

# **AutoYaST**

## **Automatic Linux Installation and Configuration with YaST2**

**SUSE Linux AG**

**Anas Nashif, *SuSE* Linux AG**

---

# **AutoYaST: Automatic Linux Installation and Configuration with YaST2**

SUSE Linux AG

by Anas Nashif

Revision History

Revision \$Revision: 1.1.6.7 \$      \$Date: 2004/10/19 17:40:47 \$

Various fixes and additions including more information about classes and rules.

Revision 1.1.6.6                      2004/06/13 01:00:16

Re-added Network installation and Installation server documentation.

Revision 1.1.6.5                      2004/06/09 17:57:30

Added section about 'netsetup'

Revision 1.1.6.4                      2004/05/24 19:09:22

Fixed for PDF output

Copyright © 2004 *SuSE* Linux AG

---

---

---

---

# Table of Contents

1. Introduction .....	1
1. Availability .....	1
2. Motivation .....	1
3. Overview and Concept .....	2
2. The Control File .....	4
1. Introduction .....	4
2. Format .....	4
3. Structure .....	5
3.1. Resources and Properties .....	5
3.2. Nested Resources .....	6
3.3. Attributes .....	7
4. The XML Document Type Definition (DTD) .....	7
4.1. Introduction .....	7
4.2. Example DTD .....	7
3. Creating A Control File .....	9
1. Collect information .....	9
2. Using the Configuration Management System .....	9
2.1. Creating a new Profile .....	10
2.2. Import of Legacy and Foreign Configuration Files .....	10
3. Creating/Editing a Control File Manually .....	10
4. Configuration and Installation Options .....	12
1. General Options .....	12
2. Reporting .....	13
3. The Boot loader .....	13
4. Partitioning .....	15
4.1. Automated Partitioning .....	15
4.2. Advanced Partitioning features .....	17
4.3. Using existing mount table (fstab) .....	22
4.4. Logical Volume Manager (LVM) .....	22
4.5. Software RAID .....	24
5. Software .....	26
5.1. Package Selections .....	26
5.2. Custom Package Selections .....	27
5.3. Installing additional and customized Packages .....	28
5.4. Kernel packages .....	28
5.5. Removing automatically selected packages .....	29
6. Services and Run-levels .....	29
7. Network configuration .....	30
7.1. Network devices, DNS and Routing. ....	30
7.2. Proxy .....	31
7.3. (X)Inetd .....	31
7.4. NIS .....	32
7.5. LDAP client .....	33
7.6. NFS Client and Server .....	33
7.7. NTP Client .....	34
8. Mail Configuration (Sendmail or Postfix) .....	34
9. Security settings .....	35
9.1. Password Settings Options .....	36
9.2. Boot Settings .....	36
9.3. Login Settings .....	37
9.4. New user settings (useradd settings) .....	37
10. Monitor and X11 Configuration .....	37
11. Users .....	37

---

12. Custom user scripts .....	38
13. System variables (Sysconfig) .....	40
14. Adding complete configurations .....	41
15. Miscellaneous hardware and system components .....	42
15.1. Printer .....	42
15.2. Sound devices .....	43
5. Network Based Installation .....	44
1. Boot Server .....	44
1.1. Introduction .....	44
1.2. Required Services on the Boot Server .....	45
1.3. Boot Server Configuration .....	46
2. Installation Server .....	51
2.1. SUSE Linux .....	51
2.2. SUSE Linux Enterprise Server .....	52
3. Configuration Server .....	59
3.1. HTTP Repository .....	59
3.2. NFS Repository .....	59
3.3. TFTP Repository .....	59
6. Rules and Classes .....	61
1. Rule based auto-installation .....	61
1.1. Rules File explained .....	62
1.2. Rules file structure .....	64
1.3. Predefined System Attributes .....	64
1.4. Rule Matching .....	65
1.5. Using Operators .....	65
2. Classes .....	65
2.1. Creating Class files and Directories .....	66
2.2. Using Classes During Installation .....	67
3. Mixing Rules and Classes .....	67
7. The Auto-Installation Process .....	68
1. Introduction .....	68
1.1. X11 Interface .....	68
1.2. Serial console .....	68
1.3. Text based YaST2-Installation .....	68
2. Choosing the right Boot Medium .....	68
2.1. Booting from a floppy .....	68
2.2. Booting from CD-ROM .....	69
3. Invoking the Auto-Installation process .....	69
3.1. Command line Options .....	69
3.2. Auto-installing a Single System .....	72
3.3. Combining linuxrc info file with YaST2 control file .....	73
4. System Configuration .....	73
4.1. Post-Install and System Configuration .....	73
4.2. System Customization .....	74
8. Legacy and foreign Configuration formats .....	75
1. Migration from YaST1 and ALICE .....	75
1.1. ALICE modules .....	75
1.2. Other configuration options with YaST2 and ALICE .....	76
2. Redhat Kickstart .....	76
2.1. Software selections and packages .....	76
2.2. User scripts .....	76
A. Handling Rules .....	77
B. Advanced Linuxrc Options .....	79
1. Passing parameters to Linuxrc .....	79
2. 'info' file format .....	79
3. Advanced Network Setup .....	81

---

---

## List of Figures

1.1. Auto-installation process .....	3
3.1. Configuration System .....	9
3.2. Editing the control file with kxmledit .....	11
4.1. Keeping partitions .....	20
6.1. Rules .....	61
6.2. Defining Classes .....	66
A.1. Rules Retrieval Process .....	77

---

## List of Tables

6.1. System Attributes .....	64
7.1. Keywords for linuxrc .....	69
7.2. Command line variables for AutoYaST .....	70
8.1. ALICE vs. YaST2 modules .....	75
B.1. Advanced linuxrc keywords .....	79

---

## List of Examples

2.1. XML Control File (Profile)	4
2.2. Control file container	5
2.3. Nested Resources	6
2.4. Nested Resources with type attributes	6
2.5. Example DTD	7
4.1. General Options	12
4.2. Reporting Behavior	13
4.3. Bootloader configuration	14
4.4. Serial console configuration with GRUB	14
4.5. Bootloader configuration for PPC	15
4.6. Automated partitioning	16
4.7. Detailed automated partitioning	17
4.8. Mount Options	18
4.9. Advanced Automated partitioning	18
4.10. Creating custom extended partitions	19
4.11. Keeping partitions	20
4.12. Auto-detection of partitions to be kept.	21
4.13. Reading existing /etc/fstab	22
4.14. Create LVM Physical Volume	22
4.15. LVM Logical Volumes (Old syntax)	23
4.16. LVM Logical Volumes (New syntax)	23
4.17. RAID1 configuration (Old Syntax)	25
4.18. RAID1 configuration (New Syntax)	25
4.19. Package selection in control file	26
4.20. Customized Package selection	27
4.21. Package selection file	28
4.22. Creating package database	28
4.23. Package selection in control file	29
4.24. Package selection in control file	29
4.25. Run-level Configuration	30
4.26. Network configuration	30
4.27. Network configuration: Proxy	31
4.28. Inetd Example	32
4.29. Network configuration: NIS	32
4.30. Network configuration: LDAP client	33
4.31. Network configuration: NFS client	33
4.32. Network configuration: NFS Server	33
4.33. Network configuration: NTP Client	34
4.34. Mail Configuration	34
4.35. Security configuration	36
4.36. X11 and Monitor configuration	37
4.37. User configuration	37
4.38. Post script configuration	39
4.39. Sysconfig Configuration	40
4.40. Dumping files into the installed system	41
4.41. Dumping files into the installed system	41
4.42. Printer configuration	42
4.43. Sound configuration	43
5.1. Tftboot directory contents	45
5.2. /etc/dhcpd.conf with the root-path option	46
5.3. DHCP server configuration with PXE and Etherboot options	46
5.4. Configuration file for PXELINUX net boot	47
5.5. Configuration file for PXELINUX local boot	47

5.6. PXELINUX Configuration .....	47
5.7. Etherboot with kernel command line options via DHCP .....	48
5.8. GRUB menu.lst .....	49
5.9. Grub image via DHCP .....	50
5.10. media directory .....	54
5.11. The contents file .....	54
6.1. Simple rules file .....	62
6.2. Simple rules file .....	63
6.3. Classes .....	67
7.1. Determine HEX code for an IP address .....	72
7.2. Linxurc options in the control file .....	73

---

# Chapter 1. Introduction

AutoYaST is a system for installing one or more SuSE Linux systems automatically and without user intervention. AutoYaST installations are performed using a control file with installation and configuration data. The control file can be created using the configuration interface of AutoYaST and can be provided to YaST2 during installation in different ways.

## 1. Availability

AutoYaST is available with recent *SuSE* products starting from *SuSE Linux 8.0* and business products starting from *SLES 8*.

Products prior to SuSE Linux 8.0 and business products based on *SLES 7* have an auto-installation system relying on *YaST*. A configuration management system is provided by *Alice* for these products.

### Updated documentation

Updated documentation can always be found at the following URL: <http://www.suse.de/~nashif/autoinstall/> [<http://www.suse.de/~nashif/autoinstallation/>]

## 2. Motivation

The Linux Journal [<http://www.linuxjournal.com/>], in an article in issue 78 [<http://www.linuxjournal.com/categories.php?op=newindex&catid=178>] writes:

“ A standard Linux installation asks many questions about what to install, what hardware to configure, how to configure the network interface, etc. Answering these questions once is informative and maybe even fun. But imagine a system engineer who has to set up a new Linux network with a large number of machines. Now, the same issues need to be addressed and the same questions answered repeatedly. This makes the task very inefficient, not to mention a source of irritation and boredom. Hence, a need arises to automate this parameter and option selection.”

“The thought of simply copying the hard disks naturally crosses one's mind. This can be done quickly, and all the necessary functions and software will be copied without option selection. However, the fact is that simple copying of hard disks causes the individual computers to become too similar. This, in turn, creates an altogether new mission of having to reconfigure the individual settings on each PC. For example, IP addresses for each machine will have to be reset. If this is not done properly, strange and inexplicable behavior results.”

Regular installation of SuSE Linux is semi-automated by default. The user is requested to select the necessary information at the beginning of the installation (In most cases language only), YaST2 then generates a proposal for the underlying system depending on different factors and system parameters. In most cases, and especially for new systems, such a proposal can be used to install the system and provides a usable installation.

The steps following the proposal are fully automated and the user is only prompted at the end of the installation to configure hardware and network services.

AutoYaST can be used where no user intervention is required or where customization is required. Using a control file, YaST2 prepares the system for a custom installation and avoids any interaction with the user, unless specified in the file controlling the installation.

AutoYaST is not an automated GUI system. This means that in most cases many screens will be skipped, i.e. you will never see the language selection interface. AutoYaST will simply pass the language parameter to the sub-system without displaying any language related interface.

### 3. Overview and Concept

Using AutoYaST, multiple systems sharing the same environment and similar but not necessarily identical hardware performing similar tasks can easily be installed in parallel and in a short time. A configuration file (referred to as "control file") is created using existing configuration resources. The control file can be easily tailored for any specific environment.

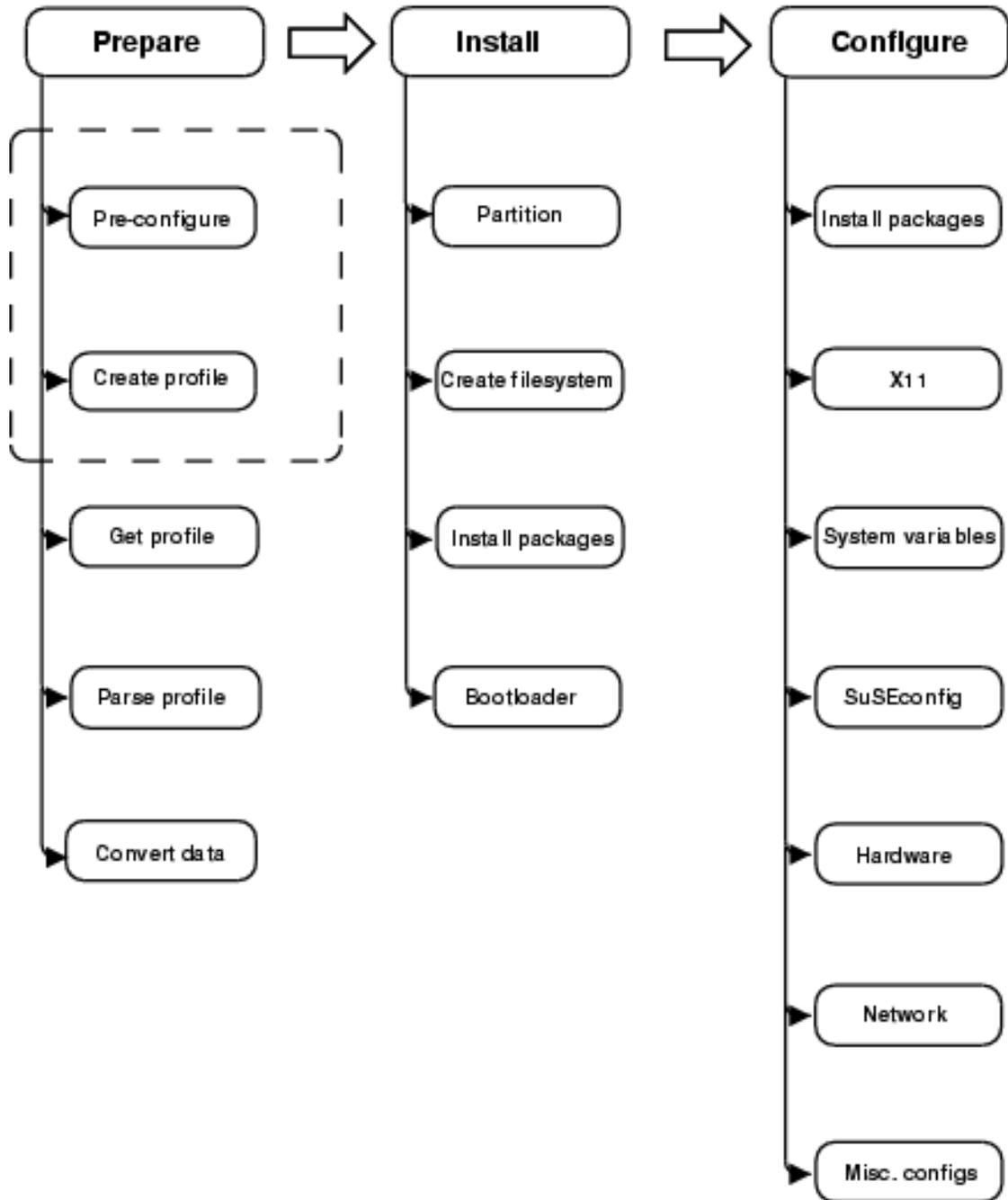
Unlike autoinstallation systems available with older *SuSE* releases, AutoYaST is fully integrated and provides various options for installing and configuring a system. The main advantage over older systems and other auto-installation systems is the possibility to configure a computer by using existing modules and avoiding using custom scripts which are normally executed at the end of the installation.

This document will guide you through the three steps of auto-installation:

- **Preparation:** All relevant information about the target system are collected and turned into the appropriate directives of the control file. The control file is transferred onto the target system where its directives will be parsed and transformed to YaST2 conforming data.
- **Installation:** follows the instructions given in the control file and installs the base system.
- **Configuration:** YaST2 in addition to user-defined post-install scripts complete the system configuration

The complete and detailed process is illustrated in the following figure:

Figure 1.1. Auto-installation process



---

# Chapter 2. The Control File

## 1. Introduction

The control file is in most cases a configuration description for a single system. It consists of sets of resources with properties including support for complex structures representations such as lists, records, trees and large embedded or referenced objects.

## 2. Format

The XML configuration format provides a consistent file structure, which is easier to learn and remember when attempting to configure a new system.

Using XML, you can eliminate (nearly) all of the configuration file parsing and error handling - an external XML parser can do that instead - (especially if it is a validating parser). To make sure the control file is well-formatted and that the syntax is valid, you can run the control file through a validating parser before it is actually used for automatic installation. This is especially required if you prefer to edit the profile manually.

The following example shows a control file in XML format:

### Example 2.1. XML Control File (Profile)

```
<?xml version="1.0"?>
<!DOCTYPE profile SYSTEM
"/usr/share/autoinstall/dtd/profile.dtd">
<profile
xmlns="http://www.suse.com/1.0/yast2ns"
xmlns:config="http://www.suse.com/1.0/configns">
  <install>
    <partitioning config:type="list">
      <drive>
        <device>/dev/hda</device>
        <partitions config:type="list">
          <partition>
            <filesystem config:type="symbol">ext2</filesystem>
            <size>520Mb</size>
            <mount>/</mount>
          </partition>
          <partition>
            <filesystem config:type="symbol">reiser</filesystem>
            <size>1200Mb</size>
            <mount>/data</mount>
          </partition>
        </partitions>
      </drive>
    </partitioning>
  </install>
  <configure>
    <scripts>
      <pre-scripts>
        <script>
          <interpreter>shell</interpreter>
          <filename>start.sh</filename>
          <source>
            <![CDATA[
#!/bin/sh
echo "Starting installation"
exit 0
]]>
          </source>
        </script>
      </pre-scripts>
    </scripts>
  </configure>
</profile>
```

## 3. Structure

Below is an example of a basic control file container, the actual content of which is explained later on in this chapter.

### Example 2.2. Control file container

```
<?xml version="1.0"?>
<!DOCTYPE profile SYSTEM
  "/usr/share/autoinstall/dtd/profile.dtd">
<profile
  xmlns="http://www.suse.com/1.0/yast2ns"
  xmlns:config="http://www.suse.com/1.0/configns">

<!-- RESOURCES -->

</profile>
```

The profile element (root node) contains one or more distinct resource elements. The permissible resource elements are specified in the DTD.

The root element in the control file can for example contain the following sub-keywords:

- installation (Tag *<install>* )
  - Bootloader configuration: bootloader device, bootloader location (Tag *<bootloader>* )
  - Partitioning: drives and partition plans (Tag *<partitioning>* )
  - General: Installation instructions, including all variables related to the client i.e. display, languages, keyboard etc. (Tag *<general>* )
  - Software: Software and Package selections (Tag *<software>* )
- configuration (Tag *<configure>* )
  - Network: network configuration for the client and servers providing services to the target client (Tag *<networking>* )
  - Users: user administration, including first user and root. (Tag *<users>* )
  - User scripts: (Tag *<scripts>* )

### 3.1. Resources and Properties

A resource element either contains multiple and distinct property and resource elements or contains mul-

multiple instances of the same resource element or is empty. The permissible content of a resource element is specified in the DTD.

A property element is either empty or contains a literal value. The permissible property elements and values in each resource element are specified in the DTD.

An element can be either a container of other elements (a resource) or have a literal value (a property), it can never be both. This restriction is specified in the DTD. A configuration component with more than one value must either be represented as some kind of embedded list in a property value or as a nested resource.

## 3.2. Nested Resources

Nested resource elements allow a tree like structure of configuration components to be built to any level.

### Example 2.3. Nested Resources

```
...
<drive>
  <device>/dev/hda</device>
  <partitions config:type="list">
    <partition>
      <size>1000mb</size>
      <mount>/</mount>
    </partition>
    <partition>
      <size>250mb</size>
      <mount>/tmp</mount>
    </partition>
  </partitions>
</drive>
....
```

In the example above the disk resource consists of a device property and a partitions resource. The partitions resource contains multiple instances of the partition resource. Each partition resource contains a size and mount property.

Although it is specified in the DTD that the partitions resource contains multiple instances, it is still required to specify this to avoid wrong data typing in YaST2. Using the example above, imagine having a drive with only one partition. This will result in interpreting the partition resource as a property. To avoid this the following syntax must be used when defining multiple instances. For more information about type attributes, see next section.

### Example 2.4. Nested Resources with type attributes

```
...
<drive>
  <device>/dev/hda</device>
  <partitions config:type="list">
    <partition>
      <size>1000</size>
      <mount>/</mount>
    </partition>
    <partition>
      <size>250</size>
      <mount>/tmp</mount>
    </partition>
  </partitions>
</drive>
....
```

### 3.3. Attributes

Global profile attributes are used to define meta-data on resources and properties. Attributes are used to define context switching. They are also used for naming and typing properties as shown in earlier sections<sup>1</sup>.

Profile attributes are defined in the configuration namespace and must always be prefixed with *config:*. All profile attributes are optional. Most can be used with both resource and property elements but some can only be used with one type of element which is specified in the DTD.

The type of an element is defined using the *config:type* attribute. The type of a resource element is always `RESOURCE`, although this can also be made explicit with this attribute (to ensure correct identification of an empty element for example when there is no DTD to refer to). A resource element cannot be any other type and this restriction is specified in the DTD. The type of a property element determines the interpretation of its literal value. The type of a property element defaults to `STRING`, as specified in the DTD. The full set of permissible types is specified in the DTD.

## 4. The XML Document Type Definition (DTD)

### 4.1. Introduction

The purpose of a DTD is to define the legal building blocks of an XML document. It defines the document structure with a list of legal elements. A DTD can be declared inline in the XML document, or as an external reference.

XML provides an application independent way of sharing data. With a DTD, the application can use a standard DTD to verify that data that the user supplies is valid. A "Valid" XML document is a "Well Formed" XML document which conforms to the rules of a Document Type Definition (DTD).

In AutoYaST, a DTD should be available to allow users to validate the control files before the installation process is initiated. The DTD can be also used with XML editors while editing the control file to avoid later errors.

### 4.2. Example DTD

- A *drive* resource containing a *device* property and a *partitions* property represented as a nested resource.
- A *partitions* resource containing multiple instances of the *partition* property represented as a nested resource.
- A *partition* resource containing a *size* property and a *mount* property.

Below is the XML for an example node view profile for the above tree which includes a DTD which validates it.

#### Example 2.5. Example DTD

---

<sup>1</sup> Profile attributes are in a separate namespace so they don't have to be treated as reserved words in the default namespace. New ones can then be added without having to potentially alter existing profiles.

```
<?xml version="1.0"?>
<!DOCTYPE profile [
<!ELEMENT profile (install)>
<!ELEMENT install (partitioning)>
<!ELEMENT partitioning (drive+)>
<!ELEMENT drive (device,partitions)>
<!ELEMENT device (#PCDATA)>
<!ELEMENT partitions (partition*)>
<!ELEMENT partition (size,mount)>
<!ELEMENT size (#PCDATA)>
<!ELEMENT mount (#PCDATA)>
]>
<profile>
.....
  <install>
    <partitioning config:type="list">
      <drive>
        <device>
          /dev/hda
        </device>
        <partitions>
          <partition>
            <size>1000mb</size>
            <mount>/</mount>
          </partition>
          <partition>
            <size>250mb</size>
            <mount>/tmp</mount>
          </partition>
        </partitions>
      </drive>
    </partitioning>
  </install>
.....
</profile>
```

---

# Chapter 3. Creating A Control File

## 1. Collect information

In order to create the control file, first you need to collect information about the systems you are going to install. This includes among other things hardware data and network information. Make sure you know the following about the machines you want to install:

- Hard disk types and sizes
- Graphic interface and attached monitor if any
- Network interface and MAC address if known (i.e. when using DHCP)

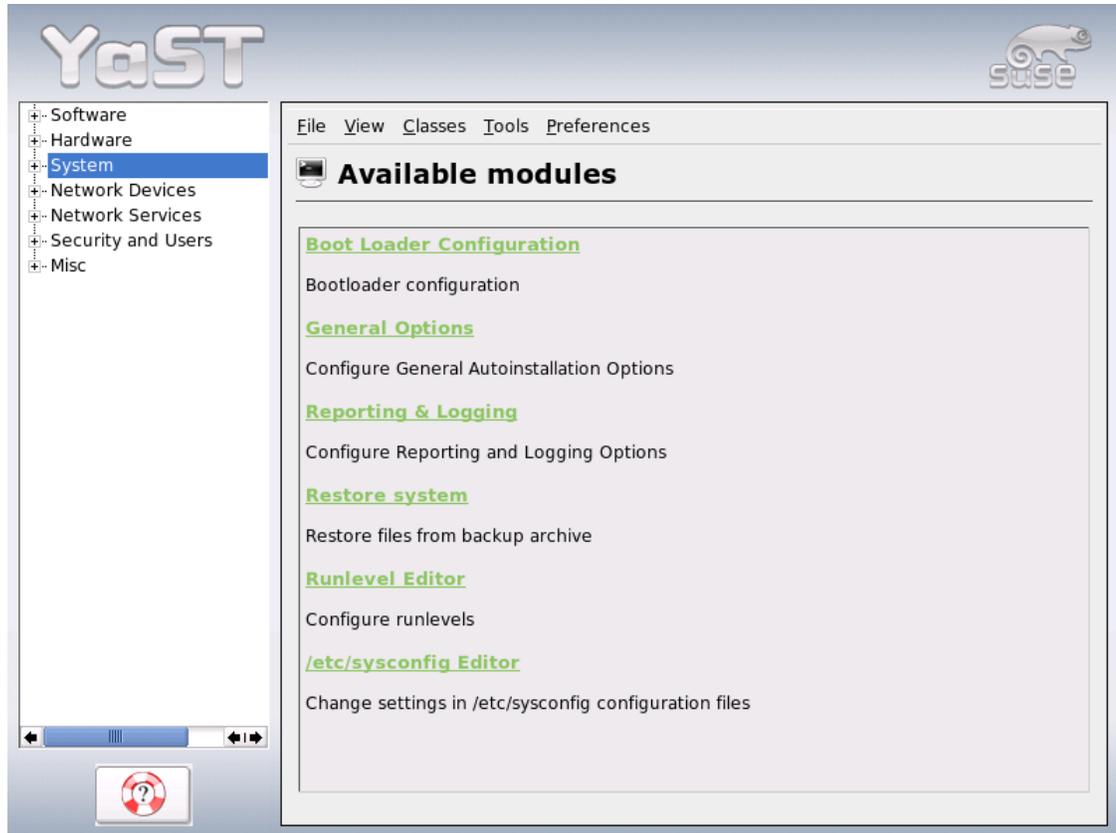
With these parameters you are ready to go and create a profile of your systems to control the auto-installation process.

## 2. Using the Configuration Management System

In order to create the control file for one or more computers, a configuration interface based on YaST2 is provided. This system depends on existing modules which are usually used to configure a computer in regular operation mode, i.e. after *SuSE* Linux is installed.

The configuration management system lets you create control files easily and additionally it lets you manage a repository of configurations for use in a networked environment and with multiple clients.

**Figure 3.1. Configuration System**



## 2.1. Creating a new Profile

With some exceptions, almost all resources of the control file can be configured using the configuration management system. The system offers flexibility and configuration of some resources is identical to this available in the YaST2 Control Center. In addition to the existing and familiar modules new interfaces were created for special and complex configurations, for example for partitioning, general options and software.

Furthermore, using the CMS guarantees that the resulting control file is valid and insures that it can be used directly to start automated installation.

Make sure the configuration system is installed (package *autoyast2*) and call it using the *YaST2 Control Center* or call it directly as root with the following command (make sure the *DISPLAY* variable is set correctly to start the graphical user interface instead of the text based one):

```
/sbin/yast2 autoyast
```

## 2.2. Import of Legacy and Foreign Configuration Files

AutoYaST offers the option to import ALICE configuration files from previous SuSE releases and foreign auto-installation systems (Kickstart). Consult the chapter dealing with these issues in this manual.

## 3. Creating/Editing a Control File Manually

If you edit the control file manually, make sure it has a valid syntax. To check the syntax, use some tools

already available on the distribution. For example to verify that the file is well formed, use the utility **xmllint** available with the *libxml2* package:

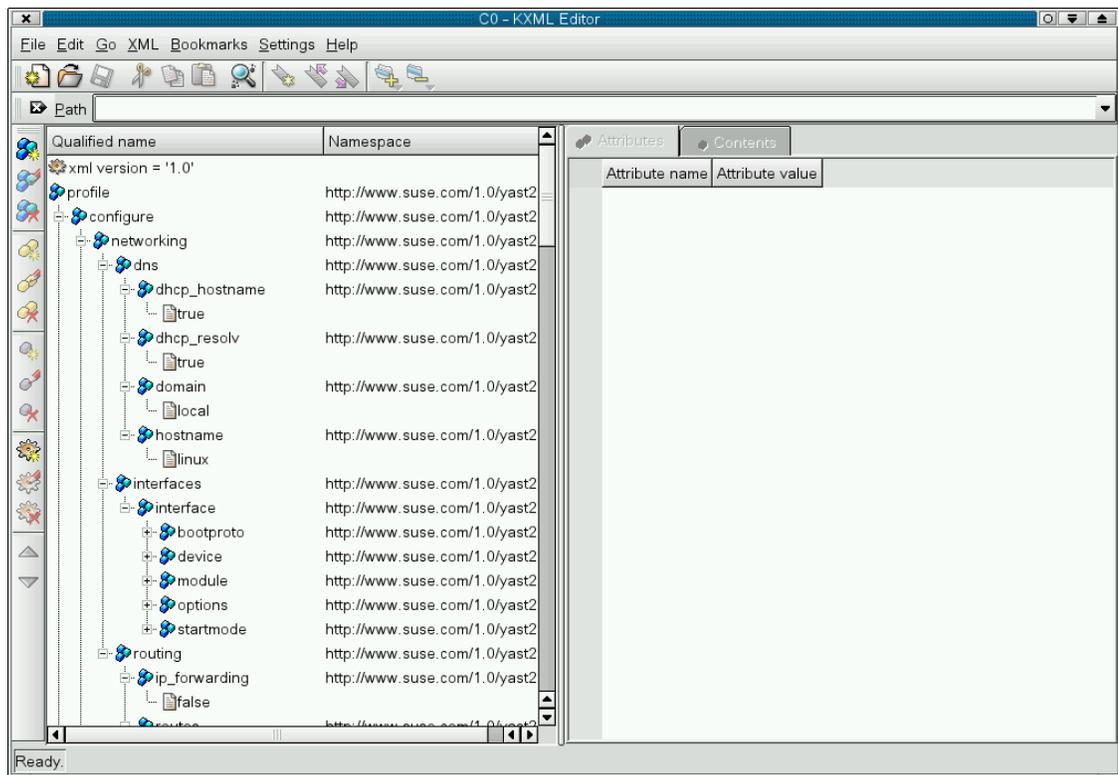
```
xmllint <control file>
```

If the control file is not well formed, i.e. if a tag is not closed, **xmllint** will report about the errors.

Before going on with the auto-installation, please fix any errors resulting from such checks. The auto-installation process can't be started with an invalid and non-well formed control file.

You can use any XML editor available on your system or use your favorite text editor with XML support (i.e. Emacs, Vim). However, it is not quite optimal to create the control file manually for large number of machines and it should only be seen as an interface between the auto-installation engine and the Configuration Management System (CMS).

**Figure 3.2. Editing the control file with kxmledit**



---

# Chapter 4. Configuration and Installation Options

This chapter introduces important parts of a control file for standard purposes. To have an idea about the other options available, use the configuration management system.

Note that for some of the configuration options to work, additional packages have to be installed, depending on the software selection you have configured. If you choose to install *Minimal* then some packages might be missing and those have to be added to the individual package selection.

YaST will install packages required by YaST modules in the second phase of the installation and before the post-installation phase of AutoYaST has started, however if the YaST modules are not available in the system, this will not happen. For example, no security settings will be configured if *yast2-security* is not installed.

## 1. General Options

This is a *required* section of the profile. General options include all the settings related to the installation process and the environment of the installed system. Among others it includes the following 4 properties which are required: *language*, *keyboard*, *clock* and *mouse* almost for any installation. If left out, default values will be used, which might not be in one hand with what you want.

### Example 4.1. General Options

```
<install>
  <general>
    <clock>
      <hwclock>UTC</hwclock>
      <timezone>US/Eastern</timezone>
    </clock>
    <keyboard>
      <keymap>german</keymap>
    </keyboard>
    <language>de_DE</language>
    <mode>
      <confirm config:type="boolean">true</confirm>
      <forceboot config:type="boolean">>false</forceboot>
    </mode>
    <mouse>
      <device>/dev/psaux</device>
      <id>ps0</id>
    </mouse>
  </general>
</install>
```

By default, the auto-installation process has to be confirmed by the user. The confirmation should be disabled if a fully unattended installation is desired. This option is used to view and change the settings on a target system before anything is committed and can be used for debugging. It is set to *true* by default to avoid recursive installs when the system schedules a reboot after initial system setup.

### Change starting from SUSE Linux 9.1/SLES 9

The *reboot* property in the *mode* resource was used to force a reboot after initial system setup and before the system is booted for the first time. Currently after initial installation all systems

must boot, which makes this option obsolete.

## SLES9 Only Options

In SLES 9, it is possible to halt the system after the initial installation phase using the boolean property *halt*

## 2. Reporting

The *report* resource manages 3 types of pop-ups that may appear during installation.

- Messages Popups (Usually non-critical, informative messages)
- Warning Popups (If something might go wrong)
- Error Popups (In the case of an error)

### Example 4.2. Reporting Behavior

```
<install>
  <report>
    <messages>
      <show config:type="boolean">true</show>
      <timeout config:type="integer">10</timeout>
      <log config:type="boolean">true</log>
    </messages>
    <errors>
      <show config:type="boolean">true</show>
      <timeout config:type="integer">10</timeout>
      <log config:type="boolean">true</log>
    </errors>
    <warnings>
      <show config:type="boolean">true</show>
      <timeout config:type="integer">10</timeout>
      <log config:type="boolean">true</log>
    </warnings>
  </report>
</install>
```

Depending on your experience, you can skip, log and show (with timeout) those messages. It is recommended to show all *messages* with timeout. Warnings can be skipped in some places but should not be ignored.

By default, the settings in auto-installation mode is to show all messages without logging and with a timeout of 10 seconds.

### Critical system messages

Note that *not* all messages during installation are controlled by the *report* resource. Some critical messages concerning package installation and partitioning will still show up ignoring your settings in the *report* section. Mostly those messages will have to be answered with *Yes* or *No*.

## 3. The Boot loader

It is now possible to specify which bootloader needs to be installed and it is possible to specify sections and more bootloader options.

If the bootloader resource is not configured, the system will propose best configuration depending on the partitioning scheme. In some cases you must decide where to install the bootloader (the Master Boot Record or the first sector of the `/boot` partition) and must specify additional options for the bootloader to be installed correctly.

## Boot Partition on IA64 Systems

The boot partition on *IA64* is `/boot/efi` and is set to this value if only `/boot` is configured in the control file.

Additionally, you can configure special kernel and boot parameters, Kernel parameters can be configured using the `kernel_parameters` property.

### Example 4.3. Bootloader configuration

```
<?xml version="1.0"?>
<!DOCTYPE profile SYSTEM "/usr/share/autoinstall/dtd/profile.dtd">
<profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configs">
  <install>
    <bootloader>
      <global config:type="list">
        <global_entry>
          <key>prompt</key>
          <value config:type="boolean">>false</value>
        </global_entry>
      </global>
      <loader_device></loader_device>
      <loader_type>lilo</loader_type>
      <location>mbr</location>
      <sections config:type="list"/>
    </bootloader>
  </install>
</profile>
```

The *global* resource is used to configure additional boot loader options. Note that bootloaders can have different configurable options. Consult the documentation for the specific bootloader you want to use before adding any options.

For example, to configure the serial console with *grub*, you can add the following options:

### Example 4.4. Serial console configuration with GRUB

```
<bootloader>
  <global config:type="list">
    <global_entry>
      <key>serial</key>
      <value>--unit=1 --speed=115200</value>
    </global_entry>
    <global_entry>
      <key>terminal</key>
      <value>serial console</value>
    </global_entry>
  </global>
  <loader_type>grub</loader_type>
  <location></location>
</bootloader>
```

## Tip

The bootloader configuration interface offers more configuration options than one might need for a regular setup. The options described in the example above should be sufficient for most cases.

In the current version, bootloader configuration also supports different architectures and boards. The configuration of the bootloader can be done offline using AutoYaST. For example, the bootloader configuration for PPC has the following additional options:

#### Example 4.5. Bootloader configuration for PPC

```
<?xml version="1.0"?>
<!DOCTYPE profile SYSTEM "/usr/share/autoinstall/dtd/profile.dtd">
<profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configs">
  <install>
    <bootloader>
      <board_type>iseries</board_type>
      <global config:type="list"/>
      <iseries_streamfile>/boot/suse_linux_bootfile</iseries_streamfile>
      <iseries_write_prepboot config:type="boolean">true</iseries_write_prepboot>
      <iseries_write_slot_a config:type="boolean">true</iseries_write_slot_a>
      <iseries_write_slot_b config:type="boolean">true</iseries_write_slot_b>
      <iseries_write_streamfile config:type="boolean">true</iseries_write_streamfile>
      <loader_device>B</loader_device>
      <loader_type>ppc</loader_type>
      <location></location>
      <prep_boot_partition>/dev/hda1</prep_boot_partition>
    </bootloader>
  </install>
</profile>
```

Currently the following bootloaders can be configured offline using the AutoYaST interface:

- LILO
- GRUB
- ELILO
- zipl
- yaboot

## 4. Partitioning

### 4.1. Automated Partitioning

For the automated partitioning to be completed, only the sizes and mount points of partitions can be provided. All other data needed for successful partitioning can be calculated during installation if they were not provided in the control file.

If no partitions are defined and the specified drive is also the drive where the root partition should be created, the following partitions are created automatically:

- */boot*

Size of the */boot* is determined by the architecture of the target system.

- *swap*

Size of the *swap* partitions is determined by the amount of memory available in the system.

- */* (root partition)

Size of the */* (root partition) is the space left after creating *swap* and */boot*.

Depending on the initial status of the drive and how it was previously partitioned, it is possible to create the *default* partitioning in the following ways:

- *Use free space*

If the drive is already partitioned, it is possible to create the new partitions using the available space on the hard drive. This requires the availability of enough space for all selected packages in addition to swap.

- *Reuse all available space*

This option will lead to the deletion of all existing partitions (Linux and non-Linux partitions).

- *Reuse all available Linux partitions*

This option will lead to the deletion of existing Linux partitions. All other partitions (i.e. Windows) will be kept. Note that this works only if the Linux partitions are at the end of the device.

- *Reuse only specified partitions*

This option will lead to the deletion of the specified partitions. The selection of the partitions scheduled for deletion should be started from the last available partition.

Repartitioning using only some of the existing partitions can be accomplished only if the region selected to be partitioned exists at the end of the device and only with neighboring partitions. This means that you cannot repartition a region which contains a partition that should not be touched in the middle.

## Important Notice

The value provided in the *use* property determines how existing data and partitions are treated. The value *all* means that *ALL* data on the disk will be erased. Make backups and use the *confirm* property if you are going to keep some partitions with important data. This is automated installation and no pop-ups will notify you about partitions being deleted.

In case of the presence of multiple drives in the target system, all drives must be identified with their device names and how the partitioning should be performed.

Partition sizes can be given in Gigabytes, Megabytes or can be set to a flexible value using the keywords *auto* and *max*. *max* is used to fill a partition to the maximal available space on a drive (Which mean that the partition should be the last one on the drive). *auto* can be used to determine the size of a *swap* or *boot* partitions depending on the memory available and the type of the system.

A fixed size can be given as shown below:

*1GB* will create a partition with 1 GB size. *1500MB* will create a partition which is 1.5 GB big.

## Example 4.6. Automated partitioning

The following is an example of a single drive system, which is not pre-partitioned and should be automatically partitioned according to the described pre-defined partition plan:

```
<partitioning config:type="list">
  <drive>
    <device>/dev/hda</device>
    <use>all</use>
  </drive>
</partitioning>
```

A more detailed example shows how existing partitions and multiple drives are handled.

### Example 4.7. Detailed automated partitioning

```
<partitioning config:type="list">
  <drive>
    <device>/dev/hda</device>
    <partitions config:type="list">
      <partition>
        <mount>/</mount>
        <size>5gb</size>
      </partition>
      <partition>
        <mount>swap</mount>
        <size>1gb</size>
      </partition>
    </partitions>
  </drive>
  <drive>
    <device>/dev/hdb</device>
    <use>all</use>
    <partitions config:type="list">
      <partition>
        <filesystem config:type="symbol">reiser</filesystem>
        <mount>/data1</mount>
        <size>15gb</size>
      </partition>
      <partition>
        <filesystem config:type="symbol">jfs</filesystem>
        <mount>/data2</mount>
        <size>auto</size>
      </partition>
    </partitions>
    <use>free</use>
  </drive>
</partitioning>
```

## 4.2. Advanced Partitioning features

### 4.2.1. Mount Options

By default a file system which is to be mounted is identified in `/etc/fstab` by the device name. This identification can be changed so the file system is found by searching for a UUID or a volume label. Note that not all file systems can be mounted by UUID or a volume label. To specify how a partition is to be mounted, use the *mountby* property which has the *symbol* type. Possible options are:

- device (default)
- label
- UUID

If you choose to mount the partition using a label, the name entered in the *label* property is used as the volume label.

Add any legal mount option allowed in the fourth field of */etc/fstab*. Multiple options are separated by commas. Possible *fstab* options:

- *Mount Read-Only (ro)*: No writable access to the file system is possible. Default is false.
- *No access time (noatime)*: Access times are not updated when a file is read. Default is false.
- *Mountable by User (user)*: The file system may be mounted by an ordinary user. Default is false.
- *Data Journaling Mode (ordered | journal | writeback)* : Specifies the journaling mode for file data. *journal* -- All data is committed into the journal prior to being written into the main file system. *ordered* -- All data is forced directly out to the main file system prior to its meta data being committed to the journal. *writeback* -- Data ordering is not preserved.
- *Access Control List (acl)*: Enable access control lists on the file system.
- *Extended User Attributes (user\_xattr)*: Allow extended user attributes on the file system.

### Example 4.8. Mount Options

```
<partitions config:type="list">
  <partition>
    <filesystem config:type="symbol">reiser</filesystem>
    <format config:type="boolean">true</format>
    <fstopt>ro,noatime,user,data=ordered,acl,user_xattr</fstopt>
    <mount>/local</mount>
    <mountby config:type="symbol">uuid</mountby>
    <partition_id config:type="integer">131</partition_id>
    <size>10gb</size>
  </partition>
</partitions>
```

## 4.2.2. Creating Primary and Extended Partitions

By default, AutoYaST will create an extended partition and will add all other new partitions as logical devices. It is possible however to instruct AutoYaST to create a certain partition as a primary or as extended partition. Additionally, it is possible to specify the size of a partition using sectors instead of the size in Mbytes.

The properties *partition\_id* and *partition\_type* control such behavior. To specify the size in sectors, the list resource *region* can be used.

### Example 4.9. Advanced Automated partitioning

```
<partitioning config:type="list">
  <drive>
    <device>/dev/hdc</device>
    <partitions config:type="list">
      <partition>
        <partition_id config:type="integer">5</partition_id>
        <region config:type="list">
```

```

        <region_entry config:type="integer">0</region_entry>
        <region_entry config:type="integer">16858</region_entry>
    </region>
</partition>
<partition>
    <filesystem config:type="symbol">reiser</filesystem>
    <mount>/</mount>
    <partition_id config:type="integer">131</partition_id>
    <region config:type="list">
        <region_entry config:type="integer">0</region_entry>
        <region_entry config:type="integer">2081</region_entry>
    </region>
</partition>
<partition>
    <mount>swap</mount>
    <partition_id config:type="integer">130</partition_id>
    <region config:type="list">
        <region_entry config:type="integer">2081</region_entry>
        <region_entry config:type="integer">781</region_entry>
    </region>
</partition>
</partitions>
<use>all</use>
</drive>
</partitioning>

```

The last example only makes sense if you exactly know the boundaries of the partitions and it does only make sense if you are creating an exact copy of a system, for example when cloning. The first region entry in the list is the beginning of the region, the second represents the length of the region.

The following example lets you create an extended partition with a custom size.

#### Example 4.10. Creating custom extended partitions

```

<partitioning config:type="list">
  <drive>
    <device>/dev/hdc</device>
    <partitions config:type="list">
      <partition>
        <filesystem config:type="symbol">ext2</filesystem>
        <mount>/boot</mount>
        <partition_id config:type="integer">131</partition_id>
        <partition_nr config:type="integer">2</partition_nr>
        <size>50mb</size>
      </partition>
      <partition>
        <mount>swap</mount>
        <partition_id config:type="integer">130</partition_id>
        <partition_nr config:type="integer">3</partition_nr>
        <size>100mb</size>
      </partition>
      <partition>
        <partition_id config:type="integer">15</partition_id>
        <partition_nr config:type="integer">4</partition_nr>
        <size>3000mb</size>
      </partition>
      <partition>
        <filesystem config:type="symbol">ext2</filesystem>
        <mount>/</mount>
        <partition_id config:type="integer">131</partition_id>
        <partition_nr config:type="integer">5</partition_nr>
        <size>1gb</size>
      </partition>
    </partitions>
    <use>free</use>
  </drive>
</partitioning>
</install>

```

### 4.2.3. Keeping Specific Partitions

In some cases you might choose to keep some partitions untouched and only format specific target partitions, rather than creating them from scratch. This might be the case of Linux installations have to co-exist with another operating system or if certain partitions contain data that you wish to keep untouched.

Such scenarios require certain knowledge about the target systems and hard drives. Depending on the scenario, you might need to know the exact partition table of the target hard drive with partition id's, sizes and numbers. With such data you can tell AutoYaST to keep certain partitions, format others and create new partitions if needed.

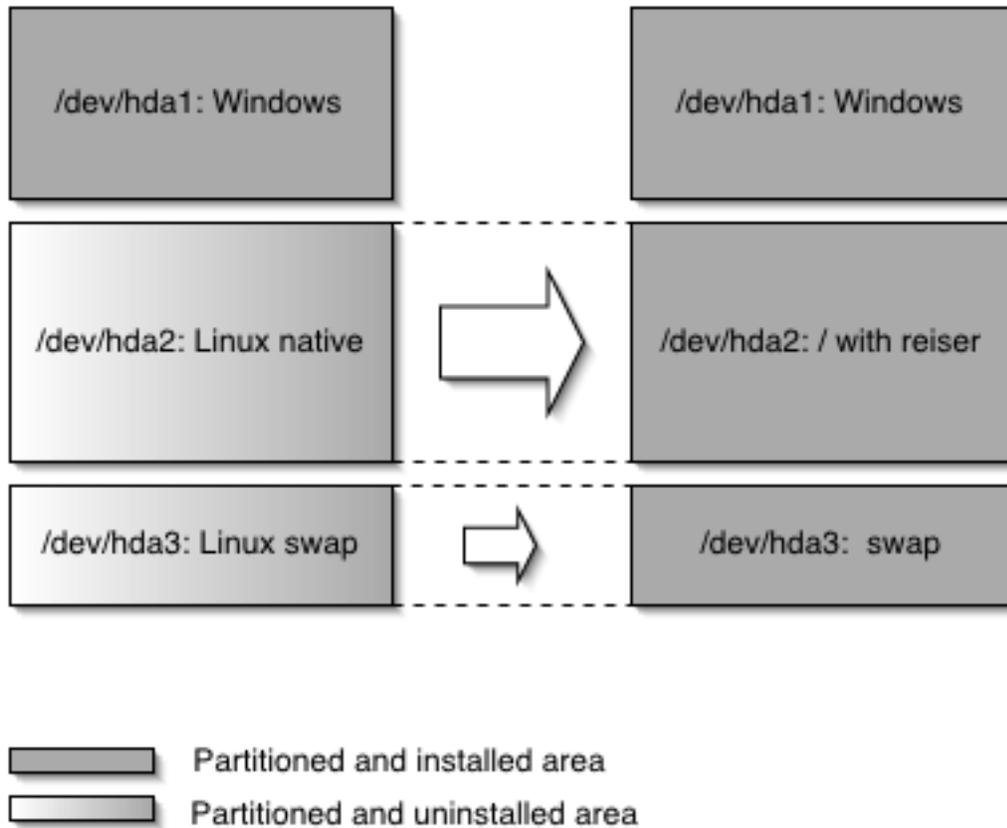
The following example will keep partitions 1, 2 and 5 and delete partition 6 to create two new partitions. All kept partitions will be only formatted.

### Example 4.11. Keeping partitions

```
<install>
  <partitioning config:type="list">
    <drive>
      <device>/dev/hdc</device>
      <partitions config:type="list">
        <partition>
          <create config:type="boolean">>false</create>
          <format config:type="boolean">>true</format>
          <mount>/</mount>
          <partition_nr config:type="integer">1</partition_nr>
        </partition>
        <partition>
          <create config:type="boolean">>false</create>
          <format config:type="boolean">>false</format>
          <partition_nr config:type="integer">2</partition_nr>
          <mount>/space</mount>
        </partition>
        <partition>
          <create config:type="boolean">>false</create>
          <format config:type="boolean">>true</format>
          <filesystem config:type="symbol">swap</filesystem>
          <partition_nr config:type="integer">5</partition_nr>
          <mount>swap</mount>
        </partition>
        <partition>
          <format config:type="boolean">>true</format>
          <mount>/space2</mount>
          <size>50mb</size>
        </partition>
        <partition>
          <format config:type="boolean">>true</format>
          <mount>/space3</mount>
          <size>max</size>
        </partition>
      </partitions>
      <use>6</use>
    </drive>
  </partitioning>
</install>
```

The last example requires exact knowledge about the existing partition table and about the partition numbers of those partitions that should be kept. In some cases however, such data might be not available, especially in a mixed hardware environment with different hard drive types and configurations. The following scenario is for a system with a non-Linux OS with a designated area for a Linux installation.

**Figure 4.1. Keeping partitions**



In this scenario and as shown in figure “Keeping partitions”, AutoYaST should not in any case create any new partitions, instead it should search for certain partition types on the system and use them according to the partitioning plan in the control file. No partition numbers are given in this case, only the mount points and the partition types (Additional configuration data can be provided, for example file system options, encryption and filesystem type)

**Example 4.12. Auto-detection of partitions to be kept.**

```

<install>
  <partitioning config:type="list">
    <drive>
      <partitions config:type="list">
        <partition>
          <create config:type="boolean">>false</create>
          <format config:type="boolean">>true</format>
          <mount/></mount>
          <partition_id config:type="integer">131</partition_id>
        </partition>
        <partition>
          <create config:type="boolean">>false</create>
          <format config:type="boolean">>true</format>
          <filesystem config:type="symbol">swap</filesystem>
          <partition_id config:type="integer">130</partition_id>
          <mount>swap</mount>
        </partition>
      </partitions>
    </drive>
  </partitioning>
</install>
    
```

## 4.3. Using existing mount table (fstab)

### New Feature

This option will allow the AutoYaST to use an existing `/etc/fstab` and use the partition data from from a previous installation. All partitions are kept and no new partitions are created. The found partitions will be formatted and mounted as specified in `/etc/fstab` found on a Linux root partition.

Although the default behaviour is to format all partitions, it is also possible to leave some partitions untouched and only mount them, for example data partitions. If multiple installations are found on the system (multiple root partitions with different *fstab* files, the installation will abort, unless the desired root partition is configured in the control file. The following example illustrates how this option can be used:

#### Example 4.13. Reading existing `/etc/fstab`

```
<install>
  <partitioning_advanced>
    <fstab>
      <!-- Read data from existing fstab. If multiple root partitions are
      found, use the one specified below. Otherwise the first root
      partition is taken -->
      <!-- <root_partition>/dev/hda5</root_partition> -->
      <use_existing_fstab config:type="boolean">true</use_existing_fstab>
      <!-- all partitions found in fstab will be formatted and mounted
      by default unless a partition is listed below with different
      settings -->
      <partitions config:type="list">
        <partition>
          <format config:type="boolean">>false</format>
          <mount>/bootmirror</mount>
        </partition>
      </partitions>
    </fstab>
  </partitioning_advanced>
</install>
```

## 4.4. Logical Volume Manager (LVM)

To configure LVM, first you need to create a *physical volume* using the normal partitioning method described above.

#### Example 4.14. Create LVM Physical Volume

The following example shows how to prepare for LVM in the *partitioning* resource:

```
<partitioning config:type="list">
  <drive>
    <device>/dev/sda</device>

    <partitions config:type="list">
      <partition>
        <lvm_group>system</lvm_group>
        <partition_type>primary</partition_type>
        <size>max</size>
      </partition>
    </partitions>
  </drive>
</partitioning>
```

The last example will create a non-formatted partition on device `/dev/sda1` of the type *LVM* and with the volume group *system*. The partition created will use all available space on this drive.

## Note

Up to SuSE Linux 8.2 the LVM configuration was done in a separate resource. This method for configuring LVM is still supported, however a new and easier way is now possible which allows you to have the LVM configuration directly in the *partitioning* resource.

Currently it is not possible to configure LVM using the configuration system, instead it is required to add the resource manually as shown in the following example:

### Example 4.15. LVM Logical Volumes (Old syntax)

```
<partitioning config:type="list">
  <drive>
    <device>/dev/sda</device>
    <partitions config:type="list">
      <partition>
        <lvm_group>system</lvm_group>
        <partition_type>primary</partition_type>
        <size>max</size>
      </partition>
    </partitions>
    <use>all</use>
  </drive>
</partitioning>

<lvm config:type="list">
  <lvm_group>
    <lvm_name>system</lvm_name>
    <logical_volumes config:type="list">
      <lv>
        <lv_fs>reiser</lv_fs>
        <lv_mount>/usr</lv_mount>
        <lv_name>usr1v</lv_name>
        <lv_size>500mb</lv_size>
      </lv>
      <lv>
        <lv_fs>reiser</lv_fs>
        <lv_mount>/opt</lv_mount>
        <lv_name>opt1v</lv_name>
        <lv_size>1500mb</lv_size>
      </lv>
      <lv>
        <lv_fs>reiser</lv_fs>
        <lv_mount>/var</lv_mount>
        <lv_name>var1v</lv_name>
        <lv_size>200mb</lv_size>
      </lv>
    </logical_volumes>
    <pesize>4M</pesize>
  </lvm_group>
</lvm>
```

Using the new method, the above configuration has the following syntax:

### Example 4.16. LVM Logical Volumes (New syntax)

```
<partitioning config:type="list">
  <drive>
    <device>/dev/sda</device>
    <partitions config:type="list">
      <partition>
        <lvm_group>system</lvm_group>
        <partition_type>primary</partition_type>
        <size>max</size>
```

```

    </partition>
  </partitions>
  <use>all</use>
</drive>
<drive>
  <device>/dev/system</device>
  <is_lvm_vg config:type="boolean">true</is_lvm_vg>
  <partitions config:type="list">
    <partition>
      <filesystem config:type="symbol">reiser</filesystem>
      <lv_name>user_lv</lv_name>
      <mount>/usr</mount>
      <size>500mb</size>
    </partition>
    <partition>
      <filesystem config:type="symbol">reiser</filesystem>
      <lv_name>opt_lv</lv_name>
      <mount>/opt</mount>
      <size>1500mb</size>
    </partition>
    <partition>
      <filesystem config:type="symbol">reiser</filesystem>
      <lv_name>var_lv</lv_name>
      <mount>/var</mount>
      <size>200mb</size>
    </partition>
  </partitions>
  <pesize>4M</pesize>
  <use>all</use>
</drive>
</partitioning>

```

## 4.5. Software RAID

Using AutoYaST, you can create and assemble software RAID devices. The supported RAID levels are the following:

- *RAID 0*: This level increases your disk performance. There is *NO* redundancy in this mode. If one of the drives crashes, data recovery will not be possible.
- *RAID 1*: This mode has the best redundancy. It can be used with two or more disks. This mode maintains an exact copy of all data on all disks. As long as at least one disk is still working, no data is lost. The partitions used for this type of RAID should have approximately the same size.
- *RAID 5*: This mode combines management of a larger number of disks and still maintains some redundancy. This mode can be used on three disks or more. If one disk fails, all data is still intact. If two disks fail simultaneously, all data is lost.
- *Multipath*: This mode allow access to the same physical device over multiple controller for redundancy against a fault in a controller card. This mode can be used with at least two devices.

As with LVM, you need to create all *RAID* partitions first and assign the partitions to the RAID device you want to create and additionally you need to specify whether a partition or a device should be configured in the RAID or if it should be configured as a *Spare* device.

### Note

Up to SuSE Linux 8.2 the raid configuration was done in a separate resource. This method for configuring raid devices is still supported, however a new and easier way is now possible which allows the user to have the raid configuration directly in the *partitioning* resource.

The following example shows a simple RAID1 configuration:

### Example 4.17. RAID1 configuration (Old Syntax)

```

<partitioning config:type="list">
  <drive>
    <device>/dev/sda</device>
    <partitions config:type="list">
      <partition>
        <format config:type="boolean">>false</format>
        <partition_id config:type="integer">253</partition_id>
        <raid_name>/dev/md0</raid_name>
        <raid_type>raid</raid_type>
        <size>4gb</size>
      </partition>

      <!-- Here come the regular partitions, i.e. / and swap -->
    </partitions>
    <use>all</use>
  </drive>
  <drive>
    <device>/dev/sdb</device>
    <use>all</use>
    <partitions config:type="list">
      <partition>
        <format config:type="boolean">>false</format>
        <partition_id config:type="integer">253</partition_id>
        <raid_name>/dev/md0</raid_name>
        <raid_type>raid</raid_type>
        <size>4gb</size>
      </partition>
    </partitions>
  </drive>
</partitioning>

<raid config:type="list">
  <raid_device>
    <chunk_size>4</chunk_size>
    <device_name>/dev/md0</device_name>
    <filesystem config:type="symbol">reiser</filesystem>
    <format config:type="boolean">>true</format>
    <parity_algorithm>left-asymmetric</parity_algorithm>
    <partition_id config:type="integer">131</partition_id>
    <persistent_superblock config:type="boolean">>true</persistent_superblock>
    <mount>/space</mount>
    <raid_type>raid1</raid_type>
  </raid_device>
</raid>

```

Using the new method, the above configuration has the following syntax:

### Example 4.18. RAID1 configuration (New Syntax)

```

<partitioning config:type="list">
  <drive>
    <device>/dev/sda</device>
    <partitions config:type="list">
      <partition>
        <partition_id config:type="integer">253</partition_id>
        <format config:type="boolean">>false</format>
        <raid_name>/dev/md0</raid_name>
        <raid_type>raid</raid_type>
        <size>4gb</size>
      </partition>

      <!-- Here come the regular partitions, i.e. / and swap -->
    </partitions>
    <use>all</use>
  </drive>
  <drive>
    <device>/dev/sdb</device>

    <partitions config:type="list">
      <partition>

```

```

<format config:type="boolean">false</format>
<partition_id config:type="integer">253</partition_id>
<raid_name>/dev/md0</raid_name>
<raid_type>raid</raid_type>
<size>4gb</size>
</partition>
</partitions>
<use>all</use>
</drive>
<drive>
<device>/dev/md</device>
<partitions config:type="list">
<partition>
<filesystem config:type="symbol">reiser</filesystem>
<format config:type="boolean">true</format>
<mount>/space</mount>
<partition_id config:type="integer">131</partition_id>
<partition_nr config:type="integer">0</partition_nr>
<raid_options>
<chunk_size>4</chunk_size>
<parity_algorithm>left-asymmetric</parity_algorithm>
<raid_type>raid1</raid_type>
</raid_options>
</partition>
</partitions>
<use>all</use>
</drive>
</partitioning>

```

The following has to be taken into consideration when configuring raid using the new syntax:

- The device for raid is always */dev/md*
- The property *partition\_nr* is used to determine the MD device number. if *partition\_nr* is equal to 0, then */dev/md0* is configured.
- All RAID specific options are contained in the *raid\_options* resource.

## 5. Software

### 5.1. Package Selections

You can install software on the new system using a pre-defined package base selection, i.e. Minimal, Minimal+X11, default etc. in addition to several *Add-on* selections. Check the first CD for available selections in *suse/setup/descr/selections*, depending on the product you are installing, some "well-known" selections might not be available.

In the control file, packages and package selections are described as the following:

#### Example 4.19. Package selection in control file

```

<software>
<addons config:type="list">
<addon>Kde</addon>
</addons>
<base>Minimal</base>
<packages config:type="list">
<package>apache</package>
<package>sendmail</package>
</packages>
</software>

```

You can install one base selection and additionally one or multiple add-on selections.

When installing from a CD-ROM, needed packages from other CD-ROMs are installed after the initial boot of the system in the second installation phase. If you are installing packages from multiple CD-ROMs, then auto-installation has to be interrupted for switching the CD-ROMs. In the case of NFS installation, all packages are installed at first stage of the installation only if the NFS repository is configured as a single medium.

It is often required, that a package should be installed in the second phase, especially custom packages which may contain scripts for configuring the system. This can be done using the *post-packages* resource.

## 5.2. Custom Package Selections

In addition to the pre-defined selections, you can create custom selections by providing a selection file in the selection directory. (*suse/setup/descr*) The selection files have a special format and any additional selection file must conform to this format, otherwise YaST2 will not be able to read it.

As an example for the selection file, take a look at the files available in the directory */suse/setup/descr/* on the CD-ROMs.

After creating a selection file, you can add it to the configuration as described earlier in this section. The selection name, for example *My.sel* has to be added to the index files *selections* and *directory.yast* to make it visible to the installer.

The file *My.sel* should have the following format:

### Example 4.20. Customized Package selection

```
# SuSE-Linux-Package-Selection 3.0 -- (c) 2004 SuSE Linux AG
# generated on Thu Apr 15 19:49:04 UTC 2004

=Ver: 3.0
=Sel: LSB

=Sum: LSB Runtime Environment
=Sum.de: LSB-Laufzeitumgebung

=Cat: addon

=Vis: true

=Ord: 108

+Ins:
XFree86-Mesa
XFree86-libs
expect
fontconfig
freetype2
gettext
glibc-118ndata
libgcj
lsb
make
makedev
patch
pax
rsync
-In:
```

To use the above selection, the following should be added in the control file:

**Example 4.21. Package selection file**

```
<install>
...
<software>
  <base>My</base>
</software>
...
</install>
```

## 5.3. Installing additional and customized Packages

In addition to the packages available for installation on the CD-ROMs, you can add external packages including customized kernels. Customized kernel packages must be compatible to the *SuSE* packages and must install the kernel files to the same locations.

Unlike earlier versions, to install custom and external packages there is no need for a special resource in the control file. Instead you need to re-create the package database and update it with any new packages or new package versions in the source repository.

A script is provided for this task which will query packages available in the repository and create the required package database.

Creating a new package database is only needed if new RPMs (i.e. update RPMs) were added. To re-create the database, use the `/usr/bin/create_package_descr` command. For example, use this command line to create the package database. (When creating the database, all languages will be reset to English).

**Example 4.22. Creating package database**

```
cd /usr/local/CDs/LATEST/suse
create_package_descr -x PATH_TO_EXTRA_PROV -d /usr/local/CDs/LATEST/suse
```

### Change starting from SUSE Linux 9.1/SLES 9

To provide extra dependencies which can not be extracted from the rpm files, an extra file with missing dependencies is available in the directory `suse/setup/descr`. The file `EXTRA_PROV` can be used when recreating the package database using the `-x` option.

In the above example, the directory `/usr/local/CDs/LATEST/suse` contains the architecture dependent and independent packages, i.e. *noarch* and *i586*. This might look different on other architectures.

The advantage of this method is that you can keep an up-to-date repository with fixed and updated package (i.e. from *SuSE* FTP server). Additionally this method makes the creation of custom CD-ROMs easier.

## 5.4. Kernel packages

Kernel packages are not part of any selection. The required kernel is determined during installation. If the kernel package is added to any selection or to the individual package selection, installation will

mostly fail due to conflicts.

To force the installation of a specific kernel, use the *kernel* property. The following is an example forcing the installation of the default kernel. In this example this kernel will be installed in any case, even if an SMP or other kernel is required

#### Example 4.23. Package selection in control file

```
<software>
  <addons config:type="list">
    <addon>Kde</addon>
  </addons>
  <base>Minimal</base>
  <kernel>kernel-default</kernel>
  <packages config:type="list">
    <package>apache2</package>
  </packages>
</software>
```

## 5.5. Removing automatically selected packages

Some packages are selected automatically either because of a dependency or because it is available in a selection.

Removing such packages might break the system consistency and it is not recommended to remove basic packages unless a replacement which provides same services is provided. Best example for this case are MTA packages. By default, *postfix* will be selected and installed. If you wish however to use another MTA like *sendmail*, then postfix can be removed from the list of selected package using a list in the software resource. The following example shows how this can be done:

#### Example 4.24. Package selection in control file

```
<software>
  <addons config:type="list">
    <addon>Kde</addon>
  </addons>
  <base>Minimal</base>
  <packages config:type="list">
    <package>sendmail</package>
  </packages>
  <remove-packages config:type="list">
    <package>postfix</package>
  </remove-packages>
</software>
```

## 6. Services and Run-levels

With the run-level resource you can set the default run-level and specify in detail which system services you want to be started in which run-level.

The default property specifies the *default* run level of the system. Changes to the default run-level will take effect the next time you boot the system. After installation is completed, the system has run-level 5, which is *Full multiuser with network and XDM*. If you have configured a system with no X11, then it is

recommended to reboot the system after the first stage using the *reboot* property in the *general* resource.

A service should run in using a space delimited list of the run-levels as shown in the following example. An alternative to specifying the exact run-levels is to change the status of the service by either enabling or disabling it using the *service\_status* property.

### Example 4.25. Run-level Configuration

```
<configure>
....
<runlevels>
<default>3</default>
<services config:type="list" >
  <service>
    <service_name>at</service_name>
    <service_start>3 5</service_start>
  </service>
  <service>
    <service_name>portmap</service_name>
    <service_status>enable</service_status>
  </service>
  <service>
    <service_name>hwsan</service_name>
    <service_status>disable</service_status>
  </service>
</services>
</runlevels>
....
</configure>
```

## 7. Network configuration

### 7.1. Network devices, DNS and Routing.

Network configuration is used to connect a single *SuSE* Linux workstation to an Ethernet-based LAN or to configure dial-up connection. More complex configuration (multiple network cards, routing, etc.) is also provided. With this module it's possible to configure and setup Ethernet Controllers and Token-Ring Controllers.

To configure network settings and activate networking automatically, one global resource is used to store the whole network configuration.

### Example 4.26. Network configuration

```
<configure>
.....
<networking>
  <dns>
    <dhcp_hostname config:type="boolean">true</dhcp_hostname>
    <dhcp_resolv config:type="boolean">true</dhcp_resolv>
    <domain>local</domain>
    <hostname>linux</hostname>
  </dns>
  <interfaces config:type="list">
    <interface>
      <bootproto>dhcp</bootproto>
      <device>eth0</device>
      <startmode>onboot</startmode>
    </interface>
  </interfaces>
  <routing>
    <ip_forward config:type="boolean">>false</ip_forward>
    <routes config:type="list">
      <route>
        <destination>default</destination>
```

```

        <device>-</device>
        <gateway>192.168.1.240</gateway>
        <netmask>-</netmask>
    </route>
</routes>
</routing>
<modules config:type="list">
  <module_entry>
    <device>eth0</device>
    <module>e100</module>
    <options></options>
  </module_entry>
</modules>
</networking>
....
</configure>

```

## 7.2. Proxy

Configure your Internet proxy (caching) settings using this resource.

*HTTP proxy* is the name of the proxy server for your access to the world wide web (WWW). *FTP proxy* is the name of the proxy server for your access to the file transfer services (FTP). *No proxy domains* is a list of domains for which the requests should be done directly without caching.

If you are using a proxy server with authorization, fill in Proxy user name and Proxy password.

### Example 4.27. Network configuration: Proxy

```

<?xml version="1.0"?>
<!DOCTYPE profile SYSTEM "/usr/share/autoinstall/dtd/profile.dtd">
<profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configns">
  <configure>
    <proxy>
      <enabled config:type="boolean">true</enabled>
      <ftp_proxy>http://192.168.1.240:3128</ftp_proxy>
      <http_proxy>http://192.168.1.240:3128</http_proxy>
      <no_proxy>localhost</no_proxy>
      <proxy_password>testpw</proxy_password>
      <proxy_user>testuser</proxy_user>
    </proxy>
  </configure>
</profile>

```

## 7.3. (X)inetd

The profile has elements to specify which superserver should be used (*netd\_service*), whether it should be enabled (*netd\_status*) and how the services should be configured (*netd\_conf*).

A service description element has conceptually two parts: key and non-key. When writing the configuration, services are matched using the key fields and to the matching service, non-key fields are applied. If no service matches, it is created. If more services match, a warning is reported. The key fields are *script*, *service*, *protocol* and *server*.

Service and protocol are matched literally. *script* is the base name of the config file: usually a file in `/etc/xinetd.d`, for example "echo-udp", or "inetd.conf". For compatibility with 8.2, *server* is matched more loosely: if it is `/usr/sbin/tcpd`, the real server name is taken from *server\_args*. After that, the basename of the first whitespace-separated word is taken and these values are compared.

## Example 4.28. Inetd Example

```
<profile>
<configure>
...
<inetd>
<netd_service config:type="symbol">xinetd</netd_service>
<netd_status config:type="integer">0</netd_status>
<netd_conf config:type="list">
  <conf>
    <script>imap</script>
    <service>pop3</service>
    <enabled config:type="boolean">>true</enabled>
  </conf>
  <conf>
    <server>in.ftpd</server>
    <server_args>-A</server_args>
    <enabled config:type="boolean">>true</enabled>
  </conf>
  <conf>
    <service>daytime</service>
    <protocol>tcp</protocol>
  </conf>
  ....
  <conf>...</conf>
</netd_conf>
</inetd>
...
</configure>
</profile>
```

## 7.4. NIS

Using the *nis* resource, you can configure the target machine as a *NIS client*. The following example shows a detailed configuration using multiple domains.

### Example 4.29. Network configuration: NIS

```
<configure>
...
<nis>
  <nis_broadcast config:type="boolean">>true</nis_broadcast>
  <nis_broken_server config:type="boolean">>true</nis_broken_server>
  <nis_by_dhcp config:type="boolean">>false</nis_by_dhcp>
  <nis_domain>test.com</nis_domain>
  <nis_local_only config:type="boolean">>true</nis_local_only>
  <nis_options></nis_options>
  <nis_other_domains config:type="list">
    <nis_other_domain>
      <nis_broadcast config:type="boolean">>false</nis_broadcast>
      <nis_domain>domain.com</nis_domain>
      <nis_servers config:type="list">
        <nis_server>10.10.0.1</nis_server>
      </nis_servers>
    </nis_other_domain>
  </nis_other_domains>
  <nis_servers config:type="list">
    <nis_server>192.168.1.1</nis_server>
  </nis_servers>
  <start_autofs config:type="boolean">>true</start_autofs>
  <start_nis config:type="boolean">>true</start_nis>
</nis>
...
</configure>
```

## 7.5. LDAP client

The installed machine can be set up as an > *LDAP client* to authenticate users with an OpenLDAP; server. Required data are the name of the search base (base DN, e.g. dc=mydomain,dc=com) and the IP address of the LDAP server (e.g., 10.20.0.2).

If LDAP is activated, *NSS* and *PAM* will be configured accordingly to use LDAP for user authentication.

### Example 4.30. Network configuration: LDAP client

```
<configure>
...
  <ldap>
    <ldap_domain> dc=mydomain,dc=com</ldap_domain>
    <ldap_server>10.10.0.1</ldap_server>
    <ldap_tls config:type="boolean">true</ldap_tls>
    <ldap_v2 config:type="boolean">true</ldap_v2>
    <pam_password>crypt</pam_password>
    <start_ldap config:type="boolean">true</start_ldap>
  </ldap>
...
</configure>
```

## 7.6. NFS Client and Server

Configuration of a system as an NFS client or an NFS server is possible and can be done using the configuration system. The following example shows how both NFS client and server can be configured.

### Example 4.31. Network configuration: NFS client

```
<configure>
...
  <nfs config:type="list">
    <nfs_entry>
      <mount_point>/home</mount_point>
      <nfs_options>defaults</nfs_options>
      <server_path>192.168.1.1:/home</server_path>
    </nfs_entry>
  </nfs>
...
</configure>
```

### Example 4.32. Network configuration: NFS Server

```
<configure>
...
  <nfs_server>
    <nfs_exports config:type="list">
      <nfs_export>
        <allowed config:type="list">
          <allowed_clients>*(ro,root_squash,sync)</allowed_clients>
        </allowed>
        <mountpoint>/home</mountpoint>
      </nfs_export>
    </nfs_exports>
  </nfs_server>
```

```

        <allowed_clients>*(ro,root_squash,sync)</allowed_clients>
    </allowed>
    <mountpoint>/work</mountpoint>
</nfs_export>
</nfs_exports>
<start_nfsserver config:type="boolean">true</start_nfsserver>
</nfs_server>
...
</configure>

```

## 7.7. NTP Client

Select whether to start the NTP daemon when booting the system. The NTP daemon resolves host names when initializing. The first synchronization of the clock is performed before the NTP daemon is started. To use this host for initial synchronization configure the property *initial\_sync*.

To run NTP daemon in chroot jail, set *start\_in\_chroot*. Starting any daemon in a chroot jail is more secure and strongly recommended. To adjust NTP servers, peers, local clocks, and NTP broadcasting, add the appropriate entry to the control file. an example of various configuration options is shown below.

### Example 4.33. Network configuration: NTP Client

```

<?xml version="1.0"?>
<!DOCTYPE profile SYSTEM "/usr/share/autoinstall/dtd/profile.dtd">
<profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configns">
  <configure>
    <ntp-client>
      <peers config:type="list">
        <peer>
          <address>10.10.0.1</address>
          <initial_sync config:type="boolean">true</initial_sync>
          <param></param>
          <type>server</type>
        </peer>
        <peer>
          <address>192.168.1.1</address>
          <initial_sync config:type="boolean">true</initial_sync>
          <param></param>
          <type>peer</type>
        </peer>
        <peer>
          <address>1.1.1.1</address>
          <type>broadcastclient</type>
        </peer>
        <peer>
          <address>127.127.2.3</address>
          <create_symlink config:type="boolean">true</create_symlink>
          <device>/dev/test</device>
          <param></param>
          <type>__clock</type>
        </peer>
      </peers>
      <start_at_boot config:type="boolean">true</start_at_boot>
      <start_in_chroot config:type="boolean">true</start_in_chroot>
    </ntp-client>
  </configure>
</profile>

```

## 8. Mail Configuration (Sendmail or Postfix)

For the mail configuration of the client this module lets you create a detailed mail configuration. The module contains various options and it is recommended to use it at least for the initial configuration.

### Example 4.34. Mail Configuration

```

<configure>
...
  <mail>
    <aliases config:type="list">
      <alias>
        <alias>root</alias>
        <comment></comment>
        <destinations>foo</destinations>
      </alias>
      <alias>
        <alias>test</alias>
        <comment></comment>
        <destinations>foo</destinations>
      </alias>
    </aliases>
    <connection_type config:type="symbol">permanent</connection_type>
    <fetchmail config:type="list">
      <fetchmail_entry>
        <local_user>foo</local_user>
        <password>bar</password>
        <protocol>POP3</protocol>
        <remote_user>foo</remote_user>
        <server>pop.foo.com</server>
      </fetchmail_entry>
      <fetchmail_entry>
        <local_user>test</local_user>
        <password>bar</password>
        <protocol>IMAP</protocol>
        <remote_user>test</remote_user>
        <server>blah.com</server>
      </fetchmail_entry>
    </fetchmail>
    <from_header>test.com</from_header>
    <listen_remote config:type="boolean">>true</listen_remote>
    <local_domains config:type="list">
      <domains>test1.com</domains>
    </local_domains>
    <masquerade_other_domains config:type="list">
      <domain>blah.com</domain>
    </masquerade_other_domains>
    <masquerade_users config:type="list">
      <masquerade_user>
        <address>joe@test.com</address>
        <comment></comment>
        <user>joeuser</user>
      </masquerade_user>
      <masquerade_user>
        <address>bar@test.com</address>
        <comment></comment>
        <user>foo</user>
      </masquerade_user>
    </masquerade_users>
    <mta config:type="symbol">postfix</mta>
    <outgoing_mail_server>test.com</outgoing_mail_server>
    <postfix_mda config:type="symbol">local</postfix_mda>
    <smtp_auth config:type="list">
      <listentry>
        <password>bar</password>
        <server>test.com</server>
        <user>foo</user>
      </listentry>
    </smtp_auth>
    <use_amavis config:type="boolean">>true</use_amavis>
    <virtual_users config:type="list">
      <virtual_user>
        <alias>test.com</alias>
        <comment></comment>
        <destinations>foo.com</destinations>
      </virtual_user>
      <virtual_user>
        <alias>geek.com</alias>
        <comment></comment>
        <destinations>bar.com</destinations>
      </virtual_user>
    </virtual_users>
  </mail>
...
</configure>

```

## 9. Security settings

Using the features of this module, you will be able to change the local security settings on the target system. The local security settings include the boot configuration, login settings, password settings, user ad-

dition settings, and file permissions.

Configuring the security settings automatically corresponds to the *Custom Settings* in the security module available in the running system which lets you create your own, customized configuration.

### Example 4.35. Security configuration

See the reference for the meaning and the possible values of the settings in the following example.

```
<configure>
...
  <security>
    <console_shutdown>ignore</console_shutdown>
    <cwd_in_root_path>no</cwd_in_root_path>
    <displaymanager_remote_access>no</displaymanager_remote_access>
    <fail_delay>3</fail_delay>
    <faillog_enab>yes</faillog_enab>
    <gid_max>60000</gid_max>
    <gid_min>101</gid_min>
    <kdm_shutdown>root</kdm_shutdown>
    <lastlog_enab>yes</lastlog_enab>
    <encryption>md5</encryption>
    <obscure_checks_enab>no</obscure_checks_enab>
    <pass_max_days>99999</pass_max_days>
    <pass_max_len>8</pass_max_len>
    <pass_min_days>1</pass_min_days>
    <pass_min_len>6</pass_min_len>
    <pass_warn_age>14</pass_warn_age>
    <passwd_use_cracklib>yes</passwd_use_cracklib>
    <permission_security>secure</permission_security>
    <run_updatedb_as>nobody</run_updatedb_as>
    <uid_max>60000</uid_max>
    <uid_min>500</uid_min>
  </security>
...
</configure>
```

## 9.1. Password Settings Options

Change various password settings. These settings are mainly stored in the `/etc/login.defs` file.

Use this resource to activate one of the *encryption* methods currently supported. If not set, *DES* is configured.

*DES*, the Linux default method, works in all network environments, but it restricts you to passwords no longer than eight characters. *MD5* allows longer passwords, thus provides more security, but some network protocols don't support this, and you may have problems with NIS. *Blowfish* is also supported.

Additionally, you can setup the system to check for password plausibility and length etc.

## 9.2. Boot Settings

Use the security resource, you can change various boot settings.

- *How to interpret Ctrl + Alt + Del*

When someone at the console has pressed the CTRL + ALT + DEL key combination, the system usually reboots. Sometimes it is desirable to ignore this event, for example, when the system serves as both workstation and server.

- *Shutdown behavior of KDM*

Set who is allowed to shut down the machine from KDM.

## 9.3. Login Settings

Change various login settings. These settings are mainly stored in the '/etc/login.defs' file.

## 9.4. New user settings (useradd settings)

Set the minimum and maximum possible user ID and set the minimum and maximum possible group ID.

# 10. Monitor and X11 Configuration

FIXME

### Example 4.36. X11 and Monitor configuration

```
<configure>
...
  <x11>
    <color_depth config:type="integer">16</color_depth>
    <configure_x11 config:type="boolean">true</configure_x11>
    <display_manager>gdm</display_manager>
    <enable_3d config:type="boolean">true</enable_3d>
    <monitor>
      <display>
        <max_hsync config:type="integer">48</max_hsync>
        <max_vsync config:type="integer">90</max_vsync>
        <min_hsync config:type="integer">30</min_hsync>
        <min_vsync config:type="integer">50</min_vsync>
      </display>
      <monitor_device>DT-1536A</monitor_device>
      <monitor_vendor>DAYTEK</monitor_vendor>
    </monitor>
    <resolution>1024x768</resolution>
    <start_x11 config:type="boolean">true</start_x11>
    <window_manager>gnome</window_manager>
  </x11>
...
</configure>
```

# 11. Users

The root user and at least one normal user can be added during install using data supplied in the control file. User data and passwords (encrypted or in clear text) are part of the *configure* resource in the control file.

At least the root user should be configured during auto-installation, which will insure you will be able to login after installation is finished and of course it will insure nobody else can login into the system (in case the password is not set).

The two users in the following example are added during system configuration.

### Example 4.37. User configuration

```
<configure>
...
<users config:type="list">
  <user>
    <username>root</username>
    <user_password>password</user_password>
    <encrypted config:type="boolean">true</encrypted>
    <forename/>
    <surname/>
  </user>
  <user>
    <username>nashif</username>
    <user_password>password</user_password>
    <encrypted config:type="boolean">true</encrypted>
    <forename>Anas</forename>
    <surname>Nashif</surname>
  </user>
</users>
...
</configure>
```

The last example shows the minimal information required for adding users. More options are available for a more customized user account management. The data in `/etc/default/useradd` is used to determine the home directory of the user to be created in addition to other parameters.

## 12. Custom user scripts

By adding scripts to the auto-installation process you can customize the installation for your needs and take control in different stages of the installation.

In the auto-installation process, three types of scripts can be executed:

- Pre-Install Scripts

Executed before YaST2 does any real change to the system (Before partitioning and package installation)

### Pre-Install Scripts with confirmation

Pre-scripts are executed at an early stage of the installation. This means if you have requested to confirm the installation, the pre-scripts will be executed before the confirmation screen shows up. (*profile/install/general/mode/confirm*)

- Post-Install Scripts

These scripts are executed after AutoYaST has completed the system configuration and after it has booted the system for the first time.

Starting from SLES9, network is not available during post-installation script execution. To access the network, network device has to be configured in the script.

It is possible to execute the post scripts in an earlier phase while the installation network is still up and before AutoYaST configures the system. To run network enabled post scripts, the boolean property *network\_needed* has to be set to true.

- Final Scripts

### Note

Available starting from SLES9 only.

These scripts are executed during the initial boot process and after YaST2 has finished. The final scripts are executed using a special *init.d* script which is executed only once. The final scripts are executed toward the end of the boot process and after network has been initialized.

- Chroot environment post-install scripts

Chroot scripts are executed after all packages have been installed and before YaST2 boots for the first time and before the boot loader is installed. Although the name of this type of scripts might imply that the scripts executed in the chroot environment, the scripts are actually executed in the system before it was mounted. To make any changes to the system, the prefix */mnt* has to be used to any path.

It is also possible to run the *chroot scripts* in the installed system by adding the boolean element *chrooted*. When run chrooted, the scripts are executed later in the process than when not chrooted and after most configuration operations have been completed in system, i.e. writing bootloader configuration.

## New Feature

It is now possible to have the scripts outside the control file. The location of the control file can be specified using a URL similar to the syntax used for referencing the location of the control file. The location of the external script should be specified using the *location* element. This new option does not work with Chroot Scripts.

When added to the control file manually, the scripts have to be included in a *CDATA* element to avoid confusion with the file syntax and other tags defined in the control file.

### Example 4.38. Post script configuration

```
<?xml version="1.0"?>
<!DOCTYPE profile SYSTEM "/usr/share/autoinstall/dtd/profile.dtd">
<profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configns">
  <configure>
    <scripts>
      <chroot-scripts config:type="list">
        <script>
          <chrooted config:type="boolean">>true</chrooted>
          <filename>chroot.sh</filename>
          <interpreter>shell</interpreter>
          <source><![CDATA[
#!/bin/sh
echo "Testing chroot (chrooted) scripts"
ls
]]>
          </source>
        </script>
        <script>
          <filename>chroot.sh</filename>
          <interpreter>shell</interpreter>
          <source><![CDATA[
#!/bin/sh
echo "Testing chroot scripts"
df
cd /mnt
ls
]]>
          </source>
        </script>
      </chroot-scripts>
      <post-scripts config:type="list">
        <script>
          <filename>post.sh</filename>
          <interpreter>shell</interpreter>
          <source><![CDATA[
#!/bin/sh
echo "Running Post-install script"
/etc/init.d/portmap start
mount -a 192.168.1.1:/local /mnt
```

```

cp /mnt/test.sh /tmp
umount /mnt
]]>
        </source>
    </script>
</script>
    <script>
        <filename>post.pl</filename>
        <interpreter>perl</interpreter>
        <source><![CDATA[
#!/usr/bin/perl
print "Running Post-install script";
]]>
            </source>
        </script>
    </post-scripts>
</pre-scripts config:type="list">
    <script>
        <interpreter>shell</interpreter>
        <location>http://192.168.1.1/profiles/scripts/prescripts.sh</location>
    </script>
    <script>
        <filename>pre.sh</filename>
        <interpreter>shell</interpreter>
        <source><![CDATA[
#!/bin/sh
echo "Running pre-install script"
]]>
            </source>
        </script>
    </pre-scripts>
</scripts>
</configure>
</profile>

```

After installation is finished, the scripts and the output logs can be found in the directory `/var/adm/autoinstall`. The scripts are located in `scripts` and the output logs of the scripts are located in the `log` directory.

The log is the output resulting when executing the shell scripts using the following command:

```
/bin/sh -x <script_name> 2> /var/adm/autoinstall/logs/<script_name>.log
```

## 13. System variables (Sysconfig)

Using the `sysconfig` resource, it is possible to define configuration variables in the `sysconfig` repository (`/etc/sysconfig`) directly. `Sysconfig` variables, offer the possibility to fine-tune many system components and environment variables exactly to your needs.

Refer to the handbook for more details about the many configuration options available in `/etc/sysconfig`

The following example shows how a variable can be set using the `sysconfig` resource.

To configure a variable in a `sysconfig` file, the following syntax can be used:

### Example 4.39. Sysconfig Configuration

```

<sysconfig config:type="list" >
  <sysconfig_entry>
    <sysconfig_key>XNTPD_INITIAL_NTPTDATE</sysconfig_key>
    <sysconfig_path>/etc/sysconfig/xntp</sysconfig_path>

```

```
<sysconfig_value>ntp.host.com</sysconfig_value>
</sysconfig_entry>
<sysconfig_entry>
  <sysconfig_key>HTTP_PROXY</sysconfig_key>
  <sysconfig_path>/etc/sysconfig/proxy</sysconfig_path>
  <sysconfig_value>proxy.host.com:3128</sysconfig_value>
</sysconfig_entry>
<sysconfig_entry>
  <sysconfig_key>FTP_PROXY</sysconfig_key>
  <sysconfig_path>/etc/sysconfig/proxy</sysconfig_path>
  <sysconfig_value>proxy.host.com:3128</sysconfig_value>
</sysconfig_entry>
</sysconfig>
```

Both relative and absolute paths can be provided. If no absolute path is given, it is treated as a sysconfig file under the `/etc/sysconfig` directory.

## 14. Adding complete configurations

For many applications and services you might have prepared a configuration file which should be copied in a complete form to some location in the installed system. This is for example if you are installing a web server and have a *ready to go* server configuration file (`httpd.conf`).

Using this resource, you can embed the file into the control file by specifying the final path on the installed system. YaST2 will copy this file to the specified location.

### Example 4.40. Dumping files into the installed system

```
<files config:type="list">
  <config_file>
    <file_path>/etc/httpd/httpd.conf</file_path>
    <file_contents>

<![CDATA[
some content
]]>

  </file_contents>
</config_file>
</files>
```

A more advanced example is shown below. This configuration will create a file using the content supplied in `file_contents` and will change the permissions and ownership of the file. After the file has been copied to the system, a script is executed which can be used to manipulate the file and prepare it for the environment of the client.

### Example 4.41. Dumping files into the installed system

```
<files config:type="list">
  <config_file>
    <file_path>/etc/someconf.conf</file_path>
    <file_contents>

<![CDATA[
some content
]]>

  </file_contents>
  <file_owner>nashif.users</file_owner>
  <file_permissions>444</file_permissions>
```

```

        <file_script>
        <interpreter>shell</interpreter>
        <source>

<![CDATA[
#!/bin/sh

echo "Testing file scripts" >> /etc/someconf.conf
df
cd /mnt
ls
]]>

        </source>
    </file_script>
</config_file>
</files>

```

## 15. Miscellaneous hardware and system components

In addition to the core component configuration, like network authentication and security, AutoYaST2 offers a wide range of hardware and system configuration which is available by default on any system installed manually and in an interactive way. For example, it is possible to configure printers, sound devices, TV cards and any other hardware components which have a module within YaST2.

Any new configuration options that will be added to YaST2 will be automatically available as an auto-installation resource.

### 15.1. Printer

Although Printer configuration, like other configurations can be done manually, it is recommended to use the Configuration System to create such a configuration because of the complexity and the range of options offered by such modules.

Using the configuration system will guarantee that the options provided are consistent. The following is an example of a configuration section which was created using the configuration system.

#### Example 4.42. Printer configuration

```

<configure>
....
  <printer>
    <default>lp</default>
    <printcap config:type="list">
      <printcap_entry>
        <cups-state>void</cups-state>
        <ff config:type="boolean">>true</ff>
        <info></info>
        <location></location>
        <lprng-state>changed</lprng-state>
        <name>lp</name>
        <options>
          <job-sheets>none,none</job-sheets>
        </options>
        <raw config:type="boolean">>true</raw>
        <type>yast2</type>
        <uri>parallel:/dev/lp0</uri>
      </printcap_entry>
    </printcap>
  </printer>
....
</configure>

```

## 15.2. Sound devices

An example of sound configuration created using the configuration system is shown below.

### Example 4.43. Sound configuration

```
<configure>
....
  <sound>
    <autoinstall config:type="boolean">true</autoinstall>
    <modules_conf config:type="list">
      <module_conf>
        <alias>snd-card-0</alias>
        <model>M5451, ALI</model>
        <module>snd-ali5451</module>
        <options>
          <snd_enable>1</snd_enable>
          <snd_index>0</snd_index>
          <snd_pcm_channels>32</snd_pcm_channels>
        </options>
      </module_conf>
    </modules_conf>
    <volume_settings config:type="list">
      <listentry>
        <Master config:type="integer">75</Master>
      </listentry>
    </volume_settings>
  </sound>
....
</configure>
```

---

# Chapter 5. Network Based Installation

The installation method using AutoYaST provides a way to automatically and identically install groups of systems. The first step when preparing AutoYaST installations is deciding how you want the systems at your site to be installed. For example, the following scenario would be ideal to set up and perform automated installations:

- You need to install SuSE Linux on 50 new systems.
- The development department owns 30 out of the 50 new dual processor and SCSI systems, and its systems must be installed as clients with development software.
- The sales department owns 20 out of the 50 new, uni-processor IDE based systems and its systems must be installed as clients with end user software and office tools.

Prerequisites:

- A boot server on the same Ethernet segment
- An install server with the SuSE Linux OS
- An AutoYaST configuration server that defines rules and profiles.

## 1. Boot Server

### 1.1. Introduction

The boot server is composed of DHCP or BOOTP and TFTP servers. In some cases the boot server has to be in the same network segment as the client due to the fact that DHCP or TFTP packets will not be forwarded across routers.

For administrative purposes, booting from a network card (NIC) is much more flexible than booting from a floppy or other types of media. In order to use this boot method, the client's NIC needs to have a boot PROM that is able to communicate with a DHCP or BOOTP server to receive configuration parameters such as network addresses and boot server location.

PXE (Pre-boot Execution Environment) is a protocol designed by Intel that allows computers to boot through the network. PXE is stored in the ROM of new generation network cards. When the computer boots up, the BIOS loads the PXE ROM in the memory and executes it. A menu can be displayed, allowing the computer to boot an operating system loaded through the network.

To install a client via Pre-Boot Execution Environment (PXE) you don't need a PXE server! PXE sends a BOOTP request to get an IP address and other network information and a bootloader program to the client. You can either use a BOOTP server or a DHCP and TFTP server.

Etherboot [<http://etherboot.sourceforge.net/>] and netboot [<http://www.han.de/~gero/netboot.html>] are capable of creating a PROM binary (which must still be programmed onto a PROM) and a corresponding "tagged" TFTP boot image which includes a kernel and the initial ramdisk (initrd).

Unlike a PXE ROM, which loads an intermediate network boot program, these other network booting solutions are designed to load a specially-marked Linux kernel directly. There are only three differences in the server configuration:

- You don't need PXELinux at all.
- In the DHCP configuration, the filename parameter contains the name of the client kernel file.
- The client kernel file needs to be processed by the **mknbi** program to correctly recognized by the ROM.

One or two protocols (depending on how you set it up) are used to boot a machine off the network. The first, DHCP, is a protocol to allow hosts to automatically configure their network parameters from a server, and is commonly used on networks to make IP address allocation and network administration easier. You'll only need to set this up if you use Etherboot or PXE. The second, TFTP, is a stripped down FTP protocol, commonly used in boot loaders where a full FTP client would be too large. The server machine (Boot server) must run servers for at least TFTP, and DHCP too if you want to load an image off the network.

## 1.2. Required Services on the Boot Server

### 1.2.1. DHCP

Install the DHCP server from ISC (<http://www.isc.org/>) by using the package available in the *SuSE* distribution. Configure the DHCP server parameter in `/etc/sysconfig/dhcpd` and make sure you have a working configuration file `/etc/dhcpd.conf`.

Note that you'll need the Ethernet address of your client machine before you can use this DHCP configuration. There are several ways to get this information. If the client machine already has Linux installed, use **ifconfig** and look for the *HWaddr* value.

The PXE ROM will often show such information either in the configuration screen or during an attempt to boot from the network. If none of those work, use **arpwatch** or **tcpdump** on the server to watch the network packets from the client as the client tries to network boot.

### 1.2.2. TFTP

PXE requires a special TFTP server. Read `/usr/share/doc/packages/syslinux/pxelinux.doc` from the already mentioned *syslinux* package for details.

The INETD based TFTP server cannot reliably handle much more than 64 clients at a time! With more clients not all of them will get an answer from your TFTP and you will see syslog messages like this:

```
tftpd: read: Connection refused.
```

To overcome this problem you can use *atftp* which is available as a package. This TFTP server can run as stand-alone daemon.

The TFTP server directory `/tftpboot` should look like the following:

#### Example 5.1. Tftpboot directory contents

```
/tftpboot/initrd
pxelinux.0
linux
```

See next section for how to get the files `linux` and `initrd`.

## 1.3. Boot Server Configuration

### 1.3.1. Kernel and Initial Ramdisk

For network booting and other configurations, it is recommended to use the images available on the first *SuSE* CD-ROM in the directory `boot/loader`. The initial ramdisk (`initrd`) contains all kernel modules needed for successful installation. In special cases, you might need to build you own kernel or use special kernels available on the CD-ROM.

Copy the kernel image and the initial ramdisk to the TFTP directory (`/tftpboot`). Those files will be called from the configuration files of either PXE or GRUB.

### 1.3.2. DHCP Configuration Examples

To allow the specification of the source media location when booting over the network, *root-path* options of DHCP can be used.

#### Example 5.2. `/etc/dhcpd.conf` with the *root-path* option

```
subnet 192.168.1.0 netmask 255.255.255.0
{
    range dynamic-bootp 192.168.1.100 192.168.1.110;
    option broadcast-address 192.168.1.255;
    option routers 192.168.1.1;
    filename "vmlinuz.nbi";
    option root-path "/tftpboot/CDs";

    next-server 192.168.1.1;
}
```

One more example shows how the DHCP server can send an image to the client, depending on the type of the requesting client (PXE or Etherboot).

#### Example 5.3. DHCP server configuration with PXE and Etherboot options

```
ddns-update-style none;
allow bootp;
allow booting;

subnet 192.168.1.0 netmask 255.255.255.0 {
    range dynamic-bootp 192.168.1.100 192.168.1.110;
    option domain-name "cluster.suse.de";
    option routers 192.168.1.240;
    option subnet-mask 255.255.255.0;
    option broadcast-address 192.168.1.255;
    filename "vmlinuz-node.nbi";
    option root-path "/local/CD1";
}

group {
    next-server 192.168.1.240;
    use-host-decl-names on;

    host n1 {
        hardware ethernet 00:00:1c:b5:6e:71;
        fixed-address n1;
        if substring (option vendor-class-identifier, 0, 9) = "PXEClient" {
            filename "/tulip.lzpxe";
        } else if substring (option vendor-class-identifier, 0, 9) = "Etherboot" {
            filename "/vmlinuz-node.nbi";
        }
    }
}
```

```

    }
  }
  host n2 {
    hardware ethernet 00:00:1c:b5:72:ea;
    fixed-address n2;
    if substring (option vendor-class-identifier, 0, 9) = "PXEClient" {
      filename "pxelinux.0";
    } else if substring (option vendor-class-identifier, 0, 9) = "Etherboot" {
      filename "/vmlinuz-node.nbi";
    }
  }
}

```

### 1.3.3. Booting with PXE

PXE can load a program into the client's memory and start it (the bootloader). The bootloader then loads its configuration file via TFTP from the server defined in *next-server* in `/etc/dhcpd.conf`.

The bootloader configuration file determines whether a client boots from its local hard disk or over the network.

The following are example configuration files for both cases:

#### Example 5.4. Configuration file for PXELINUX net boot

```

default linux
serial 0,9600n8
label linux
  kernel linux
  append console=ttyS0,9800 console=tty0 load_ramdisk=1 initrd=initrd autoyast=nfs://nfsserv/file.xml

```

Boot from local hard disk (filename default):

#### Example 5.5. Configuration file for PXELINUX local boot

```

default linux
label linux
  localboot 0

```

The file `pxelinux.0` tries to read several configuration files. It uses the first one it finds. The filenames it looks for are determined by the IP address of the client it is running on. It converts the four decimal number parts of an IP address (they are divided by dots) into hexadecimal numbers and concatenates them. Example: IP address 192.168.0.11 gets converted into `C0 A8 00 0B` (without the spaces).

The search for files starts at `COA8000B` and proceeds by removing one digit from the right (leaving `COA8000`) and so forth. When all digits are removed it will try as last resort the filename default.

On your TFTP server, this algorithm can be used to tell each single machine how to boot:

#### Example 5.6. PXELINUX Configuration

```

/tftpboot/pxelinux.cfg/
COA8000B -> default.netboot-8.0

```

```
COA8000C -> default.netboot-8.1
default.netboot-8.0
default.netboot-8.1
default
```

This is important if you install a lot of machines at the same time. You can watch the syslog file on your TFTP server and whenever a client got its initial RAM disk transmitted, you can remove the symlink for that machine from the `pxelinux.cfg` directory. This forces the client to load the default configuration which says: "Boot from local disk!" when the machine reboots after AutoYaST is done. (This process can be automated by monitoring the network or *syslog* for booting clients and removing the links with a script running in the background)

### 1.3.4. Booting with Etherboot

Etherboot, as mentioned earlier, is the piece of software that loads off of a floppy or boot EPROM and loads the GRUB, the second-stage loader, off the server. It is a freely-available, open source package which also can be found with SuSE Linux.

To use Etherboot with a boot EPROM, consult the Etherboot documentation. The Etherboot package contains pre-compiled images for boot EPROM and floppies.

To create a bootable floppy for network installation copy the image in a floppy:

```
cat /usr/lib/etherboot/dsk/<NIC> > /dev/fd0
```

Once you have a bootable floppy, test-boot it. You should receive a prompt asking whether to boot from (L)ocal or (N)etwork. Choose network. If you haven't set up a DHCP server yet, it should hang - but at least Etherboot works.

To boot using Etherboot, you need to create the tagged image using **mknbi-linux** which is part of the *mknbi* package. Assuming you have copied the linux image and the initial ramdisk to a directory (images) below `/tftpboot`, the following command line will be used to create the image:

```
mknbi-linux images/linux images/initrd --output=linux.nbi
```

Using the `--param` command line option, you can set the kernel parameter in case you don't have them applied somewhere else.

```
mknbi-linux images/linux images/initrd --output=linux.nbi --param='autoyast="http://192.168.1.1/profiles" .....
```

An alternative for adding the kernel parameters while creating the image which is not optimal for multiple clients needing different parameters is to make the DHCP server send the parameters during booting using a special option in `/etc/dhcpd.conf`.

You need to define two custom options (T128 and T129) in the DHCP configuration as described in the following example:

#### Example 5.7. Etherboot with kernel command line options via DHCP

```
allow bootp;
```

```

allow booting;

option T128 code 128 = string;
option T129 code 129 = string;
..
subnet 192.168.1.0 netmask 255.255.255.0 {
    range dynamic-bootp 192.168.1.100 192.168.1.150;

    option routers 192.168.1.240;
    option subnet-mask 255.255.255.0;
    option broadcast-address 192.168.1.255;
    option domain-name-servers 192.168.1.240;
    next-server 192.168.1.1;
}

group {

    next-server 192.168.1.1;
    option root-path "/SuSE/CDs/latest";
    use-host-decl-names on;
    option T128 e4:45:74:68:00:00;
    .
    .
    .
    host athlon {
        hardware ethernet 00:50:ba:e8:45:5b;
        fixed-address avicenna;
        option T129 "autoyast=http://192.168.1.1/profiles/  install=nfs://192.168.1.1/SuSE/CDs/latest  vga=791";
        filename "vmlinuz.nbi-9.0";
    }
    ..
    .
    .
}

```

### 1.3.5. GRUB Floppy

To create a GRUB boot floppy with the menu interface, the easiest way is:

1. Create filesystem in your floppy disk. For example:

```
$ mke2fs /dev/fd0
```

2. Mount it on somewhere, say, /mnt.
3. Copy the GRUB images from /usr/lib/grub/ to /mnt/boot/grub. Only *stage1*, *stage2* (Use *stage2.netboot* in this case) and *menu.lst* are necessary. You may not copy "stage1.5"s.
4. Unmount the floppy.
5. Run the following command:

```
$ /usr/sbin/grub --batch <<EOT
    root (fd0)
    setup (fd0)
    quit
EOT
```

The file `menu.list` can have multiple entries. the following example shows different ways for booting the client over the network:

#### Example 5.8. GRUB menu.lst

```

color white/blue black/light-gray
default 0
timeout 8
framebuffer 1

title autoinstall-bootp
    bootp
    root (nd)
    kernel (nd)/linux vga=791 install=nfs://192.168.1.1/CDs/9.0
    autoyast=http://192.168.1.1/profiles/
    initrd (nd)/initrd

title autoinstall-ip
    ifconfig --address=192.168.1.50 --server=192.168.1.1
    root (nd)
    kernel (nd)/linux install=nfs://192.168.1.1/work/CDs/full-i386 ip=192.168.1.50 netmask=255.255.255.0
    initrd (nd)/initrd

title floppy
    root (fd0)
    chainloader +1

```

## NIC Support

GRUB does not support all network interfaces and having all network interfaces enabled in the `/usr/lib/grub/stage2.netboot` might have some side effects when booting certain network devices.

### 1.3.6. Combining Etherboot with GRUB

GRUB consists of several images: two essential stages, optional stages called Stage 1.5, and two network boot images. Here is a short overview of the network boot images:

**nbgrub.** This is a network boot image for the Network Image Proposal used by some network boot loaders, such as Etherboot. This is mostly the same as Stage 2, but this also sets up a network and loads a configuration file from the network.

**pxegrub.** This is another network boot image for the Pre-boot Execution Environment used by several Netboot ROMs. This is identical to *nbgrub*, except for the format.

Those images are the same as the normal Stage 2, except that they set up a network automatically, and try to load a configuration file from the network, if specified. The usage is very simple: If the machine has a PXE ROM, use ``pxegrub'`. If the machine has a NBI loader such as Etherboot, use ``nbgrub'`. There is no difference between them but their formats. As how to load a second stage image you want to use should be described in the manual on your Net Boot ROM, please refer to the manual, for more information.

However, there is one thing specific to GRUB. Namely, how to specify a configuration file in a BOOTP/DHCP server. For now, GRUB uses the tag *150*, to get the name of a configuration file. The following is an example about a DHCP configuration:

#### Example 5.9. Grub image via DHCP

```

option domain-name "example.org";
option domain-name-servers 10.0.0.1;
option T150 code 150 = string;

subnet 10.0.0.0 netmask 255.255.255.0 {
    range 10.0.0.128 10.0.0.192;
    option routers 10.0.0.1;
    option broadcast-address 10.0.0.255;
}

```

```
# GRUB network boot stuff
filename "/tftpboot/nbgrub";
server-name "10.0.0.1";
option T150 "(nd)/tftpboot/menu.lst";
}
```

Note that you should specify the drive name (*nd*) in the name of the configuration file. That is because you can change the root drive before downloading the configuration from the TFTP server, when the preset menu feature is used.

PXEGRUB can be configured in a similar way when booting using a PXE enabled NIC.

## 2. Installation Server

### 2.1. SUSE Linux

User intervention depends much on how the server side of a network installation is prepared. In a full network installation, you have only to turn the client on to initiate the auto-installation process.

The installation server should export the *SuSE* Linux distribution's files via NFS. Create a directory on a filesystem with enough free space (several gigabytes) and copy the contents of the CD-ROMs into this directory. This directory is then to be exported via NFS (via an appropriate entry in `/etc/exports`) or it should be made available via other supported installation protocols like HTTP and FTP. The following steps describe how to create an installation repository:

Login on the machine designated as installation server and create a directory to hold the *SuSE* Linux distribution files, i.e. `/usr/local/SuSE/current`.

In our example `/usr/local/SuSE/current` is the base directory for the *SuSE* Linux distribution. The location of this directory can be specified in the *info* file or on the command line of the kernel (see below) using the *install* keyword. (i.e. `install=nfs://192.168.1.1/usr/local/SuSE/current`)

Now copy the files from all CDs into the *current* directory or just copy those CDs required for the installation. Make sure that all packages needed for the installation are copied.

Repeat this sequence for all other CDs. The directory can have 2 different structures which can be used for installation:

- The content of all CDs is copied into one directory and thus creating single directory structure with a subdirectory *suse* which included all the packages. This type of structure is recommended as it is easier to manage and will provide a true, single source installation medium.

To make the directory look like a single medium for the client, it is possible to re-create the package database available on the first CD using the script `create_package_descr` which is available in `/usr/bin/`. Install the package *autoyast2-utils* to make this script available on your system.

- Copy the CDs into sub-directories named after the CD number, i.e. CD1, CD2, etc.

Using this structure you will still be able to perform NFS installations, but the single directories will be treated as if they were different mediums.

After you have copied the CDs into the installation directory, make sure it is exported via NFS or available using other installation protocols. You can achieve this with YaST2 using the NFS server module.

Additionally, you need to make the following services start every time the system boots (Other installa-



```
-- suse
  |-- i586
  |-- setup
  |-- src
-- yast
  |-- core9
```

The media and product description is splitted to a set of files, separating the media preparation data from the contents (product) and making it possible to combine several products on a single media.

At top-level of a media, a directory `/media.1/` should exist. If it does not exist, the presence of the correct media can not be verified. This may be convenient for an on-line media which just provides a set of packages.

In this case, no verification takes place. The numeric extension depends on the media number in case of splitted medias. The first media has `.1`, the second `.2`, and so on.

This allows merging all medias of a splitted set into a single directory. YaST always knows which media to expect and can thereby directly access the correct media directory.

#### 2.2.2.1.1. Files inside boot/

the directory `boot/` contains installation images and floppy images that can be used to create boot and installation floppies. The `root` files contains a complete (cramfs based) root filesystem for YaST. This file contains the actual installer. The `root` file is fetched by **linuxrc** from the installation source and is mounted in the installation environment. **Linuxrc** starts the installer from within this file.

The directory `boot/loader` contains the kernel and the initial ramdisk used for installation. It also contains the `isolinux` files used for creating the CD.

#### 2.2.2.1.2. Files inside media.N/

Inside the `media.N/` directory the files `media` and `products` must exist. Optionally, a file named `patches` may exist to denote a media with patches (e.g. for YaST online update).

- The `/media.N/media` file

The `media` file contains the media identifier needed to determine correctness when using removable media. In case of splitted media, it must be present on every media of the set.

This should contain a key to quickly identify correctness of the inserted media. It is not shown to the user but should contain human-readable data for debugging purposes.

- The `products` file

The `products` file contains directory specifications for each product. In case of splitted media, it must be present of the first media of the set.

- The `patches` file

The `patches` file contains a single directory specification for the root of the `patches` directory tree. In case of splitted media, it must be present of the first media of the set.

- The `info.txt` file

This file contains any licensing information that should be presented to the user when YaST is started. If not present, no license screen is shown. On the SLES CD, it contains the EULA.

The identification data is stored inside the file on purpose. It could also be encoded in the file name (older SuSE media did it). But this requires a directory scan for file access and should be avoided.

By storing the vendor name in the file, the timestamp can be kept vendor specific. (It's the name of the vendor who created the media which might be different from a product vendor! It's just used as an additional key for media identification.)

The media count is needed if the installation data is split up on multiple (identical) medias. The media file on the first media should contain the total count of medias.

The media count is a numerical value (all characters are digits). It is an optional information on the other media.

A fourth line may contain flags further describing the media. In order to distinguish the flags from the count line, the flags values start with a letter.

All media of a media-set must have identical vendor and data information in the media file.

### Example 5.10. media directory

```
# ls -l media.1
info.txt
media
products

# cat media.1/media
SuSE Linux AG
20040408195328
1

# cat media.1/products
/ SUSE-Linux-SLES-i386 9
```

#### 2.2.2.1.3. The contents files

This file resides inside the product directory as specified by the products file on the media. It contains all product-specific data to describe and identify the contents of the product. If there was no products file, the product directory defaults to the root directory on the media.

The content file might be missing if the media does not contain a product (but just a set of packages).

### Example 5.11. The contents file

```
# cat content
PRODUCT SUSE SLES
VERSION 9
DISTPRODUCT SUSE-Linux-SLES-i386
DISTVERSION 9-0
BASEPRODUCT SUSE CORE
BASEVERSION 9
YOUTYPE business
YOUPTH i386/update/SUSE-SLES/9
YOUURL http://www.suse.de/cgi-bin/suseservers.cgi
VENDOR SUSE LINUX AG
RELNOTESURL http://www.suse.com/relnotes/i386/SUSE-SLES/9/release-notes.rpm
ARCH.i686 i686 i586 i486 i386 noarch
ARCH.i586 i586 i486 i386 noarch
ARCH.i486 i486 i386 noarch
ARCH.i386 i386 noarch
DEFAULTBASE i386
```

```
REQUIRES distribution-release
LINGUAS de en
LABEL SUSE SLES Version 9
LABEL.de SUSE SLES in der Version 9
DESCRDIR suse/setup/descr
DATADIR suse
FLAGS update
LANGUAGE en_US
TIMEZONE America/Los_Angeles
```

### 2.2.2.2. The order file

The order file defines which sources are needed for installation and their priority for installation. A typical example for an order file is given here:

```
# yast/order: priority of installation sources
#
# source-      product
# description  path
/
/yast/core9
```

The order file is ASCII, line based, '#' at the beginning of a line denote a comment line.

Each non-comment line should contain two (tab separated) directory specifications. If the second one is omitted, it defaults to "/".

The first directory specifies the location of the description. The second directory specifies the location of the product as defined here. For CD/DVD bases products, this is usually "/". But for network installations, or if several product are placed on a single CD, each product needs a separate path.

You can even specify a full URL (e.g. "nfs://my-nfs-server.domain.org/product/CD1") in the second column. During installation, you can't switch the type of media. If your installer source is CD, every other source must be CD based. If your installer source is NFS, every other source is expected to be on the same NFS server.

### 2.2.2.3. The instorder file

As stated above, the `/yast/order` file lists the sources in priority order. So a package from a source listed earlier in this file overrides a package (of the same name) from a later source.

But the `/yast/order` also defines the installation order, which might not be wanted when the 'base' packages are on a lower-priority source.

This is where `/yast/instorder` comes into play. This defines the installation order by repeating the entries of the first column of `/yast/order` in the right order.

A typical example for an instorder file is given here:

```
# yast/instorder: order of installation sources
# this example is used on SLES CDs.
#
/
/yast/core9
```

## 2.2.3. Setting it all up

Combining multiple sources requires that all sources comply to the UnitedLinux media description

standard.

In the source directory, copy all SLES and CORE into separate directories (CDs can also be copied into one single directory, but to keep a clean structure, CDs can be copied into separate directories, i.e. using the following scheme: CORE9/CD1, CORE9/CD2, CORE9/CD3 . CORE9/CD4, CORE9/CD5 and SLES/CD1.)

Upon boot, Linuxrc requires the presence of the boot directory (which contains the `root` file), the `media.N` directory the `control.xml` file and the `content` file. Having those files in the root of the source will insure that linuxrc can start the YaST installer.

Once YaST has started, it will search the root of source for installation files using values from the `content` file name. However, to detect if multiple sources are involved, YaST first search for the `order` and `instorder` in the `yast` directory. The files in the `yast` directory will reroute YaST and direct it to search for the installation files and media description in different locations than root of the source.

On the installer source create a `yast/order` as described above and enter the location of the description data and packages. Alternatively, you can copy the description data of all sources to separate directories in the `yast` directory (This is the case on the SLES CD which contains the description data for CORE to support multiple sources using CDs).

In the 'order' example above, the 'order' directory structure looks as follows:

```

yast
-- core9
  -- content
  -- media.1
    -- info.txt
    -- media
    -- products
  -- suse
    -- setup
      -- descr
        -- MD5SUMS
        -- common.war
        -- directory.yast
        -- packages
        -- packages.DU
        -- packages.cs
        -- packages.de
        -- packages.en
        -- packages.es
        -- packages.fr
        -- packages.hu
        -- packages.sk
        -- selections
  -- instorder
  -- order

```

YaST now takes this description instead of the one from the *real* media for the installation. So when asking for a specific media, this media must match the `media.1/media` file from the `order` directory.

All dependencies (package or selection) are fulfilled by looking at all installation sources. If multiple sources provide a dependency, the source listed first in the 'order' file wins. (The installation order equals the installation priority currently).

## 2.2.4. Example using SLES 9

You should at least copy the first CD from both CORE 9 and SLES 9 sets, depending on what selection of software you want to install.

On the server side, create a directory which will serve as the installation source and make sure it is exported via NFS when creating an NFS source or make it available using the other supported protocols. This directory will be used later to specify the installation source using **linuxrc**.

The following script illustrates what directories need to be created and where you should copy the data from the CDs. In this script, it is assumed that you have ISO images. In most cases you will have CDRoms instead. Do not use this script as provided. If you wish to use it, please make sure you have changed the directory names to something suitable to your environment.

```
#!/bin/sh

instsource="/exports/sles9"
#
# Create CD directories
#
cd $instsource
mkdir -p sles9-i386/CD1
mkdir -p core9-i386/CD{1,2,3,4,5}

#
# Copy SLES CD
#
cd sles9-i386/CD1

mount -oloop /iso/SLES-9-i386-CD1.iso /mnt
cp -a /mnt/* .
umount /mnt

#
# back to root of source
#
cd ../../

#
# Copy UL CDs
#

# 1
cd core9-i386/CD1
mount -oloop /iso/CORE9-i386-CD1.iso /mnt
cp -a /mnt/* .
umount /mnt

# 2
cd ../CD2
mount -oloop /iso/CORE9-i386-CD2.iso /mnt
cp -a /mnt/* .
umount /mnt

# 3
cd ../CD3
mount -oloop /iso/CORE9-i386-CD3.iso /mnt
cp -a /mnt/* .
umount /mnt

#
# Copy all other CDs...
#

#
# back to root of source
#
cd ../../

#
# Now we have to symlink some data to make this
# a multiple source directory
#

# Then the boot directory with the installation image
#
ln -s sles9-i386/CD1/boot

# The content file and the media directory
#
ln -s sles9-i386/CD1/content
ln -s sles9-i386/CD1/control.xml
ln -s sles9-i386/CD1/media.1

# We are almost done..
# Now we'll adapt the order files.
# Fields of the order files are TAB delimited

mkdir -p yast

printf "/sles9-i386/CD1\t/sles9-i386/CD1\n" > yast/order
printf "/core9-i386/CD1\t/core9-i386/CD1\n" >> yast/order
```

```
printf "/sles9-i386/CD1\n" > yast/instorder
printf "/core9-i386/CD1\n" >> yast/instorder

#
# End
#
```

After you have gone through all steps, you will have a structure similar to the one shown below.

```
.
|-- sles9-i386
|   |-- CD1
|       |-- boot
|       |-- docu
|       |-- media.1
|       |-- suse
|       |-- yast
|-- core9-i386
|   |-- CD1
|   |-- CD2
|   |-- CD3
-- boot -> sles9-i386/CD1/boot
-- media.1 -> sles9-i386/CD1/media.1
-- content -> sles9-i386/CD1/content
-- control.xml -> sles9-i386/CD1/control.xml
-- yast
```

And the root of the source will have the following content:

```
# ls -l
sles9-i386
core9-i386
boot
content
control.xml
media.1
yast
```

## 2.2.5. SAMBA Sources

SAMBA source are a special case because it is not possible to specify a directory below a share.

To create a SAMBA share, first you need to create a directory which will host the source tree which will should be exported as a share which will be used to specify the source in linuxrc or on the kernel command line.

Copy the CDs as specified above. Create two directories, i.e. *SLES* and *CORE* under the top directory which we will call *SLES9* in this example. Copy SLES CD1 into *SLES/CD1* and SLES CDs 2-6 (CORE 1-5) into *CORE/CD{1, 2, 3, 4, 5}*

Next you will need to add all CDs as shares, using the following scheme: SLES CDs (1 CD in this case) will be exported as a share using *SLESCD1* and the CORE CDs (5 CDs) will be exported using *CORECD1* to *CORECD5*

Then Copy the following files and directories from *SLES/CD1* to the root of the tree: *content*, *media.1*, *control.xml* and *boot*

Next you need to create the order files in the directory *yast*. Create the directory *yast* and using an editor create the file *order* and add the following lines:

```
/SLES/CD1 smb://user:password@hostname/SLESCD1
/CORE/CD1 smb://user:password@hostname/CORECD1
```

The instorder file has the following content:

```
/SLES/CD1
/CORE/CD1
```

When installing you only need to enter the following URI to access the source tree:

```
smb://user:password@hostname/SLES9
```

When done, you should be able to see the exported tree with **smbtree**. More or less, the host with the source tree should have the following shares:

```
root@avicenna:~ # smbtree
Password:
NASHIF
  \\MASTER
    \\MASTER\C$           Default share
    \\MASTER\ADMIN$      Remote Admin
    \\MASTER\F$          Default share
    \\MASTER\SLES
    \\MASTER\CORECD1
    \\MASTER\CORECD2
    \\MASTER\CORECD3
    \\MASTER\CORECD4
    \\MASTER\CORECD5
    \\MASTER\SLESCD1
    ....
```

## 3. Configuration Server

A configuration repository holds the control files for multiple machines. The control files can have any file names, which have to be specified at the boot time of a client. To avoid supplying the profile name for every client, you can only define the directory of the control files. If a directory is specified, then the client tries to load a file with a name matching its IP address in HEX mode. This has the advantage that you will be dealing with consistent file names rather than IPs as file names which might lead to some confusion.

The configuration repository is the same directory you have to define if you are using the configuration system for creating control files.

### 3.1. HTTP Repository

To be able to use the HTTP protocol to retrieve control file while auto-installing, you need a working HTTP server on the server side. Install *Apache* or your favorite web server and enable it using YaST2. Normally the web server root directory resides in `/srv/www/htdocs` so you need to create a sub-directory below the root directory of the web server which will be your configuration repository.

### 3.2. NFS Repository

Create a directory and make it available via NFS to the clients by exporting it. This directory may for example be in the same place where you have copied the CDs. (i.e. `/usr/local/SuSE`)

### 3.3. TFTP Repository

By default the TFTP directory is available under `/tftpboot` which can also contain boot images if you are booting over network. Do not forget to enable TFTP in the Inetd configuration file (`/etc/inetd.conf`). *Inetd* configuration can be done using YaST2.

---

# Chapter 6. Rules and Classes

## 1. Rule based auto-installation

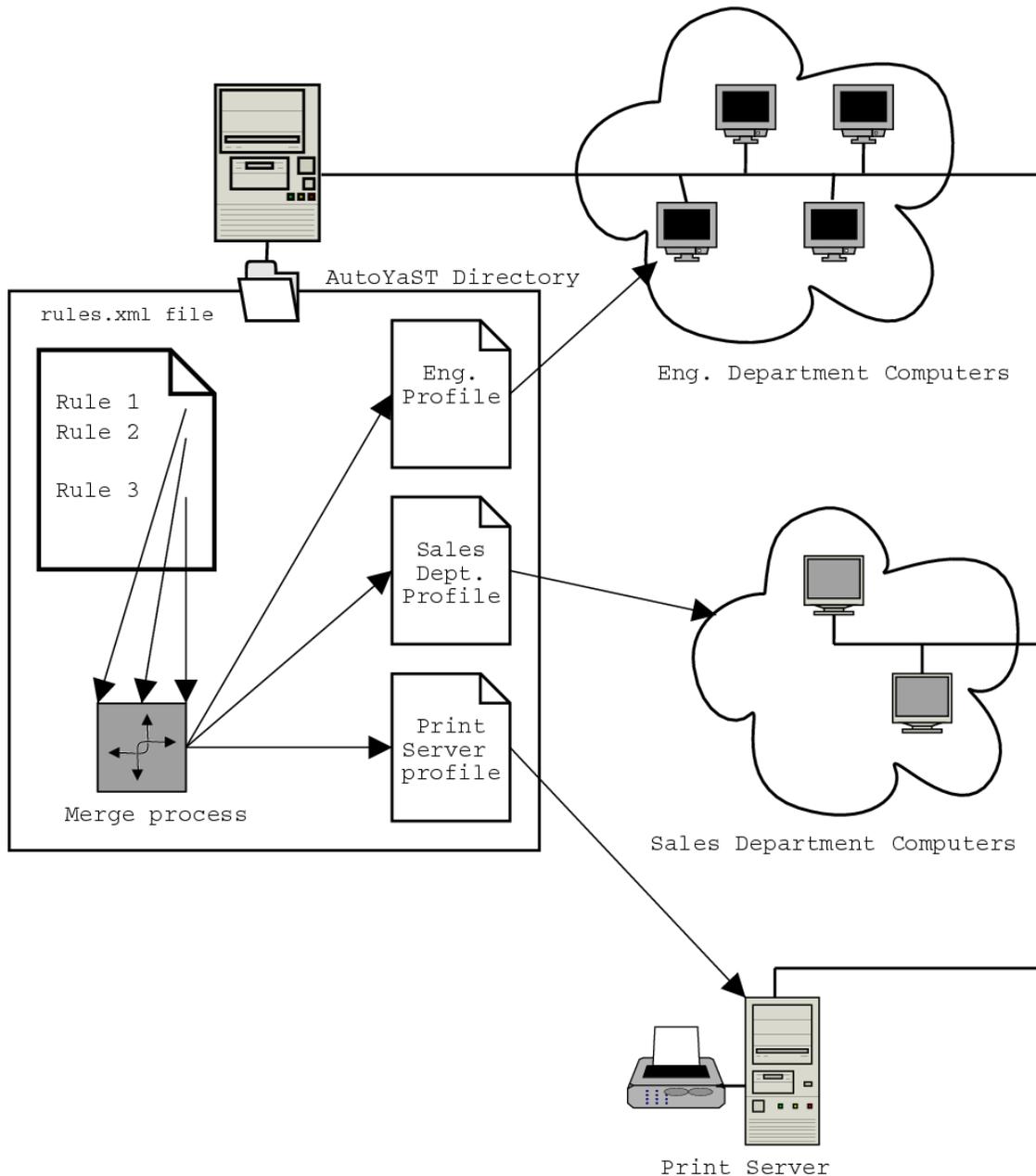
Rules offer the possibility to configure a system depending on system attributes by merging multiple control file during installation. The rules based installation is controlled by a rules file.

The rules file is an XML based file that contains rules for each group of systems (or single systems) that you want to automatically install. A set of rules distinguish a group of systems based on one or more system attributes, after passing all rules, it links each group of rules to a profile. Both the rules file and the profiles must be located in a pre-defined and accessible location.

The rules file is retrieved only if no specific control is supplied using the *autoyast* keyword. For example, if the following is used, the rules file wont be evaluated:

```
autoyast=http://10.10.0.1/profile/test.xml
```

**Figure 6.1. Rules**



If more than one rule apply, the final profile for each group is generated on the fly using a merge script. The merging process is based on the order of the rules and later rules override configuration data in earlier rules.

The use of a rules file is optional. If the rules file is not found, system installation proceeds in the classic way by just using the supplied profile or by searching for the profile depending on the *MAC* or the *IP* address of the system.

## 1.1. Rules File explained

### Example 6.1. Simple rules file

The following simple example illustrates how the rules file is used to retrieve the configuration for a client with known hardware.

```
<?xml version="1.0"?>
<!DOCTYPE autoinstall SYSTEM "/usr/share/autoinstall/dtd/rules.dtd">
<autoinstall xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configs">
  <rules config:type="list">
    <rule>
      <disksize>
        <match>/dev/hdc 1000</match>
        <match_type>greater</match_type>
      </disksize>
      <result>
        <profile>machine1.xml</profile>
        <continue config:type="boolean">>false</continue>
      </result>
    </rule>
    <rule>
      <disksize>
        <match>/dev/hda 1000</match>
        <match_type>greater</match_type>
      </disksize>
      <result>
        <profile>machine2.xml</profile>
        <continue config:type="boolean">>false</continue>
      </result>
    </rule>
  </rules>
</autoinstall>
```

The last example defines 2 rules and provides a different profile for every rule. The rule used in this case is *disksize*. After parsing the rules file, YaST2 attempts to match the system being installed to the rules in the `rules.xml` file in the following order: first rule through the last rule. A rule match occurs when the system being installed matches all of the system attributes defined in the rule. As soon as a system matches a rule, the result resource is added to the stack of profiles AutoYaST will be using to create the final profile. The *continue* property tells AutoYaST if it should continue with other rules or not after a match has been found.

If the first rule does not match, next rule in the list is examined until a match is found.

Using the *disksize* attribute, you can provide different configurations for different hard drives with different size. First rule checks if the device `/dev/hdc` is available and if it is greater than 1 GB in size using the *match* property.

A rule must have at least one attribute to be matched. If you need to check more attributes, i.e. memory or architectures, you can add more attributes in the rule resource as shown in the next example.

## Example 6.2. Simple rules file

The following simple example illustrates how the rules file is used to retrieve the configuration for a client with known hardware.

```
<?xml version="1.0"?>
<!DOCTYPE autoinstall SYSTEM "/usr/share/autoinstall/dtd/rules.dtd">
<autoinstall xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configs">
  <rules config:type="list">
    <rule>
      <disksize>
        <match>/dev/hdc 1000</match>
        <match_type>greater</match_type>
      </disksize>
      <memsize>
        <match>1000</match>
        <match_type>greater</match_type>
      </memsize>
      <result>
        <profile>machine1.xml</profile>
      </result>
    </rule>
  </rules>
</autoinstall>
```

```

        <continue config:type="boolean">false</continue>
    </result>
</rule>
<rule>
    <disksize>
        <match>/dev/hda 1000</match>
        <match_type>greater</match_type>
    </disksize>
    <memsize>
        <match>256</match>
        <match_type>greater</match_type>
    </memsize>
    <result>
        <profile>machine2.xml</profile>
        <continue config:type="boolean">false</continue>
    </result>
</rule>
</rules>
</autoinstall>

```

The rules directory must be located in the same referenced directory used with the *autoyast* keyword on boot time, so if the client was booted using *autoyast=http://10.10.0.1/profiles/*, AutoYaST will search for the rules file in *http://10.10.0.1/profiles/rules/rules.xml*.

## 1.2. Rules file structure

The `rules.xml` file must have:

- At least one rule
- It must have the name `rules.xml`
- It must be located in the directory *rules* in the profile repository
- At least one attribute to match in the rule

## 1.3. Predefined System Attributes

The following table lists the predefined system attributes you can match in the rules file.

**Table 6.1. System Attributes**

Attribute	Values	Description
hostaddress	IP address of host	This attribute must always match exactly
domain	Domain name of host	This attribute must always match exactly
network	network address of host	This attribute must always match exactly
mac	MAC address of host	This attribute must always match exactly. (MAC addresses to be matched should be in the form <i>0080C8F6484C</i> )
linux	Number of installed Linux partitions on the system	This attribute can be 0 or more
others	Number of installed non-Linux partitions on the system	This attribute can be 0 or more

Attribute	Values	Description
xserver	X Server needed for graphic adapter	This attribute must always match exactly
memsize	Memory available on host in MBytes	All match types are available
totaldisk	Total disk space available on host in MBytes	All match types are available
haspcmica	System has PCMCIA (i.e Laptops)	Exact match required, 1 for available PCMCIA or 0 for none
hostid	Hex representation of IP address	Exact match required
arch	Architecture of host	Exact match required
karch	Kernel Architecture of host (i.e. SMP kernel, Athlon Kernel)	Exact match required
disksize	Drive device and size	All match types are available
product	The hardware product name as specified in SMBIOS	Exact match required
product_vendor	The hardware vendor as specified in SMBIOS	Exact match required
board	The system board name as specified in SMBIOS	Exact match required
board_vendor	The system board vendor as specified in SMBIOS	Exact match required
custom1-5	Custom rules using shell scripts	All match types are available

## 1.4. Rule Matching

The tag *match\_type* is used to define how the rules should be checked. There exist 4 types of matching:

- exact
- greater
- lower
- range (for IPs, memsize and totaldisk only)

*exact* should always be used with all string attributes

## 1.5. Using Operators

When using multiple rules, you might want to have either all rules match or just some. For example you might want either 2 or more rules to always match or just one of a list of rules in a rule set. The operator is defined with the *operator* tag which can either be "*and*" (default) or "*or*".

## 2. Classes

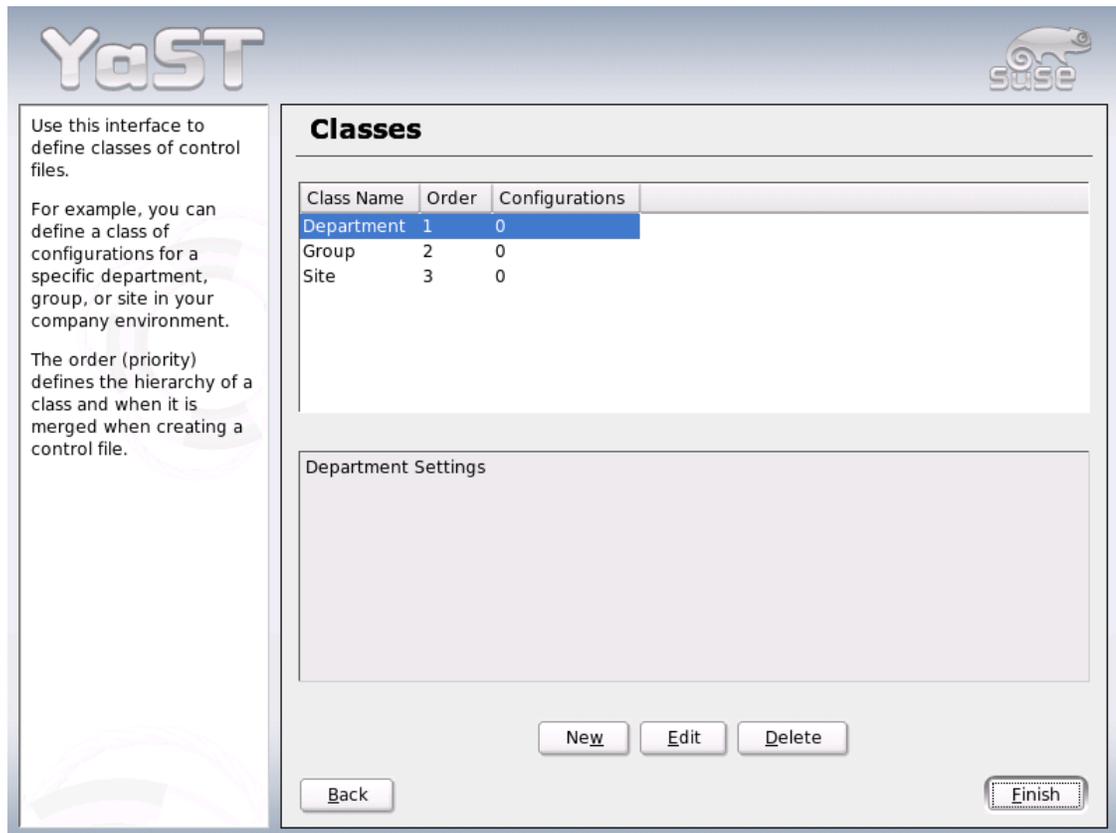
You can assign a system to different classes which can be defined in the control file. Unlike rules, classes have to be configured in the control file and represent a configuration which is typical for a group of systems.

## 2.1. Creating Class files and Directories

Using the configuration management system, you can define a set of classes. The class definition consists of the following variable for each class:

- Name: Class name
- Descriptions: Class description
- Order: Order (or priority) of the class in the stack of migration

**Figure 6.2. Defining Classes**



You can create as many classes as you need, however it is recommended to keep the set of classes as small as possible to keep the configuration system concise. As an example, the following set of classes can be used:

- site: Classes describing a physical location or site.
- machine: Classes describing a type of machine or make
- role: Classes describing the function of the machine to be installed
- group: Classes describing a department or a group within a site or a location.

A file saved in a class directory can have the same syntax and format as a regular control file but represents a subset of the configuration. For example, to create a new control file for a special computer with a specific network interface, only the resource in the control file, which controls the configuration of the network is needed. Having multiple network types, you can merge the one needed for a special type of hardware with other class files and create a new control file which suits the system being installed.

## 2.2. Using Classes During Installation

Classes can be merged during installation using a special configuration option in the control file. The classes should be on the same media where the control file is found in the directory `classes`.

The following shows a simple example of 2 classes defined in the control file which are retrieved and merged during installation

### Example 6.3. Classes

```
...
<install>
  <bootloader>
    ...
  </bootloader>
  <classes config:type="list">
    <class>
      <class_name>software</class_name>
      <configuration>sles9.xml</configuration>
    </class>
    <class>
      <class_name>hardware</class_name>
      <configuration>model_x.xml</configuration>
    </class>
  </classes>

  <general>
    ...
  </general>
</install>
...
```

The files `sles9.xml` and `model_x.xml` will be retrieved from the the directories `classes/software` and `classes/hardware` respectively.

The files above might contain one or more configuration sections.

## 3. Mixing Rules and Classes

It is possible to mix rules and classes during an auto-installation session. For example you can identify a system using rules and use profiles which contain class definitions in them. The process is described in the figures “Rules Retrieval Process”.

After retrieving the rule results and merging them, the generated control file is parsed and the presence of class definitions is checked. If classes are defined, then the class files are retrieved from the original repository and a new merge process is initiated.

---

# Chapter 7. The Auto-Installation Process

## 1. Introduction

After the system has booted and the control file has been retrieved, YaST2 performs configuration of the system according to the information provided in the control file. All the configuration is summarized in a window that is shown by default and should be deactivated if a full automatic installation is needed.

When YaST2 has reached the point where the summary of the configuration is shown, YaST2 has only probed hardware and prepared the system for auto-installation, thus, nothing has been changed in the system yet, so that in case of any error, the process still can be aborted.

A system should be automatically installable without the need to have any graphic adaptor or monitor. Having a monitor attached to the client machine is nevertheless recommended to follow the process and to get feedback in case of any errors. Choosing between the Qt and the *Ncurses* interfaces is possible. For headless clients, system messages can be monitored using the serial console.

### 1.1. X11 Interface

This is the default interface while auto-installing. No special variables are required to activate it.

### 1.2. Serial console

You can start installing a system using the serial console by adding the keyword `console` (i.e. `console=ttyS0`) to the command line of the kernel. This will start `linuxrc` in console mode and later in the process, YaST2 also is started in serial console mode.

### 1.3. Text based YaST2-Installation

This option can also be activated on the command line. This will start YaST2 in *Ncurses* mode. To start YaST2 in text mode, add `textmode=1` on the command line.

Starting YaST2 in text mode is recommended when installing a client with less than 64 MB or when X11 is not being configured at all, especially on headless machines.

## 2. Choosing the right Boot Medium

There are different methods for booting the client. The computer can boot from its network interface card (NIC) to receive the boot images via DHCP /TFTP or a suitable kernel as well as an `initrd` image are loaded from a floppy or a boot-able CD-ROM.

### 2.1. Booting from a floppy

For testing/rescue purposes or because the NIC does not have a PROM or PXE you can build a boot floppy to use with AutoYaST. Using a floppy to initiate an auto-install process is limited due to the size of the data a floppy can hold. However, it is still possible to use floppies when auto-installing a single, disconnected machine.

Floppies can be used to store the control file, especially when using the original *SuSE* CD-ROMs for a single, disconnected machine. Using the kernel command line, you can specify the location of the control file on the floppy.

Even without specifying any command line options, it is still possible to initiate the auto-install process by placing a control file on a floppy with a special, pre-defined file name. (`autoinst.xml`) YaST2 will check for `autoinst.xml` upon startup and if it was found it will switch from interactive to automated installation.

## 2.2. Booting from CD-ROM

You can use the original *SuSE* CD-ROMs in combination with other media, i.e. with a floppy to hold the control file or in combination with network where the control file can be located.

It is also possible to create customized CD-ROMs to hold only the package you need in addition to the control file which also can be saved on the CD-ROM. This method requires creation of CD-ROMs every time you wish to change the configuration though.

## 3. Invoking the Auto-Installation process

### 3.1. Command line Options

Adding the command line variable `autoyast` will make `linuxrc` start in automated mode. **Linuxrc** searches for a configuration file, which should be distinguished from the main control file in the following places:

- In the root directory of the initial ram-disk used for booting the system up
- In the root directory of the floppy

The configuration file used by **linuxrc** can have the following keywords (for a detailed description of how `linuxrc` works and other keywords, see “Advanced Linuxrc Options”):

**Table 7.1. Keywords for linuxrc**

Keyword	Value
netdevice	Which network device to use for network setup (Device used for BOOTP / DHCP requests)
server	Which server to contact for source directory (NFS Server)
serverdir	Directory on NFS Server
hostip	When empty, client sends BOOTP request, otherwise client is configured with entered IP configuration.
netmask	Netmask
gateway	Gateway
nameserver	Nameserver
insmod	Kernel modules to load.
autoyast	Location of the the control file to be used for the automatic installation, i.e. <code>autoyast=http://192.168.2.1/profiles/</code>
install	Location of the installation directory, i.e. <code>install=nfs://192.168.2.1/CDs/</code>

Keyword	Value
instmode	Installation mode, i.e. nfs, http etc. (Not needed if <i>install</i> is set)

These variables and keywords will bring the system up to the point where YaST2 can take over with the main control file. Currently, the source medium is automatically discovered, which in some cases makes it possible to initiate the auto-install process without giving any instructions to linuxrc.

The traditional **linuxrc** configuration file (`info`) should be used only in the preparation phase and has the function of giving the client enough information about the installation server and the location of the sources. In most cases this file is not needed; it is however needed in special network environments where DHCP / BOOTP are not used or when special kernel modules have to be loaded.

All linuxrc keywords can be passed to **linuxrc** using the kernel command line. The command line can for example also be set when creating network boot-able images or it can be passed to the kernel using a specially configured DHCP server in combination with Etherboot or PXE.

The format of the special command line variable *autoyast* can be used as described in table “Command line variables for AutoYaST”

**Table 7.2. Command line variables for AutoYaST**

Command line variable	Description
autoyast=default	Default auto-installation option
autoyast=file://<path>	Looks for control file in specified path (relative to source root directory, i.e. <i>file:///autoinst.xml</i> if in the top directory of a CD-ROM )
autoyast=device://<device>/<file>	Looks for control file on a storage device. (only device name needed without full path, i.e. /dev/sda1 is wrong, instead use sda1)
autoyast=floppy://<path>	Looks for control file in the floppy (Useful when booting from CD)
autoyast=nfs://<server>/<path>	Looks for control file on <server>
autoyast=http://<server>/<path>	Retrieves the control file from a web server using the HTTP protocol.
autoyast=tftp://<server>/<path>	Retrieve the control file with TFTP
autoyast=ftp://<server>/<path>	Retrieve the control file with FTP

Several scenarios for auto-installation are possible using different types of infrastructure and source media. The simplest way is by using the source media from the *SuSE* Box. In that case you have either a DVD with all *SuSE* packages or a set of CD-ROMs. To initiate the auto-installation process however, the auto-installation command line variable should be entered at system boot-up and the control file should be accessible to YaST2. The following list of scenarios explains how the control file can be supplied and the setup needed for the auto-installation process to be successful.

- Using *SuSE* original CD-ROMs from *SuSE* Linux box:

To use the original CD-ROMs, you need a media with the control file, the control file can reside on the following locations:

1. *Floppy*: Control file accessible via the *autoyast=floppy* option. YaST2 also searches upon startup for a file named `autoinst.xml`. If such a file is found, YaST2 will switch into auto-installation mode even if no special command line variables were supplied. (See “ Auto-installing a Single System ” )
  2. *Network*: Control file accessible via the *autoyast=nfs://..*, *autoyast=ftp://..*, *autoyast=http://..* or *autoyast=tftp://..* options.
- Using 'self-made' CD-ROMs:

In this case, you can include the control file on the CD-ROM for easy access (using the *autoyast=file://* option) or use one of the above mentioned methods used with the original *SuSE* CD-ROMs.

Using CD-ROMs for autoinstallation, it is required to instruct the installer to use the CD-ROM for installation and not try to find the installation files on the network. This can be accomplished by adding the *instmode=cd* option to the kernel command line (this can be done by adding the option to the `isolinux.cfg` file on the CD).

- Using NFS and Floppy, Network or CD-ROM for system boot-up.

This option is the most important one due to the fact that installations of PC farms are normally done using NFS servers and other network services like BOOTP / DHCP . The control file can reside in the following places:

1. *Floppy/CD-ROM*: Control file accessible via the *autoyast=file://..* option.
2. *Network*: Control file accessible via the *autoyast=http://..*, *autoyast=ftp://..*, *autoyast=nfs://..* or *autoyast=tftp://..* options.

## Disabling network and DHCP

To disable network during installations where network is not needed or not available, for example when auto-installing from CD-ROMs use the `linuxrc` option *netsetup* to set network configuration behavior. To disable network setup use *netsetup=0*

If *autoyast=default* is defined, YaST2 will look for a file named `autoinst.xml` in the following three places:

1. The root directory of the floppy disk.
2. The root directory of the installation medium.
3. The root directory of the initial ram disk used to boot the system.

With all *autoyast* invocation options, excluding *default*, it is possible to specify the location of the control file in the following ways:

1. Specify the exact location of the control file:

```
autoyast=http://192.168.1.1/control-files/client01.xml
```

2. Specify a directory where several control files are located

```
autoyast=http://192.168.1.1/control-files/
```

In this case the relevant control file is retrieved using the hex digit representation of the IP as described below.

If only the path prefix variable is defined, YaST2 will fetch the control file from the specified location in the following way:

1. First, it will search for the control file using its own IP address in upper case hexadecimal, e.g. *192.0.2.91* -> *C000025B*.
2. If that file is not found, it will remove one hex digit and try again. This action is repeated till the file with the correct name is found. Ultimately, it will try looking for a file with the MAC address of the clients as the file name (mac should have the following syntax: *0080C8F6484C*) and if not found a file named `default` (in lower case).

As an example, for 192.0.2.91, the HTTP client will try:

```
C000025B
C000025
C00002
C0000
C000
C00
C00
C0
C
0080C8F6484C
default
```

in that order.

To determine the hex representation of the IP address of the client, use the utility called `/usr/sbin/gethostip` available with the *syslinux* package.

### Example 7.1. Determine HEX code for an IP address

```
# /usr/sbin/gethostip 10.10.0.1
10.10.0.1 10.10.0.1 0A0A0001
```

## 3.2. Auto-installing a Single System

The easiest way to auto-install a system without any network connection is by using the standard CD-ROMs that come in the *SuSE* Linux box. Using the CD-ROMs in combination with a floppy disk lets you getting started with AutoYaST very fast and without spending much time configuring installation

server and network environments.

Create the control file and name it `autoinst.xml`. Copy the file `autoinst.xml` to a floppy by either mounting the floppy or by using the `mtools`.

```
mcopy autoinst.xml a:
```

### 3.3. Combining `linuxrc info` file with YaST2 control file

If you choose to pass information to `linuxrc` using the `info` file, it is possible to integrate the keywords in the XML control file. In the case the file has to be accessible to `linuxrc` and has to be named `info`.

`Linuxrc` will look for a string (`start_linuxrc_conf` in the control file which represents the beginning of the file. If it is found, it will parse the content starting from that string and will finish when the string `end_linuxrc_conf` is found. The options are stored in the control file in the following way:

#### Example 7.2. `Linuxrc` options in the control file

```
.....
<install>
.....
  <init>
    <info_file>
<![CDATA[
#
# Don't remove the following line:
# start_linuxrc_conf
#
install: nfs://192.168.1.1/CDS/full-i386
textmode: 1
autoyast: file:///info

# end_linuxrc_conf
# Do not remove the above comment
#
]]>

    </info_file>
  </init>
.....
</install>
.....
```

Note that the `autoyast` keyword must point to the same file, i.e. if it is on a floppy, then the protocol `floppy` has to be used. In other cases where the `info` file is stored in the initial ram-disk, the `file` option has to be used.

## 4. System Configuration

The system configuration during auto-installation can be seen as the most important part of the whole process. Customizing a system to your environment needs is what makes an auto-installation system attractive, not the installation part.

As you have seen in the previous chapters, almost anything can be configured automatically on the target system. In addition to the pre-defined directives, you can always use post-scripts to change other things in the system. Additionally you can change any system variables and if required, copy complete configuration files into the target system.

### 4.1. Post-Install and System Configuration

The Post-Installation and the System Configuration are initiated directly after the last package is installed in the target system and is continued after the system has booted for the first time.

Before the system is booted for the first time, YaST2 writes all data collected during installation into the system and finally it writes the boot loader in the specified location. In addition to these regular tasks, which are also done when performing a regular installation, YaST2 executes the *chroot-scripts* as specified in the control file. Note that these scripts are executed while the system is still not mounted.

If a different kernel than the default is installed, a hard reboot will be required. A hard reboot can also be forced during auto-installation, independent of the installed kernel. This can be accomplished using the *reboot* property of the *general* resource. (See General Options)

## 4.2. System Customization

Most of the system customization is done in the second stage of the installation. YaST2 provides most of the important resources needed to bring up a system to a usable, general state. However, you may have other requirements for the installed system. If the required customizations can't be done using YaST2 resources, then the post-install scripts can be used to accomplish this task.

You can define an unlimited number of custom scripts in the control file either by editing the control file or by using the configuration system.

---

# Chapter 8. Legacy and foreign Configuration formats

## 1. Migration from YaST1 and ALICE

ALICE, SuSEs former auto-installation system was a system built around the auto-installation features that were available with YaST1. In order to be able to use existing ALICE configuration files and resources, a special option is provided in the configuration system will let you convert ALICE configuration files into a control file readable by AutoYaST.

ALICE uses YaST1 for the installation of a Linux System. This is done by creating a boot medium with the needed control file (`info`) from a set of configuration files maintained in a CVS repository. The `info` file has the traditional format used with YaST1.

The system configuration is done almost entirely after the system is installed and is initiated using the `%post` section of the ALICE RPM package.

### 1.1. ALICE modules

Each of ALICE modules perform certain tasks and requires one or multiple configuration files. The modules are shell scripts that are invoked after installation of the machine to setup different services on the client.

YaST2 offers an extensive and rich interface to the installed system which replaces most of the modules that were available with ALICE. The following is a list of all ALICE modules, their function and how their functionality is provided by YaST2 modules which are already available or which can be integrated easily:

The modules `prepare_alice` and `make_all` provided the base and main scripts of all ALICE modules. The module `prepare_alice` is called right after the initial installation process - which is done after YaST1 has finished installation packages.

With YaST2, the alternative to these modules is part of the system and is not an addition or extension. This means that YaST2 configures the system in one single process and not, as with ALICE in two different, independent steps.

The following table show how the result of some ALICE modules can be accomplished with YaST2

**Table 8.1. ALICE vs. YaST2 modules**

Module	ALICE	YaST2	Concerned files
User configuration	Adding users is performed without any consistency checks.	Using YaST2 users module	<code>/etc/passwd</code>
Group configuration	Adding groups is performed without any consistency checks.	Using YaST2 users module	<code>/etc/group</code>
Services	X	-	<code>/etc/services</code>
Inetd	X	Using the inetd module	<code>/etc/inetd.conf</code>
Syslog	X		<code>/etc/syslog.conf</code>
Lilo	X	X	<code>/etc/lilo.conf</code>

Module	ALICE	YaST2	Concerned files
SNMP	X	-	/etc/ucdsnm-pd.conf
Cron	X	-	/etc/crontab
hosts	X	X	/etc/hosts
Routing	X	X	/etc/route.conf
Printer	X	X	/etc/printcap
SSH	X	-	/etc/ssh
Kernel modules	X	X	/etc/modules.conf

## 1.2. Other configuration options with YaST2 and ALICE

ALICE completed most of the configuration using the system configuration file `/etc/rc.config`. This interface to the system does not exist anymore with new SuSE products. Instead, configuration options are now available in `/etc/sysconfig`.

Entries in `/etc/sysconfig` can be easily set and modified using YaST2 and AutoYaST. For network services it is recommended to use the relevant YaST2 modules dealing with networking, rather than modifying `/etc/sysconfig/network` directly.

## 2. Redhat Kickstart

The Configuration Management System offers an option for importing a foreign auto-installation configuration file using the *Kickstart* system. To import a *Kickstart* file, you only need to enter the path of the configuration file and decide how to handle the data, by either saving the result into a file directly or by loading the resulting AutoYaST compatible control file into the Configuration Management System to add more configuration options available with SuSE. The following sections describe some limitations and issues to consider when importing from a foreign source:

### 2.1. Software selections and packages

It is not possible at the moment to import package selections and single package listing into AutoYaST. The packages will be added to the control file, but manual selection of the desired packages is needed. The reason is that package groups and package names might differ depending on the source distribution

### 2.2. User scripts

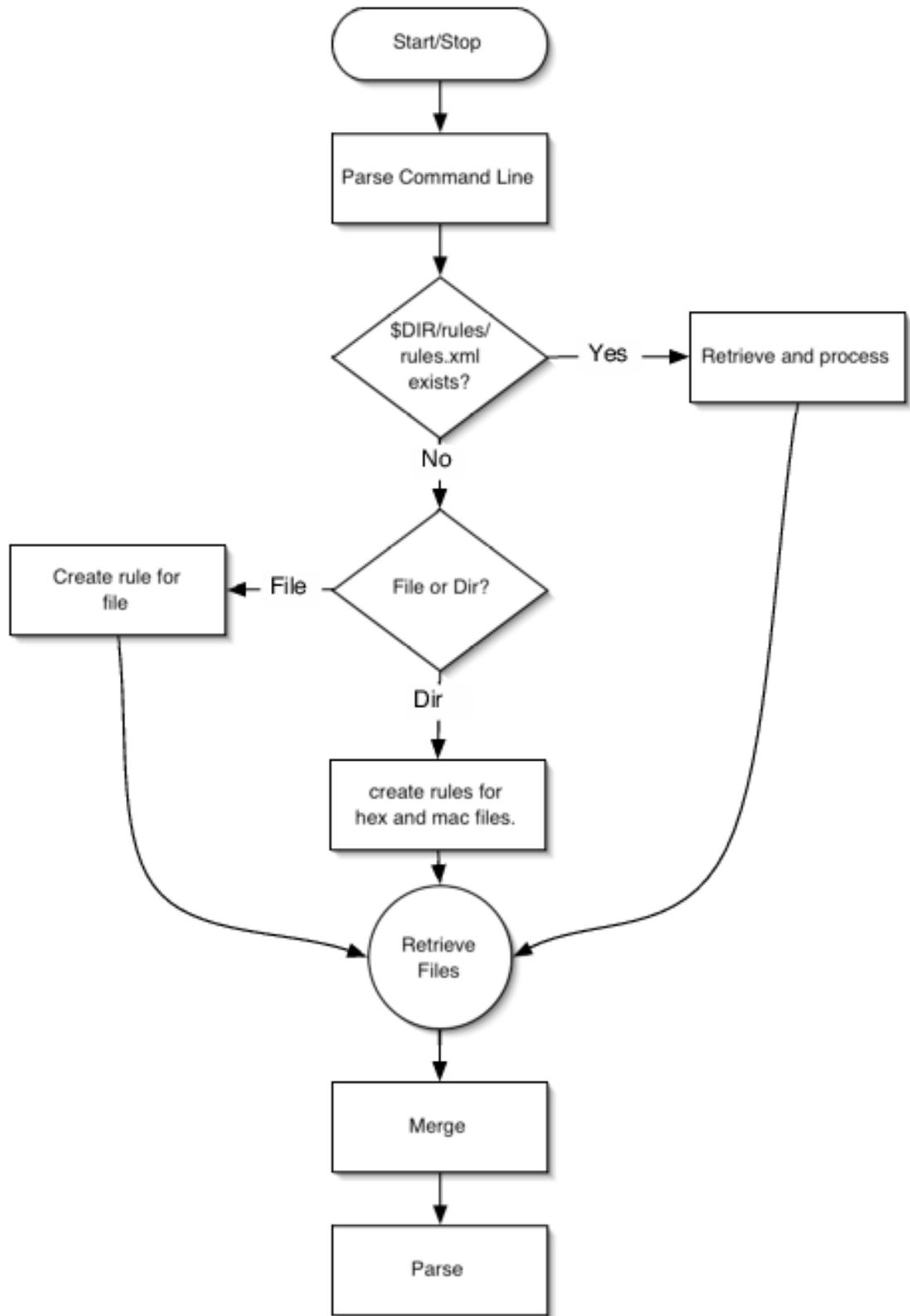
Kickstart offers two types of scripts, *pre* and *post* scripts. More scripts (>2) are not supported as in AutoYaST. So it might be needed to split large scripts into smaller components depending on the function to make such scripts manageable

---

# Appendix A. Handling Rules

The following figure illustrates how rules are handled and the processes of retrieval and merge.

**Figure A.1. Rules Retrieval Process**



---

# Appendix B. Advanced Linuxrc Options

Linuxrc is a program used for setting up the kernel for installation purposes. It allows the user to load modules, start an installed system, a rescue system or an installation via YaST.

Linuxrc is designed to be as small as possible. Therefore, all needed programs are linked directly into one binary. So there is no need for shared libraries in the initdisk.

## Note

If you run Linuxrc on an installed system, it will work slightly different as it tries not to destroy your installation. As a consequence you cannot test all features this way.

## 1. Passing parameters to Linuxrc

Unless Linuxrc is in manual mode it will look for an 'info' file in these locations: first `/info` on the floppy disk and if that does not exist for `/info` in the initrd. After that it parses the kernel command line for parameters. You may change the 'info' file Linuxrc reads using the `info` command line parameter. If you don't want Linuxrc to read the kernel command line (say, because you need to give a kernel parameter that accidentally is recognized by Linuxrc, too), use `linuxrc=nocmdline`.

Independent if the above, Linuxrc will always look for and parse a file `/linuxrc.config`. You can use this file to change default values, if you need to. But in general, use the `info` file instead. Note that `/linuxrc.config` is read before any 'info' file and even in manual mode.

## 2. 'info' file format

Lines starting with '#' are comments, valid entries are of the form

```
key: value
```

Note that *value* extends to the end of the line and so may contain spaces. *key* is matched case insensitive.

You can use the same key - value pairs on the kernel command line using the syntax `key=value` Lines that don't have the form described above are ignored.

Valid keys are (values given are just examples)

**Table B.1. Advanced linuxrc keywords**

Keyword/Value	Description
Language: de_DE	set the language
Keytable: de-lat1-nd	load this keytable
Display: Color Mono Alt	set the menu color scheme
Install: nfs://server/install/8.0-i386	install via NFS from <i>server</i> (note: you can give username, password etc. in the URL, too)
InstMode: cd hd nfs smb ftp http tftp	set installation mode
HostIP: 10.10.0.2	the client ip address
Netmask: 255.255.0.0	network mask

Keyword/Value	Description
Gateway: 10.10.0.1	gateway
Server: 10.10.0.1	installation server address
Nameserver: 10.10.0.1	nameserver
Proxy: 10.10.0.1	proxy (either ftp or http)
ProxyPort: 10.10.0.1	proxy port
Partition: hda1	partition with install sources for hard disk install
Serverdir: /install/8.0-i386	base directory of the installation sources
Netdevice: eth0	network interface to use
BOOTPWait: 5	sleep 5 seconds between network activation and starting bootp
BOOTPTimeout: 10	10 seconds timeout for BOOTP requests
DHCPTimeout: 60	60 seconds timeout for DHCP requests
TFTPTimeout: 10	10 seconds timeout for TFTP connection
ForceRootimage: 0 1	load the installation system into ramdisk
Textmode: 0 1	start YaST in text mode
Username: name	set user name (e.g. for FTP install)
Password: password	set password (e.g. for FTP install)
WorkDomain: domain	set work domain for SMB install
ForceInsmode: 0 1	use '-f' option when running <i>insmod</i>
DHCP: 0 1	start DHCP daemon <i>now</i> , but see <i>UseDHCP</i>
UseDHCP: 0 1	use DHCP instead of BOOTP (DHCP is default)
MemLimit: 10000	ask for swap if free memory drops below 10000 kB
MemYaST: 20000	run YaST in text mode if free memory is below 20000 kB
MemYaSTText: 10000	ask for swap before starting YaST if free memory is below 10000 kB
MemModules: 20000	delete all modules before starting YaST if free memory is below 20000 kB
MemLoadImage: 50000	load installation system into ramdisk if free memory is above 50000 kB
Manual: 0 1	start Linuxrc in manual mode
NoPCMCIA: 0 1	don't start card manager
Domain: zap.de	set domain name (used for name server lookups)
RootImage: /suse/images/root	installation system image
RescueImage: /suse/images/rescue	rescue system image
InstallDir: /suse/inst-sys	installation system
Rescue: 1 nfs://server/dir	load rescue system; the URL variant specifies the location of the rescue image explicitly
AutoYaST: ftp://autoyastfile	location of autoinstall file; activates autoinstall mode
VNC: 0 1	setup VNC server
VNCPassword: password	sets VNC server password

Keyword/Value	Description
UseSSH: 0 1	setup SSH server
SSHPasswd: password	sets SSH server password (this will not be the final root password!)
AddSwap: 0 3 dev/hda5	if 0, do never ask for swap; if the argument is a positive number <i>n</i> , activate the <i>n</i> 'th swap partition; is the argument is a partition name, activate this swap partition
Exec: command	run <i>command</i>
USBWait: 4	wait 4 seconds after loading USB modules
Insmod: module params	load this module
Loghost: 10.10.0.22	Enable remote logging via syslog

### 3. Advanced Network Setup

The *netsetup* keyword allows advanced network configurations and enables dialogs to setup the network where required.

- `netsetup=1`  
the normal network setup questions
- `netsetup=xxx,yyy`  
just `xxx` and `yyy`
- `netsetup=+xxx,-yyy`  
default, additionally `xxx`, but not `yyy`

`xxx` could have the following values: `dhcp`, `hostip`, `gateway`, `netmask`, `nameserver`. `nameserverN` asks for `N` nameservers (max. 4).

For example, the following can be entered on the command line:

```
netsetup=-dhcp,+nameserver3
```