 7 on your PC or notebook, set your IP address by following these steps:

1. **Click** Start > Control Panel.

2. **Select** Network and Sharing Center.

3. **Click** the network that is displayed in Connections.

4. **Click** Properties.

5. If the Security dialog box is displayed, **click** Continue.

6. **Select** Internet Protocol Version 4.

7. **Click** Properties.

8. **Select** Use the following IP address.

9. **Use 169.254.2.140** for IP address and **255.255.255.0** for Subnet mask.

10. **Click** OK > Close > Close

NOTE

If HMC1 is occupied, use HMC2. Use IP address 169.254.3.140 and Subnet mask: 255.255.255.0 on your PC or notebook. The default IP address of the HMC2 is 169.254.3.147.

10.5. ENABLING IPMI

1. The first time that you connect to the firmware, enter the admin ID admin and password admin. After you log in, you will be forced to change the password. Be sure to record this password!

2. From the main menu, select System Configuration→Firmware Configuration. Verify that OPAL is selected as your Hypervisor Mode.

3. Follow these steps to set a password for your IPMI session:

   a. From the main menu, select Login Profile → Change Passwords.

   b. Select IPMI from the list of user IDs.

   c. Enter the current password for the administrator (set in step 2) and then enter and confirm a password for IPMI.

   d. Click Continue.

4. If your Power system is not using DHCP, you need to configure Network access. From the main menu, select Network Services > Network Configuration. To configure network access, follow these steps:

   a. From the Network Configuration display, select IPv4 and Continue.

   b. Select Configure this interface?

   c. Verify that IPv4 is enabled.

   d. Select Static for the type of IP address.

   e. Enter a name for the host system.

   f. Enter an IP address for the system.

   g. Enter a subnet mask.

   h. At the bottom of the page, enter a default gateway, Domain name, and IP address for the DNS server.

   i. After you set the values for the Network configuration, click Continue.

   j. Click Save Settings.

   k. If you connected with a PC or notebook, you can remove the Ethernet cable from your PC or notebook and connect it to the network switch. To continue with a console connection, change the default IP address to the IP address that you assigned to the service processor.

10.6. POWERING ON YOUR L SERVER WITH IPMI

Intelligent Platform Management Interface (IPMI) is the default console to use when you configure your Power system. If you are using a Linux notebook or PC, use the **ipmitool** utility. If you are using a Windows notebook or PC, use the **ipmiutil** utility.

As the system powers up, you might notice the following actions:

- System reference codes appear on the control panel display while the system is being started.

- The system cooling fans are activated after approximately 30 seconds and accelerate to operating speed.
- The power LED on the control panel stops flashing and remains on, indicating that system power is on.

NOTE

After your system powers on, the Petitboot interface loads. If you do not interrupt the boot process by pressing any key within 10 seconds, Petitboot automatically boots the first option.

10.7. POWERING ON YOUR SYSTEM FROM A NOTEBOOK OR PC RUNNING LINUX

To power on your server from a notebook or PC running Linux, follow these steps:

1. Open a terminal program.
2. To power on your server, run the following command:

   ```
   ipmitool -I lanplus -H fsp_ip_address -P _ipmi_password_ power on
   ```

   Where *ipaddress* is the IP address of the Power system and *ipmi_password* is the password set up for IPMI.
3. Immediately activate your IPMI console by running this command:

   ```
   ipmitool -I lanplus -H fsp_ip_address -P ipmi_password sol activate
   ```

   TIP

   Use your keyboard up arrow to display the previous **ipmitool** command. You can edit previous commands to avoid typing the entire command again.

NOTE

If you need to restart your system, follow these steps:

1. Deactivate the console by running this command:

   ```
   ipmitool -I lanplus -H fsp_ip_address -P ipmi_password sol deactivate
   ```

2. Power your system off with this command:

   ```
   ipmitool -I lanplus -H fsp_ip_address -P ipmi_password power off
   ```

3. Power your system on with this command:

   ```
   ipmitool -I lanplus -H fsp_ip_address -P ipmi_password power on
   ```

NOTE

If you have not already done so, insert your DVD into the DVD drive or confirm the installer image in your network

10.8. POWERING ON YOUR SYSTEM FROM A NOTEBOOK OR PC RUNNING WINDOWS

To power on your server from a notebook or PC running Windows, follow these steps:

1. Open a command prompt and change the directory to **C:\Program Files\sourceforge\ipmiutil**

2. To power on your server, run the following command

   ```
   ipmiutil power -u -N ipaddress -P ipmi_password
   ```

   Where *ipaddress* is the IP address of the Power system and *ipmi_password* is the password set up for IPMI.

3. Immediately activate your IPMI console by running this command:

   ```
   ipmiutil sol -a -r -N ipaddress -P ipmi_password
   ```

TIP

Use your keyboard up arrow to display the previous **ipmiutil** command. You can edit previous commands to avoid typing the entire command again.

NOTE

If you need to restart your system, follow these steps: . Deactivate the console by running this command:

```
ipmiutil sol -d -N ipaddress -P ipmi_password
```

1. Power your system off with this command:

```
ipmiutil power -d -N ipaddress -P ipmi_password
```

1. Power your system on with this command:

```
ipmiutil power -u -N ipaddress -P ipmi_password
```

NOTE

If you have not already done so, insert your DVD into the DVD drive or confirm the installer image in your network.

10.9. CONFIGURING PETITBOOT AND INSTALLING RED HAT ENTERPRISE LINUX

After the system powers on, the Petitboot bootloader scans local boot devices and network interfaces to find boot options that are available to the system. If you do not have network connectivity or the installation DVD in the disk drive, there will not be any boot options listed.

1. On the Petitboot main screen, verify that you are booting Red Hat Enterprise Linux 8.0 from the DVD drive.

2. Select the Red Hat Enterprise Linux installer boot option and then press Enter.

3. The installation will begin.

NOTE

If you do not interrupt the boot process by pressing any key within 10 seconds after the Petitboot main screen appears, Petitboot automatically boots the first option.

PART V. INSTALLING RED HAT ENTERPRISE LINUX ON IBM Z

This section describes how to install Red Hat Enterprise Linux on the IBM Z architecture.

CHAPTER 11. PREPARING FOR INSTALLATION ON IBM Z

11.1. OVERVIEW OF THE IBM Z INSTALLATION PROCESS

You can install Red Hat Enterprise Linux on IBM Z interactively or in unattended mode. Installation on IBM Z differs from installation on other architectures in that it is typically performed over a network and not from local media. The installation consists of two phases:

1. **Booting the installation**
    - Connect with the mainframe
    - Perform an initial program load (IPL), or boot, from the medium containing the installation program.
2. **Anaconda**
   Use the **Anaconda** installation program to:
    - Configure the network
    - Specify language support
    - Specify installation source
    - Specify software packages to be installed
    - Perform the rest of the installation

11.2. PLANNING FOR INSTALLATION ON IBM Z

11.2.1. Pre-installation

Red Hat Enterprise Linux 8 runs on z13 or later IBM mainframe systems.

The installation process assumes that you are familiar with the IBM Z and can set up *logical partitions* (LPARs) and z/VM guest virtual machines.

For installation of Red Hat Enterprise Linux on IBM Z, Red Hat supports Direct Access Storage Device (DASD) and Fiber Channel Protocol (FCP) storage devices.

Pre-installation decisions

- Whether the operating system is to be run on an LPAR or as a z/VM guest operating system.
- If swap space is needed, and how much. Although it is recommended to assign enough memory to a z/VM guest virtual machine and let z/VM do the necessary swapping, there are cases where the amount of required RAM is hard to predict. Such instances should be examined on a case-by-case basis.
- Network configuration. Red Hat Enterprise Linux 8 for IBM Z supports the following network devices:
    - Real and virtual *Open Systems Adapter* (OSA)
    - Real and virtual HiperSockets

  - *LAN channel station* (LCS) for real OSA

Disk space

You will need to calculate and allocate sufficient disk space on DASDs or SCSI disks.

- A minimum of 10 GB is needed for a server installation, 20 GB if you want to install all packages.
- Disk space is also required for any application data. After the installation, you can add or delete more DASD or SCSI disk partitions.
- The disk space used by the newly installed Red Hat Enterprise Linux system (the Linux instance) must be separate from the disk space used by other operating systems you have installed on your system.

RAM

You will have to ensure enough RAM is available.

- 1 GB is recommended for the Linux instance. With some tuning, an instance might run with as little as 512 MB RAM.
- If installing from nfs, 1 GB is sufficient. However, if installing from an http source, 1.5 GB is needed.
- Running at 512 MB in text mode can be done only when installing from nfs.

> **NOTE**
>
> When initializing swap space on a Fixed Block Architecture (FBA) DASD using the **SWAPGEN** utility, the **FBAPART** option must be used.

Additional Resources

- For additional information on IBM Z, see http://www.ibm.com/systems/z.

11.3. INSTALLING UNDER Z/VM

Use the **x3270** or **c3270** terminal emulator, to log in to z/VM from other Linux systems, or use the IBM 3270 terminal emulator on the IBM Z Hardware Management Console (HMC). If you are running Microsoft Windows operating system, there are several options available, and can be found through an internet search. A free native Windows port of **c3270** called **wc3270** also exists.

When installing under z/VM, you can boot from:

- The z/VM virtual reader
- A DASD or an FCP-attached SCSI device prepared with the **zipl** boot loader
- An FCP-attached SCSI DVD drive

1. Log on to the z/VM guest virtual machine chosen for the Linux installation.

NOTE

If your 3270 connection is interrupted and you cannot log in again because the previous session is still active, you can replace the old session with a new one by entering the following command on the z/VM logon screen:

```
logon user here
```

Replace *user* with the name of the z/VM guest virtual machine. Depending on whether an external security manager, for example RACF, is used, the logon command might vary.

If you are not already running **CMS** (single-user operating system shipped with z/VM) in your guest, boot it now by entering the command:

```
cp ipl cms
```

Be sure not to use CMS disks such as your A disk (often device number 0191) as installation targets. To find out which disks are in use by CMS, use the following query:

```
query disk
```

You can use the following CP (z/VM Control Program, which is the z/VM hypervisor) query commands to find out about the device configuration of your z/VM guest virtual machine:

- Query the available main memory, which is called *storage* in IBM Z terminology. Your guest should have at least 1 GB of main memory.

  ```
  cp query virtual storage
  ```

- Query available network devices by type:

  osa

  OSA - CHPID type OSD, real or virtual (VSWITCH or GuestLAN), both in QDIO mode

  hsi

  HiperSockets - CHPID type IQD, real or virtual (GuestLAN type Hipers)

  lcs

  LCS - CHPID type OSE
  For example, to query all of the network device types mentioned above, run:

  ```
  cp query virtual osa
  ```

- Query available DASDs. Only those that are flagged **RW** for read-write mode can be used as installation targets:

  ```
  cp query virtual dasd
  ```

- Query available FCP channels:

  ```
  cp query virtual fcp
  ```

11.4. USING PARAMETER AND CONFIGURATION FILES ON IBM Z

The IBM Z architecture can use a customized parameter file to pass boot parameters to the kernel and the installation program.

You need to change the parameter file if you want to:

- Install unattended with Kickstart.
- Choose non-default installation settings that are not accessible through the installation program's interactive user interface, such as rescue mode.

The parameter file can be used to set up networking non-interactively before the installation program (**Anaconda**) starts.

The kernel parameter file is limited to 895 characters plus an end-of-line character. The parameter file can be variable or fixed record format. Fixed record format increases the file size by padding each line up to the record length. Should you encounter problems with the installation program not recognizing all specified parameters in LPAR environments, you can try to put all parameters in one single line or start and end each line with a space character.

The parameter file contains kernel parameters, such as **ro**, and parameters for the installation process, such as **vncpassword=test** or **vnc**.

11.5. REQUIRED CONFIGURATION FILE PARAMETERS ON IBM Z

Several parameters are required and must be included in the parameter file. These parameters are also provided in the file **generic.prm** in directory **images/** of the installation DVD.

- **ro**
  Mounts the root file system, which is a RAM disk, read-only.
- **ramdisk_size=*size***
  Modifies the memory size reserved for the RAM disk to ensure that the Red Hat Enterprise Linux installation program fits within it. For example: **ramdisk_size=40000**.

The **generic.prm** file also contains the additional parameter **cio_ignore=all,!condev**. This setting speeds up boot and device detection on systems with many devices. The installation program transparently handles the activation of ignored devices.

IMPORTANT

To avoid installation problems arising from **cio_ignore** support not being implemented throughout the entire stack, adapt the **cio_ignore=** parameter value to your system or remove the parameter entirely from your parameter file used for booting (IPL) the installation program.

11.6. IBM Z/VM CONFIGURATION FILE

Under z/VM, you can use a configuration file on a CMS-formatted disk. The purpose of the CMS configuration file is to save space in the parameter file by moving the parameters that configure the initial network setup, the DASD, and the FCP specification out of the parameter file.

Each line of the CMS configuration file contains a single variable and its associated value, in the following shell-style syntax: ***variable=value***.

You must also add the **CMSDASD** and **CMSCONFFILE** parameters to the parameter file. These parameters point the installation program to the configuration file:

CMSDASD=*cmsdasd_address*

Where *cmsdasd_address* is the device number of a CMS-formatted disk that contains the configuration file. This is usually the CMS user's **A** disk.
For example: **CMSDASD=191**

CMSCONFFILE=*configuration_file*

Where *configuration_file* is the name of the configuration file. This value must be specified in lower case. It is specified in a Linux file name format: ***CMS_file_name.CMS_file_type***.
The CMS file **REDHAT CONF** is specified as **redhat.conf**. The CMS file name and the file type can each be from one to eight characters that follow the CMS conventions.

For example: **CMSCONFFILE=redhat.conf**

11.7. INSTALLATION NETWORK PARAMETERS ON IBM Z

These parameters can be used to automatically set up the preliminary network, and can be defined in the CMS configuration file. These parameters are the only parameters that can also be used in a CMS configuration file. All other parameters in other sections must be specified in the parameter file.

NETTYPE="*type*"

Where *type* must be one of the following: **qeth**, **lcs**, or **ctc**. The default is **qeth**.
Choose **lcs** for:

- OSA-2 Ethernet/Token Ring
- OSA-Express Fast Ethernet in non-QDIO mode
- OSA-Express High Speed Token Ring in non-QDIO mode
- Gigabit Ethernet in non-QDIO mode
  Choose **qeth** for:
- OSA-Express Fast Ethernet
- Gigabit Ethernet (including 1000Base-T)
- High Speed Token Ring
- HiperSockets
- ATM (running Ethernet LAN emulation)

SUBCHANNELS="*device_bus_IDs*"

Where *device_bus_IDs* is a comma-separated list of two or three device bus IDs. The IDs must be specified in lowercase.
Provides required device bus IDs for the various network interfaces:

```
qeth: SUBCHANNELS="read_device_bus_id,write_device_bus_id,data_device_bus_id"
lcs or ctc: SUBCHANNELS="read_device_bus_id,write_device_bus_id"
```

For example (a sample qeth SUBCHANNEL statement):

```
SUBCHANNELS="0.0.f5f0,0.0.f5f1,0.0.f5f2"
```

PORTNAME="*osa_portname*" PORTNAME="*lcs_portnumber*"

This variable supports OSA devices operating in qdio mode or in non-qdio mode.
When using qdio mode (**NETTYPE="qeth"**), *osa_portname* is the portname specified on the OSA device when operating in qeth mode.

When using non-qdio mode (**NETTYPE="lcs"**), *lcs_portnumber* is used to pass the relative port number as a decimal integer in the range of 0 through 15.

PORTNO="*portnumber*"

You can add either **PORTNO="0"** (to use port 0) or **PORTNO="1"** (to use port 1 of OSA features with two ports per CHPID) to the CMS configuration file to avoid being prompted for the mode.

LAYER2="*value*"

Where *value* can be **0** or **1**.
Use **LAYER2="0"** to operate an OSA or HiperSockets device in layer 3 mode (**NETTYPE="qeth"**). Use **LAYER2="1"** for layer 2 mode. For virtual network devices under z/VM this setting must match the definition of the GuestLAN or VSWITCH to which the device is coupled.

To use network services that operate on layer 2 (the Data Link Layer or its MAC sublayer) such as DHCP, layer 2 mode is a good choice.

The qeth device driver default for OSA devices is now layer 2 mode. To continue using the previous default of layer 3 mode, set **LAYER2="0"** explicitly.

VSWITCH="*value*"

Where *value* can be **0** or **1**.
Specify **VSWITCH="1"** when connecting to a z/VM VSWITCH or GuestLAN, or **VSWITCH="0"** (or nothing at all) when using directly attached real OSA or directly attached real HiperSockets.

MACADDR="*MAC_address*"

If you specify **LAYER2="1"** and **VSWITCH="0"**, you can optionally use this parameter to specify a MAC address. Linux requires six colon-separated octets as pairs lower case hex digits - for example, **MACADDR=62:a3:18:e7:bc:5f**. Note that this is different from the notation used by z/VM.
If you specify **LAYER2="1"** and **VSWITCH="1"**, you must not specify the **MACADDR**, because z/VM assigns a unique MAC address to virtual network devices in layer 2 mode.

CTCPROT="*value*"

Where *value* can be **0**, **1**, or **3**.
Specifies the CTC protocol for **NETTYPE="ctc"**. The default is **0**.

HOSTNAME="*string*"

Where *string* is the host name of the newly-installed Linux instance.

IPADDR="*IP*"

Where *IP* is the IP address of the new Linux instance.

NETMASK="*netmask*"

Where *netmask* is the netmask.

The netmask supports the syntax of a prefix integer (from 1 to 32) as specified in IPv4 *classless interdomain routing* (CIDR). For example, you can specify **24** instead of **255.255.255.0**, or **20** instead of **255.255.240.0**.

GATEWAY="*gw*"

Where *gw* is the gateway IP address for this network device.

MTU="*mtu*"

Where *mtu* is the *Maximum Transmission Unit* (MTU) for this network device.

DNS="*server1:server2:additional_server_terms:serverN*"

Where "*server1:server2:additional_server_terms:serverN*" is a list of DNS servers, separated by colons. For example:

```
DNS="10.1.2.3:10.3.2.1"
```

SEARCHDNS="*domain1:domain2:additional_dns_terms:domainN*"

Where "*domain1:domain2:additional_dns_terms:domainN*" is a list of the search domains, separated by colons. For example:

```
SEARCHDNS="subdomain.domain:domain"
```

You only need to specify **SEARCHDNS=** if you specify the **DNS=** parameter.

DASD=

Defines the DASD or range of DASDs to configure for the installation.
The installation program supports a comma-separated list of device bus IDs, or ranges of device bus IDs with the optional attributes **ro**, **diag**, **erplog**, and **failfast**. Optionally, you can abbreviate device bus IDs to device numbers with leading zeros stripped. Any optional attributes should be separated by colons and enclosed in parentheses. Optional attributes follow a device bus ID or a range of device bus IDs.

The only supported global option is **autodetect**. This does not support the specification of non-existent DASDs to reserve kernel device names for later addition of DASDs. Use persistent DASD device names (for example **/dev/disk/by-path/…**) to enable transparent addition of disks later. Other global options such as **probeonly**, **nopav**, or **nofcx** are not supported by the installation program.

Only specify those DASDs that need to be installed on your system. All unformatted DASDs specified here must be formatted after a confirmation later on in the installation program.

Add any data DASDs that are not needed for the root file system or the **/boot** partition after installation.

For example:

```
DASD="eb1c,0.0.a000-0.0.a003,eb10-eb14(diag),0.0.ab1c(ro:diag)"
```

For FCP-only environments, remove the **DASD=** option from the CMS configuration file to indicate no DASD is present.

```
FCP_n="device_bus_ID WWPN FCP_LUN"
```

Where:

- *n* is typically an integer value (for example **FCP_1** or **FCP_2**) but could be any string with alphabetic or numeric characters or underscores.
- *device_bus_ID* specifies the device bus ID of the FCP device representing the *host bus adapter* (HBA) (for example **0.0.fc00** for device fc00).
- *WWPN* is the world wide port name used for routing (often in conjunction with multipathing) and is as a 16-digit hex value (for example **0x50050763050b073d**).
- *FCP_LUN* refers to the storage logical unit identifier and is specified as a 16-digit hexadecimal value padded with zeroes to the right (for example **0x4020400100000000**). These variables can be used on systems with FCP devices to activate FCP LUNs such as SCSI disks. Additional FCP LUNs can be activated during the installation interactively or by means of a Kickstart file. An example value looks similar to the following:

  ```
  FCP_1="0.0.fc00 0x50050763050b073d 0x4020400100000000"
  ```

  IMPORTANT

  Each of the values used in the FCP parameters (for example **FCP_1** or **FCP_2**) are site-specific and are normally supplied by the FCP storage administrator.

The installation program prompts you for any required parameters not specified in the parameter or configuration file except for FCP_n.

11.8. PARAMETERS FOR KICKSTART INSTALLATIONS ON IBM Z

The following parameters can be defined in a parameter file but do not work in a CMS configuration file.

inst.ks=*URL*

References a Kickstart file, which usually resides on the network for Linux installations on IBM Z. Replace *URL* with the full path including the file name of the Kickstart file. This parameter activates automatic installation with Kickstart.

inst.cmdline

When this option is specified, output on line-mode terminals (such as 3270 under z/VM or operating system messages for LPAR) becomes readable, as the installation program disables escape terminal sequences that are only applicable to UNIX-like consoles. This requires installation with a Kickstart file that answers all questions, because the installation program does not support interactive user input in cmdline mode.

Ensure that your Kickstart file contains all required parameters before you use the **inst.cmdline** option. If a required command is missing, the installation will fail.

11.9. MISCELLANEOUS PARAMETERS ON IBM Z

The following parameters can be defined in a parameter file but do not work in a CMS configuration file.

rd.live.check

Turns on testing of an ISO-based installation source; for example, when booted from an FCP-attached DVD or using **inst.repo=** with an ISO on local hard disk or mounted with NFS.

nompath

Disables support for multipath devices.

proxy=[*protocol*://][*username*[:*password*]@]*host*[:*port*]

Specify a proxy to use with installation over HTTP or HTTPS.

inst.rescue

Boot into a rescue system running from a RAM disk that can be used to fix and restore an installed system.

inst.stage2=*URL*

Specifies a path to a tree containing **install.img**, not to the **install.img** directly. Otherwise, follows the same syntax as **inst.repo=**. If **inst.stage2** is specified, it typically takes precedence over other methods of finding **install.img**. However, if **Anaconda** finds **install.img** on local media, the **inst.stage2** URL will be ignored.
If **inst.stage2** is not specified and **install.img** cannot be found locally, **Anaconda** looks to the location given by **inst.repo=** or **method=**.

If only **inst.stage2=** is given without **inst.repo=** or **method=**, **Anaconda** uses whatever repos the installed system would have enabled by default for installation.

Use the option multiple times to specify multiple HTTP or HTTPS sources. The HTTP or HTTPS paths are then tried sequentially until one succeeds:

```
inst.stage2=http://hostname/path_to_install_tree/
inst.stage2=http://hostname/path_to_install_tree/
inst.stage2=http://hostname/path_to_install_tree/
```

inst.syslog=*IP/hostname*[:*port*]

Sends log messages to a remote syslog server.

The boot parameters described here are the most useful for installations and trouble shooting on IBM Z, but only a subset of those that influence the installation program.

11.10. SAMPLE PARAMETER FILE AND CMS CONFIGURATION FILE ON IBM Z

To change the parameter file, begin by extending the shipped **generic.prm** file.

Example of **generic.prm** file:

```
ro ramdisk_size=40000 cio_ignore=all,!condev
CMSDASD="191" CMSCONFFILE="redhat.conf"
vnc
inst.repo=http://example.com/path/to/repository
```

Example of **redhat.conf** file configuring a QETH network device (pointed to by **CMSCONFFILE** in **generic.prm**):

```
NETTYPE="qeth"
SUBCHANNELS="0.0.0600,0.0.0601,0.0.0602"
PORTNAME="FOOBAR"
```

```
PORTNO="0"
LAYER2="1"
MACADDR="02:00:be:3a:01:f3"
HOSTNAME="foobar.systemz.example.com"
IPADDR="192.168.17.115"
NETMASK="255.255.255.0"
GATEWAY="192.168.17.254"
DNS="192.168.17.1"
SEARCHDNS="systemz.example.com:example.com"
DASD="200-203"
```

CHAPTER 12. CONFIGURING A LINUX INSTANCE ON IBM Z

This section describes most of the common tasks for installing Red Hat Enterprise Linux on IBM Z.

12.1. ADDING DASDS

Direct Access Storage Devices (DASDs) are a type of storage commonly used with IBM Z. Additional information about working with these storage devices can be found at the IBM Knowledge Center at http://www-01.ibm.com/support/knowledgecenter/linuxonibm/com.ibm.linux.z.lgdd/lgdd_t_dasd_wrk.html.

The following is an example of how to set a DASD online, format it, and make the change persistent.

Make sure the device is attached or linked to the Linux system if running under z/VM.

```
CP ATTACH EB1C TO *
```

To link a mini disk to which you have access, issue, for example:

```
CP LINK RHEL7X 4B2E 4B2E MR
DASD 4B2E LINKED R/W
```

12.2. DYNAMICALLY SETTING DASDS ONLINE

To set a DASD online, follow these steps:

1. Use the **cio_ignore** utility to remove the DASD from the list of ignored devices and make it visible to Linux:

   ```
   # cio_ignore -r device_number
   ```

   Replace *device_number* with the device number of the DASD. For example:

   ```
   # cio_ignore -r 4b2e
   ```

2. Set the device online. Use a command of the following form:

   ```
   # chccwdev -e device_number
   ```

   Replace *device_number* with the device number of the DASD. For example:

   ```
   # chccwdev -e 4b2e
   ```

   As an alternative, you can set the device online using sysfs attributes:

   a. Use the **cd** command to change to the /sys/ directory that represents that volume:

   ```
   # cd /sys/bus/ccw/drivers/dasd-eckd/0.0.4b2e/
   # ls -l
   total 0
   -r--r--r--  1 root root 4096 Aug 25 17:04 availability
   -rw-r--r--  1 root root 4096 Aug 25 17:04 cmb_enable
   ```

```
-r--r--r--  1 root root 4096 Aug 25 17:04 cutype
-rw-r--r--  1 root root 4096 Aug 25 17:04 detach_state
-r--r--r--  1 root root 4096 Aug 25 17:04 devtype
-r--r--r--  1 root root 4096 Aug 25 17:04 discipline
-rw-r--r--  1 root root 4096 Aug 25 17:04 online
-rw-r--r--  1 root root 4096 Aug 25 17:04 readonly
-rw-r--r--  1 root root 4096 Aug 25 17:04 use_diag
```

b. Check to see if the device is already online:

```
# cat online
0
```

c. If it is not online, enter the following command to bring it online:

```
# echo 1 > online
# cat online
1
```

3. Verify which block devnode it is being accessed as:

```
# ls -l
total 0
-r--r--r--  1 root root 4096 Aug 25 17:04 availability
lrwxrwxrwx  1 root root    0 Aug 25 17:07 block -> ../../../../block/dasdb
-rw-r--r--  1 root root 4096 Aug 25 17:04 cmb_enable
-r--r--r--  1 root root 4096 Aug 25 17:04 cutype
-rw-r--r--  1 root root 4096 Aug 25 17:04 detach_state
-r--r--r--  1 root root 4096 Aug 25 17:04 devtype
-r--r--r--  1 root root 4096 Aug 25 17:04 discipline
-rw-r--r--  1 root root    0 Aug 25 17:04 online
-rw-r--r--  1 root root 4096 Aug 25 17:04 readonly
-rw-r--r--  1 root root 4096 Aug 25 17:04 use_diag
```

As shown in this example, device 4B2E is being accessed as /dev/dasdb.

These instructions set a DASD online for the current session, but this is not persistent across reboots. For instructions on how to set a DASD online persistently, see Section 12.4, “Persistently setting DASDs online”. When you work with DASDs, use the persistent device symbolic links under **/dev/disk/by-path/**.

12.3. PREPARING A NEW DASD WITH LOW-LEVEL FORMATTING

Once the disk is online, change back to the **/root** directory and low-level format the device. This is only required once for a DASD during its entire lifetime:

```
# cd /root
# dasdfmt -b 4096 -d cdl -p /dev/disk/by-path/ccw-0.0.4b2e
Drive Geometry: 10017 Cylinders * 15 Heads =  150255 Tracks

I am going to format the device /dev/disk/by-path/ccw-0.0.4b2e in the following way:
Device number of device : 0x4b2e
Labelling device        : yes
Disk label              : VOL1
Disk identifier         : 0X4B2E
```

```
Extent start (trk no)   : 0
Extent end (trk no)     : 150254
Compatible Disk Layout  : yes
Blocksize               : 4096

--->> ATTENTION! <<---
All data of that device will be lost.
Type "yes" to continue, no will leave the disk untouched: yes
cyl    97 of  3338 |#----------------------------------------------|   2%
```

When the progress bar reaches the end and the format is complete, **dasdfmt** prints the following output:

```
Rereading the partition table...
Exiting...
```

Now, use **fdasd** to partition the DASD. You can create up to three partitions on a DASD. In our example here, we create one partition spanning the whole disk:

```
# fdasd -a /dev/disk/by-path/ccw-0.0.4b2e
reading volume label ..: VOL1
reading vtoc ..........: ok

auto-creating one partition for the whole disk...
writing volume label...
writing VTOC...
rereading partition table...
```

After a (low-level formatted) DASD is online, it can be used like any other disk under Linux. For instance, you can create file systems, LVM physical volumes, or swap space on its partitions, for example **/dev/disk/by-path/ccw-0.0.4b2e-part1**. Never use the full DASD device (**dev/dasdb**) for anything but the commands **dasdfmt** and **fdasd**. If you want to use the entire DASD, create one partition spanning the entire drive as in the **fdasd** example above.

To add additional disks later without breaking existing disk entries in, for example, **/etc/fstab**, use the persistent device symbolic links under **/dev/disk/by-path/**.

12.4. PERSISTENTLY SETTING DASDS ONLINE

The above instructions described how to activate DASDs dynamically in a running system. However, such changes are not persistent and do not survive a reboot. Making changes to the DASD configuration persistent in your Linux system depends on whether the DASDs belong to the root file system. Those DASDs required for the root file system need to be activated very early during the boot process by the **initramfs** to be able to mount the root file system.

The **cio_ignore** commands are handled transparently for persistent device configurations and you do not need to free devices from the ignore list manually.

12.5. DASDS THAT ARE PART OF THE ROOT FILE SYSTEM

The file you have to modify to add DASDs that are part of the root file system has changed in Red Hat Enterprise Linux 8. Instead of editing the **/etc/zipl.conf** file, the new file to be edited, and its location, may be found by running the following commands:

```
# machine_id=$(cat /etc/machine-id)
# kernel_version=$(uname -r)
# ls /boot/loader/entries/$machine_id-$kernel_version.conf
```

There is one boot option to activate DASDs early in the boot process: **rd.dasd=**. This option takes a comma-separated list as input. The list contains a device bus ID and optional additional parameters consisting of key-value pairs that correspond to DASD **sysfs** attributes.

Below is an example of the **/boot/loader/entries/4ab74e52867b4f998e73e06cf23fd761-4.18.0-80.el8.s390x.conf** file for a system that uses physical volumes on partitions of two DASDs for an LVM volume group **vg_devel1** that contains a logical volume **lv_root** for the root file system.

```
title Red Hat Enterprise Linux (4.18.0-80.el8.s390x) 8.0 (Ootpa)
version 4.18.0-80.el8.s390x
linux /boot/vmlinuz-4.18.0-80.el8.s390x
initrd /boot/initramfs-4.18.0-80.el8.s390x.img
options root=/dev/mapper/vg_devel1-lv_root crashkernel=auto rd.dasd=0.0.0200 rd.dasd=0.0.0207
rd.lvm.lv=vg_devel1/lv_root rd.lvm.lv=vg_devel1/lv_swap cio_ignore=all,!condev
rd.znet=qeth,0.0.0a00,0.0.0a01,0.0.0a02,layer2=1,portno=0
id rhel-20181027190514-4.18.0-80.el8.s390x
grub_users $grub_users
grub_arg --unrestricted
grub_class kernel
```

To add another physical volume on a partition of a third DASD with device bus ID **0.0.202b**. To do this, add **rd.dasd=0.0.202b** to the parameters line of your boot kernel in **/boot/loader/entries/4ab74e52867b4f998e73e06cf23fd761-4.18.0-32.el8.s390x.conf**:

```
title Red Hat Enterprise Linux (4.18.0-80.el8.s390x) 8.0 (Ootpa)
version 4.18.0-80.el8.s390x
linux /boot/vmlinuz-4.18.0-80.el8.s390x
initrd /boot/initramfs-4.18.0-80.el8.s390x.img
options root=/dev/mapper/vg_devel1-lv_root crashkernel=auto rd.dasd=0.0.0200 rd.dasd=0.0.0207
rd.dasd=0.0.202b rd.lvm.lv=vg_devel1/lv_root rd.lvm.lv=vg_devel1/lv_swap cio_ignore=all,!condev
rd.znet=qeth,0.0.0a00,0.0.0a01,0.0.0a02,layer2=1,portno=0
id rhel-20181027190514-4.18.0-80.el8.s390x
grub_users $grub_users
grub_arg --unrestricted
grub_class kernel
```

WARNING

Make sure the length of the kernel command line in the configuration file does not exceed 896 bytes. Otherwise, the boot loader cannot be saved, and the installation fails.

Run **zipl** to apply the changes of the configuration file for the next IPL:

```
# zipl -V
```

```
Using config file '/etc/zipl.conf'
Using BLS config file '/boot/loader/entries/4ab74e52867b4f998e73e06cf23fd761-4.18.0-
80.el8.s390x.conf'
Target device information
  Device..........................: 5e:00
  Partition.......................: 5e:01
  Device name.....................: dasda
  Device driver name..............: dasd
  DASD device number..............: 0201
  Type............................: disk partition
  Disk layout.....................: ECKD/compatible disk layout
  Geometry - heads................: 15
  Geometry - sectors..............: 12
  Geometry - cylinders............: 13356
  Geometry - start................: 24
  File system block size..........: 4096
  Physical block size.............: 4096
  Device size in physical blocks..: 262152
Building bootmap in '/boot'
Building menu 'zipl-automatic-menu'
Adding #1: IPL section '4.18.0-80.el8.s390x' (default)
  initial ramdisk...: /boot/initramfs-4.18.0-80.el8.s390x.img
  kernel image......: /boot/vmlinuz-4.18.0-80.el8.s390x
  kernel parmline...: 'root=/dev/mapper/vg_devel1-lv_root crashkernel=auto rd.dasd=0.0.0200
rd.dasd=0.0.0207 rd.dasd=0.0.202b rd.lvm.lv=vg_devel1/lv_root rd.lvm.lv=vg_devel1/lv_swap
cio_ignore=all,!condev rd.znet=qeth,0.0.0a00,0.0.0a01,0.0.0a02,layer2=1,portno=0'
  component address:
    kernel image....: 0x00010000-0x0049afff
    parmline........: 0x0049b000-0x0049bfff
    initial ramdisk.: 0x004a0000-0x01a26fff
    internal loader.: 0x0000a000-0x0000cfff
Preparing boot menu
  Interactive prompt......: enabled
  Menu timeout............: 5 seconds
  Default configuration...: '4.18.0-80.el8.s390x'
Preparing boot device: dasda (0201).
Syncing disks...
Done.
```

12.6. FCP LUNS THAT ARE PART OF THE ROOT FILE SYSTEM

The only file you have to modify for adding FCP LUNs that are part of the root file system has changed in Red Hat Enterprise Linux 8. Instead of editing the **/etc/zipl.conf** file, the new file to be edited, and its location, may be found by running the following commands:

```
# machine_id=$(cat /etc/machine-id)
# kernel_version=$(uname -r)
# ls /boot/loader/entries/$machine_id-$kernel_version.conf
```

Red Hat Enterprise Linux provides a parameter to activate FCP LUNs early in the boot process: **rd.zfcp=**. The value is a comma-separated list containing the device bus ID, the WWPN as 16 digit hexadecimal number prefixed with **0x**, and the FCP LUN prefixed with **0x** and padded with zeroes to the right to have 16 hexadecimal digits.

Below is an example of the **/boot/loader/entries/4ab74e52867b4f998e73e06cf23fd761-4.18.0-**

80.el8.s390x.conf file for a system that uses physical volumes on partitions of two FCP LUNs for an LVM volume group **vg_devel1** that contains a logical volume **lv_root** for the root file system. For simplicity, the example shows a configuration without multipathing.

```
title Red Hat Enterprise Linux (4.18.0-32.el8.s390x) 8.0 (Ootpa)
version 4.18.0-32.el8.s390x
linux /boot/vmlinuz-4.18.0-32.el8.s390x
initrd /boot/initramfs-4.18.0-32.el8.s390x.img
options root=/dev/mapper/vg_devel1-lv_root crashkernel=auto
rd.zfcp=0.0.fc00,0x5105074308c212e9,0x401040a000000000
rd.zfcp=0.0.fc00,0x5105074308c212e9,0x401040a100000000 rd.lvm.lv=vg_devel1/lv_root
rd.lvm.lv=vg_devel1/lv_swap cio_ignore=all,!condev
rd.znet=qeth,0.0.0a00,0.0.0a01,0.0.0a02,layer2=1,portno=0
id rhel-20181027190514-4.18.0-32.el8.s390x
grub_users $grub_users
grub_arg --unrestricted
grub_class kernel
```

To add another physical volume on a partition of a third FCP LUN with device bus ID 0.0.fc00, WWPN 0x5105074308c212e9 and FCP LUN 0x401040a300000000, add **rd.zfcp=0.0.fc00,0x5105074308c212e9,0x401040a300000000** to the parameters line of your boot kernel in **/boot/loader/entries/4ab74e52867b4f998e73e06cf23fd761-4.18.0-32.el8.s390x.conf**. For example:

```
title Red Hat Enterprise Linux (4.18.0-32.el8.s390x) 8.0 (Ootpa)
version 4.18.0-32.el8.s390x
linux /boot/vmlinuz-4.18.0-32.el8.s390x
initrd /boot/initramfs-4.18.0-32.el8.s390x.img
options root=/dev/mapper/vg_devel1-lv_root crashkernel=auto
rd.zfcp=0.0.fc00,0x5105074308c212e9,0x401040a000000000
rd.zfcp=0.0.fc00,0x5105074308c212e9,0x401040a100000000
rd.zfcp=0.0.fc00,0x5105074308c212e9,0x401040a300000000 rd.lvm.lv=vg_devel1/lv_root
rd.lvm.lv=vg_devel1/lv_swap cio_ignore=all,!condev
rd.znet=qeth,0.0.0a00,0.0.0a01,0.0.0a02,layer2=1,portno=0
id rhel-20181027190514-4.18.0-32.el8.s390x
grub_users $grub_users
grub_arg --unrestricted
grub_class kernel
```

WARNING

Make sure the length of the kernel command line in the configuration file does not exceed 896 bytes. Otherwise, the boot loader cannot be saved, and the installation fails.

Run **zipl** to apply the changes of the configuration file for the next IPL:

```
# zipl -V
Using config file '/etc/zipl.conf'
Using BLS config file '/boot/loader/entries/4ab74e52867b4f998e73e06cf23fd761-4.18.0-
32.el8.s390x.conf'
Target device information
Device..........................: 08:00
Partition.......................: 08:01
Device name.....................: sda
Device driver name..............: sd
Type............................: disk partition
Disk layout.....................: SCSI disk layout
Geometry - start................: 2048
File system block size..........: 4096
Physical block size.............: 512
Device size in physical blocks..: 10074112
Building bootmap in '/boot/'
Building menu 'rh-automatic-menu'
Adding #1: IPL section '4.18.0-32.el8.s390x' (default)
kernel image......: /boot/vmlinuz-4.18.0-32.el8.s390x
kernel parmline...: 'root=/dev/mapper/vg_devel1-lv_root crashkernel=auto
rd.zfcp=0.0.fc00,0x5105074308c212e9,0x401040a000000000
rd.zfcp=0.0.fc00,0x5105074308c212e9,0x401040a100000000
rd.zfcp=0.0.fc00,0x5105074308c212e9,0x401040a300000000 rd.lvm.lv=vg_devel1/lv_root
rd.lvm.lv=vg_devel1/lv_swap cio_ignore=all,!condev
rd.znet=qeth,0.0.0a00,0.0.0a01,0.0.0a02,layer2=1,portno=0'
initial ramdisk...: /boot/initramfs-4.18.0-32.el8.s390x.img
component address:
kernel image....: 0x00010000-0x007a21ff
parmline........: 0x00001000-0x000011ff
initial ramdisk.: 0x02000000-0x028f63ff
internal loader.: 0x0000a000-0x0000a3ff
Preparing boot device: sda.
Detected SCSI PCBIOS disk layout.
Writing SCSI master boot record.
Syncing disks...
Done.
```

12.7. ADDING A QETH DEVICE

The **qeth** network device driver supports IBM Z OSA-Express features in QDIO mode, HiperSockets, z/VM guest LAN, and z/VM VSWITCH.

The qeth device driver assigns the same interface name for Ethernet and Hipersockets devices: **encbus_ID**. The bus ID is composed of the channel subsystem ID, subchannel set ID, and device number, and does not contain leading zeros and dots. For example enca00 for a device with the bus ID **0.0.0a00**.

12.8. DYNAMICALLY ADDING A QETH DEVICE

To add a **qeth** device dynamically, follow these steps:

1. Determine whether the **qeth** device driver modules are loaded. The following example shows loaded **qeth** modules:

   ```
   # lsmod | grep qeth
   qeth_l3              69632  0
   qeth_l2              49152  1
   ```

```
qeth                 131072  2 qeth_l3,qeth_l2
qdio                  65536  3 qeth,qeth_l3,qeth_l2
ccwgroup                20480  1 qeth
```

If the output of the **lsmod** command shows that the **qeth** modules are not loaded, run the **modprobe** command to load them:

```
# modprobe qeth
```

2. Use the **cio_ignore** utility to remove the network channels from the list of ignored devices and make them visible to Linux:

   ```
   # cio_ignore -r read_device_bus_id,write_device_bus_id,data_device_bus_id
   ```

   Replace *read_device_bus_id*,*write_device_bus_id*,*data_device_bus_id* with the three device bus IDs representing a network device. For example, if the *read_device_bus_id* is **0.0.f500**, the *write_device_bus_id* is **0.0.f501**, and the *data_device_bus_id* is **0.0.f502**:

   ```
   # cio_ignore -r 0.0.f500,0.0.f501,0.0.f502
   ```

3. Use the **znetconf** utility to sense and list candidate configurations for network devices:

   ```
   # znetconf -u
   Scanning for network devices...
   Device IDs                 Type    Card Type      CHPID Drv.
   ------------------------------------------------------------
   0.0.f500,0.0.f501,0.0.f502 1731/01 OSA (QDIO)        00 qeth
   0.0.f503,0.0.f504,0.0.f505 1731/01 OSA (QDIO)        01 qeth
   0.0.0400,0.0.0401,0.0.0402 1731/05 HiperSockets      02 qeth
   ```

4. Select the configuration you want to work with and use **znetconf** to apply the configuration and to bring the configured group device online as network device.

   ```
   # znetconf -a f500
   Scanning for network devices...
   Successfully configured device 0.0.f500 (encf500)
   ```

5. Optionally, you can also pass arguments that are configured on the group device before it is set online:

   ```
   # znetconf -a f500 -o portname=myname
   Scanning for network devices...
   Successfully configured device 0.0.f500 (encf500)
   ```

   Now you can continue to configure the **encf500** network interface.

Alternatively, you can use **sysfs** attributes to set the device online as follows:

1. Create a **qeth** group device:

   ```
   # echo read_device_bus_id,write_device_bus_id,data_device_bus_id >
   /sys/bus/ccwgroup/drivers/qeth/group
   ```

For example:

```
# echo 0.0.f500,0.0.f501,0.0.f502 > /sys/bus/ccwgroup/drivers/qeth/group
```

2. Next, verify that the **qeth** group device was created properly by looking for the read channel:

```
# ls /sys/bus/ccwgroup/drivers/qeth/0.0.f500
```

You can optionally set additional parameters and features, depending on the way you are setting up your system and the features you require, such as:

- **portno**
- **layer2**
- **portname**

3. Bring the device online by writing **1** to the online **sysfs** attribute:

```
# echo 1 > /sys/bus/ccwgroup/drivers/qeth/0.0.f500/online
```

4. Then verify the state of the device:

```
# cat /sys/bus/ccwgroup/drivers/qeth/0.0.f500/online
          1
```

A return value of **1** indicates that the device is online, while a return value **0** indicates that the device is offline.

5. Find the interface name that was assigned to the device:

```
# cat /sys/bus/ccwgroup/drivers/qeth/0.0.f500/if_name
encf500
```

Now you can continue to configure the **encf500** network interface.

The following command from the **s390utils** package shows the most important settings of your **qeth** device:

```
# lsqeth encf500
Device name                     : encf500
-------------------------------------------------
card_type               : OSD_1000
cdev0                   : 0.0.f500
cdev1                   : 0.0.f501
cdev2                   : 0.0.f502
chpid                   : 76
online                  : 1
portname                : OSAPORT
portno                  : 0
state                   : UP (LAN ONLINE)
priority_queueing       : always queue 0
```

```
buffer_count          : 16
layer2                : 1
isolation             : none
```

12.9. PERSISTENTLY ADDING A QETH DEVICE

To make your new **qeth** device persistent, you need to create the configuration file for your new interface. The network interface configuration files are placed in the **/etc/sysconfig/network-scripts/** directory.

The network configuration files use the naming convention **ifcfg-*device***, where *device* is the value found in the **if_name** file in the **qeth** group device that was created earlier, for example **enc9a0**. The **cio_ignore** commands are handled transparently for persistent device configurations and you do not need to free devices from the ignore list manually.

If a configuration file for another device of the same type already exists, the simplest way to add the config file is to copy it to the new name and then edit it:

```
# cd /etc/sysconfig/network-scripts
# cp ifcfg-enc9a0 ifcfg-enc600
```

To learn IDs of your network devices, use the **lsqeth** utility:

```
# lsqeth -p
devices                    CHPID interface        cardtype       port chksum prio-q'ing rtr4 rtr6 lay'2 cnt
-------------------------- ----- ---------------- -------------- ---- ------ ---------- ---- ---- ----- -----
0.0.09a0/0.0.09a1/0.0.09a2 x00   enc9a0    Virt.NIC QDIO  0    sw     always_q_2 n/a  n/a  1     64
0.0.0600/0.0.0601/0.0.0602 x00   enc600    Virt.NIC QDIO  0    sw     always_q_2 n/a  n/a  1     64
```

If you do not have a similar device defined, you must create a new file. Use this example of **/etc/sysconfig/network-scripts/ifcfg-0.0.09a0** as a template:

```
# IBM QETH
DEVICE=enc9a0
BOOTPROTO=static
IPADDR=10.12.20.136
NETMASK=255.255.255.0
ONBOOT=yes
NETTYPE=qeth
SUBCHANNELS=0.0.09a0,0.0.09a1,0.0.09a2
PORTNAME=OSAPORT
OPTIONS='layer2=1 portno=0'
MACADDR=02:00:00:23:65:1a
TYPE=Ethernet
```

Edit the new **ifcfg-0.0.0600** file as follows:

1. Modify the **DEVICE** statement to reflect the contents of the **if_name** file from your **ccw** group.

2. Modify the **IPADDR** statement to reflect the IP address of your new interface.

3. Modify the **NETMASK** statement as needed.

4. If the new interface is to be activated at boot time, then make sure **ONBOOT** is set to **yes**.

5. Make sure the **SUBCHANNELS** statement matches the hardware addresses for your qeth device.

6. Modify the **PORTNAME** statement or leave it out if it is not necessary in your environment.

7. You can add any valid **sysfs** attribute and its value to the **OPTIONS** parameter. The Red Hat Enterprise Linux installation program currently uses this to configure the layer mode (**layer2**) and the relative port number (**portno**) of **qeth** devices.
   The **qeth** device driver default for OSA devices is now layer 2 mode. To continue using old **ifcfg** definitions that rely on the previous default of layer 3 mode, add **layer2=0** to the **OPTIONS** parameter.

/etc/sysconfig/network-scripts/ifcfg-0.0.0600

```
# IBM QETH
DEVICE=enc600
BOOTPROTO=static
IPADDR=192.168.70.87
NETMASK=255.255.255.0
ONBOOT=yes
NETTYPE=qeth
SUBCHANNELS=0.0.0600,0.0.0601,0.0.0602
PORTNAME=OSAPORT
OPTIONS='layer2=1 portno=0'
MACADDR=02:00:00:b3:84:ef
TYPE=Ethernet
```

Changes to an **ifcfg** file only become effective after rebooting the system or after the dynamic addition of new network device channels by changing the system's I/O configuration (for example, attaching under z/VM). Alternatively, you can trigger the activation of a **ifcfg** file for network channels which were previously not active yet, by executing the following commands:

1. Use the **cio_ignore** utility to remove the network channels from the list of ignored devices and make them visible to Linux:

   ```
   # cio_ignore -r read_device_bus_id,write_device_bus_id,data_device_bus_id
   ```

   Replace *read_device_bus_id*,*write_device_bus_id*,*data_device_bus_id* with the three device bus IDs representing a network device. For example, if the *read_device_bus_id* is **0.0.0600**, the *write_device_bus_id* is **0.0.0601**, and the *data_device_bus_id* is **0.0.0602**:

   ```
   #  cio_ignore -r 0.0.0600,0.0.0601,0.0.0602
   ```

2. To trigger the uevent that activates the change, issue:

   ```
   # echo add > /sys/bus/ccw/devices/read-channel/uevent
   ```

   For example:

   ```
   # echo add > /sys/bus/ccw/devices/0.0.0600/uevent
   ```

3. Check the status of the network device:

   ```
   # lsqeth
   ```

4. Now start the new interface:

```
# ifup enc600
```

5. Check the status of the interface:

```
# ip addr show enc600
3: enc600:  <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UP group default qlen 1000
link/ether 3c:97:0e:51:38:17 brd ff:ff:ff:ff:ff:ff
inet 10.85.1.245/24 brd 10.34.3.255 scope global dynamic enc600
valid_lft 81487sec preferred_lft 81487sec
inet6 1574:12:5:1185:3e97:eff:fe51:3817/64 scope global noprefixroute dynamic
valid_lft 2591994sec preferred_lft 604794sec
inet6 fe45::a455:eff:d078:3847/64 scope link
valid_lft forever preferred_lft forever
```

6. Check the routing for the new interface:

```
# ip route
default via 10.85.1.245 dev enc600  proto static  metric 1024
12.34.4.95/24 dev enp0s25  proto kernel  scope link  src 12.34.4.201
12.38.4.128 via 12.38.19.254 dev enp0s25  proto dhcp  metric 1
192.168.122.0/24 dev virbr0  proto kernel  scope link  src 192.168.122.1
```

7. Verify your changes by using the **ping** utility to ping the gateway or another host on the subnet of the new device:

```
# ping -c 1 192.168.70.8
PING 192.168.70.8 (192.168.70.8) 56(84) bytes of data.
64 bytes from 192.168.70.8: icmp_seq=0 ttl=63 time=8.07 ms
```

8. If the default route information has changed, you must also update **/etc/sysconfig/network** accordingly.

12.10. CONFIGURING AN IBM Z NETWORK DEVICE FOR NETWORK ROOT FILE SYSTEM

To add a network device that is required to access the root file system, you only have to change the boot options. The boot options can be in a parameter file, however, the **/etc/zipl.conf** file no longer contains specifications of the boot records. The file that needs to be modified can be located using the following commands:

```
# machine_id=$(cat /etc/machine-id)
# kernel_version=$(uname -r)
# ls /boot/loader/entries/$machine_id-$kernel_version.conf
```

There is no need to recreate the initramfs.

Dracut, the **mkinitrd** successor that provides the functionality in the initramfs that in turn replaces **initrd**, provides a boot parameter to activate network devices on IBM Z early in the boot process: **rd.znet=**.

As input, this parameter takes a comma-separated list of the **NETTYPE** (qeth, lcs, ctc), two (lcs, ctc) or three (qeth) device bus IDs, and optional additional parameters consisting of key-value pairs corresponding to network device sysfs attributes. This parameter configures and activates the IBM Z network hardware. The configuration of IP addresses and other network specifics works the same as for other platforms. See the **dracut** documentation for more details.

The **cio_ignore** commands for the network channels are handled transparently on boot.

Example boot options for a root file system accessed over the network through NFS:

```
root=10.16.105.196:/nfs/nfs_root cio_ignore=all,!condev
rd.znet=qeth,0.0.0a00,0.0.0a01,0.0.0a02,layer2=1,portno=0,portname=OSAPORT
ip=10.16.105.197:10.16.105.196:10.16.111.254:255.255.248.0:nfs-server.subdomain.domain:enc9a0:n
one rd_NO_LUKS rd_NO_LVM rd_NO_MD rd_NO_DM LANG=en_US.UTF-8
SYSFONT=latarcyrheb-sun16 KEYTABLE=us
```