An Oracle White Paper
January 2013

SUSE Linux to Oracle Linux: Guide for System Administrators

Disclaimer

The following is intended to outline Oracle's general product direction. It is intended for information purposes only and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Executive Overview

The purpose of this document is to give SUSE Linux administrators a quick way to understand and perform day-to-day system administration tasks on Oracle Linux.

Introduction

This document outlines similarities and differences in seven major areas of Linux system administration. It covers topics such as file system differences, boot-up sequence, setting up commonly used daemons such as mail and Web, and package management. Throughout the document, you will find actual configuration examples, complete with the steps required to achieve a particular objective. These examples are repeated for both Oracle Linux and SUSE Linux. After reading through this document, SUSE system administrators should be able to not only distinguish the subtle differences between the two operating systems but also be able to perform their daily duties with equal ease. It will also help SUSE Linux system administrators mitigate any risks related to migrating from SUSE Linux to Oracle Linux. For the purposes of this document, Oracle Linux 6.1 and SUSE Linux Enterprise Server 11 serve as the two base operating systems for comparison. All configuration examples and illustrations are based on either Oracle Linux 6.1 or SUSE Linux Enterprise Server.

Software Support Center

Every operating system vendor offers a support center for registering systems and downloading the latest updates, security patches, and errata. Oracle offers the Unbreakable Linux Network for Oracle Linux, and SUSE offers the Novell Customer Center (NCC) for support subscription, Linux software patches, updates, and fixes. The following section outlines how Unbreakable Linux Network and NCC can be configured for accessing software packages, updates, and errata.

Registering and Updating Oracle Linux 6

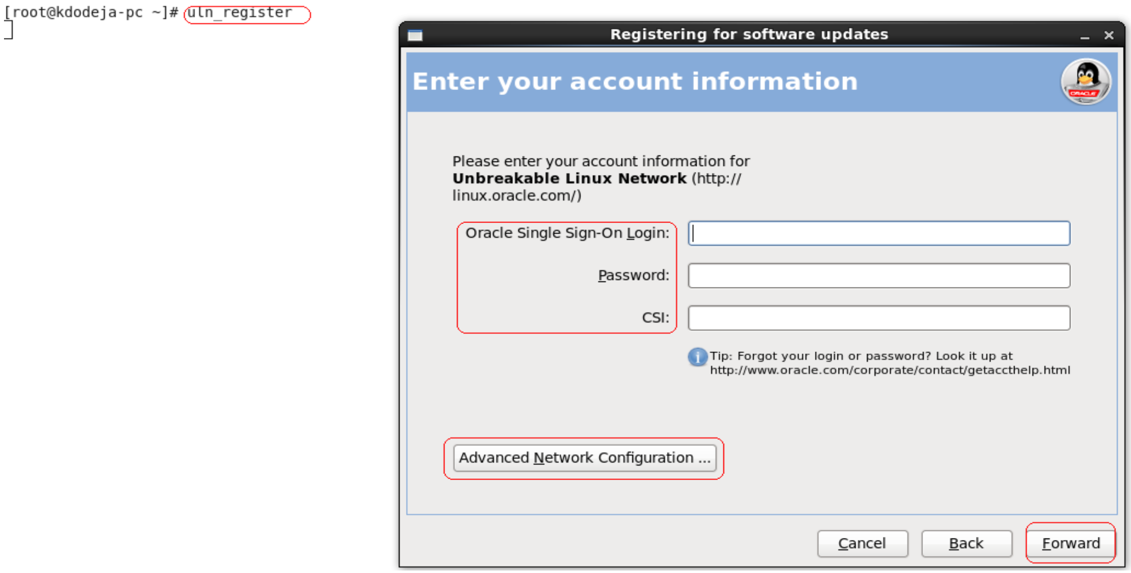
After installing the Oracle Linux 6 operating system, the first thing you should do is register your server(s) with the Oracle Unbreakable Linux Network. The Unbreakable Linux Network, a comprehensive resource for Oracle Linux support subscribers, offers access to Linux software patches, updates, and fixes. You can access the Unbreakable Linux Network at https://linux.oracle.com/.

To register your system (Oracle Linux 6) with the Unbreakable Linux Network, you will need to follow a series of steps illustrated below for your quick reference. The process is straightforward and simple. First ensure that your system has access to the internet. The Unbreakable Linux Network requires port 80 and 443 to be open for communication between the server being registered and the Unbreakable Linux Network. Work with your network administrator to ensure that the server being registered can access the Unbreakable Linux Network. Once you have made sure that the Unbreakable Linux Network can be accessed, follow the steps below.

Start a terminal session, and as the “root” user, issue the following command:

```
.# uln_register
```

You should then see the welcome screen shown in Figure 1.



```
[root@kdodeja-pc ~]# uln_register
```

Registering for software updates

Enter your account information

Please enter your account information for **Unbreakable Linux Network** (http://linux.oracle.com/)

Oracle Single Sign-On Login:

Password:

CSI:

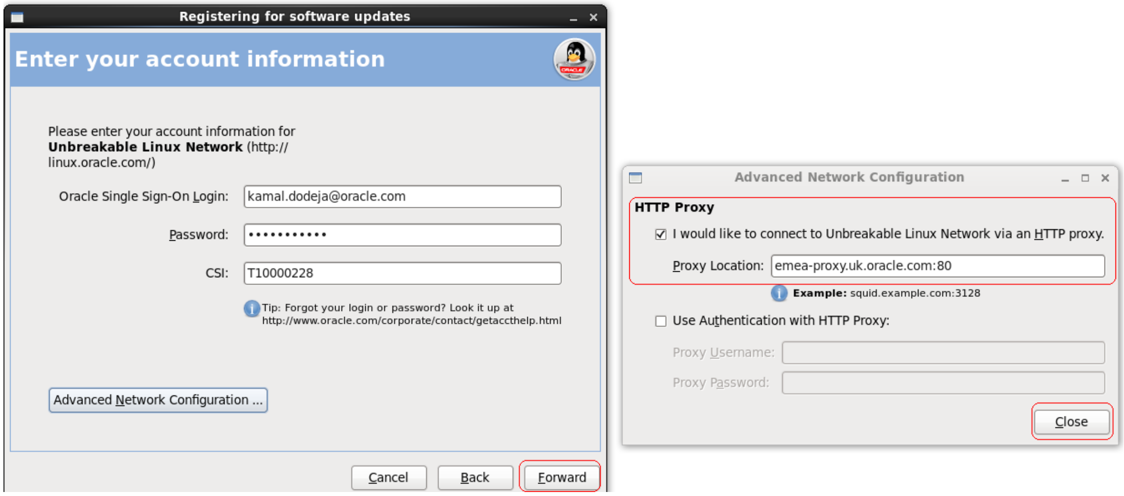
Tip: Forgot your login or password? Look it up at http://www.oracle.com/corporate/contact/getaccthelp.html

Figure 1. Unbreakable Linux Network welcome screen

Enter your authentication details on this page. You can obtain the Unbreakable Linux Network login ID required on this screen by going to http://linux.oracle.com/register. You will also require the valid Oracle Linux Support Customer Support Identifier (CSI) that is provided when you purchase an Oracle Linux Support subscription. Contact your Oracle Sales representative about purchasing an Oracle Linux Support subscription. You can also purchase Oracle Linux Support online via the Oracle Linux Store at oracle.com/linux.

Once you have the CSI, you will be able to create an Unbreakable Linux Network login ID and gain access to Oracle Linux Support, Linux software patches, updates, and fixes. You may also be able to raise customer support tickets based on the level of support you have opted for.

Once you have provided the login details, click **Advanced Network Configuration** to enter proxy details (if any); click **Close**; and to proceed to the next step, click **Forward**.



Registering for software updates
Advanced Network Configuration ...
Cancel
Back
Forward
Advanced Network Configuration
Close

Enter your account information

Please enter your account information for **Unbreakable Linux Network** (http://linux.oracle.com/)

Oracle Single Sign-On Login: kamal.dodeja@oracle.com

Password: •••••••••••

CSI: T10000228

Tip: Forgot your login or password? Look it up at http://www.oracle.com/corporate/contact/getaccthelp.html

HTTP Proxy

☑ I would like to connect to Unbreakable Linux Network via an HTTP proxy.

Proxy Location: emea-proxy.uk.oracle.com:80

Example: squid.example.com:3128

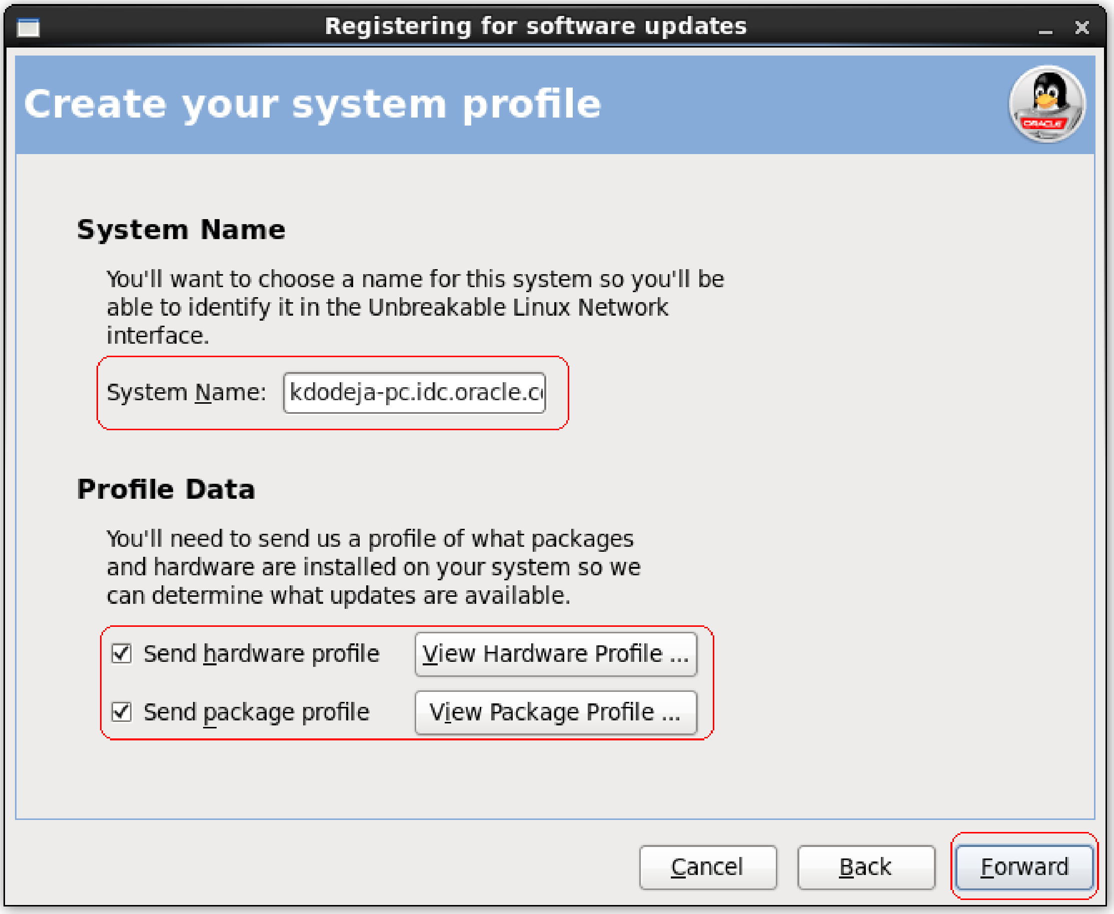
☐ Use Authentication with HTTP Proxy:

Proxy Username:

Proxy Password:

Figure 2. Unbreakable Linux Network’s Advanced Network Configuration screen

If your login details are correct, you will be presented with the following screen.



Create your system profile

System Name

You'll want to choose a name for this system so you'll be able to identify it in the Unbreakable Linux Network interface.

System Name: kdodeja-pc.idc.oracle.c

Profile Data

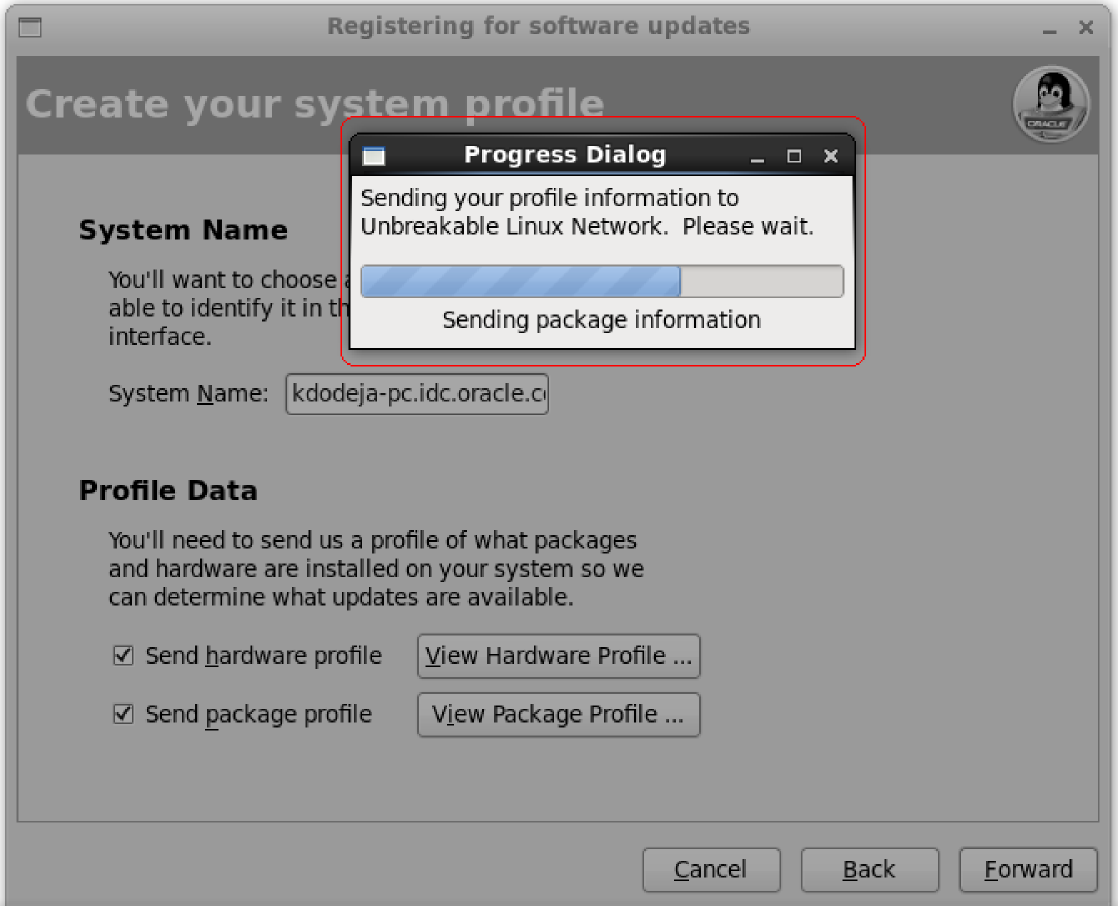
You'll need to send us a profile of what packages and hardware are installed on your system so we can determine what updates are available.

☑ Send hardware profile

☑ Send package profile

Figure 3. Unbreakable Linux Network system profile screen

When you click **Forward**, the process will collect the hardware and software package information of the server being registered and send it to the Unbreakable Linux Network. This is required so that appropriate packages can be made available for this system. It also helps in identifying the server being registered, for maintaining and managing its state later.



Sending your profile information to Unbreakable Linux Network. Please wait.

Sending package information

System Name

You'll want to choose a... able to identify it in th... interface.

System Name: kdodeja-pc.idc.oracle.c

Profile Data

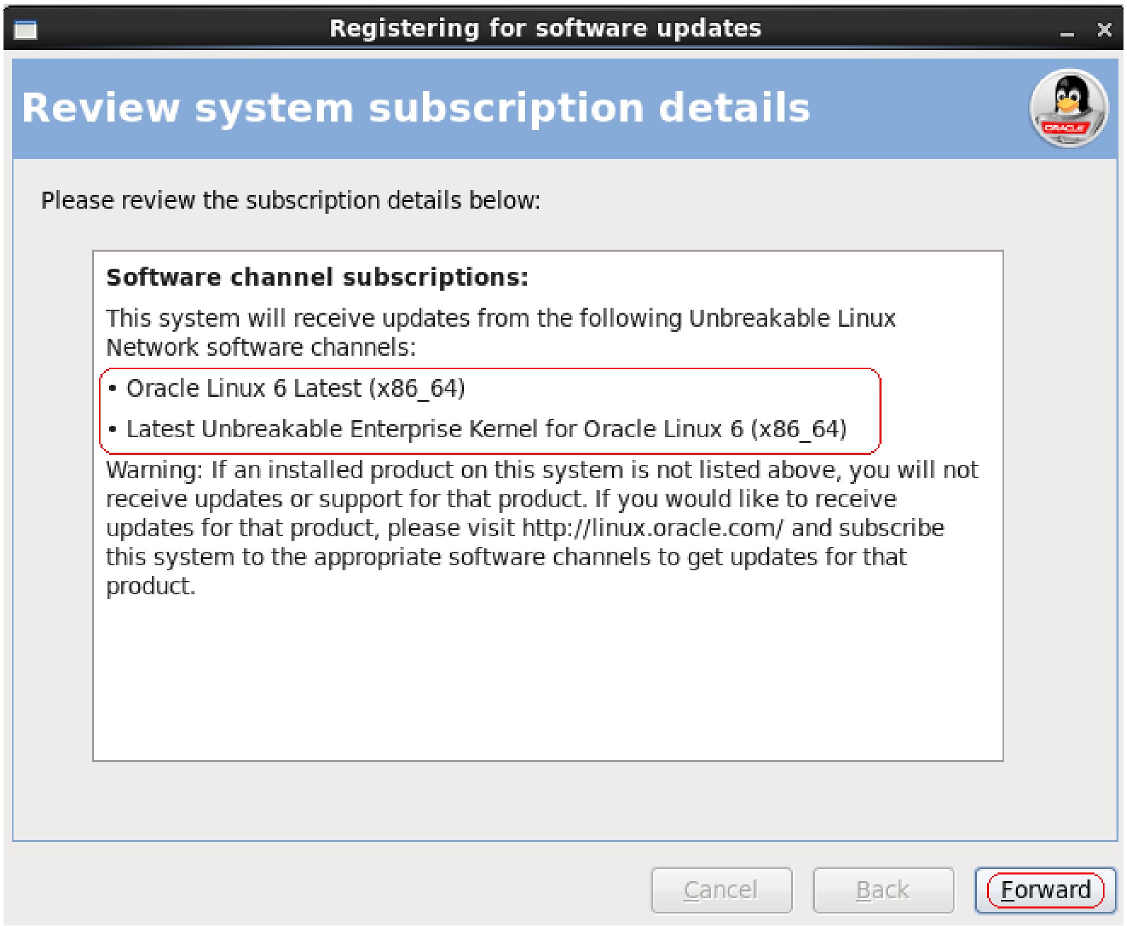
You'll need to send us a profile of what packages and hardware are installed on your system so we can determine what updates are available.

☑ Send hardware profile

☑ Send package profile

Figure 4. Unbreakable Linux Network progress dialog box

The next step shows the channels available for this system.



Review system subscription details

Please review the subscription details below:

Software channel subscriptions:

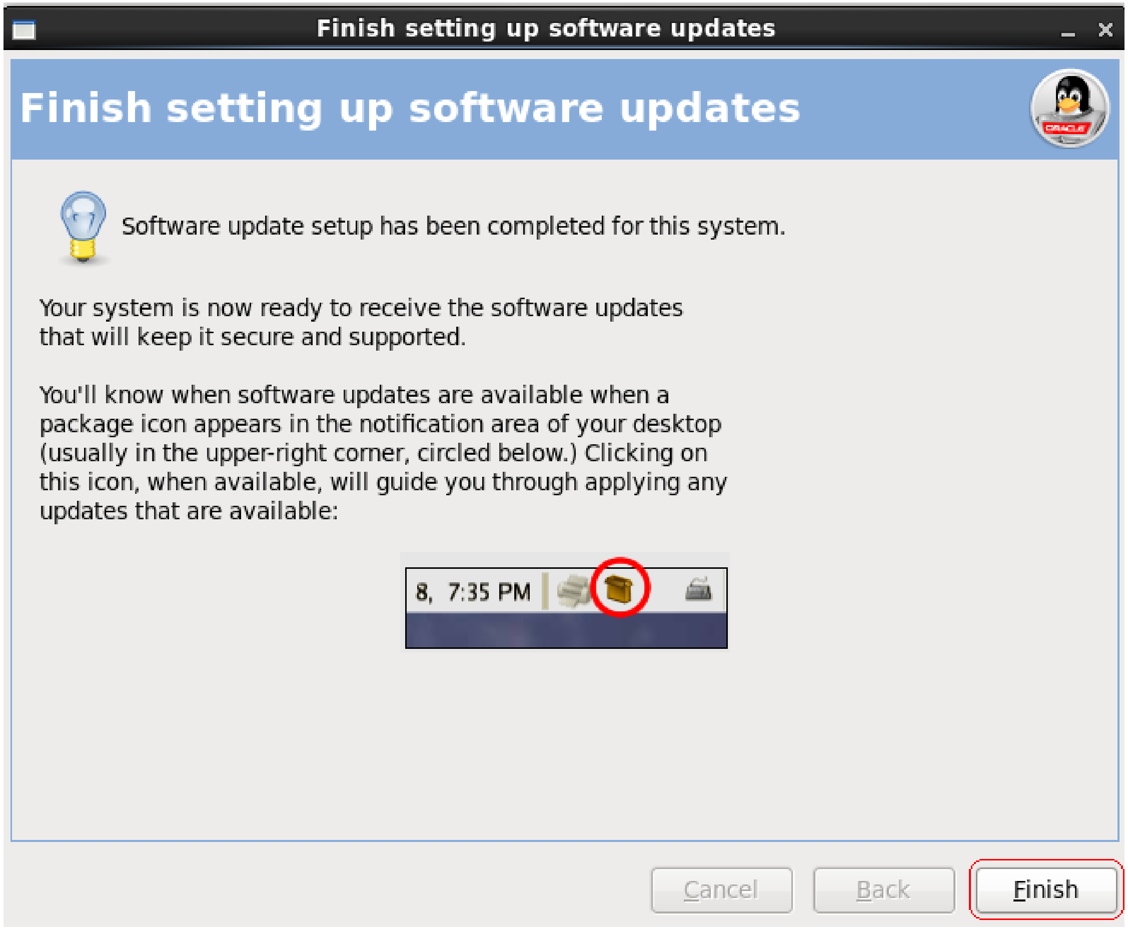
This system will receive updates from the following Unbreakable Linux Network software channels:

- Oracle Linux 6 Latest (x86_64)
- Latest Unbreakable Enterprise Kernel for Oracle Linux 6 (x86_64)

Warning: If an installed product on this system is not listed above, you will not receive updates or support for that product. If you would like to receive updates for that product, please visit http://linux.oracle.com/ and subscribe this system to the appropriate software channels to get updates for that product.

Figure 5. Unbreakable Linux Network channel subscriptions screen

Click **Finish** to complete the registration process.



Finish setting up software updates

Finish setting up software updates

Software update setup has been completed for this system.

Your system is now ready to receive the software updates that will keep it secure and supported.

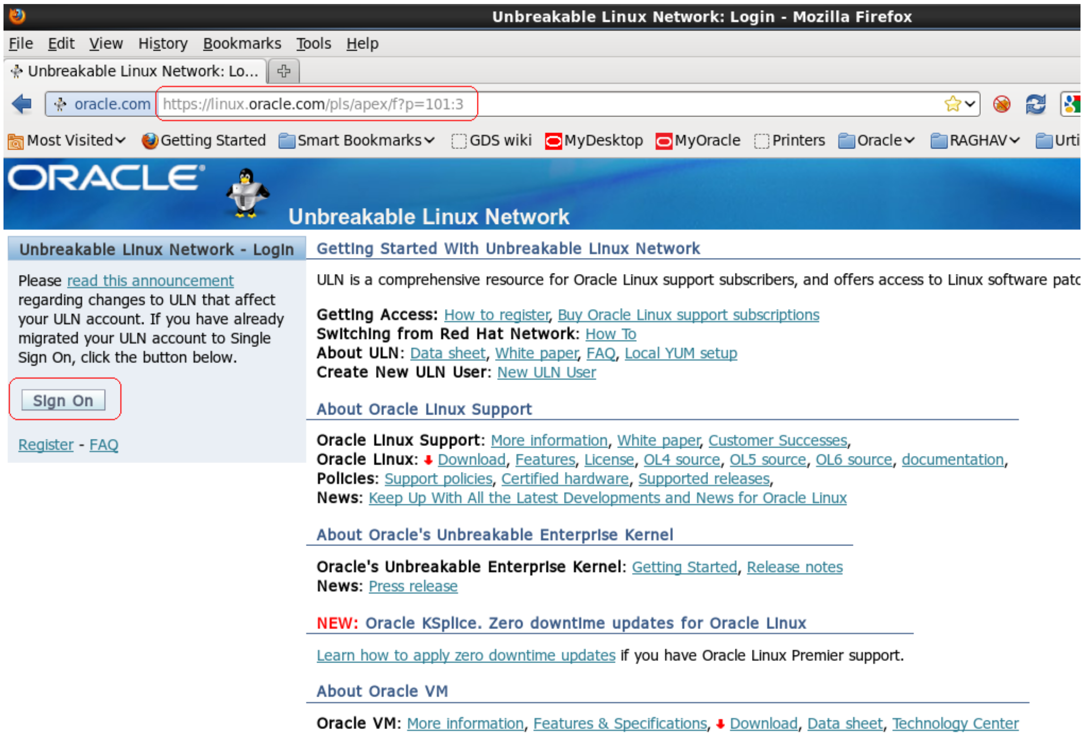
You'll know when software updates are available when a package icon appears in the notification area of your desktop (usually in the upper-right corner, circled below.) Clicking on this icon, when available, will guide you through applying any updates that are available:

Figure 6. Unbreakable Linux Network finish setup screen

After registering the server via the above process, you can visit the Oracle Unbreakable Linux Network to view, edit, and manage your subscriptions. To do this, follow these steps:

1. Open a Java-enabled Web browser, and enter https://linux.oracle.com.

2. Click **Sign On** to log in to the Unbreakable Linux Network to view registered system details and manage subscriptions.


Unbreakable Linux Network: Login - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Unbreakable Linux Network: Lo...
oracle.com https://linux.oracle.com/pls/apex/f?p=101:3
Most Visited Getting Started Smart Bookmarks GDS wiki MyDesktop MyOracle Printers Oracle RAGHAV Urti
ORACLE
Unbreakable Linux Network
Sign On

Unbreakable Linux Network - Login

Please read this announcement regarding changes to ULN that affect your ULN account. If you have already migrated your ULN account to Single Sign On, click the button below.

Register - FAQ

Getting Started With Unbreakable Linux Network

ULN is a comprehensive resource for Oracle Linux support subscribers, and offers access to Linux software patc

Getting Access: How to register, Buy Oracle Linux support subscriptions
Switching from Red Hat Network: How To
About ULN: Data sheet, White paper, FAQ, Local YUM setup
Create New ULN User: New ULN User

About Oracle Linux Support

Oracle Linux Support: More information, White paper, Customer Successes,
Oracle Linux: Download, Features, License, OL4 source, OL5 source, OL6 source, documentation,
Policies: Support policies, Certified hardware, Supported releases,
News: Keep Up With All the Latest Developments and News for Oracle Linux

About Oracle's Unbreakable Enterprise Kernel

Oracle's Unbreakable Enterprise Kernel: Getting Started, Release notes
News: Press release

NEW: Oracle Ksplice. Zero downtime updates for Oracle Linux

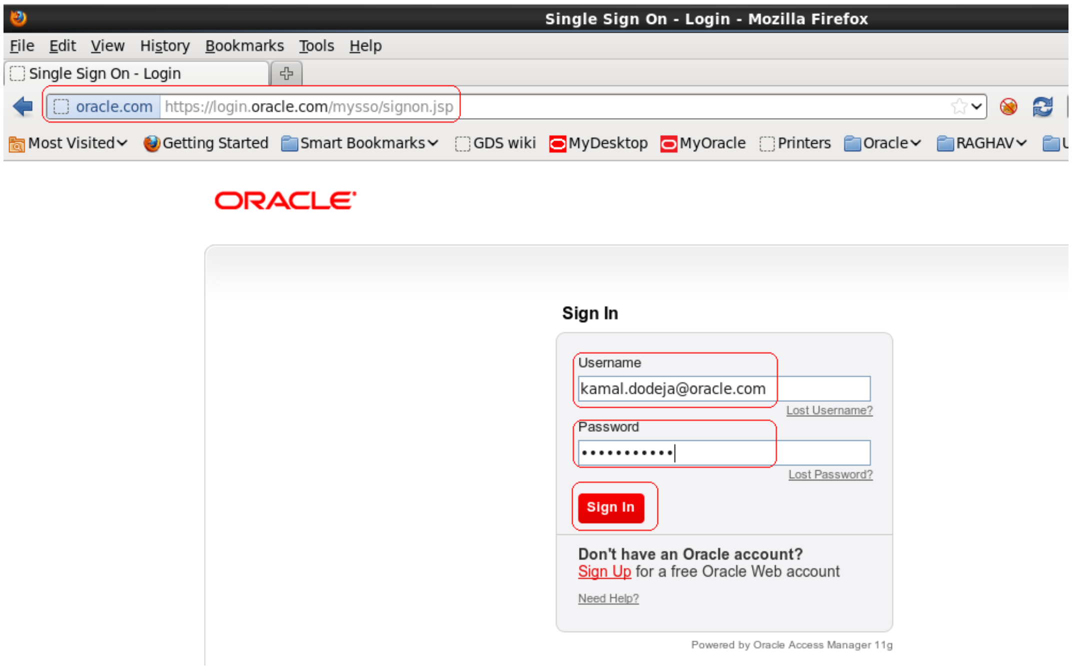
Learn how to apply zero downtime updates if you have Oracle Linux Premier support.

About Oracle VM

Oracle VM: More information, Features & Specifications, Download, Data sheet, Technology Center

Figure 7. Unbreakable Linux Network sign-on screen

3. Sign in to the Unbreakable Linux Network with a valid username and password.


Single Sign On - Login - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Single Sign On - Login
oracle.com https://login.oracle.com/mysso/signon.jsp
Most Visited Getting Started Smart Bookmarks GDS wiki MyDesktop MyOracle Printers Oracle RAGHAV U
ORACLE
Lost Username?
Lost Password?
Sign In
Need Help?

Sign In

Username: kamal.dodeja@oracle.com

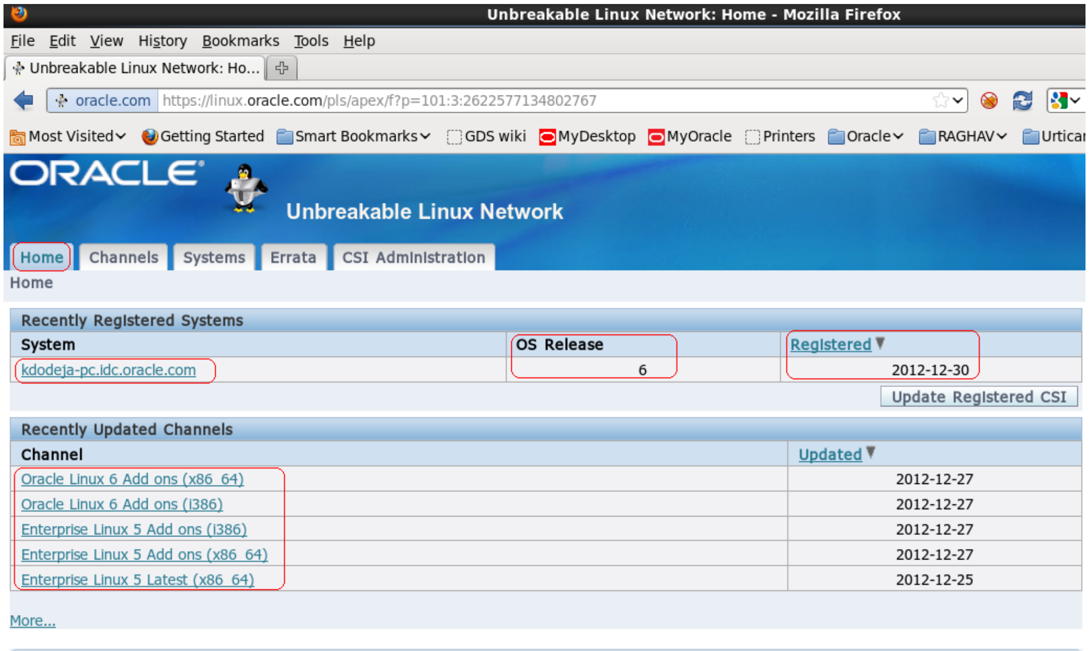
Password: ••••••••••••

Don't have an Oracle account?
Sign Up for a free Oracle Web account

Powered by Oracle Access Manager 11g

Figure 8. Unbreakable Linux Network sign-in

4. On the **Home** tab, you can see the registered system details, OS release, registration date, and channel names.


Unbreakable Linux Network: Home - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Unbreakable Linux Network: Ho...
oracle.com https://linux.oracle.com/pls/apex/f?p=101:3:2622577134802767
Most Visited Getting Started Smart Bookmarks GDS wiki MyDesktop MyOracle Printers Oracle RAGHAV Urticar
ORACLE
Unbreakable Linux Network
Home Channels Systems Errata CSI Administration
Home
Update Registered CSI
More...

Recently Registered Systems

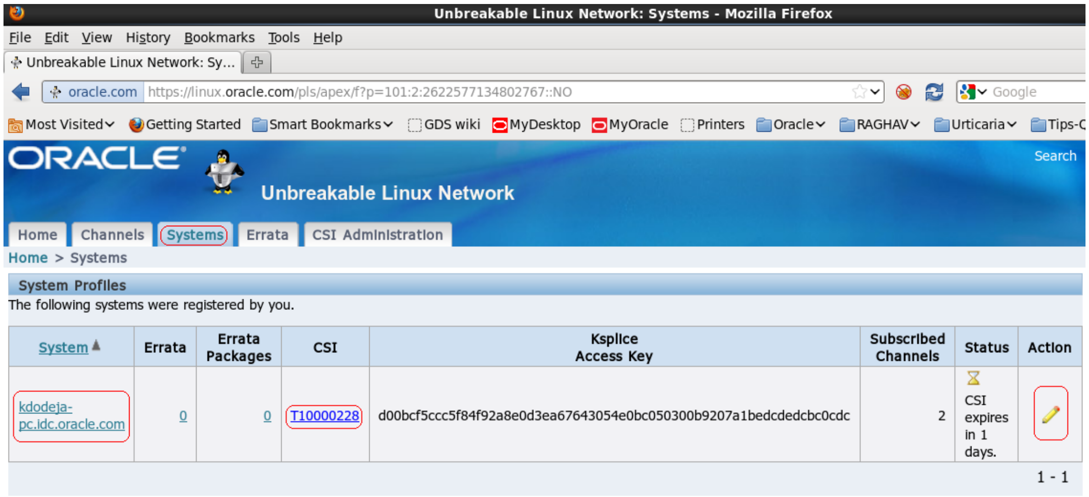
System	OS Release	Registered ▼
kdodeja-pc.idc.oracle.com	6	2012-12-30

Recently Updated Channels

Channel	Updated ▼
Oracle Linux 6 Add ons (x86_64)	2012-12-27
Oracle Linux 6 Add ons (i386)	2012-12-27
Enterprise Linux 5 Add ons (i386)	2012-12-27
Enterprise Linux 5 Add ons (x86_64)	2012-12-27
Enterprise Linux 5 Latest (x86_64)	2012-12-25

Figure 9. Unbreakable Linux Network Home tab with registered system details, OS release, registration date, and channel names

5. On the **Systems** tab, you can view registered system details. It shows the system host name, CSI number, subscribed channels count, and Ksplice access key (if you have Oracle Premier Support).


Unbreakable Linux Network: Systems - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Unbreakable Linux Network: Sy...
oracle.com https://linux.oracle.com/pls/apex/f?p=101:2:2622577134802767::NO
Google
Most Visited Getting Started Smart Bookmarks GDS wiki MyDesktop MyOracle Printers Oracle RAGHAV Urticaria Tips-C
ORACLE
Unbreakable Linux Network
Search
Home Channels Systems Errata CSI Administration
Home > Systems

System Profiles

The following systems were registered by you.

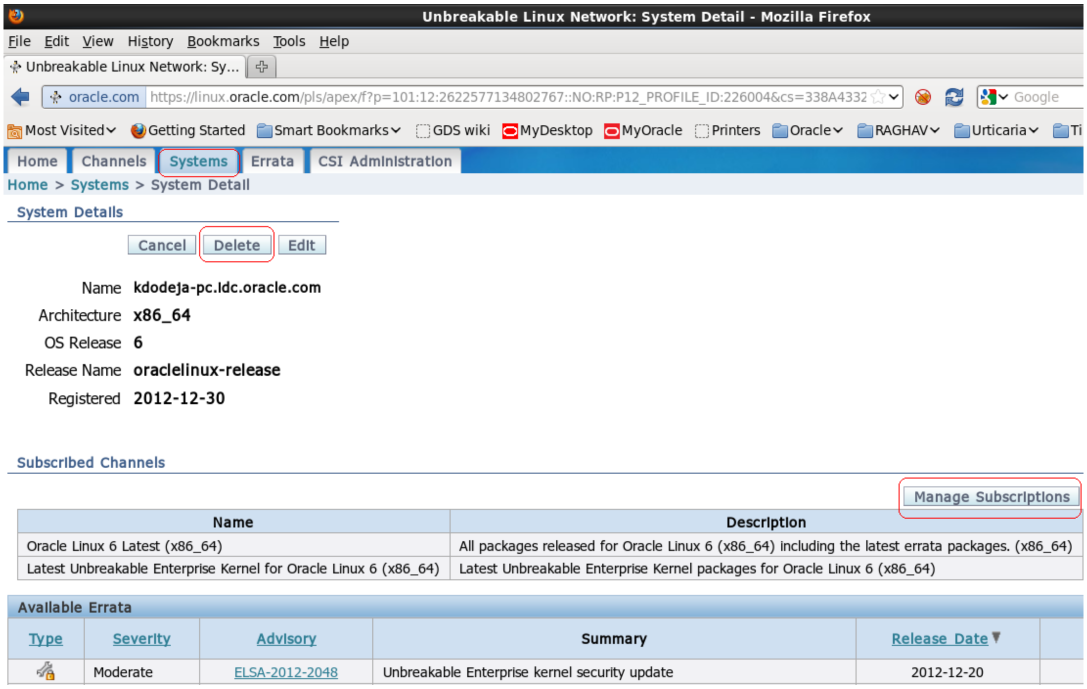
System ▲	Errata	Errata Packages	CSI	Ksplice Access Key	Subscribed Channels	Status	Action
kdodeja-pc.idc.oracle.com	0	0	T10000228	d00bcf5ccc5f84f92a8e0d3ea67643054e0bc050300b9207a1bedcdedcbc0cdc	2	⌛ CSI expires in 1 days.	✎

1 - 1

Figure 10. Unbreakable Linux Network Systems tab with system host name, CSI number, subscribed channels count, and Ksplice access key

6. Go to **Systems** -> **System Detail** to view system details. To unsubscribe the system from Unbreakable Linux Network, click **Delete**.

7. To manage a channels subscription, click **Manage Subscription**.


Unbreakable Linux Network: System Detail - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Unbreakable Linux Network: Sy...
oracle.com https://linux.oracle.com/pls/apex/f?p=101:12:2622577134802767::NO:RP:P12_PROFILE_ID:226004&cs=338A4332
Google
Most Visited Getting Started Smart Bookmarks GDS wiki MyDesktop MyOracle Printers Oracle RAGHAV Urticaria Ti
Home Channels Systems Errata CSI Administration
Home > Systems > System Detail
System Details
Cancel Delete Edit
Subscribed Channels
Manage Subscriptions
Available Errata

Name kdodeja-pc.idc.oracle.com

Architecture x86_64

OS Release 6

Release Name oraclelinux-release

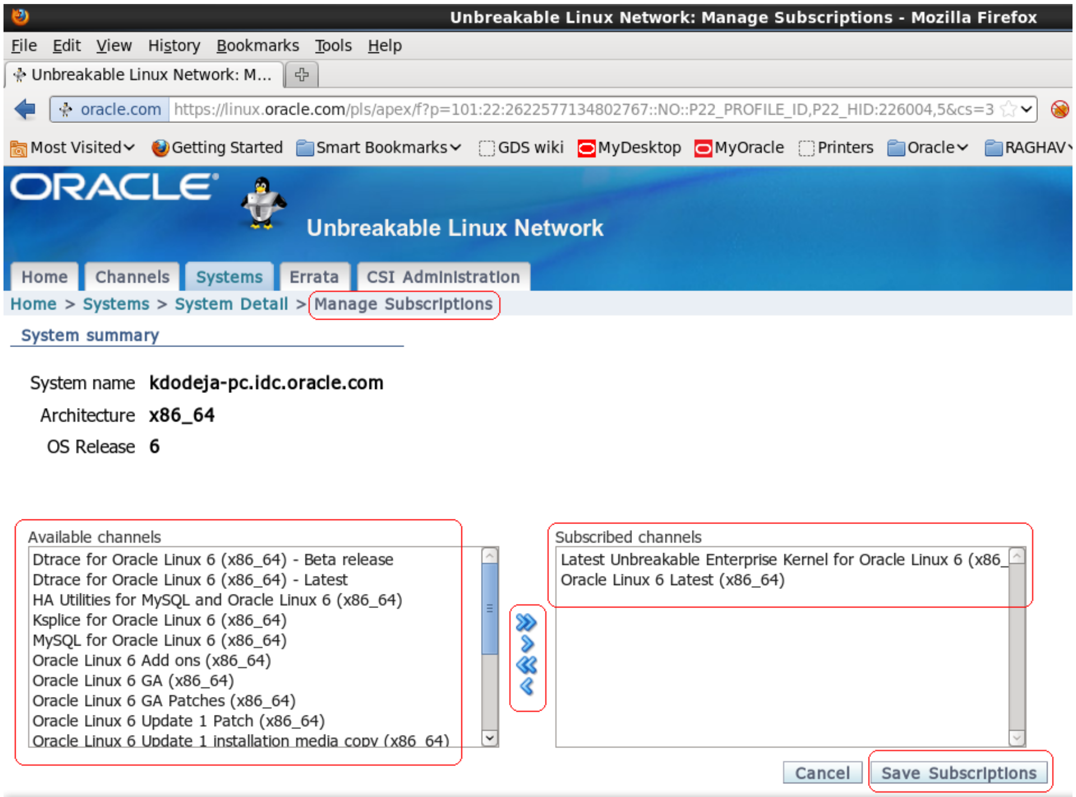
Registered 2012-12-30

Name	Description
Oracle Linux 6 Latest (x86_64)	All packages released for Oracle Linux 6 (x86_64) including the latest errata packages. (x86_64)
Latest Unbreakable Enterprise Kernel for Oracle Linux 6 (x86_64)	Latest Unbreakable Enterprise Kernel packages for Oracle Linux 6 (x86_64)

Type	Severity	Advisory	Summary	Release Date ▼
	Moderate	ELSA-2012-2048	Unbreakable Enterprise kernel security update	2012-12-20

Figure 11. Unbreakable Linux Network's System Details screen

Depending on your system configuration and support level, you will be able to access various Unbreakable Linux Network channels. As an Oracle Linux Premier Support customer, you will also have access to Ksplice technology and can subscribe to the Ksplice channel as well. The Ksplice channel provides kernel updates that can be applied in real time to a running Unbreakable Enterprise Kernel from Oracle. This is a significant advantage for Oracle Linux customers: it enables them to update the kernel of a running system and eliminates the need for any downtime. You can read more about Ksplice at http://oss.oracle.com/ksplice/docs/ksplice-quickstart.pdf or oracle.com/linux.


Unbreakable Linux Network: Manage Subscriptions - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Unbreakable Linux Network: M...
oracle.com https://linux.oracle.com/pls/apex/f?p=101:22:2622577134802767::NO::P22_PROFILE_ID,P22_HID:226004,5&cs=3
Most Visited Getting Started Smart Bookmarks GDS wiki MyDesktop MyOracle Printers Oracle RAGHAV
ORACLE
Unbreakable Linux Network
Home Channels Systems Errata CSI Administration
Home > Systems > System Detail > Manage Subscriptions
System summary
Cancel
Save Subscriptions

System name kdodeja-pc.idc.oracle.com
Architecture x86_64
OS Release 6

Available channels
Dtrace for Oracle Linux 6 (x86_64) - Beta release
Dtrace for Oracle Linux 6 (x86_64) - Latest
HA Utilities for MySQL and Oracle Linux 6 (x86_64)
Ksplice for Oracle Linux 6 (x86_64)
MySQL for Oracle Linux 6 (x86_64)
Oracle Linux 6 Add ons (x86_64)
Oracle Linux 6 GA (x86_64)
Oracle Linux 6 GA Patches (x86_64)
Oracle Linux 6 Update 1 Patch (x86_64)
Oracle Linux 6 Update 1 installation media copy (x86_64)

Subscribed channels
Latest Unbreakable Enterprise Kernel for Oracle Linux 6 (x86_
Oracle Linux 6 Latest (x86_64)

Figure 12. Unbreakable Linux Network's System Details -> Manage Subscriptions screen

8. You can now proceed to add or remove your channel subscriptions as required. The above example has the "Latest Unbreakable Enterprise Kernel for Oracle Linux 6 (x86_64)" channel added to the server you registered earlier. Similarly, you can add other channels. The list of channels available depends on the support level you have signed up for. To get access to a specific channel or group of channels, contact your Oracle sales representative.

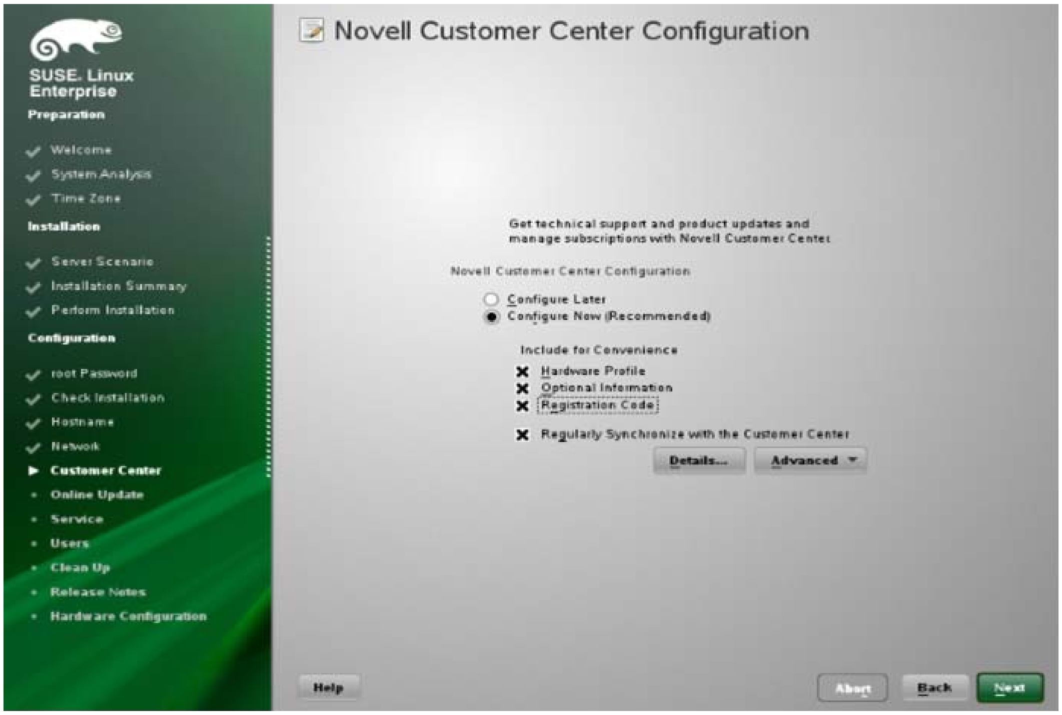
How Novell Customer Center Is Different

Registering and Updating SUSE Linux Enterprise

Novell Customer Center (NCC) is a centralized tool for managing products and subscriptions as well as customers' systems and administrators. For more information on the NCC, see www.novell.com/customercenter/. Registering a SUSE Linux Enterprise (SLE) machine with the NCC adds the system to the NCC for management and enables the system to receive online updates. Registering a machine can occur during or after SLE installation.

Registering During Installation

NCC registration is performed during installation, after the network has been configured and tested. If the network is not configured and tested, NCC configuration is skipped. To register with the NCC, choose **Configure Now (Recommended)** and click **Next** on the Novell Customer Center Configuration screen. To skip configuration and do it later, choose **Configure Later**.



Novell Customer Center Configuration

Get technical support and product updates and manage subscriptions with Novell Customer Center

Novell Customer Center Configuration

○ Configure Later
● Configure Now (Recommended)

Include for Convenience

☒ Hardware Profile
☒ Optional Information
☒ Registration Code

☒ Regularly Synchronize with the Customer Center

Details... Advanced ▾

Figure 13. Novell Customer Center Configuration screen

Registering After Installation

If the NCC configuration was skipped during installation, either intentionally or because of network problems, the configuration can be run later. To register:

1. Launch YaST.

2. Choose **Software** -> **Novell Customer Center Configuration**.

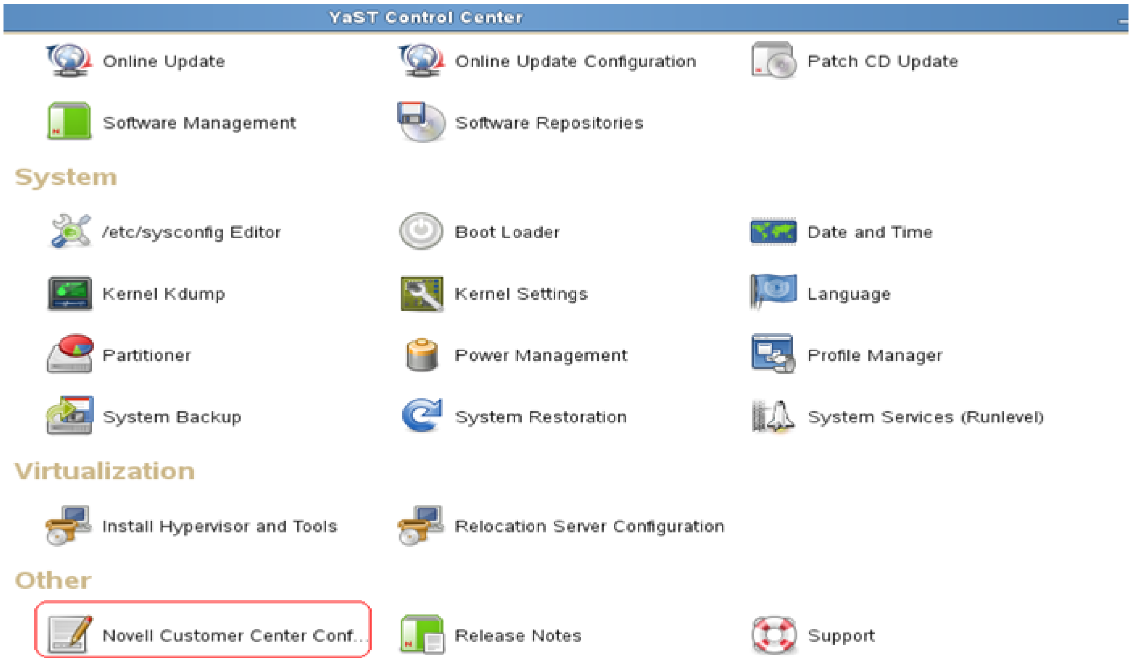
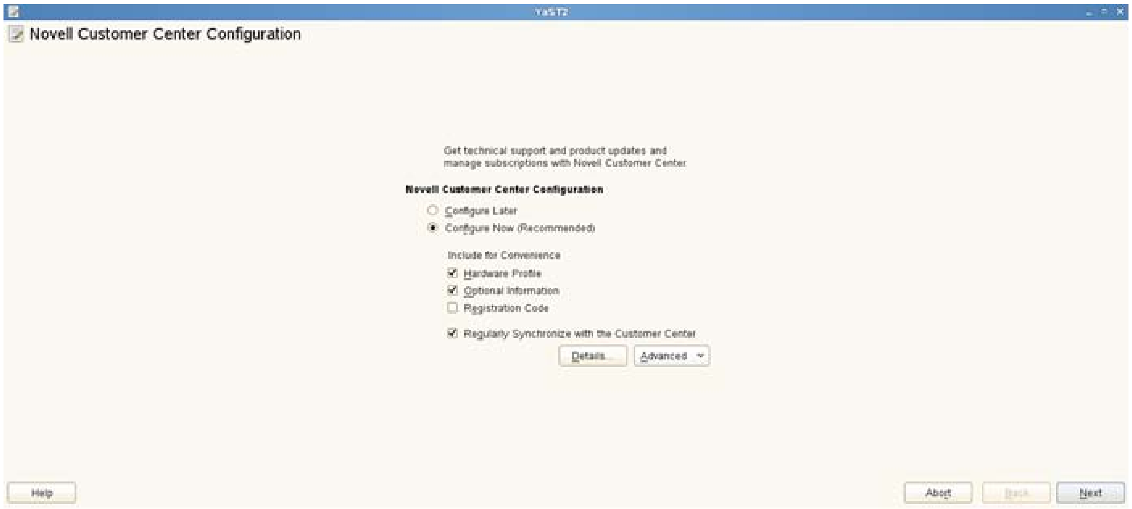


Figure 14. YaST Control Center screen with Novell Customer Center Configuration selected

3. Follow the wizard's further instructions.



Get technical support and product updates and manage subscriptions with Novell Customer Center

Novell Customer Center Configuration

○ Configure Later
● Configure Now (Recommended)

Include for Convenience

☑ Hardware Profile
☑ Optional Information
□ Registration Code

☑ Regularly Synchronize with the Customer Center

Figure 15. Another view of the Novell Customer Center Configuration screen

Booting and System Initialization

The Linux startup process is the process of Linux operating system initialization. In Linux the flow of control during the boot process is handed over from the computer BIOS to the boot loader and finally to the kernel. The kernel then starts the scheduler (to allow multitasking) and runs the first userland (outside kernel space) program, called INIT (which is mostly responsible for running startup scripts for each runlevel), at which point the kernel goes idle unless called externally. INIT (short for initialization) is a program for Linux-based computer operating systems that spawns all other processes.

Boot Process

The boot process has several phases.

- BIOS checks the system and peripheral devices as well as locating and running the Master Boot Record (MBR).
- The MBR loads the Grand Unified Bootloader (GRUB).
- The GRUB boots the kernel, using information in /boot/grub/menu.lst.
- The kernel starts initializing devices, loads additional device drivers from initrd image, and then starts the init process from /sbin/init.
- Init starts other processes based on the **/etc/inittab** file.
- /etc/rc.d/rc in Oracle Linux or /etc/init.d/rc in SUSE Linux runs the corresponding /etc/rcX.d scripts to start up other components.

Default Kernel Location

/boot contains the kernels and initrd images.

Default Kernel Modules Location

/lib/modules/'uname -r'/

Runlevels

TABLE OF RUNLEVELS

RUNLEVEL	DESCRIPTION
S or s	Minimal single-user mode in SUSE Linux. In Oracle Linux, it is the same as init level 1.
0	Power-down state. Shuts down the operating system and tries to turn power off, if supported by the system.
1	Single-user mode.
2	Multiuser without NFS resources shared. Text-only login.
3	Multiuser with NFS resources shared. Text-only login.
4	N/A (alternative multiuser).
5	Full multiuser, NFS resources shared, and graphic login with X display manager.
6	Reboot.
Emergency	Ignore the **/etc/inittab** file, and launch the default shell.

Boot Configuration Files

Boot configuration involves several files.

/etc/inittab File

When the kernel loads the /sbin/init program, it reads the**/etc/inittab** file to see what the default run level is and what scripts need to run. After initialization, the information in this file is used whenever the administrator changes the run level of the system.

If you modify the **/etc/inittab** file and want to instruct init to reload it, you can do so with the `init q` or `init Q` commands.

Run Control (rc) Files

Each run level has a set of scripts associated with it called run control files or rc files.

The scripts directory associated with each run level is /etc/rcX.d/ in Oracle Linux and /etc/init.d/rcX.d in SUSE Linux, where X is the run level, and usually the scripts in those directories are mostly symbolic links to the /etc/init.d/ main service scripts.

For instance, in Oracle Linux, /etc/rc3.d/S80sendmail is a symbolic link to the /init.d/sendmail script and /etc/rc1.d/K30sendmail is a symbolic link to the same script.

Oracle Linux has only one set of scripts for each run level, meaning that for run level 3, the init program runs only the scripts for run level 3. It does not run the lower-run-level scripts to get to its intended run level. Pay extra attention to where you manually place an rc script.

In Oracle Linux, you can restart or check the status of most services by passing the argument restart or status to the service script in the /etc/init.d directory:

```
# /etc/init.d/sendmail restart

# /etc/init.d/sendmail status
```

Running the service script without options lists the supported options for that specific script:

```
# /etc/init.d/sendmail

Usage: /etc/init.d/sendmail {start|stop|restart|condrestart|status}
```

Disabling RC Scripts

Sometimes you may need to prevent certain services from running automatically at boot time initialization. In Linux, you can use the `chkconfig` command or GUI programs such as system-config-services in Oracle Linux or the System/Runlevel Editor module from YaST2 in SUSE Linux.

As a fairly common practice, system administrators usually disable the iptables service during installation. This service provides a way to protect and secure the operating systems from network-related threats. It is a good idea to configure a set of suitable iptables rules and enable the iptables service once the Linux server is fully configured to meet requirements.

The following section first gives an overview of the `chkconfig` command and demonstrates how it can be used to check the present status of various Linux services. It then gives an example of configuring some sample iptables rules and enabling the iptables service to automatically start up during the boot-up sequence.

With the `ckhconfig -- list` command, you can view the current boot time status of various services on an Oracle Linux server.

```
# chkconfig -- list

abrtd 0:off 1:off 2:off 3:on 4:off 5:on 6:off

acpid 0:off 1:off 2:off 3:off 4:off 5:off 6:off

atd 0:off 1:off 2:off 3:on 4:on 5:on 6:off

...

…

iptables 0:off 1:off 2:off 3:off 4:off 5:off 6:off

…

…
```

…

…

In the above, you can see that

- The abrtd service is set to automatically start at runlevels 3 and 5.
- The acpid service is set to remain off at all runlevels.
- The atd service is configured to start automatically at runlevels 3, 4, and 5.
- The iptables service is set to remain off at all runlevels.
- Adding some iptables rules and then enabling the iptables service to start automatically during the boot-up sequence will illustrate the startup sequence.

A complete overview of iptables is beyond the scope of this document, but you can refer to the documentation on Netfilter and iptables(8) for more information.

Example

This example adds rules to iptables to drop all incoming connections but allow outgoing traffic originating from the server.

```
# iptables -P INPUT DROP

# iptables -P FORWARD DROP

# iptables -P OUTPUT ACCEPT

# iptables -A INPUT -m state --state NEW,ESTABLISHED -j ACCEPT

# iptables -L -v -n

### *** now ping and wget should work *** ###

# ping oracle.com

$ wget http://www.openss7.org/repos/tarballs/strx25-0.9.2.1.tar.bz2
```

At this point, the iptables rules are running in memory, but they will be lost when the server reboots. To restore them after a reboot, save these rules into a file by using the following command.

```
# /sbin/service iptables save
```

Note that the above command will run only if the iptables init script is already present in the /etc/init directory. This init script, part of the distribution, is installed during installation.

On successful execution of the above command, the iptables init script runs the /sbin/iptables-save program and writes the current iptables configuration to the **/etc/sysconfig/iptables** file. Any existing **/etc/sysconfig/iptables** file is saved as **/etc/sysconfig/iptables.save**.

The last step is to enable iptables to start up automatically at each reboot and invoke the **/etc/sysconfig/iptables** file to load the iptables rules you saved earlier. To enable this, issue the following command:

```
 # chkconfig --add iptables
```

Whenever you add a service to or remove it from `chkconfig` control, it does the following under the /etc/rc.d subdirectories:

- When the `chkconfig --add` command is executed, it creates a symbolic link file to start and stop the service under the corresponding rc directory.
- When the `chkconfig --del` command is executed, it removes the symbolic link file from the corresponding rc directory.

To verify the successful addition of the iptables service, you can check with the following command:

- `# chkconfig --list | grep iptables`

```
iptables 0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

You can see that the iptables service is now set to automatically start at boot time and will be run when the system boots up in either runlevel 3, 4, or 5. This is the default behavior when a service is added with the `chkconfig` utility.

The `chkconfig` utility can be used to manage the startup services in a variety of other ways as well. A few more examples are listed below for quick reference:

- To view other services that are configured to be started during system startup at runlevel 3, you can issue the following command:
  - `# chkconfig --list | grep 3:on`
- To check the settings of a particular service, use grep to filter the output of `chkconfig --list` for that service. For example, to check the network service, use the following command:
  - `# chkconfig --list | grep network`

Shutting Down

The `shutdown`, `reboot`, `halt`, `poweroff`, and `init` commands exist in both Oracle Linux and SUSE Linux:

• `init 6`	`reboot`
• `init 0`	`shutdown/halt/poweroff`

Package Management

Introduction to Package Management

In most operating systems, a package management system or tool is provided for automating the process of installing, upgrading, configuring, and removing software packages in a consistent manner. The package management system typically maintains a database of software dependencies and version information to prevent software mismatches and detect whether any prerequisites are missing.

Packages are distributions of software, applications, and data. They also contain metadata, such as the software name, description of its purpose, version number, vendor, checksum, and a list of dependencies necessary for the software to run properly. Postinstallation, metadata is stored in the local package database.

Oracle Linux and SUSE Linux both use the RPM Package Manager (RPM) for software package management. RPM includes features for package management such as dependency and signature checking and for other advanced options.

The RPM is a powerful command-line-driven package management system capable of installing, uninstalling, verifying, querying, and updating computer software packages. Each software package consists of an archive of files, along with information about the package such as its version, description, and dependencies. There is also an API library enabling advanced developers to manage such transactions with programming languages such as C or Python.

RPM is free software, released under the GNU general public license (GPL). It is a core component of many Linux distributions, including Oracle Linux, Red Hat Enterprise Linux, the Fedora Project, SUSE Linux, openSUSE, CentOS, and many others. Following are some noteworthy highlights:

- Oracle Linux uses RPM.
- Oracle Linux also provides the YUM utility, which
  - Resolves RPM dependencies
  - Connects to repositories to download software
- The Oracle public YUM server
  - Offers a free way to install packages
  - Has free errata
- The Unbreakable Linux Network
  - Is a comprehensive resource for support subscribers
  - Offers access to software patches, updates, and fixes

Usage of the RPM Utility

The following section outlines how the RPM utility can be used to query the packages installed on either Oracle Linux or SUSE Linux.

- Query options:
  - `# rpm –qa`
  - `# rpm –qi` *`package_name`*
  - `# rpm –ql` *`package_name`*
  - `# rpm –qf` *`filename`*
  - `# rpm –qc` *`package_name`*
- Installing and updating packages:
  - `# rpm –Uvh` *`package_name`*
- Installing a new kernel:
  - `# rpm –ivh` *`kernel_package_name`*
- Removing packages:
  - `# rpm –e` *`package_name`*

Oracle Public YUM Server

The following section outlines various methods for accessing software packages, updates, and errata. Oracle offers a public YUM server that serves as a central repository for these software packages and more. The Oracle public YUM server is a repository that contains all the updates and patches for Oracle Linux and is available to everyone, whether they have purchased Oracle Linux Support or not.

Purchasing Oracle Linux Support offer several advantages, however, and gives customers the ability to raise support tickets and receive support for their Oracle Linux systems. Apart from being able to raise support tickets, customers also become eligible for indemnification support directly from Oracle for their Oracle Linux systems. Depending on what level of support the customers opt for, other advantages of purchasing Oracle Linux Support can also include access to Ksplice updates for Oracle Linux's Unbreakable Enterprise Kernel, priority service-level agreements (SLAs) for critical systems, backporting, and lifetime support options.

Oracle Public YUM Server Benefits

The Oracle public YUM server provides customers with the following:

Errata Availability

Errata are freely available from the Oracle public YUM server. Subscribe to the Oracle errata mailing list at http://linux.oracle.com/register.

Packages

Packages can be accessed at http://public-yum.oracle.com/.

Understanding the Usage of the wget Utility

The wget utility is a popular network utility for retrieving files from the Web, using HTTP and FTP, the two most widely used internet protocols. It works noninteractively, so it can work in the background after you have logged off. It can handle most any complex download situations, such as large file downloads, recursive downloads, noninteractive downloads, and multiple file downloads.

The wget utility works particularly well with slow or unstable connections, continuing to retrieve a document until it is fully downloaded. Continuing to get files from where it left off works on servers (both HTTP and FTP) that support it. HTTP as well as FTP retrievals can be time-stamped, so wget can see if a remote file has changed since the last retrieval and automatically retrieve the new version if it has.

The wget utility supports proxy servers, which can lighten the network load, speed up retrieval, and provide access behind firewalls.

The following example downloads a file from the internet and stores it in the current directory:

- $ wget http://www.openss7.org/repos/tarballs/strx25-0.9.2.1.tar.bz2

The download in progress shows the following:

- $ wget http://www.openss7.org/repos/tarballs/strx25-0.9.2.1.tar.bz2
- Saving to: `strx25-0.9.2.1.tar.bz2.1’
- 31% [=================> 1,213,592 68.2K/s eta 34s
- Download completed.

The wget utility prints a progress bar with the following information during the download:

- Percentage of download completion (31% in the above example)
- Total number of bytes downloaded so far (1,213,592 bytes in the above example)
- Current download speed (68.2 K/s in the above example)
- Remaining time to download (eta 34 seconds in the above example)

Using the wget Utility

You can use the wget utility to download the repository file from the Oracle Linux public YUM server by following these steps:

- cd /etc/yum.repos.d
- `# wget http://public-yum.oracle.com/public-yum-ol6.repo`

After the download, enable the appropriate YUM repository by editing the YUM configuration file as follows:

- Open the YUM configuration file in a text editor.
- Locate the section in the file for the repository from which you plan to update, such as [el6_base].
- Change enabled=0 to enabled=1

Begin using YUM. For example:

- `yum list`
- `yum install firefox`

You may be prompted to confirm the import of the Oracle Open Source Software (OSS) Group GNU Privacy Guard (GnuPG or GPG) key.

YUM Configuration

To configure the YUM package management tool, you need to know that

- **/etc/yum.conf** is the primary configuration file and holds global settings.
- **/etc/yum.repos.d i**s the directory that defines repositories and contains repository files.
- Repository files define which repositories to use.
- Each repository file includes specifications for related repositories.
- The baseurl directive indicates the location of the main repository.
- The enabled directive (set to 1) designates the repository to use.

The YUM Utility

The following section outlines various methods for accessing software packages, updates, and errata via the YUM command line.

- List all packages
  - `# yum list`
- List all installed packages
  - `# yum list installed`

- List packages available to be installed
  - `# yum list available`
- Check for updates to installed packages
  - `# yum check-update`
- Update, install, remove packages, respectively
  - `# yum update package_name`
  - `# yum install package_name`
  - `# yum remove package_name`

YUM Groups

YUM groups are collections of software packages referred to by a single “group” name. YUM supports the following group commands:

- `yum grouplist`
- `yum groupinfo groupname`
- `yum groupinstall groupname`
- `yum groupupdate groupname`
- `yum groupremove groupname`

User and Group Administration

Linux is a multiuser time sharing operating system. It enables multiple users to be logged in at the same time and perform their own independent activities. Because both Oracle Linux and SUSE Linux enable multiple users to exist on the system, managing all of them requires additional tools and activities.

The complete user information is stored in the **/etc/passwd** and **/etc/shadow** files; similarly, group membership information is stored in the **/etc/group** file. The following sections briefly outline the tasks associated with managing users and groups on any Linux system. Specifically, it covers the following topics:

- User and group implementation
- User and group configuration files
- Configuring users and groups by using command-line utilities
- Implementing user private groups (UPGs)
- Configuring password aging and the hashing algorithm
- Using the User Manager GUI tool
- User and group implementation in the enterprise

Introduction to Users and Groups

Here's what you need to know about users and groups.

- User account information is stored in **/etc/passwd**.
- Group information
  - Group information is stored in **/etc/group**.
  - Each user has a private group (UPG).
  - Users can belong to more than one group.
- Oracle Linux uses shadow passwords.
  - /etc/shadow: hashed user passwords
  - /etc/gshadow: hashed group passwords
  - /etc/login.defs: security policies

User and Group Configuration Files

Here's what you need to know about user and group configuration files.

- Contents of **/etc/passwd**
  - username: placeholder: UID: GID: GECOS: home dir: shell
- Contents of **/etc/shadow**
  - username: hashed password: password aging information
- Contents of **/etc/group**
  - groupname: placeholder: GID: comma-separated members
- Contents of **/etc/gshadow**
  - groupname: hashed password: GID: comma-separated administrators: comma-separated members
  - Group passwords are rarely used.

Adding a User Account

The following is what you need to know to add a user account in Oracle Linux or SUSE Linux.

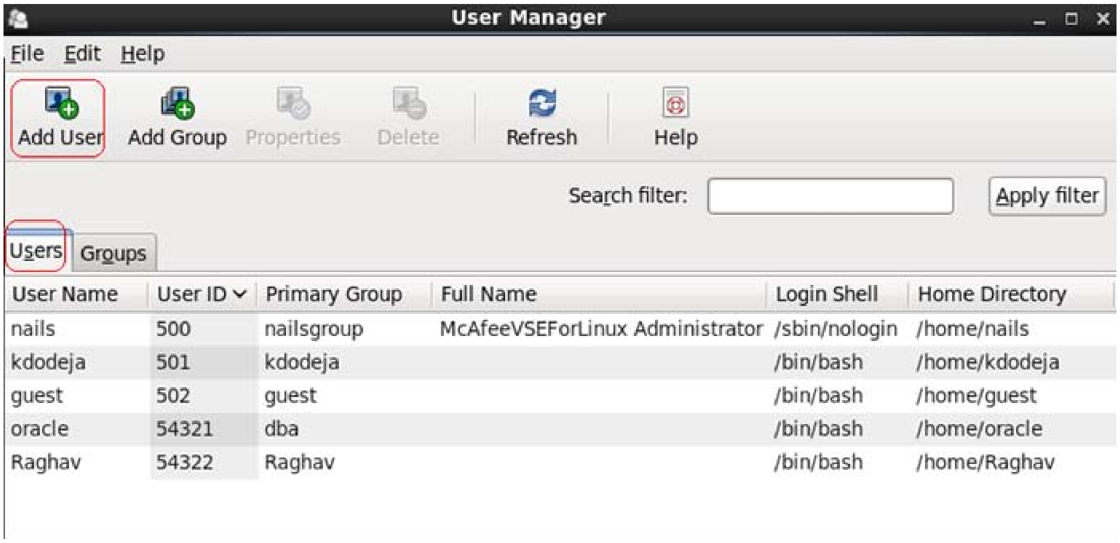
In Oracle Linux

You can add users with command-line options or via a GUI. In GUI mode, you can use the `system-config-users` command, which opens a dialog box in which new users' details can be entered. With the command line:

- Use the `useradd` command to add a user.
  - `#useradd [options] user_name`
- Use the `passwd` command to create a password.
  - `#passwd [options] user_name`
- User default settings are stored in **/etc/default/useradd**.
- Use the –D option to display or modify defaults.
  - `#useradd -D [options]`
- A new user's home directory is populated with files from the /etc/skel directory.
- You can create a nologin user.
  - `#useradd -s /sbin/nologin user_name`

With the GUI Interface in Oracle Linux

Use the `#system-config-users` command.



User Name	User ID	Primary Group	Full Name	Login Shell	Home Directory
nails	500	nailsgroup	McAfeeVSEForLinux Administrator	/sbin/nologin	/home/nails
kdodeja	501	kdodeja		/bin/bash	/home/kdodeja
guest	502	guest		/bin/bash	/home/guest
oracle	54321	dba		/bin/bash	/home/oracle
Raghav	54322	Raghav		/bin/bash	/home/Raghav

Figure 16. Oracle Linux's User Manager screen with Add User selected

In SUSE Linux

The command-line options for SUSE Linux are the same as in Oracle Linux. In GUI mode, you can use **YaST Control Center** -> **Users and Group Management**.

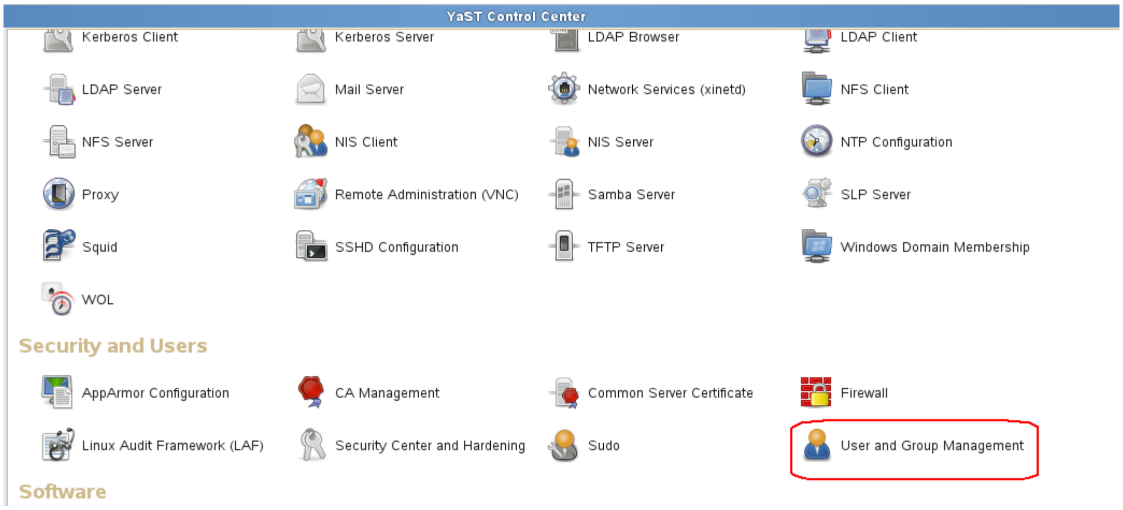


Figure 17. SUSE Linux's YaST Control Center screen with User and Group Management selected

Modifying or Deleting User Accounts

You have the following options for modifying or deleting user accounts.

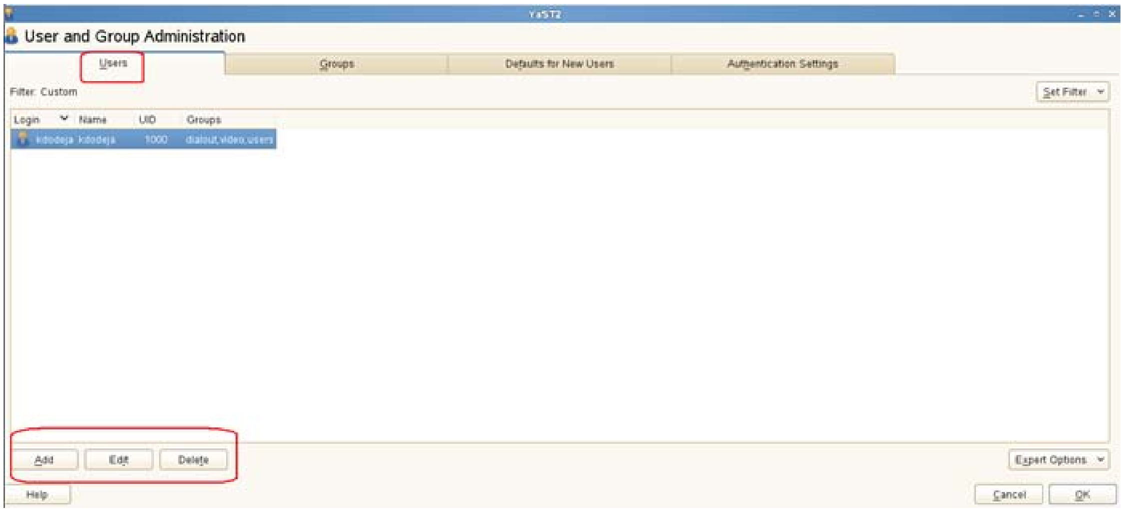
In Oracle Linux

You can modify users with command-line options or in GUI mode. The GUI can be accessed with the `system-config-users` command, which opens a dialog box in which new users' details can be edited. The command line can be used as follows:

- Use the `usermod` command to modify a user.
  - `#usermod [options] user_name`
- Add a user to a secondary group. For example, with GID=517:
  - `#usermod -aG 517 user_name`
- Use the `userdel` command to delete a user.
  - `#userdel [options] user_name`
- Options to userdel include
  - -f: Force removal even if the user is logged in
  - -r: Remove the user's home directory

In SUSE Linux

The command-line options for SUSE Linux are the same as in Oracle Linux. In GUI mode, you can use **YaST Control Center** -> **User and Group Administration** -> **Users**.



Filter: Custom

Login	Name	UID	Groups
kdodeja	kdodeja	1000	dialout,video,users

Figure 18. SUSE Linux YaST Control Center -> User and Group Administration -> Users screen

Group Account Administration

Both Oracle Linux and SUSE Linux enable you to administer group accounts.

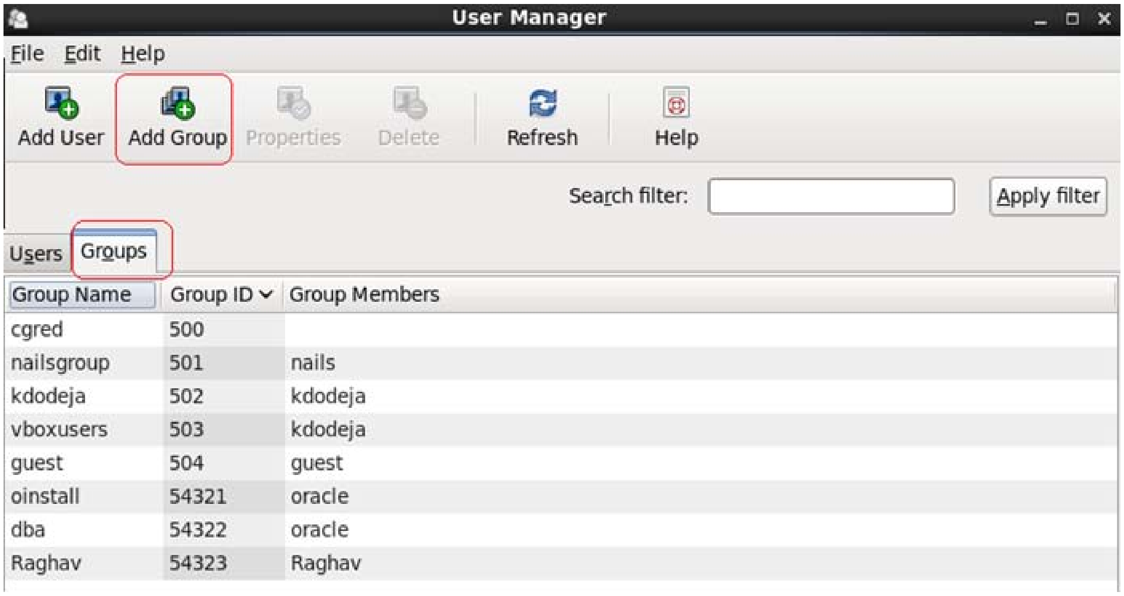
In Oracle Linux

You can add groups by using command-line options or via GUI mode. You can use the `system-config-users` command, which opens a dialog box in which new users' details can be added. The command line can be used as follows:

- Use the `groupadd` command to add a group account.
  - `#groupadd [options] group_name`
- Use the `groupmod` command to modify a group account.
  - `#groupmod [options] group_name`
- Use the `groupdel` command to delete a group account.
  - `#groupdel group_name`
- Use the `gpasswd` command to administer group accounts.
  - `#gpasswd [options] group_name`
- Add a user. For example, add (jim) to a group (students).
  - `#gpasswd –a jim students`
- The `groups` command prints the groups to which a user belongs.
- The `newgrp` command changes the current group identification.

With the GUI Interface in Oracle Linux

Use the `#system-config-users` command.

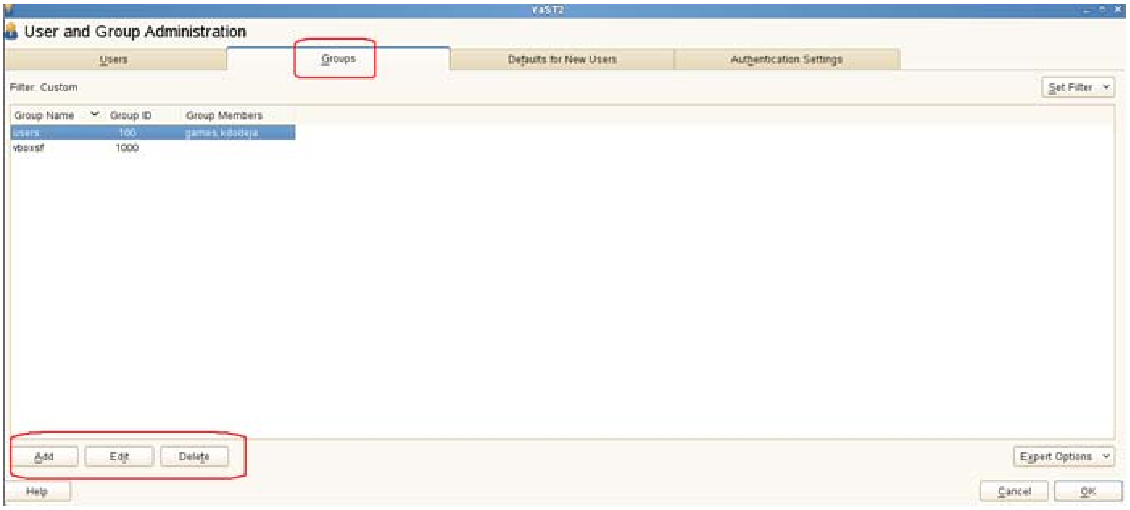


Group Name	Group ID	Group Members
cgred	500	
nailsgroup	501	nails
kdodeja	502	kdodeja
vboxusers	503	kdodeja
guest	504	guest
oinstall	54321	oracle
dba	54322	oracle
Raghav	54323	Raghav

Figure 19. Oracle Linux's User Manager screen with the Groups tab selected

In SUSE Linux

The command-line options for SUSE Linux are the same as in Oracle Linux. In GUI mode, you can use **YaST Control Center** -> **User and Group Administration** -> **Groups**.



Filter: Custom

Group Name	Group ID	Group Members
users	100	games, kdodeja
vboxsf	1000	

Figure 20. SUSE Linux's YaST Control Center -> User and Group Administration -> Groups screen

User Private Groups

Each user usually belongs to a unique group.

- Private groups eliminate the need for umask=0022 , which makes groups read-only.
- Having private groups allows umask=0002, which gives write permission to a group.

Additional steps to implement:

- Create a directory to share.
- Create a new group.
- Add users to this new group.
- Change the group ownership for the directory.
- Set the setgid bit on the directory.

Password Configuration

Password aging requires users to change their password regularly. Use the `chage` command to configure password aging:

```
chage [options] user_name
```

Current values are displayed and changed interactively:

- Minimum Password Age [0]:
- Maximum Password Age [99999]:
- Last Password Change [2011-11-06]:
- Password Expiration Warning [7]:
- Password Inactive [-1]:
- Account Expiration Date [1969-12-31]:

Use the `authconfig` command to configure the password hashing algorithm:

```
authconfig --passalgo=<algorithm> --update
```

The /etc/login.defs File

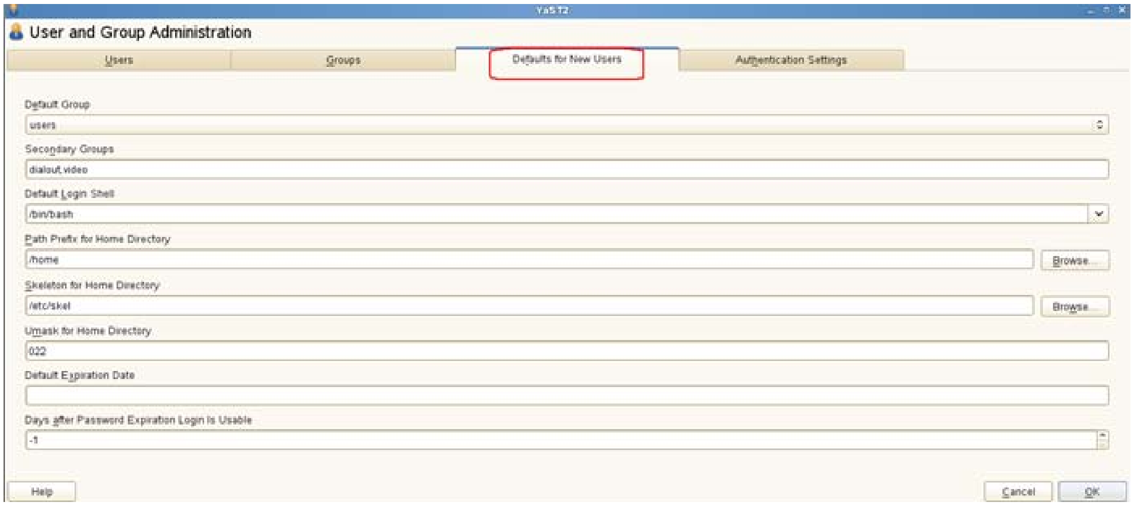
The **/etc/login.defs** file provides default user account settings. Default values include the following:

- Location of user mailboxes
- Password aging controls
- Values for automatic UID selection
- Values for automatic GID selection

- User home directory creation options
- umask value
- Encryption method used to encrypt passwords

In SUSE Linux

The command-line options for SUSE Linux are the same as in Oracle Linux. In GUI mode, you can use **YaST Control Center** -> **User and Group Administration** -> **Default for New Users.**



Default Group
users

Secondary Groups
dialout,video

Default Login Shell
/bin/bash

Path Prefix for Home Directory
/home

Skeleton for Home Directory
/etc/skel

Umask for Home Directory
022

Default Expiration Date

Days after Password Expiration Login Is Usable
-1

Figure 21. SUSE Linux's YaST Control Center -> User and Group Administration -> Default for New Users screen

User/Group Administration in the Enterprise

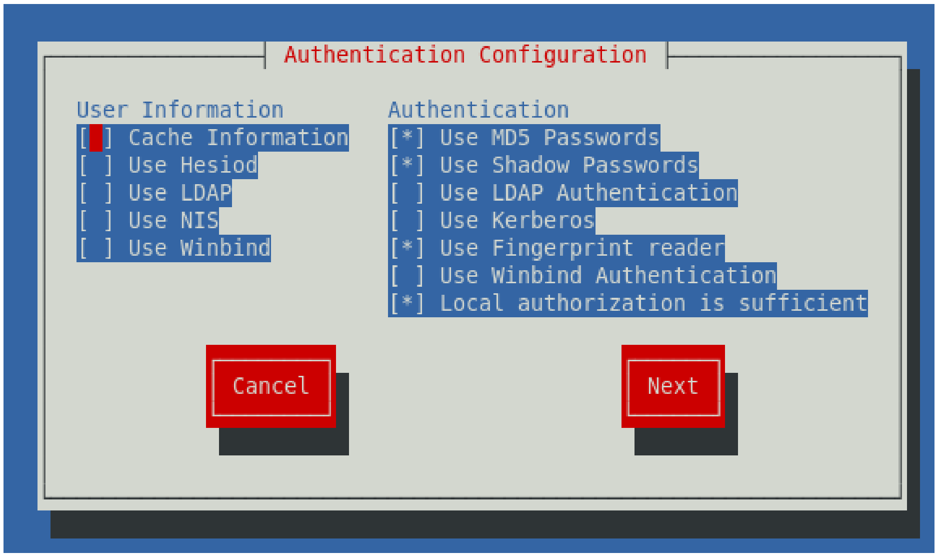
User and group account information is often centralized. Centralized information can be retrieved with

- Lightweight Directory Access Protocol (LDAP)
- Network Information Service (NIS)

User home directories can also be centralized and accessed remotely. Remote file systems can be automounted.

With the GUI Interface in Oracle Linux

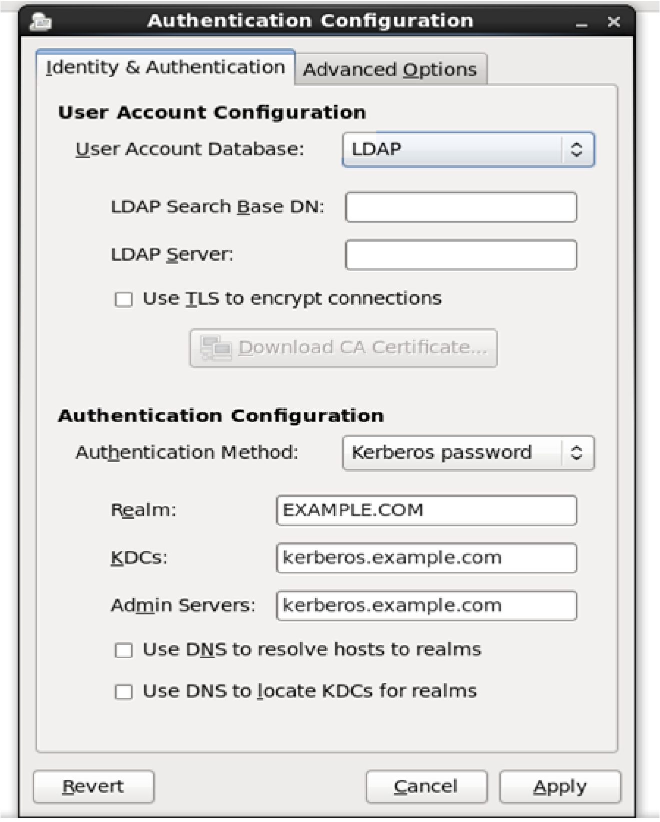
The `authconfig-gtk` or `authconfig-tui` command can be used to configure authentication settings:



```
Authentication Configuration

User Information             Authentication
[ ] Cache Information        [*] Use MD5 Passwords
[ ] Use Hesiod               [*] Use Shadow Passwords
[ ] Use LDAP                 [ ] Use LDAP Authentication
[ ] Use NIS                  [ ] Use Kerberos
[ ] Use Winbind              [*] Use Fingerprint reader
                             [ ] Use Winbind Authentication
                             [*] Local authorization is sufficient
```

Figure 22. Oracle Linux’s Authentication Configuration screen



Authentication Configuration
Identity & Authentication
Advanced Options

User Account Configuration

User Account Database: LDAP

LDAP Search Base DN:

LDAP Server:

□ Use TLS to encrypt connections

Download CA Certificate...

Authentication Configuration

Authentication Method: Kerberos password

Realm: EXAMPLE.COM

KDCs: kerberos.example.com

Admin Servers: kerberos.example.com

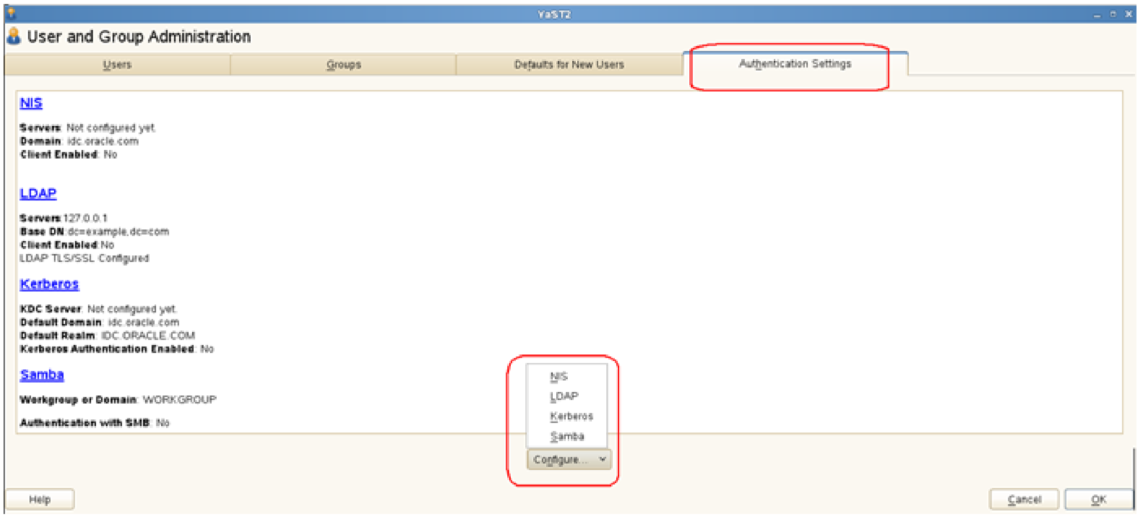
□ Use DNS to resolve hosts to realms

□ Use DNS to locate KDCs for realms

Figure 23. Oracle Linux’s Authentication Configuration -> Identity & Authentication tab

In SUSE Linux

The command-line options for SUSE Linux are the same as in Oracle Linux. In GUI mode, you can use **YaST Control Center** -> **User and Group Administration** -> **Authentication Settings**.



NIS

Servers: Not configured yet.
Domain: idc.oracle.com
Client Enabled: No

LDAP

Servers: 127.0.0.1
Base DN: dc=example,dc=com
Client Enabled: No
LDAP TLS/SSL Configured

Kerberos

KDC Server: Not configured yet.
Default Domain: idc.oracle.com
Default Realm: IDC.ORACLE.COM
Kerberos Authentication Enabled: No

Samba

Workgroup or Domain: WORKGROUP
Authentication with SMB: No

Figure 24. SUSE Linux's YaST Control Center -> User and Group Administration -> Authentication Settings screen

Network Addressing

Introduction to DHCP

DHCP stands for *dynamic host configuration protocol.* A DHCP server dynamically assigns network settings from a server to client machines. In other words, instead of configuring the parameters related to how your computer communicates with a network, this information is automatically provided by a central DHCP server. A client configured for receiving a DHCP-based network address sends out a broadcast request to the DHCP server, which, in turn, issues an IP address and other network parameters as part of the protocol. This is often referred to as an IP address lease.

The DHCP assignment process is as follows:

- Lease request – The client broadcasts a request to the DHCP server with a source address of 0.0.0.0 and a destination address of 255.255.255.255. The request includes the Media Access Control (MAC) address, which is used to direct the reply.
- IP lease offer – The DHCP server replies with an IP address, subnet mask, network gateway, domain name, name servers, lease duration, and its own IP address.
- Lease selection – The client receives an offer and broadcasts that to all the DHCP servers that will accept the given offer, so that other DHCP servers need not make an offer. The DHCP server then sends an acknowledgement to the client. The client is configured to use TCP/IP.

- Lease renewal – When half of the lease time has expired, the client issues a new request to the DHCP server.

Both Oracle Linux and SUSE Linux come bundled with a DHCP server that can be quickly set up to provide IP addresses and other network-address-related parameters to client machines.

- Client machines automatically obtain network configuration information from a DHCP server.
- The client "leases" the network information.
  - The terms of the lease are configurable.
  - The lease is renewed automatically by the client while the network is in use.
- The DHCP server can provide static IP addresses.
- DHCP is broadcast-based.
  - Therefore, the client and the server have to be on the same subnet.

Installing a DHCP Server

The DHCP package contains a DHCP server. Installing the package is straightforward. A superuser performs the following steps.

In Oracle Linux

The superuser uses the `#yum install dhcp` command.

In SUSE Linux

Packages can be installed with the Install/Remove Software option or via the YUM command line.

Configuring a DHCP Server

Installing the DHCP package creates a file, **/etc/dhcp/dhcpd.conf**—merely an empty configuration file at this point. This file can be edited to create a fully functional DHCP server that meets your requirements. For example:

```
# cat /etc/dhcp/dhcpd.conf

#

# DHCP Server Configuration file.

# see /usr/share/doc/dhcp*/dhcpd.conf.sample
```

A sample configuration file can be found at /usr/share/doc/dhcp-<version>/dhcpd.conf.sample. You can use this file to help you configure the final **/etc/dhcp/dhcpd.conf** file. This file is explained in detail below. The sample configuration file provided can be used as a starting point, and custom configuration options can be added to it. To copy it to the proper location, use one of the following commands:

In Oracle Linux

```
#cp /usr/share/doc/dhcp-<version-number>/dhcpd.conf.sample
/etc/dhcp/dhcpd.conf
```

In SUSE Linux

```
#cp /usr/share/doc/packages/dhcp-server/examples/simple_dhcpd.conf
/etc/dhcpd.conf
```

To configure a DHCP server, first use the ifconfig utility to verify that a BROADCAST address is specified in your network configuration; initial DHCP requests in IPv4 are broadcast and not sent to a specific server.

Next, edit the **/etc/dhcpd.conf** file. You'll need to configure lease times, optional subnet masks, router addresses, and DNS servers as well as the IP addresses or ranges of addresses of your clients. Leased IP addresses are kept in /var/lib/dhcpd/dhcpd.leases as they are assigned.

See the sample configuration file under /usr/share/doc/dhcp-version/ or the manual page (man 5 dhcpd.conf) when creating your site-specific DHCP server. Here are a couple of samples:

In Oracle Linux

```
# global definitions


ddns-update-style none; # turn off DDNS updates; required option

option domain-name "example.com"; # domain name given to client

option domain-name-servers 192.168.0.254;

default-lease-time 21600; # seconds till expire

max-lease-time 43200; # maximum lease time

subnet 192.168.0.0 netmask 255.255.255.0


{


# definitions in this block applicable only to given net

option routers 192.168.0.253; # local gateway

option subnet-mask 255.255.255.0; # local subnet mask

range 192.168.0.2 192.168.0.250; # Range configuration DHCP

host station1 # static configuration for each host BOOTP
{

hardware ethernet 00:a0:cc:3d:0b:39;

fixed-address 192.168.0.1;

}


}
```

You can use the **/etc/sysconfig/dhcpd** file to configure DHCPD by setting the DHCPDARGS variable. The following parameter would run the DHCPD server on the eth0 interface (usually the first Ethernet card on a Linux machine).

DHCPDARGS="eth0"

A best practice is to always run the dhcpd configtest service after editing **/etc/dhcpd.conf**, because configuration errors can prevent DHCPD from starting. The configtest parameter checks any syntax errors in the file and prints them onscreen. Once everything is OK, you can proceed to start the DHCP server.

In SUSE Linux

DHCP server configuration in SUSE Linux can be done via **YaST Control Center** -> **DHCP Server**.

The following screen shots show how a DHCP server is configured in SUSE Linux.

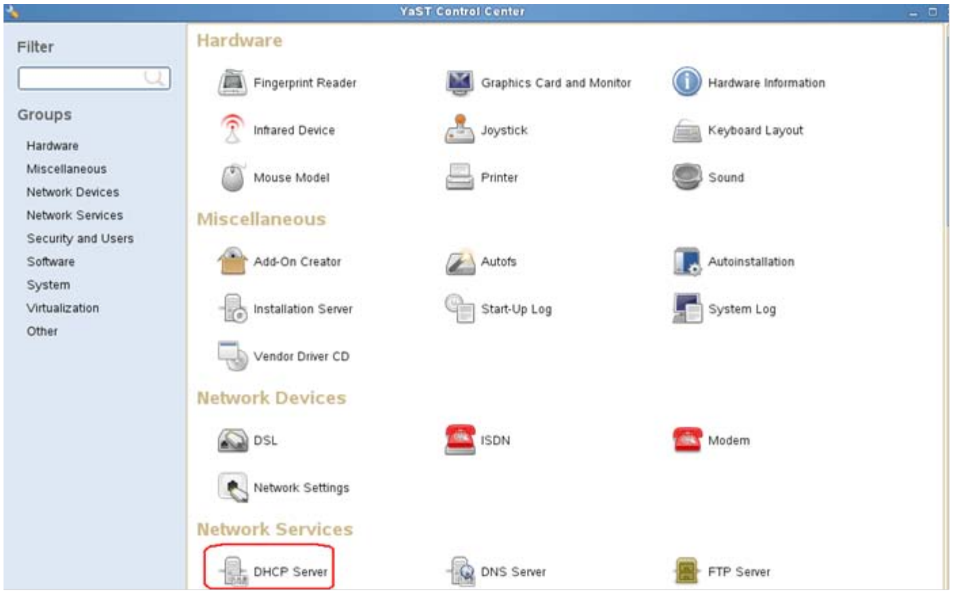
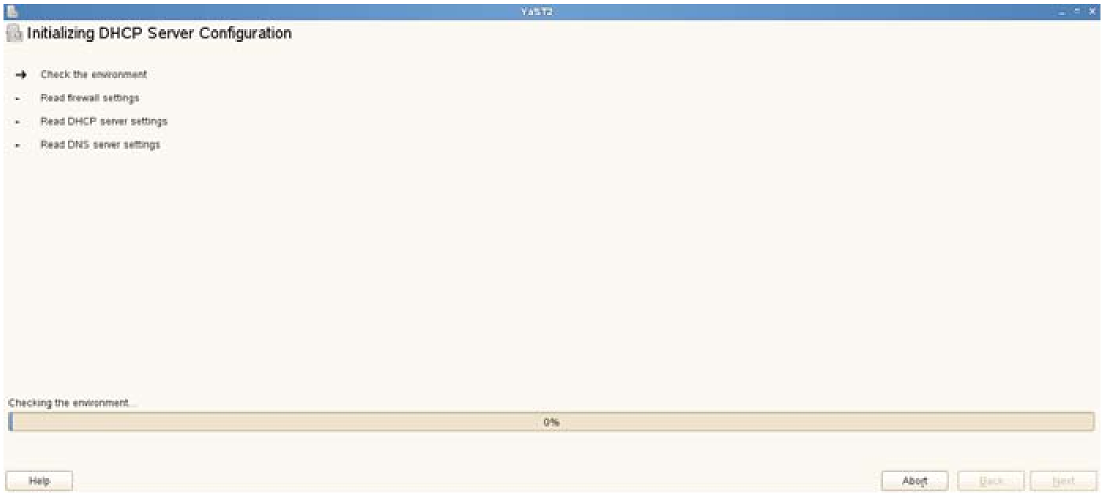


Figure 25. SUSE Linux's YaST Control Center -> DHCP Server screen

1. The DHCP server configuration is initialized, the environment is checked, and the DHCP and DNS server settings are read.



Initializing DHCP Server Configuration

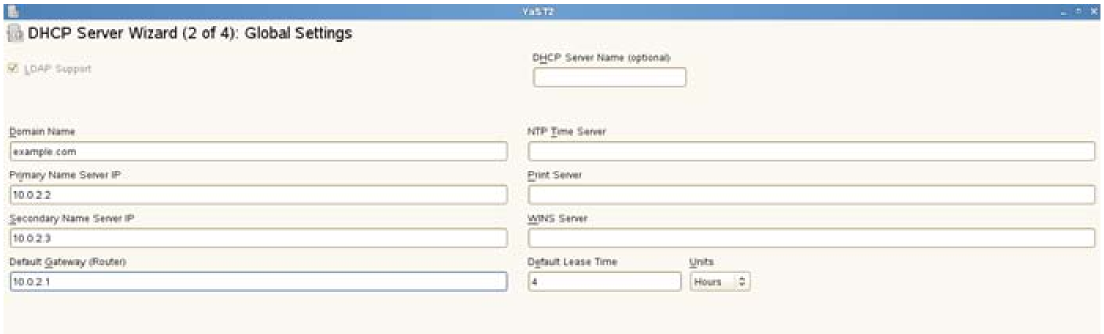
- Check the environment
- Read firewall settings
- Read DHCP server settings
- Read DNS server settings

Checking the environment...

0%

Figure 26.The DHCP server configuration process

2. The DHCP server wizard provides a Global Settings screen.



DHCP Server Wizard (2 of 4): Global Settings

☑ LDAP Support

DHCP Server Name (optional):

Domain Name: example.com

Primary Name Server IP: 10.0.2.2

Secondary Name Server IP: 10.0.2.3

Default Gateway (Router): 10.0.2.1

NTP Time Server:

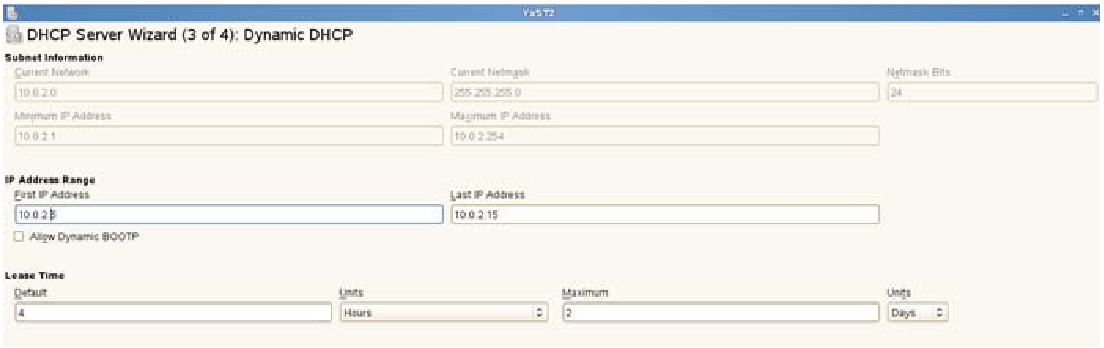
Print Server:

WINS Server:

Default Lease Time: 4 Units: Hours

Figure 27. Step 2 of DHCP server configuration: the Global Settings screen

3. The DHCP server wizard provides a Dynamic DHCP screen.



DHCP Server Wizard (3 of 4): Dynamic DHCP

Subnet Information

Current Network: 10.0.2.0

Current Netmask: 255.255.255.0

Netmask Bits: 24

Minimum IP Address: 10.0.2.1

Maximum IP Address: 10.0.2.254

IP Address Range

First IP Address: 10.0.2.5

Last IP Address: 10.0.2.15

□ Allow Dynamic BOOTP

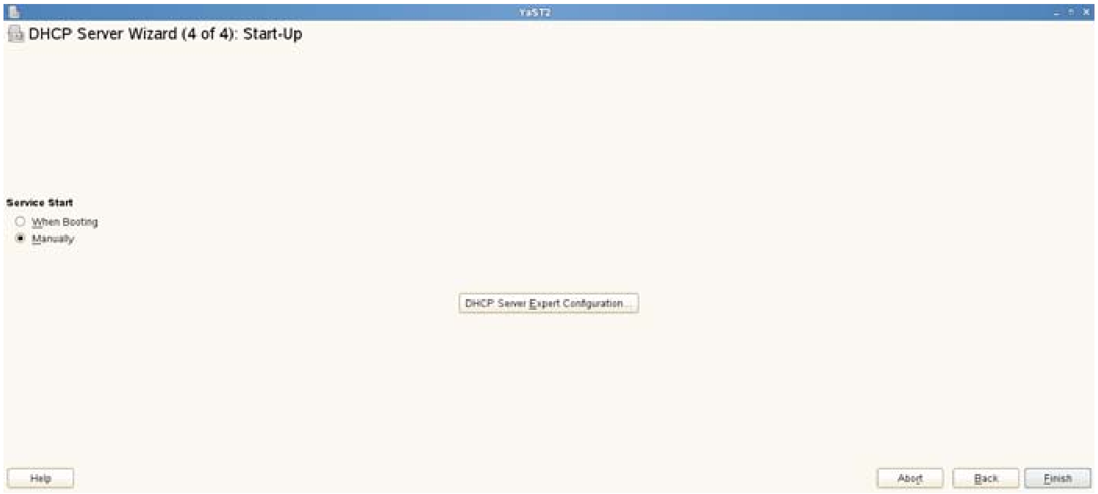
Lease Time

Default: 4 Units: Hours

Maximum: 2 Units: Days

Figure 28. Step 3 of DHCP server configuration: the Dynamic DHCP screen

4. The DHCP server wizard provides a Start-Up screen.



DHCP Server Wizard (4 of 4): Start-Up

Service Start

○ When Booting

● Manually

Figure 29. Step 4 of DHCP server configuration: the Start-Up screen

After executing the above steps, you can refer to the **# /etc/dhcpd.conf** file in SUSE Linux to view/edit the configurations. You can use any text editor or the vi editor to view this file.

Managing a DHCP Server

Starting the service after changing the configuration: After any changes to the configuration file, the DHCP server must be started or restarted (in case it was running previously) for the new changes to take effect. This can be done as follows.

In Oracle Linux

```
# service dhcpd start | stop | restart
```

In SUSE Linux

```
# service dhcpd start | stop | restart

# rcdhcpd start | stop | restart
```

Configuring a DHCP Client

Much like the DHCP server, which runs on the server, there is a DHCP client package that runs on the client machines. The client package is responsible for initiating the network configuration request for the client and contacts and obtains the IP address and other network parameters from the DHCP server on the network. Doing the configuration is easy:

In Oracle Linux

Install the dhclient package, and then

- Set NETWORKING=yes in the **/etc/sysconfig/network** file.
- Set BOOTPROTO=dhcp in the **/etc/sysconfig/network-scripts/ifcfg-<device>** file.
- Optionally, enter any custom configuration information in the DHCP client configuration file, **/etc/dhclient.conf**.
- Run the `dhclient` command to request a lease from the server.

After being configured to use DHCP, this command runs at boot time.

In SUSE Linux

DHCP client configuration in SUSE Linux can be done via **YaST** -> **Network Settings**.

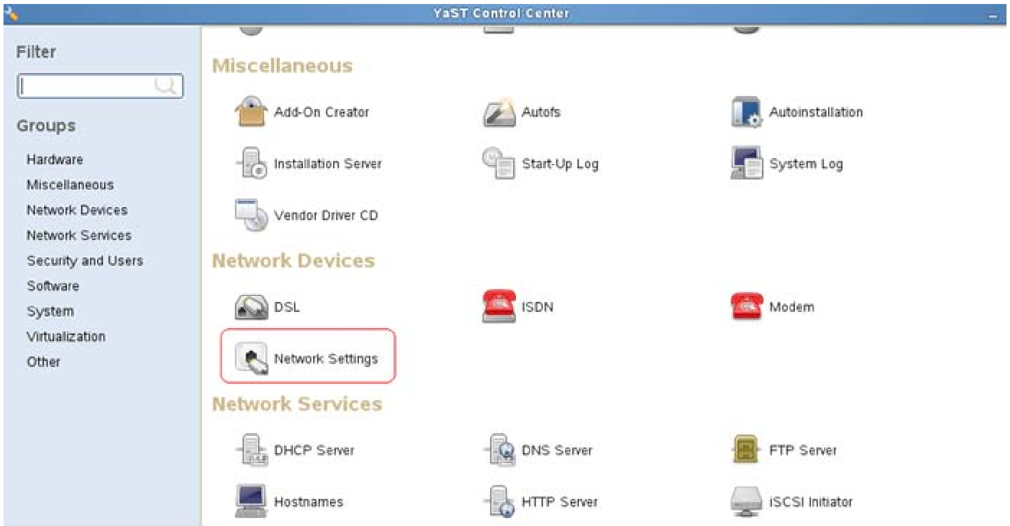
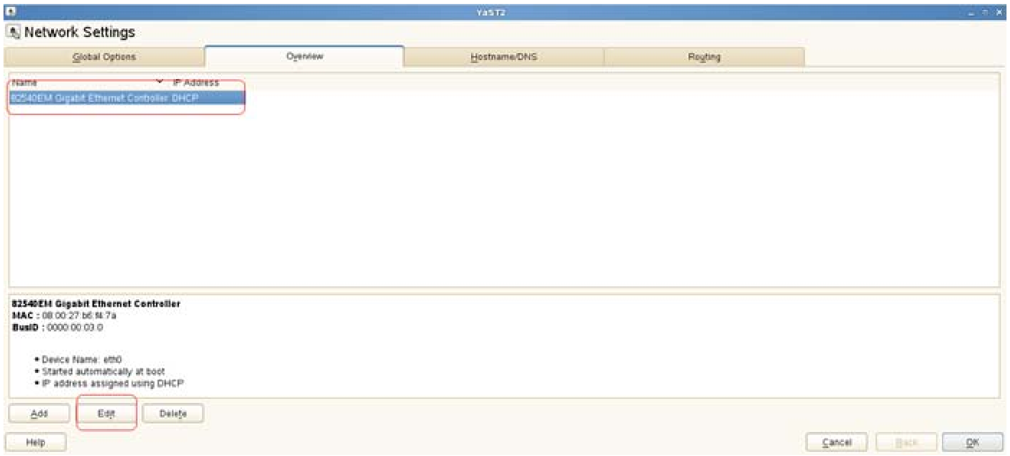


Figure 30. SUSE Linux's YaST Control Center screen with Network Settings selected

Next select **Edit** on the **Network Settings** -> **Overview** tab.



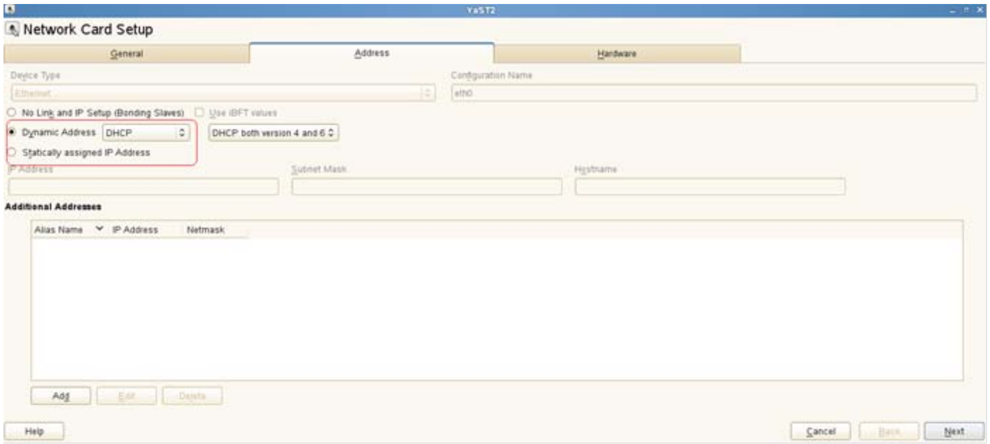
Name	IP Address
82540EM Gigabit Ethernet Controller	DHCP

82540EM Gigabit Ethernet Controller
MAC : 08:00:27:b6:f4:7a
BusID : 0000:00:03.0

- Device Name: eth0
- Started automatically at boot
- IP address assigned using DHCP

Figure 31. SUSE Linux's YaST Control Center -> Network Settings -> Overview screen with Edit selected

Then select the **Address** tab in **Network Card Setup**.



Device Type: Ethernet

Configuration Name: eth0

○ No Link and IP Setup (Bonding Slaves) □ Use iBFT values

● Dynamic Address DHCP | DHCP both version 4 and 6

○ Statically assigned IP Address

IP Address | Subnet Mask | Hostname

Figure 32. SUSE Linux's YaST Control Center -> Network Card Setup -> Address screen

Name Services

Introduction to DNS

The primary purpose of the Domain Name Service (DNS) is to translate hard-to-remember IP addresses into easier-to-remember names. In some cases, it is helpful to reverse the process, so DNS has the ability to translate IP addresses back to names. This was originally done by local files, such as **/etc/hosts**, but over time the files grew too large to be easily maintained. Today's DNS allows for queries of a dispersed, cooperative database network, to ensure that the names and numbers are reasonably synchronized.

Both Oracle Linux and SUSE Linux can be configured as DNS servers.

A typical DNS server is usually used to

- Resolve host names into IP addresses (forward lookup)
- Resolve IP addresses into host names (reverse lookup)
- Enable machines to be logically grouped
- Resolve host name.domain.tld-type domain names
- Resolve host name.subdomain.domain.tld-type domain names

Installing the DNS/BIND Server

Assuming that the YUM repositories are properly set up, you can use the following command as a superuser (root) user to install the DNS server.

```
# yum install bind
```

DNS Server Configuration

Berkeley Internet Name Domain, often called BIND, runs as the “named” daemon and provides forward lookup, reverse lookup, forwarding, and caching services. Features and highlights of the DNS server’s service are covered below.

In Oracle Linux

It runs in a chrooted environment:

```
/var/named/chroot
```

It offers global configuration:

```
/var/named/chroot/etc/named.conf
```

It can act as both a master and a slave server concurrently for different domains:

```
/var/named/chroot/var/named/*.zone

/var/named/chroot/var/named/slaves/*.zone
```

Sample Configurations in named.conf

```
Global options:

       options{

              forwarders { 203.50.0.137; };

              allow-query { 192.168.0.0/24; };

              allow-transfers { 192.168.0.253; };

              };


Master zone:

              zone "example.com" {

              type master;

              file "example.com.zone";

              };


Slave zone:

              zone "kernel.org" {

              type slave;

              masters { 172.100.10.1; };
```

```
            file "slaves/kernel.org.zone";
            };
```

Global Options

Commonly used global options for named.conf are

- Forwarders – The server forwards queries it can't answer to the name server at the IP addresses in this list. If it gets no answer, it will try a root name server unless the forward-only option is set.
- Allow-query – Specifies an address match list of hosts allowed to query this server. If this option is not set, any host can query the server. In the example above, only hosts in the 192.168.0.0/24 subnet may query the DNS server.
- Allow-transfer – Similar to the allow-query directive, the allow-transfer directive specifies hosts that may copy the server's database. It should be used to limit zone transfers to only your configured slave servers.

Zone File

- Begins with $TTL
- Has a semicolon (;) as its comments symbol
- Contains resource records:
  - A – maps name to IP address
  - PTR – maps IP address to name
  - CNAME – creates an alias
  - MX – provides mail exchange record
- FQDNs must end with a dot.

All zone files start with a TTL directive. This determines the default length of time (in seconds) for which a name server may cache the resource records. In certain advanced applications, this can be overridden on the individual resource records.

You can abbreviate names that appear in resource records by specifying only the host name. In such cases, the name inherits the domain from the $ORIGIN variable, which is assigned by the corresponding zone directive in the named.conf. You can fully qualify a host name by ending it with a dot.

Another abbreviation that can be used in a zone file is the @ symbol, which indicates that the record references the machine hosting the named process. It tells BIND if it is referencing its own machine.

Examples of Resource Records

```
@                    IN    NS     ns1.example.com.
example.com          IN    NS     ns2.example.com.
ns1.example.com.     IN    A      192.100.100.1 ; NS needs an A record
ns2                  IN    A      192.100.100.2 ; FQDNs aren’t required
mail                 IN    A      192.100.100.3
pop                  IN    CNAME mail ; alias pop to mail
@                    IN    MX 5   mail.example.com; MX needs an A record
3.100.100.192.IN-ADDR.ARPA.      IN     PTR     mail ; IP address is backwards
```

In SUSE Linux

1. Open **YaST Control Center**, and select **DNS Server**.

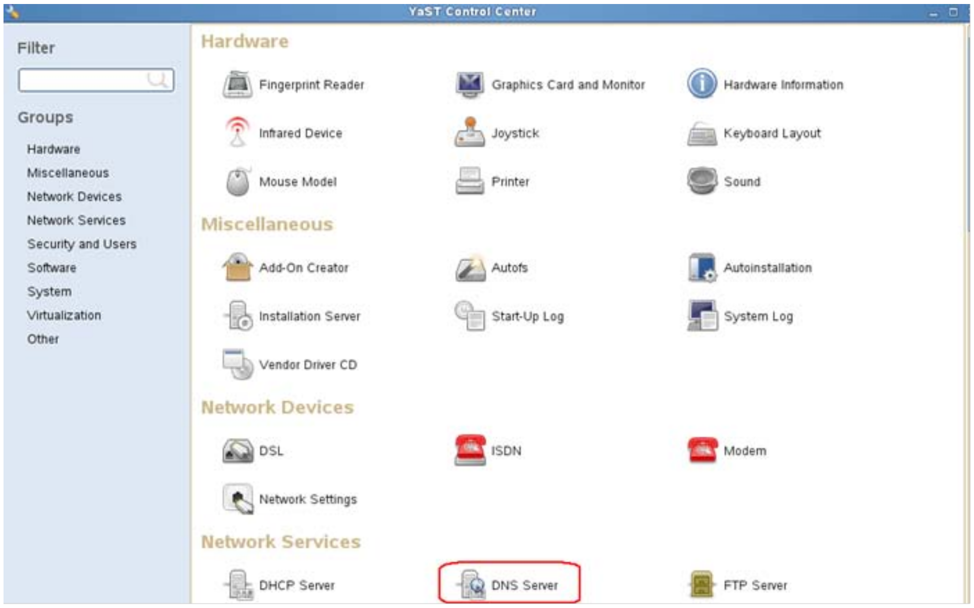
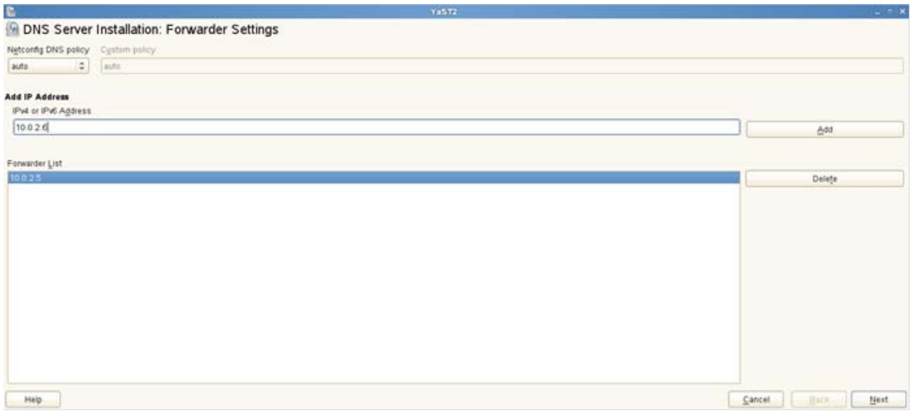


Figure 33. SUSE Linux’s YaST Control Center with DNS Server selected

2. Add an IP address.



DNS Server Installation: Forwarder Settings

Netconfig DNS policy: auto

Custom policy: auto

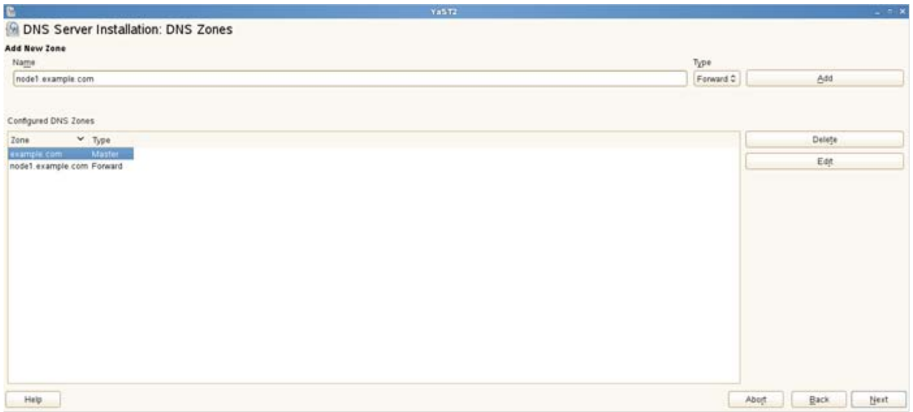
Add IP Address

IPv4 or IPv6 Address: 10.0.2.6

Forwarder List: 10.0.2.5

Figure 34. SUSE Linux's YaST Control Center -> DNS Server Installation: Forwarder Settings screen for adding an address

3. Add a new zone.



DNS Server Installation: DNS Zones

Add New Zone

Name: node1.example.com

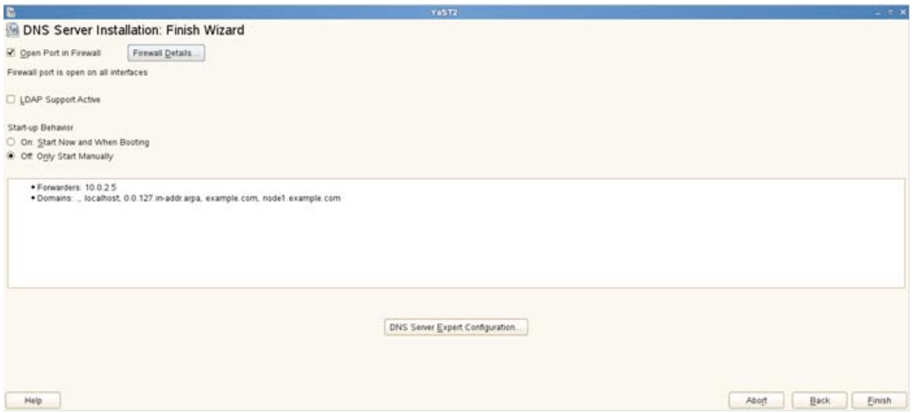
Type: Forward

Configured DNS Zones

Zone	Type
example.com	Master
node1.example.com	Forward

Figure 35. SUSE Linux's YaST Control Center -> DNS Server Installation: DNS Zones screen for adding a new zone

4. Finish.



DNS Server Installation: Finish Wizard

☑ Open Port in Firewall

Firewall port is open on all interfaces

□ LDAP Support Active

Start-up Behavior

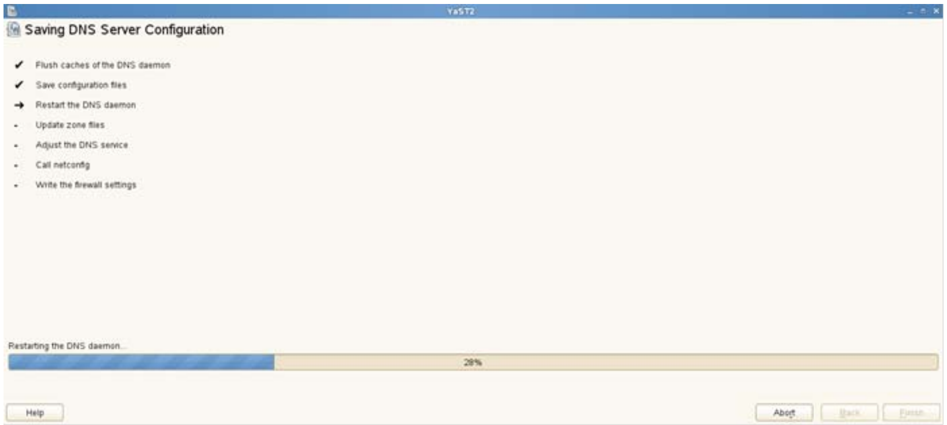
○ On: Start Now and When Booting

● Off: Only Start Manually

- Forwarders: 10.0.2.5
- Domains: ., localhost, 0.0.127.in-addr.arpa, example.com, node1.example.com

Figure 36. SUSE Linux's YaST Control Center -> DNS Server Installation: Finish Wizard screen

5. The DNS server configuration is saved.



Saving DNS Server Configuration

✓ Flush caches of the DNS daemon
✓ Save configuration files
→ Restart the DNS daemon
- Update zone files
- Adjust the DNS service
- Call netconfig
- Write the firewall settings

Restarting the DNS daemon...

28%

Figure 37. SUSE Linux's YaST Control Center -> DNS Server Installation -> Saving DNS Server Configuration screen

Managing the DNS Server

You can manage the DNS server via the Linux command line by using the following commands.

In Oracle Linux

To stop the DNS service:

```
# service named stop
```

To start the DNS service:

```
# service named start
```

In SUSE Linux

To stop the DNS service:

```
# service named stop
```

```
# rcnamed stop
```

To start the DNS service:

```
# rcnamed start
```

The RNDC Utility

The rndc utility is used to prevent unauthorized access to the named daemon. The DNS server uses a shared secret key authentication method to grant privileges to hosts. An identical key is shared between **/etc/named.conf** and the rndc configuration file, **/etc/rndc.conf**. Further, the whole process also runs in a chrooted environment.

- rndc is a command-line administration tool, also called “named,” for the DNS server.
- Use the rndc key to prevent unauthorized access.
  - Generate the rndc key by using the `# rndc-confgen –a` command, which is the same in Oracle Linux and SUSE Linux.
- Configure named to use the key in **/etc/named.conf**.
- Type `rndc` to display usage of the utility and a list of available commands.

The host and dig Utilities

The `host` and `dig` commands are command-line tools for performing DNS lookups. The `host` command has more options; a few important ones are mentioned below for your quick reference.

Examples of Queries Using host

```
# host

# host –a dns.example.com

# host –a host01

# host –a 192.0.2.101
```

Examples of Queries Using dig

```
# dig dns.example.com

# dig –x 192.0.2.101

# dig example.com NS

# dig example.com A
```

The `host` and `dig` commands are the same in Oracle Linux and SUSE Linux.

Web and E-mail Services

Apache HTTP Server

Apache HTTP Server, commonly referred to as Apache Web Server, is developed by the Apache Software Foundation. It supports a variety of features, many implemented as compiled modules that extend the core functionality.

Virtual hosting enables one Apache HTTP Server installation to serve many different actual Websites. For example, one machine with one Apache HTTP Server installation could simultaneously serve www.example.com, www.example.org, test47.test-server.example.edu, and more.

Apache HTTP Server features configurable error messages, DBMS-based authentication databases, and content negotiation. It is also supported by several GUIs. It supports password authentication and digital certificate authentication. Apache HTTP Server also has a built-in search engine and an HTML authorizing tool and even supports FTP.

Apache HTTP Server comes bundled with Oracle Linux, and by default it operates on port 80/tcp, although this is configurable, and if the mod_ssl module has been loaded, the server will also listen on port 443/tcp (Secure HTTP).

Apache HTTP Server can be installed on both Oracle Linux and SUSE Linux in similar ways.

In Oracle Linux

Assuming that the YUM repositories are properly set up, you can use the following command as a superuser (root) user to install the Apache server:

```
# yum install httpd
```

Start the HTTP daemon:

```
# service httpd start
```

The main configuration file is

/etc/httpd/conf/httpd.conf

The auxiliary configuration directory is

/etc/httpd/conf.d

Check for configuration errors:

```
# service httpd configtest
```

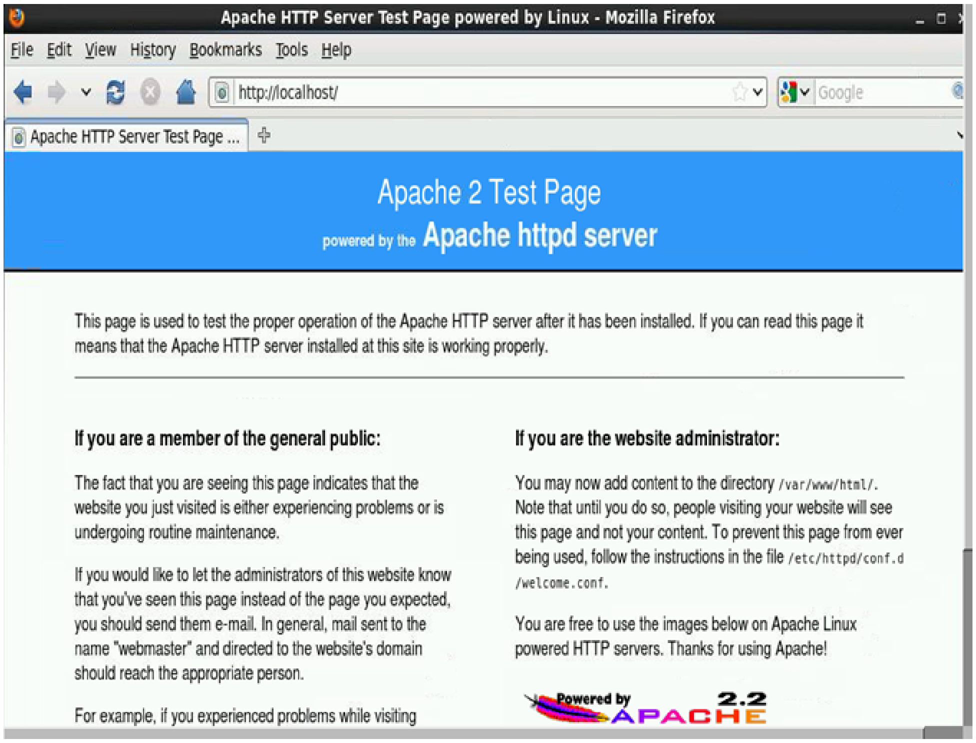
Configuring Apache

Examples of configuration directives in the configuration file:

- Listen 192.168.2.1:8080
- ServerName www.example.com:80
- ServerRoot /etc/httpd
- DocumentRoot /var/www/html
- UserDir enabled oracle
- ErrorLog logs/error_log
- LoadModule auth_basic_module modules/mod_auth_basic.so
- Order deny,allow
- Deny from all

- Allow from .example.com
- Timeout 60

Testing the Apache HTTP Server


Apache HTTP Server Test Page powered by Linux - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost/
Google
Apache HTTP Server Test Page ...

Apache 2 Test Page
powered by the Apache httpd server

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page it means that the Apache HTTP server installed at this site is working properly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting

If you are the website administrator:

You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

You are free to use the images below on Apache Linux powered HTTP servers. Thanks for using Apache!

Figure 38. Apache 2 Test Page screen

Apache Containers

Containers are special directives that group other directives.

- <Directory directory-path>
  - Applies directives to directories within *directory-path*
- <IfModule *module-name*>
  - Applies directives if *module-name* is loaded
- <Limit *method*>
  - Limits access control directives to specified methods

Containers can be nested.

Apache Virtual Hosts

A single Apache server can respond to requests directed to multiple IP addresses or host names.

Each virtual host can provide different content and be configured differently.

Use the <VirtualHost *host-name*> container:

```
<VirtualHost www.example1.com>

       ServerName www.example1.com

       DocumentRoot /var/www/example1

       ErrorLog example1.error_log

</VirtualHost>

<VirtualHost www.example2.com>

       ...

</VirtualHost>
```

E-mail Program Classifications

Often referred to as simply a “mail server,” an e-mail server is a computer within your network that works as your virtual post office. A mail server usually consists of a storage area where e-mail is stored for local users, a set of user definable rules that determine how the mail server should reach the destination of a specific message, a database of user accounts the mail server recognizes and will deal with locally, and communications modules that are the components that actually handle the transfer of messages to and from other mail servers and e-mail clients.

Sendmail and Postfix are two mail transfer agents (MTAs) that are available with both Oracle Linux and SUSE Linux. By default, the MTA servers listen on port 25/tcp, so only one of the MTA servers should be run at one time unless the listening ports for both are differently configured. The components of an e-mail system can be broadly classified as follows:

- Mail user agent (MUA)
  - This is an e-mail client application for creating and reading e-mail messages.
  - Some MUAs are capable of sending outbound messages directly to the MTA.
  - Some MUAs are capable of retrieving messages from remote servers using POP or IMAP.
- Mail transfer agent (MTA)
  - This is an e-mail server that transports e-mail messages by using the SMTP protocol.
  - Examples are Sendmail and Postfix.
- Mail delivery agent (MDA)
  - This is invoked by the MTA.

- It delivers incoming e-mail into the recipient's mailbox file.
- Examples are procmail and mail.

E-mail Protocols

- Simple Mail Transfer Protocol (SMTP)
    - This is the transport protocol used by the MTA to transport mail over the internet.
    - The standard port is defined as port 25/tcp.
- Post Office Protocol (POP)
    - This is an e-mail access protocol.
    - It is used by client programs to retrieve e-mail messages.
- Internet Message Access Protocol (IMAP)
    - This is similar to POP.
    - E-mail is kept on the server when IMAP is being used, whereas it is downloaded on the client in case of POP.
- POP and IMAP services are provided by the Dovecot package.

Postfix SMTP Server

The default MTA with Oracle Linux, the Postfix SMTP server is available for SUSE Linux as well.

- The main configuration files are in the /etc/postfix directory.
    - access – specifies which hosts can connect to Postfix
    - main.cf – the global Postfix configuration file
    - master.cf – specifies how Postfix processes interact
    - transport – maps e-mail addresses to relay hosts
- Use this command to restart the service:
    - `# service postfix restart`
- After making any configuration changes, use this command.
    - `#service postfix reload`

Refer to www.postfix.org for complete documentation.

Sendmail SMTP Server

An MTA included with Oracle Linux and available for SUSE Linux as well, Sendmail is one of the oldest and most common MTAs on the internet. To use it in Oracle Linux or SUSE Linux, do the following:

- Install two packages:
  - `# yum install sendmail sendmail-cf`
- Use configuration files located in /etc/mail :
  - **sendmail.mc** – is the main configuration file
  - **access** – specifies a relay host
  - **virtusertable** – serves e-mail to multiple domains
  - **mailertable** – forwards e-mail from one domain to another
- Regenerate the configuration files after editing:
  - `# service sendmail restart`
  - `# make all –C /etc/mail`

Configuring Sendmail on a Client

Sendmail on a client system simply relays outbound mail to an SMTP server. A remote SMTP server, typically an ISP, relays e-mail to its destination.

Configuration of Sendmail is same for both Oracle Linux and SUSE Linux and can be accomplished with the following steps:

- Edit the following line in **/etc/mail/sendmail.mc**:
  - `dnl define('SMART_host', 'smtp.your.provider')dnl`

removing the dnl at the beginning of the line and including the ISP’s SMTP server name:

- `define('SMART_host', 'smtp.isp.com')dnl`

- Restart the Sendmail service:
  - `# service sendmail restart`

SELinux

Security-Enhanced Linux (SELinux) is an implementation of a mandatory access control mechanism in the Linux kernel, checking for allowed operations after standard discretionary access controls are checked. It was created by the National Security Agency and can enforce rules on files and processes in a Linux system, and on their actions, based on defined policy.

SELinux is a security enhancement to Linux that gives users and administrators more control over which users and applications can access which resources, such as files. Standard Linux access controls, such as file modes (-rwxr-xr-x) are modifiable by the user and by applications the user runs, whereas SELinux access controls are determined by a policy loaded on the system and not changeable by careless users or misbehaving applications.

Benefits of Running SELinux

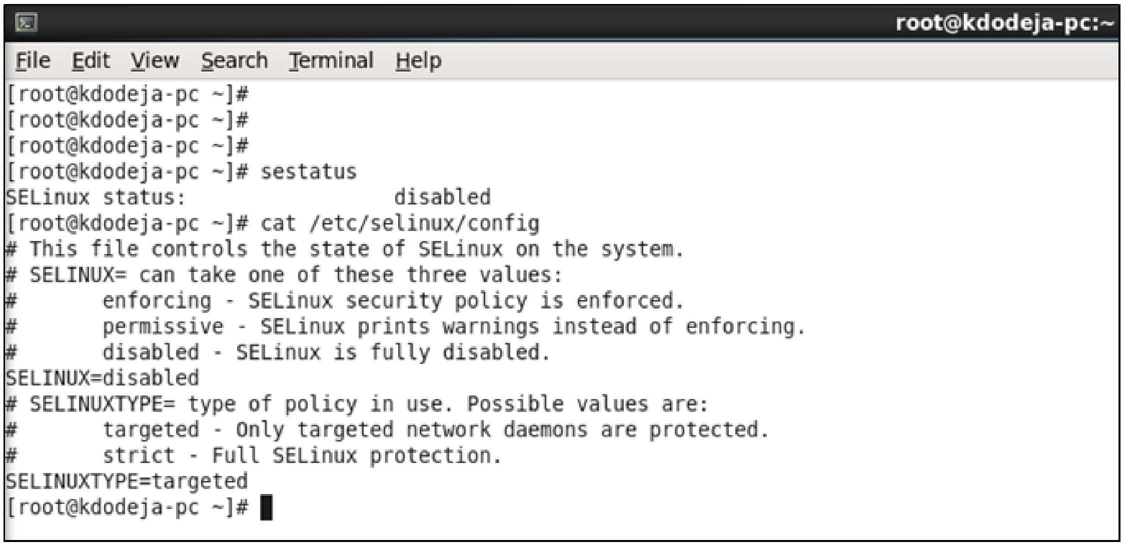
All processes and files are labeled with a type. A type defines a domain for both processes as well as files. You can separate processes from each other by running them in their own individual domains, and SELinux policy rules define how processes interact with files as well as with each other. Access is allowed only if an SELinux policy rule exists that specifically allows it:

- SELinux enables fine-grained access control. Stepping beyond traditional UNIX permissions that are controlled at a user's discretion and based on Linux user and group IDs, SELinux access decisions are based on all available information, such as an SELinux user; role; type; and, optionally, level.
- SELinux policy is administratively defined, enforced systemwide, and not set at a user's discretion.
- SELinux reduces vulnerability to privilege escalation attacks.
  - Because processes run in domains and are therefore separated from each other and because SELinux policy rules define how processes access files and other processes, the attacker in the case of a process compromise has access only to the normal functions of that process and to files the process has been configured to have access to. For example, if the Apache HTTP Server is compromised, an attacker cannot use that process to read files in user home directories unless a specific SELinux policy rule was added or configured to allow such access.
- SELinux can be used to enforce rules, but it is not
  - Antivirus software
  - A replacement for passwords, firewalls, or other security systems
  - An all-in-one security solution

SELinux is designed to enhance existing security solutions, not replace them. Even when you are running SELinux, it is important to continue to follow good security practices, such as keeping software up to date and using firewalls and hard-to-guess passwords.

SELinux comes bundled with Oracle Linux. Examine the detailed SELinux documentation to learn about its implementation of policies and contexts.

Figure 39 shows how SELinux's status can be checked with the `sestatus` command and how the **/etc/selinux/config** configuration file can be edited to change the status of SELinux on a running system. The changes to the policy don't take effect until after a reboot of the system.



```
[root@kdodeja-pc ~]#
[root@kdodeja-pc ~]#
[root@kdodeja-pc ~]#
[root@kdodeja-pc ~]# sestatus
SELinux status:                 disabled
[root@kdodeja-pc ~]# cat /etc/selinux/config
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - SELinux is fully disabled.
SELINUX=disabled
# SELINUXTYPE= type of policy in use. Possible values are:
#       targeted - Only targeted network daemons are protected.
#       strict - Full SELinux protection.
SELINUXTYPE=targeted
[root@kdodeja-pc ~]# 
```

Figure 39. SELinux status check with the sestatus command

For details on the SELinux program, see *Security-Enhanced Linux User Guide*.

File System Management

On a Linux system, everything is a file; if something is not a file, it is a process.

A file system is an abstraction for storing, retrieving, and updating a set of files. The file system manages access to the data and the metadata of the files and manages the available space of the device(s) that contain it. Ensuring reliability is a major responsibility of a file system, which organizes data in an efficient manner and can be tuned to the characteristics of the backing device.

Linux comes bundled with many file systems, such as ext2, ext3, resiserfs, ocfs2(cluster filesystem), and gfs. File system management includes creating and modifying partitions and creating, mounting, and unmounting file systems. For creation, configuration, and management of these file systems, various tools and packages come bundled with the operating system.

Commands that system administrators usually use for this purpose are `fdisk`, `mount`, `mkfs`, and `umount`. These commands are available in both the Oracle Linux and the SUSE Linux operating systems, and their usage is the same.

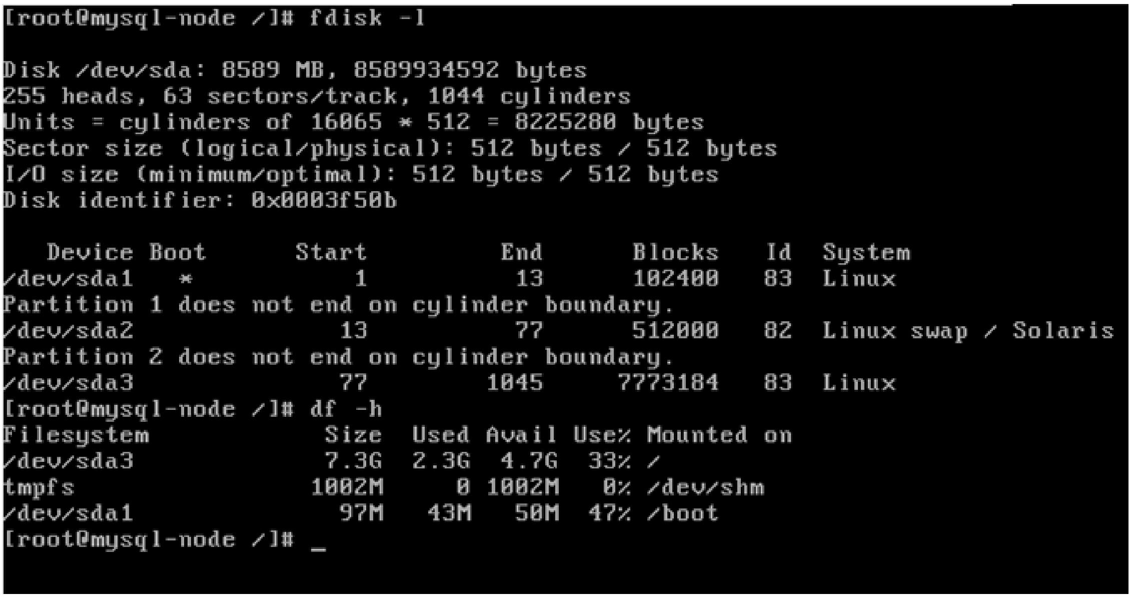
Enabling persistent mounting of file systems across server reboots involves using the **fstab** file, which is located in the same place in both operating systems: /etc/fstab.

In Oracle Linux

These three partitions are created during installation (if the user does not choose a custom layout) in Oracle Linux:

1.	/boot	Linux Type
2.	Swap	Linux Swap/Solaris Type
3.	/	Linux Type

This is the default partition scheme:



```
[root@mysql-node /]# fdisk -l

Disk /dev/sda: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x0003f50b

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1          13      102400   83  Linux
Partition 1 does not end on cylinder boundary.
/dev/sda2              13          77      512000   82  Linux swap / Solaris
Partition 2 does not end on cylinder boundary.
/dev/sda3              77        1045     7773184   83  Linux
[root@mysql-node /]# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda3             7.3G  2.3G  4.7G  33% /
tmpfs                1002M     0 1002M   0% /dev/shm
/dev/sda1              97M   43M   50M  47% /boot
[root@mysql-node /]# _
```

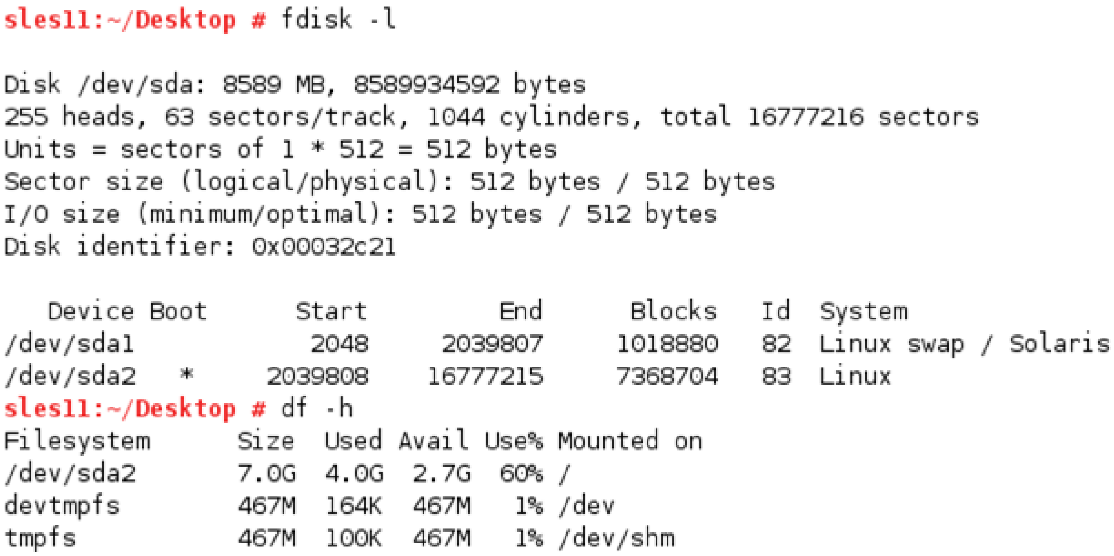
Figure 40. The default partition scheme in Oracle Linux

In SUSE Linux

These two partitions are created during installation (if the user does not choose a custom layout) in SUSE Linux:

1.	/	Linux Type
2.	Swap	Linux Swap/Solaris Type

This is the default partition scheme in SUSE Linux:



```
sles11:~/Desktop # fdisk -l

Disk /dev/sda: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 cylinders, total 16777216 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00032c21

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1            2048     2039807     1018880   82  Linux swap / Solaris
/dev/sda2   *     2039808    16777215     7368704   83  Linux
sles11:~/Desktop # df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda2       7.0G  4.0G  2.7G  60% /
devtmpfs        467M  164K  467M   1% /dev
tmpfs           467M  100K  467M   1% /dev/shm
```

Figure 41. The default partition scheme in SUSE Linux

Managing File Systems

The following sections outline the steps required to create and manage partitions and file systems, including

- Creating partitions
- Creating and mounting a file system
- Unmounting a file system

Creating Partitions

You use the `fdisk` command to create partitions as well as to do the following:

- View and manage partition tables
- List a partition table from the command line
  - `#fdisk -l`
- Manage a partition table from an interactive interface
  - `#fdisk /dev/sda`
- Use `partprobe`
- Use `#cat /proc/partitions`

Making File Systems

The default file systems available in Oracle Linux and SUSE Linux are ext3 and ext4. SUSE Linux also bundles the reiserfs file with the operating system. File systems need to be initialized before they can be used. Linux provides file system management utilities for formatting and tuning the files systems. The mkfs and mke2fs command line utility with the appropriate suffix (as shown below) can be used to quickly format and prepare a file system for use.

- `mkfs`
- `mkfs.ext2`, `mkfs.ext3`, `mkfs.msdos`, `mkfs.vfat`, `mkfs.reiserfs`
- `mke2fs [options] device`

Labeling and Mounting File Systems

File systems can be labeled and mounted.

- Alternative way to refer to devices
- Device-independent
  - `#e2label special_dev_file [fslabel]`
  - `#mount [options] LABEL=fslabel mount_point`
- `blkid` shows the labels and file system type of all devices.

Mount Points and /etc/fstab

File systems that have been created in the previous step need to be mounted before they can be used. This is usually done in the /etc/fstab file. This file lists all the available file systems that the system has access to, along with the type and options available for each of the file system. The /etc/fstab file also provides information that is used by the boot up process to correctly identify and mount file systems. Various disk utilities and other programs that manipulate file systems also rely on the information provided in the /etc/fstab file for their correct functioning. Broadly speaking the /etc/fstab file provides the following functions / details:

- Configuration of the file system hierarchy
- Information required by mount, fsck, and other programs
- Maintenance of the hierarchy between system reboots
- Use of file system volume labels in the device field
- The `mount -a` command can be used to mount all file systems listed in /etc/fstab.

Unmounting File Systems

Use the `#umount [options] device | mount_point` command to unmount file systems.

- You cannot unmount a file system that is in use.
- Use `fuser` to check and/or kill processes.
- Use the remount option to change a mounted file system's options automatically.
  - `#mount -o remount,ro /data`

Conclusion

This document has endeavored to help you understand the differences as well the similarities between Oracle Linux and SUSE Linux Enterprise Server. You have surely noticed that under the hood, both systems are largely the same. The same commands are available on the command line in both operating systems, and they also perform the same tasks. Both operating systems have some GUI-based system management tools as well. For Oracle Linux, the GUI tools are task-specific, whereas in SUSE Linux, there is a single tool called YaST2 that can help system administrators perform their tasks. It should be a fairly simple process for an experienced system administrator to configure and manage an Oracle Linux system, because the underlying file system, commands, and various services such as Web and e-mail all remain the same. Configuring a Postfix instance on Oracle Linux is no different than configuring it on SUSE Linux. This similarity makes it very easy for a SUSE Linux system administrator to quickly get up to speed when managing Oracle Linux servers.

Oracle is committed to developing practices and products that help protect the environment

SUSE Linux to Oracle Linux:
Guide for System Administrators
January 2013

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

Hardware and Software, Engineered to Work Together