



SUSE Linux Enterprise Server 15

# AutoYaST Guide

# AutoYaST Guide

SUSE Linux Enterprise Server 15

AutoYaST is a system for unattended mass deployment of SUSE Linux Enterprise Server systems. AutoYaST installations are performed using an AutoYaST control file (also called a “profile”) with your customized installation and configuration data.

Publication Date: January 05, 2023

<https://documentation.suse.com> 

Copyright © 2006– 2023 SUSE LLC and contributors. All rights reserved.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or (at your option) version 1.3; with the Invariant Section being this copyright notice and license. A copy of the license version 1.2 is included in the section entitled “GNU Free Documentation License”.

For SUSE trademarks, see <https://www.suse.com/company/legal/> . All other third-party trademarks are the property of their respective owners. Trademark symbols (®, ™ etc.) denote trademarks of SUSE and its affiliates. Asterisks (\*) denote third-party trademarks.

All information found in this book has been compiled with utmost attention to detail. However, this does not guarantee complete accuracy. Neither SUSE LLC, its affiliates, the authors nor the translators shall be held liable for possible errors or the consequences thereof.

# Contents

# 1 Introduction to AutoYaST 1

## 1.1 Motivation 1

## 1.2 Overview and Concept 1

# I UNDERSTANDING AND CREATING THE AUTOYAST CONTROL FILE 4

## 2 The AutoYaST Control File 5

### 2.1 Introduction 5

### 2.2 Format 5

### 2.3 Structure 6

Resources and Properties 7 • Nested Resources 7 • Attributes 8

## 3 Creating an AutoYaST Control File 9

### 3.1 Collecting Information 9

### 3.2 Using the Configuration Management System (CMS) 9

Creating a New Control File 10

### 3.3 Creating/Editing a Control File Manually 11

### 3.4 Creating a Control File via Script with XSLT 12

# II AUTOYAST CONFIGURATION EXAMPLES 14

## 4 Configuration and Installation Options 15

### 4.1 General Options 15

The Mode Section 16 • Configuring the Installation Settings Screen 20 • The Self-Update Section 20 • The Semi-Automatic Section 21 • The Signature Handling Section 22 • The Storage Section 24 • The Wait Section 24 • Blacklisting Unused Devices on IBM IBM Z 25 • Examples for the general Section 26

- 4.2 Reporting 28
- 4.3 System Registration and Extension Selection 29
  - Extensions 33
- 4.4 The Boot Loader 34
  - Loader Type 35 • Globals 35 • Device map 39
- 4.5 Partitioning 39
  - Drive Configuration 39 • Partition Configuration 43 • Btrfs subvolumes 49 • Using the Whole Disk 50 • Automated Partitioning 51 • Advanced Partitioning Features 54 • Logical Volume Manager (LVM) 58 • Software RAID 60 • IBM Z Specific Configuration 66
- 4.6 iSCSI Initiator Overview 68
- 4.7 Fibre Channel over Ethernet Configuration (FCoE) 69
- 4.8 Country Settings 70
- 4.9 Software 72
  - Product Selection 72 • Package Selection with Patterns and Packages Sections 73 • Installing Additional/Customized Packages or Products 74 • Kernel Packages 80 • Removing Automatically Selected Packages 80 • Installing recommended packages and patterns 81 • Installing Packages in Stage 2 82 • Installing Patterns in Stage 2 82 • Online Update in Stage 2 83
- 4.10 Upgrade 83
- 4.11 Services and Targets 84
- 4.12 Network Configuration 85
  - Persistent Names of Network Interfaces 88 • s390 Options 89 • Proxy 90
- 4.13 NIS Client and Server 91
- 4.14 NIS Server 91
- 4.15 Hosts Definition 94

- 4.16 Windows Domain Membership 94
- 4.17 Samba Server 95
- 4.18 Authentication Client 97
- 4.19 NFS Client and Server 97
- 4.20 NTP Client 98
- 4.21 Mail Server Configuration 100
- 4.22 Apache HTTP Server Configuration 101
- 4.23 Squid Server 110
- 4.24 FTP Server 117
- 4.25 TFTP Server 122
- 4.26 Firstboot Workflow 122
- 4.27 Security Settings 123
  - Password Settings Options 123 • Boot Settings 124 • Login Settings 124 • New user settings (**useradd** settings) 124
- 4.28 Linux Audit Framework (LAF) 124
- 4.29 Users and Groups 127
  - Users 127 • User Defaults 132 • Groups 133 • Login Settings 135
- 4.30 Custom User Scripts 136
  - Pre-Install Scripts 136 • Post-partitioning Scripts 137 • Chroot Environment Scripts 138 • Post-Install Scripts 138 • Init Scripts 138 • Script XML Representation 140 • Script Example 143
- 4.31 System Variables (Sysconfig) 145
- 4.32 Adding Complete Configurations 146
- 4.33 Ask the User for Values during Installation 148
  - Default Value Scripts 156 • Scripts 157

- 4.34 Kernel Dumps 162
  - Memory Reservation 163 • Dump Saving 165 • E-Mail Notification 167 • Kdump Kernel Settings 169 • Expert Settings 171
- 4.35 DNS Server 171
- 4.36 DHCP Server 174
- 4.37 Firewall Configuration 177
  - General Firewall Configuration 178 • Firewall Zones Configuration 178 • A Full Example 179
- 4.38 Miscellaneous Hardware and System Components 180
  - Printer 180 • Sound devices 182
- 4.39 Importing SSH Keys and Configuration 182
- 4.40 Configuration Management 183

### III MANAGING MASS INSTALLATIONS WITH RULES AND CLASSES 185

## 5 Rules and Classes 186

- 5.1 Rule-based Automatic Installation 186
  - Rules File Explained 187 • Custom Rules 190 • Match Types for Rules 190 • Combine Attributes 191 • Rules File Structure 191 • Predefined System Attributes 192 • Rules with Dialogs 194
- 5.2 Classes 197
- 5.3 Mixing Rules and Classes 199
- 5.4 Merging of Rules and Classes 199

### IV UNDERSTANDING THE AUTO-INSTALLATION PROCESS 202

## 6 The Auto-Installation Process 203

- 6.1 Introduction 203
  - X11 Interface (graphical) 203 • Serial Console 203 • Text-based YaST Installation 203

- 6.2 Choosing the Right Boot Medium 204
  - Booting from a Flash Disk 204 • Booting from DVD-ROM 204 • Booting via PXE over the Network 205
- 6.3 Invoking the Auto-Installation Process 205
  - Command Line Options 206 • Auto-installing a Single System 212 • Combining the **linuxrc** info File with the AutoYaST Control File 213
- 6.4 System Configuration 213
  - Post-Install and System Configuration 214 • System Customization 214

## V USES FOR AUTOYAST ON INSTALLED SYSTEMS 215

## 7 Running AutoYaST in an Installed System 216

## VI APPENDICES 218

### A Handling Rules 219

### B AutoYaST FAQ—Frequently Asked Questions 220

### C Advanced **linuxrc** Options 224

#### C.1 Passing Parameters to **linuxrc** 224

#### C.2 info File Format 225

#### C.3 Advanced Network Setup 227

### D Differences Between AutoYaST Profiles in SLE 12 and 15 229

#### D.1 Product Selection 229

#### D.2 Software 229

Adding Modules or Extensions Using the Registration Server 230 • Adding Modules or Extensions Using the SLE-15-SP0-Full-ARCH-GM-media1.iso Image 231 • Renamed Software Patterns 231

#### D.3 Registration of Module and Extension Dependencies 232



- D.4 Partitioning **233**
  - GPT Becomes the Default Partition Type on AMD64/Intel 64 **233** • Setting Partition Numbers **233** • Forcing Primary Partitions **233** • Btrfs: Default Subvolume Name **234** • Btrfs: Disabling Subvolumes **234** • Reading an Existing `/etc/fstab` Is No Longer Supported **234** • Setting for Aligning Partitions Has Been Dropped **235** • Using the `type` to Define an Volume Group **235**
- D.5 Firewall Configuration **235**
  - Assigning Interfaces to Zones **236** • Opening Ports **239** • Opening `firewalld` Services **240** • For More Information **241**
- D.6 NTP Configuration **241**
- D.7 AutoYaST Packages Are Needed for the Second Stage **242**
- D.8 The CA Management Module Has Been Dropped **242**
- D.9 Upgrade **242**
  - Software **242** • Registration **243**

# 1 Introduction to AutoYaST

## 1.1 Motivation

Standard installations of SUSE Linux Enterprise Server are based on a wizard workflow. This is user-friendly and efficient when installing on few machines. However, it becomes repetitive and time-consuming when installing on many machines.

To avoid this, you could do mass deployments by copying the hard disk of the first successful installation. Unfortunately, that leads to the issue that even minute configuration changes between each machine have to later be dealt with individually. For example, when using static IP addresses, these IP addresses would have to be reset for each machine.

A regular installation of SUSE Linux Enterprise Server is semi-automated by default. The user is prompted to select the necessary information at the beginning of the installation (usually language only). YaST then generates a proposal for the underlying system depending on different factors and system parameters. Usually—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.

AutoYaST can be used where no user intervention is required or where customization is required. Using an AutoYaST control file, YaST prepares the system for a custom installation and does not interact with the user, unless specified in the file controlling the installation.

AutoYaST is not an automated GUI system. This means that usually many screens will be skipped—you will never see the language selection interface, for example. AutoYaST will simply pass the language parameter to the sub-system without displaying any language related interface.

## 1.2 Overview and Concept

Using AutoYaST, multiple systems can easily be installed in parallel and quickly. They need to share the same environment and similar, but not necessarily identical, hardware. The installation is defined by an XML configuration file (usually named `autoinst.xml`) called the “AutoYaST control file”. It can initially be created using existing configuration resources easily be tailored for any specific environment.

AutoYaST is fully integrated and provides various options for installing and configuring a system. The main advantage over 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 is 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 fed into YaST.
- **Installation:** YaST performs the installation of the basic system using the data from the AutoYaST control file.
- **Configuration:** After the installation of the basic system, the system configuration is performed in the second stage of the installation. User-defined post-installation scripts from the AutoYaST control file will also be executed at this stage.



## Note: Second Stage

A regular installation of SUSE Linux Enterprise Server 15 is performed in a single stage. The auto-installation process, however, is divided into two stages. After the installation of the basic system the system boots into the second stage where the system configuration is done.

The packages `autoyast2` and `autoyast2-installation` have to be installed to run the second stage in the installed system correctly. Otherwise an error will be shown before booting into the installed system.

The second stage can be turned off with the `second_stage` parameter:

```
<general>
  <mode>
    <confirm config:type="boolean">false</confirm>
    <second_stage config:type="boolean">false</second_stage>
  </mode>
</general>
```

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

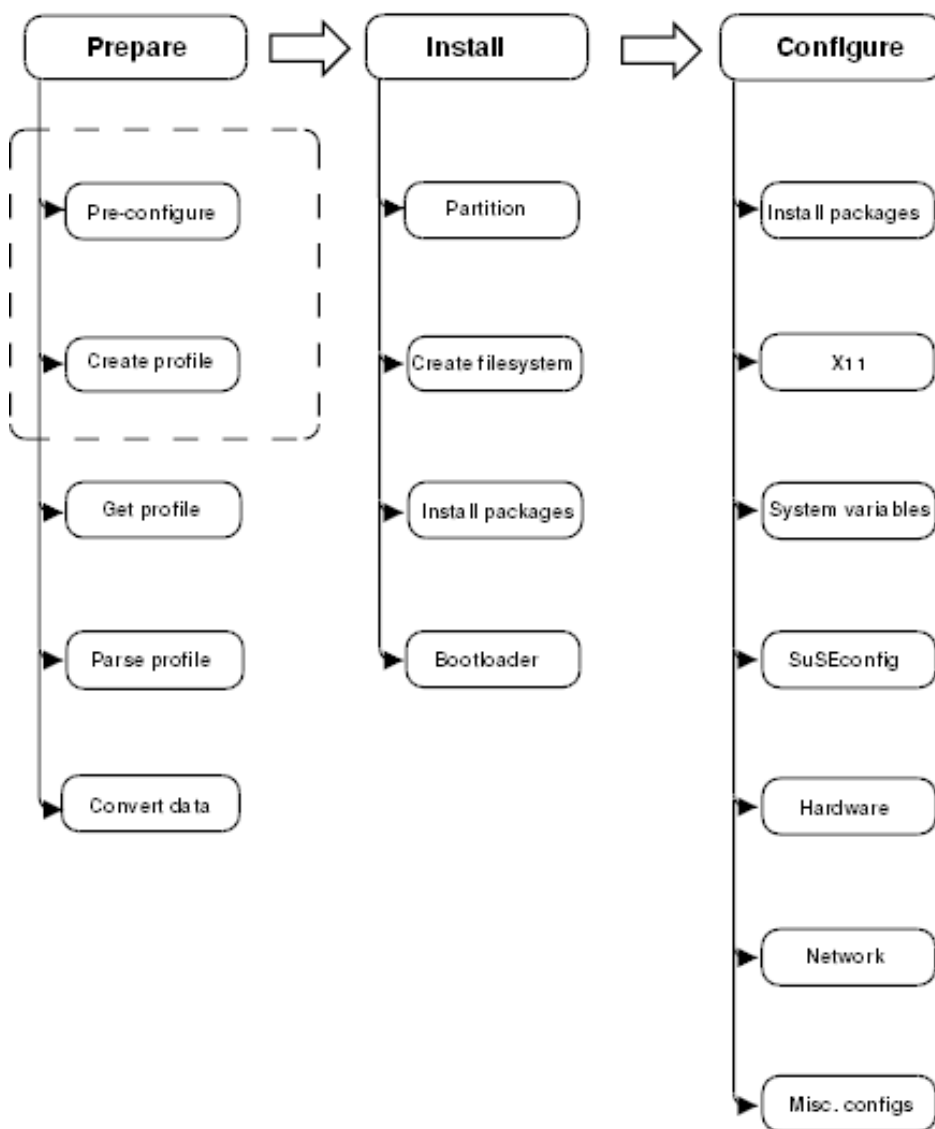


FIGURE 1.1: AUTO-INSTALLATION PROCESS

# I Understanding and Creating the AutoYaST Control File

- 2 The AutoYaST Control File 5
- 3 Creating an AutoYaST Control File 9

## 2 The AutoYaST Control File

### 2.1 Introduction

A *control file*, also known as *profile*, is a configuration description for a single system. It consists of sets of resources with properties including support for complex structures such as lists, records, trees and large embedded or referenced objects.



#### Important: Control Files from SLES 11 Releases are Incompatible

A lot of major changes were introduced with SUSE Linux Enterprise Server 12 (the switch to systemd and GRUB 2 for example). These changes also required fundamental changes in AutoYaST, therefore you cannot use AutoYaST control files created on SUSE Linux Enterprise Server 11 to install SUSE Linux Enterprise Server 15 and vice versa.

### 2.2 Format

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

The AutoYaST control file uses XML to describe the system installation and configuration. XML is a commonly used markup, and many users are familiar with the concepts of the language and the tools used to process XML files. If you edit an existing control file or create a control file using an editor from scratch, it is strongly recommended to validate the control file. This can be done using a validating XML parser such as `xmllint` or `jing`, for example (see [Section 3.3, “Creating/Editing a Control File Manually”](#)).

The following example shows a control file in XML format:

EXAMPLE 2.1: AUTOYAST CONTROL FILE (PROFILE)

```
<?xml version="1.0"?>
<!DOCTYPE profile>
<profile
  xmlns="http://www.suse.com/1.0/yast2ns"
  xmlns:config="http://www.suse.com/1.0/configns">
  <partitioning config:type="list">
```

```

<drive>
  <device>/dev/sda</device>
  <partitions config:type="list">
    <partition>
      <filesystem config:type="symbol">btrfs</filesystem>
      <size>10G</size>
      <mount></mount>
    </partition>
    <partition>
      <filesystem config:type="symbol">xfs</filesystem>
      <size>120G</size>
      <mount>/data</mount>
    </partition>
  </partitions>
</drive>
</partitioning>
<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>
</profile>

```

## 2.3 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>
<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 schema files

### 2.3.1 Resources and Properties

A resource element either contains multiple and distinct property and resource elements, or multiple instances of the same resource element, or it is empty. The permissible content of a resource element is specified in the schema files.

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 schema files

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

An empty element, such as `<foo></foo>` or `<bar/>`, will *not* be present in the parsed data model. Usually this is interpreted as wanting a sensible default value. In cases where you need an explicitly empty string instead, use a CDATA section: `<foo><![CDATA[]]></foo>`.

### 2.3.2 Nested Resources

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

There are two kinds of nested resources: maps and lists. Maps, also known as associative arrays, hashes, or dictionaries, contain mixed contents, identified by their tag names. Lists, or arrays, have all items of the same type.

#### EXAMPLE 2.3: NESTED RESOURCES

```
...
<drive>
  <device>/dev/sda</device>
  <partitions config:type="list">
    <partition>
```



```

    <size>10G</size>
    <mount></mount>
  </partition>
  <partition>
    <size>1G</size>
    <mount>/tmp</mount>
  </partition>
</partitions>
</drive>
....

```

In the example above, the `drive` resource is a map consisting of a `device` property and a `partitions` resource. The `partitions` resource is a list containing multiple instances of the `partition` resource. Each `partition` resource is a map containing a `size` and `mount` property. The default type of a nested resource is map. Lists must be marked as such using the `config:type="list"` attribute.

### 2.3.3 Attributes

Global attributes are used to define metadata on resources and properties. Attributes are used to define context switching. They are also used for naming and typing properties as shown in the previous sections. Attributes are in a separate namespace so they do not need to be treated as reserved words in the default namespace.

The `config:type` attribute determines the type of the resource or property in the parsed data model. For resources, lists need a `list` type whereas a map is the default type that does not need an attribute. For properties, `boolean`, `symbol`, and `integer` can be used, the default being a string.

Attributes are not optional. It may appear that attributes are optional, because various parts of the schema are not very consistent in their usage of data types. In some places an enumeration is represented by a symbol, elsewhere a string is required. One resource needs `config:type="integer"`, another will parse the number from a string property. Some resources use `config:type="boolean"`, others want `yes` or even `1`. If in doubt, consult the schema file.

## 3 Creating an AutoYaST Control File

### 3.1 Collecting Information

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

- Hard disk types and sizes
- Graphical interface and attached monitor, if any
- Network interface and MAC address if known (for example, when using DHCP)

Also verify that both autoyast2-installation and autoyast2 are installed.

### 3.2 Using the Configuration Management System (CMS)

To create the control file for one or more computers, a configuration interface based on YaST is provided. This system depends on existing modules which are usually used to configure a computer in regular operation mode, for example, after SUSE Linux Enterprise Server is installed. The configuration management system lets you easily create control files and manage a repository of configurations for use in a networked environment with multiple clients.

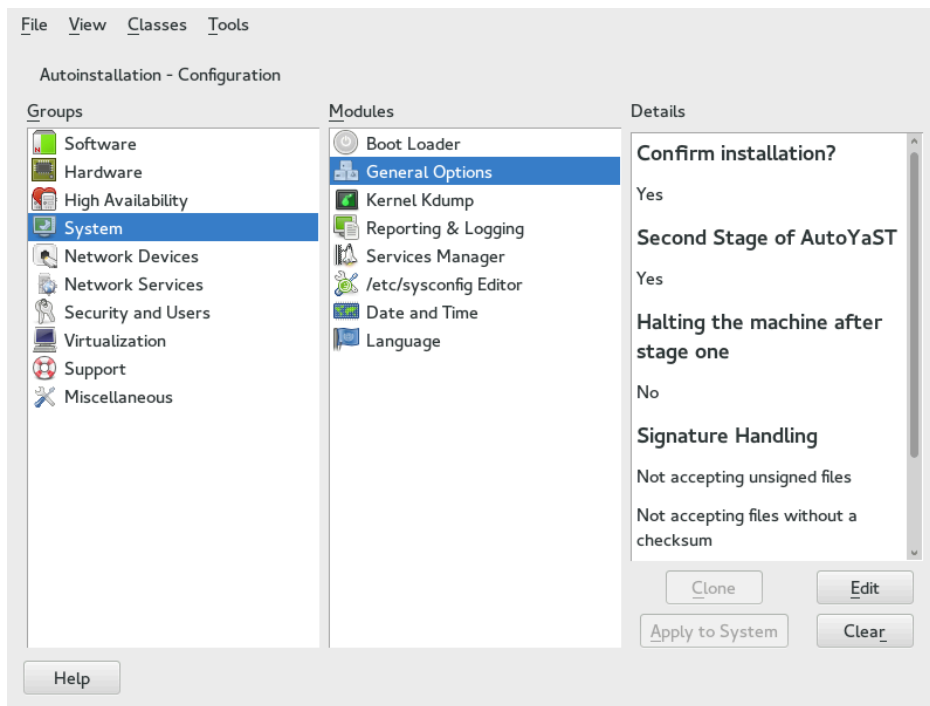


FIGURE 3.1: CONFIGURATION SYSTEM

### 3.2.1 Creating a New Control File

The easiest way to create an AutoYaST profile is to use an existing SUSE Linux Enterprise Server system as a template. On an already installed system, launch *YaST* › *Miscellaneous* › *Autoinstallation Configuration*. Then select *Tools* › *Create Reference Profile* from the menu. Choose the system components you want to include in the profile. Alternatively, create a profile containing the complete system configuration by launching *YaST* › *Miscellaneous* › *Autoinstallation Cloning System* or running `sudo yast clone_system` from the command line.

Both methods will create the file `/root/autoinst.xml`. The cloned profile can be used to set up an identical clone of the system it was created from. However, you usually want to adjust the file to allow for installing multiple machines that are very similar, but not identical. This can be done by adjusting the profile with your favorite text/XML editor.

With some exceptions, almost all resources of the control file can be configured using the configuration management system. The system offers flexibility and the configuration of some resources is identical to the one available in the YaST 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 a CMS guarantees the validity of the resulting control file and its direct use for starting automated installation.

Make sure the configuration system is installed (package `autoyast2`) and call it using the YaST control center or 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
```

### 3.3 Creating/Editing a Control File Manually

If editing the control file manually, make sure it has a valid syntax. To check the syntax, use the tools already available on the distribution. For example, to verify that the file is well-formed (has a valid XML structure), use the utility `xmllint` available with the `libxml2` package:

```
xmllint <control file>
```

If the control file is not well formed, for example, if a tag is not closed, `xmllint` will report the errors.

To validate the control file, use the tool `jing` from the package with the same name. During validation, misplaced or missing tags and attributes and wrong attribute values are detected. The `jing` package is provided with the SUSE Software Development Kit.

```
jing /usr/share/YaST2/schema/autoyast/rng/profile.rng <control file>
```

`/usr/share/YaST2/schema/autoyast/rng/profile.rng` is provided by the package `yast2-schema`. This file describes the syntax and classes of an AutoYaST profile.

Before going on with the autoinstallation, fix any errors resulting from such checks. The autoinstallation process cannot be started with an invalid and not well-formed control file.

You can use any XML editor available on your system or any text editor with XML support (for example, Emacs, Vim). However, it is not optimal to create the control file manually for many machines and it should only be seen as an interface between the autoinstallation engine and the Configuration Management System (CMS).



#### Tip: Using Emacs as an XML Editor

The built-in `nxml`-mode turns Emacs into a fully-fledged XML editor with automatic tag completion and validation. Refer to the Emacs help for instructions on how to set up `nxml`-mode.

## 3.4 Creating a Control File via Script with XSLT

If you have a template and want to change a few things via script or command line, use an XSLT processor like `xsltproc`. For example, if you have an AutoYaST control file and want to fill out the host name via script for any reason. (If doing this often, you should consider scripting it.)

First, create an XSL file:

EXAMPLE 3.1: EXAMPLE FILE FOR REPLACING THE HOST NAME/DOMAIN BY SCRIPT

```
<?xml version="1.0" encoding="utf-8"?>
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
  xmlns:y2="http://www.suse.com/1.0/yast2ns"
  xmlns:config="http://www.suse.com/1.0/configns"
  xmlns="http://www.suse.com/1.0/yast2ns"
  version="1.0">
  <xsl:output method="xml" encoding="UTF-8" indent="yes" omit-xml-declaration="no" cdata-
section-elements="source"/>

  <!-- the parameter names -->
  <xsl:param name="hostname"/>
  <xsl:param name="domain"/>

  <xsl:template match="/">
    <xsl:apply-templates select="@*|node()"/>
  </xsl:template>

  <xsl:template match="y2:dns">
    <xsl:copy>
      <!-- where to copy the parameters -->
      <domain><xsl:value-of select="string($domain)"/></domain>
      <hostname><xsl:value-of select="string($hostname)"/></hostname>
      <xsl:apply-templates select="@*|node()"/>
    </xsl:copy>
  </xsl:template>

  <xsl:template match="@*|node()" >
    <xsl:copy>
      <xsl:apply-templates select="@*|node()"/>
    </xsl:copy>
  </xsl:template>

</xsl:stylesheet>
```

This file expects the host name and the domain name as parameters from the user.

```
<xsl:param name="hostname"/>  
<xsl:param name="domain"/>
```

There will be a copy of those parameters in the DNS section of the control file. This means that if there already is a domain element in the DNS section, you will get a second one, which is not good.

For more information about XSLT, go to the official Web page [www.w3.org/TR/xslt](http://www.w3.org/TR/xslt) (<http://www.w3.org/TR/xslt>) ↗

## II AutoYaST Configuration Examples

### 4 Configuration and Installation Options 15

## 4 Configuration and Installation Options

This section contains configuration examples for services, registration, user and group management, upgrades, partitioning, configuration management, SSH key management, firewall configuration, and other installation options.

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

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

YaST will install packages required in the second phase of the installation and before the post-installation phase of AutoYaST has started. However, if necessary YaST modules are not available in the system, important configuration steps will be skipped. For example, no security settings will be configured if `yast2-security` is not installed.

### 4.1 General Options

The general section includes all settings that influence the installation workflow. The overall structure of this section looks like the following:

```
<?xml version="1.0"?>
<!DOCTYPE profile>
<profile xmlns="http://www.suse.com/1.0/yast2ns"
  xmlns:config="http://www.suse.com/1.0/configs">
  <general>
    <ask-list>❶
      ...
    </ask-list>
    <cio_ignore>❷
      ...
    </cio_ignore>
    <mode>❸
      ...
    </mode>
    <proposals>❹
      ...
    </proposals>
    <self_update>❺
```



```

...
</self_update>
<self_update_url>
...
</self_update_url>
<semi-automatic config:type="list">❶
...
</semi-automatic>
<signature-handling>❷
...
</signature-handling>
<storage>❸
...
</storage>
<wait>❹
...
</wait>
</general>
<profile>

```

- ❶ *Section 4.33, "Ask the User for Values during Installation"*
- ❷ *Section 4.1.8, "Blacklisting Unused Devices on IBM IBM Z"*
- ❸ *Section 4.1.1, "The Mode Section"*
- ❹ *Section 4.1.2, "Configuring the Installation Settings Screen"*
- ❺ *Section 4.1.3, "The Self-Update Section"*
- ❻ *Section 4.1.4, "The Semi-Automatic Section"*
- ❼ *Section 4.1.5, "The Signature Handling Section"*
- ❽ *Section 4.1.6, "The Storage Section"*
- ❾ *Section 4.1.7, "The Wait Section"*

## 4.1.1 The Mode Section

The mode section configures the behavior of AutoYaST with regards to user confirmations and rebooting. The following elements are allowed in the `mode` section:

### `activate_systemd_default_target`

If you set this entry to `false`, the default `systemd` target will not be activated via the call `systemctl isolate`. Setting this value is optional. The default is `true`.

```
<general>
```

```

<mode>
  <activate_systemd_default_target config:type="boolean">
    true
  </activate_systemd_default_target>
</mode>
...
</general>

```

### confirm

By default, the installation stops at the *Installation Settings* screen. Up to this point, no changes have been made to the system and settings may be changed on this screen. To proceed and finally start the installation, the user needs to confirm the settings. By setting this value to false the settings are automatically accepted and the installation starts. Only set to false if you want to carry out a fully unattended installation. Setting this value is optional. The default is true.

```

<general>
  <mode>
    <confirm config:type="boolean">true</confirm>
  </mode>
  ...
</general>

```

### confirm\_base\_product\_license

If you set this to true, the EULA of the base product will be shown. The user needs to accept this license. Otherwise the installation will be canceled. Setting this value is optional. The default is false. This setting applies to the base product license only. Use the flag confirm\_license in the add-on section for additional licenses (see [Section 4.9.3, "Installing Additional/Customized Packages or Products"](#) for details).

```

<general>
  <mode>
    <confirm_base_product_license config:type="boolean">
      false
    </confirm_base_product_license>
  </mode>
  ...
</general>

```

### final\_halt

If you set this to true, the machine will shut down at the very end of the installation (when everything is installed and configured at the end of the second stage). Setting this value is optional. The default is true. It makes no sense to set both this and final\_reboot to true.

```

<general>
  <mode>
    <final_halt config:type="boolean">false</final_halt>
  </mode>
  ...
</general>

```

### final\_reboot

If you set this to true, the machine will reboot at the end of the installation (when everything is installed and configured at the end of the second stage). Setting this value is optional. The default is true. It makes no sense to set both this and final\_halt to true.

```

<general>
  <mode>
    <final_reboot config:type="boolean">true</final_reboot>
  </mode>
  ...
</general>

```

### final\_restart\_services

If you set this entry to false, services will *not* be restarted at the end of the installation (when everything is installed and configured at the end of the second stage). Setting this value is optional. The default is true.

```

<general>
  <mode>
    <final_restart_services config:type="boolean">
      true
    </final_restart_services>
  </mode>
  ...
</general>

```

### halt

Shuts down the machine after the first stage. All packages and the boot loader have been installed and all your chroot scripts have run. Instead of rebooting into stage two, the machine is turned off. If you turn it on again, the machine boots and the second stage of the autoinstallation starts. Setting this value is optional. The default is false.

```

<general>
  <mode>
    <halt config:type="boolean">false</halt>
  </mode>
  ...

```

```
</general>
```

#### max\_systemd\_wait

Specifies how long AutoYaST waits (in seconds) at most for systemd to set up the default target. Setting this value is optional and should not normally be required. The default is 30 (seconds).

```
<general>
  <mode>
    <max_systemd_wait config:type="integer">30</max_systemd_wait>
  </mode>
  ...
</general>
```

#### ntp\_sync\_time\_before\_installation

Specify the NTP server with which to synchronize time before starting the installation. Time synchronization will only be done if this option is set. Keep in mind that you need a network connection and access to a time server. Setting this value is optional. By default no time synchronization will be done.

```
<general>
  <mode>
    <ntp_sync_time_before_installation>
      &ntpname;
    </max_systemd_wait>
  </mode>
  ...
</general>
```

#### second\_stage

A regular installation of SUSE Linux Enterprise Server is performed in a single stage. The auto-installation process, however, is divided into two stages. After the installation of the basic system the system boots into the second stage where the system configuration is done. Set this option to false to disable the second stage. Setting this value is optional. The default is true.

```
<general>
  <mode>
    <second_stage config:type="boolean">true</second_stage>
  </mode>
  ...
</general>
```

## 4.1.2 Configuring the Installation Settings Screen

AutoYaST allows you to configure the *Installation Settings* screen, which shows a summary of the installation settings. On this screen, the user can change the settings before confirming them to start the installation. Using the `proposal` tag, you can control which settings (“proposals”) are shown in the installation screen. A list of valid proposals for your products is available from the `/control.xml` file on the installation medium. This setting is optional. By default all configuration options will be shown.

```
<proposals config:type="list">
  <proposal>partitions_proposal</proposal>
  <proposal>timezone_proposal</proposal>
  <proposal>software_proposal</proposal>
</proposals>
```

## 4.1.3 The Self-Update Section

During the installation, YaST can update itself to solve bugs in the installer that were discovered after the release. Refer to the *Deployment Guide* for further information about this feature. Use the following tags to configure the YaST self-update:

### self\_update

If set to `true` or `false`, this option enables or disables the YaST self-update feature. Setting this value is optional. The default is `true`.

```
<general>
  <self_update config:type="boolean">true</self_update>
  ...
</general>
```

Alternatively, you can specify the boot parameter `self_update=1` on the kernel command line.

### self\_update\_url

Location of the update repository to use during the YaST self-update. For more information, refer to the *Deployment Guide*.



## Important: Installer Self-Update Repository Only

The `self_update_url` parameter expects only the installer self-update repository URL. Do not supply any other repository URL—for example the URL of the software update repository.

```
<general>
  <self_update_url>
    http://example.com/updates/$arch
  </self_update_url>
  ...
</general>
```

The URL may contain the variable `$arch`. It will be replaced by the system's architecture, such as `x86_64`, `s390x`, etc.

Alternatively, you can specify the boot parameter `self_update=1` together with `self_update=URL` on the kernel command line.

### 4.1.4 The Semi-Automatic Section

AutoYaST offers to start some YaST modules during the installation. This is useful if you want to give the administrators installing the machine the possibility to manually configure some aspects of the installation while at the same time automating the rest of the installation. Within the semi-automatic section, you can start the following YaST modules:

- The network settings module (`networking`)
- The partitioner (`partitioning`)
- The registration module (`scc`)

The following example starts all three supported YaST modules during the installation:

```
<general>
  <semi-automatic config:type="list">
    <semi-automatic_entry>networking</semi-automatic_entry>
    <semi-automatic_entry>scc</semi-automatic_entry>
    <semi-automatic_entry>partitioning</semi-automatic_entry>
  </semi-automatic>
</general>
```

## 4.1.5 The Signature Handling Section

By default AutoYaST will only install signed packages from sources with known GPG keys. Use this section to overwrite the default settings.



### Warning: Overwriting the Signature Handling Defaults

Installing unsigned packages, packages with failing checksum checks, or packages from sources you do not trust is a major security risk. Packages may have been modified and may install malicious software on your machine. Only overwrite the defaults in this section if you are sure the repository and packages can be trusted. SUSE is not responsible for any problems arising from software installed with integrity checks disabled.

Default values for all options are false. If an option is set to false and a package or repository fails the respective test, it is silently ignored and will not be installed.

#### accept\_unsigned\_file

If set to true, AutoYaST will accept unsigned files like the content file.

```
<general>
  <signature-handling>
    <accept_unsigned_file config:type="boolean">
      false
    </accept_unsigned_file>
  </signature-handling>
  ...
</general>
```

#### accept\_file\_without\_checksum

If set to true, AutoYaST will accept files without a checksum in the content file.

```
<general>
  <signature-handling>
    <accept_file_without_checksum config:type="boolean">
      false
    </accept_file_without_checksum>
  </signature-handling>
  ...
</general>
```

#### accept\_verification\_failed

If set to true, AutoYaST will accept signed files even when the signature verification fails.

```

<general>
  <signature-handling>
    <accept_verification_failed config:type="boolean">
      false
    </accept_verification_failed>
  </signature-handling>
  ...
</general>

```

#### accept\_unknown\_gpg\_key

If set to true, AutoYaST will accept new GPG keys of the installation sources, for example the key used to sign the content file.

```

<general>
  <signature-handling>
    <accept_unknown_gpg_key config:type="boolean">
      false
    </accept_unknown_gpg_key>
  </signature-handling>
  ...
</general>

```

#### accept\_non\_trusted\_gpg\_key

Set this option to true to accept known keys you have not yet trusted.

```

<general>
  <signature-handling>
    <accept_non_trusted_gpg_key config:type="boolean">
      false
    </accept_non_trusted_gpg_key>
  </signature-handling>
  ...
</general>

```

#### import\_gpg\_key

If set to true, AutoYaST will accept and import new GPG keys on the installation source in its database.

```

<general>
  <signature-handling>
    <import_gpg_key config:type="boolean">
      false
    </import_gpg_key>
  </signature-handling>
  ...
</general>

```



## 4.1.6 The Storage Section

This section lets you enable multipath support for the installation. You may also configure the partition alignment settings here.

### btrfs\_set\_default\_subvolume\_name

See [Section 4.5.3, “Btrfs subvolumes”](#) for more information.

### start\_multipath

When installing on a network storage that is accessed via multiple paths, you need to enable multipath for the installation by setting this parameter to true. Setting this value is optional. The default is false.

```
<general>
<storage>
  <start_multipath config:type="boolean">false</start_multipath>
</storage>
...
</general>
```

Alternatively, you can use the following parameter on the Kernel command line: LIBS-TORAGE\_MULTIPATH\_AUTOSTART=ON

## 4.1.7 The Wait Section

In the second stage of the installation the system is configured by running modules, for example the network configuration. Within the wait section you can define scripts that will get executed before and after a specific module has run. You can also configure a span of time in which the system is inactive (“sleeps”) before and after each module.

### pre-modules

Defines scripts and sleep time executed before a configuration module starts. The following code shows an example setting the sleep time to ten seconds and executing an echo command before running the network configuration module.

```
<general>
<wait>
  <pre-modules config:type="list">
    <module>
      <name>networking</name>
      <sleep>
        <time config:type="integer">10</time>
      </sleep>
    </module>
  </pre-modules>
</wait>
</general>
```

```

    <feedback config:type="boolean">true</feedback>
  </sleep>
</script>
  <source>echo foo</source>
  <debug config:type="boolean">>false</debug>
</script>
</module>
</pre-modules>
...
</wait>
<general>

```

### post-modules

Defines scripts and sleep time executed after a configuration module starts. The following code shows an example setting the sleep time to ten seconds and executing an echo command after running the network configuration module.

```

<general>
  <wait>
    <post-modules config:type="list">
      <module>
        <name>networking</name>
        <sleep>
          <time config:type="integer">10</time>
          <feedback config:type="boolean">true</feedback>
        </sleep>
        <script>
          <source>echo foo</source>
          <debug config:type="boolean">>false</debug>
        </script>
      </module>
    </post-modules>
    ...
  </wait>
</general>

```

## 4.1.8 Blacklisting Unused Devices on IBM IBM Z

On IBM IBM Z you can prevent the kernel from looking at unused hardware devices, by running **cio\_ignore** and blacklisting them. This is done by setting the AutoYaST parameter with the same name to true. Setting this value is optional and only applies to installations on IBM IBM Z hardware. The default is false.

```
<general>
```

```
<cio_ignore config:type="boolean">false</cio_ignore>
...
<general>
```

### 4.1.9 Examples for the general Section

Find examples covering several use cases in this section.

#### EXAMPLE 4.1: GENERAL OPTIONS

This example shows the most commonly used options in the general section. The scripts in the pre- and post-modules sections are only dummy scripts illustrating the concept.

```
<?xml version="1.0"?>
<!DOCTYPE profile>
<profile xmlns="http://www.suse.com/1.0/yast2ns"
  xmlns:config="http://www.suse.com/1.0/configns">
  <general>
    <mode>
      <halt config:type="boolean">false</halt>
      <forceboot config:type="boolean">false</forceboot>
      <final_reboot config:type="boolean">false</final_reboot>
      <final_halt config:type="boolean">false</final_halt>
      <confirm_base_product_license config:type="boolean">
        false
      </confirm_base_product_license>
      <confirm config:type="boolean">true</confirm>
      <second_stage config:type="boolean">true</second_stage>
    </mode>
    <proposals config:type="list">
      <proposal>partitions_proposal</proposal>
    </proposals>
    <self_update config:type="boolean">true</self_update>
    <self_update_url>http://example.com/updates/$arch</self_update_url>
    <signature-handling>
      <accept_unsigned_file config:type="boolean">
        true
      </accept_unsigned_file>
      <accept_file_without_checksum config:type="boolean">
        true
      </accept_file_without_checksum>
      <accept_verification_failed config:type="boolean">
        true
      </accept_verification_failed>
      <accept_unknown_gpg_key config:type="boolean">
        true
      </accept_unknown_gpg_key>
    </signature-handling>
  </general>
</profile>
```

```

</accept_unknown_gpg_key>
<import_gpg_key config:type="boolean">true</import_gpg_key>
<accept_non_trusted_gpg_key config:type="boolean">
true
</accept_non_trusted_gpg_key>
</signature-handling>
<wait>
<pre-modules config:type="list">
<module>
<name>networking</name>
<sleep>
<time config:type="integer">10</time>
<feedback config:type="boolean">true</feedback>
</sleep>
<script>
<source>&gt;![CDATA[
echo "Sleeping 10 seconds"
]]&gt;</source>
<debug config:type="boolean">false</debug>
</script>
</module>
</pre-modules>
<post-modules config:type="list">
<module>
<name>networking</name>
<sleep>
<time config:type="integer">10</time>
<feedback config:type="boolean">true</feedback>
</sleep>
<script>
<source>&gt;![CDATA[
echo "Sleeping 10 seconds"
]]&gt;</source>
<debug config:type="boolean">false</debug>
</script>
</module>
</post-modules>
</wait>
</general>
</profile>

```

## 4.2 Reporting

The `report` resource manages three types of pop-ups that may appear during installation:

- message pop-ups (usually non-critical, informative messages),
- warning pop-ups (if something might go wrong),
- error pop-ups (in case an error occurs).

### EXAMPLE 4.2: REPORTING BEHAVIOR

```
<report>
  <errors>
    <show config:type="boolean">true</show>
    <timeout config:type="integer">0</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>
  <messages>
    <show config:type="boolean">true</show>
    <timeout config:type="integer">10</timeout>
    <log config:type="boolean">true</log>
  </messages>
  <yesno_messages>
    <show config:type="boolean">true</show>
    <timeout config:type="integer">10</timeout>
    <log config:type="boolean">true</log>
  </yesno_messages>
</report>
```

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.

The default setting in auto-installation mode is to show errors without timeout and to show all warnings/messages with a timeout of 10 seconds.



## Warning: 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 show up ignoring your settings in the `report` section. Usually those messages will need to be answered with *Yes* or *No*.

## 4.3 System Registration and Extension Selection

Registering the system with the registration server can be configured within the `suse_register` resource. The following example registers the system with the SUSE Customer Center. In case your organization provides its own registration server, you need to specify the required data with the `reg_server*` properties. Refer to the list below for details.

```
<suse_register>
  <do_registration config:type="boolean">true</do_registration>
  <email>tux@example.com</email>
  <reg_code>MY_SECRET_REGCODE</reg_code>
  <install_updates config:type="boolean">true</install_updates>
  <slp_discovery config:type="boolean">false</slp_discovery>
</suse_register>
```

As an alternative to the fully automated registration, AutoYaST can also be configured to start the YaST registration module during the installation. This offers the possibility to enter the registration data manually. The following XML code is required:

```
<general>
  <semi-automatic config:type="list">
    <semi-automatic_entry>scc</semi-automatic_entry>
  </semi-automatic>
</general>
```



## Tip: Using the Installation Network Settings

In case you need to use the same network settings that were used for the installation, AutoYaST needs to run the network setup in stage 1 right before the registration is started:

```
<networking>
  <setup_before_proposal config:type="boolean">true</setup_before_proposal>
</networking>
```

Element	Description	Comment
<u>do_registration</u>	Boolean <pre>&lt;do_registration   config:type="boolean" &gt;true&lt;/do_registration&gt;</pre>	Specify whether the system should be registered or not. If set to <u>false</u> all other options are ignored and the system is not registered.
<u>e-mail</u>	E-mail address <pre>&lt;email&gt;tux@example.com&lt;/email&gt;</pre>	Optional. The e-mail address matching the registration code.
<u>reg_code</u>	Text <pre>&lt;reg_code&gt;SECRET_REGCODE&lt;/reg_code&gt;</pre>	Required. Registration code.
<u>install_updates</u>	Boolean <pre>&lt;install_updates   config:type="boolean" &gt;true&lt;/install_updates&gt;</pre>	Optional. Determines if updates from the Updates channels should be installed. The default value is to not install them ( <u>false</u> ).
<u>slp_discovery</u>	Boolean <pre>&lt;slp_discovery   config:type="boolean" &gt;true&lt;/slp_discovery&gt;</pre>	Optional. Search for a registration server via SLP. The default value is <u>false</u> . Expects to find a single server. If more than one server is found, the installation will fail. In case there is more than one registration server available, you need to specify one with <u>reg_server</u> . If neither <u>slp_discovery</u> nor <u>reg_server</u> are set, the system is registered with the SUSE Customer Center.

Element	Description	Comment
		This setting also affects the self-update feature: If it is disabled, no SLP search will be performed.
<u>reg_server</u>	URL  <pre>&lt;reg_server&gt;   https://smt.example.com &lt;/reg_server&gt;</pre>	Optional. RMT server URL. If neither <u>slp_discovery</u> nor <u>reg_server</u> are set, the system is registered with the SUSE Customer Center.  The RMT server is queried for a URL of the self-update repository. So if <u>self_update_url</u> is not set, the RMT server influences where the self-updates are downloaded from. Check out the <i>Deployment Guide</i> to find further information about this feature.
<u>reg_server_cert_fingerprint_type</u>	SHA1 or SHA256  <pre>&lt;reg_server_cert_fingerprint_type&gt;   SHA1 &lt;/reg_server_cert_fingerprint_type&gt;</pre>	Optional. Requires a checksum value provided with <u>reg_server_cert_fingerprint</u> . Using the fingerprint is recommended, since it ensures the SSL certificate is verified. The matching certificate will be automatically imported when the SSL communication fails because of a verification error.
<u>reg_server_cert_fingerprint</u>	Server Certificate Fingerprint value in hexadecimal notion (case-insensitive).	Optional. Requires a fingerprint type value provided with <u>reg_serv-</u>



Element	Description	Comment
	<pre>&lt;reg_server_cert_fingerprint&gt;   01:AB...:EF &lt;/reg_server_cert_fingerprint&gt;</pre>	<u>er_cert_fingerprint_type</u> . Using the fingerprint is recommended, since it ensures the SSL certificate is verified. The matching certificate will be automatically imported when the SSL communication fails because of a verification error.
<u>reg_server_cert</u>	URL <pre>&lt;reg_server_cert&gt;   http://smt.example.com/   smt.crt &lt;/reg_server_cert&gt;</pre>	Optional. URL of the SSL certificate on the server. Using this option is not recommended, since the certificate that is downloaded is not verified. Use <u>reg_server_cert_fingerprint</u> instead.
<u>addons</u>	Add-ons list	Specify an extension from the registration server that should be added to the installation repositories. See <a href="#">Section 4.3.1, "Extensions"</a> for details.



### Tip: Obtaining a Server Certificate Fingerprint

To obtain a server certificate fingerprint for use with the reg\_server\_cert\_fingerprint entry, run the following command on the SMT server (edit the default path to the smt.crt file, if needed):

```
openssl x509 -noout -in /srv/www/htdocs/smt.crt -fingerprint -sha256
```

To retrieve a fingerprint from the SMT server, use the following command:

```
curl --insecure -v https://scc.suse.com/smt.crt 2> /dev/null | openssl \
x509 -noout -fingerprint -sha256
```

Replace `scc.suse.com` with your server.

*Note:* This can be used in a trusted network only! In a non-trusted network, for example the Internet, you should get the fingerprint directly from the server by other means. Fingerprints can be fetched via SSH, a saved server configuration and other sources. Alternatively, you can verify that the downloaded certificate is exactly the same as on the server.

### 4.3.1 Extensions

The SUSE Customer Center provides several extensions, such as `sle-module-development-tools` (Development Tools Module) that can be included as additional sources during the installation. Extensions can be added via the `addons` property within the `suse_register` block.



#### Note: Availability of Extensions

The availability of extensions is product and architecture dependent, not all extensions are available on all architectures.

Some extensions, such as `sle-ha`, require a registration code. Depending on your subscription, either use a dedicated registration code for the extension, or restate the code for the base product.


With **SUSEConnect --list-extensions** you can list all available extensions in a registered system. The result contains lines like:

```
Install with: SUSEConnect -p sle-module-development-tools/15.0/x86_64
```

The `-p` argument displays the `NAME/VERSION/ARCH` values that can be used in the AutoYaST profile as follows:

```
<addons config:type="list">
  <addon>
    <!-- Development Tools Module -->
```

```
<name>sle-module-development-tools</name>
<version>15</version>
<arch>x86_64</arch>
</addon>
</addons>
```

You may also see modules and extensions at <https://scc.suse.com/packages> .



## Note: Extension Dependencies

Since SLES 15, AutoYaST automatically reorders the extensions according to their dependencies during registration. This means the order of the extensions in the AutoYaST profile is not important.

Also AutoYaST automatically registers the dependent extensions even though they are missing in the profile. This means you are not required to fill the extensions list completely.

However, if the dependent extension requires a registration key, this must be specified in the profile, including the registration key. Otherwise the registration would fail.

## 4.4 The Boot Loader

This documentation is for **yast2-bootloader** and applies to GRUB 2. For older product versions shipping with legacy GRUB, refer to the documentation that comes with your distribution in /usr/share/doc/packages/autoyast2/

The general structure of the AutoYaST boot loader part looks like the following:

```
<bootloader>
  <loader_type>
    <!-- boot loader type (grub2 or grub2-efi) -->
  </loader_type>
  <global>
    <!--
      entries defining the installation settings for GRUB 2 and
      the generic boot code
    -->
  </global>
  <device_map config:type="list">
    <!-- entries defining the order of devices -->
  </device_map>
</bootloader>
```

### 4.4.1 Loader Type

This defines which boot loader (UEFI or BIOS/legacy) to use. Not all architectures support both legacy and EFI variants of the boot loader. The safest (default) option is to leave the decision up to the installer.

```
<loader_type>LOADER_TYPE</loader_type>
```

Possible values for LOADER\_TYPE are:

- default: The installer chooses the correct boot loader. This is the default when no option is defined.
- grub2: Use the legacy BIOS boot loader.
- grub2-efi: Use the EFI boot loader.
- none: The boot process is not managed and configured by the installer.

### 4.4.2 Globals

This is an important if optional part. Define here where to install GRUB 2 and how the boot process will work. Again, **yast2-bootloader** proposes a configuration if you do not define one. Usually the AutoYaST control file includes only this part and all other parts are added automatically during installation by **yast2-bootloader**. Unless you have some special requirements, do not specify the boot loader configuration in the XML file.

```
<global>
  <activate config:type="boolean">true</activate>
  <timeout config:type="integer">10</timeout>
  <suse_btrfs config:type="boolean">true</suse_btrfs>
  <terminal>gfxterm</terminal>
  <gfxmode>1280x1024x24</gfxmode>
</global>
```

Attribute	Description
<u>activate</u>	Set the boot flag on the boot partition. The boot partition can be <u>/</u> if there is no separate <u>/boot</u> partition. If the boot partition is on a logical partition, the boot flag is set to the extended partition.

Attribute	Description
	<pre>&lt;activate config:type="boolean"&gt;true&lt;/activate&gt;</pre>
<u>append</u>	<p>Kernel parameters added at the end of boot entries for normal and recovery mode.</p> <pre>&lt;append&gt;nomodeset vga=0x317&lt;/append&gt;</pre>
<u>boot_boot</u>	<p>Write GRUB 2 to a separate <code>/boot</code> partition. If no separate <code>/boot</code> partition exists, GRUB 2 will be written to <code>/</code>.</p> <pre>&lt;boot_boot&gt;false&lt;/boot_boot&gt;</pre>
<u>boot_custom</u>	<p>Write GRUB 2 to a custom device.</p> <pre>&lt;boot_custom&gt;/dev/sda3&lt;/boot_custom&gt;</pre>
<u>boot_extended</u>	<p>Write GRUB 2 to the extended partition (important if you want to use generic boot code and the <code>/boot</code> partition is logical). Note: if the boot partition is logical, you should use <u>boot_mbr</u> (write GRUB 2 to MBR) rather than <u>generic_mbr</u>.</p> <pre>&lt;boot_extended&gt;false&lt;/boot_extended&gt;</pre>
<u>boot_mbr</u>	<p>Write GRUB 2 to the MBR of the first disk in the order (device.map includes order of disks).</p> <pre>&lt;boot_mbr&gt;false&lt;/boot_mbr&gt;</pre>
<u>boot_root</u>	<p>Write GRUB 2 to <code>/</code> partition.</p> <pre>&lt;boot_root&gt;false&lt;/boot_root&gt;</pre>

Attribute	Description
<u>generic_mbr</u>	<p>Write generic boot code to the MBR (will be ignored if <u>boot_mbr</u> is set to <u>true</u>).</p> <pre>&lt;generic_mbr config:type="boolean"&gt;false&lt;/generic_mbr&gt;</pre>
<u>gfxmode</u>	<p>Graphical resolution of the GRUB 2 screen (requires <code>&lt;terminal&gt;</code> to be set to <u>gfx-term</u>. Valid entries are <u>auto</u>, <u>HORIZONTALxVERTICAL</u>, or <u>HORIZONTALxVERTICALxCOLOR DEPTH</u>. You can see the screen resolutions supported by GRUB 2 on a particular system by using the <u>vbeinfo</u> command at the GRUB 2 command line in the running system.</p> <pre>&lt;gfxmode&gt;1280x1024x24&lt;/gfxmode&gt;</pre>
<u>os_prober</u>	<p>If set to <u>true</u>, automatically searches for operating systems already installed and generates boot entries for them during the installation</p> <pre>&lt;os_prober config:type="boolean"&gt;false&lt;/os_prober&gt;</pre>
<u>suse_btrfs</u>	<p>Obsolete and no longer used. Booting from Btrfs snapshots is automatically enabled since SLES 12 SP2.</p>
<u>serial</u>	<p>Command to execute if the GRUB 2 terminal mode is set to <u>serial</u>.</p> <pre>&lt;serial&gt;   serial --speed=115200 --unit=0 --word=8   --parity=no --stop=1 &lt;/serials&gt;</pre>

Attribute	Description
<u>terminal</u>	Specify the GRUB 2 terminal mode to use, Valid entries are <u>console</u> , <u>gfxterm</u> , and <u>serial</u> . If set to <u>serial</u> , the serial command needs to be specified with <u>&lt;serial&gt;</u> , too.  <pre>&lt;terminal&gt;serial&lt;/terminal&gt;</pre>
<u>timeout</u>	The timeout in seconds until the default boot entry is booted automatically.  <pre>&lt;timeout config:type="integer"&gt;10&lt;/timeout&gt;</pre>
<u>trusted_boot</u>	If set to <u>true</u> , then Trusted GRUB is used. Trusted GRUB supports Trusted Platform Module (TPM). Works only for <u>grub2</u> boot-loader.  <pre>&lt;trusted_boot&gt;true&lt;/trusted_boot&gt;</pre>
<u>vgamode</u>	Adds the kernel parameter <u>vga=VALUE</u> to the boot entries.  <pre>&lt;vgamode&gt;0x317&lt;/vgamode&gt;</pre>
<u>xen_append</u>	Kernel parameters added at the end of boot entries for Xen guests.  <pre>&lt;xen_append&gt;nomodeset vga=0x317&lt;/xen_append&gt;</pre>
<u>xen_kernel_append</u>	Kernel parameters added at the end of boot entries for Xen kernels on the VM Host Server.  <pre>&lt;xen_kernel_append&gt;dom0_mem=768M&lt;/xen_kernel_append&gt;</pre>

### 4.4.3 Device map

GRUB 2 avoids mapping problems between BIOS drives and Linux devices by using device ID strings (UUIDs) or file system labels when generating its configuration files. GRUB 2 utilities create a temporary device map on the fly, which is usually sufficient, particularly on single-disk systems. However, if you need to override the automatic device mapping mechanism, create your custom mapping in this section.

```
<device_map config:type="list">
  <device_map_entry>
    <firmware>hd0</firmware> <!-- order of devices in target map -->
    <linux>/dev/disk/by-id/ata-ST3500418AS_6VM23FX0</linux> <!-- name of device (disk) -->
  </device_map_entry>
</device_map>
```

## 4.5 Partitioning

### 4.5.1 Drive Configuration

The elements listed below must be placed within the following XML structure:

```
<profile>
  <partitioning config:type="list">
    <drive>
      ...
    </drive>
  </partitioning>
</profile>
```

Attribute	Values	Description
<u>device</u>	The device you want to configure in this <drive> section. You can use persistent device names via id, like <u>/dev/disk/by-id/ata-WD-C_WD3200AAKS-75L9A0_WD-WMAY27368122</u> or <i>by-path</i> , like <u>/</u>	Optional. If left out, AutoYaST tries to guess the device. See <i>Tip: Skipping Devices</i> on how to influence guessing. If set to <u>ask</u> , AutoYaST will ask the user which device to use during installation.



Attribute	Values	Description
	<code>dev/disk/by-path/ pci-0001:00:03.0-sc- si-0:0:0:0.</code>  <code>&lt;device&gt;/dev/sda&lt;/device&gt;</code>	
<u>initialize</u>	<p>If set to <code>true</code>, the partition table gets wiped out before AutoYaST starts the partition calculation.</p> <pre>&lt;initialize   config:type="boolean"&gt;true&lt;/initialize&gt;</pre>	Optional. The default is <u>false</u> .
<u>partitions</u>	<p>A list of <code>&lt;partition&gt;</code> entries (see <a href="#">Section 4.5.2, "Partition Configuration"</a>).</p> <pre>&lt;partitions   config:type="list"&gt;   &lt;partition&gt;...&lt;/partition&gt;   ... &lt;/partitions&gt;</pre>	Optional. If no partitions are specified, AutoYaST will create a reasonable partitioning (see <a href="#">Section 4.5.5, "Automated Partitioning"</a> ).
<u>pesize</u>	<p>This value only makes sense with LVM.</p> <pre>&lt;pesize&gt;8M&lt;/pesize&gt;</pre>	Optional. Default is 4M for LVM volume groups.
<u>use</u>	<p>Specifies the strategy AutoYaST will use to partition the hard disk.</p>	This parameter should be provided.

Attribute	Values	Description
	<p>Choose between:</p> <ul style="list-style-type: none"> <li>• <code>all</code> (uses the whole device while calculating the new partitioning),</li> <li>• <code>linux</code> (only existing Linux partitions are used),</li> <li>• <code>free</code> (only unused space on the device is used, no other partitions are touched),</li> <li>• <code>1,2,3</code> (a list of comma separated partition numbers to use).</li> </ul>	
<code>type</code>	<p>Specify the type of the <code>drive</code>,</p> <p>Choose between:</p> <ul style="list-style-type: none"> <li>• <code>CT_DISK</code> for physical hard disks (default).</li> <li>• <code>CT_DMMULTIPATH</code> for Multipath devices (deprecated, implied with <code>CT_DISK</code>).</li> <li>• <code>CT_LVM</code> for LVM volume groups.</li> </ul> <pre>&lt;type   config:type="symbol"&gt;CT_LVM&lt;/type&gt;</pre>	Optional. Default is <code>CT_DISK</code> for a normal physical hard disk.

Attribute	Values	Description
<u>disklabel</u>	<p>Describes the type of the partition table.</p> <p>Choose between:</p> <ul style="list-style-type: none"> <li>• <u>msdos</u></li> <li>• <u>gpt</u></li> <li>• <u>none</u></li> </ul> <pre>&lt;disklabel&gt;gpt&lt;/disklabel&gt;</pre>	Optional. By default YaST decides what makes sense. If a partition table of a different type already exists, it will be recreated with the given type only if it does not include any partition that should be kept or reused. To use the disk without creating any partition, set this element to <u>none</u> .
<u>keep_unknown_lv</u>	<p>This value only makes sense for type = CT_LVM drives. If you are reusing a logical volume group and you set this to <u>true</u>, all existing logical volumes in that group will not be touched unless they are specified in the &lt;partitioning&gt; section. So you can keep existing logical volumes without specifying them.</p> <pre>&lt;keep_unknown_lv   config:type="boolean" &gt;false&lt;/keep_unknown_lv&gt;</pre>	Optional. The default is <u>false</u> .
<u>enable_snapshots</u>	<p>Enables snapshots on Btrfs file systems mounted at <u>/</u> (does not apply to other file systems, or Btrfs file systems not mounted at <u>/</u>).</p> <pre>&lt;enable_snapshots   config:type="boolean"</pre>	Optional. The default is <u>true</u> .

Attribute	Values	Description
	<code>&gt;false&lt;/enable_snapshots&gt;</code>	



## Tip: Skipping Devices

You can influence AutoYaST's device-guessing for cases where you do not specify a `<device>` entry on your own. Usually AutoYaST would use the first device it can find that looks reasonable but you can configure it to skip some devices like this:

```
<partitioning config:type="list">
  <drive>
    <initialize config:type="boolean">true</initialize>
    <skip_list config:type="list">
      <listentry>
        <!-- skip devices that use the usb-storage driver -->
        <skip_key>driver</skip_key>
        <skip_value>usb-storage</skip_value>
      </listentry>
      <listentry>
        <!-- skip devices that are smaller than 1GB -->
        <skip_key>size_k</skip_key>
        <skip_value>1048576</skip_value>
        <skip_if_less_than config:type="boolean">true</skip_if_less_than>
      </listentry>
      <listentry>
        <!-- skip devices that are larger than 100GB -->
        <skip_key>size_k</skip_key>
        <skip_value>104857600</skip_value>
        <skip_if_more_than config:type="boolean">true</skip_if_more_than>
      </listentry>
    </skip_list>
  </drive>
</partitioning>
```

For a list of all possible `<skip_key>`s, run **yast2 ayast\_probe** on a system that has already been installed.

## 4.5.2 Partition Configuration

The elements listed below must be placed within the following XML structure:

```
<drive>
```

```
<partitions config:type="list">
  <partition>
    ...
  </partition>
</partitions>
</drive>
```

#### create

Specify if this partition or logical volume must be created or if it already exists.

```
<create config:type="boolean">false</create>
```

If set to false, you also need to set partition\_nr, lv\_name or uuid to tell AutoYaST which device to use.

#### crypt\_fs

Partition will be encrypted.

```
<crypt_fs config:type="boolean">false</crypt_fs>
```

Default is false.

#### crypt\_key

Encryption key

```
<crypt_key>xxxxxxxx</crypt_key>
```

Needed if crypt\_fs has been set to true, as well as to open and reuse an existing encrypted device.

#### mount

The mount point of this partition.

```
<mount>/</mount>
<mount>swap</mount>
```

You should have at least a root partition (/) and a swap partition.

#### fstop

Mount options for this partition.

```
<fstopt>
  ro,noatime,user,data=ordered,acl,user_xattr
</fstopt>
```

See man mount for available mount options.

## label

The label of the partition (useful for the mountby parameter; see below).

```
<label>mydata</label>
```

See man e2label for an example.

## uuid

The uuid of the partition (only useful for the mountby parameter; see below).

```
<uuid>1b4e28ba-2fa1-1d2-883f-b9a761bde3fb</uuid>
```

See man uuidgen.

## size

The size of the partition, for example 4G, 4500M, etc. The /boot partition and the swap partition can have auto as size. Then AutoYaST calculates a reasonable size. One partition can have the value max to use all remaining space.

You can also specify the size in percentage. So 10% will use 10% of the size of the hard disk or volume group. You can mix auto, max, size, and percentage as you like.

```
<size>10G</size>
```

Starting with SUSE Linux Enterprise Server 15, all values (including auto and max) can be used for resizing partitions as well.

## format

Specify if AutoYaST should format the partition.

```
<format config:type="boolean">false</format>
```

If you set create to true, then you likely want this option set to true as well.

## file system

Specify the file system to use on this partition:

- btrfs
- ext2
- ext3
- ext4
- fat

- xfs
- swap

```
<filesystem config:type="symbol">ext3</filesystem>
```

Optional. The default is btrfs for the root partition (/) and xfs for data partitions.

#### mkfs\_options

Specify an option string that is added to the mkfs command.

```
<mkfs_options>-I 128</mkfs_options>
```

Optional. Only use this when you know what you are doing.

#### partition\_nr

The partition number of this partition. If you have set create=false or if you use LVM, then you can specify the partition via partition\_nr. You can force AutoYaST to only create primary partitions by assigning numbers below 5.

```
<partition_nr config:type="integer">2</partition_nr>
```

Usually, numbers 1 to 4 are primary partitions while 5 and higher are logical partitions.

#### partition\_id

The partition\_id sets the id of the partition. If you want different identifiers than 131 for Linux partition or 130 for swap, configure them with partition\_id.

```
<partition_id config:type="integer">131</partition_id>
```

Possible values are:

FAT16 (MS-DOS): 6

NTFS (MS-DOS): 7

FAT32 (MS-DOS): 12

Extended FAT16 (MS-DOS): 15

DIAG, Diagnostics and firmware (MS-DOS, GPT): 18

PPC PReP Boot partition (MS-DOS, GPT): 65

Swap (MS-DOS, GPT, DASD, implicit): 130

Linux (MS-DOS, GPT, DASD): 131

Intel Rapid Start Technology (MS-DOS, GPT): 132

LVM (MS-DOS, GPT, DASD): 142

EFI System Partition (MS-DOS, GPT): 239

MD RAID (MS-DOS, GPT, DASD): [253](#)

BIOS boot (GPT): [257](#)

Windows basic data (GPT): [258](#)

EFI (GPT): [259](#)

Microsoft reserved (GPT): [261](#)

The default is [131](#) for Linux partition and [130](#) for swap.

### partition\_type

When using an [msdos](#) partition table, this element sets the type of the partition. The value can be [primary](#) or [logical](#). This value is ignored when using a [gpt](#) partition table, because such a distinction does not exist in that case.

```
<partition_type>primary</partition_type>
```

Optional. Allowed values are [primary](#) (default) and [logical](#).

### mountby

Instead of a partition number, you can tell AutoYaST to mount a partition by [device](#), [label](#), [uuid](#), [path](#) or [id](#), which are the udev path and udev id (see [/dev/disk/...](#)).

```
<mountby config:type="symbol">label</mountby>
```

See [label](#) and [uuid](#) documentation above. The default depends on YaST and usually is [id](#).

### subvolumes

List of subvolumes to create for a file system of type Btrfs. This key only makes sense for file systems of type Btrfs. See [Section 4.5.3, "Btrfs subvolumes"](#) for more information.

```
<subvolumes config:type="list">
  <path>tmp</path>
  <path>opt</path>
  <path>srv</path>
  <path>var/crash</path>
  <path>var/lock</path>
  <path>var/run</path>
  <path>var/tmp</path>
  <path>var/spool</path>
  ...
</subvolumes>
```

If no [subvolumes](#) section has been defined for a partition description, AutoYaST will create a predefined set of subvolumes for the given mount point.



### create\_subvolumes

Determine whether Btrfs subvolumes should be created or not.

It is set to true by default. When set to false, no subvolumes will be created.

### subvolumes\_prefix

Set the Btrfs subvolumes prefix name. If no prefix is wanted, it must be set to an empty value:

```
<subvolumes_prefix><![CDATA[]]></subvolumes_prefix>
```

It is set to @ by default.

### lv\_name

If this partition is on a logical volume in a volume group, specify the logical volume name here (see the type parameter in the drive configuration).

```
<lv_name>opt_lv</lv_name>
```

### stripes

An integer that configures LVM striping. Specify across how many devices you want to stripe (spread data).

```
<stripes config:type="integer">2</stripes>
```

### stripesize

Specify the size of each block in KB.

```
<stripesize config:type="integer">4</stripesize>
```

### lvm\_group

If this is a physical partition used by (part of) a volume group (LVM), you need to specify the name of the volume group here.

```
<lvm_group>system</lvm_group>
```

### pool

pool must be set to true if the LVM logical volume should be an LVM thin pool.

```
<pool config:type="boolean">>false</pool>
```

### used\_pool

The name of the LVM thin pool that is used as a data store for this thin logical volume. If this is set to something non-empty, it implies that the volume is a so-called thin logical volume.

```
<used_pool>my_thin_pool</used_pool>
```

#### raid\_name

If this physical volume is part of a RAID, specify the name of the RAID.

```
<raid_name>/dev/md/0</raid_name>
```

#### raid\_options

Specify RAID options, see below.

```
<raid_options>...</raid_options>
```

Setting the RAID options at partition level is deprecated. See [Section 4.5.8, "Software RAID"](#).

#### resize

This boolean must be true if an existing partition should be resized. In this case, you need to tell AutoYaST to reuse the device (see create) and specify a size.

```
<resize config:type="boolean">false</resize>
```

Starting with SUSE Linux Enterprise Server 15 resizing works with physical disk partitions and with LVM volumes.



### Important: Creating Boot Partitions Automatically

When AutoYaST determines that a boot partition might be required in order to boot properly, it will automatically add one even if it is not specified in the profile.

However, if for any reason the boot partition does not fit in the current partitioning layout, AutoYaST will just display a warning, allowing the installation to proceed.

## 4.5.3 Btrfs subvolumes

As mentioned in [Section 4.5.2, "Partition Configuration"](#), it is possible to define a set of subvolumes for each Btrfs file system. In its simplest form, this is just a list of entries:

```
<subvolumes config:type="list">
  <path>tmp</path>
  <path>opt</path>
  <path>srv</path>
  <path>var/crash</path>
  <path>var/lock</path>
  <path>var/run</path>
```

```
<path>var/tmp</path>
<path>var/spool</path>
</subvolumes>
```

AutoYaST supports disabling copy-on-write for a given subvolume. In that case, a slightly more complex syntax should be used:

```
<subvolumes config:type="list">
<listentry>tmp</listentry>
<listentry>opt</listentry>
<listentry>srv</listentry>
<listentry>
  <path>var/lib/pgsql</path>
  <copy_on_write config:type="boolean">false</copy_on_write>
</listentry>
</subvolumes>
```

If there is a default subvolume used for the distribution (for example `@` in SUSE Linux Enterprise Server), the name of this default subvolume is automatically prefixed to the names in this list. This behavior can be disabled by setting the `subvolumes_prefix`.

```
<subvolumes_prefix><![CDATA[]]></subvolumes_prefix>
```

#### 4.5.4 Using the Whole Disk



#### Note: Available in SUSE Linux Enterprise Server 15 via Installer Updates

Support to use whole disks was included in SUSE Linux Enterprise Server 15 as a late feature. To use the feature in this specific version, the installer self-update must be enabled. See Book “Deployment Guide”, Chapter 8 “Installation Steps”, Section 8.2 “Installer Self-Update” for more information about installer updates.

AutoYaST allows to use a whole disk without creating any partition by setting the `disklabel` to `none` as described in [Section 4.5.1, “Drive Configuration”](#). In such cases, the configuration in the first `partition` from the `drive` will be applied to the whole disk.

In the example below, we are using the second disk (`/dev/sdb`) as the `/home` file system.

##### EXAMPLE 4.3: USING A WHOLE DISK AS A FILE SYSTEM

```
<partitioning config:type="list">
```

```

<drive>
  <device>/dev/sda</device>
  <partitions config:type="list">
    <partition>
      <create config:type="boolean">true</create>
      <format config:type="boolean">true</format>
      <mount>/</mount>
      <size>max</size>
    </partition>
  </partitions>
</drive>
<drive>
  <device>/dev/sdb</device>
  <disklabel>none</disklabel>
  <partitions config:type="list">
    <partition>
      <format config:type="boolean">true</format>
      <mount>/home</mount>
    </partition>
  </partitions>
</drive>

```

In addition, the whole disk can be used as an LVM physical volume or as a software RAID member. See [Section 4.5.7, “Logical Volume Manager \(LVM\)”](#) and [Section 4.5.8, “Software RAID”](#) for further details about setting up an LVM or a software RAID.

## 4.5.5 Automated Partitioning

For automated partitioning, you only need to provide the sizes and mount points of partitions. All other data needed for successful partitioning is calculated during installation—unless 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

The size of the /boot partition is determined by the architecture of the target system.

- swap

The size of the swap partition is determined by the amount of memory available in the system.

- / (root partition)

The size of the root partition is determined by 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 free space on the hard disk. This requires the availability of sufficient space for all selected packages in addition to swap.

#### Reuse all available space

Use this option to delete all existing partitions (Linux and non-Linux).

#### Reuse all available Linux partitions

This option deletes all existing Linux partitions. Other partitions (for example Windows partitions) remain untouched. Note that this works only if the Linux partitions are at the end of the device.

#### Reuse only specified partitions

This option allows you to select specific partitions to delete. Start the selection with the last available partition.

Repartitioning only works if the selected partitions are neighbors and located at the end of the device.



### Important: Beware of Data Loss

The value provided in the use property determines how existing data and partitions are treated. The value all means that the entire disk will be erased. Make backups and use the confirm property if you need to keep some partitions with important data. Otherwise, no pop-ups will notify you about partitions being deleted.

If multiple drives are in the target system, identify all drives with their device names and specify 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 uses all available space on a drive, therefore should only be set for the last partition on the drive. With auto the size of a swap or boot partition is determined automatically, depending on the memory available and the type of the system.

A fixed size can be given as shown below:

1GB, 1G, 1000MB, or 1000M will all create a partition of the size 1 Gigabyte.

#### EXAMPLE 4.4: 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. If you do not specify the device, it will be automatically detected.

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

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

#### EXAMPLE 4.5: DETAILED AUTOMATED PARTITIONING

```
<partitioning config:type="list">
  <drive>
    <device>/dev/sda</device>
    <use>all</use>
    <partitions config:type="list">
      <partition>
        <mount>/</mount>
        <size>10G</size>
      </partition>
      <partition>
        <mount>swap</mount>
        <size>1G</size>
      </partition>
    </partitions>
  </drive>
  <drive>
    <device>/dev/sdb</device>
    <use>free</use>
    <partitions config:type="list">
      <partition>
        <filesystem config:type="symbol">ext4</filesystem>
        <mount>/data1</mount>
        <size>15G</size>
      </partition>
      <partition>
        <filesystem config:type="symbol">xfs</filesystem>
```

```
<mount>/data2</mount>
<size>auto</size>
</partition>
</partitions>
</drive>
</partitioning>
```

## 4.5.6 Advanced Partitioning Features

### 4.5.6.1 Wipe out Partition Table

Usually this is not needed because AutoYaST can delete partitions one by one automatically. But you need the option to let AutoYaST clear the partition table instead of deleting partitions individually.

Go to the drive section and add:

```
<initialize config:type="boolean">true</initialize>
```

With this setting AutoYaST will delete the partition table before it starts to analyze the actual partitioning and calculates its partition plan. Of course this means, that you cannot keep any of your existing partitions.

### 4.5.6.2 Mount Options

By default a file system 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 for the label property is used as the volume label.

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

**Mount read-only (`ro`)**

No write access to the file system. 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 can be mounted by a normal user. Default is `false`.

**Data Journaling Mode (`ordered`, `journal`, `writeback`)**

`journal`

All data is committed to the journal prior to being written to the main file system.

`ordered`

All data is directly written to the main file system before its metadata is 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 4.6: MOUNT OPTIONS**

```
<partitions config:type="list">
  <partition>
    <filesystem config:type="symbol">ext4</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>10G</size>
  </partition>
</partitions>
```





## Note: Check Supported File System Options

Different file system types support different options. Check the documentation carefully before setting them.

### 4.5.6.3 Keeping Specific Partitions

In some cases you should leave partitions untouched and only format specific target partitions, rather than creating them from scratch. For example, if different Linux installations coexist, or you have another operating system installed, likely you do not want to wipe these out. You may also want to leave data partitions untouched.

Such scenarios require specific knowledge about the target systems and hard disks. Depending on the scenario, you might need to know the exact partition table of the target hard disk with partition IDs, sizes and numbers. With this 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 remaining partitions will only be formatted.

#### EXAMPLE 4.7: KEEPING PARTITIONS

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

```

    </partition>
    <partition>
      <format config:type="boolean">true</format>
      <mount>/space2</mount>
      <size>5G</size>
    </partition>
    <partition>
      <format config:type="boolean">true</format>
      <mount>/space3</mount>
      <size>max</size>
    </partition>
  </partitions>
  <use>6</use>
</drive>
</partitioning>

```

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

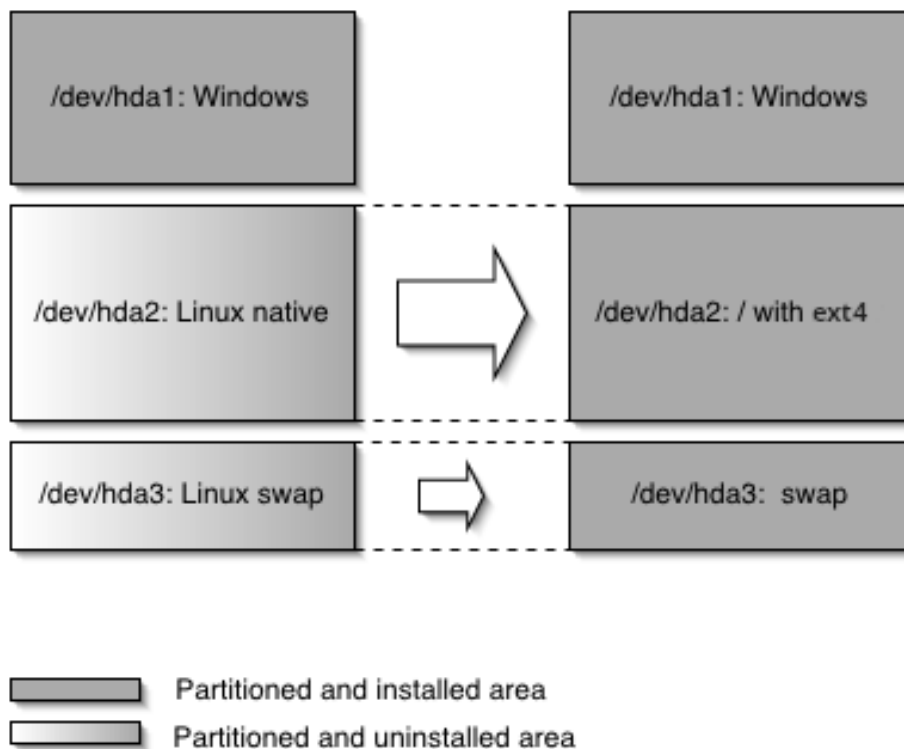


FIGURE 4.1: KEEPING PARTITIONS

In this scenario, shown in figure *Figure 4.1, "Keeping partitions"*, AutoYaST will not create new partitions. Instead it searches for certain partition types on the system and uses 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 file system type).

EXAMPLE 4.8: **AUTO-DETECTION OF PARTITIONS TO BE KEPT.**

```
<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>
```



### Note: Keeping Encrypted Devices

When AutoYaST is probing the storage devices, the partitioning section from the profile is not yet analyzed. In some scenarios, it is not clear which key should be used to unlock a device. For example, this can happen when more than one encryption key is defined. To solve this problem, AutoYaST will try all defined keys on all encrypted devices until a working key is found.

## 4.5.7 Logical Volume Manager (LVM)

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

#### EXAMPLE 4.9: CREATE LVM PHYSICAL VOLUME

The following example shows how to prepare for LVM in the `partitioning` resource. A non-formatted partition is created on device `/dev/sda1` of the type `LVM` and with the volume group `system`. This partition will use all space available on the drive.

```
<partitioning config:type="list">
  <drive>
    <device>/dev/sda</device>
    <partitions config:type="list">
      <partition>
        <create config:type="boolean">true</create>
        <lvm_group>system</lvm_group>
        <partition_type>primary</partition_type>
        <partition_id config:type="integer">142</partition_id>
        <partition_nr config:type="integer">1</partition_nr>
        <size>max</size>
      </partition>
    </partitions>
    <use>all</use>
  </drive>
</partitioning>
```

#### EXAMPLE 4.10: LVM LOGICAL VOLUMES

```
<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>
    <type config:type="symbol">CT_LVM</type>
    <partitions config:type="list">
      <partition>
        <filesystem config:type="symbol">ext4</filesystem>
        <lv_name>user_lv</lv_name>
        <mount>/usr</mount>
        <size>15G</size>
      </partition>
```

```

<partition>
  <filesystem config:type="symbol">ext4</filesystem>
  <lv_name>opt_lv</lv_name>
  <mount>/opt</mount>
  <size>10G</size>
</partition>
<partition>
  <filesystem config:type="symbol">ext4</filesystem>
  <lv_name>var_lv</lv_name>
  <mount>/var</mount>
  <size>1G</size>
</partition>
</partitions>
<pesize>4M</pesize>
<use>all</use>
</drive>
</partitioning>

```

It is possible to set the size to max for the logical volumes. Of course, you can only use max for one(!) logical volume. You cannot set two logical volumes in one volume group to max.

#### 4.5.8 Software RAID



#### Note: Available in SUSE Linux Enterprise Server 15 via Installer Updates

Enhanced support for software RAID devices is available for SUSE Linux Enterprise Server 15. To use the feature in this specific version, the installer self-update feature must be enabled. See *Book "Deployment Guide", Chapter 8 "Installation Steps", Section 8.2 "Installer Self-Update"* for more information about installer updates.

If needed, see [Section 4.5.8.1, "Using the Deprecated Syntax"](#) to find out further details about the old way of specifying a software RAID, which is still supported for backward compatibility.

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 offers the best redundancy. It can be used with two or more disks. An exact copy of all data is maintained 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 allows access to the same physical device via multiple controllers for redundancy against a fault in a controller card. This mode can be used with at least two devices.

Similar to LVM, a software RAID definition in an AutoYaST profile is composed of two different parts:

- Determining which disks or partitions are going to be used as RAID members. In order to do that, you need to set the `raid_name` element in such devices.
- Defining the RAID itself by using a dedicated `drive` section.

The following example shows a RAID1 configuration that uses a partition from the first disk and another one from the second disk as RAID members:

### EXAMPLE 4.11: RAID1 CONFIGURATION

```
<partitioning config:type="list">
  <drive>
    <device>/dev/sda</device>
    <partitions config:type="list">
      <partition>
        <mount>/</mount>
        <size>20G</size>
      </partition>
      <partition>
        <raid_name>/dev/md/0</raid_name>
        <size>max</size>
      </partition>
    </partitions>
    <use>all</use>
  </drive>
  <drive>
```

```

<device>/dev/sdb</device>
<disklabel>none</disklabel>
<partitions config:type="list">
  <partition>
    <raid_name>/dev/md/0</raid_name>
  </partition>
</partitions>
<use>all</use>
</drive>
<drive>
  <device>/dev/md/0</device>
  <partitions config:type="list">
    <partition>
      <mount>/home</mount>
      <size>40G</size>
    </partition>
    <partition>
      <mount>/srv</mount>
      <size>10G</size>
    </partition>
  </partitions>
  <raid_options>
    <chunk_size>4</chunk_size>
    <parity_algorithm>left_asymmetric</parity_algorithm>
    <raid_type>raid1</raid_type>
  </raid_options>
  <use>all</use>
</drive>
</partitioning>

```

If you do not want to create partitions in the software RAID, set the disklabel to none as you would do for a regular disk. In the example below, only the RAID drive section is shown for simplicity's sake:

#### EXAMPLE 4.12: RAID1 WITHOUT PARTITIONS

```

<drive>
  <device>/dev/md/0</device>
  <disklabel>none</disklabel>
  <partitions config:type="list">
    <partition>
      <mount>/home</mount>
      <size>40G</size>
    </partition>
  </partitions>
  <raid_options>
    <chunk_size>4</chunk_size>

```

```

    <parity_algorithm>left_asymmetric</parity_algorithm>
    <raid_type>raid1</raid_type>
  </raid_options>
  <use>all</use>
</drive>

```

#### 4.5.8.1 Using the Deprecated Syntax

If the installer self-update feature is enabled, it is possible to partition a software RAID for SUSE Linux Enterprise Server 15. However, that scenario was not supported in previous versions and hence the way to define a software RAID was slightly different.

This section defines what the old-style configuration looks like because it is still supported for backward compatibility.

Keep the following in mind when configuring a RAID using this deprecated 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/md/0 is configured. Adding several partition sections means that you want to have multiple software RAIDs (/dev/md/0, /dev/md/1, etc.).
- All RAID-specific options are contained in the raid\_options resource.

##### EXAMPLE 4.13: OLD STYLE RAID1 CONFIGURATION

```

<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>4G</size>
      </partition>

      <!-- Insert a configuration for the regular partitions located on
           /dev/sda here (for example / 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>
      <size>4gb</size>
    </partition>
  </partitions>
  <use>all</use>
</drive>
<drive>
  <device>/dev/md</device>
  <partitions config:type="list">
    <partition>
      <filesystem config:type="symbol">ext4</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_options>
    </partition>
  </partitions>
  <use>all</use>
</drive>
</partitioning>

```

#### 4.5.8.2 RAID Options

The following elements must be placed within the following XML structure:

```

<partition>
  <raid_options>
    ...
  </raid_options>
</partition>

```

Attribute	Values	Description
<u>chunk_size</u>	<chunk_size>4</chunk_size>	

Attribute	Values	Description
<u>parity_algorithm</u>	<p>Possible values are:</p> <p><u>left_asymmetric</u>,  <u>left_symmetric</u>,  <u>right_asymmetric</u>,  <u>right_symmetric</u>.</p> <p>For RAID6 and RAID10 the following values can be used:</p> <p><u>parity_first</u>, <u>parity_last</u>, <u>left_asymmetric_6</u>, <u>left_symmetric_6</u>, <u>right_asymmetric_6</u>, <u>right_symmetric_6</u>, <u>parity_first_6</u>, <u>n2</u>, <u>o2</u>, <u>f2</u>, <u>n3</u>, <u>o3</u>, <u>f3</u></p> <pre>&lt;parity_algorithm   &gt;left_asymmetric&lt;/ parity_algorithm&gt;</pre>	
<u>raid_type</u>	<p>Possible values are: <u>raid0</u>, <u>raid1</u>, <u>raid5</u>, <u>raid6</u> and <u>raid10</u>.</p> <pre>&lt;raid_type&gt;raid1&lt;/ raid_type&gt;</pre>	The default is <u>raid1</u> .
<u>device_order</u>	<p>This list contains the order of the physical devices:</p> <pre>&lt;device_order   config:type="list"&gt;     &lt;device&gt;/dev/ sdb2&lt;/device&gt;     &lt;device&gt;/dev/ sda1&lt;/device&gt;     ...</pre>	This is optional and the default is alphabetical order.

Attribute	Values	Description
	<code>&lt;/device_order&gt;</code>	

## 4.5.9 IBM Z Specific Configuration

### 4.5.9.1 Configuring DASD Disks

The elements listed below must be placed within the following XML structure:

```
<dasd>
  <devices config:type="list">
    <listentry>
      ...
    </listentry>
  </devices>
</dasd>
```

tags in the `<profile>` section. Each disk needs to be configured in a separate `<listentry>` ... `</listentry>` section.

Attribute	Description	Values
<u>device</u>	<u>DASD</u> is the only value allowed  <code>&lt;device&gt;DASD&lt;/dev_name&gt;</code>	
<u>dev_name</u>	The device ( <u>dasdN</u> ) you want to configure in this section.  <code>&lt;dev_name&gt;/dev/dasda&lt;/dev_name&gt;</code>	Optional but recommended. If left out, AutoYaST tries to guess the device.
<u>channel</u>	Channel by which the disk is accessed.  <code>&lt;channel&gt;0.0.0150&lt;/channel&gt;</code>	Mandatory.

Attribute	Description	Values
<u>diag</u>	<p>Enable or disable the use of <u>DIAG</u>. Possible values are <u>true</u> (enable) or <u>false</u> (disable).</p> <pre>&lt;diag config:type="boolean"&gt;true&lt;/diag&gt;</pre>	Optional.

#### 4.5.9.2 Configuring zFCP disks

The following elements must be placed within the following XML structure:

```
<profile>
  <zfc>
    <devices config:type="list">
      <listentry>
        ...
      </listentry>
    </devices>
  </zfc>
</profile>
```

Each disk needs to be configured in a separate listentry section.

##### **controller\_id**

Channel number

```
<controller_id>0.0.fc00</controller_id>
```

The controller\_id element is required.

There are two optional elements, wwpn (Worldwide Port Number, the target port through which the SCSI device is attached), and fcplun (logical unit number of the SCSI device). It is not necessary to specify these for FCP devices running in NPIV (Node Port ID Virtualization) mode, and when the zfc module parameter allow\_lun\_scan is set to 1 (the default setting), which enables automatic LUN scanning by the zfc device driver.

If automatic LUN scanning is not available, set the wwpn and fcplun options manually.

wwpn

Worldwide port number

```
<wwpn>0x500507630300c562</wwpn>
```

fcp\_lun

Logical unit number

```
<fcp_lun>0x4010403200000000</fcp_lun>
```

See the IBM documentation for more information, <https://www.ibm.com/docs/en/linux-on-systems?topic=wsd-configuring-devices>.

## 4.6 iSCSI Initiator Overview

Using the `iscsi-client` resource, you can configure the target machine as an iSCSI client.

EXAMPLE 4.14: **ISCSI CLIENT**

```
<iscsi-client>
  <initiatorname>iqn.2013-02.de.suse:01:e229358d2dea</initiatorname>
  <targets config:type="list">
    <listentry>
      <authmethod>None</authmethod>
      <portal>192.168.1.1:3260</portal>
      <startup>onboot</startup>
      <target>iqn.2001-05.com.doe:test</target>
      <iface>default</iface>
    </listentry>
  </targets>
  <version>1.0</version>
</iscsi-client>
```

Attribute	Description
initiatorname	<code>InitiatorName</code> is a value from <code>/etc/iscsi/initiatorname.iscsi</code> . In case you have iBFT, this value will be added from there and you are only able to change it in the BIOS setup.
version	Version of the YaST module. Default: 1.0

Attribute	Description
targets	List of targets. Each entry contains: <u>authmethod</u> Authentication method: None/CHAP <u>portal</u> Portal address <u>startup</u> Value: manual/onboot <u>target</u> Target name <u>iface</u> Interface name

## 4.7 Fibre Channel over Ethernet Configuration (FCoE)

Using the fcoe\_cfg resource, you can configure a Fibre Channel over Ethernet (FCoE).

### EXAMPLE 4.15: FCOE CONFIGURATION

```
<fcoe-client>
  <fcoe_cfg>
    <DEBUG>no</DEBUG>
    <USE_SYSLOG>yes</USE_SYSLOG>
  </fcoe_cfg>
  <interfaces config:type="list">
    <listentry>
      <dev_name>eth3</dev_name>
      <mac_addr>01:000:000:000:42:42</mac_addr>
      <device>Gigabit 1313</device>
      <vlan_interface>200</vlan_interface>
      <fcoe_vlan>eth3.200</fcoe_vlan>
      <fcoe_enable>yes</fcoe_enable>
      <dc_b_required>yes</dc_b_required>
      <auto_vlan>no</auto_vlan>
      <dc_b_capable>no</dc_b_capable>
      <cfg_device>eth3.200</cfg_device>
    </listentry>
  </interfaces>
  <service_start>
    <fcoe config:type="boolean">true</fcoe>
    <lldpad config:type="boolean">true</lldpad>
  </service_start>
</fcoe-client>
```

Attribute	Description	Values
fcoe_cfg	<p><u>DEBUG</u> is used to enable or disable debugging messages from the fcoe service script and fcoemon.</p> <p><u>USE_SYSLOG</u> messages are sent to the system log if set to yes.</p>	yes/no
interfaces	List of network cards including the status of VLAN and FCoE configuration.	
service_start	<p>Enable or disable the start of the services fcoe and lldpad at boot time.</p> <p>Starting the service fcoe means starting the Fibre Channel over Ethernet service daemon fcoemon which controls the FCoE interfaces and establishes a connection with the daemon lldpad.</p> <p>The lldpad service provides the Link Layer Discovery Protocol agent daemon lldpad that informs fcoemon about DCB (Data Center Bridging) features and configuration of the interfaces.</p>	yes/no

## 4.8 Country Settings

Language, timezone, and keyboard settings.

EXAMPLE 4.16: **LANGUAGE**

```
<language>
  <language>en_GB</language>
  <languages>de_DE,en_US</languages>
</language>
```

Attribute	Description	Values
<u>language</u>	Primary language	A list of available languages can be found under <u>/usr/share/YaST2/data/lan-</u> <u>guages</u>
<u>languages</u>	Secondary languages separated by commas	A list of available languages can be found under <u>/usr/share/YaST2/data/lan-</u> <u>guages</u>

If the configured value for the primary language is unknown, it will be reset to the default, en\_US.

EXAMPLE 4.17: **TIMEZONE**

```
<timezone>
  <hwclock>UTC</hwclock>
  <timezone>Europe/Berlin</timezone>
</timezone>
```

Attribute	Description	Values
hwclock	Whether the hardware clock uses local time or UTC	localtime/UTC
timezone	Timezone	A list of available time zones can be found under <u>/usr/share/YaST2/data/time-</u> <u>zone_raw.ycp</u>

EXAMPLE 4.18: **KEYBOARD**

```
<keyboard>
```



```
<keymap>german</keymap>
</keyboard>
```

Attribute	Description	Values
keymap	Keyboard layout	A list of available keymaps can be found in <u>/usr/share/YaST2/data/key-board_raw.ycp</u>

## 4.9 Software

### 4.9.1 Product Selection

Starting with SUSE Linux Enterprise Server 15, all products are distributed using a single installation medium. Therefore you need to choose which product to install by using the product tag. The available values for the product tag are:

#### SLES

SUSE Linux Enterprise Server

#### SLE\_HPC

SUSE Linux Enterprise High Performance Computing

#### SLES\_SAP

SUSE Linux Enterprise Server for SAP Applications

#### SLED

SUSE Linux Enterprise Desktop

#### EXAMPLE 4.19: EXPLICIT PRODUCT SELECTION

In the following example, SUSE Linux Enterprise Desktop is the chosen product:

```
<software>
  <products config:type="list">
    <product>SLED</product>
  </products>
```

```
</software>
```

In special cases, the medium might contain only one product. If so, you do not need to select a product explicitly as described above. AutoYaST will select the only available product automatically.



### Note: Using AutoYaST Files from Previous Versions

If you are using or migrating an AutoYaST configuration file from an older version of SUSE Linux Enterprise Server, be aware that there are some special considerations. For details, refer to [Section D.1, “Product Selection”](#).

## 4.9.2 Package Selection with Patterns and Packages Sections

Patterns or packages are configured like this:

### EXAMPLE 4.20: PACKAGE SELECTION IN THE CONTROL FILE WITH PATTERNS AND PACKAGES SECTIONS

```
<software>
  <patterns config:type="list">
    <pattern>directory_server</pattern>
  </patterns>
  <packages config:type="list">
    <package>apache</package>
    <package>postfix</package>
  </packages>
  <do_online_update config:type="boolean">true</do_online_update>
</software>
```



### Note: Package and Pattern Names

The values are real package or pattern names. If the package name has been changed due to an upgrade, you will have to adapt these settings too.

It is possible to specify package and pattern names using regular expressions. In that case, AutoYaST will select all packages or patterns that match the expression. Beware that such expressions must be enclosed within slashes. In [Example 4.21, “Packages selection using a regular expression”](#), all packages whose name starts with nginx will be selected (e.g., nginx and nginx-macros).

```
<software>
  <packages config:type="list">
    <package>/nginx.*</package>
  </packages>
</software>
```

### 4.9.3 Installing Additional/Customized Packages or Products

In addition to the packages available for installation on the DVD-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 in earlier in versions, you do not need a special resource in the control file to install custom and external packages. 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 package database. Use the command `/usr/bin/create_package_descr`. It can be found in the `inst-source-utils` package in the openSUSE Build Service. When creating the database, all languages will be reset to English.

The unpacked DVD is located in `/usr/local/DVDs/LATEST`.

```
> cp /tmp/inst-source-utils-2016.7.26-1.2.noarch.rpm /usr/local/DVDs/LATEST/suse/
noarch
> cd /usr/local/DVDs/LATEST/suse
> create_package_descr -d /usr/local/CDs/LATEST/suse
```

In the above example, the directory `/usr/local/CDs/LATEST/suse` contains the architecture dependent (for example `x86_64`) and architecture independent packages (`noarch`). 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. Additionally this method makes the creation of custom CD-ROMs easier.

To add your own module such as the SDK (SUSE Software Development Kit), add a file `add_on_products.xml` to the installation source in the root directory.

The following example shows how the SDK module can be added to the base product repository. The complete SDK repository will be stored in the directory `/sdk`.

This file describes an SDK module included in the base product.

```
<?xml version="1.0"?>
<add_on_products xmlns="http://www.suse.com/1.0/yast2ns"
  xmlns:config="http://www.suse.com/1.0/configns">
  <product_items config:type="list">
    <product_item>
      <name>SUSE Linux Enterprise Software Development Kit</name>
      <url>relurl:///sdk?alias=SLE_SDK</url>
      <path></path>
      <!-- Users are asked whether to add such a product -->
      <ask_user config:type="boolean">false</ask_user>
      <!-- Defines the default state of pre-selected state in case of ask_user
      used. -->
      <selected config:type="boolean">true</selected>
    </product_item>
  </product_items>
</add_on_products>
```

Besides this special case, all other modules, extensions and add-on products can be added from almost all other locations during an AutoYaST installation.

```
<add-on>
  <add_on_products config:type="list">
    <listentry>
      <media_url>cd:///sdk</media_url>
      <product>sle-sdk</product>
      <alias>SLES SDK</alias>
      <product_dir></product_dir>
      <priority config:type="integer">20</priority>
      <ask_on_error config:type="boolean">false</ask_on_error>
      <confirm_license config:type="boolean">false</confirm_license>
      <name>SUSE Linux Enterprise Software Development Kit</name>
    </listentry>
  </add_on_products>
</add-on>
```

Attribute	Values
<code>media_url</code>	Product URL. Can have the prefix <code>cd:///</code> , <code>http://</code> , <code>ftp://</code> , etc. This entry is mandatory.

Attribute	Values
<u>product</u>	Internal product name if the add-on is a product. The command <b>zypper products</b> shows these names of installed products.
<u>alias</u>	Repository alias name. Defined by the user.
<u>product_dir</u>	Additional subpath.
<u>priority</u>	Sets the repository libzypp priority. Priority of 1 is the highest. The higher the number, the lower the priority. Default is 99.
<u>ask_on_error</u>	AutoYaST can ask the user to make add-on products, modules or extensions available instead of reporting a time-out error when no repository can be found at the given location. Set ask_on_error to <u>true</u> (the default is <u>false</u> ).
<u>confirm_license</u>	The user has to confirm the license. Default is <u>false</u> .
<u>name</u>	Repository name. The command <b>zypper lr</b> shows these names of added repositories.

To use unsigned installation sources with AutoYaST, turn off the checks with the following configuration in your AutoYaST control file.



### Note: Unsigned Installation Sources—Limitations

You can only disable signature checking during the first stage of the auto-installation process. In stage two, the installed system's configuration takes precedence over AutoYaST configuration.

The elements listed below must be placed within the following XML structure:

```
<general>
```

```

<signature-handling>
...
</signature-handling>
</general>

```

Default values for all options are `false`. If an option is set to `false` and a package or repository fails the respective test, it is silently ignored and will not be installed. Note that setting any of these options to `true` is a potential security risk. Never do it when using packages or repositories from third party sources.

Attribute	Values
<u>accept_unsigned_file</u>	<p>If set to <code>true</code>, AutoYaST will accept unsigned files like the content file.</p> <pre> &lt;accept_unsigned_file   config:type="boolean" &gt;true&lt;/accept_unsigned_file&gt; </pre>
<u>accept_file_without_checksum</u>	<p>If set to <code>true</code>, AutoYaST will accept files without a checksum in the content file.</p> <pre> &lt;accept_file_without_checksum   config:type="boolean" &gt;true&lt;/accept_file_without_checksum&gt; </pre>
<u>accept_verification_failed</u>	<p>If set to <code>true</code>, AutoYaST will accept signed files even when the verification of the signature failed.</p> <pre> &lt;accept_verification_failed   config:type="boolean" &gt;true&lt;/accept_verification_failed&gt; </pre>
<u>accept_unknown_gpg_key</u>	<p>If set to <code>true</code>, AutoYaST will accept new GPG keys of the installation sources, for example the key used to sign the content file.</p> <pre> &lt;accept_unknown_gpg_key   config:type="boolean" &gt;true&lt;/accept_unknown_gpg_key&gt; </pre>

Attribute	Values
<u>accept_non_trusted_gpg_key</u>	<p>Set this option to <u>true</u> to accept known keys you have not yet trusted.</p> <pre>&lt;accept_non_trusted_gpg_key   config:type="boolean" &gt;true&lt;/accept_non_trusted_gpg_key&gt;</pre>
<u>import_gpg_key</u>	<p>If set to <u>true</u>, AutoYaST will accept and import new GPG keys on the installation source in its database.</p> <pre>&lt;import_gpg_key config:type="boolean" &gt;true&lt;/import_gpg_key&gt;</pre>

It is possible to configure the signature handling for each add-on product, module, or extension individually. The following elements must be between the `signature-handling` section of the individual add-on product, module, or extension. All settings are optional. If not configured, the global signature-handling from the `general` section is used.

Attribute	Values
<u>accept_unsigned_file</u>	<p>If set to <u>true</u>, AutoYaST will accept unsigned files like the content file for this add-on product.</p> <pre>&lt;accept_unsigned_file   config:type="boolean" &gt;true&lt;/accept_unsigned_file&gt;</pre>
<u>accept_file_without_checksum</u>	<p>If set to <u>true</u>, AutoYaST will accept files without a checksum in the content file for this add-on.</p> <pre>&lt;accept_file_without_checksum   config:type="boolean" &gt;true&lt;/accept_file_without_checksum&gt;</pre>

Attribute	Values
<u>accept_verification_failed</u>	<p>If set to <code>true</code>, AutoYaST will accept signed files even when the verification of the signature fails.</p> <pre>&lt;accept_verification_failed   config:type="boolean" &gt;true&lt;/accept_verification_failed&gt;</pre>
<u>accept_unknown_gpg_key</u>	<p>If <code>all</code> is set to <code>true</code>, AutoYaST will accept new GPG keys on the installation source.</p> <pre>&lt;accept_unknown_gpg_key&gt;   &lt;all config:type="boolean"&gt;true&lt;/all&gt; &lt;/accept_unknown_gpg_key&gt;</pre> <p>Otherwise you can define single keys too.</p> <pre>&lt;accept_unknown_gpg_key&gt;   &lt;all config:type="boolean"&gt;false&lt;/all&gt;   &lt;keys config:type="list"&gt;     &lt;keyid&gt;3B3011B76B9D6523&lt;/keyid&gt;   &lt;/keys&gt; &lt;/accept_unknown_gpg_key&gt;</pre>
<u>accept_non_trusted_gpg_key</u>	<p>This means, the key is known, but it is not trusted by you.</p> <p>You can trust all keys by adding:</p> <pre>&lt;accept_non_trusted_gpg_key&gt;   &lt;all config:type="boolean"&gt;true&lt;/all&gt; &lt;/accept_non_trusted_gpg_key&gt;</pre> <p>Or you can trust specific keys:</p> <pre>&lt;accept_non_trusted_gpg_key&gt;   &lt;all config:type="boolean"&gt;false&lt;/all&gt;   &lt;keys config:type="list"&gt;     &lt;keyid&gt;3B3011B76B9D6523&lt;/keyid&gt;   &lt;/keys&gt; &lt;/accept_non_trusted_gpg_key&gt;</pre>



Attribute	Values
<code>import_gpg_key</code>	<p>If <code>all</code> is set to <code>true</code>, AutoYaST will accept and import all new GPG keys on the installation source into its database.</p> <pre>&lt;import_gpg_key&gt;   &lt;all config:type="boolean"&gt;true&lt;/all&gt; &lt;/import_gpg_key&gt;</pre> <p>This can be done for specific keys only:</p> <pre>&lt;import_gpg_key&gt;   &lt;all config:type="boolean"&gt;false&lt;/all&gt;   &lt;keys config:type="list"&gt;     &lt;keyid&gt;3B3011B76B9D6523&lt;/keyid&gt;   &lt;/keys&gt; &lt;/import_gpg_key&gt;</pre>

#### 4.9.4 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 because of conflicts.

To force the installation of a specific kernel, use the `kernel` property. The following is an example of forcing the installation of the default kernel. This kernel will be installed even if an SMP or other kernel is required.

##### EXAMPLE 4.25: KERNEL SELECTION IN THE CONTROL FILE

```
<software>
  <kernel>kernel-default</kernel>
  ...
</software>
```

#### 4.9.5 Removing Automatically Selected Packages

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

Removing these packages might break the system consistency, and it is not recommended to remove basic packages unless a replacement which provides the same services is provided. The best example for this case are mail transfer agent (MTA) packages. By default, `postfix` will be selected and installed. To use another MTA like `sendmail`, then `postfix` can be removed from the list of selected package using a list in the software resource. However, note that `sendmail` is not shipped with SUSE Linux Enterprise Server. The following example shows how this can be done:

EXAMPLE 4.26: PACKAGE SELECTION IN CONTROL FILE

```
<software>
  <packages config:type="list">
    <package>sendmail</package>
  </packages>
  <remove-packages config:type="list">
    <package>postfix</package>
  </remove-packages>
</software>
```



### Note: Package Removal Failure

Note that it is not possible to remove a package that is part of a pattern (see [Section 4.9.2, “Package Selection with Patterns and Packages Sections”](#)). When specifying such a package for removal, the installation will fail with the following error message:

```
The package resolver run failed. Check
your software section in the AutoYaST profile.
```

## 4.9.6 Installing recommended packages and patterns

AutoYaST enables you to control which *recommended* packages and patterns are installed. There are three options:

- Install all recommended packages and patterns
- Install only required packages and patterns
- Install recommended packages, ignore recommended patterns

Set the `install_recommended` flag to `true` in the configuration file to install all recommended packages and patterns.

If you want just a minimal installation and to install only *required* packages and patterns, set the flag to `false`.

Omit the flag from the configuration file to install only recommended packages, and ignore all recommended patterns. Note that this flag only affects a fresh installation and will be ignored during an upgrade.

```
<software>
  <install_recommended config:type="boolean">false
</install_recommended>
</software>
```

*Default:* If this flag has not been set in the configuration file *all* recommended packages and *no* recommended pattern will be installed.

### 4.9.7 Installing Packages in Stage 2

To install packages after the reboot during stage two, you can use the post-packages element for that:

```
<software>
  <post-packages config:type="list">
    <package>yast2-cim</package>
  </post-packages>
</software>
```

### 4.9.8 Installing Patterns in Stage 2

You can also install patterns in stage 2. Use the post-patterns element for that:

```
<software>
  <post-patterns config:type="list">
    <pattern>apparmor</pattern>
  </post-patterns>
</software>
```

## 4.9.9 Online Update in Stage 2

You can perform an online update at the end of the installation. Set the boolean `do_online_update` to `true`. Of course this only makes sense if you add an online update repository in the `suse-register/customer-center` section, for example, or in a post-script. If the online update repository was already available in stage one via the add-on section, then AutoYaST has already installed the latest packages available. If a kernel update is done via `online-update`, a reboot at the end of stage two is triggered.

```
<software>
  <do_online_update config:type="boolean">true</do_online_update>
</software>
```

## 4.10 Upgrade

AutoYaST can also be used for doing a system upgrade. Besides upgrade packages, the following sections are supported too:

- `scripts/pre-scripts` Running user scripts very early, before anything else really happens.
- `add-on` Defining an additional add-on product.
- `language` Setting language.
- `timezone` Setting timezone.
- `keyboard` Setting keyboard.
- `software` Installing additional software/patterns. Removing installed packages.
- `suse_register` Running registration process.

To control the upgrade process the following sections can be defined:

### EXAMPLE 4.27: UPGRADE AND BACKUP

```
<upgrade>
  <stop_on_solver_conflict config:type="boolean">true</stop_on_solver_conflict>
</upgrade>
<backup>
```

```
<sysconfig config:type="boolean">true</sysconfig>
<modified config:type="boolean">true</modified>
<remove_old config:type="boolean">true</remove_old>
</backup>
```

Element	Description	Comment
stop_on_solver_conflict	Halt installation if there are package dependency issues.	
modified	Create backup of modified files.	
sysconfig	Create backup of <u>/etc/sysconfig</u> directory.	
remove_old	Remove backups from previous updates.	

To start the AutoYaST upgrade mode, you need:

#### PROCEDURE 4.1: STARTING AUTOYAST IN UPGRADE MODE

1. Copy the AutoYaST profile to /root/autoupg.xml into its file system.
2. Boot the system from the installation media.
3. Select the Installation menu item.
4. On the command line, set autoupgrade=1.
5. Press **Enter** to start the upgrade process.

## 4.11 Services and Targets

With the services-manager resource you can set the default systemd target and specify in detail which system services you want to start or deactivate and how to start them.

The default-target property specifies the default systemd target into which the system boots. Valid options are graphical for a graphical login, or multi-user for a console login.

To specify the set of services that should be started on boot, use the `enable` and `disable` lists. To start a service, add its name to the `enable` list. To make sure that the service is not started on boot, add it to the `disable` list.

If a service is not listed as enabled or disabled, a default setting is used. The default setting may be either disabled or enabled.

Finally, some services like `cups` support on-demand activation (socket activated services). If you want to take advantage of such a feature, list the names of those services in the `on_demand` list instead of `enable`.

#### EXAMPLE 4.28: CONFIGURING SERVICES AND TARGETS

```
<services-manager>
  <default_target>multi-user</default_target>
  <services>
    <disable config:type="list">
      <service>libvirtd</service>
    </disable>
    <enable config:type="list">
      <service>sshd</service>
    </enable>
    <on_demand config:type="list">
      <service>cups</service>
    </on_demand>
  </services>
</services-manager>
```

## 4.12 Network Configuration

Network configuration is used to connect a single workstation to an Ethernet-based LAN or to configure a dial-up connection. More complex configurations (multiple network cards, routing, etc.) are also provided.

If the following setting is set to `true`, YaST will keep network settings created during the installation (via `linuxrc`) and/or merge it with network settings from the AutoYaST control file (if defined).



### Note: The `linuxrc` program

For a detailed description of how `linuxrc` works and its keywords, see [Appendix C, Advanced `linuxrc` Options](#).

AutoYaST settings have higher priority than any configuration files already present. YaST will write ifcfg-\* files based on the entries in the control file without removing old ones. If there is an empty or absent DNS and routing section, YaST will keep any pre-existing values. Otherwise, settings from the control file will be applied.

```
<keep_install_network  
config:type="boolean">true</keep_install_network>
```

During the second stage, installation of additional packages will take place before the network, as described in the profile, is configured. `keep_install_network` is set by default to `true` to ensure that a network is available in case it is needed to install those packages. If all packages are installed during the first stage and the network is not needed early during the second one, setting `keep_install_network` to `false` will avoid copying the configuration.

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

#### EXAMPLE 4.29: NETWORK CONFIGURATION

```
<networking>  
  <dns>  
    <dhcp_hostname config:type="boolean">true</dhcp_hostname>  
    <domain>site</domain>  
    <hostname>linux-bqua</hostname>  
    <nameservers config:type="list">  
      <nameserver>192.168.1.116</nameserver>  
      <nameserver>192.168.1.117</nameserver>  
      <nameserver>192.168.1.118</nameserver>  
    </nameservers>  
    <resolv_conf_policy>auto</resolv_conf_policy>  
    <searchlist config:type="list">  
      <search>example.com</search>  
      <search>example.net</search>  
    </searchlist>  
    <write_hostname config:type="boolean">>false</write_hostname>  
  </dns>  
  <interfaces config:type="list">  
    <interface>  
      <bootproto>dhcp</bootproto>  
      <device>eth0</device>  
      <startmode>auto</startmode>  
    </interface>  
    <interface>  
      <bootproto>static</bootproto>  
      <broadcast>127.255.255.255</broadcast>  
      <device>lo</device>
```

```

    <firewall>no</firewall>
    <ipaddr>127.0.0.1</ipaddr>
    <netmask>255.0.0.0</netmask>
    <network>127.0.0.0</network>
    <prefixlen>8</prefixlen>
    <startmode>nfsroot</startmode>
    <usercontrol>no</usercontrol>
  </interface>
</interfaces>
<ipv6 config:type="boolean">true</ipv6>
<keep_install_network config:type="boolean">false</keep_install_network>
## false means use Wicked, true means use NetworkManager
<managed config:type="boolean">false</managed>
<net-udev config:type="list">
  <rule>
    <name>eth0</name>
    <rule>ATTR{address}</rule>
    <value>00:30:6E:08:EC:80</value>
  </rule>
</net-udev>
<s390-devices config:type="list">
  <listentry>
    <chanids>0.0.0800 0.0.0801 0.0.0802</chanids>
    <type>qeth</type>
  </listentry>
</s390-devices>
<routing>
  <ipv4_forward config:type="boolean">false</ipv4_forward>
  <ipv6_forward config:type="boolean">false</ipv6_forward>
  <routes config:type="list">
    <route>
      <destination>192.168.2.1</destination>
      <device>eth0</device>
      <extrapara>foo</extrapara>
      <gateway>-</gateway>
      <netmask>-</netmask>
    </route>
    <route>
      <destination>default</destination>
      <device>eth0</device>
      <gateway>192.168.1.1</gateway>
      <netmask>-</netmask>
    </route>
    <route>
      <destination>default</destination>
      <device>lo</device>
      <gateway>192.168.5.1</gateway>
    </route>
  </routes>
</routing>

```



```

    <netmask>-</netmask>
  </route>
</routes>
</routing>
</networking>

```

#### EXAMPLE 4.30: BRIDGE INTERFACE CONFIGURATION

```

<interfaces config:type="list">
  <interface>
    <device>br0</device>
    <bootproto>static</bootproto>
    <bridge>yes</bridge>
    <bridge_forwarddelay>0</bridge_forwarddelay>
    <bridge_ports>eth0 eth1</bridge_ports>
    <bridge_stp>off</bridge_stp>
    <ipaddr>192.168.1.100</ipaddr>
    <netmask>255.255.255.0</netmask>
    <network>192.168.1.0</network>
    <prefixlen>24</prefixlen>
    <startmode>auto</startmode>
  </interface>
  <interface>
    <device>eth0</device>
    <bootproto>none</bootproto>
    <startmode>hotplug</startmode>
  </interface>
  <interface>
    <device>eth1</device>
    <bootproto>none</bootproto>
    <startmode>hotplug</startmode>
  </interface>
</interfaces>

```



#### Tip: IPv6 Address Support

Using IPv6 addresses in AutoYaST is fully supported. To disable IPv6 Address Support, set `<ipv6 config:type="boolean">false</ipv6>`

### 4.12.1 Persistent Names of Network Interfaces

The following elements must be between the `<net-udev> ... </net-udev>` tags.

Element	Description	Comment
name	Network interface name, for example <code>eth3</code>	required
rule	<code>ATTR{address}</code> for a MAC based rule, <code>KERNELS</code> for a bus ID based rule	required
value	for example <code>f0:de:f1:6b:da:69</code> for a MAC rule, <code>0000:00:1c.1</code> or <code>0.0.0700</code> for a bus ID rule	required



### Tip: Handling Collisions in Device Names

When creating an incomplete *udev* rule set, the chosen device name can collide with existing device names. For example, when renaming a network interface to `eth0`, a collision with a device automatically generated by the kernel can occur. AutoYaST tries to handle such cases in a best effort manner and renames colliding devices.

## 4.12.2 s390 Options

The following elements must be between the `<s390-devices> ... </s390-devices>` tags.

Element	Description	Comment
type	qeth, ctc or iucv	
chanids	channel ids separated by spaces  <pre>&lt;chanids&gt;0.0.0700 0.0.0701 0.0.0702&lt;/chanids&gt;</pre>	
layer2	<pre>&lt;layer2   config:type="boolean"&gt;true&lt;/ layer2&gt;</pre>	boolean; default: false

Element	Description	Comment
portname	QETH port name (deprecated since SLE 12 SP2)	
protocol	CTC / LCS protocol, a small number (as a string)  <protocol>1</protocol>	optional
router	IUCV router/user	

In addition to the options mentioned above, AutoYaST also supports IBM Z-specific options in other sections of the configuration file. In particular, you can define the logical link address, or LLADDR (in the case of Ethernet, that is the MAC address). To do so, use the option LLADDR in the device definition.



### Tip: LLADDR for VLANs

VLAN devices inherit their LLADDR from the underlying physical devices. To set a particular address for a VLAN device, set the LLADDR option for the underlying physical device.

## 4.12.3 Proxy

Configure your Internet proxy (caching) settings.

Configure proxies for HTTP, HTTPS, and FTP with http\_proxy, https\_proxy and ftp\_proxy, respectively. Addresses or names that should be directly accessible need to be specified with no\_proxy (space separated values). If you are using a proxy server with authorization, fill in proxy\_user and proxy\_password,

EXAMPLE 4.31: NETWORK CONFIGURATION: PROXY

```
<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>www.example.com .example.org localhost</no_proxy>
  <proxy_password>testpw</proxy_password>
  <proxy_user>testuser</proxy_user>
</proxy>
```

## 4.13 NIS Client and Server

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 4.32: NETWORK CONFIGURATION: NIS

```
<nis>
  <nis_broadcast config:type="boolean">true</nis_broadcast>
  <nis_broken_server config:type="boolean">true</nis_broken_server>
  <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>
```

## 4.14 NIS Server

You can configure the target machine as a NIS server. NIS Master Server and NIS Slave Server and a combination of both are available.

EXAMPLE 4.33: NIS SERVER CONFIGURATION

```
<nis_server>
  <domain>mydomain.de</domain>
  <maps_to_serve config:type="list">
    <nis_map>auto.master</nis_map>
    <nis_map>ethers</nis_map>
  </maps_to_serve>
  <merge_passwd config:type="boolean">false</merge_passwd>
```

```

<mingid config:type="integer">0</mingid>
<minuid config:type="integer">0</minuid>
<nopush config:type="boolean">>false</nopush>
<pwd_chfn config:type="boolean">>false</pwd_chfn>
<pwd_chsh config:type="boolean">>false</pwd_chsh>
<pwd_srcdir>/etc</pwd_srcdir>
<securenets config:type="list">
  <securenet>
    <netmask>255.0.0.0</netmask>
    <network>127.0.0.0</network>
  </securenet>
</securenets>
<server_type>master</server_type>
<slaves config:type="list"/>
<start_ybind config:type="boolean">>false</start_ybind>
<start_yppasswdd config:type="boolean">>false</start_yppasswdd>
<start_ypxfrd config:type="boolean">>false</start_ypxfrd>
</nis_server>

```

Attribute	Values	Description
<u>domain</u>	NIS domain name.	
<u>maps_to_serve</u>	List of maps which are available for the server.	Values: auto.master, ethers, group, hosts, netgrp, networks, passwd, protocols, rpc, services, shadow
<u>merge_passwd</u>	Select if your passwd file should be merged with the shadow file (only possible if the shadow file exists).	Value: true/false
<u>mingid</u>	Minimum GID to include in the user maps.	
<u>minuid</u>	Minimum UID to include in the user maps.	
<u>nopush</u>	Do not push the changes to slave servers. (Useful if there are none).	Value: true/false

Attribute	Values	Description
<u>pwd_chfn</u>	YPPWD_CHFN - allow changing the full name	Value: true/false
<u>pwd_chsh</u>	YPPWD_CHSH - allow changing the login shell	Value: true/false
<u>pwd_srcdir</u>	YPPWD_SRCDIR - source directory for passwd data	Default: <u>/etc</u>
<u>securenets</u>	List of allowed hosts to query the NIS server	<p>A host address will be allowed if network is equal to the bitwise AND of the host's address and the netmask.</p> <p>The entry with netmask 255.0.0.0 and network 127.0.0.0 must exist to allow connections from the local host.</p> <p>Entering netmask 0.0.0.0 and network 0.0.0.0 gives access to all hosts.</p>
<u>server_type</u>	Select whether to configure the NIS server as a master or a slave or not to configure a NIS server.	Values: master, slave, none
<u>slaves</u>	List of host names to configure as NIS server slaves.	
<u>start_ybind</u>	This host is also a NIS client (only when client is configured locally).	Value: true/false

Attribute	Values	Description
<u>start_yppasswdd</u>	Also start the password daemon.	Value: true/false
<u>start_ypxfrd</u>	Also start the map transfer daemon. Fast Map distribution; it will speed up the transfer of maps to the slaves.	Value: true/false

## 4.15 Hosts Definition

Using the host resource, you can add more entries to the /etc/hosts file. Already existing entries will not be deleted. The following example shows details.

EXAMPLE 4.34: **/ETC/HOSTS**

```
<host>
  <hosts config:type="list">
    <hosts_entry>
      <host_address>133.3.0.1</host_address>
      <names config:type="list">
        <name>booking</name>
      </names>
    </hosts_entry>
    <hosts_entry>
      <host_address>133.3.0.5</host_address>
      <names config:type="list">
        <name>test-machine</name>
      </names>
    </hosts_entry>
  </hosts>
</host>
```

## 4.16 Windows Domain Membership

Using the samba-client resource, you can configure membership of a workgroup, NT domain, or Active Directory domain.

#### EXAMPLE 4.35: SAMBA CLIENT CONFIGURATION

```
<samba-client>
  <disable_dhcp_hostname config:type="boolean">true</disable_dhcp_hostname>
</global>
  <security>domain</security>
  <usershare_allow_guests>No</usershare_allow_guests>
  <usershare_max_shares>100</usershare_max_shares>
  <workgroup>WORKGROUP</workgroup>
</global>
  <winbind config:type="boolean">>false</winbind>
</samba-client>
```

Attribute	Values	Description
<u>disable_dhcp_hostname</u>	Do not allow DHCP to change the host name.	Value: true/false
<u>global/security</u>	Kind of authentication regime (domain technology or Active Directory server (ADS)).	Value: ADS/domain
<u>global/usershare_allow_guests</u>	Sharing guest access is allowed.	Value: No/Yes
<u>global/user-share_max_shares</u>	Max. number of shares from <u>smb.conf</u> .	0 means that shares are not enabled.
<u>global/workgroup</u>	Workgroup or domain name.	
<u>winbind</u>	Using winbind.	Value: true/false

## 4.17 Samba Server

Configuration of a simple Samba server.

#### EXAMPLE 4.36: SAMBA SERVER CONFIGURATION

```
<samba-server>
```



```

<accounts config:type="list"/>
<backend/>
<config config:type="list">
  <listentry>
    <name>global</name>
    <parameters>
      <security>domain</security>
      <usershare_allow_guests>No</usershare_allow_guests>
      <usershare_max_shares>100</usershare_max_shares>
      <workgroup>WORKGROUP</workgroup>
    </parameters>
  </listentry>
</config>
<service>Disabled</service>
<trustdom/>
<version>2.11</version>
</samba-server>

```

Attribute	Values	Description
<u>accounts</u>	List of Samba accounts.	
<u>backend</u>	List of available back-ends	Value: true/false
<u>config</u>	Setting additional user-defined parameters in <u>/etc/samba/smb.conf</u> .	The example shows parameters in the <u>global</u> section of <u>/etc/samba/smb.conf</u> .
<u>service</u>	Samba service starts during boot.	Value: Enabled/Disabled
<u>trustdom/</u>	Trusted Domains.	A map of two maps (keys: <u>establish</u> , <u>revoke</u> ). Each map contains entries in the format key: domainname value: password.
<u>version</u>	Samba version.	Default: 2.11

## 4.18 Authentication Client

The configuration file must be in the JSON format. Verify that both `autoyast2` and `autoyast2-installation` are installed. Use the *Autoinstallation Configuration* module in YaST to generate a valid JSON configuration file. Launch YaST and switch to the *Miscellaneous > Autoinstallation Configuration*. Choose *Network Services > User Logon Management*, press *Edit*, and configure the available settings. Press *OK* when done. To save the generated configuration file, use the *File > Save*.



### Tip: Using ldaps://

To use LDAP with native SSL (rather than TLS), add the `ldaps` resource.

## 4.19 NFS Client and Server

Configuring a system as an NFS client or an NFS server can be done using the configuration system. The following examples show how both NFS client and server can be configured.

From SUSE Linux Enterprise Server 15 on, the structure of NFS client configuration has changed. Some global configuration options were introduced: `enable_nfs4` to switch NFS4 support on/off and `idmapd_domain` to define domain name for `rpc.idmapd` (this only makes sense when NFS4 is enabled). Attention: the old structure is not compatible with the new one and the control files with an NFS section created on older releases will not work with newer products.

### EXAMPLE 4.37: NETWORK CONFIGURATION: NFS CLIENT

```
<nfs>
  <enable_nfs4 config:type="boolean">true</enable_nfs4>
  <idmapd_domain>suse.cz</idmapd_domain>
  <nfs_entries config:type="list">
    <nfs_entry>
      <mount_point>/home</mount_point>
      <nfs_options>sec=krb5i,intr,rw</nfs_options>
      <server_path>saurus.suse.cz:/home</server_path>
      <vfstype>nfs4</vfstype>
    </nfs_entry>
    <nfs_entry>
      <mount_point>/work</mount_point>
      <nfs_options>defaults</nfs_options>
      <server_path>bivoj.suse.cz:/work</server_path>
      <vfstype>nfs</vfstype>
  </nfs_entries>
</nfs>
```

```

</nfs_entry>
<nfs_entry>
  <mount_point>/mnt</mount_point>
  <nfs_options>defaults</nfs_options>
  <server_path>fallback.suse.cz:/srv/dist</server_path>
  <vfstype>nfs</vfstype>
</nfs_entry>
</nfs_entries>
</nfs>

```

EXAMPLE 4.38: NETWORK CONFIGURATION: NFS SERVER

```

<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_export>
      <allowed config:type="list">
        <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>

```

## 4.20 NTP Client



### Important: NTP Client Profile Incompatible

Starting with SUSE Linux Enterprise Server 15, the NTP client profile has a new format and is *not* compatible with previous profiles. You need to update your NTP client profile used in prior SUSE Linux Enterprise Server versions to be compatible with version 15 and newer.

Following is an example of the NTP client configuration:

EXAMPLE 4.39: NETWORK CONFIGURATION: NTP CLIENT

```

<ntp-client>

```

```

<ntp_policy>auto</ntp_policy>❶
<ntp_servers config:type="list">
  <ntp_server>
    <address>cz.pool.ntp.org</address>❷
    <iburst config:type="boolean">false</iburst>❸
    <offline config:type="boolean">false</offline>❹
  </ntp_server>
</ntp_servers>
<ntp_sync>15</ntp_sync>❺
</ntp-client>

```

- ❶ The `ntp_policy` takes the same values as the `NETCONFIG_NTP_POLICY` option in `/etc/sysconfig/network/config`. The most common options are 'static' and 'auto' (default). See [man 8 netconfig](#) for more details.
- ❷ URL of the time server or pool of time servers.
- ❸ `iburst` speeds up the initial time synchronization for the specific time source after `chronyd` is started.
- ❹ When the `offline` option is set to `true` it will prevent the client from polling the time server if it is not available when `chronyd` is started. Polling will not resume until it is started manually with `chronyc online`. This command does not survive a reboot. Setting it to `false` ensures that clients will always attempt to contact the time server, without administrator intervention.
- ❺ For `ntp_sync`, enter 'systemd' (default) when running an NTP daemon, an *integer* interval in seconds to synchronize using cron, or 'manual' for no automatic synchronization.

The following example illustrates an IPv6 configuration. You may use the server's IP address, host name, or both:

```

<ntp-server>
  <address>2001:418:3ff::1:53</address>
</ntp-server>

<ntp-server>
  <address>2.pool.ntp.org</address>
</ntp-server>

```

## 4.21 Mail Server Configuration

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

EXAMPLE 4.40: MAIL CONFIGURATION

```
<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>

```

## 4.22 Apache HTTP Server Configuration

This section is used for configuration of an Apache HTTP server.

For less experienced users, we would suggest to configure the Apache server using the HTTP server YaST module. After that, call the AutoYaST configuration module, select the HTTP server YaST module and clone the Apache settings. These settings can be exported via the menu File.

```

<http-server>
  <Listen config:type="list">
    <listentry>
      <ADDRESS/>
      <PORT>80</PORT>
    </listentry>
  </Listen>
  <hosts config:type="list">
    <hosts_entry>
      <KEY>main</KEY>
      <VALUE config:type="list">
        <listentry>
          <KEY>DocumentRoot</KEY>
          <OVERHEAD>
            #
            # Global configuration that will be applicable for all
            # virtual hosts, unless deleted here or overridden elsewhere.
            #
          </OVERHEAD>
          <VALUE>"/srv/www/htdocs"</VALUE>
        </listentry>
        <listentry>
          <KEY>_SECTION</KEY>
          <OVERHEAD>
            #
            # Configure the DocumentRoot
            #
          </OVERHEAD>
          <SECTIONNAME>Directory</SECTIONNAME>
          <SECTIONPARAM>"/srv/www/htdocs"</SECTIONPARAM>
          <VALUE config:type="list">
            <listentry>
              <KEY>Options</KEY>
              <OVERHEAD>
                # Possible values for the Options directive are "None", "All",
                # or any combination of:
                #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch
                #   ExecCGI MultiViews
                #
                # Note that "MultiViews" must be named *explicitly*
                # --- "Options All"
                # does not give it to you.
                #
                # The Options directive is both complicated and important.
                # Please see

```

```

# http://httpd.apache.org/docs/2.4/mod/core.html#options
# for more information.
</OVERHEAD>
<VALUE>None</VALUE>
</listentry>
<listentry>
  <KEY>AllowOverride</KEY>
  <OVERHEAD>
    # AllowOverride controls what directives may be placed in
    # .htaccess files. It can be "All", "None", or any combination
    # of the keywords:
    #   Options FileInfo AuthConfig Limit
  </OVERHEAD>
  <VALUE>None</VALUE>
</listentry>
<listentry>
  <KEY>_SECTION</KEY>
  <OVERHEAD>
    # Controls who can get stuff from this server.
  </OVERHEAD>
  <SECTIONNAME>IfModule</SECTIONNAME>
  <SECTIONPARAM>!mod_access_compat.c</SECTIONPARAM>
  <VALUE config:type="list">
    <listentry>
      <KEY>Require</KEY>
      <VALUE>all granted</VALUE>
    </listentry>
  </VALUE>
</listentry>
<listentry>
  <KEY>_SECTION</KEY>
  <SECTIONNAME>IfModule</SECTIONNAME>
  <SECTIONPARAM>mod_access_compat.c</SECTIONPARAM>
  <VALUE config:type="list">
    <listentry>
      <KEY>Order</KEY>
      <VALUE>allow,deny</VALUE>
    </listentry>
    <listentry>
      <KEY>Allow</KEY>
      <VALUE>from all</VALUE>
    </listentry>
  </VALUE>
</listentry>
</VALUE>
</listentry>
<listentry>

```



```

<KEY>Alias</KEY>
<OVERHEAD>
# Aliases: aliases can be added as needed (with no limit).
# The format is Alias fakename realname
#
# Note that if you include a trailing / on fakename then the
# server will require it to be present in the URL. So "/icons"
# is not aliased in this example, only "/icons/". If the fakename
# is slash-terminated, then the realname must also be slash
# terminated, and if the fakename omits the trailing slash, the
# realname must also omit it.
# We include the /icons/ alias for FancyIndexed directory listings.
# If you do not use FancyIndexing, you may comment this out.
#
</OVERHEAD>
<VALUE>/icons/ "/usr/share/apache2/icons/"</VALUE>
</listentry>
<listentry>
  <KEY>_SECTION</KEY>
  <OVERHEAD>
  </OVERHEAD>
  <SECTIONNAME>Directory</SECTIONNAME>
  <SECTIONPARAM>"/usr/share/apache2/icons"</SECTIONPARAM>
  <VALUE config:type="list">
    <listentry>
      <KEY>Options</KEY>
      <VALUE>Indexes MultiViews</VALUE>
    </listentry>
    <listentry>
      <KEY>AllowOverride</KEY>
      <VALUE>None</VALUE>
    </listentry>
  </listentry>
  <KEY>_SECTION</KEY>
  <SECTIONNAME>IfModule</SECTIONNAME>
  <SECTIONPARAM>!mod_access_compat.c</SECTIONPARAM>
  <VALUE config:type="list">
    <listentry>
      <KEY>Require</KEY>
      <VALUE>all granted</VALUE>
    </listentry>
  </VALUE>
</listentry>
<listentry>
  <KEY>_SECTION</KEY>
  <SECTIONNAME>IfModule</SECTIONNAME>
  <SECTIONPARAM>mod_access_compat.c</SECTIONPARAM>

```

```

        <VALUE config:type="list">
            <listentry>
                <KEY>Order</KEY>
                <VALUE>allow,deny</VALUE>
            </listentry>
            <listentry>
                <KEY>Allow</KEY>
                <VALUE>from all</VALUE>
            </listentry>
        </VALUE>
    </listentry>
</VALUE>
</listentry>
<listentry>
    <KEY>ScriptAlias</KEY>
    <OVERHEAD>
        # ScriptAlias: This controls which directories contain server
        # scripts. ScriptAliases are essentially the same as Aliases,
        # except that documents in the realname directory are treated
        # as applications and run by the server when requested rather
        # than as documents sent to the client.
        # The same rules about trailing "/" apply to ScriptAlias
        # directives as to Alias.
        #
    </OVERHEAD>
    <VALUE>/cgi-bin/ "/srv/www/cgi-bin/"</VALUE>
</listentry>
<listentry>
    <KEY>_SECTION</KEY>
    <OVERHEAD>
        # "/srv/www/cgi-bin" should be changed to wherever your
        # ScriptAliased CGI directory exists, if you have that configured.
        #
    </OVERHEAD>
    <SECTIONNAME>Directory</SECTIONNAME>
    <SECTIONPARAM>"/srv/www/cgi-bin"</SECTIONPARAM>
    <VALUE config:type="list">
        <listentry>
            <KEY>AllowOverride</KEY>
            <VALUE>None</VALUE>
        </listentry>
        <listentry>
            <KEY>Options</KEY>
            <VALUE>+ExecCGI -Includes</VALUE>
        </listentry>
        <listentry>
            <KEY>_SECTION</KEY>

```

```

<SECTIONNAME>IfModule</SECTIONNAME>
<SECTIONPARAM>!mod_access_compat.c</SECTIONPARAM>
<VALUE config:type="list">
  <listentry>
    <KEY>Require</KEY>
    <VALUE>all granted</VALUE>
  </listentry>
</VALUE>
</listentry>
<listentry>
  <KEY>_SECTION</KEY>
  <SECTIONNAME>IfModule</SECTIONNAME>
  <SECTIONPARAM>mod_access_compat.c</SECTIONPARAM>
  <VALUE config:type="list">
    <listentry>
      <KEY>Order</KEY>
      <VALUE>allow,deny</VALUE>
    </listentry>
    <listentry>
      <KEY>Allow</KEY>
      <VALUE>from all</VALUE>
    </listentry>
  </VALUE>
</listentry>
</VALUE>
</listentry>
<listentry>
  <KEY>_SECTION</KEY>
  <OVERHEAD>
  # UserDir: The name of the directory that is appended onto a
  # user's home directory if a ~user request is received.
  # To disable it, simply remove userdir from the list of modules
  # in APACHE_MODULES in /etc/sysconfig/apache2.
  #
  </OVERHEAD>
  <SECTIONNAME>IfModule</SECTIONNAME>
  <SECTIONPARAM>mod_userdir.c</SECTIONPARAM>
  <VALUE config:type="list">
    <listentry>
      <KEY>UserDir</KEY>
      <OVERHEAD>
      # Note that the name of the user directory ("public_html")
      # cannot simply be changed here, since it is a compile time
      # setting. The apache package would have to be rebuilt.
      # You could work around by deleting /usr/sbin/suexec, but
      # then all scripts from the directories would be executed
      # with the UID of the webserver.

```

```

        </OVERHEAD>
        <VALUE>public_html</VALUE>
    </listentry>
    <listentry>
        <KEY>Include</KEY>
        <OVERHEAD>
        # The actual configuration of the directory is in
        # /etc/apache2/mod_userdir.conf.
        </OVERHEAD>
        <VALUE>/etc/apache2/mod_userdir.conf</VALUE>
    </listentry>
</VALUE>
</listentry>
<listentry>
    <KEY>IncludeOptional</KEY>
    <OVERHEAD>
    # Include all *.conf files from /etc/apache2/conf.d/.
    #
    # This is mostly meant as a place for other RPM packages to drop
    # in their configuration snippet.
    #
    # You can comment this out here if you want those bits include
    # only in a certain virtual host, but not here.
    </OVERHEAD>
    <VALUE>/etc/apache2/conf.d/*.conf</VALUE>
</listentry>
<listentry>
    <KEY>IncludeOptional</KEY>
    <OVERHEAD>
    # The manual... if it is installed ('?' means it will not complain)
    </OVERHEAD>
    <VALUE>/etc/apache2/conf.d/apache2-manual?conf</VALUE>
</listentry>
<listentry>
    <KEY>ServerName</KEY>
    <VALUE>linux-wtyj</VALUE>
</listentry>
<listentry>
    <KEY>ServerAdmin</KEY>
    <OVERHEAD>
    </OVERHEAD>
    <VALUE>root@linux-wtyj</VALUE>
</listentry>
<listentry>
    <KEY>NameVirtualHost</KEY>
    <VALUE>192.168.43.2</VALUE>

```

```

        </listentry>
    </VALUE>
</hosts_entry>
<hosts_entry>
    <KEY>192.168.43.2/secondserver.suse.de</KEY>
    <VALUE config:type="list">
        <listentry>
            <KEY>DocumentRoot</KEY>
            <VALUE>/srv/www/htdocs</VALUE>
        </listentry>
        <listentry>
            <KEY>ServerName</KEY>
            <VALUE>secondserver.suse.de</VALUE>
        </listentry>
        <listentry>
            <KEY>ServerAdmin</KEY>
            <VALUE>second_server@suse.de</VALUE>
        </listentry>
        <listentry>
            <KEY>_SECTION</KEY>
            <SECTIONNAME>Directory</SECTIONNAME>
            <SECTIONPARAM>/srv/www/htdocs</SECTIONPARAM>
            <VALUE config:type="list">
                <listentry>
                    <KEY>AllowOverride</KEY>
                    <VALUE>None</VALUE>
                </listentry>
                <listentry>
                    <KEY>Require</KEY>
                    <VALUE>all granted</VALUE>
                </listentry>
            </VALUE>
        </listentry>
    </VALUE>
</hosts_entry>
</hosts>
<modules config:type="list">
    <module_entry>
        <change>enable</change>
        <name>socache_shmcb</name>
        <userdefined config:type="boolean">true</userdefined>
    </module_entry>
    <module_entry>
        <change>enable</change>
        <name>reqtimeout</name>
        <userdefined config:type="boolean">true</userdefined>
    </module_entry>

```

```

<module_entry>
  <change>enable</change>
  <name>authn_core</name>
  <userdefined config:type="boolean">true</userdefined>
</module_entry>
<module_entry>
  <change>enable</change>
  <name>authz_core</name>
  <userdefined config:type="boolean">true</userdefined>
</module_entry>
</modules>
<service config:type="boolean">true</service>
<version>2.9</version>
</http-server>

```

List Name	List Elements	Description
Listen		List of host <u>Listen</u> settings
	PORT	port address
	ADDRESS	Network address. All addresses will be taken if this entry is empty.
hosts		List of Hosts configuration
	KEY	Host name; <u>&lt;KEY&gt;main&lt;/KEY&gt;</u> defines the main hosts, for example <u>&lt;KEY&gt;192.168.43.2/sec-ondserver.suse.de&lt;/KEY&gt;</u>
	VALUE	List of different values describing the host.
modules		Module list. Only user-defined modules need to be described.
	name	Module name

List Name	List Elements	Description
	userdefined	For historical reasons, it is always set to <u>true</u> .
	change	For historical reasons, it is always set to <u>enable</u> .

Element	Description	Comment
version	Version of used Apache server	Only for information. Default 2.9
service	Enable Apache service	Optional. Default: false



### Note: Firewall

To run an Apache server correctly, make sure the firewall is configured appropriately.

## 4.23 Squid Server

Squid is a caching and forwarding Web proxy.

EXAMPLE 4.42: **SQUID SERVER CONFIGURATION**

```
<squid>
  <acls config:type="list">
    <listentry>
      <name>QUERY</name>
      <options config:type="list">
        <option>cgi-bin \?</option>
      </options>
      <type>urlpath_regex</type>
    </listentry>
    <listentry>
      <name>apache</name>
      <options config:type="list">
        <option>Server</option>
        <option>^Apache</option>
      </options>
      <type>rep_header</type>
    </listentry>
```

```

<listentry>
  <name>all</name>
  <options config:type="list">
    <option>0.0.0.0/0.0.0.0</option>
  </options>
  <type>src</type>
</listentry>
<listentry>
  <name>manager</name>
  <options config:type="list">
    <option>cache_object</option>
  </options>
  <type>proto</type>
</listentry>
<listentry>
  <name>localhost</name>
  <options config:type="list">
    <option>127.0.0.1/255.255.255.255</option>
  </options>
  <type>src</type>
</listentry>
<listentry>
  <name>to_localhost</name>
  <options config:type="list">
    <option>127.0.0.0/8</option>
  </options>
  <type>dst</type>
</listentry>
<listentry>
  <name>SSL_ports</name>
  <options config:type="list">
    <option>443</option>
  </options>
  <type>port</type>
</listentry>
<listentry>
  <name>Safe_ports</name>
  <options config:type="list">
    <option>80</option>
  </options>
  <type>port</type>
</listentry>
<listentry>
  <name>Safe_ports</name>
  <options config:type="list">
    <option>21</option>
  </options>

```



```

    <type>port</type>
</listentry>
<listentry>
  <name>Safe_ports</name>
  <options config:type="list">
    <option>443</option>
  </options>
  <type>port</type>
</listentry>
<listentry>
  <name>Safe_ports</name>
  <options config:type="list">
    <option>70</option>
  </options>
  <type>port</type>
</listentry>
<listentry>
  <name>Safe_ports</name>
  <options config:type="list">
    <option>210</option>
  </options>
  <type>port</type>
</listentry>
<listentry>
  <name>Safe_ports</name>
  <options config:type="list">
    <option>1025-65535</option>
  </options>
  <type>port</type>
</listentry>
<listentry>
  <name>Safe_ports</name>
  <options config:type="list">
    <option>280</option>
  </options>
  <type>port</type>
</listentry>
<listentry>
  <name>Safe_ports</name>
  <options config:type="list">
    <option>488</option>
  </options>
  <type>port</type>
</listentry>
<listentry>
  <name>Safe_ports</name>
  <options config:type="list">

```

```

        <option>591</option>
      </options>
    </type>port</type>
  </listentry>
</listentry>
  <name>Safe_ports</name>
  <options config:type="list">
    <option>777</option>
  </options>
  <type>port</type>
</listentry>
</listentry>
  <name>CONNECT</name>
  <options config:type="list">
    <option>CONNECT</option>
  </options>
  <type>method</type>
</listentry>
</acls>
<http_accesses config:type="list">
  <listentry>
    <acl config:type="list">
      <listentry>manager</listentry>
      <listentry>localhost</listentry>
    </acl>
    <allow config:type="boolean">true</allow>
  </listentry>
  <listentry>
    <acl config:type="list">
      <listentry>manager</listentry>
    </acl>
    <allow config:type="boolean">>false</allow>
  </listentry>
  <listentry>
    <acl config:type="list">
      <listentry>!Safe_ports</listentry>
    </acl>
    <allow config:type="boolean">>false</allow>
  </listentry>
  <listentry>
    <acl config:type="list">
      <listentry>CONNECT</listentry>
      <listentry>!SSL_ports</listentry>
    </acl>
    <allow config:type="boolean">>false</allow>
  </listentry>
</listentry>

```

```

    <acl config:type="list">
      <listentry>localhost</listentry>
    </acl>
    <allow config:type="boolean">true</allow>
  </listentry>
  <listentry>
    <acl config:type="list">
      <listentry>all</listentry>
    </acl>
    <allow config:type="boolean">>false</allow>
  </listentry>
</http_accesses>
<http_ports config:type="list">
  <listentry>
    <host/>
    <port>3128</port>
    <transparent config:type="boolean">>false</transparent>
  </listentry>
</http_ports>
<refresh_patterns config:type="list">
  <listentry>
    <case_sensitive config:type="boolean">true</case_sensitive>
    <max>10080</max>
    <min>1440</min>
    <percent>20</percent>
    <regexp>^ftp:</regexp>
  </listentry>
  <listentry>
    <case_sensitive config:type="boolean">true</case_sensitive>
    <max>1440</max>
    <min>1440</min>
    <percent>0</percent>
    <regexp>^gopher:</regexp>
  </listentry>
  <listentry>
    <case_sensitive config:type="boolean">true</case_sensitive>
    <max>4320</max>
    <min>0</min>
    <percent>20</percent>
    <regexp>.</regexp>
  </listentry>
</refresh_patterns>
<service_enabled_on_startup config:type="boolean">true</service_enabled_on_startup>
<settings>
  <access_log config:type="list">
    <listentry>/var/log/squid/access.log</listentry>
  </access_log>

```

```

<cache_dir config:type="list">
  <listentry>ufs</listentry>
  <listentry>/var/cache/squid</listentry>
  <listentry>100</listentry>
  <listentry>16</listentry>
  <listentry>256</listentry>
</cache_dir>
<cache_log config:type="list">
  <listentry>/var/log/squid/cache.log</listentry>
</cache_log>
<cache_mem config:type="list">
  <listentry>8</listentry>
  <listentry>MB</listentry>
</cache_mem>
<cache_mgr config:type="list">
  <listentry>webmaster</listentry>
</cache_mgr>
<cache_replacement_policy config:type="list">
  <listentry>lru</listentry>
</cache_replacement_policy>
<cache_store_log config:type="list">
  <listentry>/var/log/squid/store.log</listentry>
</cache_store_log>
<cache_swap_high config:type="list">
  <listentry>95</listentry>
</cache_swap_high>
<cache_swap_low config:type="list">
  <listentry>90</listentry>
</cache_swap_low>
<client_lifetime config:type="list">
  <listentry>1</listentry>
  <listentry>days</listentry>
</client_lifetime>
<connect_timeout config:type="list">
  <listentry>2</listentry>
  <listentry>minutes</listentry>
</connect_timeout>
<emulate_httpd_log config:type="list">
  <listentry>off</listentry>
</emulate_httpd_log>
<error_directory config:type="list">
  <listentry/>
</error_directory>
<ftp_passive config:type="list">
  <listentry>on</listentry>
</ftp_passive>
<maximum_object_size config:type="list">

```

```

    <listentry>4096</listentry>
    <listentry>KB</listentry>
  </maximum_object_size>
  <memory_replacement_policy config:type="list">
    <listentry>lru</listentry>
  </memory_replacement_policy>
  <minimum_object_size config:type="list">
    <listentry>0</listentry>
    <listentry>KB</listentry>
  </minimum_object_size>
</settings>
</squid>

```

Attribute	Values	Description
<u>acls</u>	List of Access Control Settings (ACLs).	Each list entry contains the name, type, and additional options. Use the YaST Squid configuration module to get an overview of possible entries.
<u>http_accesses</u>	In the Access Control table, access can be denied or allowed to ACL Groups.	<p>If there are more ACL Groups in one definition, access will be allowed or denied to members who belong to all ACL Groups at the same time.</p> <p>The Access Control table is checked in the order listed here. The first matching entry is used.</p>
<u>http_ports</u>	Define all ports where Squid will listen for clients' HTTP requests.	<p><u>Host</u> can contain a host name or IP address or remain empty.</p> <p><u>transparent</u> disables PMTU discovery when transparent.</p>

Attribute	Values	Description
<u>refresh_patterns</u>	Refresh patterns define how Squid treats the objects in the cache.	<p>The refresh patterns are checked in the order listed here. The first matching entry is used.</p> <p><u>Min</u> determines how long (in minutes) an object should be considered fresh if no explicit expiry time is given. <u>Max</u> is the upper limit of how long objects without an explicit expiry time will be considered fresh. <u>Percent</u> is the percentage of the object's age (time since last modification). An object without an explicit expiry time will be considered fresh.</p>
<u>settings</u>	Map of all available general parameters with default values.	Use the YaST Squid configuration module to get an overview about possible entries.
<u>service_enabled_on_startup</u>	Squid service start when booting.	Value: true/false

## 4.24 FTP Server

Configure your FTP Internet server settings.

EXAMPLE 4.43: **FTP SERVER CONFIGURATION:**

```
<ftp-server>
  <AnonAuthen>2</AnonAuthen>
  <AnonCreatDirs>NO</AnonCreatDirs>
  <AnonMaxRate>0</AnonMaxRate>
```

```

<AnonReadOnly>NO</AnonReadOnly>
<AntiWarez>YES</AntiWarez>
<Banner>Welcome message</Banner>
<CertFile/>
<ChrootEnable>NO</ChrootEnable>
<EnableUpload>YES</EnableUpload>
<FTPUser>ftp</FTPUser>
<FtpDirAnon>/srv/ftp</FtpDirAnon>
<FtpDirLocal/>
<GuestUser/>
<LocalMaxRate>0</LocalMaxRate>
<MaxClientsNumber>10</MaxClientsNumber>
<MaxClientsPerIP>3</MaxClientsPerIP>
<MaxIdleTime>15</MaxIdleTime>
<PasMaxPort>40500</PasMaxPort>
<PasMinPort>40000</PasMinPort>
<PassiveMode>YES</PassiveMode>
<SSL>0</SSL>
<SSLEnable>NO</SSLEnable>
<SSLv2>NO</SSLv2>
<SSLv3>NO</SSLv3>
<StartDaemon>2</StartDaemon>
<TLS>YES</TLS>
<Umask/>
<UmaskAnon/>
<UmaskLocal/>
<VerboseLogging>NO</VerboseLogging>
<VirtualUser>NO</VirtualUser>
</ftp-server>

```

Element	Description	Comment
AnonAuthen	Enable/disable anonymous and local users.	Authenticated Users Only: 1; Anonymous Only: 0; Both: 2
AnonCreatDirs	Anonymous users can create directories.	Values: YES/NO
AnonReadOnly	Anonymous users can upload.	Values: YES/NO
AnonMaxRate	The maximum data transfer rate permitted for anonymous clients.	KB/s

Element	Description	Comment
AntiWarez	Disallow downloading of files that were uploaded but not validated by a local admin.	Values: YES/NO
Banner	Specify the name of a file containing the text to display when someone connects to the server.	
CertFile	DSA certificate to use for SSL-encrypted connections	This option specifies the location of the DSA certificate to use for SSL-encrypted connections.
ChrootEnable	When enabled, local users will be (by default) placed in a chroot jail in their home directory after login.	Warning: This option has security implications. Values: YES/NO
EnableUpload	If enabled, FTP users can upload.	To allow anonymous users to upload, enable <u>AnonReadOnly</u> . Values: YES/NO
FTPUser	Defining anonymous FTP user.	
FtpDirAnon	FTP directory for anonymous users.	Specify a directory which is used for FTP anonymous users.
FtpDirLocal	FTP directory for authenticated users.	Specify a directory which is used for FTP authenticated users.



Element	Description	Comment
LocalMaxRate	The maximum data transfer rate permitted for local authenticated users.	KB/s
MaxClientsNumber	The maximum number of clients allowed to connect.	
MaxClientsPerIP	Max clients for one IP.	The maximum number of clients allowed to connect from the same source Internet address.
MaxIdleTime	The maximum time (timeout) a remote client may wait between FTP commands.	Minutes
PasMaxPort	Maximum value for a port range for passive connection replies.	<u>PassiveMode</u> needs to be set to YES.
PasMinPort	Minimum value for a port range for passive connection replies.	<u>PassiveMode</u> needs to be set to YES.
PassiveMode	Enable Passive Mode	Value: YES/NO
SSL	Security Settings	Disable SSL/TLS: 0; Accept SSL and TLS: 1; Refuse Connections Without SSL/TLS: 2
SSLEnable	If enabled, SSL connections are allowed.	Value: YES/NO
SSLv2	If enabled, SSL version 2 connections are allowed.	Value: YES/NO

Element	Description	Comment
SSLv3	If enabled, SSL version 3 connections are allowed.	Value: YES/NO
StartDaemon	FTP daemon is started.	Manually: 0; when booting: 1; via <code>systemd</code> socket: 2
TLS	If enabled, TLS connections are allowed.	Value: YES/NO
Umask	File creation mask. (umask for files):(umask for directories).	For example <code>177:077</code> if you feel paranoid.
UmaskAnon	The value to which the umask for file creation is set for anonymous users.	To specify octal values, remember the "0" prefix, otherwise the value will be treated as a base 10 integer.
UmaskLocal	Umask for authenticated users.	To specify octal values, remember the "0" prefix, otherwise the value will be treated as a base 10 integer.
VerboseLogging	When enabled, all FTP requests and responses are logged.	Value: YES/NO
VirtualUser	By using virtual users, FTP accounts can be administrated without affecting system accounts.	Value: YES/NO



### Note: Firewall

Proper Firewall setting will be required for the FTP server to run correctly.

## 4.25 TFTP Server

Configure your TFTP Internet server settings.

Use this to enable a server for TFTP (trivial file transfer protocol). The server will be started using the `systemd` socket.

Note that TFTP and FTP are not the same.

### EXAMPLE 4.44: TFTP SERVER CONFIGURATION:

```
<tftp-server>
  <start_tftpd config:type="boolean">true</start_tftpd>
  <tftp_directory>/tftpboot</tftp_directory>
</tftp-server>
```

Element	Description	Comment
start_tftpd	Enabling TFTP server service.	Value: true/false
tftp_directory	Boot Image Directory: Specify the directory where served files are located.	The usual value is /tftpboot. The directory will be created if it does not exist. The server uses this as its root directory (using the -s option).

## 4.26 Firstboot Workflow

The YaST firstboot utility (YaST Initial System Configuration), which runs after the installation is completed, lets you configure the freshly installed system. On the first boot after the installation, users are guided through a series of steps that allow for easier configuration of a system. YaST firstboot does not run by default and needs to be configured to run.

### EXAMPLE 4.45: ENABLING FIRSTBOOT WORKFLOW

```
<firstboot>
  <firstboot_enabled config:type="boolean">true</firstboot_enabled>
</firstboot>
```

## 4.27 Security Settings

Using the features of this module, you can to change the local security settings on the target system. The local security settings include the boot configuration, login settings, password settings, user addition settings, and file permissions.

Configuring the security settings automatically is similar to the [Custom Settings](#) in the security module available in the running system. This allows you create a customized configuration.

### EXAMPLE 4.46: SECURITY CONFIGURATION

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

```
<security>
  <console_shutdown>ignore</console_shutdown>
  <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>
  <gdm_shutdown>root</gdm_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>
```

### 4.27.1 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 do not support this, and you may have problems with NIS. Blowfish is also supported.

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

## 4.27.2 Boot Settings

Use the security resource, to 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 GDM

Configure a list of users allowed to shut down the machine from GDM.

## 4.27.3 Login Settings

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

## 4.27.4 New user settings (`useradd` settings)

Set the minimum and maximum possible user and group ID

# 4.28 Linux Audit Framework (LAF)

This module allows the configuration of the audit daemon and to add rules for the audit subsystem.

EXAMPLE 4.47: LAF CONFIGURATION

```
<audit-laf>
  <auditd>
    <flush>INCREMENTAL</flush>
    <freq>20</freq>
```

```

<log_file>/var/log/audit/audit.log</log_file>
<log_format>RAW</log_format>
<max_log_file>5</max_log_file>
<max_log_file_action>ROTATE</max_log_file_action>
<name_format>NONE</name_format>
<num_logs>4</num_logs>
</auditd>
<rules/>
</audit-laf>

```

Attribute	Values	Description
<u>auditd/flush</u>	Describes how to write the data to disk.	If set to <u>INCREMENTAL</u> the Frequency parameter tells how many records to write before issuing an explicit flush to disk. <u>NONE</u> means: no special effort is made to flush data, <u>DATA</u> : keep data portion synchronized, <u>SYNC</u> : keep data and metadata fully synchronized.
<u>auditd/freq</u>	This parameter tells how many records to write before issuing an explicit flush to disk.	The parameter <u>flush</u> needs to be set to <u>INCREMENTAL</u> .
<u>auditd/log_file</u>	The full path name to the log file.	
<u>auditd/log_fomat</u>	How much information needs to be logged.	Set <u>RAW</u> to log all data (store in a format exactly as the kernel sends it) or <u>NOLOG</u> to discard all audit information instead of writing it to disk (does not affect data sent to the dispatcher).

Attribute	Values	Description
<u>auditd/max_log_file</u>	How much information needs to be logged.	Unit: Megabytes
<u>auditd/num_logs</u>	Number of log files.	<u>max_log_file_action</u> needs to be set to <u>ROTATE</u>
<u>auditd/max_log_file_action</u>	What happens if the log capacity has been reached.	If the action is set to <u>ROTATE</u> the Number of Log Files specifies the number of files to keep. Set to <u>SYSLLOG</u> , the audit daemon will write a warning to the system log. With <u>SUSPEND</u> the daemon stops writing records to disk. <u>IGNORE</u> means do nothing, <u>KEEP_LOGS</u> is similar to <u>ROTATE</u> , but log files are not overwritten.
<u>auditd/name_format</u>	Computer Name Format describes how to write the computer name to the log file.	If <u>USER</u> is set, the user-defined name is used. <u>NONE</u> means no computer name is inserted. <u>HOSTNAME</u> uses the name returned by the 'gethostname' syscall. <u>FQD</u> uses the fully qualified domain name.
<u>rules</u>	Rules for auditctl	You can edit the rules manually, which we only recommend for advanced users. For more information about all options, see <b>man auditctl</b> .

## 4.29 Users and Groups

AutoYaST supports defining local users, groups, special login settings and even default options for new users. Those settings are defined in the following sections:

### users

List of users

### user\_defaults

Default options for new users

### groups

List of groups

### login\_settings

Special login settings like password-less login or autologin



### Note: Users and groups set up during the first stage

Users and groups are set up during the first stage, so you can set up a usable system without running the second stage.

### 4.29.1 Users

A list of users can be defined in the `<users>` section. To be able to log in, make sure that either the `root` users are set up or `rootpassword` is specified as a `linuxrc` option.

#### EXAMPLE 4.48: MINIMAL USER CONFIGURATION

```
<users config:type="list">
  <user>
    <username>root</username>
    <user_password>password</user_password>
    <encrypted config:type="boolean">>false</encrypted>
  </user>
  <user>
    <username>tux</username>
    <user_password>password</user_password>
    <encrypted config:type="boolean">>false</encrypted>
  </user>
```



```
</users>
```

The following example shows a more complex scenario. System-wide default settings from `/etc/default/useradd`, such as the shell or the parent directory for the home directory, are applied.

EXAMPLE 4.49: COMPLEX USER CONFIGURATION

```
<users config:type="list">
  <user>
    <username>root</username>
    <user_password>password</user_password>
    <uid>1001</uid>
    <gid>100</gid>
    <encrypted config:type="boolean">false</encrypted>
    <fullname>Root User</fullname>
    <authorized_keys config:type="list">
      <listentry>command="/opt/login.sh" ssh-rsa
      AAAAB3NzaC1yc2EAAAADAQABAAQDKLt1vnW2vTJpBp3VK91rFsBvpY97NljsVLdgUrlPbZ/
      L51FerQQ+djQ/ivDASQj0+567nMGqfYGFA/De1EGMMEoeShza67qjNi14L1HBGgVojaNajMR/
      NI2d1kDyvsgRy7D7FT5UGGUNT0dlcSD3b85zgwHeYLidgcGIoKeRi7HpVD00TyhwUv4sq3ubrPCWARgPe0LdVFfa9clC8PTZdxSeKp4j
      PvMDa96DpxH1VlzJlAIHQsMkMHbsCazPNC0++Kp5ZVERiH root@example.net</listentry>
    </authorized_keys>
  </user>
  <user>
    <username>tux</username>
    <user_password>password</user_password>
    <uid>1002</uid>
    <gid>100</gid>
    <encrypted config:type="boolean">false</encrypted>
    <fullname>Plain User</fullname>
    <home>/Users/plain</home>
    <password_settings>
      <max>120</max>
      <inact>5</inact>
    </password_settings>
  </user>
</users>
```



### Note: `authorized_keys` File Will Be Overwritten

If the profile defines a set of SSH authorized keys for a user in the `authorized_keys` section, an existing `$HOME/.ssh/authorized_keys` file will be overwritten. If not existing, the file will be created with the content specified. Avoid overwriting an existing `authorized_keys` file by not specifying the respective section in the AutoYaST control file.



## Note: Combine rootpassword and Root User Options

It is possible to specify `rootpassword` in `linuxrc` and also have a user section for the `root` user. If this section is missing the password, then the password from `linuxrc` will be used. Passwords in profiles take precedence over `linuxrc` passwords.



## Note: Specifying a User ID (uid)

Each user on a Linux system has a numeric user ID. You can either specify such a user ID within the AutoYaST control file manually by using `uid`, or let the system automatically choose a user ID by not using `uid`.

User IDs should be unique throughout the system. If not, some applications such as the login manager `gdm` may no longer work as expected.

When adding users with the AutoYaST control file, it is strongly recommended not to mix user-defined IDs and automatically provided IDs. When doing so, unique IDs cannot be guaranteed. Either specify IDs for all users added with the AutoYaST control file or let the system choose the ID for all users.

username

Text

```
<username>suzanne</username>
```

Required. It should be a valid user name. Check `man 8 useradd` if you are not sure.

fullname

Text

```
<fullname>Suzanne Geeko</fullname>
```

Optional. User's full name.

forename

Text

```
<forename>Suzanne</forename>
```

Optional. User's forename.

surname

Text

```
<surname>Geeko</surname>
```

Optional. User's surname.

#### uid

Number

```
<uid>1001</uid>
```

Optional. User ID. It should be a unique and must be a non-negative number. If not specified, AutoYaST will automatically choose a user ID. Also refer to *Note: Specifying a User ID (uid)* for additional information.

#### gid

Number

```
<gid>100</gid>
```

Optional. Initial group ID. It must be a unique and non-negative number. Moreover it must refer to an existing group.

#### home

Path

```
<home>/home/suzanne</home>
```

Optional. Absolute path to the user's home directory. By default, /home/username will be used (for example, alice's home directory will be /home/alice).

#### home\_btrfs\_subvolume

Boolean

```
<home_btrfs_subvolume config:type="boolean">true</home_btrfs_subvolume>
```

Optional. Generates the home directory in a Btrfs subvolume. Disabled by default.

#### shell

Path

```
<shell>/usr/bin/zsh</shell>
```

Optional. /bin/bash is the default value. If you choose another one, make sure that it's installed (adding the corresponding package to the software section).

## user\_password

Text

```
<user_password>some-password</user_password>
```

Optional. A user's password can be written in plain text (not recommended) or in encrypted form. To create an encrypted password, use **mkpasswd**. Enter the password as written in `/etc/shadow` (second column). To enable or disable the use of encrypted passwords in the profile, see the `encrypted` parameter. With encrypted passwords disabled, if you enter an exclamation mark (`!`), a random password will be generated. With encrypted passwords enabled, the value is copied to the password field of `/etc/shadow`. If you enter an exclamation mark (`!`) in this case, you get an account with locked password that cannot login on console.

## encrypted

Text

```
<user_password>some-password</user_password>
```

Boolean

```
<encrypted config:type="boolean">true</encrypted>
```

Optional. Considered `false` if not present. Indicates if the user's password in the profile is encrypted or not. AutoYaST supports the standard encryption algorithms (see **man 3 crypt**).

## password\_settings

Password settings

```
<password_settings>
  <expire/>
  <max>60</max>
  <warn>7</warn>
</password_settings>
```

Optional. Some password settings can be customized: `expire` (account expiration date in format `YYYY-MM-DD`), `flag` (`/etc/shadow` flag), `inact` (number of days after password expiration that account is disabled), `max` (maximum number of days a password is valid), `min` (grace period in days until which a user can change password after it has expired) and `warn` (number of days before expiration when the password change reminder starts).

## authorized\_keys

List of authorized keys

```
<authorized_keys config:type="list">
  <listentry>ssh-rsa ...</listentry>
</authorized_keys>
```

A list of authorized keys to be written to `$HOME/.ssh/authorized_keys`. See example below.

## 4.29.2 User Defaults

The profile can specify a set of default values for new users like password expiration, initial group, home directory prefix, etc. Besides using them as default values for the users that are defined in the profile, AutoYaST will write those settings to `/etc/default/useradd` to be read for `useradd`.

### group

Text

```
<group>100</group>
```

Optional. Default initial login group.

### groups

Text

```
<groups>users</groups>
```

Optional. List of additional groups.

### home

Path

```
<home>/home</home>
```

Optional. User's home directory prefix.

### expire

Date

```
<expire>2017-12-31</expire>
```

Optional. Default password expiration date in YYYY-MM-DD format.

#### inactive

Number

```
<inactive>3</inactive>
```

Optional. Number of days after which an expired account is disabled.

#### no\_groups

Boolean

```
<no_groups config:type="boolean">true</no_groups>
```

Optional. Do not use secondary groups.

#### shell

Path

```
<shell>/usr/bin/fish</shell>
```

Default login shell. /bin/bash is the default value. If you choose another one, make sure that it is installed (adding the corresponding package to the software section).

#### skel

Path

```
<skel>/etc/skel</skel>
```

Optional. Location of the files to be used as skeleton when adding a new user. You can find more information in man 8 useradd.

#### umask

File creation mode mask

```
<umask>022</umask>
```

Set the file creation mode mask for the home directory. By default useradd will use 022. Check man 8 useradd and man 1 umask for further information.

### 4.29.3 Groups

A list of groups can be defined in <groups> as shown in the example.

#### EXAMPLE 4.50: GROUP CONFIGURATION

```
<groups config:type="list">
  <group>
    <gid>100</gid>
    <groupname>users</groupname>
    <userlist>bob,alice</userlist>
  </group>
</groups>
```

##### group

Text

```
<group>100</group>
```

Optional. Default initial login group.

##### groups

Text

```
<groups>users</groups>
```

Optional. List of additional groups.

##### home

Path

```
<home>/home</home>
```

Optional. User's home directory prefix.

##### expire

Date

```
<expire>2017-12-31</expire>
```

Optional. Default password expiration date in YYYY-MM-DD format.

##### inactive

Number

```
<inactive>3</inactive>
```

Optional. Number of days after which an expired account is disabled.

### no\_groups

Boolean

```
<no_groups config:type="boolean">true</no_groups>
```

Optional. Do not use secondary groups.

### shell

Path

```
<shell>/usr/bin/fish</shell>
```

Default login shell. /bin/bash is the default value. If you choose another one, make sure that it is installed (adding the corresponding package to the software section).

### skel

Path

```
<skel>/etc/skel</skel>
```

Optional. Location of the files to be used as skeleton when adding a new user. You can find more information in man 8 useradd.

### umask

File creation mode mask

```
<umask>022</umask>
```

Set the file creation mode mask for the home directory. By default useradd will use 022. Check man 8 useradd and man 1 umask for further information.

## 4.29.4 Login Settings

Two special login settings can be enabled through an AutoYaST profile: autologin and password-less login. Both of them are disabled by default.

### EXAMPLE 4.51: ENABLING AUTOLOGIN AND PASSWORD-LESS LOGIN

```
<login_settings>
  <autologin_user>vagrant</autologin_user>
  <password_less_login config:type="boolean">true</password_less_login>
```



```
</login_settings>
```

password\_less\_login

Boolean

```
<password_less_login config:type="boolean">true</password_less_login>
```

Optional. Enables password-less login. It only affects graphical login.

autologin\_user

Text

```
<autologin_user>alice</autologin_user>
```

Optional. Enables autologin for the given user.

## 4.30 Custom User Scripts

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

In the auto-installation process, five types of scripts can be executed at different points in time during the installation:

All scripts need to be in the `<scripts>` section.

- pre-scripts (very early, before anything else really happens)
- postpartitioning-scripts (after partitioning and mounting to `/mnt` but before RPM installation)
- chroot-scripts (after the package installation, before the first boot)
- post-scripts (during the first boot of the installed system, no services running)
- init-scripts (during the first boot of the installed system, all services up and running)

### 4.30.1 Pre-Install Scripts

Executed before YaST does any real change to the system (before partitioning and package installation but after the hardware detection).

You can use a pre-script to modify your control file and let AutoYaST reread it. Find your control file in `/tmp/profile/autoinst.xml`. Adjust the file and store the modified version in `/tmp/profile/modified.xml`. AutoYaST will read the modified file after the pre-script finishes.

It is also possible to change the partitioning in your pre-script.



### Note: 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`).



### Note: Pre-Install and Zypper

To call *zypper* in the pre-install script you will need to set the environment variable `ZYPP_LOCKFILE_ROOT="/var/run/autoyast"` to prevent conflicts with the running YaST process.

Pre-Install Script elements must be placed as follows:

```
<scripts>
  <pre-scripts config:type="list">
    <script>
      ...
    </script>
  </pre-scripts>
</scripts>
```

## 4.30.2 Post-partitioning Scripts

Executed after YaST has done the partitioning and written the `fstab`. The empty system is already mounted to `/mnt`.

Post-partitioning script elements must be placed as follows:

```
<scripts>
  <postpartitioning-scripts config:type="list">
    <script>
      ...
    </script>
  </postpartitioning-scripts>
```

```
</scripts>
```

### 4.30.3 Chroot Environment Scripts

Chroot scripts are executed before the machine reboots for the first time. You can execute chroot scripts before the installation chroots into the installed system and configures the boot loader or you can execute a script after the chroot into the installed system has happened (look at the `chrooted` parameter for that).

Chroot Environment script elements must be placed as follows:

```
<scripts>
  <chroot-scripts config:type="list">
    <script>
      ...
    </script>
  </chroot-scripts>
</scripts>
```

### 4.30.4 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.

Post-install script elements must be placed as follows:

```
<scripts>
  <post-scripts config:type="list">
    <script>
      ...
    </script>
  </post-scripts>
</scripts>
```

### 4.30.5 Init Scripts

These scripts are executed when YaST has finished, during the initial boot process after the network has been initialized. These final scripts are executed using `/usr/lib/YaST2/bin/autoyast-initscripts.sh` and are executed only once. Init scripts are configured using the tag *init-scripts*.

Init scripts elements must be placed as follows:

```
<scripts>
  <init-scripts config:type="list">
    <script>
      ...
    </script>
  </init-scripts>
</scripts>
```

Init scripts are different from the rest of script types because they are not executed by YaST, but after YaST has finished. For this reason, their XML representation is different from other script types.

TABLE 4.1: INIT SCRIPT XML REPRESENTATION

Element	Description	Comment
<u>location</u>	Define a location from where the script gets fetched. Locations can be the same as for the profile (HTTP, FTP, NFS, etc.).  <pre>&lt;location&gt;http://10.10.0.1/myInitScript.sh&lt;/location&gt;</pre>	Either <location> or <source> must be defined.
<u>source</u>	The script itself (source code), encapsulated in a CDATA tag. If you do not want to put the whole shell script into the XML profile, use the location parameter.  <pre>&lt;source&gt; &lt;![CDATA[ echo "Testing the init script" &gt; /tmp/init_out.txt ]]&gt; &lt;/source&gt;</pre>	Either <location> or <source> must be defined.

Element	Description	Comment
<u>filename</u>	<p>The file name of the script. It will be stored in a temporary directory under <u>/tmp</u></p> <pre>&lt;filename&gt;myinitScript5.sh&lt;/filename&gt;</pre>	<p>Optional in case you only have a single init script. The default name (<u>init-scripts</u>) is used in this case. If having specified more than one init script, you must set a unique name for each script.</p>
<u>rerun</u>	<p>A script is only run once. Even if you use <code>ayast_setup</code> to run an XML file multiple times, the script is only run once. Change this default behavior by setting this boolean to <u>true</u>.</p> <pre>&lt;rerun   config:type="boolean"&gt;true&lt;/rerun&gt;</pre>	<p>Optional. Default is <u>false</u> (scripts only run once).</p>

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

### 4.30.6 Script XML Representation

Most of the XML elements described below can be used for all the script types described above, except for *init scripts*, whose definitions can contain only a subset of these elements. See [Section 4.30.5, “Init Scripts”](#) for further information about them.

TABLE 4.2: SCRIPT XML REPRESENTATION

Element	Description	Comment
<u>location</u>	<p>Define a location from where the script gets fetched. Locations can be the same as for the control file (HTTP, FTP, NFS, etc.).</p>	<p>Either <u>location</u> or <u>source</u> must be defined.</p>

Element	Description	Comment
	<pre>&lt;location&gt; http://10.10.0.1/myPreScript.sh&lt;/location&gt;</pre>	
<u>source</u>	<p>The script itself (source code), encapsulated in a CDATA tag. If you do not want to put the whole shell script into the XML control file, refer to the location parameter.</p> <pre>&lt;source&gt; &lt;![CDATA[ echo "Testing the pre script" &gt; /tmp/pre-script_out.txt ]]&gt; &lt;/source&gt;</pre>	Either <u>location</u> or <u>source</u> must be defined.
<u>interpreter</u>	<p>Specify the interpreter that must be used for the script. Supported options are <u>shell</u> and <u>perl</u>.</p> <pre>&lt;interpreter&gt;perl&lt;/interpreter&gt;</pre>	Optional (default is <u>shell</u> ).
<u>file name</u>	<p>The file name of the script. It will be stored in a temporary directory under <u>/tmp</u>.</p> <pre>&lt;filename&gt;myPreScript5.sh&lt;/filename&gt;</pre>	Optional. Default is the type of the script (pre-scripts in this case). If you have more than one script, you should define different names for each script.
<u>feedback</u>	<p>If this boolean is <u>true</u>, output and error messages of the script (STDOUT and STDERR) will be shown in a pop-up. The user needs to confirm them via the OK button.</p> <pre>&lt;feedback config:type="boolean"&gt;true&lt;/feedback&gt;</pre>	Optional, default is <u>false</u> .

Element	Description	Comment
<u>feed-back_type</u>	<p>This can be <u>message</u>, <u>warning</u> or <u>error</u>. Set the timeout for these pop-ups in the <code>&lt;report&gt;</code> section.</p> <pre>&lt;feedback_type&gt;warning&lt;/feedback_type&gt;</pre>	Optional, if missing, an always blocking pop-up is used.
<u>debug</u>	<p>If this is <u>true</u>, every single line of a shell script is logged. Perl scripts are run with warnings turned on.</p> <pre>&lt;debug config:type="boolean"&gt;true&lt;/debug&gt;</pre>	Optional, default is <u>true</u> .
<u>notification</u>	<p>This text will be shown in a pop-up for the time the script is running in the background.</p> <pre>&lt;notification&gt;Please wait while script is running...&lt;/notification&gt;</pre>	Optional, if not configured, no notification pop-up will be shown.
<u>param-list</u>	<p>It is possible to specify parameters given to the script being called. You may have more than one <code>param</code> entry. They are concatenated by a single space character on the script command line. If any shell quoting should be necessary (for example to protect embedded spaces) you need to include this.</p> <pre>&lt;param-list config:type="list"&gt;   &lt;param&gt;par1&lt;/param&gt;   &lt;param&gt;par2 par3&lt;/param&gt;   &lt;param&gt;"par4.1 par4.2"&lt;/param&gt; &lt;/param-list&gt;</pre>	Optional, if not configured, no parameters get passed to script.
<u>rerun</u>	<p>A script is only run once. Even if you use <code>ayast_setup</code> to run an XML file multiple times, the script is only run once. Change this default behavior by setting this boolean to <u>true</u>.</p>	Optional, default is <u>false</u> (scripts only run once).

Element	Description	Comment
	<pre>&lt;rerun config:type="boolean"&gt;true&lt;/rerun&gt;</pre>	
<u>chrooted</u>	<p>If set to <u>false</u>, the installed system remains mounted at <u>/mnt</u> and no chroot happens. The boot loader is not installed either at this stage. Setting it to <u>true</u> means, a chroot into <u>/mnt</u> is performed, where the installed system is mounted. The boot loader is installed, and if you want to change anything in the installed system, you do not need to use the <u>/mnt</u> prefix anymore.</p> <pre>&lt;chrooted config:type="boolean"&gt;true&lt;/chrooted&gt;</pre>	<p>Optional, default is <u>false</u>. This option is only available for chroot environment scripts.</p>

### 4.30.7 Script Example

EXAMPLE 4.52: SCRIPT CONFIGURATION

```
<?xml version="1.0"?>
<!DOCTYPE profile>
<profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/
configs">
<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"
systemctl start portmap
mount -a 192.168.1.1:/local /mnt
cp /mnt/test.sh /tmp
umount /mnt
]]>
    </source>
</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>
<postpartitioning-scripts config:type="list">
    <script>
        <filename>postpart.sh</filename>
        <interpreter>shell</interpreter>
        <debug config:type="boolean">false</debug>
        <feedback config:type="boolean">true</feedback>
        <source><![CDATA[
touch /mnt/testfile
echo Hi
]]>
        </source>
    </script>
</postpartitioning-scripts>
</scripts>
</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 the subdirectory `scripts` and the output logs in the `log` directory.

The log consists of the output produced when executing the shell scripts using the following command:

```
/bin/sh -x SCRIPT_NAME 2&>/var/adm/autoinstall/logs/SCRIPT_NAME.log
```

## 4.31 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.

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

### EXAMPLE 4.53: SYSCONFIG CONFIGURATION

```

<sysconfig config:type="list" >
  <sysconfig_entry>
    <sysconfig_key>XNTPD_INITIAL_NTPDATE</sysconfig_key>
    <sysconfig_path>/etc/sysconfig/xntp</sysconfig_path>
    <sysconfig_value>ntp.host.com</sysconfig_value>
  </sysconfig_entry>
</sysconfig>

```

```

</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.

## 4.32 Adding Complete Configurations

For many applications and services you may have a configuration file which should be copied to the appropriate location on the installed system. For example, if you are installing a Web server, you may have a 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. YaST will copy this file to the specified location.

This feature requires the `autoyast2` package to be installed. If the package is missing, AutoYaST will automatically install the package if it is missing.

You can specify the `file_location` where the file should be retrieved from. This can also be a location on the network such as an HTTP server: `<file_location>http://my.server.site/issue</file_location>`.

You can create directories by specifying a `file_path` that ends with a slash.

### EXAMPLE 4.54: DUMPING FILES INTO THE INSTALLED SYSTEM

```

<files config:type="list">
  <file>
    <file_path>/etc/apache2/httpd.conf</file_path>
    <file_contents>

<![CDATA[
some content
]]>

```

```

    </file_contents>
  </file>
  <file>
    <file_path>/mydir/a/b/c/</file_path> <!-- create directory -->
  </file>
</files>

```

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

#### EXAMPLE 4.55: DUMPING FILES INTO THE INSTALLED SYSTEM

```

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

    <![CDATA[
some content
]]>

    </file_contents>
    <file_owner>tux.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>
  </file>
</files>

```

## 4.33 Ask the User for Values during Installation

You have the option to let the user decide the values of specific parts of the control file during the installation. If you use this feature, a pop-up will ask the user to enter a specific part of the control file during installation. If you want a full auto installation, but the user should set the password of the local account, you can do this via the `ask` directive in the control file.

The elements listed below must be placed within the following XML structure:

```
<general>
  <ask-list config:type="list">
    <ask>
      ...
    </ask>
  </ask-list>
</general>
```

TABLE 4.3: ASK THE USER FOR VALUES: XML REPRESENTATION

Element	Description	Comment
<u>question</u>	The question you want to ask the user.  <code>&lt;question&gt;Enter the LDAP server&lt;/question&gt;</code>	The default value is the path to the element (the path often looks strange, so we recommend entering a question).
<u>default</u>	Set a preselection for the user. A text entry will be filled out with this value. A check box will be true or false and a selection will have the given value preselected.  <code>&lt;default&gt;dc=suse,dc=de&lt;/default&gt;</code>	Optional.
<u>help</u>	An optional help text that is shown on the left side of the question.	Optional.

Element	Description	Comment
	<pre>&lt;help&gt;Enter the LDAP server address.&lt;/help&gt;</pre>	
<u>title</u>	<p>An optional title that is shown above the questions.</p> <pre>&lt;title&gt;LDAP server&lt;/title&gt;</pre>	Optional.
<u>type</u>	<p>The type of the element you want to change. Possible values are <u>symbol</u>, <u>boolean</u>, <u>string</u> and <u>integer</u>. The file system in the partition section is a symbol, while the <u>encrypted</u> element in the user configuration is a boolean. You can see the type of that element if you look in your control file at the <u>config:type="..."</u> attribute. You can also use <u>static_text</u> as type. A <u>static_text</u> is a text that does not require any user input and can be used to show information not included in the help text.</p> <pre>&lt;type&gt;symbol&lt;/type&gt;</pre>	Optional. The default is <u>string</u> . If type is <u>symbol</u> , you must provide the selection element too (see below).
<u>password</u>	<p>If this boolean is set to <u>true</u>, a password dialog pops up instead of a simple text entry. Setting this to <u>true</u> only makes sense if <u>type</u> is <u>string</u>.</p>	Optional. The default is <u>false</u> .

Element	Description	Comment
	<pre>&lt;password   config:type="boolean"&gt;true&lt;/ password&gt;</pre>	
<u>pathlist</u>	<p>A list of <u>path</u> elements. A path is a comma separated list of elements that describes the path to the element you want to change. For example, the LDAP server element can be found in the control file in the <u>&lt;ldap&gt;&lt;ldap_server&gt;</u> section. So if you want to change that value, you need to set the path to <u>ldap, l- dap_server</u>.</p> <pre>&lt;pathlist   config:type="list"&gt;    &lt;path&gt;networking,dns,hostname&lt;/ path&gt;   &lt;path&gt;...&lt;/path&gt; &lt;/pathlist&gt;</pre> <p>To change the password of the first user in the control file, you need to set the path to <u>users, 0, user_pass- word</u>. The <u>0</u> indicates the first user in the <u>&lt;users con- fig:type="list"&gt;</u> list of users in the control file. <u>1</u> would be the second one, and so on.</p> <pre>&lt;users config:type="list"&gt;   &lt;user&gt;</pre>	<p>This information is optional but you should at least provide <u>path</u> or <u>file</u>.</p>

Element	Description	Comment
	<pre>         &lt;username&gt;root&lt;/ username&gt;         &lt;user_password&gt;password to change&lt;/user_password&gt;         &lt;encrypted config:type="boolean"&gt;&gt;false&lt;/ encrypted&gt;         &lt;/user&gt;         &lt;user&gt;         &lt;username&gt;tux&lt;/ username&gt;         &lt;user_password&gt;password to change&lt;/user_password&gt;         &lt;encrypted config:type="boolean"&gt;&gt;false&lt;/ encrypted&gt;         &lt;/user&gt; &lt;/users&gt; </pre>	
<u>file</u>	<p>You can store the answer to a question in a file, to use it in one of your scripts later. If you ask during <u>stage=initial</u> and you want to use the answer in stage 2, then you need to copy the answer-file in a chroot script that is running as <u>chroot-ed=false</u>. Use the command: <b><u>cp /tmp/my_answer /mnt/tmp/</u></b>. The reason is that <u>/tmp</u> in stage 1 is in the RAM disk and will be lost after the reboot, but the installed system is already mounted at <u>/mnt/</u>.</p> <pre> &lt;file&gt;/tmp/ answer_hostname&lt;/file&gt; </pre>	<p>This information is optional, but you should at least provide <u>path</u> or <u>file</u>.</p>



Element	Description	Comment
stage	<p>Stage configures the installation stage in which the question pops up. You can set this value to <code>cont</code> or <code>initial</code>. <code>initial</code> means the pop-up comes up very early in the installation, shortly after the pre-script has run. <code>cont</code> means, that the dialog with the question comes after the first reboot when the system boots for the very first time. Questions you answer during the <code>initial</code> stage will write their answer into the control file on the hard disk. You should know that if you enter clear text passwords during <code>initial</code>. Of course it does not make sense to ask for the file system to use during the <code>cont</code> phase. The hard disk is already partitioned at that stage and the question will have no effect.</p> <pre>&lt;stage&gt;cont&lt;/stage&gt;</pre>	Optional. The default is <code>initial</code> .
<u>selection</u>	The selection element contains a list of <code>entry</code> elements. Each entry represents a possible option for the user to choose. The user cannot	Optional for <code>type=string</code> , not possible for <code>type=boolean</code> and mandatory for <code>type=symbol</code> .

Element	Description	Comment
	<p>enter a value in a text box, but they can choose from a list of values.</p> <pre> &lt;selection   config:type="list"&gt;   &lt;entry&gt;     &lt;value&gt;       btrfs     &lt;/value&gt;     &lt;label&gt;       Btrfs File System     &lt;/label&gt;   &lt;/entry&gt;   &lt;entry&gt;     &lt;value&gt;       ext3     &lt;/value&gt;     &lt;label&gt;       Extended3 File       System     &lt;/label&gt;   &lt;/entry&gt; &lt;/selection&gt; </pre>	
<u>dialog</u>	<p>You can ask more than one question per dialog. To do so, specify the dialog-id with an integer. All questions with the same dialog-id belong to the same dialog. The dialogs are sorted by the id too.</p> <pre> &lt;dialog   config:type="integer"&gt;3&lt;/   dialog&gt; </pre>	Optional.
<u>element</u>	<p>you can have more than one question per dialog. To make that possible you need to</p>	Optional (see dialog).

Element	Description	Comment
	<p>specify the element-id with an integer. The questions in a dialog are sorted by id.</p> <pre>&lt;element   config:type="integer"&gt;1&lt;/element&gt;</pre>	
<u>width</u>	<p>You can increase the default width of the dialog. If there are multiple width specifications per dialog, the largest one is used. The number is roughly equivalent to the number of characters.</p> <pre>&lt;width   config:type="integer"&gt;50&lt;/width&gt;</pre>	Optional.
<u>height</u>	<p>You can increase default height of dialog. If there are multiple height specifications per dialog, largest one is used. The number is roughly equivalent to number of lines.</p> <pre>&lt;height   config:type="integer"&gt;15&lt;/height&gt;</pre>	Optional.
<u>frametitle</u>	<p>You can have more than one question per dialog. Each question on a dialog has a frame that can have a frame title, a small caption for each</p>	Optional. Default is no frame title.

Element	Description	Comment
	<p>question. You can put multiple elements into one frame. They need to have the same frame title.</p> <pre>&lt;frametitle&gt;User data&lt;/frametitle&gt;</pre>	
<u>script</u>	<p>You can run scripts after a question has been answered (see the table below for detailed instructions about scripts).</p> <pre>&lt;script&gt;...&lt;/script&gt;</pre>	Optional (default is no script).
<u>ok_label</u>	<p>You can change the label on the <i>Ok</i> button. The last element that specifies the label for a dialog wins.</p> <pre>&lt;ok_label&gt;Finish&lt;/ok_label&gt;</pre>	Optional.
<u>back_label</u>	<p>You can change the label on the <i>Back</i> button. The last element that specifies the label for a dialog wins.</p> <pre>&lt;back_label&gt;change values&lt;/back_label&gt;</pre>	Optional.
<u>timeout</u>	<p>You can specify an integer here that is used as timeout in seconds. If the user does not answer the question before the timeout, the default value is taken as an-</p>	Optional. A missing value is interpreted as <u>0</u> , which means that there is no timeout.

Element	Description	Comment
	<p>swer. When the user touches or changes any widget in the dialog, the timeout is turned off and the dialog needs to be confirmed via <i>Ok</i>.</p> <pre>&lt;timeout   config:type="integer"&gt;30&lt;/timeout&gt;</pre>	
<u>default_value_script</u>	<p>You can run scripts to set the default value for a question (see <a href="#">Section 4.33.1, “Default Value Scripts”</a> for detailed instructions about default value scripts). This feature is useful if you can <u>calculate</u> a default value, especially in combination with the <u>timeout</u> option.</p> <pre>&lt;default_value_script&gt;...&lt;/default_value_script&gt;</pre>	Optional. Default is no script.

### 4.33.1 Default Value Scripts

You can run scripts to set the default value for a question. This feature is useful if you can calculate a default value, especially in combination with the timeout option.

The elements listed below must be placed within the following XML structure:

```
<general>
  <ask-list config:type="list">
    <ask>
      <default_value_script>
        ...
      </default_value_script>
    </ask>
```

```
</ask-list>
</general>
```

TABLE 4.4: DEFAULT VALUE SCRIPTS: XML REPRESENTATION

Element	Description	Comment
<u>source</u>	<p>The source code of the script. Whatever you <b>echo</b> to STDOUT will be used as default value for the ask-dialog. If your script has an exit code other than 0, the normal default element is used. Take care you use <b>echo -n</b> to suppress the <code>\n</code> and that you echo reasonable values and not “okay” for a boolean</p> <pre>&lt;source&gt;...&lt;/source&gt;</pre>	This value is required, otherwise nothing would be executed.
<u>interpreter</u>	<p>The interpreter to use.</p> <pre>&lt;interpreter&gt;perl&lt;/interpreter&gt;</pre>	The default value is <code>shell</code> . You can also set <code>/bin/myinterpreter</code> as value.

### 4.33.2 Scripts

You can run scripts after a question has been answered.

The elements listed below must be placed within the following XML structure:

```
<general>
  <ask-list config:type="list">
    <ask>
      <script>
        ...
      </script>
    </ask>
  </ask-list>
</general>
```

TABLE 4.5: SCRIPTS: XML REPRESENTATION

Element	Description	Comment
<u>file name</u>	<p>The file name of the script.</p> <pre>&lt;filename&gt;my_ask_script.sh&lt;/filename&gt;</pre>	The default is ask_script.sh
<u>source</u>	<p>The source code of the script. Together with <u>re-run_on_error</u> activated, you check the value that was entered for sanity. Your script can create a file <code>/tmp/next_dialog</code> with a dialog id specifying the next dialog AutoYaST will raise. A value of -1 terminates the ask sequence. If that file is not created, AutoYaST will run the dialogs in the normal order (since 11.0 only).</p> <pre>&lt;source&gt;...&lt;/source&gt;</pre>	This value is required, otherwise nothing would be executed.
<u>environment</u>	<p>A boolean that passes the value of the answer to the question as an environment variable to the script. The variable is named <u>VAL</u>.</p> <pre>&lt;environment config:type="boolean"&gt;true&lt;/environment&gt;</pre>	Optional. Default is <u>false</u> .
<u>feedback</u>	<p>A boolean that turns on feedback for the script execution. STDOUT will be displayed in</p>	Optional, default is <u>false</u> .

Element	Description	Comment
	<p>a pop-up window that must be confirmed after the script execution.</p> <pre>&lt;feedback   config:type="boolean"&gt;true&lt;/feedback&gt;</pre>	
<u>debug</u>	<p>A boolean that turns on debugging for the script execution.</p> <pre>&lt;debug   config:type="boolean"&gt;true&lt;/debug&gt;</pre>	<p>Optional, default is <u>true</u>. This value needs <u>feedback</u> to be turned on, too.</p>
<u>rerun_on_error</u>	<p>A boolean that keeps the dialog open until the script has an exit code of 0 (zero). So you can parse and check the answers the user gave in the script and display an error with the <u>feedback</u> option.</p> <pre>&lt;rerun_on_error   config:type="boolean"&gt;true&lt;/rerun_on_error&gt;</pre>	<p>Optional, default is <u>false</u>. This value should be used together with the feedback option.</p>

Below you can see an example of the usage of the ask feature.

```
<general>
  <ask-list config:type="list">
    <ask>
      <pathlist config:type="list">
        <path>ldap,ldap_server</path>
      </pathlist>
      <stage>cont</stage>
      <help>Choose your server depending on your department</help>
      <selection config:type="list">
        <entry>
```



```

        <value>ldap1.mydom.de</value>
        <label>LDAP for development</label>
    </entry>
    <entry>
        <value>ldap2.mydom.de</value>
        <label>LDAP for sales</label>
    </entry>
</selection>
<default>ldap2.mydom.de</default>
<default_value_script>
    <source> <![CDATA[
echo -n "ldap1.mydom.de"
]]>
        </source>
    </default_value_script>
</ask>
<ask>
    <pathlist config:type="list">
        <path>networking,dns,hostname</path>
    </pathlist>
    <question>Enter Hostname</question>
    <stage>initial</stage>
    <default>enter your hostname here</default>
</ask>
<ask>
    <pathlist config:type="list">
        <path>partitioning,0,partitions,0,filesystem</path>
    </pathlist>
    <question>File System</question>
    <type>symbol</type>
    <selection config:type="list">
        <entry>
            <value config:type="symbol">ext4</value>
            <label>default File System (recommended)</label>
        </entry>
        <entry>
            <value config:type="symbol">ext3</value>
            <label>Fallback File System</label>
        </entry>
    </selection>
</ask>
</ask-list>
</general>

```

The following example shows a to choose between AutoYaST control files. AutoYaST will read the modified.xml file again after the ask-dialogs are done. This way you can fetch a complete new control file.

```

<general>
  <ask-list config:type="list">
    <ask>
      <selection config:type="list">
        <entry>
          <value>part1.xml</value>
          <label>Simple partitioning</label>
        </entry>
        <entry>
          <value>part2.xml</value>
          <label>encrypted /tmp</label>
        </entry>
        <entry>
          <value>part3.xml</value>
          <label>LVM</label>
        </entry>
      </selection>
      <title>XML Profile</title>
      <question>Choose a profile</question>
      <stage>initial</stage>
      <default>part1.xml</default>
      <script>
        <filename>fetch.sh</filename>
        <environment config:type="boolean">true</environment>
        <source>
<![CDATA[
wget http://10.10.0.162/$VAL -O /tmp/profile/modified.xml 2>/dev/null
]]>
          </source>
          <debug config:type="boolean">false</debug>
          <feedback config:type="boolean">false</feedback>
        </script>
      </ask>
    </ask-list>
  </general>

```

You can verify the answer of a question with a script like this:

```

<general>
  <ask-list config:type="list">
    <ask>
      <script>
        <filename>my.sh</filename>
        <rerun_on_error config:type="boolean">true</rerun_on_error>
        <environment config:type="boolean">true</environment>
        <source><![CDATA[
if [ "$VAL" = "myhost" ]; then

```

```

        echo "Illegal Hostname!";
        exit 1;
    fi
    exit 0
}]>
    </source>
    <debug config:type="boolean">false</debug>
    <feedback config:type="boolean">true</feedback>
</script>
<dialog config:type="integer">0</dialog>
<element config:type="integer">0</element>
<pathlist config:type="list">
    <path>networking,dns,hostname</path>
</pathlist>
<question>Enter Hostname</question>
<default>enter your hostname here</default>
</ask>
</ask-list>
</general>

```

## 4.34 Kernel Dumps



### Note: Availability

This feature is not available on the IBM Z (s390x) architecture.

With Kdump the system can create crashdump files if the whole kernel crashes. Crash dump files contain the memory contents while the system crashed. Such core files can be analyzed later by support or a (kernel) developer to find the reason for the system crash. Kdump is mostly useful for servers where you cannot easily reproduce such crashes but it is important to get the problem fixed.

There is a downside to this. Enabling Kdump requires between 64 MB and 128 MB of additional system RAM reserved for Kdump in case the system crashes and the dump needs to be generated. This section only describes how to set up Kdump with AutoYaST. It does not describe how Kdump works. For details, refer to the `kdump(7)` manual page.

The following example shows a general Kdump configuration.

#### EXAMPLE 4.56: KDUMP CONFIGURATION

```
<kdump>
```

```

<!-- memory reservation -->
<add_crash_kernel config:type="boolean">true</add_crash_kernel>
<crash_kernel>256M-:64M</crash_kernel>
<general>

    <!-- dump target settings -->
    <KDUMP_SAVEDIR>ftp://stravinsky.suse.de/incoming/dumps</KDUMP_SAVEDIR>
    <KDUMP_COPY_KERNEL>true</KDUMP_COPY_KERNEL>
    <KDUMP_FREE_DISK_SIZE>64</KDUMP_FREE_DISK_SIZE>
    <KDUMP_KEEP_OLD_DUMPS>5</KDUMP_KEEP_OLD_DUMPS>

    <!-- filtering and compression -->
    <KDUMP_DUMPFORMAT>compressed</KDUMP_DUMPFORMAT>
    <KDUMP_DUMPLEVEL>1</KDUMP_DUMPLEVEL>

    <!-- notification -->
    <KDUMP_NOTIFICATION_TO>tux@example.com</KDUMP_NOTIFICATION_TO>
    <KDUMP_NOTIFICATION_CC>spam@example.com devnull@example.com</KDUMP_NOTIFICATION_CC>
    <KDUMP_SMTP_SERVER>mail.example.com</KDUMP_SMTP_SERVER>
    <KDUMP_SMTP_USER></KDUMP_SMTP_USER>
    <KDUMP_SMTP_PASSWORD></KDUMP_SMTP_PASSWORD>

    <!-- kdump kernel -->
    <KDUMP_KERNELVER></KDUMP_KERNELVER>
    <KDUMP_COMMANDLINE></KDUMP_COMMANDLINE>
    <KDUMP_COMMANDLINE_APPEND></KDUMP_COMMANDLINE_APPEND>

    <!-- expert settings -->
    <KDUMP_IMMEDIATE_REBOOT>yes</KDUMP_IMMEDIATE_REBOOT>
    <KDUMP_VERBOSE>15</KDUMP_VERBOSE>
    <KEXEC_OPTIONS></KEXEC_OPTIONS>
</general>
</kdump>

```

### 4.34.1 Memory Reservation

The first step is to reserve memory for Kdump at boot-up. Because the memory must be reserved very early during the boot process, the configuration is done via a kernel command line parameter called `crashkernel`. The reserved memory will be used to load a second kernel which will be executed without rebooting if the first kernel crashes. This second kernel has a special `initrd`, which contains all programs necessary to save the dump over the network or to disk, send a notification e-mail, and finally reboot.

To reserve memory for Kdump, specify the `amount` (such as `64M` to reserve 64 MB of memory from the RAM) and the `offset`. The syntax is `crashkernel=AMOUNT@OFFSET`. The kernel can auto-detect the right offset (except for the Xen hypervisor, where you need to specify `16M` as offset). The amount of memory that needs to be reserved depends on architecture and main memory. Refer to *Book "System Analysis and Tuning Guide", Chapter 17 "Kexec and Kdump", Section 17.7.1 "Manual Kdump Configuration"* for recommendations on the amount of memory to reserve for Kdump.

You can also use the extended command line syntax to specify the amount of reserved memory depending on the System RAM. That is useful if you share one AutoYaST control file for multiple installations or if you often remove or install memory on one machine. The syntax is:

```
BEGIN_RANGE_1-END_RANGE_1:AMOUNT_1,BEGIN_RANGE_2-END_RANGE_2:AMOUNT_2@OFFSET
```

`BEGIN_RANGE_1` is the start of the first memory range (for example: `0M`) and `END_RANGE_1` is the end of the first memory range (can be empty in case `infinity` should be assumed) and so on. For example, `256M-2G:64M,2G-:128M` reserves 64 MB of crashkernel memory if the system has between 256 MB and 2 GB RAM and reserves 128 MB of crashkernel memory if the system has more than 2 GB RAM.

On the other hand, it is possible to specify multiple values for the `crashkernel` parameter. For example, when you need to reserve different segments of low and high memory, use values like `72M,low` and `256M,high`:

#### EXAMPLE 4.57: KDUMP MEMORY RESERVATION WITH MULTIPLE VALUES

```
<kdump>
  <!-- memory reservation (high and low) -->
  <add_crash_kernel config:type="boolean">true</add_crash_kernel>
  <crash_kernel config:type="list">
    <listentry>72M,low</listentry>
    <listentry>256M,high</listentry>
  </crash_kernel>
</kdump>
```

The following list shows the settings necessary to reserve memory:

TABLE 4.6: KDUMP MEMORY RESERVATION SETTINGS:XML REPRESENTATION

Element	Description	Comment
<code>add_crash_kernel</code>	Set to <code>true</code> if memory should be reserved and Kdump enabled.	required

Element	Description	Comment
	<pre>&lt;add_crash_kernel   config:type="boolean"&gt;true&lt;/ add_crash_kernel&gt;</pre>	
<u>crash_kernel</u>	<p>Use the syntax of the crashkernel command line as discussed above.</p> <pre>&lt;crash_kernel&gt;256M:64M&lt;/ crash_kernel&gt;</pre> <p>A list of values is also supported.</p> <pre>&lt;crash_kernel   config:type="list"&gt;   &lt;listentry&gt;72M,low&lt;/ listentry&gt;   &lt;listentry&gt;256M,high&lt;/ listentry&gt; &lt;/crash_kernel&gt;</pre>	required

## 4.34.2 Dump Saving

### 4.34.2.1 Target

The element KDUMP\_SAVEDIR specifies the URL to where the dump is saved. The following methods are possible:

- file to save to the local disk,
- ftp to save to an FTP server (without encryption),
- sftp to save to an SSH2 SFTP server,
- nfs to save to an NFS location and
- cifs to save the dump to a CIFS/SMP export from Samba or Microsoft Windows.

For details see the `kdump(5)` manual page. Two examples are: `file:///var/crash` (which is the default location according to FHS) and `ftp://user:password@host:port/incoming/dumps`. A subdirectory, with the time stamp contained in the name, will be created and the dumps saved there.

When the dump is saved to the local disk, `KDUMP_KEEP_OLD_DUMPS` can be used to delete old dumps automatically. Set it to the number of old dumps that should be kept. If the target partition would end up with less free disk space than specified in `KDUMP_FREE_DISK_SIZE`, the dump is not saved.

To save the whole kernel and the debug information (if installed) to the same directory, set `KDUMP_COPY_KERNEL` to `true`. You will have everything you need to analyze the dump in one directory (except kernel modules and their debugging information).

#### 4.34.2.2 Filtering and Compression

The kernel dump is uncompressed and unfiltered. It can get as large as your system RAM. To get smaller files, compress the dump file afterward. The dump needs to be decompressed before opening.

To use page compression, which compresses every page and allows dynamic decompression with the `crash(8)` debugging tool, set `KDUMP_DUMPFORMAT` to `compressed` (default).

You may not want to save all memory pages, for example those filled with zeroes. To filter the dump, set the `KDUMP_DUMPLEVEL`. 0 produces a full dump and 31 is the smallest dump. The manual pages `kdump(5)` and `makedumpfile(8)` list for each value which pages will be saved.

#### 4.34.2.3 Summary

TABLE 4.7: DUMP TARGET SETTINGS: XML REPRESENTATION

Element	Description	Comment
<code>KDUMP_SAVEDIR</code>	A URL that specifies the target to which the dump and related files will be saved.  <pre>&lt;KDUMP_SAVEDIR&gt;file:///var/crash/&lt;/KDUMP_SAVEDIR&gt;</pre>	required

Element	Description	Comment
<u>KDUMP_COPY_KERNEL</u>	<p>Set to <code>true</code>, if not only the dump should be saved to <u>KDUMP_SAVEDIR</u> but also the kernel and its debugging information (if installed).</p> <pre>&lt;KDUMP_COPY_KERNEL&gt;false&lt;/KDUMP_COPY_KERNEL&gt;</pre>	optional
<u>KDUMP_FREE_DISK_SIZE</u>	<p>Disk space in megabytes that must remain free after saving the dump. If not enough space is available, the dump will not be saved.</p> <pre>&lt;KDUMP_FREE_DISK_SIZE&gt;64&lt;/KDUMP_FREE_DISK_SIZE&gt;</pre>	optional
<u>KDUMP_KEEP_OLD_DUMPS</u>	<p>The number of dumps that are kept (not deleted) if <u>KDUMP_SAVEDIR</u> points to a local directory. Specify 0 if you do not want any dumps to be automatically deleted, specify -1 if all dumps except the current one should be deleted.</p> <pre>&lt;KDUMP_KEEP_OLD_DUMPS&gt;4&lt;/KDUMP_KEEP_OLD_DUMPS&gt;</pre>	optional

### 4.34.3 E-Mail Notification

Configure e-mail notification if you want to be informed when a machine crashes and a dump is saved.



Because Kdump runs in the initrd, a local mail server cannot send the notification e-mail. An SMTP server needs to be specified (see below).

You need to provide exactly one address in `KDUMP_NOTIFICATION_TO`. More addresses can be specified in `KDUMP_NOTIFICATION_CC`. Only use e-mail addresses in both cases, not a real name. Specify `KDUMP_SMTP_SERVER` and (if the server needs authentication) `KDUMP_SMTP_USER` and `KDUMP_SMTP_PASSWORD`. Support for TLS/SSL is not available but may be added in the future.

TABLE 4.8: E-MAIL NOTIFICATION SETTINGS: XML REPRESENTATION

Element	Description	Comment
<code>KDUMP_NOTIFICATION_TO</code>	Exactly one e-mail address to which the e-mail should be sent. Additional recipients can be specified in <code>KDUMP_NOTIFICATION_CC</code> .  <pre>&lt;KDUMP_NOTIFICATION_TO &gt;tux@example.com&lt;/ KDUMP_NOTIFICATION_TO&gt;</pre>	optional (notification disabled if empty)
<code>KDUMP_NOTIFICATION_CC</code>	Zero, one or more recipients that are in the cc line of the notification e-mail.  <pre>&lt;KDUMP_NOTIFICATION_CC &gt;wilber@example.com suzanne@example.com&lt;/ KDUMP_NOTIFICATION_CC&gt;</pre>	optional
<code>KDUMP_SMTP_SERVER</code>	Host name of the SMTP server used for mail delivery. SMTP authentication is supported (see <code>KDUMP_SMTP_USER</code> and <code>KDUMP_SMTP_PASSWORD</code> ) but TLS/SSL are not.  <pre>&lt;KDUMP_SMTP_SERVER&gt;email.suse.de&lt;/ KDUMP_SMTP_SERVER&gt;</pre>	optional (notification disabled if empty)

Element	Description	Comment
<u>KDUMP_SMTP_USER</u>	User name used together with <u>KDUMP_SMTP_PASSWORD</u> for SMTP authentication.  <pre>&lt;KDUMP_SMTP_USER&gt;bwalke&lt;/KDUMP_SMTP_USER&gt;</pre>	optional
<u>KDUMP_SMTP_PASSWORD</u>	Password used together with <u>KDUMP_SMTP_USER</u> for SMTP authentication.  <pre>&lt;KDUMP_SMTP_PASSWORD&gt;geheim&lt;/KDUMP_SMTP_PASSWORD&gt;</pre>	optional

#### 4.34.4 Kdump Kernel Settings

As already mentioned, a special kernel is booted to save the dump. If you do not want to use the auto-detection mechanism to find out which kernel is used (see the `kdump(5)` manual page that describes the algorithm which is used to find the kernel), you can specify the version of a custom kernel in KDUMP\_KERNELVER. If you set it to `foo`, then the kernel located in `/boot/vmlinuz-foo` or `/boot/vmlinux-foo` (in that order on platforms that have a `vmlinuz` file) will be used.

You can specify the command line used to boot the Kdump kernel. Normally the boot command line is used, minus settings that are not relevant for Kdump (like the `crashkernel` parameter) plus some settings needed by Kdump (see the manual page `kdump(5)`). To specify additional parameters, use KDUMP\_COMMANDLINE\_APPEND. If you know what you are doing and you want to specify the entire command line, set KDUMP\_COMMANDLINE.

TABLE 4.9: KERNEL SETTINGS: XML REPRESENTATION

Element	Description	Comment
<u>KDUMP_KERNELVER</u>	Version string for the kernel used for Kdump. Leave it empty to use the auto-detection mechanism (strongly recommended).  <pre>&lt;KDUMP_KERNELVER&gt;2.6.27-default&lt;/KDUMP_KERNELVER&gt;</pre>	optional (auto-detection if empty)
<u>KDUMP_COMMANDLINE_APPEND</u>	Additional command line parameters for the Kdump kernel.  <pre>&lt;KDUMP_COMMANDLINE_APPEND&gt;console=ttyS0,57600&lt;/KDUMP_COMMANDLINE_APPEND&gt;</pre>	optional
<u>KDUMP_Command Line</u>	Overwrite the automatically generated Kdump command line. Use with care. Usually, <u>KDUMP_COMMANDLINE_APPEND</u> should suffice.  <pre>&lt;KDUMP_COMMANDLINE_APPEND&gt;root=/dev/sda5 maxcpus=1 irqpoll&lt;/KDUMP_COMMANDLINE&gt;</pre>	optional

## 4.34.5 Expert Settings

TABLE 4.10: EXPERT SETTINGS: XML REPRESENTATIONS

Element	Description	Comment
<u>KDUMP_IMMEDIATE_REBOOT</u>	<p><u>true</u> if the system should be rebooted automatically after the dump has been saved, <u>false</u> otherwise. The default is to reboot the system automatically.</p> <pre>&lt;KDUMP_IMMEDIATE_REBOOT&gt;true&lt;/KDUMP_IMMEDIATE_REBOOT&gt;</pre>	optional
<u>KDUMP_VERBOSE</u>	<p>Bitmask that specifies how verbose the Kdump process should be. Read kdump(5) for details.</p> <pre>&lt;KDUMP_VERBOSE&gt;3&lt;/KDUMP_VERBOSE&gt;</pre>	optional
<u>KEXEC_OPTIONS</u>	<p>Additional options that are passed to kexec when loading the Kdump kernel. Normally empty.</p> <pre>&lt;KEXEC_OPTIONS&gt;--noio&lt;/KEXEC_OPTIONS&gt;</pre>	optional

## 4.35 DNS Server

The Bind DNS server can be configured by adding a dns-server resource. The three more straightforward properties of that resource can have a value of 1 to enable them or 0 to disable.

Attribute	Value	Description
<u>chroot</u>	0 / 1	The DNS server must be jailed in a chroot.
<u>start_service</u>	0 / 1	Bind is enabled (executed on system start).
<u>use_ldap</u>	0 / 1	Store the settings in LDAP instead of native configuration files.

EXAMPLE 4.58: BASIC DNS SERVER SETTINGS

```
<dns-server>
  <chroot>0</chroot>
  <start_service>1</start_service>
  <use_ldap>0</use_ldap>
</dns-server>
```

In addition to those basic settings, there are three properties of type list that can be used to fine-tune the service configuration.

List	Description
<u>logging</u>	Options of the DNS server logging.
<u>options</u>	Bind options like the files and directories to use, the list of forwarders and other configuration settings.
<u>zones</u>	List of DNS zones known by the server, including all the settings, records and SOA records.

EXAMPLE 4.59: CONFIGURING DNS SERVER ZONES AND ADVANCED SETTINGS

```
<dns-server>
  <logging config:type="list">
    <listentry>
      <key>channel</key>
      <value>log_syslog { syslog; }</value>
    </listentry>
  </logging>
</dns-server>
```

```

</logging>
<options config:type="list">
  <option>
    <key>forwarders</key>
    <value>{ 10.10.0.1; }</value>
  </option>
</options>
<zones config:type="list">
  <listentry>
    <is_new>1</is_new>
    <modified>1</modified>
    <options config:type="list"/>
    <records config:type="list">
      <listentry>
        <key>mydom.uwe.</key>
        <type>MX</type>
        <value>0 mail.mydom.uwe.</value>
      </listentry>
      <listentry>
        <key>mydom.uwe.</key>
        <type>NS</type>
        <value>ns.mydom.uwe.</value>
      </listentry>
    </records>
    <soa>
      <expiry>1w</expiry>
      <mail>root.aaa.aaa.cc.</mail>
      <minimum>1d</minimum>
      <refresh>3h</refresh>
      <retry>1h</retry>
      <serial>2005082300</serial>
      <server>aaa.aaa.cc.</server>
      <zone>@</zone>
    </soa>
    <soa_modified>1</soa_modified>
    <ttl>2d</ttl>
    <type>master</type>
    <update_actions config:type="list">
      <listentry>
        <key>mydom.uwe.</key>
        <operation>add</operation>
        <type>NS</type>
        <value>ns.mydom.uwe.</value>
      </listentry>
    </update_actions>
    <zone>mydom.uwe</zone>
  </listentry>

```

```
</zones>
</dns-server>
```

## 4.36 DHCP Server

The `dhcp-server` resource makes it possible to configure all the settings of a DHCP server by means of the six following properties.

Element	Value	Description
<u>chroot</u>	0 / 1	A value of 1 means that the DHCP server must be jailed in a chroot.
<u>start_service</u>	0 / 1	Set this to 1 to enable the DHCP server (that is, run it on system startup).
<u>use_ldap</u>	0 / 1	If set to 1, the settings will be stored in LDAP instead of native configuration files.
<u>other_options</u>	Text	String with parameters that will be passed to the DHCP server executable when started. For example, use "-p 1234" to listen on a non-standard 1234 port. For all possible options, consult the <code>dhcpcd</code> manual page. If left blank, default values will be used.

Element	Value	Description
<u>allowed_interfaces</u>	List	List of network cards in which the DHCP server will be operating. See the example below for the exact format.
<u>settings</u>	List	List of settings to configure the behavior of the DHCP server. The configuration is defined in a tree-like structure where the root represents the global options, with subnets and host nested from there. The <u>children</u> , <u>parent_id</u> and <u>parent_type</u> properties are used to represent that nesting. See the example below for the exact format.

EXAMPLE 4.60: EXAMPLE DHCP-SERVER SECTION

```

<dhcp-server>
  <allowed_interfaces config:type="list">
    <allowed_interface>eth0</allowed_interface>
  </allowed_interfaces>
  <chroot>0</chroot>
  <other_options>-p 9000</other_options>
  <start_service>1</start_service>
  <use_ldap>0</use_ldap>

  <settings config:type="list">
    <settings_entry>
      <children config:type="list"/>
      <directives config:type="list">
        <listentry>
          <key>fixed-address</key>
          <type>directive</type>
          <value>192.168.0.10</value>
        </listentry>
      </directives>
    </settings_entry>
  </settings>
</dhcp-server>

```



```

    <listentry>
      <key>hardware</key>
      <type>directive</type>
      <value>ethernet d4:00:00:bf:00:00</value>
    </listentry>
  </directives>
  <id>static10</id>
  <options config:type="list"/>
  <parent_id>192.168.0.0 netmask 255.255.255.0</parent_id>
  <parent_type>subnet</parent_type>
  <type>host</type>
</settings_entry>
<settings_entry>
  <children config:type="list">
    <child>
      <id>static10</id>
      <type>host</type>
    </child>
  </children>
  <directives config:type="list">
    <listentry>
      <key>range</key>
      <type>directive</type>
      <value>dynamic-bootp 192.168.0.100 192.168.0.150</value>
    </listentry>
    <listentry>
      <key>default-lease-time</key>
      <type>directive</type>
      <value>14400</value>
    </listentry>
    <listentry>
      <key>max-lease-time</key>
      <type>directive</type>
      <value>86400</value>
    </listentry>
  </directives>
  <id>192.168.0.0 netmask 255.255.255.0</id>
  <options config:type="list"/>
  <parent_id/>
  <parent_type/>
  <type>subnet</type>
</settings_entry>
<settings_entry>
  <children config:type="list">
    <child>
      <id>192.168.0.0 netmask 255.255.255.0</id>
      <type>subnet</type>
    </child>
  </children>

```

```

    </child>
  </children>
  <directives config:type="list">
    <listentry>
      <key>ddns-update-style</key>
      <type>directive</type>
      <value>none</value>
    </listentry>
    <listentry>
      <key>default-lease-time</key>
      <type>directive</type>
      <value>14400</value>
    </listentry>
  </directives>
</id>
<options config:type="list"/>
</parent_id>
</parent_type>
</type>
</settings_entry>
</settings>
</dhcp-server>

```

## 4.37 Firewall Configuration

SuSEfirewall2 has been replaced by `firewalld` starting with SLES 15. Profiles using SuSEfirewall2 properties will be translated to `firewalld` profiles. However, not all profile properties can be converted. For details about `firewalld` refer to *Book "Security and Hardening Guide", Chapter 23 "Masquerading and Firewalls", Section 23.4 "firewalld"*.



### Important: Limited Backward Compatibility with SuSEFirewall2 Based Profiles

The use of SuSEFirewall2 based profiles will be only partially supported as many options are not valid in `firewalld` and some missing configuration could affect your network security.

### 4.37.1 General Firewall Configuration

In `firewalld` the general configuration only exposes a few properties and most of the configuration is done by zones.

Attribute	Value	Description
<code>start_firewall</code>	Boolean	Whether <code>firewalld</code> should be started right after applying the configuration.
<code>enable_firewall</code>	Boolean	Whether <code>firewalld</code> should be started on every system startup.
<code>default_zone</code>	Zone name	The default zone is used for everything that is not explicitly assigned.
<code>log_denied_packets</code>	Type of dropped packages to be logged	Enable logging of dropped packages for the type selected. Values: <code>off</code> , <code>unicast</code> , <code>multicast</code> , <code>broadcast</code> , <code>all</code> .

### 4.37.2 Firewall Zones Configuration

The configuration of `firewalld` is based on the existence of several zones which define the trust level for a connection, interface or source address. The behavior of each zone can be tweaked in several ways although not all the properties are exposed yet.

Attributes	Value	Description
<code>interfaces</code>	List of interface names	List of interface names assigned to this zone. Interfaces or sources can only be part of one zone.

Attributes	Value	Description
<u>services</u>	List of services	List of services accessible in this zone.
<u>ports</u>	List of ports	List of single ports or ranges to be opened in the assigned zone.
<u>protocols</u>	List of protocols	List of protocols to be opened or be accessible in the assigned zone.
<u>masquerade</u>	Enable masquerade	It will enable or disable network address translation (NAT) in the assigned zone.

### 4.37.3 A Full Example

A full example of the firewall section, including general and zone specific properties could look like this.

#### EXAMPLE 4.61: EXAMPLE FIREWALL SECTION

```
<firewall>
  <enable_firewall config:type="boolean">true</enable_firewall>
  <log_denied_packets>all</log_denied_packets>
  <default_zone>external</default_zone>
  <zones config:type="list">
    <zone>
      <name>public</name>
      <interfaces config:type="list">
        <interface>eth0</interface>
      </interfaces>
      <services config:type="list">
        <service>ssh</service>
        <service>dhcp</service>
        <service>dhcpv6</service>
        <service>samba</service>
        <service>vnc-server</service>
      </services>
    </zone>
  </zones>
</firewall>
```

```
<ports config:type="list">
  <port>21/udp</port>
  <port>22/udp</port>
  <port>80/tcp</port>
  <port>443/tcp</port>
  <port>8080/tcp</port>
</ports>
</zone>
<zone>
  <name>dmz</name>
  <interfaces config:type="list">
    <interface>eth1</interface>
  </interfaces>
</zone>
</zones>
</firewall>
```

## 4.38 Miscellaneous Hardware and System Components

In addition to the core component configuration, like network authentication and security, AutoYaST offers a wide range of hardware and system configuration options, the same as 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 YaST.

Any new configuration options added to YaST will be automatically available in AutoYaST.

### 4.38.1 Printer

AutoYaST support for printing is limited to basic settings defining how CUPS is used on a client for printing via the network.

There is no AutoYaST support for setting up local print queues. Modern printers are usually connected via USB. CUPS accesses USB printers by a model-specific device URI like `usb://ACME/FunPrinter?serial=1a2b3c`. Usually it is not possible to predict the correct USB device URI in advance, because it is determined by the CUPS back-end `usb` during runtime. Therefore it is not possible to set up local print queues with AutoYaST.

Basics on how CUPS is used on a client workstation to print via network:

On client workstations application programs submit print jobs to the CUPS daemon process (`cupsd`). `cupsd` forwards the print jobs to a CUPS print server in the network where the print jobs are processed. The server sends the printer specific data to the printer device.

If there is only a single CUPS print server in the network, there is no need to have a CUPS daemon running on each client workstation. Instead it is simpler to specify the CUPS server in `/etc/cups/client.conf` and access it directly (only one CUPS server entry can be set). In this case application programs that run on client workstations submit print jobs directly to the specified CUPS print server.

*Example 4.62, "Printer configuration"* shows a `printer` configuration section. The `cupsd_conf_content` entry contains the whole verbatim content of the `cupsd` configuration file `/etc/cups/cupsd.conf`. The `client_conf_content` entry contains the whole verbatim content of `/etc/cups/client.conf`. The `printer` section contains the `cupsd` configuration but it does not specify whether the `cupsd` should run.

#### EXAMPLE 4.62: PRINTER CONFIGURATION

```
<printer>
  <client_conf_content>
    <file_contents><![CDATA[
... verbatim content of /etc/cups/client.conf ...
]]></file_contents>
  </client_conf_content>
  <cupsd_conf_content>
    <file_contents><![CDATA[
... verbatim content of /etc/cups/cupsd.conf ...
]]></file_contents>
  </cupsd_conf_content>
</printer>
```



#### Note: `/etc/cups/cups-files.conf`

With release 1.6 the CUPS configuration file has been split into two files: `cupsd.conf` and `cups-files.conf`. As of SUSE Linux Enterprise Server 15, AutoYaST only supports modifying `cupsd.conf` since the default settings in `cups-files.conf` are sufficient for usual printing setups.

## 4.38.2 Sound devices

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

EXAMPLE 4.63: SOUND CONFIGURATION

```
<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>
```

## 4.39 Importing SSH Keys and Configuration

YaST allows to import SSH keys and server configuration from previous installations. The behavior of this feature can also be controlled through an AutoYaST profile.

EXAMPLE 4.64: IMPORTING SSH KEYS AND CONFIGURATION FROM /DEV/SDA2

```
<ssh_import>
  <import config:type="boolean">true</import>
  <copy_config config:type="boolean">true</copy_config>
  <device>/dev/sda2</device>
</ssh_import>
```

Attributes	Value	Description
<u>import</u>	true / false	SSH keys will be imported. If set to <u>false</u> , nothing will be imported.
<u>copy_config</u>	true / false	Additionally, SSH server configuration will be imported. This setting will not have effect if <u>import</u> is set to <u>false</u> .
<u>device</u>	Partition	Partition to import keys and configuration from. If it is not set, the partition which contains the most recently accessed key is used.

## 4.40 Configuration Management

AutoYaST allows delegating part of the configuration to a configuration management tool like Salt:

- AutoYaST takes care of system installation (partitioning, network setup, etc.)
- System configuration can be delegated to a configuration management tool

This module configures the connection to a configuration management tool and uploads SSH keys which are needed for establishing connections. At the end of the installation, the configuration management Master will be contacted to retrieve state files and other resources.

### EXAMPLE 4.65: CONFIGURING SALT MANAGER

```
<configuration_management>
  <type>salt</type>
  <master>linux-addc</master>
  <auth_attempts config:type="integer">5</auth_attempts>
  <auth_time_out config:type="integer">10</auth_time_out>
  <keys_url>http://keys.example.de/keys</keys_url>
```



</configuration\_management>

Attributes	Value	Description
<u>type</u>	Configuration management type	Configuration management name. Currently only <u>salt</u> is supported.
<u>master</u>	Host name	Host name or IP address of the configuration management master.
<u>auth_attempts</u>	Integer	At the end of installation, YaST connects to the configuration management master with maximum <u>auth_attempts</u> attempts. The default is three attempts.
<u>auth_time_out</u>	Integer	Time between the configuration management master connection attempts. The default is 15 seconds.
<u>keys_url</u>	URL of used key	Path to an HTTP server, hard disk, USB drive or similar with the files <u>default.key</u> and <u>default.pub</u> . This key has to be known to the configuration management master.
<u>enable_services</u>	True/false	Enables the configuration management services on the client side. Default is <u>true</u> .

# III Managing Mass Installations with Rules and Classes

5 Rules and Classes **186**

## 5 Rules and Classes

Rules and classes allow customizing installations for sets of machines in different ways:

- Rules allow configuring a system depending on its attributes.
- Classes represent configurations for groups of target systems. Classes can be assigned to systems.



### Note: Use autoyast Boot Option Only

Rules and classes are only supported by the boot parameter `autoyast=URL`.

`autoyast2=URL` is not supported, because this option downloads a single AutoYaST control file only.

### 5.1 Rule-based Automatic Installation

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

For example, this could be useful to install systems in two departments in one go. Assume a scenario where machines in department A need to be installed as office desktops, whereas machines in department B need to be installed as developer workstations. You would create a rules file with two different rules. For each rule, you could use different system parameters to distinguish the installations from one another. Each rule would also contain a link to an appropriate profile for each department.

The rules file is an XML file containing 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, each group of systems is linked to a control file. Both the rules file and the control files must be located in a pre-defined and accessible location. The rules file is retrieved only if no specific control file is supplied using the `autoyast` keyword. For example, if the following is used, the rules file will not be evaluated:

```
autoyast=http://10.10.0.1/profile/myprofile.xml
autoyast=http://10.10.0.1/profile/rules/rules.xml
```

Instead use:

```
autoyast=http://10.10.0.1/profile/
```

which will load `http://10.10.0.1/profile/rules/rules.xml` (the slash at the end of the directory name is important).

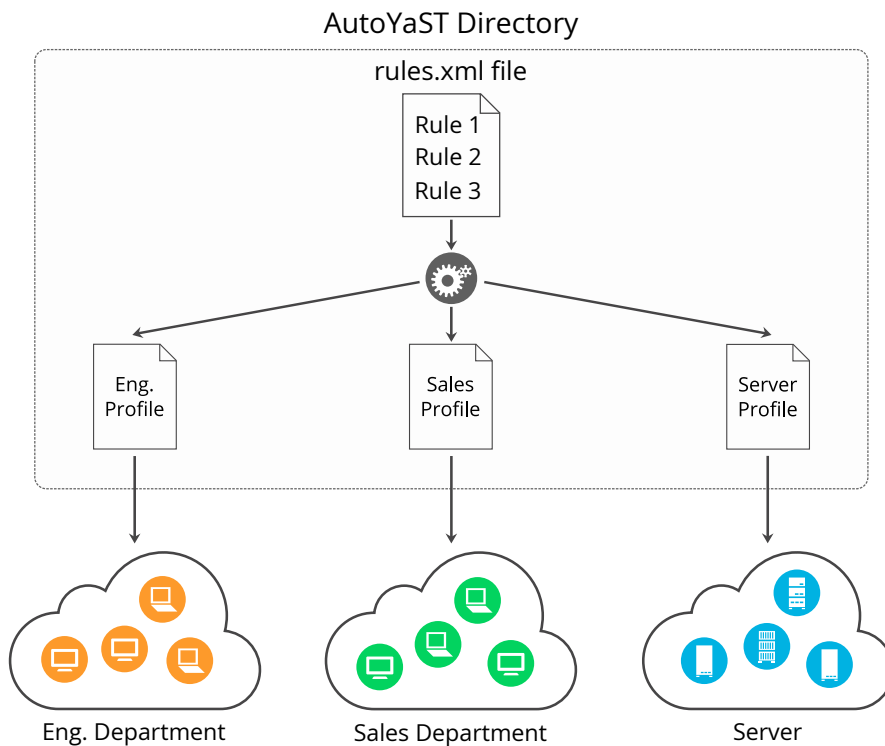


FIGURE 5.1: RULES

If more than one rule applies, the final control file 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. Note that the names of the top sections in the merged XML files need to be in alphabetical order for the merge to succeed.

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

### 5.1.1 Rules File Explained

#### EXAMPLE 5.1: 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>
<autoinstall xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://
www.suse.com/1.0/configns">
  <rules config:type="list">
    <rule>
      <disksize>
        <match>/dev/sdc 1000</match>
        <match_type>greater</match_type>
      </disksize>
      <result>
        <profile>department_a.xml</profile>
        <continue config:type="boolean">>false</continue>
      </result>
    </rule>
    <rule>
      <disksize>
        <match>/dev/sda 1000</match>
        <match_type>greater</match_type>
      </disksize>
      <result>
        <profile>department_b.xml</profile>
        <continue config:type="boolean">>false</continue>
      </result>
    </rule>
  </rules>
</autoinstall>

```

The last example defines two rules and provides a different control file for every rule. The rule used in this case is disksize. After parsing the rules file, YaST attempts to match the target system with the rules in the rules.xml file. A rule match occurs when the target system matches all system attributes defined in the rule. When the system matches a rule, the respective resource is added to the stack of control files AutoYaST will use to create the final control file. The continue property tells AutoYaST whether it should continue with other rules after a match has been found.

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

Using the disksize attribute, you can provide different configurations for systems with hard disks of different sizes. The first rule checks if the device /dev/sdc 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, such as memory or architectures, you can add more attributes in the rule resource as shown in the next example.

#### EXAMPLE 5.2: SIMPLE RULES FILE

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

```
<?xml version="1.0"?>
<!DOCTYPE autoinstall>
<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/sdc 1000</match>
        <match_type>greater</match_type>
      </disksize>
      <memsize>
        <match>1000</match>
        <match_type>greater</match_type>
      </memsize>
      <result>
        <profile>department_a.xml</profile>
        <continue config:type="boolean">>false</continue>
      </result>
    </rule>
    <rule>
      <disksize>
        <match>/dev/shda 1000</match>
        <match_type>greater</match_type>
      </disksize>
      <memsize>
        <match>256</match>
        <match_type>greater</match_type>
      </memsize>
      <result>
        <profile>department_b.xml</profile>
        <continue config:type="boolean">>false</continue>
      </result>
    </rule>
  </rules>
</autoinstall>
```

The rules directory must be located in the same directory specified via the `autoyast` keyword at boot time. If the client was booted using `autoyast=http://10.10.0.1/profiles/`, AutoYaST will search for the rules file at `http://10.10.0.1/profiles/rules/rules.xml`.

### 5.1.2 Custom Rules

If the attributes AutoYaST provides for rules are not enough for your purposes, use custom rules. Custom rules contain a shell script. The output of the script (STDOUT, STDERR is ignored) can be evaluated.

Here is an example for the use of custom rules:

```
<rule>
  <custom1>
    <script>
if grep -i intel /proc/cpuinfo > /dev/null; then
echo -n "intel"
else
echo -n "non_intel"
fi;
    </script>
    <match>*</match>
    <match_type>exact</match_type>
  </custom1>
  <result>
    <profile>@custom1.xml</profile>
    <continue config:type="boolean">true</continue>
  </result>
</rule>
```

The script in this rule can echo either intel or non\_intel to STDOUT (the output of the grep command must be directed to /dev/null in this case). The output of the rule script will be filled between the two '@' characters, to determine the file name of the control file to fetch. AutoYaST will read the output and fetch a file with the name intel.xml or non\_intel.xml. This file can contain the AutoYaST profile part for the software selection; for example, in case you want a different software selection on Intel hardware than on others.

The number of custom rules is limited to five. So you can use custom1 to custom5.

### 5.1.3 Match Types for Rules

You can use five different match\_types:

- exact (default)
- greater
- lower

- range
- regex (a simple == operator like in Bash)

If using exact, the string must match exactly as specified. regex can be used to match substrings like ntel will match Intel, intel and intelligent. greater and lower can be used for memsize or totaldisk for example. They can match only with rules that return an integer value. A range is only possible for integer values too and has the form of value1-value2, for example 512-1024.

### 5.1.4 Combine Attributes

Multiple attributes can be combined via a logical operator. It is possible to let a rule match if disksize is greater than 1GB or memsize is exactly 512MB.

You can do this with the operator element in the rules.xml file. and and or are possible operators, and being the default. Here is an example:

```
<rule>
  <disksize>
    <match>/dev/sda 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>
  <operator>or</operator>
</rule>
```

### 5.1.5 Rules File Structure

The rules.xml file needs to:

- have at least one rule,
- have the name rules.xml,



- be located in the directory `rules` in the profile repository,
- have at least one attribute to match in the rule.

## 5.1.6 Predefined System Attributes

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

If you are unsure about a value on your system, run `/usr/lib/YaST2/bin/y2base ayast_probe ncurses`. The text box displaying the detected values can be scrolled. Note that this command will not work while another YaST process that requires a lock (for example the installer) is running. Therefore you cannot run it during the installation.

TABLE 5.1: SYSTEM ATTRIBUTES

Attribute	Values	Description
<code>hostaddress</code>	IP address of the host	This attribute must always match exactly.
<code>host name</code>	The name of the host	This attribute must always match exactly.
<code>domain</code>	Domain name of host	This attribute must always match exactly.
<code>installed_product</code>	The name of the product to be installed.	This attribute must always match exactly.
<code>installed_product_version</code>	The version of the product to be installed.	This attribute must always match exactly.
<code>network</code>	network address of host	This attribute must always match exactly.
<code>mac</code>	MAC address of host	This attribute must always match exactly (the MAC addresses should have the form <code>0080c8f6484c</code> ).

Attribute	Values	Description
<u>linux</u>	Number of installed Linux partitions on the system	This attribute can be 0 or more.
<u>others</u>	Number of installed non-Linux partitions on the system	This attribute can be 0 or more.
<u>xserver</u>	X Server needed for graphic adapter	This attribute must always match exactly.
<u>memsize</u>	Memory available on host in megabytes	All match types are available.
<u>totaldisk</u>	Total disk space available on host in megabytes	All match types are available.
<u>hostid</u>	Hex representation of the IP address	Exact match required
<u>arch</u>	Architecture of host	Exact match required
<u>karch</u>	Kernel Architecture of host (for example SMP kernel, Xen kernel)	Exact match required
<u>disksize</u>	Drive device and size	All match types are available.
<u>product</u>	The hardware product name as specified in SMBIOS	Exact match required
<u>product_vendor</u>	The hardware vendor as specified in SMBIOS	Exact match required
<u>board</u>	The system board name as specified in SMBIOS	Exact match required
<u>board_vendor</u>	The system board vendor as specified in SMBIOS	Exact match required

Attribute	Values	Description
<u>custom1-5</u>	Custom rules using shell scripts	All match types are available.

### 5.1.7 Rules with Dialogs

You can use dialog pop-ups with check boxes to select rules you want matched.

The elements listed below must be placed within the following XML structure in the rules.xml file:

```
<rules config:type="list">
  <rule>
    <dialog>
      ...
    </dialog>
  </rule>
</rules>
```

Attribute	Values	Description
<u>dialog_nr</u>	<p>All rules with the same <u>dialog_nr</u> are presented in the same pop-up dialog. The same <u>dialog_nr</u> can appear in multiple rules.</p> <pre>&lt;dialog_nr   config:type="integer"&gt;3&lt;/dialog_nr&gt;</pre>	This element is optional and the default for a missing <u>dialog_nr</u> is always <u>0</u> . To use one pop-up for all rules, you do not need to specify the <u>dialog_nr</u> .
<u>element</u>	Specify a unique ID. Even if you have more than one dialog, you must not use the same id twice. Using id <u>1</u> on dialog 1 and id <u>1</u> on dialog 2 is not supported. (This behavior is contrary to the <u>ask</u>	Optional. If left out, AutoYaST adds its own ids internally. Then you cannot specify conflicting rules (see below).

Attribute	Values	Description
	<p>dialog, where you can have the same ID for multiple dialogs.)</p> <pre>&lt;element   config:type="integer"&gt;3&lt;/element&gt;</pre>	
<u>title</u>	<p>Caption of the pop-up dialog</p> <pre>&lt;title&gt;Desktop Selection&lt;/title&gt;</pre>	Optional
<u>question</u>	<p>Question shown in the pop-up behind the check box.</p> <pre>&lt;question&gt;GNOME Desktop&lt;/question&gt;</pre>	Optional. If you do not configure a text here, the name of the XML file that is triggered by this rule will be shown instead.
<u>timeout</u>	<p>Timeout in seconds after which the dialog will automatically “press” the okay button. Useful for a non-blocking installation in combination with rules dialogs.</p> <pre>&lt;timeout   config:type="integer"&gt;30&lt;/timeout&gt;</pre>	Optional. A missing timeout will stop the installation process until the dialog is confirmed by the user.
<u>conflicts</u>	<p>A list of element ids (rules) that conflict with this rule. If this rule matches or is selected by the user, all conflicting rules are deselected and disabled in the pop-up. Take care that you do not create deadlocks.</p>	<u>optional</u>

Attribute	Values	Description
	<pre> &lt;conflicts   config:type="list"&gt;     &lt;element       config:type="integer"&gt;1&lt;/ element&gt;     &lt;element       config:type="integer"&gt;5&lt;/ element&gt;     ... &lt;/conflicts&gt; </pre>	

Here is an example of how to use dialogs with rules:

```

<rules config:type="list">
  <rule>
    <custom1>
      <script>
echo -n 100
      </script>
      <match>100</match>
      <match_type>exact</match_type>
    </custom1>
    <result>
      <profile>rules/gnome.xml</profile>
      <continue config:type="boolean">true</continue>
    </result>
    <dialog>
      <element config:type="integer">0</element>
      <question>GNOME Desktop</question>
      <title>Desktop Selection</title>
      <conflicts config:type="list">
        <element config:type="integer">1</element>
      </conflicts>
      <dialog_nr config:type="integer">0</dialog_nr>
    </dialog>
  </rule>
  <rule>
    <custom1>
      <script>
echo -n 100
      </script>
      <match>101</match>
      <match_type>exact</match_type>
    </custom1>

```

```

    <result>
      <profile>rules/gnome.xml</profile>
      <continue config:type="boolean">true</continue>
    </result>
    <dialog>
      <element config:type="integer">1</element>
      <dialog_nr config:type="integer">0</dialog_nr>
      <question>Gnome Desktop</question>
      <conflicts config:type="list">
        <element config:type="integer">0</element>
      </conflicts>
    </dialog>
  </rule>
  <rule>
    <custom1>
      <script>
echo -n 100
      </script>
      <match>100</match>
      <match_type>exact</match_type>
    </custom1>
    <result>
      <profile>rules/all_the_rest.xml</profile>
      <continue config:type="boolean">>false</continue>
    </result>
  </rule>
</rules>

```

## 5.2 Classes

Classes represent configurations for groups of target systems. Unlike rules, classes need to be configured in the control file. Then classes can be assigned to target systems.

Here is an example of a class definition:

```

<classes config:type="list">
  <class>
    <class_name>TrainingRoom</class_name>
    <configuration>Software.xml</configuration>
  </class>
</classes>

```

In the example above, the file Software.xml must be placed in the subdirectory classes/TrainingRoom/. It will be fetched from the same place the AutoYaST control file and rules were fetched from.

If you have multiple control files and those control files share parts, better use classes for common parts. You can also use XIncludes.

Using the configuration management system, you can define a set of classes. A class definition consists of the following variables:

- Name: class name
- Description:
- Order: order (or priority) of the class in the stack of migration

Class Name	Order	Configurations
Department	1	0
Group	2	0
Site	3	0

Department Settings

New Edit Delete

Help Back Finish

FIGURE 5.2: 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. For example, the following sets of classes can be used:

- site: classes describing a physical location or site,
- machine: classes describing a type of machine,
- role: classes describing the function of the machine,
- 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 computer with a specific network interface, you only need the control file resource that controls the configuration of the network. 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.

## 5.3 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 which contain class definitions in them. The process is described in the figure *Figure A.1, "Rules Retrieval Process"*.

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

## 5.4 Merging of Rules and Classes

With classes and with rules, multiple XML files get merged into one resulting XML file. This merging process is often confusing for people, because it behaves different than one would expect. First of all, it is important to note that the names of the top sections in the merged XML files must be in alphabetical order for the merge to succeed.

For example, the following two XML parts should be merged:

```
<partitioning config:type="list">
  <drive>
    <partitions config:type="list">
      <partition>
        <filesystem config:type="symbol">swap</filesystem>
        <format config:type="boolean">true</format>
        <mount>swap</mount>
        <partition_id config:type="integer">130</partition_id>
        <size>2000mb</size>
      </partition>
      <partition>
        <filesystem config:type="symbol">xfs</filesystem>
        <partition_type>primary</partition_type>
        <size>4Gb</size>
      </partition>
    </partitions>
  </drive>
</partitioning>
```



```

    <mount>/data</mount>
  </partition>
</partitions>
</drive>
</partitioning>

```

```

<partitioning config:type="list">
  <drive>
    <initialize config:type="boolean">>false</initialize>
    <partitions config:type="list">
      <partition>
        <format config:type="boolean">>true</format>
        <filesystem config:type="symbol">xfs</filesystem>
        <mount>/</mount>
        <partition_id config:type="integer">131</partition_id>
        <partition_type>primary</partition_type>
        <size>max</size>
      </partition>
    </partitions>
    <use>all</use>
  </drive>
</partitioning>

```

You might expect the control file to contain three partitions. This is not the case. You will end up with two partitions and the first partition is a mix up of the swap and the root partition. Settings configured in both partitions, like mount or size, will be used from the second file. Settings that only exist in the first or second partition, will be copied to the merged partition too.

In this example, you do not want a second drive. The two drives should be merged into one. With regard to partitions, three separate ones should be defined. Using the dont\_merge method solves the merging problem:

```

<classes config:type="list">
  <class>
    <class_name>swap</class_name>
    <configuration>largeswap.xml</configuration>
    <dont_merge config:type="list">
      <element>partition</element>
    </dont_merge>
  </class>
</classes>

```

```

<rule>
  <board_vendor>
    <match>intel</match>
    <match_type>regex</match_type>

```

```

</board_vendor>
<result>
  <profile>classes/largeswap.xml</profile>
  <continue config:type="boolean">true</continue>
  <dont_merge config:type="list">
    <element>partition</element>
  </dont_merge>
</result>
<board_vendor>
  <match>PowerEdge [12]850</match>
  <match_type>regex</match_type>
</board_vendor>
<result>
  <profile>classes/smallswap.xml</profile>
  <continue config:type="boolean">true</continue>
  <dont_merge config:type="list">
    <element>partition</element>
  </dont_merge>
</result>
</rule>

```

## IV Understanding the Auto-Installation Process

6	The Auto-Installation Process	203
---	-------------------------------	-----

## 6 The Auto-Installation Process

### 6.1 Introduction

After the system has booted into an automatic installation and the control file has been retrieved, YaST configures the system according to the information provided in the control file. All configuration settings are summarized in a window that is shown by default and should be deactivated if a fully automatic installation is needed.

By the time YaST displays the summary of the configuration, YaST has only probed hardware and prepared the system for auto-installation. Nothing has been changed in the system yet. In case of any error, you can still abort the process.

A system should be automatically installable without the need to have any graphic adapter or monitor. Having a monitor attached to the client machine is nevertheless recommended so you can supervise the process and to get feedback in case of errors. Choose between the graphical and the text-based Ncurses interfaces. For headless clients, system messages can be monitored using the serial console.

#### 6.1.1 X11 Interface (graphical)

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

#### 6.1.2 Serial Console

Start installing a system using the serial console by adding the keyword `console` (for example `console=ttyS0`) to the command line of the kernel. This starts **linuxrc** in console mode and later YaST in serial console mode.

#### 6.1.3 Text-based YaST Installation

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

Starting YaST in the text mode is recommended when installing a client with less than 64 MB or when X11 should not be configured, especially on headless machines.

## 6.2 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 or TFTP. Alternatively a suitable kernel and initrd image can be loaded from a flash disk or a bootable DVD-ROM.

YaST will check for `autoinst.xml` in the root directory of the boot medium or the initrd upon start-up and switch to an automated installation if it was found. In case the control file is named differently or located elsewhere, specify its location on the kernel command line with the parameter `AutoYaST=URL`.

Alternatively, you can place the `autoinst.xml` to a device, mounted either physically or virtually, that is labeled `OEMDRV`. In this case, you do not need to specify the location of the `autoinst.xml` on the kernel command line. The `autoinst.xml` must be located in the root directory of the device.

### 6.2.1 Booting from a Flash Disk

For testing/rescue purposes or because the NIC does not have a PROM or PXE you can build a bootable flash disk to use with AutoYaST. Flash disks can also store the control file.



#### Tip: Creating a Bootable Flash Disk

To create a bootable flash disk, copy either the SUSE Linux Enterprise Server ISO image of DVD1 or the Mini CD ISO image to the disk using the `dd` command (the flash disk must not be mounted, all data on the device will be erased):

```
> sudo dd if=PATH_TO_ISO_IMAGE of=USB_STORAGE_DEVICE bs=4M
```

### 6.2.2 Booting from DVD-ROM

You can use the original SUSE Linux Enterprise Server DVD-ROM number one in combination with other media. For example, the control file can be provided via a flash disk or a specified location on the network. Alternatively, create a customized DVD-ROM that includes the control file.

### 6.2.3 Booting via PXE over the Network

Booting via PXE requires a DHCP and a TFTP server in your network. The computer will then boot without a physical medium. For instructions on setting up the required infrastructure, see *Book "Deployment Guide", Chapter 11 "Remote Installation"*.

If you install via PXE, the installation will run in an endless loop. This happens because after the first reboot, the machine performs the PXE boot again and restarts the installation instead of booting from the hard disk for the second stage of the installation.

There are several ways to solve this problem. You can use an HTTP server to provide the AutoYaST control file. Alternatively, instead of a static control file, run a CGI script on the Web server that provides the control file and changes the TFTP server configuration for your target host. This way, the next PXE boot of the machine will be from the hard disk by default.

Another way is to use AutoYaST to upload a new PXE boot configuration for the target host via the control file:

```
<pxe>
  <pxe_localboot config:type="boolean">true</pxe_localboot>
  <pxelinux-config>
    DEFAULT linux
    LABEL linux
    localboot 0
  </pxelinux-config>
  <tftp-server>192.168.1.115</tftp-server>
  <pxelinux-dir>/pxelinux.cfg</pxelinux-dir>
  <filename>__MAC__</filename>
</pxe>
```

This entry will upload a new configuration for the target host to the TFTP server shortly before the first reboot happens. In most installations the TFTP daemon runs as user `nobody`. You need to make sure this user has write permissions to the `pxelinux.cfg` directory. You can also configure the file name that will be uploaded. If you use the “magic” `__MAC__` file name, the file name will be the MAC address of your machine like, for example `01-08-00-27-79-49-ee`. If the file name setting is missing, the IP address will be used for the file name.

To do another auto-installation on the same machine, you need to remove the file from the TFTP server.

## 6.3 Invoking the Auto-Installation Process

### 6.3.1 Command Line Options

Adding the command line variable `autoyast` causes `linuxrc` to start in automated mode. The `linuxrc` program 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;
- in the root directory of the boot medium.

The `linuxrc` configuration file supports multiple keywords. For a detailed description of how `linuxrc` works and other keywords, see [Appendix C, Advanced linuxrc Options](#). Some of the more common ones are:

#### `autoupgrade`

Initiate an automatic upgrade using AutoYaST; see [Section 4.10, “Upgrade”](#).

#### `autoyast`

Location of the control file for automatic installation; see [AutoYaST Control File Locations](#) for details.

#### `ifcfg`

Configure and start the network. Required if the AutoYaST is to be fetched from a remote location. See [Section C.3, “Advanced Network Setup”](#) for details.

#### `insmod`

Kernel modules to load

#### `install`

Location of the installation directory, for example `install=nfs://192.168.2.1/CDs/`.



#### Note: Disabling SSL checks

When you are using HTTPS, SSL checking is enabled by default. If necessary, you can disable SSL checking by appending `ssl_verify=no` to your HTTPS URL, like the following examples:

```
install=https://192.168.2.1/CDs/?ssl_verify=no
```

If you are passing multiple query options, separate them with ampersands:

```
install=https://192.168.2.1/CDs/?foo=bar&ssl_verify=no
```

See the "FTP/HTTP/HTTPS directory tree" section of **man 8 zypper** for more information.

**instmode**

Installation mode, for example nfs, http etc. (not needed if install is set).

**rootpassword**

Password for root user if not specified in AutoYaST profile

**server**

Server (NFS) to contact for source directory

**serverdir**

Directory on NFS Server

**y2confirm**

Even with `<confirm>no</confirm>` in the control file, the confirm proposal comes up.

These variables and keywords will bring the system up to the point where YaST 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) has the function of giving the client enough information about the installation server and the location of the sources. Usually, this file is not required, but it is needed in special network environments where DHCP and BOOTP are not used or when special kernel modules need to be loaded.

You can pass keywords to **linuxrc** using the kernel command line. This can be done in several ways. You can specify **linuxrc** keywords along with other kernel parameters interactively at boot time, in the usual way. You can also insert kernel parameters into custom network-bootable disk images. It is also possible to configure a DHCP server to pass kernel parameters in combination with Etherboot or PXE.

The command line variable autoyast can be used in the format described in the following list.



### Format of URIs

The `autoyast` syntax for the URIs for your control file locations can be confusing. The format is `SCHEMA://HOST/PATH-TO-FILE`. The number of forward slashes to use varies. For remote locations of your control file, the URI looks like this example for an NFS server, with two slashes: `autoyast=nfs://SERVER/PATH`.

It is different when your control file is on a local filesystem. For example, `autoyast=usb:///profile.xml` is the same as `autoyast=usb://localhost/profile.xml`. You may omit the local host name, but you must keep the third slash. `autoyast=usb://profile.xml` will fail because `profile.xml` is interpreted as the host name.

### When no control file specification is needed

For upgrades, no `autoyast` variable is needed for an automated offline upgrade.

For new installations, `autoyast` will be started if a file named `autoinst.xml` is in one of the following three locations:

1. The root directory of the installation flash disk (e.g. USB stick)
2. The root directory of the installation medium
3. Or the root directory of the initial RAM disk used to boot the system

`autoyast=file:///PATH`

Looks for control file in the specified path, relative to the source root directory, for example `file:///autoinst.xml` when the control file is in the top-level directory of any local filesystem, including mounted external devices such as a CD or USB drive. (This is the same as `file://localhost/autoinst.xml`.)

`autoyast=device://DEVICE/FILENAME`

Looks for the control file on a storage device. Do not specify the full path to the device, but the device name only (e.g. `device://vda1/autoyast.xml`). You may also omit specifying the device and trigger `autoyast` to search all devices, for example. `autoyast=device://localhost/autoinst.xml`, or `autoyast=device:///autoinst.xml`.

`autoyast=nfs://SERVER/PATH`

Looks for the control file on an NFS server.

`autoyast=http://[user:password@]SERVER/PATH`

Retrieves the control file from a Web server using the HTTP protocol. Specifying a user name and a password is optional.

autoyast=https://[user:password@]SERVER/PATH

Retrieves the control file from a Web server using HTTPS. Specifying a user name and a password is optional.

autoyast=tftp://SERVER/PATH

Retrieve the control file via TFTP.

autoyast=ftp://[user:password@]SERVER/PATH

Retrieve the control file via FTP. Specifying a user name and a password is optional.

autoyast=usb:///PATH

Retrieve the control file from USB devices (autoyast will search all connected USB devices).

autoyast=relurl://PATH

Retrieve the control file from the installation source. Either from the default installation source or from the installation source defined in install=INSTALLATION\_SOURCE\_PATH.

autoyast=cifs://SERVER/PATH

Looks for the control file on a CIFS server.

autoyast=label://LABEL/PATH

Searches for a control file on a device with the specified label.

Several scenarios for auto-installation are possible using different types of infrastructure and source media. The simplest way is to use the source media (DVD number one) of SUSE Linux Enterprise Server. But to initiate the auto-installation process, the auto-installation command-line variable should be entered at system boot-up and the control file should be accessible for YaST. In a scripting context, you can use a serial console for your virtual machine, that allows you to work in text mode. Then you can pass the needed parameters from an expect script or equivalent. The following list of scenarios explains how the control file can be supplied:

#### Using the Original SUSE Linux Enterprise Server DVD-ROM

When using the original DVD-ROM (DVD #1 is needed), the control file needs to be accessible via flash disk or network:

**Flash Disk.** Access the control file via the autoyast=usb:///PATH option.

**Network.** Access the control file via the following commands: autoyast=nfs://..., autoyast=ftp://..., autoyast=http://..., autoyast=https://..., autoyast=tftp://..., or autoyast=cifs://...

## Using a Custom DVD-ROM

In this case, you can include the control file directly on the DVD-ROM. When placing it in the root directory and naming it `autoinst.xml`, it will automatically be found and used for the installation. Otherwise use `autoyast=file:///PATH` to specify the path to the control file.

When using a DVD-ROM for auto-installation, it is necessary to instruct the installer to use the DVD-ROM for installation instead of trying to find the installation files on the network. This can be done by adding the `instmode=cd` option to the kernel command line (this can be automated by adding the option to the `isolinux.cfg` file on the DVD).

## Using a Network Installation Source

This option is the most important one because installations of multiple machines are usually done using SLP or NFS servers and other network services like BOOTP and DHCP. The easiest way to make the control file available is to place it in the root directory of the installation source, naming it `autoinst.xml`. In this case, it will automatically be found and used for the installation. The control file can also reside in the following places:

**Flash Disk.** Access the control file via the `autoyast=usb:///PATH` option.

**Network.** Access the control file via the following commands: `autoyast=nfs://..`, `autoyast=ftp://..`, `autoyast=http://..`, `autoyast=https://..`, `autoyast=tftp://..`, or `autoyast=cifs://...`



### Note: Disabling Network and DHCP

To disable the network during installations where it is not needed or unavailable, for example when auto-installing from DVD-ROMs, use the `linuxrc` option `netsetup=0` to disable the network setup.



## Note: Difference between the `autoyast` and `autoyast2` Options

The options `autoyast` and `autoyast2` are very similar but differ in one important point:

- When you use `autoyast=http://...`, you need to provide `linuxrc` with the network configuration.
- When you use `autoyast2=http://...`, `linuxrc` tries to configure the network for you.

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

1. the root directory of the flash 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, YaST 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 uppercase hexadecimal, for example 192.0.2.91 -> C000025B.
2. If this file is not found, YaST will remove one hex digit and try again. This action is repeated until the file with the correct name is found. Ultimately, it will try looking for a file with the MAC address of the client as the file name (mac should have the following syntax: 0080C8F6484C ) and if not found a file named default (in lowercase).

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

```
C000025B
C000025
C00002
C0000
C000
C000
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/bin/gethostip available with the syslinux package.

#### EXAMPLE 6.1: DETERMINE HEX CODE FOR AN IP ADDRESS

```
> /usr/bin/gethostip 10.10.0.1
10.10.0.1 10.10.0.1 0A0A0001
```

## 6.3.2 Auto-installing a Single System

The easiest way to auto-install a system without any network connection is to use the original SUSE Linux Enterprise Server DVD-ROMs and a flash disk. You do not need to set up an installation server nor the network environment.

Create the control file and name it autoinst.xml. Copy the file autoinst.xml to the flash disk.

### 6.3.3 Combining the **linuxrc** info File with the AutoYaST Control File

If you choose to pass information to **linuxrc** using the `info` file or as boot options, you may integrate the keywords into the AutoYaST control file. Add an `info_file` section as shown in the example below. This section contains keyword—value pairs, separated by colons, one pair per line.

The **linuxrc** program will look for the string `start_linuxrc_conf` in the AutoYaST control file, which represents the beginning of the embedded **linuxrc** control file. If the string is found, **linuxrc** 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 6.2: **linuxrc** OPTIONS IN THE AUTOYAST CONTROL FILE

```
....
  <install>
....
  <init>
    <info_file>
install: nfs://192.168.1.1/CDs/full-x86_64
dud: https://example.com/driver_updates/filename.dud
upgrade: 1
textmode: 1
    </info_file>
  </init>
.....
</install>
....
```

Note that the `autoyast` keyword must point to the same file. If it is on a flash disk, then the option `usb:///` needs to be used. If the `info` file is stored in the initial RAM disk, the `file://` option needs to be used.

## 6.4 System Configuration

The system configuration during auto-installation is the most important part of the whole process. 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.

### 6.4.1 Post-Install and System Configuration

The post-installation and system configuration are initiated directly after the last package is installed on the target system and continue after the system has booted for the first time.

Before the system is booted for the first time, AutoYaST writes all data collected during installation and writes the boot loader in the specified location. In addition to these regular tasks, AutoYaST executes the chroot-scripts as specified in the control file. Note that these scripts are executed while the system is not yet 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. Use the reboot property of the general resource (see [Section 4.1, “General Options”](#)).

### 6.4.2 System Customization

Most of the system customization is done in the second stage of the installation. If you require customization that cannot be done using AutoYaST resources, use post-install scripts for further modifications.

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.

## V Uses for AutoYaST on Installed Systems

- 7 Running AutoYaST in an Installed System **216**



## 7 Running AutoYaST in an Installed System

In some cases it is useful to run AutoYaST in a running system.

In the following example, an additional software package ( `foo` ) is going to be installed. To run this software, a user needs to be added and an NTP client needs to be configured.

The respective AutoYaST profile needs to include a section for the package installation ([Section 4.9.7, “Installing Packages in Stage 2”](#)), a user ([Section 4.29.1, “Users”](#)) section and an NTP-client ([Section 4.20, “NTP Client”](#)) section:

```
<?xml version="1.0"?>
<!DOCTYPE profile>
<profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/
configns">
  <ntp-client>
    <peers config:type="list">
      <peer>
        <address>us.pool.ntp.org</address>
        <comment/>
        <options> iburst</options>
        <type>server</type>
      </peer>
    </peers>
    <start_at_boot config:type="boolean">true</start_at_boot>
    <start_in_chroot config:type="boolean">false</start_in_chroot>
    <sync_interval config:type="integer">5</sync_interval>
    <synchronize_time config:type="boolean">false</synchronize_time>
  </ntp-client>
  <software>
    <post-packages config:type="list">
      <package>ntp</package>
      <package>yast2-ntp-client</package>
      <package>foo</package>
    </post-packages>
  </software>
  <users config:type="list">
    <user>
      <encrypted config:type="boolean">false</encrypted>
      <fullname>Foo user</fullname>
      <gid>100</gid>
      <home>/home/foo</home>
      <password_settings>
        <expire/>
        <flag/>
        <inact/>
      </password_settings>
    </user>
  </users>
</profile>
```

```
<max>99999</max>
<min>0</min>
<warn>7</warn>
</password_settings>
<shell>/bin/bash</shell>
<uid>1001</uid>
<user_password>linux</user_password>
<username>foo</username>
</user>
</users>
</profile>
```

Store this file as /tmp/install\_foo.xml and start the AutoYaST installation process by calling:

```
> sudo yast2 ayast_setup setup filename=/tmp/install_foo.xml dopackages="yes"
```

For more information, run **yast2 ayast\_setup longhelp**

## VI Appendices

- A Handling Rules 219
- B AutoYaST FAQ—Frequently Asked Questions 220
- C Advanced **linuxrc** Options 224
- D Differences Between AutoYaST Profiles in SLE 12 and 15 229

## A Handling Rules

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

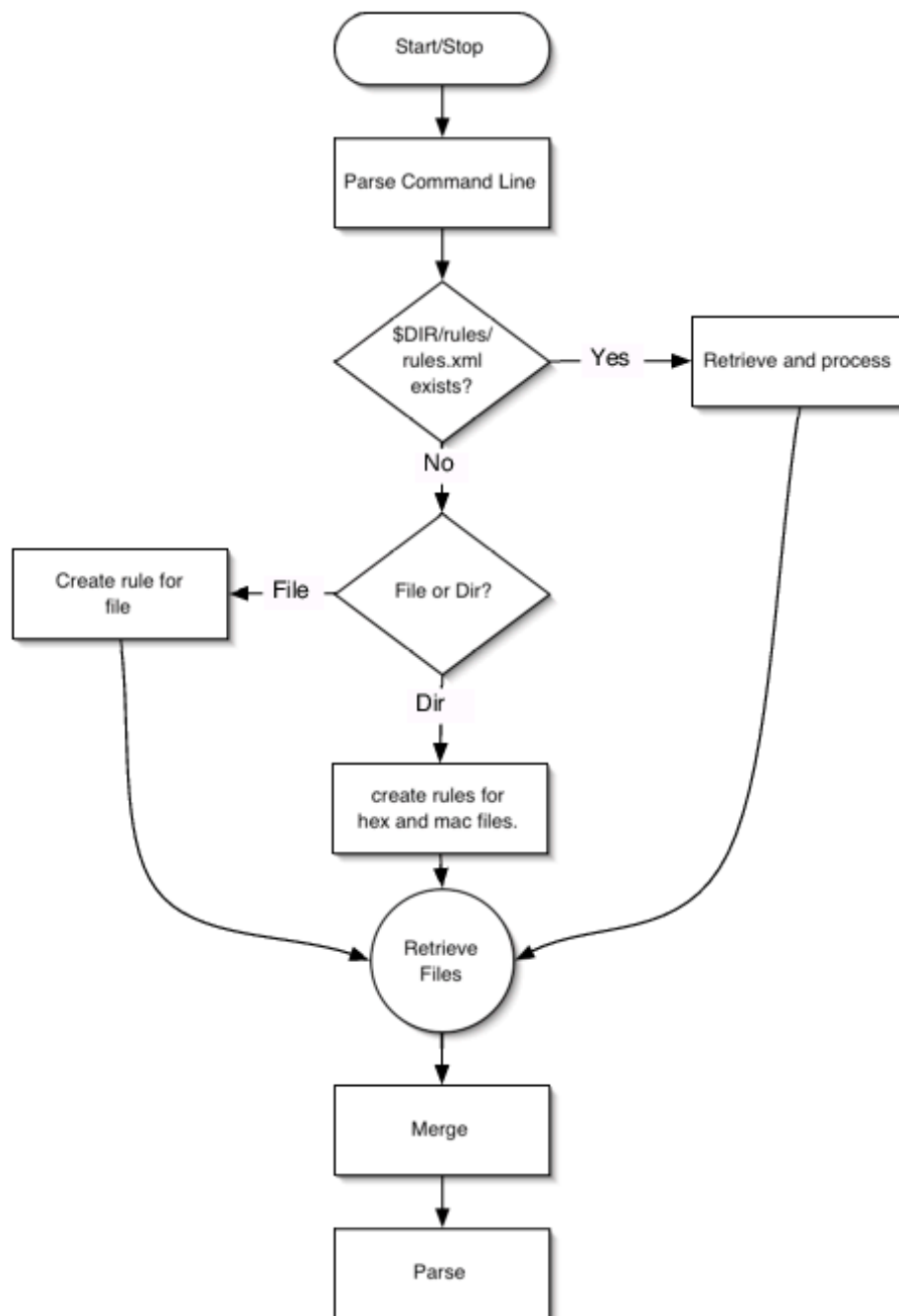


FIGURE A.1: RULES RETRIEVAL PROCESS

## B AutoYaST FAQ—Frequently Asked Questions

### 1. *How do I invoke an AutoYaST installation?*

On all SUSE Linux Enterprise Server versions, the automatic installation gets invoked by adding `autoyast=<PATH_TO_PROFILE>` to the kernel parameter list. So for example adding `autoyast=http://MYSERVER/MYCONFIG.xml` will start an automatic installation where the profile with the AutoYaST configuration gets fetched from the Web server `myserver`. See [Section 6.3, “Invoking the Auto-Installation Process”](#) for more information.

### 2. *What is an AutoYaST profile?*

A profile is the AutoYaST configuration file. The content of the AutoYaST profile determines how the system will be configured and which packages will get installed. This includes partitioning, network setup, and software sources, to name but a few. Almost everything that can be configured with YaST in a running system can also be configured in an AutoYaST profile. The profile format is an ASCII XML file.

### 3. *How do I create an AutoYaST profile?*

The easiest way to create an AutoYaST profile is to use an existing SUSE Linux Enterprise Server system as a template. On an already installed system, start `YaST > Miscellaneous > Autoinstallation`. Now select `Tools > Create Reference Profile` from the menu. Choose the system components you want to include in the profile. Alternatively, create a profile containing the complete system configuration by running `sudo yast clone_system` from the command line.

Both methods will create the file `/root/autoinst.xml`. The version created on the command line can be used to set up an identical clone of the system on which the profile was created. However, usually you will want to adjust the file to make it possible to install several machines that are very similar, but not identical. This can be done by adjusting the profile using your favorite text/XML editor.

### 4. *How can I check the syntax of a created AutoYaST profile?*

The most efficient way to check your created AutoYaST profile is by using `jing` or `xmllint`.

See [Section 3.3, “Creating/Editing a Control File Manually”](#) for details.

5. *What is smallest AutoYaST profile that makes sense?*

If a section has not been defined in the AutoYaST profile the settings of the general YaST installation proposal will be used. However, you need to specify at least the root password to be able to log in to the machine after the installation.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE profile>
<profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://
www.suse.com/1.0/configs">
  <users config:type="list">
    <user>
      <encrypted config:type="boolean">>false</encrypted>
      <user_password>linux</user_password>
      <username>root</username>
    </user>
  </users>
</profile>
```

6. *How do I do an automatic installation with autodetection of my sound card?*

Use the following sound section in your profile:

```
<sound>
  <autoinstall config:type="boolean">>true</autoinstall>
  <configure_detected config:type="boolean">>true</configure_detected>
</sound>
```

7. *I want to install from DVD only. Where do I put the AutoYaST profile?*

Put the profile in the root of the DVD. Refer to it with file:///PROFILE.xml.

8. *How can I test a merging process on the command line?*

To merge two profiles, a.xml with base.xml, run the following command:

```
> /usr/bin/xsltproc --novalid --param replace "'false'" \
--param dontmerge1 "'package'" --param with "'a.xml'" --output out.xml \
/usr/share/autoinstall/xslt/merge.xslt base.xml
```

This requires sections in both profiles to be in alphabetical order (<software>, for example, needs to be listed after <add-on>). If you have created the profile with YaST, profiles are automatically sorted correctly.

The dontmerge1 parameter is optional and an example of what to do when you use the dont\_merge element in your profile. See [Section 5.4, "Merging of Rules and Classes"](#) for more information.

9. *May I call Zypper from scripts?*

Zypper can only be called from AutoYaST init scripts, because during the post-script phase, YaST still has an exclusive lock on the RPM database.

If you really need to use other script types (for example a post-script) you will need to break the lock at your own risk:

```
<post-scripts config:type="list">
  <script>
    <filename>yast_clone.sh</filename>
    <interpreter>shell</interpreter>
    <location/>
    <feedback config:type="boolean">false</feedback>
    <source><![CDATA[#!/bin/sh
mv /var/run/zypp.pid /var/run/zypp.sav
zypper in foo
mv /var/run/zypp.sav /var/run/zypp.pid
]]></source>
  </script>
</post-scripts>
```

10. *Is the order of sections in an AutoYaST profile important?*

Actually the order is not important. The order of sections in the profile has no influence on the AutoYaST workflow. However, if you want to *merge* different profiles, sections need to be in alphabetical order.

11. linuxrc blocks the installation with File not signed. I need to manually interact.

linuxrc found an unsigned file, such as a driver update. To use an unsigned file, you can suppress that message by passing insecure=1 to the linuxrc parameter list (together with the autoyast=... parameter).

12. *I want to install from DVD/USB/HD but fetch the XML file from the network.*

You need to pass ifcfg to linuxrc. This is required to set up the network, otherwise AutoYaST cannot download the profile from the remote host. See [Section C.3, "Advanced Network Setup"](#) for more information.

13. *Is installation onto an NFS root ( / ) possible?*

Yes, but it is more complex than other methods. The environment (DHCP, TFTP, etc.) must be set up very carefully. The AutoYaST profile must look like the following:


```
<?xml version="1.0"?>
<!DOCTYPE profile>
```

```

<profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://
www.suse.com/1.0/configs">
  <partitioning config:type="list">
    <drive>
      <device>/dev/nfs</device>
      <initialize config:type="boolean">>false</initialize>
      <type config:type="symbol">CT_NFS</type>
      <partitions config:type="list">
        <partition>
          <filesystem config:type="symbol">nfs</filesystem>
          <fstopt>nolock</fstopt>
          <device>10.10.1.53:/tmp/m4</device>
          <mount>/</mount>
        </partition>
      </partitions>
      <use>all</use>
    </drive>
  </partitioning>
</profile>

```

14. *Where can I ask questions which have not been answered here?*

There is an AutoYaST mailing list where you can post your questions. Join us at <http://lists.opensuse.org/opensuse-autoinstall/> .



## C Advanced **linuxrc** Options

**linuxrc** is a small program that runs after the kernel has loaded, but before AutoYaST or other stages. It prepares the system for installation. It allows the user to load modules, start an installed system or a rescue system, and to guide the operation of YaST.



### Note: AutoYaST and **linuxrc** Settings Are Not Identical

Some **linuxrc** settings coincidentally have the same names as settings used by AutoYaST in its `autoyast.xml` file. This does *not* mean that they take the same parameters or function in the same way. For example, AutoYaST takes a **self\_update** setting. If this value is set to `1`, another setting, **self\_update\_url** will be read and followed. Although **linuxrc** also has a **self\_update** setting, **linuxrc**'s setting takes values of either `0` or a URL.

Do not pass AutoYaST parameters to **linuxrc**, as this will almost certainly not give the desired results.

If **linuxrc** is installed on a machine, information about it can be found in the folder `/usr/share/doc/packages/linuxrc/`. Alternatively, its documentation can be found online at: <https://en.opensuse.org/SDB:Linuxrc>.



### Note: Running **linuxrc** on an Installed System

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

To keep the **linuxrc** binary file as small as possible, all its libraries and other supplemental files are linked directly into the main program binary file. This means that there is no need for any shared libraries in the initial RAM disk, `initrd`.

## C.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 flash 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 by setting

the `info` command line parameter. If you do not want `linuxrc` to read the kernel command line (for example, because you need to specify a kernel parameter that `linuxrc` recognizes as well), use `linuxrc=nocmdline`.

`linuxrc` will always look for and parse a file called `/linuxrc.config`. Use this file to change default values if you need to. In general, it is better to use the `info` file instead. Note that `/linuxrc.config` is read before any `info` file, even in manual mode.

## C.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 therefore may contain spaces. The matching of `key` is on a case-insensitive basis.

You can use the same key-value pairs on the kernel command line using the syntax `key=value`. Lines that do not have the form described above will be ignored.

The table below lists important keys and example values. For a complete list of `linuxrc` parameters, refer to <https://en.opensuse.org/SDB:Linuxrc>.

TABLE C.1: ADVANCED `linuxrc` KEYWORDS

Keyword: Example Value	Description
<code>addswap: 0 3 /dev/sda5</code>	If 0, never ask for swap; if the argument is a positive number <code>n</code> , activate the swap partition; if the argument is a partition name, activate this swap partition.
<code>autoyast: ftp://AU-TOYASTFILE</code>	Location of the auto installation file; activates auto installation mode. See <i>AutoYaST Control File Locations</i> for details.
<code>bootptimeout: 10</code>	10 seconds timeout for BOOTP requests.
<code>bootpwait: 5</code>	Sleep 5 seconds between network activation and starting bootp.
<code>display: color mono alt</code>	Set the menu color scheme.

Keyword: Example Value	Description
<code>exec: <i>COMMAND</i></code>	Run <i>command</i> .
<code>forceinsmod: 0 1</code>	Use the <code>-f</code> option (force) when running <code>insmod</code> commands.
<code>forcerootimage: 0 1</code>	Load the installation system into RAM disk.
<code>ifcfg: <i>NETWORK_CONFIGURATION</i></code>	Set up and start the network. See <a href="#">Section C.3, “Advanced Network Setup”</a> for more information.
<code>insmod: <i>MODULE</i></code>	Load <i>MODULE</i> .
<code>install: <i>URL</i></code>	Install from the repository specified with <i>URL</i> . For the syntax of <i>URL</i> refer to <a href="https://en.opensuse.org/SDB:Linuxrc#url_descr">https://en.opensuse.org/SDB:Linuxrc#url_descr</a> .
<code>keytable: de-lat1-nd</code>	Virtual console keyboard map to load.
<code>language: de_DE</code>	Language preselected for the installation.
<code>loghost: 10.10.0.22</code>	Enable remote logging via syslog via UDP port 514
<code>loghost: @10.10.0.22</code>	Enable remote logging via syslog via TCP port 514
<code>memloadimage: 50000</code>	Load installation system into RAM disk if free memory is above 50000 KB.
<code>memlimit: 10000</code>	Ask for swap if free memory drops below 10000 KB.
<code>memYaST: 20000</code>	Run YaST in text mode if free memory is below 20000 KB.
<code>memYaSTText: 10000</code>	Ask for swap before starting YaST if free memory is below 10000 KB.
<code>proxy: 10.10.0.1</code>	Proxy (either FTP or HTTP).
<code>rescue: 1 nfs://server/dir</code>	Load the rescue system; the URL variant specifies the location of the rescue image explicitly.

Keyword: Example Value	Description
<code>rescueimage: /suse/images/rescue</code>	Location of the rescue system image.
<code>rootimage: /suse/images/root</code>	Location of the installation system image.
<code>textmode: 1</code>	Start YaST in text mode.
<code>usbwait: 4</code>	Wait four seconds after loading the USB modules.
<code>y2confirm</code>	Overrides the confirm parameter in a control file and requests confirmation of installation proposal.

## C.3 Advanced Network Setup

Even if parameters like `hostip`, `nameserver`, and `gateway` are passed to `linuxrc`, the network is only started when it is needed (for example, when installing via SSH or VNC). Because `autoyast` is not a `linuxrc` parameter (this parameter is ignored by `linuxrc` and is only passed to YaST), the network will *not* be started automatically when specifying a remote location for the AutoYaST profile.

Therefore, the network needs to be started explicitly. This used to be done with the `linuxrc` parameter `netsetup`. Starting with SUSE Linux Enterprise Server 12, the parameter `ifcfg` is available. It offers more configuration options, for example configuring more than one interface. `ifcfg` directly controls the content of the `/etc/sysconfig/network/ifcfg-*` files.

### DHCP Network Configuration

The general syntax to configure DHCP is

```
ifcfg=INTERFACE=DHCP*,OPTION1=VALUE1,OPTION2=VALUE2
```

where `INTERFACE` is the interface name, for example `eth0`, or `eth*` for all interfaces. `DHCP*` can either be `dhcp` (IPv4 and IPv6), `dhcp4`, or `dhcp6`.

To set up DHCP for `eth0` use:

```
ifcfg=eth0=dhcp
```

To set up DHCP on all interfaces use:

```
ifcfg=eth*=dhcp
```

### Static Network Configuration

The general syntax to configure a static network is

```
ifcfg=INTERFACE=IP_LIST,GATEWAY_LIST,NAMESERVER_LIST,DOMAINSEARCH_LIST,\
OPTION1=value1,...
```

where *INTERFACE* is the interface name, for example *eth0*. If using *eth\**, the first device available will be used. The other parameters need to be replaced with the respective values in the given order. Example:

```
ifcfg=eth0=192.168.2.100/24,192.168.5.1,192.168.1.116,example.com
```

When specifying multiple addresses for a parameter, use spaces to separate them and quote the complete string. The following example uses two name servers and a search list containing two domains.

```
ifcfg="eth0=192.168.2.100/24,192.168.5.1,192.168.1.116 192.168.1.117,example.com
example.net"
```

For more information refer to [https://en.opensuse.org/SDB:Linuxrc#Network\\_Configuration](https://en.opensuse.org/SDB:Linuxrc#Network_Configuration).

## D Differences Between AutoYaST Profiles in SLE 12 and 15

Significant changes in SUSE Linux Enterprise Server 15, like the new modules concept or replacing `SuSEfirewall2` with `firewalld`, required changes in AutoYaST. If you want to reuse existing SUSE Linux Enterprise Server 12 profiles with SUSE Linux Enterprise Server 15, you need to adjust them as documented here.

### D.1 Product Selection

For backward compatibility with profiles created for pre-SLE 15 products, AutoYaST implements a heuristic that selects products automatically. This heuristic will be used when the profile does not contain a `product` element. Automatic product selection is based on the package and pattern selection in the profile. However, whenever possible, avoid relying on this mechanism and adapt old profiles to use explicit product selection.

For information about explicit product selection, refer to [Section 4.9.1, “Product Selection”](#).

If automatic product selection fails, an error is shown and the installation will not be continued.

### D.2 Software

The SUSE Linux Enterprise Server 15 installation medium only contains a very minimal set of packages to install. This minimal set only provides an installation environment and does not include any server applications or advanced tools. Additional software repositories, providing more packages are offered as “modules” or “extensions”. They are provided via two alternatives:

- via a registration server (the SUSE Customer Center or a local SMT/RMT proxy)
- via the SLE-15-SP0-Full-*ARCH*-GM-media1.iso image containing all modules and extensions. Using this medium does not require access to a registration server during installation. It can be shared on the local network via an installation server.



## Note: Maintenance Updates

Only using the registration server will grant access to all maintenance updates at installation time. Maintenance updates are not available when using the DVD medium without registration.

### D.2.1 Adding Modules or Extensions Using the Registration Server

To add a module or extension from the registration server, use the `addons` tag for each module/extension in the `suse_register` section. Extensions require an additional registration code, which can be specified with the `reg_code` tag.

The following XML code adds the Basesystem and Server Applications modules and the Live Patching extension. To get the respective values for the tags `name`, `version`, and `arch`, run the command **`SUSEConnect --list-extensions`** on a system that already has SLE 15 installed.

#### EXAMPLE D.1: ADDING MODULES AND EXTENSIONS (ONLINE)

```
<suse_register>
  <addons config:type="list">
    <addon>
      <name>sle-module-basesystem</name>
      <version>15.0</version>
      <arch>x86_64</arch>
    </addon>
    <addon>
      <name>sle-module-server-applications</name>
      <version>15.0</version>
      <arch>x86_64</arch>
    </addon>
    <addon>
      <name>sle-module-live-patching</name>
      <version>15.0</version>
      <arch>x86_64</arch>
      <reg_code>REGISTRATION_CODE</reg_code>
    </addon>
  </addons>
</suse_register>
```

Refer to [Section 4.3, "System Registration and Extension Selection"](#) for more information.

## D.2.2 Adding Modules or Extensions Using the SLE-15-SP0-Full-ARCH-GM-media1.iso Image

To add a module or extension using the SLE-15-SP0-Full-*ARCH*-GM-media1.iso image, create entries in the add-on section as shown in the example below. The following XML code adds the Basesystem module from a USB flash drive that contains the image:

### EXAMPLE D.2: ADDING MODULES AND EXTENSIONS (OFFLINE)

```
<add-on>
  <add_on_products config:type="list">
    <listentry>
      <media_url><![CDATA[dvd:///?devices=/dev/sda%2C/dev/sdb%2C/dev/sdc%2C/dev/sdd]]></media_url>
      <product_dir>/Module-Basesystem</product_dir>
      <product>sle-module-basesystem</product>
    </listentry>
  </add_on_products>
</add-on>
```



#### Note: Product Name Matching

The `product` tag must match the internal product name contained in the repository. If the product name does not match at installation AutoYaST will report an error.



#### Tip: Using the Packages Image from a Local Server

You can share the content of the USB flash drive on the local network via an NFS, FTP or HTTP server. To do so replace the URL in the `media_url` tag so it points to root of the medium on the server, for example:

```
<media_url>ftp://ftp.example.com/sle_15_packages/</media_url>
```

## D.2.3 Renamed Software Patterns

Software patterns have also changed since SUSE Linux Enterprise Server 15. Some patterns have been renamed; a short summary is provided in the following table.



Old SLE 12 Pattern	New SLE 15 Pattern
Basis-Devel	devel_basis
gnome-basic	gnome_basic
Minimal	enhanced_base
printing	print_server
SDK-C-C + +	devel_basis
SDK-Doc	technical_writing
SDK-YaST	devel_yast

Carefully check if all required packages are available in the defined patterns and adjust the profiles accordingly. Additionally, the required patterns and packages have to be available in the activated extensions or modules.

#### NOTES

- The pattern renames in the table above are not 1:1 replacements; the content of some patterns has been changed as well, some packages were moved to a different pattern or even removed from SUSE Linux Enterprise Server 15.
- Check that the required packages are still included in the used patterns, and optionally use the `packages` tag to specify additional packages.
- The list above might be incomplete, as some products have not been released for SUSE Linux Enterprise Server 15, yet.

## D.3 Registration of Module and Extension Dependencies

Starting with SUSE Linux Enterprise Server 15, AutoYaST automatically reorders the extensions according to their dependencies during registration. This means the order of the extensions in the AutoYaST profile is not important.

Also AutoYaST automatically adds the dependent modules even though they are missing in the profile. This means you are not required to specify all required modules. However, if an extension depends on another extension, it needs to be specified in the profile, including the registration key. Otherwise the registration would fail.

You can list the available extensions and modules in a registered system using the `SUSEConnect --list-extensions` command.

## D.4 Partitioning

The partitioning back-end previously used by YaST, `libstorage`, has been replaced by `lib-storage-ng` which is designed to allow new capabilities that were not possible before. Despite the back-end change, the XML syntax for profiles has *not* changed. However, SUSE Linux Enterprise Server 15 comes with some general changes, which are explained below.

### D.4.1 GPT Becomes the Default Partition Type on AMD64/Intel 64

On AMD64/Intel 64 systems, GPT is now the preferred partition type. However, if you would like to retain the old behavior, you can explicitly indicate this in the profile by setting the `disklabel` element to `msdos`.

### D.4.2 Setting Partition Numbers

AutoYaST will no longer support forcing partition numbers, as it might not work in some situations. Moreover, GPT is now the preferred partition table type, so partition numbers are less relevant.

However, the `partition_nr` tag is still available in order to specify a partition to be reused. Refer to [Section 4.5.2, “Partition Configuration”](#) for more information.

### D.4.3 Forcing Primary Partitions

It is still possible to force a partition as `primary` (only on MS-DOS partition tables) by setting the `primary_type` to `primary`. However, any other value, like `logical`, will be ignored by AutoYaST, which will automatically determine the partition type.

## D.4.4 Btrfs: Default Subvolume Name

The new storage layer allows the user to set different default subvolumes (or none at all) for every Btrfs file system. As shown in the example below, a prefix name can be specified for each partition using the `subvolumes_prefix` tag:

EXAMPLE D.3: SPECIFYING THE BTRFS DEFAULT SUBVOLUME NAME

```
<partition>
  <mount>/</mount>
  <filesystem config:type="symbol">btrfs</filesystem>
  <size>max</size>
  <subvolumes_prefix>@</subvolumes_prefix>
</partition>
```

To omit the subvolume prefix, set the `subvolumes_prefix` tag:

EXAMPLE D.4: DISABLING BTRFS SUBVOLUMES

```
<partition>
  <mount>/</mount>
  <filesystem config:type="symbol">btrfs</filesystem>
  <size>max</size>
  <subvolumes_prefix>@</subvolumes_prefix>
</partition>
```

As a consequence of the new behavior, the old `btrfs_set_default_subvolume_name` tag is not needed and, therefore, it is not supported anymore.

## D.4.5 Btrfs: Disabling Subvolumes

Btrfs subvolumes can be disabled by setting `create_subvolumes` to `false`. To skip the default `@` subvolume, specify `subvolumes_prefix`.

```
<partition>
  <create_subvolumes config:type="boolean">>false</create_subvolumes>
  <subvolumes_prefix><![CDATA[]]></subvolumes_prefix>
</partition>]]>
```

## D.4.6 Reading an Existing `/etc/fstab` Is No Longer Supported

On SUSE Linux Enterprise Server 15 the ability to read an existing `/etc/fstab` from a previous installation when trying to determine the partitioning layout, is no longer supported.

## D.4.7 Setting for Aligning Partitions Has Been Dropped

As cylinders have become obsolete, the `partition_alignment > tag` makes no sense and it is no longer available. AutoYaST will always try to align partitions in an optimal way.

## D.4.8 Using the type to Define an Volume Group

The `is_lvm_vg` element has been dropped in favor of setting the `type` to the `CT_LVM` value. Refer to the [Section 4.5.7, “Logical Volume Manager \(LVM\)”](#) for further details.

## D.5 Firewall Configuration

In SUSE Linux Enterprise Server 15, `SuSEfirewall2` has been replaced by `firewalld` as the default firewall. The configuration of these two firewalls differs significantly, and therefore the respective AutoYaST profile syntax has changed.

Old profiles will continue working, but the supported configuration will be very limited. It is recommended to update profiles for SLE 15 as outlined below. If keeping SLE 12 profiles, we recommend to check the final configuration to avoid unexpected behavior or network security threats.

TABLE D.1: AUTOYAST FIREWALL CONFIGURATION IN SLE 15: BACKWARD COMPATIBILITY

Supported (but deprecated)	Unsupported
<code>FW_CONFIGURATIONS_{DMZ, EXT, INT}</code>	<code>FW_ALLOW_FW_BROADCAST_{DMZ, EXT, INT}</code>
<code>FW_DEV_{DMZ, EXT, INT}</code>	<code>FW_IGNORE_FW_BROADCAST_{DMZ, EXT, INT}</code>
<code>FW_LOG_DROP_ALL</code>	<code>FW_IPSECT_TRUST</code>
<code>FW_LOG_DROP_CRIT</code>	<code>FW_LOAD_MODULES</code>
<code>FW_MASQUERADE</code>	<code>FW_LOG_ACCEPT_ALL</code>
<code>FW_SERVICES_{DMZ, INT, EXT}_{TCP, UDP, IP}</code>	<code>FW_LOG_ACCEPT_CRIT</code>

Supported (but deprecated)	Unsupported
	<u>FW_PROTECT_FROM_INT</u>
	<u>FW_ROUTE</u>
	<u>FW_SERVICES_{DMZ, EXT, INT}_RPC</u>
	<u>FW_SERVICES_ACCEPT_RELATED_{DMZ, EXT, INT}</u>

Configuration options from SuSEfirewall2 that are no longer available either have no equivalent mapping in `firewalld` or will be supported in future releases of SUSE Linux Enterprise Server. Some `firewalld` features are not yet supported by YaST and AutoYaST—you can make use of them with post installation scripts in your AutoYaST profile. See [Section 4.30, “Custom User Scripts”](#) for more information.



### Note: Enabling and Starting the Firewall

Enabling and starting the `systemd` service for `firewalld` is done with the same syntax as in SLE 12. This is the only part of the firewall configuration syntax in AutoYaST that has not changed:

```
<firewall>
  <enable_firewall config:type="boolean">true</enable_firewall>
  <start_firewall config:type="boolean">true</start_firewall>
  ...
</firewall>
```

The following examples show how to convert deprecated (but still supported) profiles to the SLE 15 syntax:

## D.5.1 Assigning Interfaces to Zones

Both SuSEfirewall2 and `firewalld` are zone-based, but have a different set of predefined rules and a different level of trust for network connections.

TABLE D.2: MAPPING OF SUSEFIREWALL2 AND firewalld ZONES

firewalld (SLE 15)	SuSEfirewall2 (SLE 12)
dmz	DMZ
external	EXT with <code>FW_MASQUERADE</code> set to <code>yes</code>
public	EXT with <code>FW_MASQUERADE</code> set to <code>no</code>
internal	INT with <code>FW_PROTECT_FROM_INT</code> set to <code>yes</code>
trusted	INT with <code>FW_PROTECT_FROM_INT</code> set to <code>no</code>
block	N/A
drop	N/A
home	N/A
work	N/A

In SuSEfirewall2 the default zone is the external one (EXT) but it also allows the use of the special keyword `any` to assign all the interfaces that are not listed anywhere to a specified zone.

### D.5.1.1 Default Configuration

The following two examples show the default configuration that is applied for the interfaces `eth0`, `eth1`, `wlan0` and `wlan1`.

EXAMPLE D.5: ASSIGNING ZONES: DEFAULT CONFIGURATION (DEPRECATED SYNTAX)

```
<firewall>
<FW_DEV_DMZ>any eth0</FW_DEV_DMZ>
<FW_DEV_EXT>eth1 wlan0</FW_DEV_EXT>
<FW_DEV_INT>wlan1</FW_DEV_INT>
</firewall>
```

EXAMPLE D.6: ASSIGNING ZONES: DEFAULT CONFIGURATION (SLE 15 SYNTAX)

```
<firewall>
<default_zone>dmz</default_zone>
<zones config:type="list">
```

```

<zone>
  <name>dmz</name>
  <interfaces>
    <interface>eth0</interface>
  </interfaces>
</zone>
<zone>
  <name>public</name>
  <interfaces>
    <interface>eth1</interface>
  </interfaces>
</zone>
<zone>
  <name>trusted</name>
  <interfaces>
    <interface>wlan1</interface>
  </interfaces>
</zone>
</zones>
</firewall>

```

### D.5.1.2 Masquerading and Protecting Internal Zones

The following two examples show how to configure the interfaces eth0, eth1, wlan0 and wlan1 with masquerading and protected internal zones.

#### EXAMPLE D.7: MASQUERADING AND PROTECTING INTERNAL ZONES (DEPRECATED SYNTAX)

```

<firewall>
  <FW_DEV_DMZ>any eth0</FW_DEV_DMZ>
  <FW_DEV_EXT>eth1 wlan0</FW_DEV_EXT>
  <FW_DEV_INT>wlan1</FW_DEV_INT>
  <FW_MASQUERADE>yes</FW_MASQUERADE>
  <FW_PROTECT_FROM_INT>yes</FW_PROTECT_FROM_INT>
</firewall>

```

#### EXAMPLE D.8: MASQUERADING AND PROTECTING INTERNAL ZONES (SLE 15 SYNTAX)

```

<firewall>
  <default_zone>dmz</default_zone>
  <zones config:type="list">
    <zone>
      <name>dmz</name>
      <interfaces config:type="list">
        <interface>eth0</interface>
      </interfaces>
    </zone>
  </zones>
</firewall>

```

```

</zone>
<zone>
  <name>external</name>
  <interfaces config:type="list">
    <interface>eth1</interface>
  </interfaces>
</zone>
<zone>
  <name>internal</name>
  <interfaces config:type="list">
    <interface>wlan1</interface>
  </interfaces>
</zone>
</zones>
</firewall>

```

## D.5.2 Opening Ports

In SuSEfirewall2 the `FW_SERVICES_{DMZ,EXT,INT}_{TCP,UDP,IP,RPC}` tags were used to open ports in different zones.

For `TCP` or `UDP`, SuSEfirewall2 supported a port number or range, or a service name from `/etc/services` with a single tag for the respective zone and service. For IP services a port number or range, or a protocol name from `/etc/protocols` could be specified with `FW_SERVICES_ZONE_IP`.

For `firewalld` each port, port range, and service requires a separate entry in the `port` section for the respective zone. IP services need separate entries in the `protocol` section.

RPC services, which were supported by SuSEfirewall2, are no longer supported with `firewalld`.

### EXAMPLE D.9: OPENING PORTS (DEPRECATED SYNTAX)

```

<firewall>
  <FW_SERVICES_DMZ_TCP>ftp ssh 80 5900:5999</FW_SERVICES_DMZ_TCP>
  <FW_SERVICES_EXT_UDP>1723 ipsec-nat-t</FW_SERVICES_EXT_UDP>
  <FW_SERVICES_EXT_IP>esp icmp gre</FW_SERVICES_EXT_IP>
  <FW_MASQUERADE>yes</FW_MASQUERADE>
</firewall>

```

### EXAMPLE D.10: OPENING PORTS (SLE 15 SYNTAX)

```

<firewall>
  <zones config:type="list">
    <zone>
      <name>dmz</name>

```



```

<ports config:type="list">
  <port>ftp/tcp</port>
  <port>ssh/tcp</port>
  <port>80/tcp</port>
  <port>5900-5999/tcp</port>
</ports>
</zone>
<zone>
  <name>external</name>
  <ports config:type="list">
    <port>1723/udp</port>
    <port>ipsec-nat-t/udp</port>
  </ports>
  <protocols config:type="list">
    <protocol>esp</protocol>
    <protocol>icmp</protocol>
    <protocol>gre</protocol>
  </protocols>
</zone>
</zones>
</firewall>

```

### D.5.3 Opening firewalld Services

For opening a combination of ports and/or protocols, SuSEfirewall2 provides the `FW_CONFIGURATIONS_{EXT, DMZ, INT}` tags which are equivalent to services in `firewalld`.

EXAMPLE D.11: **OPENING SERVICES (DEPRECATED SYNTAX)**

```

<firewall>
  <FW_CONFIGURATIONS_EXT>dhcp dhcpv6 samba vnc-server</FW_CONFIGURATIONS_EXT>
  <FW_CONFIGURATIONS_DMZ>ssh</FW_CONFIGURATIONS_DMZ>
</firewall>

```

EXAMPLE D.12: **OPENING SERVICES (SLE 15 SYNTAX)**

```

<firewall>
  <zones config:type="list">
    <zone>
      <name>dmz</name>
      <services config:type="list">
        <service>ssh</service>
      </services>
    </zone>
  </zones>

```

```

<name>public</name>
<services config:type="list">
  <service>dhcp</service>
  <service>dhcpv6</service>
  <service>samba</service>
  <service>vnc-server</service>
</services>
</zone>
</zones>
</firewall>

```

The services definition can be added via packages in both cases:

- SuSEfirewall2 Service Definitions: [https://en.opensuse.org/SuSEfirewall2/Service\\_Definitions\\_Added\\_via\\_Packages](https://en.opensuse.org/SuSEfirewall2/Service_Definitions_Added_via_Packages) ↗
- `firewalld` RPM Packaging [https://en.opensuse.org/firewalld/RPM\\_Packaging](https://en.opensuse.org/firewalld/RPM_Packaging) ↗  
`firewalld` already provides support for the majority of important services in `/usr/lib/firewalld/services`. Check this directory for an existing configuration before defining a new one.

## D.5.4 For More Information

- SuSEfirewall2/AutoYaST Documentation for SLE 12 ([https://www.suse.com/documentation/sles-12/book\\_autoyast/data/createprofile\\_firewall.html](https://www.suse.com/documentation/sles-12/book_autoyast/data/createprofile_firewall.html)) ↗
- Official `firewalld` Documentation (<http://www.firewalld.org/documentation/>) ↗

## D.6 NTP Configuration

The time server synchronization daemon `ntpd` has been replaced with the more modern daemon `chrony`. Therefore the configuration syntax for the time-keeping daemon in AutoYaST has changed. AutoYaST profiles from SLE 12 that contain a section with `ntp:client` need to be updated.

Instead of containing low level configuration options, NTP is now configured by a set of high level options that are applied on top of the default settings:

EXAMPLE D.13: NTP CONFIGURATION (SLE 15 SYNTAX)

```

<ntp-client>

```

```
<ntp_policy>auto</ntp_policy>
<ntp_servers config:type="list">
  <ntp_server>
    <iburst config:type="boolean">false</iburst>
    <address>cz.pool.ntp.org</address>
    <offline config:type="boolean">true</offline>
  </ntp_server>
</ntp_servers>
<ntp_sync>systemd</ntp_sync>
</ntp-client>
```

## D.7 AutoYaST Packages Are Needed for the Second Stage

A regular installation is performed in a single stage, while an installation performed via AutoYaST needs two stages in most cases. In order to perform the second stage of the installation AutoYaST requires a few additional packages, for example autoyast2-installation and autoyast2. If these are missing, a warning will be shown.

## D.8 The CA Management Module Has Been Dropped

The module for CA Management (yast2-ca-management) has been removed from SUSE Linux Enterprise Server 15, and for the time being there is no replacement available. In case you are reusing an SLE 12 profile, make sure it does not contain a ca\_mgm section.

## D.9 Upgrade

### D.9.1 Software

SLE 12 has two modes of evaluating which packages need to be upgraded. In SUSE Linux Enterprise Server 15, upgrades are always determined by the dependency solver, equivalent to using **zypper dup**.

This makes the option only\_installed\_packages in the software section obsolete.

## D.9.2 Registration

When upgrading a registered system, all old repositories are removed. This is done to avoid possible conflicts between the new and old repositories and to clean-up the repositories for the dropped products. If you need to keep custom repositories, add them again using the add-on option.

EXAMPLE D.14: MINIMAL REGISTRATION CONFIGURATION FOR UPGRADE

```
<suse_register>
  <do_registration config:type="boolean">true</do_registration>
</suse_register>
```

If the registration server returns more than one possible migration target, AutoYaST will automatically select the first one. Currently you cannot select a different migration target.

After upgrading an unregistered system or skipping registration upgrade by omitting the suse\_register option, you might need to adjust the repository setup manually.