4.2.6 GRUB2 Bootloader Facts

GRUB2, the updated version of the Grand Unified Bootloader (GRUB) utility, is any version of GRUB 1.98 or later.

This lesson covers the following topics:

- Determining GRUB versions
- Configuring GRUB2
- GRUB Menu Display
- Boot Security

Determining GRUB Versions

The following commands can be used to view the version of GRUB used by the Linux distribution you have installed. The actual command used will vary between distributions:

- **grub-install -V** or **grub-install --version**
- **grub2-install -V** or **grub2-install --version**

Earlier versions of GRUB are sometimes called GRUB Legacy.

Configuring GRUB2

Be aware of the following details about GRUB2 configurations:

- The configuration files for GRUB2 are /boot/grub/grub.cfg or /boot/grub2/grub.cfg (depending upon the distribution). These files are similar to the GRUB Legacy's /boot/grub/menu.lst or /boot/grub/grub.conf files.
- Depending on the distribution, the **update-grub** or **grub2-mkconfig** commands generate the /boot/grub2/grub.cfg or /boot/grub/grub.cfg files. Specifically, these commands use the /etc/default/grub file and the scripts in the /etc/grub.d/ directory to generate the /boot/grub2/grub.cfg or /boot/grub/grub.cfg configuration files.
- Some distributions, such as Fedora and Centos, create an /etc/grub2/grub.cfg file. This file is a symbolic link to the /boot/grub2/grub.cfg file. Other distributions, such as Ubuntu and Debian, typically store the file as /boot/grub/grub.cfg.

- The /etc/grub.d/ directory holds script files that are read when the **update-grub** or the **grub2-mkconfig** commands are used.

grub2-mkconfig commands are used.

> The **grub.cfg** file should not be edited directly. Instead, the appropriate configuration file below should be edited when a change needs to be made. Then run either the **update-grub** or **grub2-mkconfig** command.

GRUB Menu Display

Common script files in the **/etc/grub.d/** directory that control the GRUB2 menu include the following:

Script File	Description
00_header	Sets initial appearance items, such as the graphics mode, default selection, timeout, etc. These settings are typically imported from the **/etc/default/grub** file.
10_linux	Identifies all Linux kernels installed on the root device and creates corresponding GRUB2 menu entries for each one. This allows you to select which Linux kernel you want to load when you initially boot the system.
30_os-prober	Executes **os-prober** to search for other operating systems (such as Microsoft Windows) and automatically creates GRUB2 menu items for them.
40_custom	Allows for custom menu entries, which are imported directly into **/boot/grub/grub.cfg** without any changes.

The **/etc/default/grub** file is the primary configuration file for changing menu display settings. The following table describes several common options in the configuration file:

Option	Description	Examples
GRUB_DEFAULT	Sets the default menu entry. Typical entries include: • Numeric (such as 0, 1, 2) • Complete menu entry quotation (such as "Ubuntu, Linux 20.4.2")	**GRUB_DEFAULT=0** sets the first mer default. **GRUB_DEFAULT="Ubuntu, Linux 2(** menu entry as the default.
GRUB_SAVEDEFAULT	Sets the last selected OS from the menu as the default OS on the next boot. **GRUB_DEFAULT=saved** is also required for this option to work	**GRUB_SAVEDEFAULT=true** sets the from the menu as the default OS on

	correctly.	
GRUB_HIDDEN_TIMEOUT	Determines how long a blank screen will be displayed. While the screen is blank, the user can press the Shift key to display the GRUB2 menu. Options include, **0**, *X*, and (null): • **0** disables this functionality. • *X* (an integer value) pauses and shows a blank screen for *X* seconds. • (null) uses the value specified in the GRUB_TIMEOUT entry.	**GRUB_HIDDEN_TIMEOUT=0** disable functionality. **GRUB_HIDDEN_TIMEOUT=3** display for 3 seconds and then boots to the there is no user interaction.
GRUB_HIDDEN_TIMEOUT_QUIET	Works in conjunction with the GRUB_HIDDEN_TIMEOUT parameter. It displays a counter (countdown) while the screen is blank. Options include **true** and **false**: • **true** does not display a counter. • **false** displays the counter for the duration specified in the GRUB_HIDDEN_TIMEOUT entry.	**GRUB_HIDDEN_TIMEOUT_QUIET=tr** display a counter.
GRUB_TIMEOUT	Determines how long to wait for user interaction before booting the default operating system. Options include *X* and -**1**: • *X* (an integer value of 1 or higher) sets the display duration in seconds. • **-1** causes the menu to display until the user makes a selection. The GRUB2 menu is	**GRUB_TIMEOUT=4** causes the menu four seconds and then boots into th operating system. **GRUB_TIMEOUT=-1** causes the men the user makes a selection.

	hidden by default unless another OS is detected by the system.	
GRUB_CMDLINE_LINUX	Passes options to the kernel. With the GRUB Legacy bootloader, this was done by adding options to the end of the kernel line. In GRUB2, this is done using the GRUB_CMDLINE_LINUX parameter.	
GRUB_GFXMODE	Sets the resolution of the graphical GRUB2 menu. Multiple resolutions may be specified if they are separated by commas.	**GRUB_GFXMODE=1440x900x24** set resolution to 1440 x 900 with a color
GRUB_BACKGROUND	Sets the background image during the GRUB2 menu display. The full path should be used. Must be in the PNG, TGA, or JPG/JPEG file formats.	**GRUB_BACKGROUND=/usr/share/i** displays back.png as the backgrounc
GRUB_DISABLE_OS_PROBER	Enables and disables the os-prober check of other partitions for operating systems, including Windows and Linux, during execution of the **update-grub** command. If the os-prober is enabled, operating systems are placed in the GRUB2 menu.	**GRUB_DISABLE_OS_PROBER=true** c prober. **GRUB_DISABLE_OS_PROBER=false** prober and adds found operating sy GRUB2 menu.

Boot Security

With all computer systems, maintaining security of your data should be of utmost concern. Most operating systems provide login security, but this just prevents people from logging into your operating system. To further protect your Linux computers, you should consider including UEFI/BIOS and bootloader passwords.

Security type	Description
Bootloader password	These passwords prevent a person from accessing the bootloader menu without knowing the password. Bootloader passwords can be implemented on one or all of the available boot

	menu options. For example, this can prevent a user from loading a Linux kernel.
UEFI/BIOS	These passwords allow you set low-level passwords to restrict people from booting the computer, booting from removable devices, and changing BIOS or UEFI settings without knowing the password.