SUSE Manager

1.7

August 14, 2012

Reference Guide

SUSE

Reference Guide

Contents

C   Minimalist AutoYaST Profile for Automated Installations   323

D   About SUSE Manager and Spacewalk   325

Glossary   329

About This Guide

SUSE® Manager enables you to efficiently manage a set of Linux systems and keep them up-to-date. It provides automated and cost-effective software management, asset management, system provisioning, and monitoring capabilities. SUSE Manager is compatible with Red Hat Network Satellite Server and offers seamless management of both SUSE® Linux Enterprise and Red Hat Enterprise Linux client systems.

This manual is intended for system administrators. It guides you through registering systems with SUSE Manager, configuring its daemon, using the Web interface, monitoring client systems, and other features. Furthermore it gives you an overview how multiple organizations and their systems can be administered and which virtualization scenarios are possible.

Many chapters in this manual contain links to additional documentation resources. These include additional documentation available on the installed system as well as documentation on the Internet.

For an overview of the documentation available for your product and the latest documentation updates, refer to [http://www.novell.com/documentation/suse _manager/](http://www.novell.com/documentation/suse_manager/) or to the following section.

HTML versions of the manuals are also available from the *Help* tab of the SUSE Manager Web interface.

> **NOTE: Obtaining the Release Notes**
>
> Although this manual reflects the most current information possible, read the *SUSE Manager Release Notes* for information that may not have been available prior to the finalization of the documentation. The notes can be found at http://www.novell.com/documentation/suse_manager/.

1 Available Documentation

The following manuals are available on this product:

Quick Start (↑Quick Start)

Guides you step by step through the installation, setup and basic configuration of SUSE Manager.

Proxy Quick Start (↑Proxy Quick Start)

Gives an overview of the installation and setup of SUSE Manager Proxy.

Installation Guide (↑Installation Guide)

Lists installation scenarios and example topologies for different SUSE Manager setups. Also contains detailed information about SUSE Manager maintenance and troubleshooting.

Client Configuration Guide (↑Client Configuration Guide)

Describes best practices for setting up clients to connect to a SUSE Manager server or SUSE Manager Proxy.

Reference Guide (page i)

Reference documentation that covers administration topics like registering and updating client systems, configuring the SUSE Manager daemon, using the Web interface, monitoring client systems, and more. Also contains a glossary with key terms used in the SUSE Manager context.

HTML versions of the product manuals can be found in the installed system under `/usr/share/doc/manual`. Find the latest documentation updates at `http://www.novell.com/documentation` where you can download PDF or HTML versions of the manuals for your product.

2 Feedback

Several feedback channels are available:

Bugs and Enhancement Requests

For services and support options available for your product, refer to `http://www.suse.com/support/`.

To report bugs for a product component, log into the Novell Customer Center from `http://www.suse.com/support/` and select *My Support > Service Request*.

User Comments

    We want to hear your comments about and suggestions for this manual and the other documentation included with this product. Use the User Comments feature at the bottom of each page in the online documentation or go to `http://www.suse.com/documentation/feedback.html` and enter your comments there.

Mail

    For feedback on the documentation of this product, you can also send a mail to `doc-team@suse.de`. Make sure to include the document title, the product version and the publication date of the documentation. To report errors or suggest enhancements, provide a concise description of the problem and refer to the respective section number and page (or URL).

3 Documentation Conventions

The following typographical conventions are used in this manual:

- `/etc/passwd`: directory names and filenames.

- *placeholder*: replace *placeholder* with the actual value.

- `PATH`: the environment variable PATH.

- `ls, --help`: commands, options, and parameters.

- `user`: users or groups.

- Alt, Alt + F1: a key to press or a key combination; keys are displayed with uppercase letters as on a keyboard.

- *File*, *File > Save As*: menu items, buttons.

- ▶ **amd64 em64t:** This paragraph is only relevant for the specified architectures. The arrows mark the beginning and the end of the text block. ◀

- *Dancing Penguins* (Chapter *Penguins*, ↑Another Manual): This is a reference to a chapter in another manual.

SUSE Manager Overview

1

SUSE Manager is an server solution for managing a network of SUSE Linux Enterprise or Red Hat Enterprise Linux systems. All security alerts, bug fix alerts, and enhancement alerts (collectively known as patch alerts) can be downloaded directly from SUSE, or Novell, or your own custom collection. You can even schedule updates for delivery to your system immediately after release.

The main components of SUSE Manager are:

- the update agent (`rhn_check`),

- the SUSE Manager website, whether this is hosted by a SUSE Manager or fed through an proxy server,

- SUSE Manager daemon,

SUSE Manager daemon enables channel subscription, package installs, and management of system profiles. See Section 2.3, "Red Hat Update Agent (RHEL 4)" (page 26) for further information.

The SUSE Manager daemon (`rhnsd`) runs in the background as a service and probes SUSE Manager for notifications and updates at set time intervals (see Chapter 3, *SUSE Manager Daemon* (page 47) for further information). This daemon is necessary in order to schedule updates or other actions through the website.

Find out more about SUSE Manager at `http://www.novell.com/products/suse-manager/technical-information/`.

1.1 Management

In addition to the features offered in the SUSE Manager update subscription level, the SUSE Manager management subscription service allows you to manage your network of SUSE Linux Enterprise systems, users, and system groups through its *System Set Manager* interface.

SUSE Manager management is based upon the concept of organizations. Each management-level SUSE customer has the ability to establish users who have administration privileges to system groups. An organization administrator has overall control over each SUSE Manager organization with the ability to add and remove systems and users. When users other than the SUSE Manager administrator log into the SUSE Manager website, they see only the systems they have permission to administer.

The SUSE Manager features available to you depend on the subscription level for each SUSE Linux Enterprise system. With each management subscription, you receive the functionality to update users, plus:

- Package Profile Comparison — Compare the package set on one system with the package sets of similar systems with one click.

- Search Systems — Search through systems based on a number of criteria: packages, networking information, even hardware asset tags.

- System Grouping — Web servers, database servers, workstations and other workload-focused systems may be grouped so that each set can be administered in common ways.

- Multiple Administrators — Administrators may be given rights to particular system groups, easing the burden of system management over very large organizations.

- System Set Manager — You can apply actions to sets of systems instead of single systems, work with members of a predefined system group, or work with an ad-hoc collection of systems. Install a single software package on each, subscribe the systems to a new channel, or apply all patches to them with a single action.

- Batch Processing — Compiling a list of outdated packages for a thousand systems would take days even for an experienced sysadmin. SUSE Manager can do it for you in seconds.

1.2 Provisioning

Provisioning service level is optional and encompasses all of the features offered in the update and management subscription levels. It is designed to allow you to deploy and manage your network of SUSE Linux Enterprise systems, users, and system groups.

Like management, provisioning is based on an organization. It takes this concept a step further by enabling customers with provisioning entitlements to autoinstall using AutoYaST or Kickstart, reconfigure, track, and revert systems on the fly.

In addition to all of the features mentioned in lower service levels, Provisioning provides:

- Autoinstalling — Systems with provisioning entitlements may be automatically installed via AutoYaST or Kickstart. This process can be adjusted to your needs with various options, including the type of bootloader, time zone, packages included/excluded, and IP address ranges allowed. Even GPG and SSL keys can be pre-configured.

- Client Configuration — SUSE Manager customers may use SUSE Manager to manage the configuration files on Provisioning-entitled systems. Users can upload files to custom configuration channels on the Satellite, verify local configuration files against those stored on the Satellite, and deploy files from the Satellite.

- Custom System Information — Provisioning customers can add any type of information about their registered systems via custom keys and values. This differs from system profile information, which is generated automatically, and also from the Notes, which are completely unrestricted. Custom system information allows you to create keys of your choice and assign searchable values for these key to each provisioning-entitled system. For instance, this feature allows you to specify the cubicle in which each system is located and search through all registered systems according to their cubicle.

1.3 Monitoring

Monitoring entitlements are available to SUSE Manager customers with SUSE Linux Enterprise systems.

Monitoring allows an organization to install probes that can immediately detect failures and identify performance degradation before it becomes critical. Used properly, the monitoring entitlement can provide insight into the applications, services, and devices on each system.

Specifically, monitoring provides:

- Probes — Dozens of probes can be run against each system. These range from simple `ping` checks to custom remote programs designed to return valuable data.

- Notification — Alerts can be sent to email and pager addresses with contact methods identified by you when a probe changes state. Each probe notification can be sent to a different method, or address.

- Central Status — The results of all probes are summarized in a single *Probe Status* page, with the systems affected broken down by state.

- Reporting — By selecting a probe and identifying the particular metric and a range of time, you can generate graphs and event logs depicting precisely how the probe has performed. This can be instrumental in predicting and preventing costly system failures.

- Probe Suites — Groups of probes may be assigned to a system or set of systems at once rather than individually. This allows administrators to be certain that similar systems are monitored in the same way and saves time configuring individual probes.

- Notification Filters — Probe notifications may be redirected to another recipient, halted, or sent to an additional recipient for a specified time based on probe criteria, notification method, scout or organization.

1.4 Patch Notifications and Scheduled Package Installations

You can configure SUSE Manager to send you email notifications of new and updated software packages as soon as the packages are available through Novell Customer Center. You receive one email per patch, regardless of the number of affected systems. You can also schedule package installs or package updates. The benefits include:

- Reduced time and effort required by system administrators to stay on top of the patches list

- Minimized security vulnerabilities in your network through the application of updates as soon as SUSE releases them

- Filtered list of package updates (packages not relevant to your network are not included)

- Reliable method of managing multiple systems with similar configurations

1.5 Security, Quality Assurance, and SUSE Manager

SUSE Manager provides significant benefits to your network, including security and quality assurance. All transactions made between your systems and SUSE Manager are encrypted and all RPM packages are signed with GNU Privacy Guard (GPG) signature to ensure authenticity.

SUSE Manager incorporates the following security measures:

1. Your system profile, available at Novell Customer Center `http://novell.com/center` is accessible only with an username and password.

2. A digital certificate is written to the client system after registration and is used to authenticate the system during each transaction between the client and SUSE Manager. The file is only readable by the root user on the client system.

3. SUSE signs all communications with an electronic signature using GPG. RPM can be used to verify the authenticity of the package before it is installed.

4. SUSE encrypts all transactions using a secure sockets layer (SSL) connection.

5. The SUSE quality assurance team tests and verifies all packages before they are added to the patch list and Novell Customer Center.

Package Update Tools (SLE and RHEL)

2

On the supported client systems various software management and package update tools are available—not only GUI programs and desktop applets, but also command-line tools.

WARNING: Updating SUSE Manager

For updating SUSE Manager server, additional steps might be required. Refer to Section "Updating SUSE Manager" (Chapter 6, *Maintenance*, ↑Installation Guide) for detailed instructions.

2.1 Updating Packages on SLE

YaST Online Update (`yast2 online_update`) is the desktop update application for SUSE Linux Enterprise. Using this tool, you can update packages and read additional information about the updated packages, such as bug fix details, security alerts, enhancements, and more. For more information, refer to Section 2.1.1, "Using YaST Online Update" (page 8).

Use `zypper` if you prefer to manage software updates on the command line. For more information, refer to Section 2.1.2, "Updating Packages from the Command Line with Zypper" (page 12).

For background information, see the SUSE Linux Enterprise Deployment Guide, Chapter 9.0 *Installing or Removing Software* (using desktop applets). SUSE Linux

Enterprise Administration Guide, Chapter 1.0 *YaST Online Update*, and Chapter 4.0 *Managing Software with Command Line Tools* (zypper).

If you enable the *Auto Patch Update*, updates will be installed automatically, pushed from SUSE Manager. For more information about this feature, refer to "Auto Patch Update" (page 71).

2.1.1 Using YaST Online Update

Novell offers a continuous stream of software security updates for your product. By default the update applet is used to keep your system up-to-date. This section covers the tool for updating software packages: YaST Online Update.

Figure 2.1   *YaST Software Repositories*
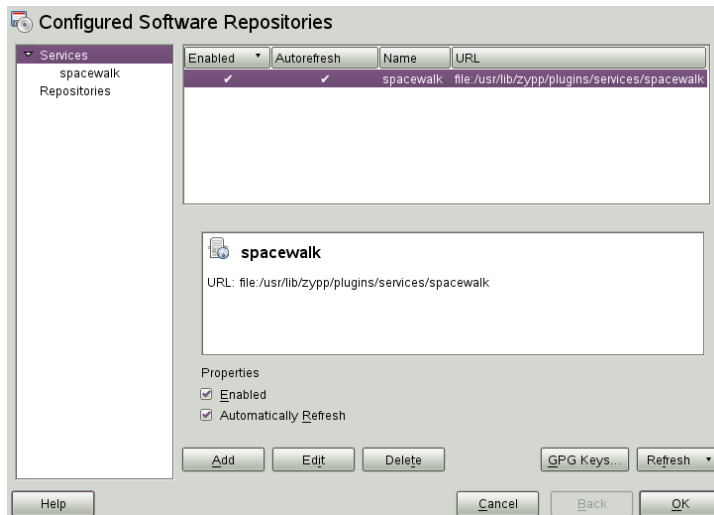
After activating the SUSE Linux Enterprise Server client system, SUSE Manager channels are available as a `spacewalk` repository service (see Figure 2.1, "YaST Software Repositories" (page 8)) and you can use YaST to install software updates on the client system. For more information about client activation, refer to Section "Client Setup" (↑Quick Start) and Section 4.4.6, "Activation Keys — [Mgmt]" (page 99).

Novell provides updates with different relevance levels. `Security` updates fix severe security hazards and should definitely be installed. `Recommended` updates fix issues that could compromise your computer, whereas `Optional` updates fix non-security relevant issues or provide enhancements.

Procedure 2.1   *Installing Patches with YaST Online Update*

1 Run *Software > Online Update* in YaST

2 All new patches (except the optional ones) that are currently available for your system are already marked for installation. Click the confirmation button to automatically install them.

3 Confirm with *Finish* after the installation has completed. Your system is now up-to-date.

2.1.1.1 Installing Patches Manually Using the Qt Interface

The *Online Update* window consists of four sections. The list of all patches available is on the left. Find the description of the selected patch displayed below the list of patches. The right column lists the packages included in the selected patch (a patch can consist of several packages) and below, a detailed description of the selected package.

Figure 2.2   *YaST Online Update*
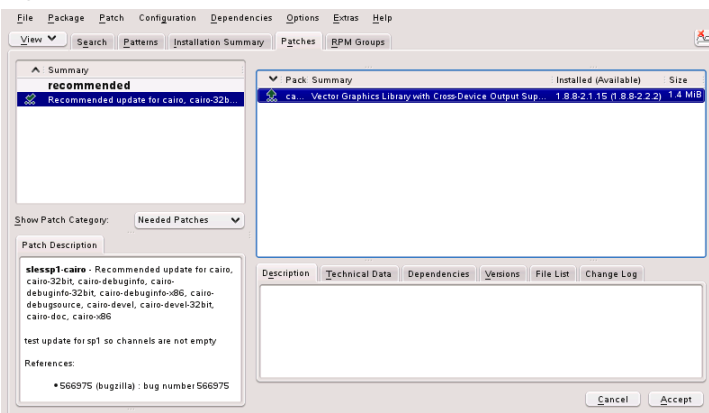
The patch display lists the available patches for the client system. The patches are sorted by security relevance (`security`, `recommended`, and `optional`). There are three different views on patches. Use *Show Patch Category* to toggle the views:

Needed Patches (default view)
> Non-installed patches that apply to packages installed on your system.

Unneeded Patches
> Patches that either apply to packages not installed on your system, or patches that have requirements which have already have been fulfilled (because the relevant packages have already been updated from another source).

All Patches
> All patches available for the client system.

A list entry consists of a symbol and the patch name. For a list of possible symbols, press Shift + F1. Actions required by `Security` and `Recommended` patches are automatically preset. These actions are *Autoinstall*, *Autoupdate* and *Autodelete*. Actions for `Optional` patches are not preset—right-click on a patch and choose an action from the list.

If you install an up-to-date package from a repository other than the update repository, the requirements of a patch for this package may be fulfilled with this installation. In this case a check mark is displayed in front of the patch summary. The patch will be visible in the list until you mark it for installation. This will in fact not install the patch (because the package already is up-to-date), but mark the patch as having been installed.

Most patches include updates for several packages. If you want to change actions for single packages, right-click on a package in the package window and choose an action. Once you have marked all patches and packages as desired, proceed with *Accept*.

2.1.1.2 Installing Patches Manually Using the GTK Interface

The *Online Update* window consists of two main sections. The left pane lists all patches and provides different filters for the patch list. See the right pane for a list of changes that will be carried out once you *Apply* them.

Figure 2.3 *YaST Online Update*
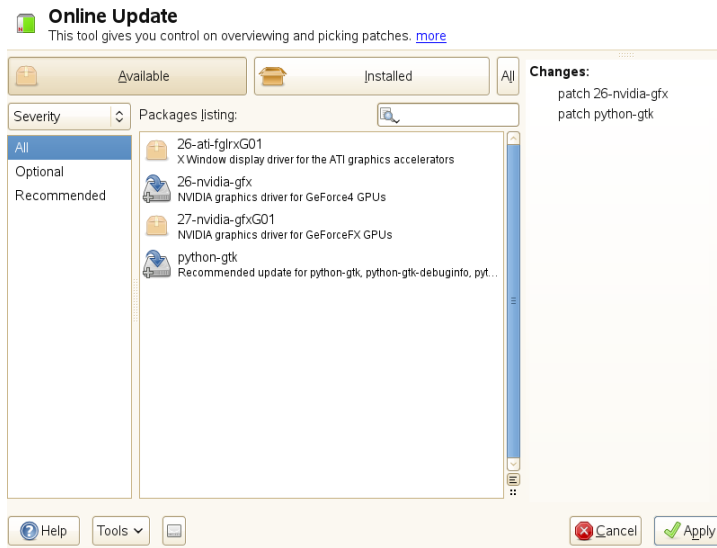
Patch List Filters

Available
> Non-installed patches that apply to packages installed on your system.

Installed
> Patches that are already installed.

All
> Patches that are either already installed or available.

Severity
> Only show *Optional*, *Recommended*, or *Security* patches. By default, *All* patches are shown.

Repositories
> This filter lets you display the patches per repository.

Packages Listing
> Apply your custom filter here.

Click on a patch entry to open a row with detailed information about the patch in the bottom of the window. Here you can see a detailed patch description as well as the versions available. You can also choose to *Install* optional patches—security and recommended patches are already preselected for installation.

2.1.1.3 Automatic Online Update

YaST also offers the possibility to set up an automatic update. Open *Software > Online Update Configuration*. Check *Automatic Online Update* and choose whether to update *Daily*, *Weekly*, or *Monthly*. Some patches, such as kernel updates, require user interaction, which would cause the automatic update procedure to stop. Therefore you should check *Skip Interactive Patches* if you want the update procedure to proceed fully automatically. Having done so, you should run a manual *Online Update* from time to time in order to install patches that require interaction.

2.1.2 Updating Packages from the Command Line with Zypper

Zypper is a command line package manager for installing, updating and removing packages as well as for managing repositories. It is especially useful for remote software management tasks or managing software from shell scripts.

For more information on managing software from the command line, enter `zypper help` or `zypper help` *command* or see the `zypper(8)` manpage. .

2.1.2.1 General Usage

The general syntax of Zypper is:

```
zypper [global-options] command [command-options] [arguments] ...
```

The components enclosed in brackets are not required. The simplest way to execute Zypper is to type its name, followed by a command. For example, to apply all needed patches to the system type:

```
zypper patch
```

Additionally, you can choose from one or more global options by typing them just before the command. For example, `--non-interactive` means running the command without asking anything (automatically applying the default answers):

```
zypper --non-interactive patch
```

To use the options specific to a particular command, type them right after the command. For example, `--auto-agree-with-licenses` means applying all needed patches to the system without asking to confirm any licenses (they will automatically be accepted):

```
zypper patch --auto-agree-with-licenses
```

Some commands require one or more arguments. When using the install command, for example, you need to specify which package(s) to install:

```
zypper install mplayer
```

Some options also require an argument. The following command will list all known patterns:

```
zypper search -t pattern
```

You can combine all of the above. For example, the following command will install `mplayer` and `amarok` packages using the `factory` repository only, and be verbose:

```
zypper -v install --repo factory mplayer amarok
```

Most Zypper commands have a `dry-run` option that does a simulation of the given command. It can be used for test purposes. This could useful to finding out beforehand if and which package dependencies will break.

```
zypper remove --dry-run MozillaFirefox
```

2.1.2.2 Installing and Removing Software with Zypper

To install or remove packages use the following commands:

```
zypper install package
zypper remove package
```

Zypper knows various ways to address packages for the install and remove commands:

by the exact package name

```
zypper in MozillaFirefox
```

by repository alias and package name

```
zypper in mozilla:MozillaFirefox
```

In this example `mozilla` is the alias of the repository from which to install.

by package name using wildcards
The following command will install all packages that have names starting with "Moz". Use with care, especially when removing packages.

```
zypper in 'Moz*'
```

by capability
If you, for example, would like to install a perl module without knowing the name of the package, capabilities come in handy:

```
zypper in 'perl(Time::ParseDate)'
```

by capability and/or architecture and/or version
Together with a capability you can specify an architecture (such as `i586` or `x86_64`) and a version. The version must be preceded by an operator: < (lesser than), <= (lesser than or equal), = (equal>, >= (greater than or equal), > (greater than).

```
zypper in 'firefox.x86_64'
zypper in 'firefox>=3.5.3'
zypper in 'firefox.x86_64>=3.5.3'
```

by path
Specify a local or remote path to a package:

```
zypper in /tmp/install/MozillaFirefox.rpm
zypper in –
http://download.opensuse.org/repositories/mozilla/SUSE_Factory/x86_64/MozillaFirefox-3.5.3-1.3.x86_64.rpm
```

To install and remove packages simultaneously use the +/− modifiers. To install `emacs` and remove `vim` simultaneously, use:

```
zypper install emacs –vim
```

To remove `emacs` and install `vim` simultaneously, use:

```
zypper remove emacs +vim
```

To prevent the package name starting with the − being interpreted as a command option, always use it as the second argument. If this is not possible, precede it with −−:

```
zypper install -emacs +vim       # Wrong
zypper install vim -emacs        # Correct
zypper install -- -emacs +vim    # Correct, same as above
zypper remove emacs +vim         # Correct, same as above
```

By default, Zypper asks for a confirmation before installing or removing a selected package, or when a problem occurs. You can override this behavior using the `--non-interactive` option. This option must be given before the actual command (install, remove, and patch) as in the following:

```
zypper --non-interactive install package_name
```

This option allows the use of Zypper in scripts and cron jobs.

WARNING: Do not Remove Mandatory System Packages

Do not remove packages such as `glibc`, `zypper`, `kernel`, or similar packages. These packages are mandatory for the system and, if removed, may cause the system to become unstable or stop working altogether.

Installing Source Packages

If you want to install the corresponding source package of a package, use:

```
zypper source-install package_name
```

That command will also install the build dependencies of the specified package. If you do not want this, add the switch `-D`. To install only the build dependencies use `-d`.

```
zypper source-install -D package_name # source package only
zypper source-install -d package_name # build dependencies only
```

Of course, this will only work if you have the repository with the source packages enabled in your repository list (it is added by default, but not enabled). See Section 2.1.2.4, "Managing Repositories with Zypper" (page 18) for details on repository management.

A list of all source packages available in your repositories can be obtained with:

```
zypper search -t srcpackage
```

Utilities

To verify whether all dependencies are still fulfilled and to repair missing dependencies, use:

```
zypper verify
```

In addition to dependencies that must be fulfilled, some packages "recommend" other packages. These recommended packages are only installed if actually available. In case recommended packages were made available after the recommending package has been installed (by adding additional packages), use the following command:

```
zypper install-new-recommends
```

2.1.2.3 Updating Software with Zypper

There are three different ways to update software using Zypper: by installing patches, by installing a new version of a package or by updating the entire distribution. The latter is achieved with the `zypper dist-upgrade` command .

Installing Patches

To install all officially released patches applying to your system, just run:

```
zypper patch
```

In this case, all patches available in your repositories are checked for relevance and installed, if necessary. After registering your SUSE Manager installation, an official update repository containing such patches will be added to your system. The above command is all you must enter in order to apply patches when needed.

Zypper knows three different commands to query for the availability of patches:

`zypper patch-check`
> Lists the number of needed patches (patches, that apply to your system but are not yet installed)
>
> ```
> ~ # zypper patch-check
> Loading repository data...
> Reading installed packages...
> 5 patches needed (1 security patch)
> ```

`zypper list-patches`

Lists all needed patches (patches, that apply to your system but are not yet installed)

```
~ # zypper list-updates
Loading repository data...
Reading installed packages...
S | Repository | Name                        | Current | Available  | Arch
--+------------+-----------------------------+---------+------------+------
v | Updates    | update-test-interactive     | 0-2.35  | 0-9999.1.2 | noarch
v | Updates    | update-test-optional        | 0-2.35  | 0-9999.1.2 | noarch
v | Updates    | update-test-reboot-needed   | 0-2.35  | 0-9999.1.2 | noarch
v | Updates    | update-test-relogin-suggested | 0-2.35 | 0-9999.1.2 | noarch
v | Updates    | update-test-security        | 0-2.35  | 0-9999.1.2 | noarch
```

`zypper patches`

Lists all patches available for SUSE Manager, regardless of whether they are already installed or apply to your installation.

It is also possible to list and install patches relevant to specific issues. To list specific patches, use the `zypper list-patches` command with the following options:

`-b`

Lists all needed patches for Bugzilla issues.

`--bugzilla[=number]`

Lists needed patches for a Bugzilla issue with the specified number.

To install a patch for a specific issue, use command:

```
zypper patch --bugzilla=number
  -
```

Installing Updates

If a repository contains only new packages, but does not provide patches, `zypper patch` does not show any effect. To update all installed packages with newer available versions, use:

```
zypper update
```

To update individual packages, specify the package with either the update or install command:

```
zypper update package
zypper install package
```

A list of all new packages available can be obtained with the command:

```
zypper list-updates
```

NOTE: Differences between `zypper update` and `zypper dist-upgrade`

Choose `zypper update` to update packages to newer versions available for your product version while maintaining system integrity. `zypper update` will honor the following rules:

- no vendor changes

- no architecture changes

- no downgrades

- keep installed packages

To upgrade your installation to a new product version use `zypper dist-upgrade` with the required repositories (see Section 2.1.2.4, "Managing Repositories with Zypper" (page 18) for details). This command ensures that all packages will be installed from the repositories currently enabled. This rule is enforced, so packages might change vendor or architecture or even might get downgraded. All packages that have unfulfilled dependencies after the upgrade will be uninstalled.

2.1.2.4 Managing Repositories with Zypper

All installation or patch commands of Zypper rely on a list of known repositories. To list all repositories known to the system, use the command:

```
zypper repos
```

The result will look similar to the following output:

```
# | Alias                       | Name                           -
    | Enabled | Refresh
—+—————————————————————————————+—————————————————————————————————+—————————+———————
1 | SUSE-Linux-Enterprise-Server 11-0 | SUSE-Linux-Enterprise-Server  -
11-0 | Yes      | No
2 | SLES-11-Updates             | SLES 11 Online Updates          -
```

```
   | Yes     | Yes
3 | broadcomdrv                  | Broadcom Drivers         —
   | Yes     | No      —
```

When specifying repositories in various commands, an alias, URI or repository number from the `zypper repos` command output can be used. Note however that the numbers can change after modifying the list of repositories. The alias will never change by itself.

By default, details such as the URI or the priority of the repository are not displayed. Use the following command to list all details:

```
zypper repos -d
```

Adding Repositories

To add a repository, run

```
zypper addrepo URI Alias
```

URI can either be an Internet repository, a network resource, a directory or a CD or DVD (see http://en.opensuse.org/Libzypp/URI for details). The *Alias* is a shorthand and unique identifier of the repository. You can freely choose it, with the only exception that is has to be unique. Zypper will issue a warning if you specify an alias that is already in use. Use short and easy-to-remember aliases for your own convenience.

Removing Repositories

If you want to remove a repository from the list, use the command `zypper removerepo` together with the alias or number of the repository you want to delete. To remove the 3rd entry from the example, use the following command:

```
zypper removerepo 3
```

Modifying Repositories

Enable or disable repositories with `zypper modifyrepo`. You can also alter the repository's properties (such as refreshing behavior, name or priority) with this command. The following command will enable the repository name "updates", turn on auto-refresh and set it's priority to 20:

```
zypper mr -er -p 20 'updates'
```

Modifying repositories is not limited to a single repository—you can also operate on groups:

- `-a`: all repositories

- `-l`: local repositories

- `-t`: remote repositories

- `-m` *TYPE*: repositories of a certain type (*TYPE* can be one of the following: http, https, ftp, cd, dvd, dir, file, cifs, smb, nfs, hd, iso)

To rename a repository alias, use the `renamerepo` command. The following example changes the alias from "Mozilla Firefox" to just "firefox":

```
zypper renamerepo 'Mozilla Firefox' firefox
```

2.1.2.5 Querying Repositories and Packages with Zypper

Zypper offers various methods to query repositories or packages. To get lists of all products, patterns, packages or patches available, use the following commands:

```
zypper products
zypper patterns
zypper packages
zypper patches
```

To query all repositories for certain packages, use `search`. It works on package names, capabilities or, optionally, on package summaries and descriptions. Using the wildcards * and ? in the search term is allowed. By default, the search is not case-sensitive.

```
zypper se firefox       # simple search for "firefox"
zypper se '*fire*'      # using wildcards
zypper se -d fire       # also search in package descriptions and summaries
zypper se -u firefox    # only display packages not already installed
```

To search for packages which provide a special capability, use the command `what-provides`. For example, if you would like to know which package provides the perl Module `SVN::Core`, use the following command:

```
zypper what-provides 'perl(SVN::Core)'
```

To query single packages, use `info` with an exact package name as an argument. It displays detailed information about a package. Use the options `--requires` and `--recommends` to also show what is required/recommended by the package:

```
zypper info --requires MozillaFirefox
```

The `what-provides` *package* is similar to `rpm -q --whatprovides` *package*, but rpm is only able to query the RPM database (that is the database of all installed packages). Zypper, on the other hand, will tell you about providers of the capability from any repository, not only those that are installed.

2.2 Updating Packages on RHEL 5

Depending on your version of Red Hat Enterprise Linux, systems registered with SUSE Manager can update client systems directly using various tools and applications installed on the system. For Red Hat Enterprise Linux 5, you can use the Package Updater (or `pup`) to keep systems updated.

The Package Updater (`pup`) is the desktop update application for Red Hat Enterprise Linux 5. Using this tool, you can update packages and read information about the updated packages, such as bug fix details, security alerts, enhancements, and more.

2.2.1 Using the Package Updater

To start the Package Updater from the desktop, open *Applications* (main menu on the panel), then click *System Tools > Package Updater*.

If you are at a shell prompt window, type `pup` to open the Package Updater.

Figure 2.4 *Package Updater Interface*
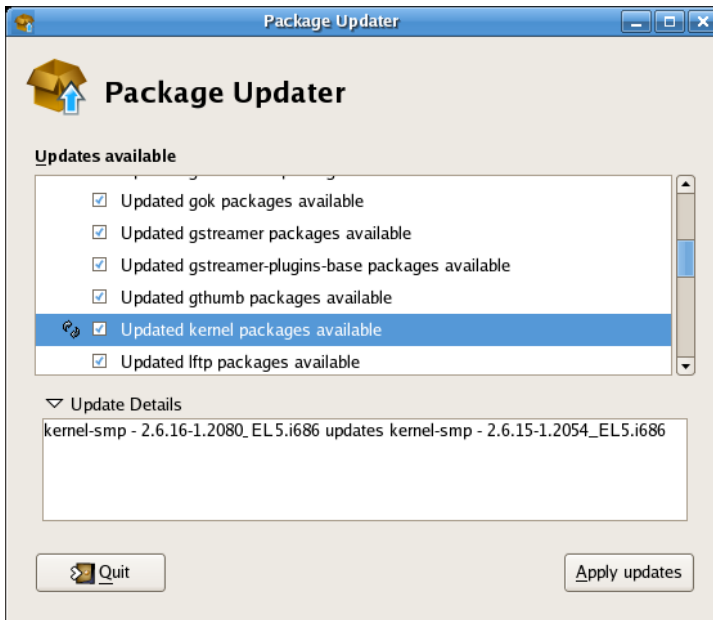
If there are multiple package updates, they will be listed with checkmarks next to them so that you can choose which files to update. Some packages (for example, kernel packages) may have a circular arrow icon next to them, indicating that you are required to reboot your system after updating the package.

To view the update details of any package, highlight the package and click the arrow next to *Update Details*.

When you are ready to update the packages, click *Apply updates*. The Updater will re-solve any dependencies, and notify you when a package must be installed to meet a dependency for an updated package.

Figure 2.5 *Package Dependency*
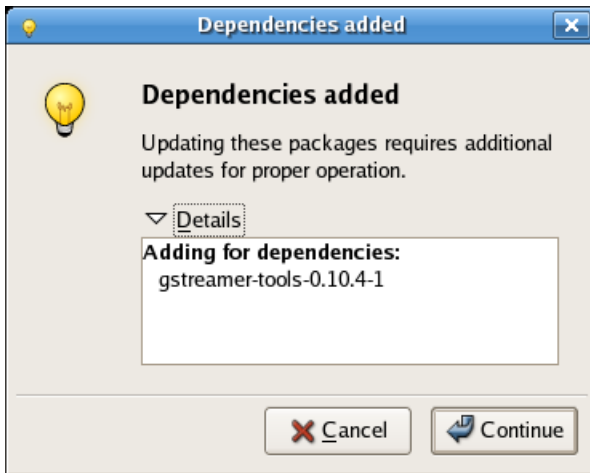
Click *Continue* to accept the dependency and resume the update.

If this is the first time you're using the Package Updater, the program will prompt you to imort the Red Hat GPG security key that verifies that a package has been signed and is certified for Red Hat Enterprise Linux.

Click *Import Key* to accept the Key and continue with the update.

When the update completes, you may be prompted to reboot your system for the changes to take effect.

Figure 2.6 *Reboot Prompt*

You can choose to reboot now or later, but it is recommended to click *Reboot Now* to start using the updated packages.

2.2.2 The Package Updater Applet

Red Hat Enterprise Linux 5 also features an applet on the graphical desktop panel that periodically checks for updates from the SUSE Manager server and will alert users when a new update is available.

Figure 2.7   *Package Updater Applet*
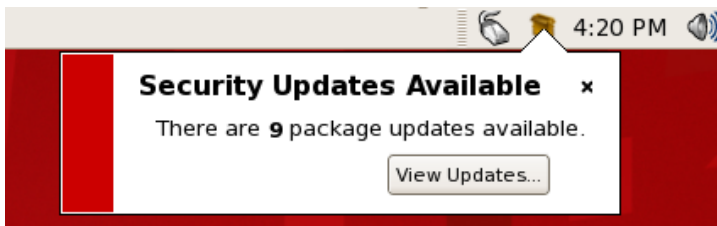
The Package Updater applet stays in the notification tray of the desktop panel and checks for new updates periodically. The applet also allows you to perform basic package maintenance tasks by clicking the notification icon and choosing from the following actions:

- *Refresh* — Check SUSE Manager for new updates

- *View Updates* — launches the Package Updater application so that you can see any available updates in more detail and configure the updates to your specifications

- *Apply Updates* — Download and Install all updated packages.

- *Quit* — close the applet

2.2.3 Updating Packages from the Command Line with yum

The foundation of the Package Updater is the Yum package manager, developed by Duke University. yum searches supported repositories for packages and their dependen-

cies so they may be installed together in an effort to alleviate dependency issues. Red Hat Enterprise Linux 5 uses `yum` to fetch and install packages.

`up2date` is not available on Red Hat Enterprise Linux 5. The entire stack of update and installation tools is now based on Yum.

2.2.3.1 yum Commands

Yum commands are typically typed as follows:

```
yum command [package_name]
```

By default, Yum will automatically attempt to check all configured repositories to resolve all package dependencies during an installation or upgrade. The following is a list of the most commonly-used `yum` commands. For a complete list of available yum commands, refer to `man yum`.

`yum install package_name`
> Installs the latest version of a package or group of packages. If no package matches the specified package name, the name is treated as a shell wildcard. In this case, all matches are installed.

`yum update package_name`
> Updates the specified packages to the latest available version. If no packages are specified, `yum` will attempt to update all installed packages.
>
> If the `--obsoletes` option is used (i.e. `yum --obsoletes package_name`), yum will process obsolete packages. Packages that are obsoleted across updates will be removed and replaced accordingly.

`yum check-update`
> This command determines whether updates are available for your installed packages. `yum` returns a list of all package updates from all repositories where updates are available.

`yum remove package_name`
> Removes specified packages and along with it all dependent packages.

`yum provides package_name`
> Determines which packages provide a specific file or feature.

yum search `keyword`
> This command finds any packages containing the specified keyword in the description, summary, packager and package name fields of RPMs in all supported repositories.

yum localinstall `absolute path to filename`
> Installs a local package stored on your system.

2.3 Red Hat Update Agent (RHEL 4)

The Red Hat Update Agent is your connection to SUSE Manager on Red Hat Enterprise Linux 4. It enables you to register your systems, create *System Profiles*, and alter the settings for the interaction between organization and SUSE Manager. Once registered, your systems can use the Red Hat Update Agent to retrieve the latest software packages. This tool allows you to always have the most up-to-date Red Hat Enterprise Linux systems with all security updates, bug fixes, and software package enhancements.

Remember, this tool must be run on the system you wish to update. This system must be entitled to a SUSE Manager service offering.

WARNING

Customers with Expanded Support using SUSE Manager must be entitled to retrieve updates to their Red Hat Enterprise Linux system via Novell Customer Center. Installing the Red Hat GPG key is also required. For more information, refer to Section 2.3.3.1, "Installing the Red Hat GPG key" (page 36).

2.3.1 Starting the Red Hat Update Agent

If you are not running the X Window System or prefer the command line version of the Red Hat Update Agent, skip to Section 2.3.3, "Command-Line Version" (page 31).

You must be root to run the Red Hat Update Agent. If started as a standard user, Red Hat Update Agent prompts you to enter the root password before proceeding. The Red Hat Update Agent can be started as follows:

- For Red Hat Enterprise Linux 5: At a shell prompt (for example, an xterm or gnome-terminal), type the command `system-config-packages`.

- For Red Hat Enterprise Linux 4: At a shell prompt (for example, an xterm or gnome-terminal), type the command `up2date`.

If you start the application from a shell prompt, you can specify the options in Table 2.1, "Graphical Update Agent Options" (page 27). To view these options, type the command `up2date --help`. For example, use the following command to specify the directory in which to download the updated packages (temporarily overriding your saved configuration):

`up2date --tmpdir=/tmp/up2date/`

Table 2.1 *Graphical Update Agent Options*

Option	Description
`--configure`	Configure Red Hat Update Agent options. Refer to Section 2.3.4, "Configuration" (page 38) for detailed instructions.
`-d, --download`	Download packages; do not install them. This argument temporarily overrides the configuration option *Do not install packages after retrieval.* Use this option if you prefer to install the packages manually.
`-f, --force`	Force package installation. This option temporarily overrides the file, package, and configuration skip lists.
`-i, --install`	Install packages after they are downloaded. This argument temporarily overrides the configuration option *Do not install packages after retrieval.*

Option	Description
-k, --packagedir	Specify a colon separated path of directories in which to look for packages before trying to download them.
--nosig	Do not use GPG to check package signatures. This option temporarily overrides the saved configuration option.
--tmpdir=*directory*	Temporarily override the configured package directory. The default location is /var/spool/up2date. This option is useful if you do not have enough space in the default or configured location.
--dbpath=*dir*	Specify an alternate RPM database to use temporarily.

The first time you run the Red Hat Update Agent, two dialog boxes appear that you will not see in subsequent startups: *Configure Proxy Server* and *Install GPG Key*.

The first dialog box prompts you for HTTP Proxy Server information. This is useful if your network connection requires you to use a proxy server to make HTTP connections. To use this feature, select the *Enable HTTP Proxy* checkbox and type your proxy server in the text field with the format HOST:PORT, such as squid.mysite.org:3128. Additionally, if your proxy server requires a username and password, select the *Use Authentication* checkbox and enter your username and password in the respective text fields.

An HTTP Proxy Server is not required by SUSE Manager. If you do not want to use this feature, click the *OK* button without making any selections.

The second dialog box prompts you to install the Red Hat GPG key. This key is used to verify the packages you download for security purposes. Click *Yes* to install the key, and you will not see this message again.

2.3.2 Registration

Before you can install or update packages from SUSE Manager, you must create a username, password, and *System Profile*. If the system is not yet registered, Red Hat Update Agent guides you through the registration process.

If you need to force the Red Hat Update Agent into registration mode to re-register a system issue the following command:

```
up2date --register
```

IMPORTANT

If your username is part of a larger organizational account, you should take care when registering systems. By default, all systems registered with the Red Hat Update Agent end up in the Ungrouped section of systems visible only to SUSE Manager administrators. To ensure you retain management of these systems, your organization is recommended to create an activation key associated with a specific system group and grant you permissions to that group. You may then register your systems using that activation key and find those *System Profiles* within SUSE Manager immediately. Refer to Section 2.3.5, "Registering with Activation Keys" (page 42) for instructions.

After installing the Red Hat GPG Key, the Welcome screen appears. Click *Forward* to continue.

2.3.2.1 Channels

Next, Red Hat Update Agent displays all package channels to which you have access. The channels you select from this screen must match the base operating system of the machine you are registering. If any child channels are available, you may select them as well. Additional information regarding the selected channel is displayed in the *Channel Information* pane. When finished, click *Forward* to continue.

Red Hat Update Agent now compares the packages in your RPM database with those available from the channel you selected. The progress bar is displayed during this process.

2.3.2.2 Packages Flagged to be Skipped

The next step in the initial update is the selection of files to be skipped. Any packages checked here will not be downloaded and updated by the Red Hat Update Agent. This screen is displayed whenever packages are available that are currently selected to be ignored.

Make your selections and click *Forward* to continue.

2.3.2.3 Available Package Updates

Next, the Red Hat Update Agent displays all available updates except those you chose to skip in the previous screen. Select those you wish to download and click *Forward* to continue. To view the complete Patch (Errata) Advisory text for an update, highlight the relevant package and click the *View Advisory* button. When finished, click *OK*.

Select those you wish to download and click *Forward* to continue.

Figure 2.8   *Available Package Updates*
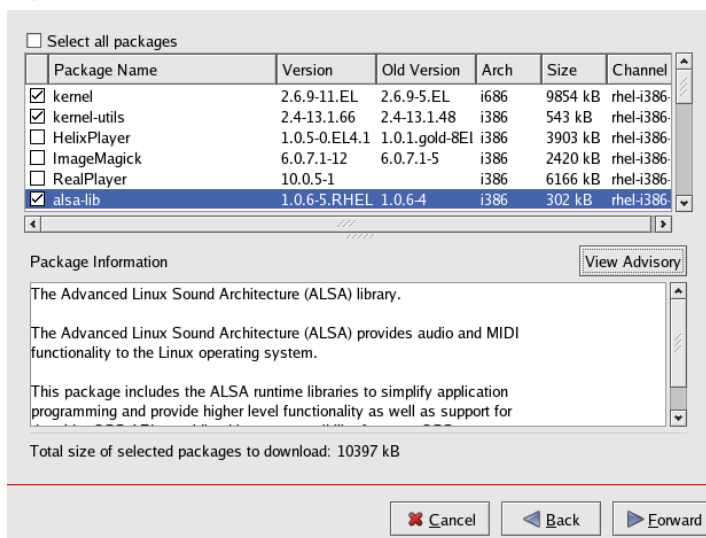
2.3.2.4 Retrieving Packages

The Red Hat Update Agent checks the packages you selected to ensure that all requirements of each RPM are met. If any additional packages are required, Red Hat Update Agent displays an error message. Click *OK* to continue.

Once all dependencies are fulfilled, Red Hat Update Agent retrieves the packages from SUSE Manager. As the packages are downloaded, they are temporarily stored in `/var/spool/up2date/`.

When all packages have been downloaded, click *Forward* to continue.

2.3.2.5 Installing Packages

The packages must be installed after downloading them via the Red Hat Update Agent. If you chose not to install the downloaded packages, refer to Section 2.3.3.2, "Manual Package Installation" (page 36) for further instructions. If you configured the Red Hat Update Agent to install the packages (the default setting), the installation process begins. The progress of installing each package, as well as the total progress, is displayed. When the packages have been installed, click *Forward* to continue.

Click *Finish* to exit the Red Hat Update Agent.

2.3.3 Command-Line Version

If you are not running X, you can still run the Red Hat Update Agent from a virtual console or remote terminal. If you are running X but prefer the command-line version, you can force it not to display the graphical interface with the following command:

```
up2date --nox
```

The command-line version of the Red Hat Update Agent allows you to perform advanced functions or to perform actions with little or no interaction. For example, the following command updates your system with no interaction. It downloads newer packages and installs them if you configured it to do so.

```
up2date -u
```

The following arguments are accepted:

Table 2.2 *Update Agent Command-Line Arguments*

Option	Description
`-?, --usage`	Briefly describes the available options.
`-h, --help`	Lists the available options and exits.
`--arch=`*architecture*	Forces `up2date` to install this architecture of the package. Not valid with `--update, --list,` or `--dry-run`.
`--channel=`*channel*	Specifies from which channels to update using channel labels.
`--configure`	Configures Red Hat Update Agent options. Refer to Section 2.3.4, "Configuration" (page 38) for detailed instructions.
`-d, --download`	Downloads packages only without installing them. This argument temporarily overrides the configuration option *Do not install packages after retrieval.* Use this option if you prefer to install the packages manually.
`--dbpath=`*dir*	Specifies an alternate RPM database to use temporarily.
`--dry-run`	Does everything but download and install packages. This is useful in checking dependencies and other requirements prior to actual installation.
`-f, --force`	Forces package installation. This option temporarily overrides the file, package, and configuration skip lists.

Option	Description
`--firstboot`	Pops up in the center of the screen for Firstboot.
`--get`	Fetches the package specified without resolving dependencies.
`--get-source`	Fetches the source package specified without resolving dependencies.
`--gpg-flags`	Shows the flags with which GPG is invoked, such as the keyring.
`--hardware`	Updates the system's hardware profile on SUSE Manager.
`-i, --install`	Installs packages after they are downloaded. This argument temporarily overrides the configuration option *Do not install packages after retrieval*.
`--installall=<channel-label>`	Installs all available packages from a given channel
`--justdb`	Only adds packages to the database and does not install them.
`-k, --packagedir`	Specifies a colon-separated path of directories in which to look for packages before trying to download them.
`-l, --list`	Lists packages relevant to the system.
`--list-rollbacks`	Shows the package rollbacks available.
`--nodownload`	Does not download packages at all. This is useful in testing.

Option	Description
`--nosig`	Does not use GPG to check package signatures. This option temporarily overrides the saved configuration option.
`--nosrc`	Does not download source packages (SRPMs).
`--nox`	Does not attempt to run in X. This launches the command line version of the Red Hat Update Agent.
`-p, --packages`	Updates packages associated with this System Profile.
`--proxy=proxy URL`	Specifies an HTTP proxy to use.
`--proxyPassword=proxy password`	Specifies a password to use with an authenticated HTTP proxy.
`--proxyUser=proxy user ID`	Specifies a username to use with an authenticated HTTP proxy.
`--register`	Registers (or re-registers) this system with SUSE Manager. Refer to Section 2.3.2, "Registration" (page 29) for detailed instructions.
`--serverUrl=server URL`	Specifies an alternative server from which to retrieve packages.
`--showall`	Lists all packages available for download.
`--show-available`	Lists all packages available that are not currently installed.

Option	Description
`--show-channels`	Shows the channel name associated with each package.
`--show-orphans`	Lists all packages currently installed that are not in channels to which the system is subscribed.
`--show-package-dialog`	Shows the package installation dialog in GUI mode.
`--solvedeps=dependencies`	Finds, downloads, and installs the packages necessary to resolve dependencies.
`--src`	Downloads source packages, as well as binary RPMs.
`--tmpdir=directory`	Temporarily overrides the configured package directory. The default location is `/var/spool/up2date`. This option is useful if you do not have enough space in the configured location.
`-u, --update`	Updates system with all relevant packages.
`--undo`	Reverses the last package set update.
`--upgrade-to-release=release version`	Upgrades to the channel specified.
`--uuid=uuid`	Passes on a Unique User ID generated by the Alert Notification tool.
`-v, --verbose`	Shows additional output while updating.

Option	Description
`--version`	Shows `up2date` version information.
`--whatprovides=`*`dependencies`*	Shows the packages that resolve the comma-separated list of dependencies.

NOTE

The `--solvedeps` and `--whatprovides` options can be used to solve the dependencies for an RPM, even if your system does not currently have access to a channel that contains that package.

2.3.3.1 Installing the Red Hat GPG key

The first time you run the graphical version of the Red Hat Update Agent, it prompts you to install the Red Hat GPG key. This key is required to authenticate the packages downloaded from Red Hat Network. If you run the command-line version the first time you start Red Hat Update Agent, you must install the Red Hat GPG key manually. If you do not have it installed, you will see the following message:

```
Your GPG keyring does not contain the Red Hat, Inc. public key.
Without it, you will be unable to verify that packages Update Agent downloads
are securely signed by Red Hat.
```

```
[...]
```

NOTE

GPG keys must be installed for each user. To install the key with SUSE Manager, import the key while logged in as root.

Issue the following command at a shell prompt as root:

```
rpm --import /usr/share/rhn/RPM-GPG-KEY
```

2.3.3.2 Manual Package Installation

If you chose to download, but not install, the software updates with the Red Hat Update Agent, you must install them manually using RPM.

To install them, change to the directory that contains the downloaded packages. The default directory is `/var/spool/up2date`. Type the command `rpm -Uvh *.rpm`. When the packages finish installing, you can delete the RPM files. You do not need them anymore.

After installing the packages, you must update your System Profile so that you are not prompted to download them again. Refer to Section 2.3.3.3, "Synchronizing Your System Profile" (page 37) for details.

2.3.3.3 Synchronizing Your System Profile

If you configured the Red Hat Update Agent to install the latest packages, the System Profile stored by SUSE Manager is updated after the packages are installed. However, if you only downloaded the latest RPM packages using the Red Hat Update Agent, downloaded the RPM packages from the website, or upgraded, installed, or removed RPM packages manually, your System Profile is not updated automatically. You must send your updated System Profile to the SUSE Manager server.

To synchronize the RPM package list on your local Red Hat Enterprise Linux 5 system, run the command:

```
rhn-profile-sync
```

After running this command, your SUSE Manager System Profile reflects the latest software versions installed on your system.

For Red Hat Enterprise Linux 4 systems, use the following command to update the package list:

```
up2date -p
```

2.3.3.4 Log File

The Red Hat Update Agent keeps a log of all the actions that it performs on your system in the file `/var/log/up2date`. It uses the standard logrotate method. Thus, older logs are in `/var/log/up2date.1`, `/var/log/up2date.2`, and `/var/log/up2date.3`. The log files store actions performed by the Red Hat Update Agent, for example when your RPM database is opened, when it connects to SUSE Manager to retrieve information from your system profile, which packages are downloaded, which packages are installed using the Red Hat Update Agent, and which packages are deleted

from your system after installation. If you choose to install and delete packages yourself, this is not logged in this file. It is recommended that you keep a log of actions not performed with the Red Hat Update Agent.

2.3.4 Configuration

The Red Hat Update Agent offers various options to configure its settings.

If you are not running the X Window System or prefer the command line version, skip to Section 2.3.4.2, "Command-Line Version" (page 41).

2.3.4.1 Using the Red Hat Update Agent Configuration Tool

You must be root to run the Red Hat Update Agent Configuration Tool. If started by a user other than root, the Red Hat Update Agent prompts you for the root password. The Red Hat Update Agent Configuration Tool can be started by typing the command `up2date --config` at a shell prompt (for example, an xterm or a gnome-terminal).

General Settings

The *General* tab allows you to enable an HTTP Proxy Server. If your network connection requires you to use an HTTP Proxy Server to make HTTP connections, select the *Enable HTTP Proxy* option and type your proxy server in the text field with the format http://HOST:PORT. For example, to use the proxy server squid.mysite.org on port 3128, you would enter `squid.mysite.org:3128` in the text field. Additionally, if your proxy server requires a user name and password, select the *Use Authentication* option and enter your user name and password in the respective text fields.

Retrieval/Installation Settings

The *Retrieval/Installation* tab allows you to customize your software package retrieval and package installation preferences.

Figure 2.9 *Retrieval/Installation Settings*
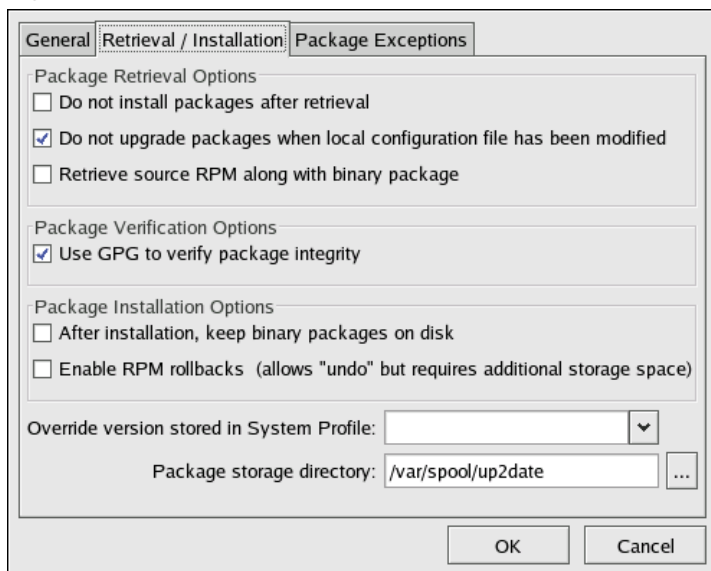
The following package retrieval options can be selected (see Figure 2.9, "Retrieval/Installation Settings" (page 39)):

- *Do not install packages after retrieval* — Download selected RPM packages to the specified directory and ignore the installation preferences.

- *Do not upgrade packages when local configuration file has been modified* — If the configuration file has been modified for a package such as apache or squid, do not attempt to upgrade it. This option is useful if you are installing custom RPMs on your system and you do not want them updated or reverted to the default Red Hat Enterprise Linux packages.

- *Retrieve source RPM along with binary package* — Download both the source (*.src.rpm) and the binary (*.[architecture].rpm) files.

The following installation options are configurable (see Figure 2.9, "Retrieval/Installation Settings" (page 39)):

- *Use GPG to verify package integrity* — Before installing packages, verify Red Hat's GPG signature (highly recommended for security reasons).

- *After installation, keep binary packages on disk* — Save binary packages in the specified directory instead of deleting them after installation.

The following additional options are configurable from this tab:

- *Override version stored in System Profile* — Override the Red Hat Linux version in your system profile.

- *Package storage directory* — Change the directory where packages are downloaded; the default location is `/var/spool/up2date/`.

Package Exceptions Settings

The *Package Exceptions* tab allows you to define which packages to exclude from the list of RPM packages to be updated by package or file name (see Figure 2.10, "Package Exceptions Settings" (page 41)).

To define a set of packages to be excluded by package name, enter a character string including wild cards (*) in the *Add new* text field in the *Package Names to Skip* section. A wild card at the end of the character string indicates that all packages beginning with the character string are excluded from the list. A wild card at the beginning of the character string indicates that any packages that end with the character string are excluded from the list.

For example, if the string `kernel*` is in the *Package Names to Skip* section, the Red Hat Update Agent will not display any packages beginning with kernel.

To exclude packages by file name, apply the same rules to the field below *File Names to Skip*.

Figure 2.10 *Package Exceptions Settings*
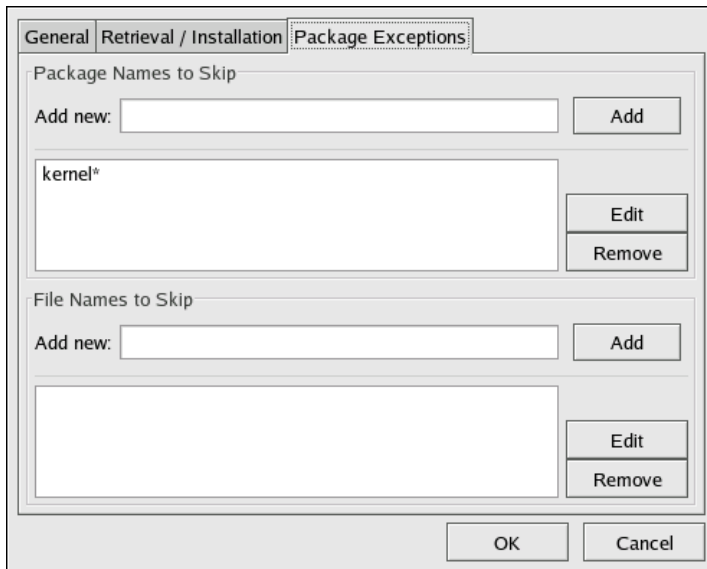
2.3.4.2 Command-Line Version

The command-line version of the Red Hat Update Agent performs the same function as the graphical version. It allows you to configure the settings and stores them in the configuration file /etc/sysconfig/rhn/up2date.

To run the command-line version, use the following command:

```
up2date --nox --configure
```

You are presented with a list of options and their current values:

```
0.  adminAddress       ['root@localhost']
1.  debug              No
2.  disallowConfChange ['noReboot', 'sslCACert', 'useNoSSLForPackages',
3.  enableProxy        No
4.  enableProxyAuth    No
5.  enableRollbacks    No
6.  fileSkipList       []
7.  forceInstall       No
8.  gpgKeyRing         /etc/sysconfig/rhn/up2date-keyring.gpg
9.  headerCacheSize    40
10. headerFetchCount   10
11. httpProxy
12. isatty             Yes
```

```
13. keepAfterInstall    No
14. networkRetries      5
15. noBootLoader        No
16. noReboot            No
17. noReplaceConfig     Yes
18. noSSLServerURL      http://xmlrpc.rhn.redhat.com/XMLRPC
19. pkgSkipList         ['kernel*']
20. pkgsToInstallNotUp  ['kernel', 'kernel-modules', 'kernel-devel']
21. proxyPassword
22. proxyUser
23. removeSkipList      ['kernel*']
24. retrieveOnly        No
25. retrieveSource      No
26. rhnuuid             a8aea05c-f174-11df-af94-55bad1b1e05f
27. serverURL           http://ix64ph001.example.com/XMLRPC
28. showAvailablePacka  No
29. sslCACert           /usr/share/rhn/RHNS-CA-CERT
30. storageDir          /var/spool/up2date
31. systemIdPath        /etc/sysconfig/rhn/systemid
32. updateUp2date       Yes
33. useGPG              Yes
34. useNoSSLForPackage  No
35. useRhn              Yes
36. versionOverride

Enter number of item to edit <return to exit, q to quit without saving>:
```

Enter the number of the item to modify and set a new value for the option. When you finish changing your configuration, press Enter to save your changes and exit. Press q then Enter to quit without saving your changes.

IMPORTANT

Note that the port used by the Red Hat Update Agent is 443 for SSL (HTTPS) and 80 for non-SSL (HTTP). These ports cannot be changed. By default, up2date uses SSL only. For this reason, users should ensure that their firewalls allow connections over port 443. To bypass SSL, change the protocol for serverURL from https to http in the /etc/sysconfig/rhn/up2date configuration file.

2.3.5 Registering with Activation Keys

In addition to the standard Red Hat Update Agent interface, up2date offers a utility aimed at batch processing system registrations: activation keys. Each unique key can be used to register Red Hat Enterprise Linux systems, entitle them to a SUSE Manager

service level, and subscribe them to specific channels and system groups, all in one action.

Alternatively, both the Red Hat Network Registration Client and Red Hat Update Agent offer the activation keys utility `rhnreg_ks` as part of their packages.

Before using an activation key you must first generate one through the SUSE Manager website. Refer to Section 4.4.6, "Activation Keys — [Mgmt]" (page 99) for precise steps.

To use an activation key, run the following command as root from a shell prompt on the system to be registered:

```
rhnreg_ks --activationkey=7202f3b7d218cf59b764f9f6e9fa281b
```

The precise value of the activation key varies.

In addition, provisioning-entitled systems may use multiple activation keys at once, either at the command line or in Kickstart profiles. This allows administrators to include a series of key separated by commas, for example:

```
rhnreg_ks --activationkey=7202f3b7d218cf59b764f9f6e9fa281b,\
39f41081f0329c20798876f37cb9p6a3
```

NOTE

The trailing backslash (\) in this command example is a continuation character; omit it and write all keys in one line.

Refer to Section 4.4.6.2, "Using Multiple Activation Keys at Once — [Prov]" (page 102) to understand how differences in activation keys are handled.

The above command performs all the actions of the Registration Client and the registration function of the Red Hat Update Agent. Do not run either of these applications for registration after running `rhnreg_ks`.

A System Profile, including software and hardware information, is created for the system and sent to the SUSE Manager server along with the unique activation key. The system is registered with SUSE Manager under the account used to generate the key, entitled to a SUSE Manager service offering, and subscribed to the SUSE channels and system groups selected during key generation. The system cannot subscribe to channels that

contain packages unsuitable for the system. For example, a Red Hat Enterprise Linux 4 system cannot to subscribe to the Red Hat Enterprise Linux 5 channel.

The unique Digital Certificate for the system is generated on the system in the file /etc/sysconfig/rhn/systemid.

When using activation keys to assign channels, follow these rules:

• A key may specify either zero or one base channel. If specified, it must be a custom base channel. If not, the base channel corresponding to the system's Red Hat distribution is chosen.

• A key may specify any number of child channels. For each child channel, subscription is attempted. If the child channel matches the system's base channel, subscription succeeds. If it does not, the subscription fails silently. Refer to Section 4.6, "Channels" (page 131) for more information.

• Keys may be modified by any user with the role of Activation Key Administrator or SUSE Manager Administrator. These permissions are set in the *Users* tab of the SUSE Manager website. Refer to Section 4.9, "Users — [Mgmt]" (page 150) for details.

• Systems registered with activation keys are tied to the organization account in which the key was created, not the key itself. After registration, a key can be deleted safely without any effect on the systems it was used to register.

2.3.6 Registering a System to an Organization

SUSE Manager supports the Organizations feature, which allows administrators to distribute software and system entitlements across various organizations, as well as control an organization's access to systems management. Systems can be registered directly with an organization.

To register a system with an organization on a SUSE Manager server, you can use the username and password of an account that is created within that organization. For example, if there is an organization called *Sales Team*, with a username salesadmin and password abc123, using these credentials assures that a system is registered with the proper organization.

For example:

```
rhnreg_ks --user=salesadmin --password=abc123
```

> **IMPORTANT**
>
> The --orgid option (for RHEL 4 and 5) and the --orgpassword option (in RHEL 4) in the rhnreg_ks command *are not related* to the Organizations feature and should not be used in the context of registering systems with organizations.

For more information about the Organizations feature, refer to Section 4.11.1, "*Admin > Organizations*" (page 165).

SUSE Manager Daemon

3

The SUSE Manager daemon (`rhnsd`) runs on the client systems and periodically connects to SUSE Manager to check for updates and notifications. The daemon, which runs in the background, is typically started by the `rcrhnsd` initialization script.

To check for updates, `rhnsd` runs the external `mgr_check` program located in `/usr/sbin/`. This is a small application that makes the network connection to SUSE Manager. The SUSE Manager daemon does not listen on any network ports or talk to the network directly. All network activity is done via the `mgr_check` utility.

3.1 Configuring

The SUSE Manager daemon can be configured by editing the `/etc/sysconfig/rhn/rhnsd` configuration file. This is actually the configuration file the `rhnsd` initialization script uses. The most important setting for the daemon is its check-in frequency. The default interval time is four hours (240 minutes). If you modify the configuration file, you must (as `root`) restart the daemon with the command `rcrhnsd restart`.

> **IMPORTANT**
>
> The minimum time interval allowed is one hour (60 minutes). If you set the interval below one hour, it will default to four hours (240 minutes).

3.2 Viewing Status

You can view the status of the rhnsd by typing the command `rcrhnsd status` at a shell prompt.

3.3 Disabling Service

To disable the daemon, (as `root`) run the command `chkconfig rhnsd off`. Using this method only disables the service the next time the system is started. To stop the service immediately, use the command `rcrhnsd stop`.

3.4 Troubleshooting

If you see messages in the SUSE Manager Web interface indicating that check-ins are not taking place, the SUSE Manager client is not successfully reaching SUSE Manager. Make sure that:

• your client is configured correctly,

• your system can communicate with SUSE Manager via SSL (port 443). You may test this by running the following command from a shell prompt:

```
telnet xmlrpc.example.com 443
```

• the SUSE Manager daemon is activated and running. Ensure it by running:

```
chkconfig --level 345 rhnsd on
rcrhnsd start
```

SUSE Manager Web Interface

4

Use the SUSE Manager Web interface to manage multiple SUSE Linux Enterprise and Red Hat Enterprise Linux systems simultaneously, including viewing alerts, applying updates, patches and security fixes, and installing software packages. This chapter explains all categories, pages, and tabs within the Web interface and how to use them.

4.1 Navigation

The top navigation bar is divided into tabs. SUSE Manager Administrators see Figure 4.1, "Top Navigation Bar—SUSE Manager" (page 49) as the top navigation bar. Note that only SUSE Manager Administrators see the *Monitoring* and *Admin* tabs.

Figure 4.1   *Top Navigation Bar—SUSE Manager*

The left navigation bar is divided into pages. The links are context-sensitive. The Figure 4.2, "Left Navigation Bar—Users" (page 49) is an example of the left navigation bar for the *Users* tab.

Figure 4.2   *Left Navigation Bar—Users*

Some pages have subtabs. These tabs offer an additional layer of granularity in performing tasks for systems or users. Figure 4.3, "Subtabs—System Details" (page 50) is a menu bar for all *System Details* subtabs. This system has Management and Provisioning entitlements, but not Monitoring.

Figure 4.3 *Subtabs—System Details*

Details	Software	Configuration	Provisioning	Groups	Events

Overview	Properties	Remote Command	Reactivation	Hardware	Migrate	Notes	Custom Info
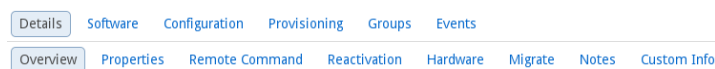
4.1.1 Entitlement Views

Keep in mind, since this guide covers all entitlement levels, some tabs, pages, and even whole categories described here may not be visible to you. For this reason, text markers are used here to identify, which functions are available to each entitlement level.

Table 4.1 *Entitlement Markers*

Marker	Entitlement
[Mgmt]	Management or higher
[Prov]	Provisioning
[Mon]	Monitoring

If no marker follows a category, page, or tab label, the area described is available to all SUSE Manager users. If a marker follows, the associated entitlement is required. Provisioning inherits all the functions of Management. Management features are visible to users with Provisioning entitlement, but not vice versa.

If a marker precedes a paragraph, only the part of the page or tab discussed afterwards requires the indicated entitlement level. When a page or tab is associated with a particular entitlement level, all of its tabs and subtabs require at least the same entitlement level but may need a higher entitlement. Regardless, each tab is identified separately.

4.1.2 Categories and Pages

This section summarizes all of the categories and primary pages (those linked from the top and left navigation bars) within the SUSE Manager Web interface. It does not list the many subpages, tabs and subtabs accessible from the left navigation bar and individual pages. Each area of the website is explained in detail later in this chapter.

- *Overview* — View and manage your primary account information and get help.

    - *Overview* — Obtain a quick overview of your account. This page notifies you if your systems need attention, provides a quick link directly to these systems, and displays the most recent patch alerts for your account.

    - *Your Account* — Update your personal profile and addresses.

    - *Your Preferences* — Indicate if you wish to receive e-mail notifications about available patches for your systems. Set how many items are displayed in system and group lists, set your time zone, and manage your contact options.

    - *Subscription Management* — Manage base and add-on system entitlements, such as Management, Provisioning, and Virtualization.

    - *Organization Trusts* — Display the trusts established with your organization.

- *Systems* — Manage all your systems (including virtual guests) here.

    - *Overview* — [Mgmt] — View a summary of your systems or system groups showing how many available patches each system has and which systems are entitled.

    - *Systems* — Select and view subsets of your systems by specific criteria, such as Virtual Systems, Unentitled, Recently Registered, Proxy, and Inactive.

    - *System Groups* — [Mgmt] — List your system groups. Create additional groups.

    - *System Set Manager* — [Mgmt] — Perform various actions on sets of systems, including scheduling patch updates, package management, listing and creating new groups, and managing channel entitlements.

- *Advanced Search* — [Mgmt] — Quickly search all your systems by specific criteria, such as name, hardware, devices, system info, networking, packages, and location.

- *Activation Keys* — [Mgmt] — Generate an activation key for a SUSE Manager-entitled system. This activation key can be used to grant a specific level of entitlement or group membership to a newly registered system using the `rhnreg_ks` command.

- *Stored Profiles* — [Prov] — View system profiles used to provision systems.

- *Custom System Info* — [Prov] — Create and edit system information keys with completely customizable values assigned while provisioning systems.

- *Autoinstallation* — [Prov] — Display and modify various aspects of autoinstallation profiles (Kickstart and AutoYaST) used in provisioning systems.

- *Patches* — View and manage patch (errata) alerts here.

  - *Patches* — Lists patch alerts and downloads associated RPMs.

  - *Advanced Search* — Search patch alerts based on specific criteria, such as synopsis, advisory type, and package name.

  - *Manage Patches* — Manage the patches for an organization's channels.

  - *Clone Patches* — Clone patches for an organization for ease of replication and distribution across an organization.

- *Channels* — View and manage the available SUSE Manager channels and the files they contain.

  - *Software Channels* — View a list of all software channels and those applicable to your systems.

  - *Package Search* — Search packages using all or some portion of the package name, description, or summary, with support for limiting searches to supported platforms.

  - *Manage Software Channels* — [Prov] — Create and edit channels used to deploy configuration files.

- *Configuration* — Keep track of and manage configuration channels, actions, and individual configuration files.

    - *Overview* — A general dashboard view that shows a configuration summary.

    - *Configuration Channels* — List and create configuration channels from which any subscribed system can receive configuration files.

    - *Configuration Files* — List and create files from which systems receive configuration input.

    - *Systems* — List the systems that have SUSE Manager-managed configuration files.

- *Schedule* — Keep track of your scheduled actions.

    - *Pending Actions* — List scheduled actions that have not been completed.

    - *Failed Actions* — List scheduled actions that have failed.

    - *Completed Actions* — List scheduled actions that have been completed. Completed actions can be archived at any time.

    - *Archived Actions* — List completed actions that have been selected to archive.

- *Users* — [Prov] — View and manage users in your organization.

    - *User List* — [Prov] — List users in your organization.

- *Monitoring* — [Mon] — Run probes and receive notifications regarding systems.

    - *Status* — [Mon] — View probes by state.

    - *Scout Config Push* — [Mon] — Display the status of your monitoring infrastructure.

    - *Notification* — [Mon] — View contact methods established for your organization.

    - *Probe Suites* — [Mon] — Manage your monitoring infrastructure using suites of monitoring probes that apply to one or more assigned systems.

- *Admin* (visible only to SUSE Manager administrators) — List, create, and manage one or more SUSE Manager organizations. The SUSE Manager administrator can assign channel entitlements, create and assign administrators for each organization, and other tasks.

  - *Organizations* — List and create new organizations.

  - *Subscriptions* — List and manage the software and system entitlements for all organizations covered by SUSE Manager.

  - *Users* — List all users known by SUSE Manager, across all organizations. Click individual user names to change administrative privileges of the user.

    NOTE

    Users created for organization administration can only be configured by the organization administrator, *not* the SUSE Manager administrator.

  - *SUSE Manager Configuration* — Make General configuration changes to the SUSE Manager server, including Proxy settings, Certificate configuration, Bootstrap Script configuration, Organization changes, and Restart the SUSE Manager server.

  - *Show Tomcat Logs* — Display the log entries of the Tomcat server, on which the SUSE Manager server is running.

- *Help* — List references to available help resources.

4.1.3 Patch Alert Icons

Throughout SUSE Manager you will see three patch (errata) alert icons. represents a security alert. represents a bug fix alert. represents an enhancement alert.

In the *Overview* page, click on the patch advisory to view details about the patch or click on the number of affected systems to see which are affected by the patch alert. Both links take you to tabs of the *Patch Details* page. Refer to Section 4.5.2.2, "Patch Details" (page 128) for more information.

4.1.4 Quick Search

In addition to the Advanced Search functionality for Packages, Patches (Errata), Documentation, and Systems offered within some categories, SUSE Manager also offers a Quick Search tool near the top of each page. To use it, select the search item (choose from *Systems*, *Packages*, *Documentation*, and *Patches*) and type a keyword to look for a name match. Click the *Search* button. Your results appear at the bottom of the page.

If you misspell a word during your search query, the SUSE Manager search engine performs approximate string (or fuzzy string) matching, returning results that may be similar in spelling to your misspelled queries.

For example, if you want to search for a certain development system called `test-1.example.com` that is registered with SUSE Manager, but you misspell your query `tset`, the `test-1.example.com` system still appears in the search results.

> **NOTE**
>
> If you add a distribution or register a system with a SUSE Manager server, it may take several minutes for it to be indexed and appear in search results.

- For advanced System searches, refer to Section 4.4.5, "Advanced Search — [Mgmt]" (page 96).

- For advanced Patch or Errata searches, refer to Section 4.5.3, "Advanced Search" (page 129).

- For advanced Package searches, refer to Section 4.6.2, "Package Search" (page 136).

- For advanced Documentation searches, refer to Section 4.12.7, "Search" (page 169).

4.1.5 Systems Selected

Near the top of the page you find a tool for keeping track of the systems you have selected for use in the System Set Manager. At any time, it identifies the number of selected systems and provides the means to work with them. Clicking the *Clear* button deselects all systems, while clicking the *Manage* button launches the System Set Manager with your selected systems in place.

These systems can be selected in a number of ways. Only systems with at least a Management entitlement are eligible for selection. On all system and system group lists, a Select column exists for this purpose. Select the checkboxes next to the systems or groups and click the *Update List* button below the column. Each time the Systems Selected tool at the top of the page changes to reflect the new number of systems ready for use in the System Set Manager. Refer to Section 4.4.4, "*System Set Manager — [Mgmt]*" (page 88) for details.

4.1.6 Lists

The information within most categories is presented in the form of lists. These lists have some common features for navigation. For instance, you can navigate through virtually all lists by clicking the back and next arrows above and below the right side of the table. Some lists also offer the option to retrieve items alphabetically by clicking letters above the table.

NOTE: Performing Large List Operations

Performing operations on large lists— such as removing RPM packages from the database with the SUSE Manager Web interface— may take some time and the system may become unresponsive or signal "Internal Server Error 500". Nevertheless, the command will succeed in the background if you wait long enough.

4.2 Getting your Novell Customer Center Mirror Credentials

Start a Web browser and navigate to http://novell.com/center. On the Novell Customer Center (NCC) login page, log in to view your mirror credentials and see all entitlements for your registered systems. If you have not yet registered a system or do not have a Novell account, create a new account by following the *Create Account* link. After creating a new user account, you must register a system before using SUSE Manager. On the Web page, click *My Products > Mirror Credentials* to get your channels for your Novell products. For detailed information about the NCC, refer to the NCC guide available at http://www.novell.com/documentation/ncc.

4.3 Overview

After logging into the Web interface of SUSE Manager, the first page to appear is *Overview*. This page contains important information about your systems, including summaries of system status, actions, and patch alerts.

> **NOTE**
>
> If you are new to the SUSE Manager Web interface, read Section 4.1, "Navigation" (page 49) to familiarize yourself with the layout and symbols used throughout the interface.

Figure 4.4   *Overview*
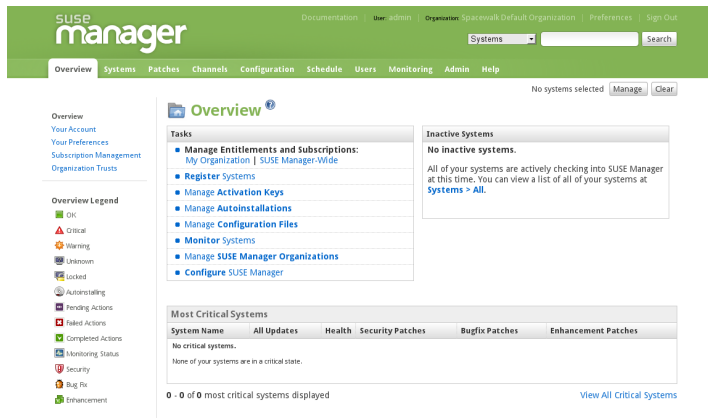
This page is split into functional areas, with the most critical areas displayed first. Users can control which of the following areas are displayed by making selections on the *Overview > Your Preferences* page. Refer to Section 4.3.2, "Your Preferences" (page 59) for more information.

- The *Tasks* area lists the most common tasks an administrator performs via the web. Click any link to reach the page within SUSE Manager that allows you to accomplish that task.

- If any systems have not been checking in to SUSE Manager, they are listed under *Inactive System* to the right. Highlighting them in this way allows an administrator to quickly select those systems for troubleshooting.

- [Mon] — Customers with monitoring enabled on their SUSE Manager can also choose to include a list of all probes in the Warning state.

- [Mon] — Customers with monitoring enabled on their SUSE Manager can also choose to include a list of all probes in the Critical state.

- The *Most Critical Systems* section lists the most critical systems within your organization. It provides a link to quickly view those systems, and displays a summary of the patch updates that have yet to be applied to those systems. Click the name of the system to see its *System Details* page and apply the patch updates. Below the list is a link to *View All Critical Systems* on one page.

- The *Recently Scheduled Actions* section lists all actions less than thirty days old and their status: failed, completed, or pending. Click the label of any given action to view its details page. Below the list is a link to *View All Scheduled Actions* on one page, which lists all actions that have not yet been carried out your client systems.

- The *Relevant Security Patches* section lists all available security patches that have yet to be applied to some or all of your client systems. It is critical that you apply these security patches to keep your systems secure. Below this list find links to all patches (*View All Patches*) and to the patches that apply to your systems (*View All Relevant Patches*).

- The *System Group Names* section lists groups you may have created and indicates whether the systems in those groups are fully updated. Click the link below this section to get to the *System Groups* page, where you can choose *System Groups* to use with the System Set Manager.

- The *Recently Registered Systems* section lists the systems added to the SUSE Manager in the past 30 days. Click a system's name to see its *System Details* page. Click the link below this section to *View All Recently Registered Systems* on one page.

To return to this page, click *Overview* on the left navigation bar.

4.3.1 Your Account

On the *Your Account* page modify your personal information, such as name, password, and title. To modify any of this information, make the changes in the appropriate text fields and click the *Update* button in the bottom right-hand corner.

If you change your SUSE Manager password, for security reasons you will not see the new password while you enter it. Replace the asterisks in the *Password* and *Confirm Password* text fields with the new password.

4.3.1.1 Addresses

On the *Addresses* page manage your mailing, billing and shipping addresses, as well as the associated phone numbers. Just click *Edit this address* below the address to be modified, make the changes, and click *Update*.

4.3.1.2 Change E-mail

The e-mail address listed in the *Your Account* page is the address to which SUSE Manager sends e-mail notifications if you select to receive patch alerts or daily summaries for your systems on the *Your Preferences* page.

To change your preferred e-mail address, click *Change E-mail* in the left navigation bar. Enter your new e-mail address and click the *Update* button. A confirmation e-mail is sent to the new e-mail address; responding to the confirmation e-mail validates the new e-mail address. Invalid e-mail addresses like those ending in `@localhost` are filtered and rejected.

4.3.1.3 Account Deactivation

The *Account Deactivation* page provides a means to cancel your SUSE Manager service. To do so, click the *Deactivate Account* button. The Web interface returns you to the login screen. If you attempt to log back in, an error message advises you to contact the SUSE Manager administrator for your organization. Note that if you are the only SUSE Manager Administrator for your organization, you are unable to deactivate your account.

4.3.2 Your Preferences

The *Your Preferences* page allows you to configure SUSE Manager options, including:

- *E-mail Notifications* — Determine whether you want to receive e-mail every time a patch alert is applicable to one or more systems in your account.

> **IMPORTANT**
>
> This setting also enables Management and Provisioning customers to receive a daily summary of system events. These include actions affecting packages, such as scheduled patches, system reboots, or failures to check in. In addition to selecting this checkbox, you must identify each system to be included in this summary e-mail. By default, all Management and Provisioning systems are included in the summary. Add more systems either individually on the *System Details* page or for multiple systems at once in the *System Set Manager* interface. Note that SUSE Manager sends these summaries only to verified e-mail addresses. To disable all messages, simply deselect this checkbox.

- *SUSE Manager List Page Size* — Maximum number of items that appear in a list on a single page. If more items are in the list, clicking the *Next* button displays the next group of items. This preference applies to system lists, patch lists, package lists, and so on.

- *"Overview" Start Page* — Select the information areas that are displayed on the *Overview* Start Page. Check the box to the left of the information area you would like to include.

After making changes to any of these options, click the *Save Preferences* button in the bottom right-hand corner.

4.3.3 Locale Preferences

On the *Overview > Locale Preferences* page set your SUSE Manager interface to your local time by selecting the appropriate *Time Zone* from the drop-down box, then click the *Save Preferences* button to apply the selection.

4.3.4 Subscription Management

To use all of the features of SUSE Manager, your systems must be entitled — subscribed to Novell Customer Center. Use the *System Entitlements* page to configure which systems are entitled to which service offerings.

4.3.5 Organization Trusts

The *Organization Trusts* page displays the trusts established with your organization (that is, the organization with which you, the logged-in user, are associated). The page also lists *Channels Shared*: that is channels available to your organization via others in the established trusts.

You can filter the list of trusts by keyword using the *Filter by Organization* text box and clicking *Go*.

For more information about organizational trusts, refer to Section 6.6, "Organizational Trusts" (page 201).

4.4 Systems

If you click the *Systems* tab on the top navigation bar, the *Systems* category and links appear. Here you can select systems to perform actions on them and create System Profiles.

4.4.1 Overview — [Mgmt]

The *Overview* page provides a summary of your systems, including their status, number of associated patches (errata) and packages, and their entitlement level. Clicking on the name of a system takes you to its *System Details* page. Refer to Section 4.4.2.10, "System Details" (page 66) for more information.

Clicking the *View System Groups* link at the top of the *Overview* page takes you to a similar summary of your system groups. It identifies group status and displays the number of systems contained. Clicking on the number of systems takes you to the *Systems* tab of the *System Group Details* page, while clicking on the system name takes you to the *Details* tab for that system. Refer to Section 4.4.3.3, "System Group Details — [Mgmt]" (page 86) for more information.

You can also click the *Use Group* button in the *System Groups* section of the *Overview* page to go directly to the *System Set Manager*. Refer to Section 4.4.4, "*System Set Manager* — [Mgmt]" (page 88) for more information.

4.4.2 Systems

The *Systems* page displays a list of all your registered systems. Several columns provide information for each system:

- *Select* — Unentitled systems cannot be selected. To select systems, mark the appropriate checkboxes. Selected systems are added to the *System Set Manager* where actions can be carried out simultaneously on all systems in the set. Refer to Section 4.4.4, "*System Set Manager* — [Mgmt]" (page 88) for details.

- *System* — The name of the system specified during registration. The default name is the hostname of the system. Clicking on the name of a system displays its *System Details* page. Refer to Section 4.4.2.10, "System Details" (page 66) for more information.

- *Update* — Shows which type of update action is applicable to the system or confirms that the system is up-to-date. Some icons are linked to related tasks. For instance, the standard Updates icon is linked to the *Upgrade* subtab of the packages list, while the Critical Updates icon links directly to the *Update Confirmation* page. The Not Checking In icon is linked to instructions for resolving the issue.

  - ■ — System is up-to-date.

  - ⚠ — Critical patch (errata) available, update *strongly* recommended.

  - ⬤ — Updates available and recommended.

  - ▣ — System is locked; Actions prohibited.

  - ▣ — System is being deployed using AutoYaST or Kickstart.

  - ▣ — Updates have been scheduled.

  - ▣ — System not checking in properly (for 24 hours or more).

  - ■ — System not entitled to any update service.

- *Patches* — Total number of patch alerts applicable to the system.

- *Packages* — Total number of package updates for the system, including packages related to patch alerts as well as newer versions of packages not related to patch alerts. For example, if a client system that has an earlier version of a package installed gets subscribed to the appropriate base channel of SUSE Manager (such as SUSE Linux Enterprise11 SP1), that channel may have an updated version of the package. If so, the package appears in the list of available package updates.

> **IMPORTANT**
>
> If SUSE Manager identifies package updates for the system, but the package updater (such as Red Hat Update Agent or YaST) responds with a message like "Your system is fully updated", a conflict likely exists in the system's package profile or in the `up2date` configuration file. To resolve the conflict, either schedule a package list update or remove the packages from the Package Exceptions list. Refer to Section 4.4.2.10, "System Details" (page 66) or Section "Package Exceptions Settings" (page 40), respectively, for instructions.

- *Configs* — Total number of configuration files applicable to the system.

- *Base Channel* — The primary channel for the system based upon its operating system. Refer to Section 4.6.1, "Software Channels" (page 131) for more information.

- *Entitlement* — Shows whether or not the system is entitled and at what service level.

Links in the left navigation bar below *Systems* enable you to select and view predefined sets of your systems. All of the options described above can be applied within these pages.

4.4.2.1 All

The *All* page contains the default set of your systems. It displays every system you have permission to manage. You have permission if you are the only user in your organization, if you are a SUSE Manager Administrator, or if the system belongs to a group for which you have admin rights.

4.4.2.2 Virtual Systems

To reach this page, select the *Systems* tab, followed by the *Systems* subtab from the left navigation bar, and finally select *Virtual Systems* from the left navigation bar. This page lists each virtual host of which SUSE Manager is aware and the guest systems on those hosts.

System
> This column displays the name of each guest system.

Updates
> This column shows whether there are patches (errata updates) available for the guest systems that have not yet been applied.

Status
> This column indicates whether a guest is running, paused, or stopped.

Base Channel
> This column displays the base channel to which the guest is currently subscribed.

Only guests registered with SUSE Manager are displayed with blue text. Clicking on the hostname of such a guest system displays its *System Details* page.

4.4.2.3 Out of Date

The *Out of Date* page displays all systems where applicable patch alerts have not been applied.

4.4.2.4 Unentitled — [Mgmt]

The *Unentitled* page displays systems that have not yet been entitled for SUSE Manager service.

4.4.2.5 Ungrouped

The *Ungrouped* page displays systems not yet assigned to a specific system group.

4.4.2.6 Inactive

The *Inactive* page displays systems that have not checked into SUSE Manager for 24 hours or more. Checking in means that the Red Hat Update Agent on Red Hat Enterprise Linux or the YaST Online Update on SUSE Linux Enterprise client systems connects to SUSE Manager to see if there are any updates available or if any actions have been scheduled. If you see a message telling you that check-ins are not taking place, the client system is not successfully connecting to SUSE Manager. The reason may be one of the following:

- The system is not entitled to any SUSE Manager service. System Profiles that remain unentitled for 180 days (6 months) are removed.

- The system is entitled, but the SUSE Manager daemon (`rhnsd`) has been disabled on the system. Refer to Chapter 3, *SUSE Manager Daemon* (page 47) for instructions on restarting and troubleshooting.

- The system is behind a firewall that does not allow connections over `https` (port 443).

- The system is behind an HTTP proxy server that has not been properly configured.

- The system is connected to a SUSE Manager Proxy Server or SUSE Manager that has not been properly configured.

- The system itself has not been properly configured, perhaps pointing at the wrong SUSE Manager Server.

- The system is not in the network.

- Some other barrier exists between the system and the SUSE Manager Server.

4.4.2.7 Recently Registered

The *Recently Registered* page displays any systems that have been registered in a given period. Use the drop-down menu to specify the period in days, weeks, 30- and 180-day increments, and years.

4.4.2.8 Proxy

The *Proxy* page displays the SUSE Manager Proxy Server systems registered with your SUSE Manager server.

4.4.2.9 Duplicate Systems

The *Duplicate Systems* page lists current systems and any active and inactive entitlements associated with them. Active entitlements are in gray, while inactive entitlements are highlighted in yellow and their checkboxes checked by default for you to delete them as needed by clicking the *Delete Selected* button. Entitlements are inactive, if the system has not checked into SUSE Manager in a time specified by the *A system profile is inactive if its system has not checked in for:* drop-down.

You can filter duplicate entitlements by *IP Address*, *Hostname*, or *MAC address* by clicking on the respective subtab. You may filter further by typing in the system's hostname, IP address, or MAC address in the corresponding *Filter by:* text box.

To compare up to three duplicate entitlements at one time, click the *Compare Systems* link in the *Last Checked In* column. Inactive components of the systems are highlighted in yellow. You can then determine which systems are inactive or duplicate and delete them by clicking the *Delete System Profile* button. Click the *Confirm Deletion* button to confirm your choice.

4.4.2.10 System Details

Click the name of a system on any page and SUSE Manager displays that client's *System Details* page. Here, you may modify the displayed information or remove the system altogether by clicking the *delete system* link on the top-right corner.

NOTE

The *delete system* link in the upper right of this screen refers to the system profile only. Deleting a host system profile will not destroy or remove the registration of guest systems. Deleting a guest system profile does not remove it from the list of guests for its host, nor does it stop or pause the guest. It does, however, remove your ability to manage it via SUSE Manager.

If you mistakenly delete a system profile from SUSE Manager, you may re-register the system using the bootstrap script (see Chapter 5, *Using Bootstrap* (↑Client Configuration Guide)) or `rhnreg_ks` manually.

The *System Details* page is further divided into the *Details*, *Software*, *Configuration*, *Groups*, *Provisioning* ([Prov]), *Monitoring* ([Mon]), and *Events* subtabs.

The following sections discuss these tabs and their subtabs in detail.

System Details > Details

This page is not accessible from any of the standard navigation bars. However, clicking on the name of a system anywhere in the Web interface displays this page. By default the *Details > Overview* subtab is displayed. Other tabs are available, depending on the current entitlement level of the system.

System Details > Details > Overview

This system summary page displays the system status message and the following key information about the system:

System Status

> This message indicates the current state of your system in relation to SUSE Manager.

> **NOTE**

> If updates are available for any entitled system, the message *Critical updates available* appears. To apply these updates, click the *update now* link.

System Info

Hostname
   The hostname as defined by the client system.

IP Address
   The IP address of the client.

Kernel
   The kernel installed and operating on the client system.

SUSE Manager System ID

A unique identifier generated each time a system registers with SUSE Manager.

NOTE

The system ID can be used to eliminate duplicate profiles from SUSE Manager. Compare the system ID listed on this page with the information stored on the client system in the `/etc/sysconfig/rhn/systemid` file. In that file, the system's current ID is listed under `system_id`. The value starts after the characters `ID-`. If the value stored in the file does not match the value listed in the profile, the profile is not the most recent one and may be removed.

Lock Status

Indicates whether a system has been locked.

Actions cannot be scheduled for locked systems on the Web interface until the lock is removed manually. This does not include preventing automated patch updates scheduled via the Web interface. To prevent the application of automated patch updates, de-select *Auto Patch Update* from the *System Details > Details > Properties* subtab. For more information, refer to Section "System Details > Details > Properties" (page 71).

Locking a system can prevent you from accidentally changing a system. For example, the system may be a production system that you do not wish to receive updates or new packages until you decide to unlock it.

IMPORTANT

Locking a system in the Web interface *will not* prevent any actions that originate from the client system. For example, if a user logs into the client directly and runs YaST Online Update (on SLE) or `up2date` (resp. `pup` on RHEL), the update tool will install available patches whether or not the system is locked in the Web interface.

Locking a system *does not* restrict the number of users who can access the system via the Web interface. If you wish to restrict access to the system, associate that system with a System Group and assign a System Group Administrator to it. Refer to Section 4.4.3, "System Groups — [Mgmt]" (page 84) for more information about System Groups.

It is also possible to lock multiple systems via the System Set Manager. Refer to Section "System Set Manager > Misc > Lock Systems — [Mgmt]" (page 95) for instructions.

Subscribed Channels

List of subscribed channels. Click the *(Alter Channel Subscriptions)* link right beside the title to assign available base and child channels to this system. When finished making selections, click the *Change Subscriptions* button to confirm the changes. For more information, refer to Section "System Details > Software > Software Channels " (page 77).

Base Channel
The first line indicates the base channel to which this system is subscribed. The base channel should match the operating system of the client.

Child Channels
The subsequent lines of text, which depend on the base channel, list child channels. An example is the *SUSE Manager Tools* channel.

System Events

Checked In
The date and time at which the system last checked in with SUSE Manager.

Registered
The date and time at which the system registered with SUSE Manager and created this profile.

Last Booted
The date and time at which the system was last started or restarted.

NOTE

Systems with a Management entitlement can be rebooted from this screen.

1. Select *Schedule system reboot*.

2. Provide the earliest date and time at which the reboot may take place.

3. Click the *Schedule Reboot* button in the lower right.

> When the client checks in after the scheduled start time, SUSE Manager
> will instruct the system to restart itself.

[Prov] — OSA status is also displayed for client systems registered with SUSE Manager that have a Provisioning entitlement and have enabled OSA. For more information about OSA, refer to Section "Enabling Push to Clients" (Chapter 6, *Maintenance*, ↑Installation Guide).

Push enables SUSE Manager customers to immediately initiate tasks on Provisioning-entitled systems rather than wait for those systems to check in with SUSE Manager. Scheduling actions through push is identical to the process of scheduling any other action, except that the task begins immediately instead of waiting the set interval.

In addition to the configuration of SUSE Manager, each client system to receive pushed actions must have the `osad` package installed and its service started. Refer to the Section "Enabling Push to Clients" (Chapter 6, *Maintenance*, ↑Installation Guide) for details.

System Properties

Entitlement
   The base entitlement currently applied to this system.

Notifications
   Indicates the notification options for this system. You can choose whether you wish to receive email notifying you of available patch updates for this system. In addition, you may choose to include Management-entitled systems in the daily summary e-mail.

Auto Patch Update
   Indicates whether this system is configured to accept updates automatically.

Description
   This information is automatically generated at registration. You can edit the description to include any information you wish.

Location
   This field displays the physical address of the system if specified.

Clicking the *Edit These Properties* link right beside the *System Properties* title opens the *System Details > Properties* subtab. On this page, edit any text you choose, then click the *Update Properties* button to confirm.

System Details > Details > Properties

This subtab allows you to alter the following basic properties of your system:

System Details Properties

System Name
> By default, this is the hostname of the system. You can however alter the profile name to anything that allows you to distinguish this system from others.

Base Entitlement
> Select a base channel for the system from the available base entitlements.

Add-on entitlements
> If available, apply a Monitoring, Provisioning, Virtualization, or Virtualization Platform entitlement to the system.

Notifications
> Toggle whether notifications about this system are sent and whether this system is included in the daily summary. (By default, all Management and Provisioning systems are included in the summary.) This setting keeps you aware of all advisories pertaining to the system. Anytime an update is released for the system, you receive an e-mail notification.
>
> The daily summary reports system events that affect packages, such as scheduled patch updates, system reboots, or failures to check in. In addition to including the system here, you must choose to receive e-mail notification in the *Your Preferences* page of the *Overview* category.

Auto Patch Update
> If this box is checked, available patches are automatically applied to the system when it checks in. This action takes place without user intervention. The SUSE Manager Daemon (`rhnsd`) must be enabled on the system for this feature to work.

> **NOTE: Conflicts With Third Party Packages**
>
> Enabling auto-update might lead to failures because of conflicts between system updates and third party packages. To avoid failures caused by those issues, it is better to leave this box unchecked.

Description

By default, this text box records the operating system, release, and architecture of the system when it first registers. You may edit this information to include anything you like.

The remaining fields record the physical address at which the system is stored. To confirm any changes to these fields, click the *Update Properties* button.

NOTE: Setting Properties to Multiple Systems

Many of these properties can be set for multiple systems in one go via the System Set Manager interface. Refer to Section 4.4.4, "*System Set Manager —* [Mgmt]" (page 88) for details.

System Details > Details > Remote Command — [Prov]

This subtab allows you to run a remote command on the system if the system possesses a Provisioning entitlement. Before doing so, you must first configure the system to accept such commands.

1 On SLE clients, subscribe the system to the SUSE Manager Tools child channel and use `zypper` to install the `rhncfg`, `rhncfg-client`, and `rhncfg-actions` packages, if not already installed:

```
zypper in rhncfg rhncfg-client rhncfg-actions
    -
```

On RHEL clients, subscribe the system to the Tools child channel and use `up2date` or `yum` to install the `rhncfg`, `rhncfg-client`, and `rhncfg-actions` packages, if not already installed:

```
up2date rhncfg rhncfg-client rhncfg-actions
    -
```

2 Log into the system as root and add the following file to the local SUSE Manager configuration directory: `allowed-actions/scripts/run`.

2a Create the necessary directory on the target system:

```
mkdir -p /etc/sysconfig/rhn/allowed-actions/script
```

2b Create an empty `run` file in that directory to act as a flag to SUSE Manager signaling permission to allow remote commands:

```
touch /etc/sysconfig/rhn/allowed-actions/script/run
```

Once the setup is complete, refresh the page in order to view the text fields for remote commands. Identify a specific user, group, and timeout period, as well as the script to run. Select a date and time to execute the command, and click *Schedule Remote Command*.

System Details > Details > Reactivation — [Prov]

Reactivation keys, available only for systems that have a Provisioning entitlement, include this system's ID, history, groups, and channels. This key can then be used only once with the `rhnreg_ks` command line utility to re-register this system and regain all SUSE Manager settings. Refer to Section 2.3.5, "Registering with Activation Keys" (page 42) for instructions. Unlike typical activation keys, which are not associated with a specific system ID, keys created here do not show up within the *Activation Keys* page.

Reactivation keys can be combined with activation keys to aggregate the settings of multiple keys for a single system profile. For example:

```
rhnreg_ks --server=server-url \
  --activationkey=reactivation-key,activationkey --force
```

WARNING

When autoinstalling a system with its existing SUSE Manager profile, the profile uses the system-specific activation key created here to re-register the system and return its other SUSE Manager settings. For this reason, you should not regenerate, delete, or use this key (with `rhnreg_ks`) while a profile-based autoinstallation is in progress. If you do, the autoinstallation will fail.

System Details > Details > Hardware

This subtab provides detailed information about the system, including networking, BIOS, memory, and other devices but only if you included the hardware profile for this machine during registration. If the hardware profile looks incomplete or outdated, click the *Schedule Hardware Refresh* button. The next time the SUSE Manager Daemon

(`rhnsd`) connects to SUSE Manager, it will update your System Profile with the latest hardware information.

System Details > Details > Migrate

This subtab provides the option to migrate systems between organizations. Select an *Organization Name* and click *Migrate System* to initiate the migration.

System Details > Details > Notes

This subtab provides a place to create notes about the system. To add a new note, click the *create new note* link, type a subject and write your note, then click the *Create* button. To modify a note, click on its subject in the list of notes, make your changes, and click the *Update* button. To remove a note, click on its subject in the list of notes then click the *delete note* link.

System Details > Details > Custom Info — [Prov]

This subtab, available for systems with a Provisioning entitlement, provides completely customizable information about the system. Unlike *Notes*, *Custom Info* is structured, formalized, and can be searched. Before you can provide custom information about a system, you must have *Custom Information Keys*. Click on *Custom System Info* in the left navigation bar. Refer to Section 4.4.8, "Custom System Info — [Prov]" (page 104) for instructions.

Once you have created one or more keys, you may assign values for this system by selecting the *create new value* link. Click the name of the key in the resulting list and enter a value for it in the *Description* field, then click the *Update Key* button.

System Details > Details > Proxy

This tab is only available for SUSE Manager Proxy systems and lists all clients registered with the selected SUSE Manager Proxy server.

System Details > Software

This tab and its subtabs allow you to manage the software on the system: patches (errata), packages and package profiles, and software channel memberships.

System Details > Software > Patches

This subtab contains a list of patch (errata) alerts applicable to the system. Refer to Section 4.1.3, "Patch Alert Icons" (page 54) for meanings of the icons on this tab. To apply updates, select them and click the *Apply Patches* button. Double-check the updates to be applied on the confirmation page, then click the *Confirm* button. The action is added to the *Pending Actions* list under *Schedule*. Patches that have been scheduled cannot be selected for update. In the place of a checkbox is a clock icon. Click on the clock to see the *Action Details* page.

A *Status* column in the patches table shows whether an update has been scheduled. Possible values are: None, Pending, Picked Up, Completed, and Failed. This column displays only the latest action related to a patch. For instance, if an action fails and you reschedule it, this column shows the status of the patch as `Pending` with no mention of the previous failure. Clicking a status other than `None` takes you to the *Action Details* page. This column corresponds to the one on the *Affected Systems* tab of the *Patch Details* page.

System Details > Software > Packages

Manage the software packages on the system.

[Prov] — When selecting packages to install, upgrade, or remove, Provisioning customers have the option of running a remote command automatically before or after the package installation. Refer to Section "System Details > Details > Remote Command — [Prov]" (page 72) for more information.

Packages
    The default display of the *Packages* tab describes the options available and provides the means to update your package list. To update or complete a potentially outdated list, possibly due to the manual installation of packages, click the *Update Package List* button in the bottom right-hand corner of this page. The next time the SUSE Manager Daemon (`rhnsd`) connects to SUSE Manager, it updates your System Profile with the latest list of installed packages.

List/Remove
    Lists installed packages and enables you to remove them. View and sort packages by name, architecture, and the date they were installed on the system. Search for the desired packages by typing its name in the *Filter by Package Name* text box, or by clicking the letter or number corresponding to the first character of the

package name. Click on a package name to view its *Package Details* page. To delete packages from the system, select their checkboxes and click the *Remove Packages* button on the bottom right-hand corner of the page. A confirmation page appears with the packages listed. Click the *Confirm* button to remove the packages.

Upgrade

Displays a list of packages with newer versions available in the subscribed channels. Click on the latest package name to view its *Package Details* page. To upgrade packages immediately, select them and click the *Upgrade Packages* button. To download the packages as a .tar file, select them and click the *Download Packages* button.

Install

Install new packages on the system from the available channels. Click on the package name to view its *Package Details* page. To install packages, select them and click the *Install Selected Packages* button.

Verify

Validates the packages installed on the system against its RPM database. This is the equivalent of running `rpm -V`. The metadata of the system's packages is compared with information from the database, such as file checksum, file size, permissions, owner, group and type. To verify a package or packages, select them, click the *Verify Selected Packages* button, and confirm. When the check is finished, select this action in the *History* subtab under *Events* to see the results.

Profiles

Compare installed packages with the package lists in stored profiles and other Management and Provisioning systems. Select a stored profile from the dropdown menu and click the *Compare* button. To compare with packages installed on a different system, select the system from the associated dropdown menu and click the *Compare* button. To create a stored profile based upon the existing system, click the *Create System Profile* button, enter any additional information you desire, and click the *Create Profile* button. These profiles are kept within the *Stored Profiles* page linked from the left navigation bar.

[Prov] — Once installed package have been compared with a profile, Provisioning customers have the option to synchronize the selected system with the profile. Note that all changes apply to the system not the profile. Packages might get deleted and additional packages installed on the system. To install only specific packages, click the respective checkboxes in the profile. To remove specific packages installed on

the system, select the checkboxes of these packages showing a difference of *This system only.* To completely synchronize the system's packages with the compared profile, select the master checkbox at the top of the column. Then click the *Sync Packages to* button. On the confirmation screen, review the changes, select a time frame for the action, and click the *Schedule Sync* button.

System Details > Software > Software Channels

Software channels provide a well-defined method to determine which packages should be available to a system for installation or upgrade based upon its operating systems, installed packages, and functionality. Click a channel name to view its *Channel Details* page. To modify the child channels associated with this system, use the checkboxes next to the channels and click the *Change Subscriptions* button. You will receive a success message or be notified of any errors. To change the system's base channel, select the new one from the pulldown menu and click the *Modify Base Channel* button. Refer to Section 4.6.1, "Software Channels" (page 131) for more information.

System Details > Configuration — [Prov]

This tab and its subtabs, which do not appear without a Provisioning entitlement, assist in managing the configuration files associated with the system. These configuration files may be managed solely for the current system, or may be distributed widely via a Configuration Channel. The following sections describe these and other available options on the *System Details > Configuration* subtabs.

NOTE

To manage the configuration of a system, it must have the latest `rhncfg*` packages installed. Refer to Section 4.7.1, "Preparing Systems for Config Management" (page 140) for instructions on enabling and disabling scheduled actions for a system.

This section is available to normal users with access to systems that have configuration management enabled. Like software channels, configuration channels store files to be installed on systems. While software updates are provided by NCC, configuration files are managed solely by you. Also unlike with software packages, various versions of configuration files may prove useful to a system at any given time. Only the latest version can be deployed.

System Details > Configuration > Overview

This subtab provides access to the configuration statistics of your system and to the most common tasks used to manage configuration files. You may change the settings listed under Configuration Stats by clicking on the blue text for that setting. Alternatively, you may perform any of the common configuration management tasks listed on the right of the screen by clicking one of the links.

System Details > Configuration > Managed Files

This subtab lists all configuration files currently associated with the system.

Filename
> This column shows both the name and the deployment path for this file.

Revision
> This column increments any time you make a change to the managed file.

From Config Channel
> This column indicates the name of the channel containing the file or displays *(system override)* for files available to this system only.

Overrides
> If this configuration file overrides another, the overridden file is listed in this column along with its host channel.

If you wish to deploy any of these files to the client system and overwrite changes that have been made locally, check the box to the left of the file and click the *Deploy Configuration* button. On the following screen, choose a deployment time and click the *Schedule Deploy* button to confirm.

NOTE

If you click on the *Filename* of a *(system override)* file, you can edit its contents.

The *Overrides* column identifies the configuration file in an unsubscribed channel that would replace the same file in a currently subscribed channel. For example, if a system has /etc/foo from channel bar and /etc/foo from channel baz is in the Overrides column, then unsubscribing from channel bar will mean that the file from channel baz will be applicable. If no file is listed in the *Overrides* column for a given file path,

then unsubscribing from the channel providing the file will mean that the file is no longer managed (though it will *not* be removed from the system).

System Details > Configuration > Compare Files

This subtab compares a configuration file stored on the SUSE Manager with the file stored on the client. (It does not, compare versions of the same file stored in different channels.) Select the files to be compared, click the *Compare Files* button, select a time to perform the diff, and click the *Schedule Compare* button to confirm. After the diff has been performed, return to this page to see the results.

System Details > Configuration > Manage Configuration Channels

This subtab allows you to subscribe to and rank configuration channels associated with the system, lowest first.

The *List/Unsubscribe from Channels* subtab contains a list of the system's configuration channel subscriptions. Click the checkbox next to the Channel and click *Unsubscribe* to remove the subscription to the channel.

The *Subscribe to Channels* subtab lists all available configuration channels. To subscribe to a channel, select the checkbox next to it and press *Continue*. To subscribe to all configuration channels, click *Select All* and press *Continue*. The *View/Modify Rankings* page automatically loads.

The *View/Modify Rankings* subtab allows users to set the priority with which files from a particular configuration channel are ranked. The higher the channel is on the list, the more its files take precedence over files on lower-ranked channels. For example, the higher-ranked channel may have an `httpd.conf` file that will take precedence over the same file in a lower-ranked channel.

System Details > Configuration > Local Overrides

This subtab displays the default configuration files for the system and allows you to manage them. If no files exist, use the *add files*, *upload files*, and *add directories* links within the page description to associate files with this system. These tabs correspond to those on the *Configuration Channel Details* page affecting your entire organization and available only to Configuration Administrators. Refer to Section 4.7.3.1, "*Configuration > Configuration Channels > Configuration Channel Details*" (page 142) for more information.

If a file exists, click its name to go to the *Configuration File Details* page. Refer to Section 4.7.4, "Configuration Files" (page 144) for instructions. To replicate the file within a config channel, select its checkbox, click the *Copy to Config Channel* button, and select the destination channel. To remove a file, select it and click *Delete Selected Files*.

System Details > Configuration > Sandbox

Manipulate configuration files without deploying them. This sandbox allows you to experiment with files without affecting your systems. To add files, click the *import new files* link, enter the path to the file on you local system, and click the *Add* button. Select the *Import Files* button to confirm.

System Details > Provisioning — [Prov]

This tab and its subtabs allow you to schedule and monitor AutoYaST or Kickstart installations and to restore your system to a previous state. AutoYaST is a SUSE Linux and Kickstart is a Red Hat utility—both allow you to automate the re-installation of a system. Snapshot rollbacks provide the ability to revert certain changes on the system. You can roll back a set of RPM packages, but rolling back across multiple update levels is not supported. Both features are described in the sections that follow.

System Details > Provisioning > Autoinstallation — [Prov]

This subtab is further divided into *Session Status*, which tracks the progress of previously scheduled autoinstallations, and *Schedule*, which allows you to configure and schedule an autoinstallation for this system.

In the *Schedule* subtab schedule the selected system for autoinstallation. Choose from the list of available profiles, select a time for the autoinstallation to begin, and click the *Schedule Autoinstall and Finish* button to begin the autoinstallation. You may want to alter autoinstallation settings by clicking the *Advanced Configuration* button.

NOTE

You must first create a profile before it appears on this subtab. If you have not created any profiles, refer to Section 4.4.9.4, "Create a New Kickstart Profile" (page 113) before scheduling an autoinstallation for a system.

The *Variables* subtab can be used to create Kickstart variables, which substitute values in Kickstart files. To define a variable, create a name-value pair (`name/value`) in the text box.

For example, if you want to Kickstart a system that joins the network of a specified organization (for instance the Engineering department) you can create a profile variable to set the IP address and the gateway server address to a variable that any system using that profile will use. Add the following line to the *Variables* text box:

```
IPADDR=192.168.0.28
GATEWAY=192.168.0.1
```

To use the system variable, use the name of the variable in the profile instead of the value. For example, the `network` portion of a Kickstart file could look like the following:

```
network --bootproto=static --device=eth0 --onboot=on --ip=$IPADDR
--gateway=$GATEWAY
```

The `$IPADDR` will be `192.168.0.28`, and the `$GATEWAY` will be `192.168.0.1`

NOTE

There is a hierarchy when creating and using variables in Kickstart files. System Kickstart variables take precedence over profile variables, which in turn take precedence over distribution variables. Understanding this hierarchy can alleviate confusion when using variables in Kickstarts.

Using variables are just one part of the larger Cobbler infrastructure for creating templates that can be shared between multiple profiles and systems. For more information about Cobbler and Kickstart templates, refer to Chapter 8, *Cobbler* (page 225).

System Details > Provisioning > Snapshots — [Prov]

Snapshots enable you to roll back the system's package profile, configuration files, and SUSE Manager settings. Snapshots are captured whenever an action takes place on a Provisioning-entitled system. The *Snapshots* subtab lists all snapshots for the system, including the reason why the snapshot was taken, the time it was taken, and the number of tags applied to each snapshot. To revert to a previous configuration, click the *Reason* for the snapshot and review the potential changes on the provided subtabs, starting with *Rollback*.

> **NOTE**
>
> Snapshot roll backs support the ability to revert *certain* changes to the system, but not in every scenario. For example, you can roll back a set of RPM packages, but rolling back across multiple update levels is not supported.

Each subtab provides the specific changes that will be made to the system during the rollback:

- group memberships,

- channel subscriptions,

- installed packages,

- configuration channel subscriptions,

- configuration files,

- snapshot tags.

When satisfied with the reversion, return to the *Rollback* subtab and click the *Rollback to Snapshot* button. To see the list again, click *Return to snapshot list*.

System Details > Provisioning > Snapshot Tags — [Prov]

Provides a means to add meaningful descriptions to your most recent system snapshot. This can be used to indicate milestones, such as a known working configuration or a successful upgrade. To tag the most recent snapshot, click *create new system tag*, enter a descriptive term in the *Tag name* field, and click the *Tag Current Snapshot* button. You may then revert using this tag directly by clicking its name in the Snapshot Tags list. To delete tags, select their checkboxes, click *Remove Tags*, and confirm the action.

System Details > Monitoring — [Mon]

This tab is only visible for systems registered with SUSE Manager that are Monitoring enabled and entitled. All probes monitoring the system are listed here. The *State* column shows icons representing the status of each probe. Refer to Section 4.10, "Monitoring — [Mon]" (page 157) for descriptions of these states. Clicking the *Probe Description* takes you to its *Current State* page. The *Status String* column displays the last message received from the probe.

To add a probe to the system, click the *create new probe* link at the top-right corner and fill in the fields on the following page. Refer to Section 5.5.1, "Managing Probes" (page 180) for detailed instructions.

Once the probe has been added, you must reconfigure your Monitoring infrastructure to recognize it. Refer to Section 4.10.2, "Scout Config Push — [Mon]" (page 160) for details. After the probe has run, its results become available on the *Current State* page. Refer to Section 4.10.1.7, "*Current State* — [Mon]" (page 159) for details.

To remove a probe from a system, click on the name of the probe, then click the *delete probe* link in the upper right corner. Click the *Delete Probe* button to complete the process.

System Details > Groups — [Mgmt]

This tab and its subtabs allow you to manage the system's group memberships.

System Details > Groups > List/Leave — [Mgmt]

This subtab lists groups to which the system belongs and enables you to cancel membership. Only System Group Administrators and SUSE Manager Administrators can remove systems from groups. Non-admins just see a *Review this system's group membership* page. To remove the system from one or more groups, select the respective checkboxes of these groups, and click the *Leave Selected Groups* button. To see the *System Group Details*page, click on the group's name. Refer to Section 4.4.3.3, "System Group Details — [Mgmt]" (page 86) for more information.

System Details > Groups > Join — [Mgmt]

Lists groups that the system can be subscribed to. Only System Group Administrators and SUSE Manager Administrators can add a system to groups. Non-admins see a *Review this system's group membership* page. To add the system to groups, select the groups' checkboxes and click the *Join Selected Groups* button.

System Details > Events

Displays past, current, and scheduled actions on the system. You may cancel pending events here. The following sections describe the *Events* subtabs and the features they offer.

System Details > Events > Pending

Lists events that are scheduled but have not started. A prerequisite action must complete successfully before the given action is attempted. If an action has a prerequisite, no checkbox is available to cancel that action. Instead, a checkbox appears next to the prerequisite action; canceling the prerequisite action causes the action in question to fail.

Actions can be chained so that action 'a' requires action 'b' which requires action 'c'. Action 'c' is performed first and has a checkbox next to it until it is completed successfully. If any action in the chain fails, the remaining actions also fail. To unschedule a pending event, select the event and click the *Cancel Events* button at the bottom of the page. The following icons indicate the type of events:

- — Package Event,

- — Patch Event,

- — Preferences Event,

- — System Event.

System Details > Events > History

The default display of the *Events* tab lists the type and status of events that have failed, occurred or are occurring. To view details of an event, click its summary in the *System History* list. To the table again, click *Return to history list* at the bottom of the page.

4.4.3 System Groups — [Mgmt]

The *System Groups* page allows all SUSE Manager Management and Provisioning users to view the *System Groups* list. Only System Group Administrators and SUSE Manager Administrators may perform the following additional tasks:

1. Create system groups. (Refer to Section 4.4.3.1, "Creating Groups" (page 86).)

2. Add systems to system groups. (Refer to Section 4.4.3.2, "Adding and Removing Systems in Groups" (page 86).)

3. Remove systems from system groups. (Refer to Section 4.4.2.10, "System De-
tails" (page 66).)

4. Assign system group permissions to users. (Refer to Section 4.9, "Users —
[Mgmt]" (page 150).)

The *System Groups* list displays all your system groups. The list contains several columns
for each group:

- *Select* — Add systems in groups to the *System Set Manager*. To select groups, mark
the appropriate checkboxes and click the *Update* button below the column. All systems
in the selected groups are added to the *System Set Manager*. You can then use the
System Set Manager to perform actions on them simultaneously. It is possible to select
only those systems that are members of all of the selected groups, excluding those
systems that belong only to one or some of the selected groups. To do so, select the
relevant groups and click the *Work with Intersection* button. To add all systems of
all selected groups, click the *Work with Union* button. Each system will show up
once, regardless of the number of groups to which it belongs. Refer to Section 4.4.4,
"*System Set Manager* — [Mgmt]" (page 88) for details.

- *Updates* — Shows which type of patch alerts are applicable to the group or confirms
that all systems are up-to-date. Clicking on a group's status icon takes you to the
Patch tab of its *System Group Details* page. Refer to Section 4.4.3.3, "System Group
Details — [Mgmt]" (page 86) for more information.

  The status icons call for differing degrees of attention:

  - ◻ — All systems in the group are up-to-date.

  - ⚠ — Critical patches available, update *strongly* recommended.

  - ⬦ — Updates available and recommended.

- *Group Name* — The name of the group as configured during its creation. The name
should be explicit enough to distinguish from other groups. Clicking on the name of
a group takes you to the *Details* tab of its *System Group Details* page. Refer to Sec-
tion 4.4.3.3, "System Group Details — [Mgmt]" (page 86) for more information.

- *Systems* — Total number of systems in the group. Clicking on the number takes you
to the *Systems* tab of the *System Group Details* page for the group. Refer to Sec-
tion 4.4.3.3, "System Group Details — [Mgmt]" (page 86) for more information.

- *Use in SSM* — Clicking the *Use Group* button in this column loads the group from that row and launches the *System Set Manager* immediately. Refer to Section 4.4.4, "*System Set Manager* — [Mgmt]" (page 88) for more information.

4.4.3.1 Creating Groups

To add a new system group, click the *create new group* link at the top-right corner of the page. Type a name and description and click the *Create Group* button. Make sure you use a name that clearly sets this group apart from others. The new group will appear in the *System Groups* list.

4.4.3.2 Adding and Removing Systems in Groups

Systems can be added and removed from system groups in two places: the *Target Systems* tab of the *System Group Details* page and the *Groups* tab of the *System Details* page. The process is similar in both instances. Select the systems to be added or removed and click the *Add Systems* or *Remove Systems* button.

4.4.3.3 System Group Details — [Mgmt]

At the top of each *System Group Details* page are two links: *work with group* and *delete group*. Clicking *delete group* deletes the System Group and should be used with caution. Clicking *Work with Group* loads the group's systems and launches the *System Set Manager* immediately just like the *Use Group* button from the *System Groups* list. Refer to Section 4.4.4, "*System Set Manager* — [Mgmt]" (page 88) for more information.

The *System Group Details* page is split into the following tabs:

System Group Details > Details — [Mgmt]

Provides the group name and group description. To change this information, click *Edit Group Properties*, make your changes in the appropriate fields, and click the *Modify Details* button.

System Group Details > Systems — [Mgmt]

Lists all members of the system group. Clicking links within the table takes you to corresponding tabs within the *System Details* page for the associated system. To remove systems from the group, select the appropriate checkboxes and click the *Remove from group* button on the bottom of the page. Clicking it does not delete systems from SUSE Manager entirely. This is done through the *System Set Manager* or *System Details* pages. Refer to Section 4.4.4, "*System Set Manager* — [Mgmt]" (page 88) or Section 4.4.2.10, "System Details" (page 66), respectively.

System Group Details > Target Systems — [Mgmt]

Target Systems — Lists all systems in your organization. To add systems to the specified system group, click the checkboxes to their left and click the *Add Systems* button on the bottom right-hand corner of the page.

System Group Details > Patches — [Mgmt]

List of relevant patches for systems in the system group. Clicking the advisory takes you to the *Details* tab of the *Patch Details* page. (Refer to Section 4.5.2.2, "Patch Details" (page 128) for more information.) Clicking the Affected Systems number lists all of the systems affected by the patch. To apply the patch updates in this list, select the systems and click the *Apply Patches* button.

System Group Details > Admins — [Mgmt]

List of all organization users that have permission to manage the system group. SUSE Manager Administrators are clearly identified. System Group Administrators are marked with an asterisk (*). To change the system group's users, select and unselect the appropriate checkboxes and click the *Update* button.

System Group Details > Probes — [Prov]

List of all probes assigned to systems in the system group. *State* shows the status of the probe. Click the individual *System* for details on the probe and to make changes to the probe configuration. Click *Probe* to generate a customizable report on the monitoring.

4.4.4 *System Set Manager* — [Mgmt]

Many actions performed for individual systems through the System Details page may be performed for multiple systems via the System Set Manager, including:

- Apply patch updates.

- Upgrade packages to the most recent versions available.

- Add/remove systems to/from system groups.

- Subscribe/unsubscribe systems to/from channels.

- Update system profiles.

- Modify system preferences such as scheduled download and installation of packages.

- Autoinstall several Provisioning-entitled systems at once.

- Set the subscription and rank of configuration channels for Provisioning-entitled systems.

- Tag the most recent snapshots of your selected Provisioning-entitled systems.

- Revert Provisioning-entitled systems to previous snapshots.

- Run remote commands on Provisioning-entitled systems.

Before performing actions on multiple systems, select the systems you wish to modify. To do so, click the *List the systems* link, check the boxes to the left of the systems you wish to select, and click the *Update List* button.

You can access the System Set Manager in three different ways:

1. Click the *System Set Manager* link in the left gray navigation area.

2. Click the *Use Group* button in the *System Groups* list.

3. Check the *Work with Group* link on the *System Group Details* page.

4.4.4.1 System Set Manager > Overview — [Mgmt]

Description of the various options available to you in the remaining tabs.

4.4.4.2 System Set Manager > Systems — [Mgmt]

List of selected systems. To remove systems from this set, select them and click the *Remove* button.

4.4.4.3 System Set Manager > Patches — [Mgmt]

List of patch updates applicable to the current system set. Click the number in the Systems column to see to which systems in the System Set Manager a patch applies. To apply updates, select the patches and click the *Apply Patches* button.

4.4.4.4 System Set Manager > Packages — [Mgmt]

Click the number in the Systems column to see the systems in the System Set Manager to which a package applies. Modify packages on the system via the following subtabs:

[Prov] — When selecting packages to install, upgrade, or remove, Provisioning customers have the option of running a remote command automatically before or after the package installation. Refer to Section "System Details > Details > Remote Command — [Prov]" (page 72) for more information.

System Set Manager > Packages > Upgrade — [Mgmt]

A list of all the packages installed on the selected systems that might be upgraded. Systems must be subscribed to a channel providing the packages to be upgraded. If multiple versions of a package are available, note that your system will be upgraded to the latest version. Select the packages to be upgraded, then click the *Upgrade Packages* button.

System Set Manager > Packages > Install — [Mgmt]

This list includes all channels to which systems in the set are subscribed. A package is only installed on a system if the system is subscribed to the channel providing the

package. Click on the channel name and select the packages from the list. Then click the *Install Packages* button.

System Set Manager > Packages > Remove — [Mgmt]

A list of all the packages installed on the selected systems that might be removed. Multiple versions appear if systems in the System Set Manager have more than one version installed. Select the packages to be deleted, then click the *Remove Packages* button.

4.4.4.5 System Set Manager > Verify — [Mgmt]

A list of all installed package whose contents, file checksum, and other details may be verified. At the next check in, the verify event issues the command `rpm --verify` for the specified package. If there are any discrepancies, they are displayed in the System Details page for each system.

Select the checkbox next to all packages to be verified, then click the *Verify Packages* button. On the next page, select either *Schedule actions ASAP* or choose a date and time for the verification, then click the *Schedule Verifications* button.

4.4.4.6 System Set Manager > Groups — [Mgmt]

Tools to create groups and manage membership. These functions are limited to SUSE Manager Administrators and System Group Administrators. To add a new group, click *create new group* on the top-right corner. In the next page, type the group name and description in the respective fields and click the *Create Group* button. To add or remove selected systems in any of the system groups, toggle the appropriate radio buttons and click the *Alter Membership* button.

4.4.4.7 System Set Manager > Channels — [Mgmt]

Manage channel associations through the following subtabs:

System Set Manager > Channels > Channel Subscriptions — [Mgmt]

To subscribe or unsubscribe selected systems to any of the channels, toggle the appropriate checkboxes and click the *Alter Subscriptions* button. Keep in mind that subscribing to a channel uses a channel entitlement for each system in the selected group. If too few entitlements are available, some systems fail to subscribe. Systems must subscribe to a base channel before subscribing to a child channel.

4.4.4.8 System Set Manager > Configuration — [Prov]

Like in the *System Details > Channels > Configuration* tab, the subtabs here can be used to subscribe the selected systems to configuration channels and deploy and compare the configuration files on the systems. The channels are created in the *Manage Config Channels* interface within the *Channels* category. Refer to Section 4.7.2, "Overview" (page 141) for channel creation instructions.

To manage the configuration of a system, install the latest `rhncfg*` packages. Refer to Section 4.7.1, "Preparing Systems for Config Management" (page 140) for instructions on enabling and disabling scheduled actions for a system.

System Set Manager > Configuration > Deploy Files — [Prov]

Use this subtab to distribute configuration files from your central repository on SUSE Manager to each of the selected systems. The table lists the configuration files associated with any of the selected systems. Clicking its system count displays the systems already subscribed to the file.

To subscribe the selected systems to the available configuration files, select the checkbox for each desired file. When done, click *Deploy Configuration* and schedule the action. Note that the latest versions of the files, at the time of scheduling, are deployed. Newer versions created after scheduling are disregarded.

System Set Manager > Configuration > Compare Files — [Prov]

Use this subtab to validate configuration files on the selected systems against copies in your central repository on SUSE Manager. The table lists the configuration files associated with any of the selected systems. Clicking a file's system count displays the systems already subscribed to the file.

To compare the configuration files deployed on the systems with those in SUSE Manager, select the checkbox for each file to be validated. Then click *Analyze Differences* and schedule the action. The comparisons for each system will not complete until each system checks in to SUSE Manager. Once each comparison is complete, any differences between the files will be accessible from each system's events page.

Note that the latest versions of the files, at the time of scheduling, are compared. Newer versions created after scheduling are disregarded. Find the results in the main *Schedule* category or within the *System Details > Events* tab.

System Set Manager > Configuration > Subscribe to Channels — [Prov]

Subscribe systems to configuration channels according to the order of preference. This tab is available only to SUSE Manager Administrators and Configuration Administrators. Enter a number in the *Rank* column to subscribe to a channel. Channels are accessed in the order of their rank, starting from the number 1. Channels not assigned a numeric value are not associated with the selected systems. Your local configuration channel always overrides all other channels. Once you have established the rank of the config channels, you must decide how they are applied to the selected systems.

The three buttons below the channels reflect your options. Clicking *Subscribe with Highest Priority* places all the ranked channels before any other channels to which the selected systems are currently subscribed. Clicking *Subscribe With Lowest Priority* places the ranked channels after those channels to which the selected systems are currently subscribed. Clicking *Replace Existing Subscriptions* removes any existing association and creates new ones with the ranked channels, leaving every system with the same config channels in the same order.

In the first two cases, if any of the newly ranked config channels are already in a system's existing config channel list, the duplicate channel is removed and replaced according to the new rank, effectively reordering the system's existing channels. When such conflicts exist, you are presented with a confirmation page to ensure the intended action is correct. When the change has taken place, a message appears at the top of the page indicating the update was successful.

System Set Manager > Configuration > Unsubscribe from Channels — [Mgmt]

Administrators may unsubscribe from configuration channels by clicking the checkbox next to the channel name and clicking the *Unsubscribe Systems* button.

System Set Manager > Configuration > Enable Configuration — [Mgmt]

Administrators may enable configuration channel management by clicking the checkbox next to the channel name and clicking the *Enable Configuration Management* button. You can also schedule the action by clicking the *Schedule package installs for no sooner than* radio button and using the drop-down menus to configure date and time, then clicking *Enable Configuration Management*.

4.4.4.9 System Set Manager > Provisioning — [Prov]

Set the options for provisioning systems via the following subtabs.

System Set Manager > Provisioning > Autoinstallation — [Prov]

Use this subtab to re-install a client on the selected Provisioning-entitled systems. To schedule autoinstallations for these systems, select a distribution, identify the type (IP address or manual), and click *Continue*. Select from the options available on the subsequent screen. If any of the systems connect to SUSE Manager via a Proxy Server, choose either the *Preserve Existing Configuration* radio button or the *Use Proxy* radio button. If you choose to autoinstall through a Proxy Server, select from the available Proxies listed in the drop-down box beside the *Use Proxy* radio button. All of the selected systems will autoinstall through the selected Proxy. Click the *Schedule Autoinstall* button to confirm your selections. When the autoinstallations for the selected systems are successfully scheduled, the web interface returns you to the System Set Manager page.

System Set Manager > Provisioning > Tag Systems — [Prov]

Use this subtab to add meaningful descriptions to the most recent snapshots of your selected systems. To tag the most recent system snapshots, enter a descriptive term in the *Tag name* field and click the *Tag Current Snapshots* button.

System Set Manager > Provisioning > Rollback — [Prov]

Use this subtab to rollback selected Provisioning-entitled systems to previous snapshots marked with a tag. Click the name of the tag, verify the systems to be reverted, and click the *Rollback Systems* button.

System Set Manager > Provisioning > Remote Command — [Prov]

Use this subtab to issue remote commands on selected Provisioning-entitled systems. First create a `run` file on the client systems to allow this function to operate. Refer to Section "System Details > Details > Remote Command — [Prov]" (page 72) for instructions. Then identify a specific user, group, timeout period, and the script to run. Select a date and time to execute the command, and click *Schedule Remote Command*.

4.4.4.10 System Set Manager > Misc — [Mgmt]

Misc — Update System Profiles and preferences for the system set through the following links:

System Set Manager > Misc > System Profile Updates — [Mgmt]

Click *Update Hardware Profile* then the *Confirm Refresh* button to schedule a hardware profile update. Click *Update Package Profile* then the *Confirm Refresh* button to schedule a package profile update.

System Set Manager > Misc > Custom System Information — [Prov]

Click *Set a custom value for selected systems* then the name of a key. Enter values for all selected systems then click the *Set Values* button. To remove values for all selected systems, click *Remove a custom value from selected systems* then the name of the key. Click the *Remove Values* button to delete.

System Set Manager > Misc > Reboot Systems — [Mgmt]

Select the appropriate systems then click the *Reboot Systems* link to select these systems for reboot. To cancel this action, click the *list of systems* link that appears within the

confirmation message at the top of the page, select the systems, and click *Unschedule Action*.

System Set Manager > Misc > Lock Systems — [Mgmt]

Select the appropriate systems and click the *Lock Systems* link to prevent the scheduling of any action through SUSE Manager on these systems. To grant SUSE Manager access again, click the *Unlock Systems* link.

System Set Manager > Misc > Delete Systems — [Mgmt]

Click *Delete System Profiles* then the *Confirm Deletions* button to remove the selected profiles permanently.

System Set Manager > Misc > Add or Remove Add-On Entitlements — [Mgmt]

Select, via the radio button, whether to *Add*, *Remove*, or make *No Change* in the entitlements of the selected systems. Click the *Change Entitlements* button to confirm your selection.

System Set Manager > Misc > System Preferences — [Mgmt]

Toggle the *Yes* and *No* radio buttons and click the *Change Preferences* button to alter your notification preferences for the selected systems. You may apply these preferences to individual systems through the *Properties* subtab of the *System Details* page. Refer to Section "System Details > Details > Properties " (page 71) for instructions.

- *Receive Notifications of Updates/Patches* — This setting keeps you aware of all advisories pertaining to your systems. Any time an update is released for a system you administer, a notification is sent via e-mail.

- *Include system in Daily Summary* — This setting includes the selected systems in a daily summary of system events. By default, all Management and Provisioning systems are included in the summary. These system events are actions that affect packages, such as scheduled patch updates, system reboots, or failures to check in. Select receive e-mail notifications on the *Your Preferences* page. Refer to Section 4.3.2, "Your Preferences" (page 59) for instructions. Note that SUSE Manager sends these summaries only to verified e-mail addresses.

- *Automatic application of relevant Patches* — This setting enables the automatic application of patch updates to the selected systems. Packages associated with patches are updated without any user intervention. The use of the auto-update feature for production systems is not recommend because conflicts between packages and environments can cause system failures.

4.4.5 Advanced Search — [Mgmt]

Carry out a *System Search* on your systems according to the following criteria: custom system information, system details, hardware, devices, interface, networking, packages, and location.

Refine searches using the *Fields to Search* drop-down menu, which is set to *Name/Description* by default.

The following list details the *Fields to Search* drop-down menu.

- *DMI Info* — The Desktop Management Interface (DMI) is a standard for management of components on computer system. Search for SUSE Manager systems using the following DMI retrieval methods:

    - System — Product names or numbers, manufacturer names, serial numbers, and other information that may be unique to a system.

    - BIOS — BIOS support information such as BIOS vendor name and version, hardware support enabled in the BIOS, and more.

    - Asset Tag — A unique identifier assigned by an IT department (or vendor) to a system for better tracking, management and inventory.

- *Location* — The physical location of a system, which includes the following:

    - Address — the address of the system or system set,

    - Building — the building or site in an address,

    - Room — the server or system room within a building,

    - Rack — the designated location within a server room where a system is situated.

- *Details* — The unique identifiers assigned to a system by administrators and particularly SUSE Manager Administrators. These unique identifiers include:

    - Name/Description — The name assigned to a system by the SUSE Manager Administrator upon adding it to the SUSE Manager server.

    - ID — An identifier that is unique to a system or system set.

    - Custom Info — Information which only applies to this one system.

    - Snapshot Tag — The name assigned to a new or previous system snapshot.

    - Running Kernel — The currently running kernel on a system registered with SUSE Manager.

- *Hardware* — Systems can be searched by particular components in the system, including the following:

    - CPU Model — The CPU model name (such as *Pentium* or *Athlon*).

    - CPU MHz Less Than — Search systems with a processor less than the selected speed in Megahertz.

    - CPU MHz More Than — Search systems with a processor more than a user-designated speed in Megahertz.

    - Number of CPUs Less Than — Search systems with a sum of processors less than the user-designated quantity.

    - Number of CPUs Greater Than — Search systems with a sum of processors greater than the specified quantity.

    - RAM Less Than — Search systems with less memory than the user-designated quantity in megabytes.

    - RAM More Than — Search systems with more memory than the user-designated quantity in megabytes.

- *Packages* — Search by the packages installed (and not yet installed) on the system.

    - Installed Packages — Filter systems based on certain installed packages.

- Needed Packages — Filter systems based on particular packages that have yet to be installed.

- *Activity* — Search by the amount of time elapsed since the systems first or last checked into SUSE Manager.

  - Days Since Last Check-in — Search by the amount of days passed since the systems last checked into SUSE Manager.

  - Days Since First Check-in — Search by the amount of days passed since the systems first checked into SUSE Manager.

- *Network Info* — Search systems based on specific networking details such as IP address.

  - Hostname — The name of a system registered with SUSE Manager.

  - IP Address — The network address of a system registered with SUSE Manager.

- *Hardware Devices* — Search systems by specific hardware details such as driver names and device or vendor IDs.

  - Description — Device summary information, such as brand or model name/number (for instance `Intel 82801HBM/HEM`)

  - Driver — The kernel driver or module name (such as `tulip.o` or `iwl3945`)

  - Device ID — The hexadecimal number corresponding to the device installed in the system.

  - Vendor ID — The hexadecimal number corresponding to the vendor of the device installed in the system.

The Activity selections (*Days Since Last Checkin*, for instance) are useful in finding and removing outdated System Profiles.

Type the keyword, select the criterion to search by, use the radio buttons to specify whether you wish to query all systems or only those in the *System Set Manager*, and click the *Search* button. To list all systems that do *not* match the criteria, select the *Invert Result* checkbox.

The results appear at the bottom of the page. For details on how to use the resulting system list, refer to Section 4.4.2, "Systems" (page 62).

4.4.6 Activation Keys — [Mgmt]

SUSE Manager Management and Provisioning customers with the Activation Key Administrator role (including SUSE Manager Administrators) can generate activation keys in the SUSE Manager Web interface. With such an activation key, register a SUSE Linux Enterprise or Red Hat Enterprise Linux system, entitle the system to a SUSE Manager service level and subscribe the system to specific channels and system groups through the `rhnreg_ks` command line utility. Refer to Section 2.3.5, "Registering with Activation Keys" (page 42) for instructions.

NOTE

System-specific activation keys created through the *Reactivation* subtab of the *System Details* page are not part of this list because they are not reusable across systems.

4.4.6.1 Managing Activation Keys

To create an activation key:

Procedure 4.1 *Creating Activation Keys*

1 Select *Systems* from the top navigation bar then *Activation Keys* from the left navigation bar.

2 Click the *create new key* link at the upper right corner.

3 *Description* — Enter a *Description* to identify the generated activation key.

4 *Key* — In addition to the fields listed below, SUSE Manager customers may also populate the *Key* field itself. This string of characters can then be used with `rhnreg_ks` to register client systems with SUSE Manager. Refer to Section 4.4.6.2, "Using Multiple Activation Keys at Once — [Prov]" (page 102) for details.

> **WARNING: Allowed Characters**
>
> Do not insert commas in the key. All other characters are allowed. Commas
> are problematic because they are used as separator when two or more
> activation keys are used at once.

5 *Usage Limit* — The maximum number systems that can be registered with the
activation key concurrently. Leave blank for unlimited use. Deleting a system
profile reduces the usage count by one and registering a system profile with the
key increases the usage count by one.

6 *Base Channel* — The primary channel for the key. This can be either the `SUSE`
`Manager Default` channel or a custom base channel.

Selecting `SUSE Manager Default` allows client systems to register with the
SUSE-provided default channel that corresponds with their installed version of
SUSE Linux Enterprise. You can also associate the key with a custom base
channel. If a system using this key is not compatible with the selected channel,
it will fall back to the SUSE Manager default channel.

7 *Add-on Entitlements* — The supplemental entitlements for the key, including
Monitoring, Provisioning, Virtualization, and Virtualization Platform. All systems
will receive these entitlements with the key.

8 *Universal default* — Select whether or not this key should be considered the pri-
mary activation key for your organization.

> **WARNING: Changing the Default Activation Key**
>
> Only one universal default activation key can be defined per organization.
> If a universal key already exists for this organization, you will unset the
> currently used universal key by activating the checkbox.

9 Click *Create Key*.

10 To create more activation keys, repeat the steps above.

Figure 4.5 *Activation Keys*
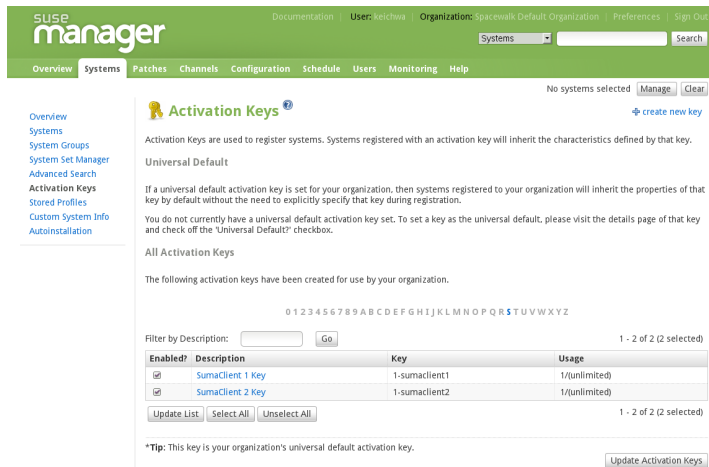
After creating the unique key, it appears in the list of activation keys along with the number of times it has been used (see Figure 4.5, "Activation Keys" (page 101)). Note that only Activation Key Administrators can see this list. At this point, you can associate the key with child channels (e.g., the Tools child channel), packages (e.g., the `rhncfg-actions` package) and groups. Systems registered with the key get automatically subscribed to them.

To change the information about a key, click the key's description in the list to display its *Details* page (see Figure 4.6, "Activation Key Details With Subtabs" (page 102)). Modify the appropriate tab then click the *Update Key* button. To disassociate channels and groups from a key, deselect them in their respective menus by Ctrl-clicking their highlighted names. To remove a key entirely, click the *delete key* link in the upper right corner of the edit page.

Figure 4.6 *Activation Key Details With Subtabs*

A system may be subscribed to a base channel during registration with an activation key. However, if the activation key specifies a base channel that is not compatible with the operating system running on the system, the registration fails. For example, a SUSE Linux Enterprise Server for x86 system cannot register with an Activation Key that specifies a SUSE Linux Enterprise Server for x86_64 base channel. A system can always subscribe to a custom base channel.

To disable system activations with a key, uncheck the corresponding box under the *Enabled* column in the key list. The key can be re-enabled by selecting the checkbox. Click the *Update Keys* button on the bottom right-hand corner of the page to activate your changes.

4.4.6.2 Using Multiple Activation Keys at Once — [Prov]

Provisioning customers should note that multiple activation keys can be specified at the command-line or in a single autoinstallation profile. This allows you to aggregate the aspects of various keys without recreating a new key specific for every system that you want to register, simplifying the registration and autoinstallation processes while slowing the growth of your key list.

Without this stacking ability, your organization would need at least six activation keys to manage four server groups and subscribe a server to any two groups. Factor in two versions of the operating system, such as Red Hat Enterprise Linux 4 and 5, and you need twice the number of activation keys. A larger organization would need keys in the dozens.

Registering with multiple activation keys requires some caution; conflicts between some values cause registration to fail. Conflicts in the following values do not cause registration to fail, a combination of values is applied: software packages, software child channels, and config channels. Conflicts in the remaining properties are resolved in the following manner:

• base software channels — registration fails,

• entitlements — registration fails,

• enable config flag — configuration management is set.

Do not use system-specific activation keys along with other activation keys; registration fails in this event.

You are now ready to use multiple activation keys at once. Separate keys with a comma at the command line with `rhnreg_ks` or in a Kickstart profile in the *Activation Keys* tab of the *Autoinstallation Details* page. Refer to Section 2.3.5, "Registering with Activation Keys" (page 42) and Section "Activation Keys — [Prov]" (page 120), respectively, for instructions.

4.4.7 Stored Profiles — [Mgmt]

SUSE Manager Provisioning customers can create package profiles through the *Profiles* subtab of the *Packages* tab on the *System Details* page. Those profiles are displayed on the *Stored Profiles* page, where they may be edited or deleted.

To edit a profile, click its name in the list, alter its name or description, and click the *Update Profile* button. To view software associated with the profile, click the *Packages* subtab. To remove the profile entirely, click *delete profile* at the upper-right corner of the page.

4.4.8 Custom System Info — [Prov]

SUSE Manager Provisioning customers may include completely customizable information about their systems. Unlike with notes, the information here is more formal and can be searched. For instance, you may decide to specify an asset tag for each system. To do this, you must create an `asset` key within the *Custom System Info* page.

Click *create new key* in the upper-right corner of the page. Enter a suitable label and description, such as `Asset` and `Precise location of each system`, then click *Create Key*. The key will show up in the custom info keys list.

Once the key exists, you may assign a value to it through the *Custom Info* tab of the *System Details* page. Refer to Section "System Details > Details > Custom Info — [Prov]" (page 74) for instructions.

4.4.8.1 mgr-custom-info

In addition to creating and listing custom information keys via the SUSE Manager Web interface, there is a command-line tool called `mgr-custom-info` (`rhn-custom-info` package) that performs the same actions at a shell prompt.

The usage of `mgr-custom-info` is as follows:

```
mgr-custom-info options key1 value1
```

For example:

```
mgr-custom-info --username=admin --password=f00b4rb4z \
  --server-url=manager.example.com --list-values
```

The command lists the custom keys and their values for the manager.example.com SUSE Manager server.

For more information, refer to the help file by typing `mgr-custom-info -h`.

4.4.9 Autoinstallation — [Prov]

> **NOTE: Autoinstallation Types: AutoYaST and Kickstart**
>
> In the following section AutoYaST and AutoYaST features apply for SUSE Linux Enterprise client systems only. For RHEL systems, use Kickstart and Kickstart features.

AutoYaST and Kickstart configuration files allow administrators to create an environment for automating otherwise time-consuming system installations, such as multiple servers or workstations. AutoYaST files have to be uploaded to be managed with SUSE Manager. Kickstart files can be created, modified, and managed within the SUSE Manager Web interface.

SUSE Manager also features the Cobbler installation server. For more information on Cobbler, refer to Chapter 8, *Cobbler* (page 225).

To satisfy the provisioning needs of customers, SUSE Manager provides an interface for developing Kickstart and AutoYaST profiles that can be used to install Red Hat Enterprise Linux or SUSE Linux Enterprise on either new or already-registered systems automatically according to certain specifications.

Figure 4.7 *Autoinstallation Overview*
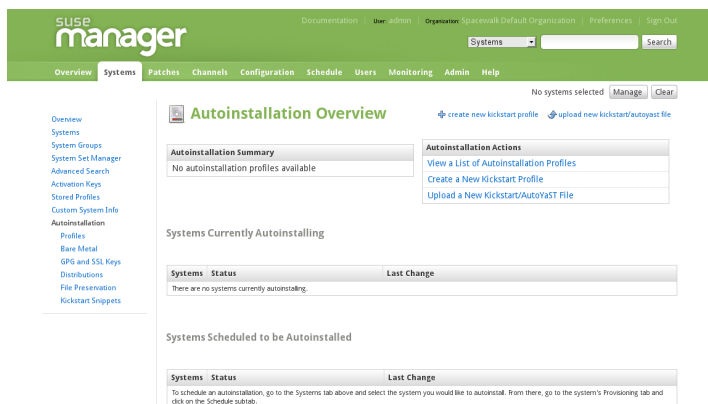
This overview page displays the status of automated installations (Kickstart and Auto-YaST) on your client systems: the types and number of profiles you have created and the progress of systems that are scheduled to be installed using Kickstart or AutoYaST.

In the upper right is the *Autoinstallation Actions* section, which contains a series of links to management actions for your Kickstart or AutoYaST profiles. Before explaining the various automated installation options on this page, the next two sections provide an introduction to AutoYaST and Kickstart.

4.4.9.1 Introduction to AutoYaST

Using AutoYaST, a system administrator can create a single file containing the answers to all the questions that would normally be asked during a typical installation of SUSE Linux Enterprise Server.

AutoYaST files can be kept on a single server system and read by individual computers during the installation. This way the same AutoYaST file is used to install SUSE Linux Enterprise on multiple machines.

The *SUSE Linux Enterprise Server Deployment Guide* (`http://www.novell .com/documentation/sles11/book_sle_deployment/data/cha _deployment_autoinst.html`) contains an in-depth discussion of "Automated Installation" using AutoYaST.

AutoYaST Explained

When a machine is to receive a network-based AutoYaST installation, the following events must occur in this order:

1. After being connected the network and turned on, the machine's PXE logic broadcasts its MAC address and requests to be discovered.

2. If no static IP address is used, the DHCP server recognizes the discovery request and offers network information needed for the new machine to boot. This includes an IP address, the default gateway to be used, the netmask of the network, the IP address of the TFTP or HTTP server holding the bootloader program, and the full path and file name to that program (relative to the server's root).

3. The machine applies the networking information and initiates a session with the server to request the bootloader program.

4. The bootloader searches for its configuration file on the server from which it was loaded. This file dictates which Kernel and Kernel options, such as the initial RAM disk (initrd) image, should be executed on the booting machine. Assuming the

bootloader program is SYSLINUX, this file is located in the `pxelinux.cfg` directory on the server and named the hexadecimal equivalent of the new machine's IP address. For example, a bootloader configuration file for SUSE Linux Enterprise Server should contain:

```
port 0
prompt 0
timeout 1
default autoyast
label autoyast
  kernel vmlinuz
  append autoyast=http://my_susemanager_server/path \
    install=http://my_susemanager_server/repo_tree
```

5. The machine accepts and uncompresses the initrd and kernel, boots the kernel, fetches the instsys from the install server and initiates the AutoYaST installation with the options supplied in the bootloader configuration file, including the server containing the AutoYaST configuration file.

6. The new machine is installed based upon the parameters established within the AutoYaST configuration file.

AutoYaST Prerequisites

Some preparation is required for your infrastructure to handle AutoYaST installations. For instance, before creating AutoYaST profiles, you may consider:

• A DHCP server is not required for AutoYaST, but it can make things easier. If you are using static IP addresses, you should select static IP while developing your AutoYaST profile.

• Host the AutoYaST distribution trees via HTTP, properly provided by SUSE Manager.

• If conducting a so-called bare metal AutoYaST installation, you should do the following:

   • Configure DHCP to assign the required networking parameters and the bootloader program location.

   • In the bootloader configuration file, specify the kernel and appropriate kernel options to be used.>

Building Bootable AutoYaST ISOs

While you can schedule a registered system to be installed by AutoYaST with a new operating system and package profile, you can also automatically install a system that is not registered with SUSE Manager, or does not yet have an operating system installed. One common method of doing this is to create a bootable CD-ROM that is inserted into the target system. When the system is rebooted or switched on, it boots from the CD-ROM, loads the AutoYaST configuration from your SUSE Manager, and proceeds to install SUSE Linux Enterprise Server according to the AutoYaST profile you have created.

To create an AutoYaST profile, copy the contents of `/loader` (e.g., `/boot/i386/loader/`) from the installation medium of the target distribution. Then edit the `isolinux.cfg` file to default to `autoyast` and add an `autoyast` section:

```
label autoyast
kernel vmlinuz
  append textmode=1 autoyast=url initrd=initrd \
    install=url_repo_tree
```

The AutoYaST distribution selected by the IP range should match the distribution from which you are building, otherwise errors will occur.

Next, you may customize `isolinux.cfg` according to your needs, for example, by adding multiple AutoYaST options, different boot messages, shorter timeout periods, etc.

Next, issue the command:

```
mkisofs -o file.iso -b isolinux.bin -c boot.cat -no-emul-boot \
  -boot-load-size 4 -boot-info-table -R -J -v -T loader/
```

Note that `loader/` is the relative path to the directory containing the modified isolinux files copied from the distribution medium, while `file.iso` is the output ISO file, which is placed into the current directory.

Burn the ISO on a CD-ROM. To use the disc, boot the system and type "autoyast" at the prompt (assuming you left the label for the AutoYaST boot as 'autoyast'). When you press Enter, the AutoYaST installation begins.

For more information about image creation, refer to the *SUSE Linux Enterprise Server Deployment Guide*, Part "Imaging and Creating Products".

Integrating AutoYaST with PXE

In addition to CD-ROM-based installations, AutoYaST installation through a Pre-Boot Execution Environment (PXE) is supported. This is less error-prone than CDs, enables AutoYaST installation from bare metal, and integrates with existing PXE/DHCP environments.

To use this method, make sure your systems have network interface cards (NIC) that support PXE, install and configure a PXE server, ensure DHCP is running, and place the installation repository on an HTTP server for deployment. Finally upload the AutoYaST profile with the Web interface to the SUSE Manager server. Once the AutoYaST profile has been created, use the URL from the *Autoinstallation Overview* page, as for CD-ROM-based installations.

To obtain specific instructions for conducting PXE AutoYaST installation, refer to the *Using PXE Boot* section of the *SUSE Linux Enterprise Deployment Guide*.

Starting with Section 4.4.9.3, "Autoinstallation Profiles (Kickstart and Auto-YaST)" (page 113), AutoYaST options available from *Systems > Kickstart* are described.

4.4.9.2 Introduction to Kickstart

Using Kickstart, a system administrator can create a single file containing the answers to all the questions that would normally be asked during a typical installation of Red Hat Enterprise Linux.

Kickstart files can be kept on a single server and read by individual computers during the installation. This method allows you to use one Kickstart file to install Red Hat Enterprise Linux on multiple machines.

The *Red Hat Enterprise Linux System Administration Guide* contains an in-depth description of Kickstart (http://www.redhat.com/docs/manuals/enterprise/).

Kickstart Explained

When a machine is to receive a network-based Kickstart, the following events must occur in this order:

1. After being connected to the network and turned on, the machine's PXE logic broadcasts its MAC address and requests to be discovered.

2. If no static IP address is used, the DHCP server recognizes the discovery request and offers network information needed for the new machine to boot. This information includes an IP address, the default gateway to be used, the netmask of the network, the IP address of the TFTP or HTTP server holding the bootloader program, and the full path and file name of that program (relative to the server's root).

3. The machine applies the networking information and initiates a session with the server to request the bootloader program.

4. The bootloader searches for its configuration file on the server from which it was loaded. This file dictates which kernel and kernel options, such as the initial RAM disk (initrd) image, should be executed on the booting machine. Assuming the bootloader program is SYSLINUX, this file is located in the `pxelinux.cfg` directory on the server and named the hexadecimal equivalent of the new machine's IP address. For example, a bootloader configuration file for Red Hat Enterprise Linux AS 2.1 should contain:

```
port 0
prompt 0
timeout 1
default My_Label
label My_Label
     kernel vmlinuz
     append ks=http://my_susemanager_server/path \
         initrd=initrd.img network apic
```

5. The machine accepts and uncompresses the init image and kernel, boots the kernel, and initiates a Kickstart installation with the options supplied in the bootloader configuration file, including the server containing the Kickstart configuration file.

6. This Kickstart configuration file in turn directs the machine to the location of the installation files.

7. The new machine is built based upon the parameters established within the Kickstart configuration file.

Kickstart Prerequisites

Some preparation is required for your infrastructure to handle Kickstarts. For instance, before creating Kickstart profiles, you may consider:

- A DHCP server is not required for kickstarting, but it can make things easier. If you are using static IP addresses, select static IP while developing your Kickstart profile.

- An FTP server can be used instead of hosting the Kickstart distribution trees via HTTP.

- If conducting a bare metal Kickstart, you should configure DHCP to assign required networking parameters and the bootloader program location. Also, specify within the bootloader configuration file the kernel to be used and appropriate kernel options.

Building Bootable Kickstart ISOs

While you can schedule a registered system to be kickstarted to a new operating system and package profile, you can also Kickstart a system that is not registered with SUSE Manager or does not yet have an operating system installed. One common method of doing this is to create a bootable CD-ROM that is inserted into the target system. When the system is rebooted, it boots from the CD-ROM, loads the Kickstart configuration from your SUSE Manager, and proceeds to install Red Hat Enterprise Linux according to the Kickstart profile you have created.

To do this, copy the contents of /isolinux from the first CD-ROM of the target distribution. Then edit the isolinux.cfg file to default to 'ks'. Change the 'ks' section to the following template:

```
label ks
kernel vmlinuz
  append text ks=url initrd=initrd.img lang= devfs=nomount \
    ramdisk_size=16438 ksdevice
```

IP address-based Kickstart URLs will look like this:

```
http://my.manager.server/kickstart/ks/mode/ip_range
```

The Kickstart distribution selected by the IP range should match the distribution from which you are building, or errors will occur. *ksdevice* is optional, but looks like:

```
ksdevice=eth0
```

It is possible to change the distribution for a Kickstart profile within a family, such as Red Hat Enterprise Linux AS 4 to Red Hat Enterprise Linux ES 4, by specifying the new distribution label. Note that you cannot move between versions (4 to 5) or between updates (U1 to U2).

Next, customize isolinux.cfg further for your needs by adding multiple Kickstart options, different boot messages, shorter timeout periods, etc.

Next, create the ISO as described in the *Making an Installation Boot CD-ROM* section of the *Red Hat Enterprise Linux Installation Guide*. Alternatively, issue the command:

```
mkisofs -o file.iso -b isolinux.bin -c boot.cat -no-emul-boot \
  -boot-load-size 4 -boot-info-table -R -J -v -T isolinux/
```

Note that isolinux/ is the relative path to the directory containing the modified isolinux files copied from the distribution CD, while file.iso is the output ISO file, which is placed into the current directory.

Burn the ISO to CD-ROM and insert the disc. Boot the system and type "ks" at the prompt (assuming you left the label for the Kickstart boot as 'ks'). When you press Enter, Kickstart starts running.

Integrating Kickstart with PXE

In addition to CD-ROM-based installs, Kickstart supports a Pre-Boot Execution Environment (PXE). This is less error-prone than CDs, enables kickstarting from bare metal, and integrates with existing PXE/DHCP environments.

To use this method, make sure your systems have network interface cards (NIC) that support PXE. Install and configure a PXE server and ensure DHCP is running. Then place the appropriate files on an HTTP server for deployment. Once the Kickstart profile has been created, use the URL from the *Kickstart Details* page, as for CD-ROM-based installs.

To obtain specific instructions for conducting PXE Kickstarts, refer to the *PXE Network Installations* chapter of the *Red Hat Enterprise Linux 4 System Administration Guide*.

NOTE: Tip

Running the Network Booting Tool, as described in the Red Hat Enterprise Linux 4: System Administration Guide, select "HTTP" as the protocol and include

the domain name of the SUSE Manager in the Server field if you intend to use it to distribute the installation files.

The following sections describe the autoinstallation options available from the *Systems > Autoinstallation* page.

4.4.9.3 Autoinstallation Profiles (Kickstart and AutoYaST)

Figure 4.8 *Profiles*
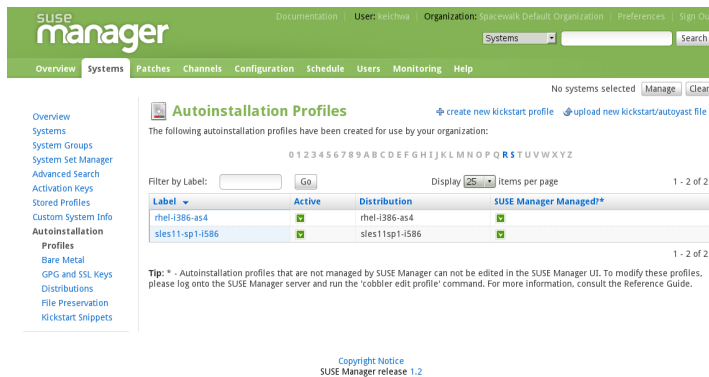
This page lists all profiles for your organization, shows whether these profiles are active, and specifies the distribution tree with which each profile is associated. You can either create a new Kickstart profile by clicking the *create new kickstart profile* link, upload or paste the contents of a new profile using the *upload new kickstart/autoyast file*, or edit an existing Kickstart profile by clicking the name of the profile. Note, you can only update AutoYaST profiles using the upload button. You can also view AutoYaST profiles in the edit box or change the virtualization type using the selection list.

4.4.9.4 Create a New Kickstart Profile

Click on the *create new kickstart profile* link from the *Systems > Autoinstallation* page to start the wizard that populates the base values needed for a Kickstart profile.

Procedure 4.2 *Creating a New Kickstart Profile*

1 On the first line, enter a Kickstart profile label. This label cannot contain spaces, so use dashes (-) or underscores (_) as separators.

2 Select a *Base Channel* for this profile, which consists of packages based on a specific architecture and Red Hat Enterprise Linux release.

3 Select an *Autoinstallable Tree* for this profile. The autoinstallable tree drop-down menu is only populated if one or more distributions have been created for the selected base channel.

4 Select the *Virtualization Type* from the drop-down menu.

5 On the second page, select (or enter) the location of the Kickstart tree.

6 On the third page, select a root password for the system.

Depending on your base channel, your newly created Kickstart profile might be subscribed to a channel that is missing required packages. In order for Kickstart to work properly, the following packages should be present in its base channel: `pyOpenSSL`, `rhnlib`, `libxml2-python`, and `spacewalk-koan` and associated packages.

To resolve this issue:

• Make sure that the Tools software channel for the Kickstart profile's base channel is available to your organization. If it is not, you must request entitlements for the Tools software channel from the SUSE Manager administrator.

• Make sure that the Tools software channel for this Kickstart profile's base channel is available to your SUSE Manager as a child channel.

• Make sure that `rhn-kickstart` and associated packages corresponding to this Kickstart are available in the Tools child channel.

The final stage of the wizard presents the *Autoinstallation Details > Details* tab. On this tab and the other subtabs, nearly every option for the new Kickstart profile can be customized.

Once created, you can access the Kickstart profile by downloading it from the *Autoinstallation Details* page by clicking the *Autoinstallation File* subtab and clicking the *Download Autoinstallation File* link.

If the Kickstart file is *not* managed by SUSE Manager, you can access it via the following URL:

```
http://my.manager.server/ks/dist/ks-rhel-ARCH-VARIANT-VERSION
```

In the above example, `ARCH` is the architecture of the Kickstart file, `VARIANT` is either `client` or `server`, and `VERSION` is the release of Red Hat Enterprise Linux associated with the Kickstart file.

The following sections describe the options available on each subtab.

Autoinstallation Details > Details — [Prov]

Figure 4.9   *Autoinstallation Details*

| Autoinstallation Details | System Details | Software | Activation Keys | Scripts | Autoinstallation F |
| Details | Operating System | Variables | Advanced Options | Bare Metal Autoinstallation |
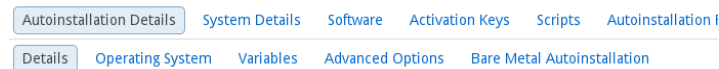
Figure 4.9, "Autoinstallation Details" (page 115) shows the subtabs that are available from the *Autoinstallation Details* tab. In the *Autoinstallation Details > Details* page, you have the following options:

• Rename the profile.

• Change the operating system it installs by clicking *(Change)*.

• Change the *Virtualization Type*.

> **NOTE**
>
> Changing the *Virtualization Type* may require changes to the Kickstart profile bootloader and partition options, potentially overwriting user customizations. Consult the *Partitioning* tab to verify any new or changed settings.

• Change the amount of *Virtual Memory* (in Megabytes of RAM) allocated to virtual guests autoinstalled with this profile.

- Change the number of *Virtual CPUs* for each virtual guest.

- Change the *Virtual Storage Path* from the default in `/var/lib/xen/`.

- Change the amount of *Virtual Disk Space* (in GB) allotted to each virtual guest.

- Change the *Virtual Bridge* for networking of the virtual guest.

- Deactivate the profile so that it cannot be used to schedule a Kickstart by removing the *Active* checkmark.

- Check whether to enable logging for custom `%post` scripts to the `/root/ks-post.log` file.

- Decide whether to enable logging for custom `%pre` scripts to the `/root/ks-pre.log` file.

- Choose whether to preserve the `ks.cfg` file and all `%include` fragments to the `/root/` directory of all systems autoinstalled with this profile.

- Select whether this profile is the default for all of your organization's Kickstarts by checking or unchecking the box.

- Add any *Kernel Options* in the corresponding text box.

- Add any *Post Kernel Options* in the corresponding text box.

- Enter comments that are useful to you in distinguishing this profile from others.

Autoinstallation Details > Operating System — [Prov]

On this page, you can make the following changes to the operating system that the Kickstart profile installs:

Change the base channel
> Select from the available base channels. SUSE Manager administrators see a list of all base channels that are currently synced to the SUSE Manager.

Child Channels
> Subscribe to available child channels of the base channel, such as the Tools channel.

Available Trees
Use the drop-down menu to choose from available trees associated with the base channel.

Software URL (File Location)
The exact location from which the Kickstart tree is mounted. This value is determined when the profile is created. You can view it on this page but you cannot change it.

Autoinstallation Details > Variables

Autoinstallation variables can substitute values in Kickstart and AutoYaST profiles. To define a variable, create a name-value pair (*name/value*) in the text box.

For example, if you want to autoinstall a system that joins the network of a specified organization (for example the Engineering department), you can create a profile variable to set the ip address and the gateway server address to a variable that any system using that profile will use. Add the following line to the *Variables* text box.

```
IPADDR=192.168.0.28
GATEWAY=192.168.0.1
```

Now you can use the name of the variable in the profile instead of a specific value. For example, the `network` part of a Kickstart file looks like the following:

```
network --bootproto=static --device=eth0 --onboot=on --ip=$IPADDR \
  --gateway=$GATEWAY
```

The $IPADDR will be resolved to 192.168.0.28, and the $GATEWAY to 192.168.0.1

NOTE

There is a hierarchy when creating and using variables in Kickstart files. System Kickstart variables take precedence over *Profile* variables, which in turn take precedence over *Distribution* variables. Understanding this hierarchy can alleviate confusion when using variables in Kickstarts.

Using variables are just one part of the larger Cobbler infrastructure for creating templates that can be shared between multiple profiles and systems. For more information about Cobbler and templates, refer to Chapter 8, *Cobbler* (page 225).

Autoinstallation Details > Advanced Options — [Prov]

From this page, you can toggle several installation options on and off by checking and unchecking the boxes to the left of the option. For most installations, the default options are correct. The *Red Hat Enterprise Linux System Administration Guide* discusses each of these options in detail.

Autoinstallation Details > Bare Metal Autoinstallation — [Prov]

This subtab provides the information necessary to Kickstart systems that are not currently registered with SUSE Manager. Using the on-screen instructions, you may either autoinstall systems using boot media (CD-ROM) or by IP address.

System Details > Details — [Prov]

Figure 4.10   *System Details*

Figure 4.10, "System Details" (page 118) shows the subtabs that are available from the *System Details* tab.

On the *System Details > Details* page, you have the following options:

- Select between DHCP and static IP, depending on your network.

- Choose the level of SELinux that is configured on kickstarted systems.

- Enable configuration management or remote command execution on kickstarted systems.

- Change the root password associated with this profile.

System Details > Locale — [Prov]

Change the timezone for kickstarted systems.

System Details > Partitioning — [Prov]

From this subtab, indicate the partitions that you wish to create during installation. For example:

```
partition /boot --fstype=ext3 --size=200
partition swap --size=2000
partition pv.01 --size=1000 --grow
volgroup myvg pv.01 logvol / --vgname=myvg --name=rootvol --size=1000 --grow
```

System Details > File Preservation — [Prov]

If you have previously created a file preservation list, include this list as part of the Kickstart. This will protect the listed files from being over-written during the installation process. Refer to Section 4.4.9.9, "Autoinstallation > File Preservation — [Prov]" (page 125) for information on how to create a file preservation list.

System Details > GPG & SSL — [Prov]

From this subtab, select the GPG keys and/or SSL certificates to be exported to the kickstarted system during the %post section of the Kickstart. For SUSE Manager customers, this list includes the SSL Certificate used during the installation of SUSE Manager.

NOTE

Any GPG key you wish to export to the kickstarted system must be in ASCII rather than binary format.

System Details > Troubleshooting — [Prov]

From this subtab, change information that may help with troubleshooting hardware problems:

Bootloader
    For some headless systems, it is better to select the non-graphic LILO bootloader.

Kernel Parameters
    Enter kernel parameters here that may help to narrow down the source of hardware issues.

Software > Package Groups — [Prov]

Figure 4.11 *Software*

Autoinstallation Details   System Details   Software   Activation Keys   Scripts   Autoinstallation File

Package Groups   Package Profiles
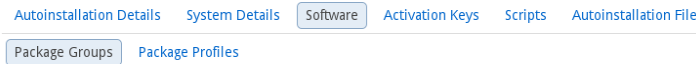
Figure 4.11, "Software" (page 120) shows the subtabs that are available from the *Software* tab.

Enter the package groups, such at `@office` or `@admin-tools` you would like to install on the kickstarted system in the large text box. If you would like to know what package groups are available, and what packages they contain, refer to the `RedHat/base/` file of your Kickstart tree.

Software > Package Profiles — [Prov]

If you have previously created a Package Profile from one of your registered systems, you can use that profile as a template for the files to be installed on a kickstarted system. Refer to Section "System Details > Software > Packages " (page 75) for more information about package profiles.

Activation Keys — [Prov]

Figure 4.12 *Activation Keys*

Autoinstallation Details   System Details   Software   Activation Keys   Scripts   Autoinstallation File

The *Activation Keys* tab allows you select Activation Keys to include as part of the Kickstart profile. These keys, which must be created before the Kickstart profile, will be used when re-registering kickstarted systems.

Scripts — [Prov]

Figure 4.13 *Scripts*

Autoinstallation Details   System Details   Software   Activation Keys   Scripts   Autoinstallation File

The *Scripts* tab is where %pre and %post scripts are created. This page lists any scripts that have already been created for this Kickstart profile. To create a new Kickstart script, perform the following procedure:

1 Click the *add new kickstart script* link in the upper right.

2 Enter the path to the scripting language used to create the script, such as
`/usr/bin/perl`.

3 Enter the full script in the large text box.

4 Indicate whether this script is to be executed in the %pre or %post section of the
Kickstart process.

5 Indicate whether this script is to run outside of the chroot environment. Refer to the
Post-installation Script section of the *Red Hat Enterprise Linux System Administration
Guide* for further explanation of the `nochroot` option.

NOTE

SUSE Manager supports the inclusion of separate files within the Partition Details
section of the Kickstart profile. For instance, you may dynamically generate a
partition file based on the machine type and number of disks at Kickstart time.
This file can be created via %pre script and placed on the system, such as `/tmp/
part-include`. Then you can call for that file by entering the following line
in the Partition Details field of the *System Details > Partitioning* tab:

`%include /tmp/part-include`

Autoinstallation File — [Prov]

Figure 4.14 *Autoinstallation File*

Autoinstallation Details   System Details   Software   Activation Keys   Scripts   [Autoinstallation File]

The *Autoinstallation File* tab allows you to view or download the profile that has been
generated from the options chosen in the previous tabs.

4.4.9.5 Upload a New Kickstart/AutoYaST File

Click on the *upload new kickstart/autoyast file* link from the *Systems > Autoinstallation*
page to upload an externally prepared AutoYaST or Kickstart profile.

1 In the first line, enter a profile *Label* for the automated installation. This label cannot contain spaces, so use dashes (-) or underscores (_) as separators.

2 Select an *Autoinstallable Tree* (installation data) for this profile. The *Autoinstallable Tree* drop-down menu is only populated if one or more distributions have been created for the selected base channel.

3 Select the *Virtualization Type* from the drop-down menu.

> **NOTE**
>
> If you do not intend to use the autoinstall profile to create virtual guest systems, you can leave the drop-down set to the default choice *KVM Virtualized Guest*.

4 Finally, either provide the file contents with cut-and-paste or update the file from the local storage medium:

   • Paste it into the *File Contents* box and click *Create*, or

   • enter the file name in the *File to Upload* field and click *Upload File*.

Once done, four subtabs are available: *Details* (see Section "System Details > Details — [Prov]" (page 118)), *Bare Metal Kickstart* (see Section "Autoinstallation Details > Bare Metal Autoinstallation — [Prov]" (page 118)),*Variables* (see Section "Autoinstallation Details > Variables" (page 117)), and *Autoinstallable File* (see Section "Autoinstallation File — [Prov]" (page 121)) are available.

4.4.9.6 Autoinstallation > Bare Metal — [Prov]

Lists the IP addresses that have been associated with the profiles created by your organization. Click either the range or the profile name to access different tabs of the *Autoinstallation Details* page.

4.4.9.7 Autoinstallation > GPG and SSL Keys — [Prov]

Lists keys and certificates available for inclusion in Kickstart profiles and provides a means to create new ones. This is especially important for customers of SUSE Manager or the Proxy Server because systems kickstarted by them must have the server key im-

ported into SUSE Manager and associated with the relevant Kickstart profiles. Import it by creating a new key here and then make the profile association in the *GPG and SSL keys* subtab of the *Autoinstallation Details* page.

To create a new key/certificate, click the *create new stored key/cert* link in the upper-right corner of the page. Enter a description, select the type, upload the file, and click the *Update Key* button. Note that a unique description is required.

IMPORTANT

The GPG key you upload to SUSE Manager must be in ASCII format. Using a GPG key in binary format causes anaconda, and therefore the Kickstart process, to fail.

4.4.9.8 Autoinstallation > Distributions — [Prov]

The *Distributions* page enables you to find and create custom installation trees that may be used for automated installations.

NOTE

The *Distributions* page does not display distributions already provided. They can be found within the *Distribution* dropdown menu of the *Autoinstallation Details* page.

Before creating a distribution, you must make an installation tree available, as described in the *Automated Installation* chapter of the *SUSE Linux Enterprise Deployment Guide* or, respectively, the *Kickstart Installations* chapter of the *Red Hat Enterprise Linux System Administration Guide*. This tree must be located in a local directory on the SUSE Manager server.

Procedure 4.3   *Creating Distribution for Autoinstallation*

1 To create a new distribution, on the *Autoinstallable Distributions* plage click *create new distribution* in the upper right corner.

2 On the *Create Autoinstallable Distribution* page, provide the following data:

   2a Enter a label (without spaces) in the *Distribution Label* field, such as
   `my-orgs-sles-11-sp1` or `my-orgs-rhel-as-5`.

2b In the *Tree Path* field, paste the path to the base of the installation tree. For Red Hat Enterprise Linux systems, you can test this by appending "images/pxe-boot/README" to the URL in a Web browser, pressing Enter, and ensuring that the readme file appears.

2c Select the matching distribution from the *Base Channel* and *Installer Generation* drop-down menus, such as SUSE Linux for SUSE Linux Enterprise, or Red Hat Enterprise Linux 5 for Red Hat Enterprise Linux 5 client systems.

3 When finished, click the *Create Autoinstallable Distribution* button.

Autoinstallation > Distributions > Variables

Autoinstallation variables can be used to substitute values into Kickstart and AutoYaST profiles. To define a variable, create a name-value pair (*name/value*) in the text box.

For example, if you want to autoinstall a system that joins the network of a specified organization (for example the Engineering department) you can create a profile variable to set the ip address and the gateway server address to a variable that any system using that profile will use. Add the following line to the *Variables* text box.

```
IPADDR=192.168.0.28
GATEWAY=192.168.0.1
```

To use the distribution variable, use the name of the variable in the profile to substitute the value. For example, the network part of a Kickstart file looks like the following:

```
network --bootproto=static --device=eth0 --onboot=on --ip=$IPADDR \
  --gateway=$GATEWAY
```

The $IPADDR will be resolved to 192.168.0.28, and the $GATEWAY to 192.168.0.1.

NOTE

There is a hierarchy when creating and using variables in Kickstart files. System Kickstart variables take precedence over Profile variables, which in turn take precedence over Distribution variables. Understanding this hierarchy can alleviate confusion when using variables in Kickstarts.

Using variables are just one part of the larger Cobbler infrastructure for creating templates that can be shared between multiple profiles and systems. For more information about Cobbler and templates, refer to Chapter 8, *Cobbler* (page 225).

4.4.9.9 Autoinstallation > File Preservation — [Prov]

Collects lists of files to be protected and re-deployed on systems during Kickstart. For instance, if you have many custom configuration files located on a system to be kickstarted, enter them here as a list and associate that list with the Kickstart profile to be used.

To use this feature, click the *create new file preservation list* link at the top. Enter a suitable label and all files and directories to be preserved. Enter absolute paths to all files and directories. Then click *Create List*.

IMPORTANT

Although file preservation is useful, it does have limitations. Each list is limited to a total size of 1 MB. Special devices like `/dev/hda1` and `/dev/sda1` are not supported. Only file and directory names may be entered. No regular expression wildcards can be used.

When finished, you may include the file preservation list in the Kickstart profile to be used on systems containing those files. Refer to Section 4.4.9.4, "Create a New Kickstart Profile" (page 113) for precise steps.

4.4.9.10 Autoinstallation > Snippets — [Prov]

Use snippets to store common blocks of code that can be shared across multiple Kickstart or AutoYaST profiles in SUSE Manager. When you create a snippet, all profiles including that snippet will be updated accordingly.

4.5 Patches

Select the *Patches* tab from the top navigation bar to track the availability and application of patches to your managed systems.

The *Patches Overview* page displays relevant patches for at least one of your managed systems that have not been applied yet.

NOTE: Receiving Patches for Your System

To receive an e-mail when patches are issued for your system, go to *Overview > Your Preferences* and select *Receive e-mail notifications*.

SUSE distinguishes three types of patches: security updates, bug fix updates, and enhancement updates. Each patch is comprised of a summary of the problem and solution, including the RPM packages fixing the problem.

Icons are used to identify the three types:

- — Security Updates available, *strongly* recommended

- — Bug Fix Updates available, recommended

- — Enhancement Updates available, optional

A summary of each patch is provided in list form displaying the type, severity (for security updates), and subject of the patch, as well as the number of affected systems in your network.

In addition, you may view patches by product line at the following location: `http://download.novell.com/patch/psdb/`. An RSS feed with security updates is available at `http://www.novell.com/linux/security/suse_security.xml`.

4.5.1 Relevant Patches

The *Relevant Patches* page displays a customized list of patches applying to your registered systems. The list provides a summary of each patch, including its type, severity (for security updates), advisory number, synopsis, systems affected, and date updated.

Clicking on *Advisory* takes you to the *Details* page of the *Patch Details* page. Clicking on the number of associated systems takes you to the *Affected Systems* page of the *Patch Details* page. Refer to Section 4.5.2.2, "Patch Details" (page 128) for more information.

4.5.2 All Patches

The *All Patches* page displays a list of all patches released by SUSE. Like in the *Relevant Patches* page clicking either *Advisory* or the number of systems affected takes you to related tabs of the *Patch Details* page. Refer to Section 4.5.2.2, "Patch Details" (page 128) for more information.

4.5.2.1 Apply Patches

Patches include a list of updated packages. To apply patches to a system, the system must be entitled.

Apply all applicable patches to a system by clicking on *Systems > Systems* in the top and left navigation bars. Click on the name of an entitled system. Then in the *System Details* page click the *Patches* tab. When the relevant patch list appears, click *Select All* then *Apply Patches* on the bottom right-hand corner of the page. Only patches not scheduled, scheduled but failed, or canceled patches are listed. Pending updates are excluded.

In addition, management users can apply patches using two other methods:

- To apply a specific patch to one or more systems, locate it in the patch list and click on the number of systems affected, which takes you to the *Affected Systems* page of the *Patch Details* page. Select the individual systems to be updated and click the *Apply Patches* button. Double-check the systems to be updated on the confirmation page, then click the *Confirm* button.

- To apply more than one patch to one or more systems, select the systems from the *Systems* list and click the *Update List* button. Click the *System Set Manager* link in the left navigation bar, then click the *Systems* tab. After ensuring the appropriate systems are selected, click the *Patch* tab, select the patches to apply, and click the *Apply Patch* button. You can apply the patch as soon as possible or schedule a date and time for the patch to be applied. Then click the *Schedule Updates* button. You can follow the progress of the patch application via the *Pending Actions* list. Refer to Section 4.8, "Schedule" (page 148) for more details.

IMPORTANT

If you use scheduled package installation, the packages or patches are installed via the SUSE Manager daemon. You must enable the SUSE Manager daemon on your systems. Refer to Chapter 3, *SUSE Manager Daemon* (page 47) for more details.

The following rules apply to patches:

• Each package is a member of one or more channels. If a selected system is not subscribed to a channel containing the package, the update will not be installed on that system.

• If a newer version of the package is already installed on the system, the update will not be installed.

• If an older version of the package is installed, the package will be upgraded.

4.5.2.2 Patch Details

If you click on the advisory of a patch in the *Relevant* or *All* pages, its *Patch Details* page appears. This page is further divided into the following tabs:

Patch Details > Details

This subtab displays the patch report issued by SUSE. It provides a synopsis of the patch first, including the severity (for security updates), issue date, and any update dates. This is followed by a description of the patch and the steps required to resolve the issue.

Below the *Affected Channels* label, all channels that contain the affected package are listed. Clicking on a channel name displays the *Packages* subtab of the *Channel Details* page for that channel. Refer to Section 4.6.1.9, "Software Channel Details" (page 133) for more information.

Security updates list the specific vulnerability as tracked by http://cve.mitre.org. This information is listed below the *CVEs* label.

OVAL is an open vulnerability and assessment language promoted by Mitre, http://oval.mitre.org. Clicking on the link below the *Oval* label downloads this information to your system. More useful are the collected Novell/SUSE Linux security updates on http://support.novell.com/security/cve/.

Patch Details > Packages

This page provides links to each of the updated RPMs by channel. Clicking on the name of a package displays its *Package Details* page.

Patch Details > Affected Systems

This page lists systems affected by the patches. You can apply updates here. (See Section 4.5.2.1, "Apply Patches" (page 127).) Clicking on the name of a system takes you to its *System Details* page. Refer to Section 4.4.2.10, "System Details" (page 66) for more information.

To determine whether an update has been scheduled, refer to the *Status* column in the affected systems table. Possible values are: None, Pending, Picked Up, Completed, and Failed. This column identifies only the last action related to a patch. For instance, if an action fails and you reschedule it, this column shows the status of the patch as pending with no mention of the previous failure. Clicking a status other than None takes you to the *Action Details* page. This column corresponds to one on the *Patch* tab of the *System Details* page.

4.5.3 Advanced Search

The *Patches Search* page allows you to search through patches by specific criteria.

Figure 4.15 *Patches Search*

- *All Fields* — Search patches by synopsis, description, topic, or solution.

- *Patch Advisory* — The SUSE security team codifies advisories in the following way:

  ```
  SUSE-RU-2011:0030
  ```

  Searches can be done by year (such as 2011), by type of advisory, or full advisory name as in the example above.

- *Package Name* — Search particular packages by name:

  ```
  kernel
  ```

  Results will be grouped by advisory. For example, searching for 'kernel' returns all package names containing the term `kernel` grouped by advisory.

- *CVE* — The name assigned to the security advisory by the Common Vulnerabilities and Exposures (CVE) project at http://cve.mitre.org. For example:

  ```
  CVE-2006-4535
  ```

To filter patch search results, check or uncheck the boxes next to the type of advisory:

- Bug Fix Advisory — Patches that fix issues reported by users or discovered during development or testing.

- Security Advisory — Patches fixing a security issue found during development, testing, or reported by users or a software security clearing house. A security advisory usually has one or more CVE names associated with each vulnerability found in each package.

- Product Enhancement Advisory — Patches providing new features, improving functionality, or enhancing performance of a package.

4.6 Channels

If you click the *Channels* tab on the top navigation bar, the *Channels* category and links appear. The pages in the *Channels* category enable you to view and manage the channels and packages associated with your systems.

4.6.1 Software Channels

The *Software Channels* page is the first to appear in the *Channels* page. A software channel provides packages grouped by products or applications to ease the selection of packages to be installed on a system.

There are two types of software channels: base channels and child channels.

4.6.1.1 Base Channels

A base channel consists of packages built for a specific architecture and release. For example, all of the packages in SUSE Linux Enterprise Server 11 for the x86_64 architecture make up a base channel. The list of packages in SUSE Linux Enterprise Server 11 for the i586 architecture make up a different base channel.

A system must be subscribed to only one base channel assigned automatically during registration based upon the SUSE Linux Enterprise release and system architecture. In the case of paid base channels, an associated entitlement must exist.

4.6.1.2 Child Channels

A child channel is associated with a base channel and provides extra packages. For instance, an organization can create a child channel associated with SUSE Linux Enterprise Server on i586 architecture that contains extra packages for a custom application.

A system can be subscribed to multiple child channels of its base channel. Only packages provided by a subscribed channel can be installed or updated. Further, SUSE Manager customers have channel management authority. This authority gives them the ability to create and manage their own custom channels.

NOTE

Do not create child channels containing packages that are not compatible with the client system.

Channels can be further distinguished by relevance: *All Channels*, *SUSE Channels*, *Popular Channels*, *My Channels*, *Shared Channels*, and *Retired Channels*.

4.6.1.3 All Channels

Click *Software Channels* in the navigation bar to reach the *All Channels* page shown in Figure 4.16, "All Channels" (page 132). All channels available to your organization are listed. Links within this list go to different tabs of the *Software Channel Details* page. Clicking on a channel name takes you to the *Details* tab. Clicking on the number of packages takes you to the *Packages* tab. Clicking on the number of systems takes you to the *Subscribed Systems* tab. Refer to Section 4.6.1.9, "Software Channel Details" (page 133) for details.

Figure 4.16   *All Channels*
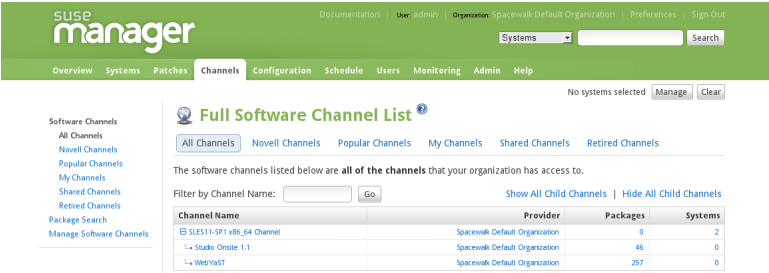
4.6.1.4 SUSE Channels

The *SUSE Channels* page displays the SUSE channels and their available child channels.

WARNING: SUSE Channels Cannot be Deleted

Once imported, SUSE channels cannot be deleted. Only custom software channels can be deleted.

4.6.1.5 Popular Channels

The *Popular Channels* page displays the software channels most subscribed by systems registered to your organization. You can refine the search by using the drop-down menu to list only the channels with at least a certain number of systems subscribed.

4.6.1.6 My Channels

The *My Channels* page displays all software channels that belong to your organization, including both SUSE and custom channels. Use the text box to filter by channel name.

4.6.1.7 Shared Channels

The *Shared Channels* page displays the channels shared with others in the organizational trust. For more information, refer to Section 6.6.2, "Sharing Content Channels between Organizations in a Trust" (page 202).

4.6.1.8 Retired Channels

The *Retired Channels* page displays available channels that have reached their end-of-life dates and do not receive updates.

4.6.1.9 Software Channel Details

If you click on the name of a channel, the *Software Channel Details* page appears. Here the following tabs are available:

Software Channel Details > Details

General information about the channel and its parent if applicable. This summary, description, and architecture is also displayed when clicking on a channel.

[Mgmt] — In addition, *Per-User Subscription Restrictions* can be set globally by SUSE Manager administrators and channel administrators. By default, any user can subscribe channels to a system. To manage user permissions, select *Only selected users within your organization may subscribe to this channel* and click *Update* to enter the *Subscribers* tab and grant specific users subscription permissions to a channel. SUSE Manager administrators and channel administrators can always subscribe any channels to a system.

[Mgmt] — Only customers with custom base channels can change their systems' base channel assignments via the SUSE Manager Web interface in two ways:

- Assign the system to a custom base channel.

- Revert subscriptions from a custom base channel to the appropriate distribution-based base channel.

NOTE

The assigned base channel must match the installed system. For example, a system running SUSE Linux Enterprise 10 for i586 cannot be registered to a SUSE Linux Enterprise 11 for i586 base channel. Use the file `/etc/SuSE -release` to check your product, architecture, version, and patchlevel.

Software Channel Details > Patches

List of patches to be applied to packages provided in the channel. The list displays advisory types, names, summaries, and issue dates. Clicking on an advisory name takes you to its *Patch Details* page. Refer to Section 4.5.2.2, "Patch Details" (page 128) for more information.

Software Channel Details > Packages

List of packages in the channel. Clicking on a package name takes you to the *Package Details* page. This page displays a set of tabs with information about the package, including architectures on which it runs, the package size, build date, package dependen-

cies, change log, list of files in the package, newer versions, and which systems have the package installed. Download the packages as RPMs.

To search for a specific package or a subset of packages, use the package filter at the top of the list. Enter a substring to search for package names containing the string. For example, typing `ks` in the filter might return: `ksconfig`, `krb5-workstation`, and `links`. The filter is case-insensitive.

Software Channel Details > Subscribed Systems

The list displays system names, base channels, and their levels of entitlement. Clicking on a system name takes you to its *System Details* page. Refer to Section 4.4.2.10, "System Details" (page 66) for more information.

[Mgmt] — In the case a child channel, you have the option to unsubscribe systems from this channel. Use the checkboxes to select the systems, then click the *Unsubscribe* button.

Software Channel Details > Target Systems

List of entitled systems eligible for subscription to the channel. This tab appears only for child channels. Use the checkboxes to select the systems, then click the *Confirm* and *Subscribe* button on the bottom right-hand corner. You will receive a success message or be notified of any errors. This can also be accomplished through the *Channels* tab of the *System Details* page. Refer to Section 4.4.2.10, "System Details" (page 66) for more information.

4.6.2 Package Search

Figure 4.17 *Package Search*

The *Package Search* page allows you to search through packages using various criteria (provided by the *What to search for* selection list):

- *Free Form* — a general keyword search useful when the details of a particular package and its contents are unknown.

- *Name Only* — Targeted search to find a specific package known by name.

- *Name and Summary* — Search for a package or program which might not show up in the respective package name but in its one-line summary.

- *Name and Description* — Search package names and their description. Search results for "web browser" include both graphical and text-based browsers.

The *Free Form* field additionally allows you to search using field names that you prepend to search queries and filter results by that field keyword.

For example, if you wanted to search all of the SUSE Linux Enterprise packages for the word `java` in the description and summary, type the following in the *Free Form* field:

```
summary:java  and description:java
```

Other supported field names for documentation search include:

- `name` — Search package names for a particular keyword,

- `version` — Search for a particular package version,

- `filename` — Search the package filenames for a particular keyword,

- `description` — Search the packages' detailed descriptions for a particular keyword,

- `summary` — Search the packages' brief summary for a particular keyword,

- `arch` — Search the packages by their architecture (such as i586, x86_64, or s390).

You can also limit searches to *Channels relevant to your systems* by clicking the checkbox. Additionally, you can restrict your search by platform or architecture.

4.6.3 Manage Software Channels

This tab allows administrators to create, clone, and delete custom channels. These channels may contain altered versions of distribution-based channels or custom packages.

4.6.3.1 *Manage Software Channels > Channel Details*

The default screen of the *Manage Software Channels* tab lists all available channels including custom, distribution-based, and child channels.

To clone an existing channel, click the *clone channels* link. Select the channel to be cloned from the dropdown menu, and click the *Create Channel* button. In the next screen select options for the new channel, including base architecture and GPG, then click *Create Channel*.

To create a new channel, click the *create new channel* link. Select the appropriate options for the new channel, including base architecture and GPG options, then click *Create Channel*. Note that a channel created in this manner is blank, containing no packages.

You must either upload software packages or add packages from other repositories. You may also choose to include patches in your custom channel.

Manage Software Channels > Channel Details > Details

This screen lists the selections made during channel creation and includes the *Globally Subscribable* checkbox that permits all users to subscribe systems to the channel.

Manage Software Channels > Channel Details > Managers

SUSE Manager administrators and channel administrators may alter or delete any channel. To grant other users rights to alter or delete this channel, check the box next to the user's name and click *Update*.

To allow all users to manage the channel, click the *Select All* button at the bottom of the list then click *Update*. To remove a user's right to manage the channel, uncheck the box next to their name and click *Update*.

Manage Software Channels > Channel Details > Patches

Channel managers can list, remove, clone, and add patches to their custom channel. Custom channels not cloned from a distribution may not contain patches until packages are available. Only patches that match the base architecture and apply to a package in that channel may be added. Finally, only cloned or custom patches may be added to custom channels. Patches may be included in a cloned channel if they are selected during channel creation.

Manage Software Channels > Channel Details > Packages

As with patches, administrators can list, remove, compare, and add packages to a custom channel.

To list all packages in the channel, click the *List / Remove Packages* link. Check the box to the left of any package you wish to remove, then click *Remove Packages*.

To add packages, click the *Add Packages* link. From the drop down menu choose a channel from which to add packages and click *View* to continue. Check the box to the left of any package you wish to add to the custom channel, then click *Add Packages*.

To compare packages in the current channel with those in another, select that channel from the drop-down menu and click *Compare*. Packages in both channel are compared, including architecture and version, and the results displayed on the next screen.

To make the two channels identical, click the *Merge Differences* button. In the next dialog, resolve any conflicts. *Preview Merge* allows you to review the changes before applying them to the channels. Select those packages that you wish to merge. Click *Merge Packages* then *Confirm* to perform the merge.

4.6.3.2 *Manage Software Channels > Manage Software Packages*

To manage custom software packages, list all software or view only packages in a custom channel. Select the respective channel from the drop-down menu and click *View Packages*.

4.6.3.3 *Manage Software Channels > Manage Repositories*

Add or manage custom or third-party package repositories and link the repositories to an existing channel. The repositories feature currently supports repomd repositories.

To create a new repository click the *create new repository* link at the top right of the *Manage Repositories* page. The *Create Repository* screen prompts you to enter a *Repository Label* such as `sles-11-x86_64` and a *Repository URL*. You may enter URLs pointing to mirror lists or direct download repositories, then click *Create Repository*.

To link the new repository to an existing software channel, select *Manage Software Channels* from the left menu, then click the Channel you want to link. In the channel's Detail page, click the *Repositories* subtab, then check the box next to the repository you want to link to the channel. Click *Update Repositories*.

To synchronize packages from a custom repository to your channel, click the *Sync* link from the channel's *Repositories* subtab, and confirm by clicking the *Sync* button.

You can also perform a sync via command-line by using the `spacewalk-repo-sync` command, which additionally allows you to accept keys.

4.7 Configuration

Only Configuration Administrators or a SUSE Manager Administrators see the *Configuration* tab. In addition, they must have at least one Provisioning entitlement, or the tab does not appear.

In this configuration portal, manage your configuration channels and files, centrally or limited to a single system. Centrally-managed files are available to multiple systems; changes to a single file affect all these systems. Each system with a Provisioning entitlement has also a local configuration channel, sometimes referred to as an override channel, and a sandbox channel.

4.7.1 Preparing Systems for Config Management

To manage a system's configuration with SUSE Manager, it must have the appropriate tools and the `config-enable` file installed. These tools should be available if you installed the system with the configuration management functionality using AutoYaST or Kickstart. If not, they can be found in the Tools child channel for your distribution. Download and install the latest `rhncfg*` packages:

- `rhncfg` — the base libraries and functions needed by all `rhncfg-*` packages,

- `rhncfg-actions` — the RPM package required to run configuration actions scheduled via SUSE Manager,

- `rhncfg-client` — the RPM package with a command line interface to the client features of the Configuration Management system,

- `rhncfg-management` — the RPM package with a command line interface used to manage SUSE Manager configuration.

First, enable your system to schedule configuration actions via Actions Control. Enter the `mgr-actions-control` command, provided by the `rhncfg-actions` RPM, on the client system to enable or disable specific actions. Refer to Section A.1, "Actions Control" (page 235) for instructions.

4.7.2 Overview

In the *Configuration Overview* monitor the status of your configuration files and the systems using them.

Configuration Summary
>   The panel provides quick information about your configuration files. Click on the blue text to the right to display relevant systems, channel details, or configuration files.

Configuration Actions
>   *Configuration Actions* offers direct access to the most common configuration management tasks. View or create files and channels or enable configuration management on your systems.

Recently Modified Configuration Files
>   The list shows which files have changed when and to which channel they belong. If no files have been changed, no list appears. Click on the name of a file to see its *Details* page. Click on the channel name to see its *Channel Details* page.

Recently Scheduled Configuration Deployments
>   Each scheduled action is listed along with the status of the action. Any scheduled configuration task, from enabling configuration management on a system to deploying a specific configuration file, is displayed. Here you can quickly assess if all tasks have been successfully carried out or fix any problems. Clicking on the blue text displays the *System Details > Schedule* page for the specified system.

4.7.3 Configuration Channels

As mentioned above, SUSE Manager manages both central and local configuration channels and files. Central configuration management allows you to deploy configuration files to multiple systems. Local configuration management allows you to specify overrides or configuration files that are not changed by subscribing the system to a central channel.

Central configuration channels must be created via the link on this page. Local configuration channels already exist for each system to which a Provisioning entitlement has been applied.

Click on the name of the configuration channel to see the details page for that channel. If you click on the number of files in the channel, you are taken to the *List/Remove Files* page of that channel. If you click on the number of systems subscribed to the configuration channel, you are taken to the *Systems > Subscribed Systems* page for that channel.

To create a new central configuration channel:

1. Click the *create new config channel* link in the upper right of this screen.

2. Enter a name for the channel.

3. Enter a label for the channel. This field must contain only alphanumeric characters, "-", "_", and "."

4. Enter a mandatory description for the channel that allows you to distinguish it from other channels. No character restrictions apply.

5. Press the *Create Config Channel* button to create the new channel.

6. The following page is a subset of the *Channel Details* page and has three subtabs: *Overview*, *Add Files*, and *Systems*. The *Channel Details* page is discussed in Section 4.7.3.1, "*Configuration > Configuration Channels > Configuration Channel Details*" (page 142).

4.7.3.1 *Configuration > Configuration Channels > Configuration Channel Details*

Overview
> This subtab is very similar to the *Configuration Overview* page. The *Channel Information* panel provides status information for the contents of the channel. The *Configuration Actions* panel provides access to the most common configuration tasks. The main difference is the *Channel Properties* panel. By clicking on the *Edit Properties* link, you can edit the name, label, and description of the channel.

List/Remove Files
> This tab only appears if there are files in the configuration channel. You can remove files or copy the latest versions into a set of local overrides or into other central configuration channels. Check the box next to files you wish to manipulate and click the respective action button.

Add Files

The *Add Files* subtab has three subtabs of its own, which allow you to *Upload*, *Import*, or *Create* configuration files to be included in the channel.

Upload File

To upload a file into the configuration channel, browse for the file on your local system, populate all fields, and click the *Upload Configuration File* button. The *Filename/Path* field is the absolute path where the file will be deployed.

You can set the *Ownership* via the *user name* and *group name* as well as the *Permissions* of the file when it is deployed.

If the client has SELinux enabled, you can configure *SELinux contexts* to enable the required file attributes (such as user, role, and file type) that allow it to be used on the system.

If the configuration file includes a macro (a variable in a configuration file), enter the symbol that marks the beginning and end of the macro.

Import Files

To import files from other configuration channels, including any locally-managed channels, check the box to the left of any file you wish to import. Then press the *Import Configuration File(s)* button.

NOTE

A sandbox icon indicates that the listed file is currently located in a local sandbox channel. Files in a system's sandbox channel are considered experimental and could be unstable. Use caution when selecting them for a central configuration channel.

Create File

Create a configuration file, directory, or symbolic link from scratch to be included in the configuration channel.

First, choose whether you want to create a text file, directory, or symbolic link (symlink) in the *File Type* section. In the `Filename/Path` text box, set the absolute path to where the file should be deployed. If you are creating a symlink, indicate the target file and path in the *Symbolic Link Target Filename/Path* text box.

Enter the *User name* and *Group name* for the file in the *Ownership* section, as well as the *File Permissions Mode*.

If the client has SELinux enabled, you can configure *SELinux contexts* to enable the required file attributes (such as user, role, and file type) that allow it to be used on the system.

If the configuration file includes a macro, enter the symbol that marks the beginning and end of the macro. Then enter the configuration file content in the *File Contents* field, using the script dropdown menu to choose the appropriate scripting language. Press the *Create Configuration File* button to create the new file.

Deploy Files

This subtab only appears when there are files in the channel. Deploy all files by clicking the *Deploy All Files* button or check selected files and click the *Deploy Selected Files* button. Select to which systems the file(s) should be applied. All systems subscribed to this channel are listed. If you wish to apply the file to a different system, subscribe it to the channel first. To deploy the files, press *Confirm and Deploy to Selected Systems*.

Systems

Manage systems subscribed to the configuration channel via two subtabs:

Subscribed Systems

All systems subscribed to the current channel are displayed. Click on the name of a system to see the *System Details* page.

Target Systems

This subtab displays a list of systems enabled for configuration management but not yet subscribed to the channel. To add a system to the configuration channel, check the box to the left of the system's name and press the *Subscribe System* button.

4.7.4 Configuration Files

This tab allows you to manage your configuration files independently. Both centrally-managed and locally-managed files can be reached from subtabs.

> **NOTE**
>
> By default, the maximum file size for configuration files is 128KB. If you need to change that value, find and modify the following line in the `/etc/rhn/default/rhn_web.conf` file:
>
> ```
> web.maximum_config_file_size=128
> ```
>
> You must also find and change the following line in the `/etc/rhn/default/rhn_server.conf` file to the same value:
>
> ```
> maximum_config_file_size=131072
> ```
>
> Change the value in both files from `131072` to the desired value in bytes.

4.7.4.1 Centrally-managed Files

Centrally-managed files are available to multiple systems. Changing a file within a centrally-managed channel may result in changes to several systems.

This page lists all files currently stored in your central configuration channel. Click on the *Path* of a file to see its *Configuration File Details* page. Click the name of the configuration channel to see its *Channel Details* page. Clicking on the number of systems shows you all systems currently subscribed to the channel containing that file. Click on the number of overriding systems to see all systems that have a local (or override) version of the configuration file. The centrally-managed file will not be deployed to those systems.

4.7.5 Locally-Managed Files

Locally-managed configuration files apply to only one system. They may be files in the system's sandbox or files that can be deployed to the system at any time. Local files have higher priority than centrally-managed files. If a system is subscribed to a configuration channel with a given file and also has a locally-managed version of that file, the locally-managed version will be deployed.

The list of all local (override) configuration files for your systems includes the local configuration channels and the sandbox channel for each Provisioning-entitled system.

Click the *Path* of the file to see its *Config File Details*. Click the name of the system to which it belongs to see its *System Details > Configuration > Configuration > Overview* page.

4.7.5.1 Including Macros in your Configuration Files

Being able to store and share identical configurations is useful, but what if you have many variations of the same configuration file? What do you do if you have configuration files that differ only in system-specific details, such as host name and MAC address?

Traditional file management would require to upload and distribute each file separately, even if the distinction is nominal and the number of variations is in the hundreds or thousands. SUSE Manager addresses this by allowing the inclusion of macros, or variables, within the configuration files it manages for Provisioning-entitled systems. In addition to variables for custom system information, the following standard macros are supported:

- rhn.system.sid

- rhn.system.profile_name

- rhn.system.description

- rhn.system.hostname

- rhn.system.ip_address

- rhn.system.custom_info(key_name)

- rhn.system.net_interface.ip_address(eth_device)

- rhn.system.net_interface.netmask(eth_device)

- rhn.system.net_interface.broadcast(eth_device)

- rhn.system.net_interface.hardware_address(eth_device)

- rhn.system.net_interface.driver_module(eth_device)

To use this powerful feature, either upload or create a configuration file via the *Configuration Channel Details* page. Then open its *Configuration File Details* page and in-

clude the supported macros of your choice. Ensure that the delimiters used to offset your variables match those set in the *Macro Start Delimiter* and *Macro End Delimiter* fields and do not conflict with other characters in the file. We recommend that the delimiters be two characters in length and must not contain the percent (%) symbol.

For example, you may have a file applicable to all of your servers that differs only in IP address and host name. Rather than manage a separate configuration file for each server, you may create a single file, such as `server.conf`, with the IP address and host name macros included.

```
hostname={| rhn.system.hostname |}
ip_address={| rhn.system.net_interface.ip_address(eth0) |}
```

Upon delivery of the file to individual systems, whether through a scheduled action in the SUSE Manager website or at the command line with the SUSE Manager Configuration Client (`mgrcfg-client`), the variables will be replaced with the host name and IP address of the system as recorded in SUSE Manager's System Profile. In the above example configuration file the deployed version resembles the following:

```
hostname=test.example.domain.com
ip_address=177.18.54.7
```

To capture custom system information, insert the key label into the custom information macro (rhn.system.custom_info). For instance, if you developed a key labeled "asset" you can add it to the custom information macro in a configuration file to have the value substituted on any system containing it. The macro would look like this:

```
asset={@ rhn.system.custom_info(asset) @}
```

When the file is deployed to a system containing a value for that key, the macro gets translated, resulting in a string similar to the following:

```
asset=Example#456
```

To include a default value, for instance if one is required to prevent errors, you can append it to the custom information macro, like this:

```
asset={@ rhn.system.custom_info(asset) = 'Asset #' @}
```

This default is overridden by the value on any system containing it.

Using the SUSE Manager Configuration Manager (`mgrcfg-manager`) will not translate or alter files, as this tool is system agnostic. `mgrcfg-manager` does not depend on system settings. Binary files cannot be interpolated.

4.7.6 Systems

This page displays status information about your system in relation to configuration. There are two subtabs: *Managed Systems* and *Target Systems*.

4.7.6.1 Managed Systems

By default the *Configuration > Systems* page is displayed. The listed systems have been fully prepared for configuration file deployment. The number of local and centrally-managed files is displayed. Clicking the name of a system shows its *System Details > Configuration > Overview* page. Clicking on the number of local files takes you to the *System Details > Configuration > View/Modify Files > Locally-Managed Files* page, where you manage which local (override) files apply to the system. Clicking on the number of centrally-managed files takes you to the *System Details > Configuration > Manage Configuration Channels > List/Unsubscribe from Channels* page. Here you unsubscribe from any channels you wish.

4.7.6.2 Target Systems

Here you see the systems either not prepared for configuration file deployment or not yet subscribed to a configuration channel. The table has three columns. The first identifies the system name, the second shows whether the system is prepared for configuration file deployment, and the third lists the steps necessary to prepare the system. To prepare a system, check the box to the left of the profile name then press the *Enable SUSE Manager Configuration Management* button. All of the preparatory steps that can be automatically performed are scheduled by SUSE Manager.

> **NOTE**
>
> You will have to perform some manual tasks to enable configuration file deployment. Follow the on-screen instructions provided to assist with each step.

4.8 Schedule

If you click the *Schedule* tab on the top navigation bar, the *Schedule* category and links appear. These pages enable you to track the actions carried out on your systems. An

action is a scheduled task to be performed on one or more client systems. For example, an action can be scheduled to apply all patches to a system.

SUSE Manager keeps track of the following action types:

1. package alteration (installation, upgrade, and removal),

2. rollback package actions,

3. system reboots,

4. patches,

5. configuration file alteration (deploy, upload, and diff),

6. hardware profile updates,

7. package list profile updates,

8. automated installation initiation,

9. remote commands.

Each page in the *Schedule* category represents an action status.

4.8.1 Pending Actions

As shown in Figure 4.18, "Schedule - Pending Actions" (page 150), the *Pending Actions* page appears by default when clicking *Schedule* in the top navigation bar. It displays actions not yet started or still in progress.

Figure 4.18 *Schedule - Pending Actions*
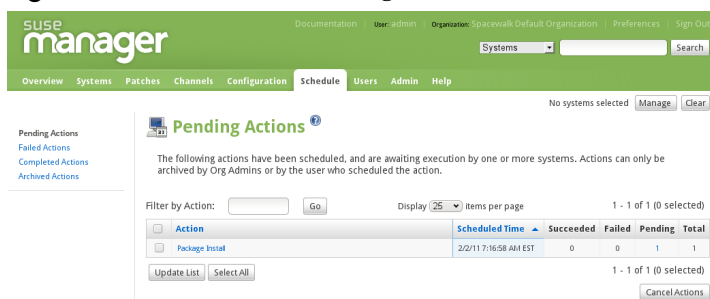
4.8.2 Failed Actions

Sometimes actions cannot be completed. If the action returns an error, it is displayed here.

4.8.3 Completed Actions

List of actions successfully carried out.

4.8.4 Archived Actions

If you selected actions to store for review, they are displayed here.

4.9 Users — [Mgmt]

Only SUSE Manager administrators can see the *Users* tab on the top navigation bar. If you click the tab, the *Users* category and links appear. Here you grant and edit permissions for those who administer your system groups. Click on a name in the *User List* to modify the user.

To add new users to your organization, click the *create new user* link on the top right corner of the page. On the next page, the *Create User*, fill in the required values for the new user.

Once all fields are completed, click the *Create Login* button. SUSE Manager now sends an e-mail to the specified address and takes you back to the *Users > User List* page. If you wish to set permissions and options for the new user, click on the name in the list. The *User Details* page for this user provides several subtabs of options. Refer to Section 4.9.1.1, "*User List > Active > User Details* — [Mgmt]" (page 152) for detailed descriptions of each subtab.

4.9.1 *User List > Active* — [Mgmt]

The user list shows all active users of your SUSE Manager account and displays basic information about each user: username, real name, roles, and date of their last sign in.

As shown in Figure 4.19, "User List" (page 151), each row in the *User List* represents a user within your organization. There are four columns of information for each user:

- *Username* — The login name of the user. Clicking on a username, displays the *User Details* page for the user. Refer to Section 4.9.1.1, "*User List > Active > User Details* — [Mgmt]" (page 152) for more information.

- *Real Name* — The full name of the user (last name first).

- *Roles* — List of the user's privileges, such as organization administrator, Channel administrator and normal user. Users can have multiple roles.

- *Last Sign In* — Shows when the user last logged into SUSE Manager.

Figure 4.19   *User List*

4.9.1.1 *User List > Active > User Details* — [Mgmt]

In the *User Details* page SUSE Manager administrators manage the permissions and activity of all users. Here you can also delete or deactivate users.

Users can be deactivated directly in the SUSE Manager Web interface. SUSE Manager administrators can deactivate or delete users of their organization, but users can also deactivate their own accounts.

Deactivated users cannot log in to the SUSE Manager Web interface or schedule any actions. SUSE Manager administrators cannot be deactivated until that role is removed from their account. Actions scheduled by a user prior to their deactivation remain in the action queue. Deactivated users can be reactivated by SUSE Manager administrators.

WARNING: Irreversible Deletion

User deletion is irreversible; exercise it with caution. Consider deactivating the user first in order to assess the effect deletion will have on your infrastructure.

To deactivate a user:

1 Click on a user name to navigate to the *User Details* tab.

2 Verify that the user is not a SUSE Manager administrator. If they are, uncheck the box to the left of that role and click the *Submit* button.

3 Click the *deactivate user* link in the upper right of the screen.

4 Click the *Deactivate User* button in the lower right to confirm.

To delete a user:

1 Click on a user name to navigate to the *User Details* tab.

2 Verify that the user is not a SUSE Manager administrator. Uncheck the box to remove the role if necessary.

3 Click the *delete user* link in the upper right.

4 Click the *Delete User* button to permanently delete the user.

For instructions to deactivate your own account, refer to Section 4.3.1.3, "Account Deactivation" (page 59).

User List > Active > User Details > Details — **[Mgmt]**

This is the default *User Details* tab, which displays the username, first name, last name, e-mail address, and roles of a user. Edit this information as needed and click *Update*. When changing a user's password, you will only see asterisks as you type.

To delegate responsibilities within your organization, SUSE Manager provides several roles with varying degrees of access. This list describes the permissions of each role and the differences between them:

- *User* — Also known as a *System Group User*, this is the standard role associated with any newly created user. This person may be granted access to manage system groups and software channels, if the SUSE Manager administrator sets the roles accordingly. The systems must be in system groups for which the user has permissions to manage them. Remember, however, all globally subscribable channels may be used by anyone.

- *Activation Key Administrator* — This role is designed to manage your collection of activation keys. A user assigned to this role can modify and delete any key within your organization.

- *Channel Administrator* — This role provides a user with full access to all software channels within your organization. These requires the SUSE Manager synchronization tool (`mgr-ncc-sync`). The channel administrator may change the base channels of systems, make channels globally subscribable, and create entirely new channels.

- *Organization Administrator* — This role provides a user with all the permissions other admistrators have, namely the activation key, configuration, monitoring, channel, and system group administrator.

- *Configuration Administrator* — This role enables a user to manage the configuration of systems within the organization, using either the SUSE Manager Web interface or the `rhncfg-management`.

- *Monitoring Administrator* — This role allows for the scheduling of probes and oversight of other monitoring infrastructure. This role is available only on a monitoring-enabled SUSE Manager server. Activate monitoring in *Admin > SUSE Manager*

Configuration > General and click on *Enable Monitoring*. See Section 4.10, "Monitoring — [Mon]" (page 157) for more information.

- *SUSE Manager Administrator* — This role allows a user to perform any function available in SUSE Manager. As the master account for your organization, the person holding this role can alter the privileges of all other accounts, as well as conduct any of the tasks available to the other roles. Like with other roles, multiple SUSE Manager administrators may exist. Go to *Admin > Users* and click the check box in the *SUSE Manager Admin?* row. *SUSE Manager Administrator* manage foreign organizations; for example, a *SUSE Manager Administrator* can only create users for an organization, if he is entitled with organization administrator privileges for this organization.

- *System Group Administrator* — This role is one step below SUSE Manager administrator: full authority is limited to systems or system groups to which access is granted. The System Group Administrator can create new system groups, delete any assigned systems from groups, add systems to groups, and manage user access to groups.

Being a SUSE Manager administrator enables you to remove administrator rights from other users. It is possible to remove your own privileges as long as you are not the only SUSE Manager administrator.

To assign a new role to a user, check the respective box. SUSE Manager administrators are automatically granted administration access to all other roles, signified by grayed-out checkboxes. Click *Submit* to submit your changes.

User List > Active > User Details > System Groups — [Mgmt]

This tab displays a list of system groups the user may administer. SUSE Manager administrators may use the check boxes to set this user's access permissions to each system group. Check or uncheck the box to the left of the system group and click the *Update Permissions* button to save the changes.

SUSE Manager administrators may select one or more default system groups for a user. When the user registers a system, it gets assigned to the selected group or groups. This allows the user to access the newly-registered system immediately. System groups to which this user has access are preceded by an (*).

User List > Active > User Details > Systems — [Mgmt]

This tab lists all systems a user can access according to the system groups assigned to the user. To carry out tasks on some of these systems, select the set of systems by checking the boxes to the left and click the *Update List* button. Use the System Set Manager page to execute actions on those systems. Clicking the name of a system takes you to its *System Details* page. Refer to Section 4.4.2.10, "System Details" (page 66) for more information.

User List > Active > User Details > Channel Permissions — [Mgmt]

This tab lists all channels available to your organization. Grant explicit channel subscription permission to a user for each of the channels listed by checking the box to the left of the channel, then click the *Update Permissions* button. Permissions granted by a SUSE Manager administrator or channel administrator have no checkbox but a check icon just like globally subscribable channels.

User List > Active > User Details > Channel Permissions > Subscription — [Mgmt]

Identifies channels to which the user may subscribe systems. To change these, select or unselect the appropriate checkboxes and click the *Update Permissions* button. Note that channels subscribable due to the user's administrator status or the channel's global settings cannot be altered. They are identified with a check icon.

User List > Active > User Details > Channel Permissions > Management — [Mgmt]

Identifies channels the user may manage. To change these, select or unselect the appropriate checkboxes and click the *Update Permissions* button. The permission to manage channels does not enable the user to create new channels. Note that channels automatically manageable through the user's admin status cannot be altered. These channels are identified with a check icon. Remember, SUSE Manager administrators and channel administrators can subscribe to or manage any channel.

User List > Active > User Details > Preferences — **[Mgmt]**

Configure whether the user receives e-mail notifications, the number of entries displayed per list page, and the timezone of the user. Make selections and click the *Save Preferences* button to update.

- E-Mail Notification — Determine whether this user should receive e-mail every time a patch alert is applicable to one or more systems in his or her SUSE Manager account, as well as daily summaries of system events.

- SUSE Manager List Page Size — Maximum number of items that appear in a list on a single page. If the list contains more items than can be displayed on one page, click the *Next* button to see the next page. This preference applies to the user's view of system lists, Errata lists, package lists, and so on.

- "Overview" Start Page — Configure, which information to be displayed regarding on the "Overview" page upon login.

Change these options to fit your needs then click the *Save Preferences* button.

User List > Active > User Details > Addresses — **[Mgmt]**

This tab lists the addresses associated with the user's account. To update this information, click the appropriate *Edit this address* link, enter the relevant information, and click the *Update* button.

User List > Active > User Details > Notification Methods — **[Mon]**

This tab lists e-mail and pager addresses designated to receive alerts from monitoring probes. To set up alerts, click *Create New Method* and fill in the fields accordingly. To receive alerts via pager, select the associated checkbox to have the messages sent in a shorter format. When finished, click *Create Method*. The method shows up in the methods list, where it can be edited and deleted.

If a notification method has probes attached, they are listed as well. If you are a monitoring administrator but don't have management rights for a system, its *System Details* and probe's *Current State* page are not accessible via links in their names. As always, SUSE Manager administrators have full access to all aspects of your SUSE Manager account.

4.9.2 *User List > Deactivated* — [Mgmt]

The list of deactivated users also allows you to reactivate any of them. Click the check box to the left of their name and click the *Reactivate* button then the *Confirm* button. Reactivated users retain the permissions and system group associations they had when they were deactivated. Clicking a user name shows the *User Details* page.

4.9.3 *User List > All* — [Mgmt]

The *All* page lists all users that belong to your organization. In addition to the fields listed in the previous two screens, the table of users includes a *Status* field. This field indicates whether the user is *Active* or *Deactivated*. Deactivated users are also grayed out to indicate their status. Click on the user name to see the *User Details* page.

4.10 Monitoring — [Mon]

If you click the *Monitoring* tab on the top navigation bar, the *Monitoring* category and links appear. If you do not see the tab, activate monitoring in *Admin > SUSE Manager Configuration > General* and click the *Enable Monitoring* checkbox.

Manage the configuration of your monitoring infrastructure and view the results of probes monitoring entitled systems.

Initiate monitoring of a system through the *Probes* tab on the *System Details* page. Refer to Section 4.4.2.10, "System Details" (page 66) for a description of the tab. See Appendix B, *Probes* (page 251) for the complete list of available probes.

4.10.1 *Status* — [Mon]

Click *Monitoring* in the top navigation bar to see the *Probe Status List*. The page displays the summary count of probes in the various states and provides a simple interface to find problematic probes quickly. Note that the probe totals in the tabs at the top of the page may not match the numbers of probes displayed in the tables below. The counts at the top include probes for all systems in your organization, while the tables only display probes on those systems you have access to as system group administrator. Also, the probe counts displayed here may be out of sync by as much as one minute.

The following list describes each state and identifies the icons associated with them:

- — Critical - The probe has crossed a "critical" threshold.

- — Warning - The probe has crossed a "warning" threshold.

- — Unknown - The probe is not able to accurately report metric or state data.

- — Pending - The probe has been scheduled but not yet run or is unable to run.

- — OK - The probe is running successfully.

The *Probe Status List* page contains tabs for each of the possible states, as well as one that lists all probes. Each table contains columns indicating probe state, the monitored system, the probes used, and the date and time the state was last updated.

In these tables, clicking the name of the system takes you to the *Probes* tab of the *System Details* page. Clicking the name of the probe takes you to its *Current State* page. From there, you may edit the probe, delete it, and generate reports based upon its results.

Monitoring data and probe status information is also available on the Web interface of SUSE Manager, but here it can be exported as a CSV file. Click on the *Download CSV* links throughout the Monitoring pages to download CSV files of relevant information. The exported data may include, but is not limited to:

- probe status,

- all probes in a given state ("ok", "warn", "unknown", "critical", "pending"),

- a probe event history.

4.10.1.1 *Probe Status > Critical* — [Mon]

The probes that have crossed their "critical" thresholds or reached a critical status by some other means. For instance, some probes become critical (rather than unknown) when exceeding their timeout period.

4.10.1.2 *Probe Status > Warning* — **[Mon]**

The probes that have crossed their "warning" thresholds.

4.10.1.3 *Probe Status > Unknown* — **[Mon]**

The probes that cannot collect the metrics needed to determine probe state. Most but not all probes enter an unknown state when exceeding their timeout period. This may mean that the timeout period should be increased, or the connection cannot be established to the monitored system.

It is also possible the probes' configuration parameters are not correct and their data cannot be found. This state may also indicate that a software error has occurred.

4.10.1.4 *Probe Status > Pending* — **[Mon]**

The probes whose data have not been received by SUSE Manager. This state is expected for a probe that has just been scheduled but has not yet run. If all probes go into a pending state, your monitoring infrastructure may be failing.

4.10.1.5 *Probe Status > OK* — **[Mon]**

The probes that have run successfully without exception. This is the state desired for all probes.

4.10.1.6 *Probe Status > All* — **[Mon]**

All probes scheduled on systems in your account, listed in alphabetical order by the name of system.

4.10.1.7 *Current State* — **[Mon]**

Identifies the selected probe's status and when it last ran, while providing the ability to generate a report on the probe. Although this page is integral to monitoring, it is found under the *Probes* tab within the *System Details* page since its configuration is specific to the system being monitored.

To view a report of the probe's results, choose a relevant duration using the *date* fields and decide whether you would like to see metric data, the state change history or both. To obtain metric data, select the metric(s) on which you wish to see a report, and decide via the checkboxes whether the results should be shown in a graph, an event log, or both. Then click the *Generate report* button at the bottom of the page. If no data exist for the probe's metrics, you are presented with the following message:

```
NO DATA SELECTED TIME PERIOD AND METRIC
```

4.10.2 Scout Config Push — [Mon]

Displays the status of your monitoring infrastructure. Anytime you make a change to your monitoring configuration, such as adding a probe to a system or editing a probe's thresholds, you must reconfigure your monitoring infrastructure. Do this by selecting the SUSE Manager Server's checkbox and clicking *Push Scout Configs*. The table on this page identifies the date and time of requested and completed pushes.

Clicking the name of the server opens its SUSE Manager monitoring daemon SSH public key. This allows you to copy and paste the SSH key to the systems that are monitored by the scout. This is required in order for the SUSE Manager network monitoring daemon to connect to SUSE Manager.

4.10.3 *Notification* — [Mon]

Identifies the contact methods that have been established for your organization. These methods contain email or pager addresses designated to receive alerts from probes.

The various notification methods available to your organization are listed here on the default *Notification* screen. The methods are listed by user.

To create a new notification method, click on the name of the user to be notified. The *User Details > Notification Methods* page appears. Refer to Section "*User List > Active > User Details > Notification Methods* — [Mon]" (page 156) for further information. Click on the title of the notification method to edit the properties of the method.

4.10.3.1 *Notification > Filters*

Notification filters allow you to create long-term rules that suspend, redirect, or automatically acknowledge standard notifications or send supplemental notifications. This may help to manage verbose or frequent probe communication.

Notification > Notification Filters > Active Filters

This is the default screen for the *Notification Filters* tab. It lists all active filters available for your organization. Click the name of the filter to edit the properties of the filter.

To create a notification filter, click the *create new notification filter* link in the upper right of the screen. Configure each option listed below and click the *Save Filter* button to create the filter.

1. *Description*: Enter a value that allows you to distinguish this filter from others.

2. *Type*: Determine what action the filter should take: redirect, acknowledge, suspend, or supplement the incoming notification.

3. *Send to*: The *Redirect Notification* and *Supplemental Notification* options in step two require an email address to which to send the notifications. The remaining options require no email address.

4. *Scope*: Determine which monitoring components are subject to the filter.

5. *Organization/Scout/Probe*: This option allows you to select the organization, scout(s), or probe(s) to which this filter applies. To select multiple items from the list, hold the Ctrl key while clicking the names of the items. To select a range of items, hold the Shift key while clicking on the first and last items in the range.

6. *Probes in State*: Select which probe state(s) relate to the filter. For example, you may choose to create a supplemental notification for critical probes only. Un-check the box to the left of any state you want the filter to ignore.

7. *Notifications sent to*: This is the method to which the notification would be sent if no filter were in place. You may, for example, redirect notifications that would normally go to a user should that individual go on vacation, leaving all other notifications from the probe unchanged.

8. *Match Output*: Select precise notification results by entering a regular expression here. If the "Message:" portion of the notification does not match the regular expression, the filter is not applied.

9. *Recurring*: Select whether a filter runs continuously or on a recurring basis. A recurring filter runs multiple times for a period of time smaller than the duration of the filter. For example, a recurring filter could run for 10 minutes of every hour between the start and end times of the filter. A non-recurring filter runs continuously between the start and end times of the filter.

10. *Beginning*: Enter a date and time for the filter to begin operation.

11. *Ending*: Enter an end date and time for the filter.

12. *Recurring Duration*: Choose how long a recurring filter instance is active. It starts at the *Beginning* time specified above. Any notification generated outside the specified duration is not filtered.

13. *Recurring Frequency*: Specify how often the filter is activated.

Notification filters cannot be deleted. However, a filter may be canceled. Set the end date to some time in the past but after the start date, or else the change fails. Another method is to select a set of filters from the *Active* page and click the *Expire Notification Filters* button in the lower right. These filters are then canceled and appear in the *Expired Filters* tab.

Notification > Notification Filters > Expired Filters

This tab lists all notification filters whose end date has passed. Expired filters are stored indefinitely; this allows an organization to recycle useful filters as needed and provides a record for troubleshooting.

4.10.4 Probe Suites — [Mon]

Probe suites allow you to configure and apply one or more probes to a system or systems. Probe suites may be configured once and then applied to any number of systems in a batch. This approach saves time and provides consistency for Monitoring customers.

To create and apply a probe suite, first create an empty probe suite, then configure member probes, and finally apply the suite to selected systems. Proceed as follows:

1 From the *Monitoring > Probe Suites* page, select the *create probe suite* link. Enter a distinct name for the probe suite a brief description of the suite. Click the *Create Probe Suite* button to continue.

2 Add and configure the probes comprised in the suite. Click the *create new probe* link in the upper right.

3 Configure the probe as described in Section "System Details > Monitoring — [Mon]" (page 82) and click the *Create Probe* button. Repeat this process until all desired probes have been added.

NOTE

Your mail transfer agent must be configured correctly on your SUSE Manager server and each client system to which the probe suite is applied must have the `rhnmd` daemon installed and running. Refer to the Installation Guide (↑Installation Guide) for additional information.

---

4 Add the systems to which the probe suite applies. Click the *add systems to probe suite* link in the upper right of the screen to continue.

5 The next page displays a list of all systems with monitoring entitlements. Check the box to the left of the system(s) to which you wish to apply the probe suite, select the monitoring scout you wish to use, and click the *Add systems to probe suite* button to create the probe suite.

You can either delete or detach probes from the suite. Detaching a probe disassociates the probe from the suite and converts it to a system-specific probe. Changes to the detached probe only affect that system. Deleting a probe removes it from the suite and from all systems.

To remove a probe from a suite do the following:

1 In the *Monitoring > Probe Suites* page, click on the name of the probe suite you wish to modify.

2 Select the *Probes* subtab.

3 Check the box next to the probe you wish to remove.

4 Click the *Delete probes from Probe Suites* button.

You may also remove a system from the probe suite. There are two ways to accomplish this. The first method is to detach the system from the probe suite. When you do so, the system still has the same probes assigned to it. However, you now have the ability to configure these probes individually without affecting any other systems. For more information about removing probes from an individual system, refer to Section "System Details > Monitoring — [Mon]" (page 82).

To detach a system from the suite:

1 From the *Monitoring > Probe Suites* page, click the name of the probe suite you wish to modify.

2 Select the *Systems* subtab.

3 Check the box next to the system(s) you wish to remove from the probe suite.

4 Click the *Detach System(s) from Probe Suite* button.

The second method is to detach the suite from the system and with it all probes.

NOTE

This action deletes all of the suites' probes from the system as well as time and event logs. This action is irreversible.

To remove a probe suite from a system and delete all associated probes follow these steps:

1 On the *Monitoring > Probe Suites* page, click the name of the probe suite you wish to remove.

2 Select the *Systems* subtab.

3 Check the box next to the system(s) you wish to remove from the probe suite.

4 Click the *Remove System(s) from Probe Suite* button.

Finally, as with single probes, you may download a CSV file containing information about probe suites. Click the *Download CSV* link at the bottom of the *Monitoring > Probe Suites* page to download the file.

4.10.5 General Config — [Mon]

The default monitoring settings are derived from your SUSE Manager installation and can be changed here. Configure your organization-wide monitoring infrastructure, change the mail exchange server or the recipient of all administrative e-mails from SUSE Manager. Beware that modifying this page causes the monitoring services on the SUSE Manager to reset. This triggers restart events for the monitoring services on all monitoring-enabled SUSE Manager servers to ensure they immediately reload the changed configuration. To save and roll out the changed configuration, click *Update Config*.

4.11 Admin

The *Admin* page allows SUSE Manager customers to manage the basic configuration, including creating and managing multiple organizations. Only the SUSE Manager administrator can access the *Admin* page.

4.11.1 *Admin > Organizations*

The multiple organizations feature allows administrators to create and manage multiple organizations across SUSE Manager. Administrators can appropriate software and system entitlements across various organizations, as well as control an organization's access to system management tasks. For more information about using the multiple organizations feature, refer to Chapter 6, *Multiple Organizations* (page 187).

4.11.2 *Admin > SUSE Manager Configuration*

This tab is split into subtabs that allow you to configure most aspects of SUSE Manager. If you change the configuration, restart SUSE Manager on the final tab for the changes to take effect.

4.11.2.1 *Admin > SUSE Manager Configuration > General*

This page allows you to alter the most basic settings, such as the admin e-mail address.

4.11.2.2 *Admin > SUSE Manager Configuration > Monitoring*

This page is only available on monitor-enabled systems. See Section 4.10, "Monitoring — [Mon]" (page 157) for more details. Configure the monitoring aspects of the SUSE Manager. The local mail exchanger and the local main domain specified here are used to send e-mail notification messages to administrators. This is only required if you intend to receive alert notifications from probes monitoring your systems. If you do, provide the mail server (exchanger) and domain to be used. Note that sendmail must be configured to handle e-mail redirects of notifications. When finished, click *Update Config*.

4.11.2.3 *Admin > SUSE Manager Configuration > Certificate*

On the *SUSE Manager Configuration > Certificate* page upload a new SUSE Manager certificate. To identify the certificate's path, click *Browse*, navigate to the file, and select it. Open your certificate in a text editor, copy all lines, and paste them directly into the large text field at the bottom. SUSE recommends using the file browser as it is less error prone. Click *Update* to continue. If you receive errors related to DNS, ensure your SUSE Manager server is configured correctly.

4.11.2.4 *Admin > SUSE Manager Configuration > Bootstrap Script*

The *SUSE Manager Configuration > Bootstrap Script* page allows you to generate a bootstrap script for redirecting client systems from the central Novell Customer Center to SUSE Manager. This script, to be placed in the `/srv/www/htdocs/pub/bootstrap/` directory of SUSE Manager, significantly reduces the effort involved in reconfiguring all systems, which by default obtain packages from the central Novell Customer Center. The required fields are pre-populated with values derived from previous installation steps. Ensure this information is accurate.

Checkboxes offer options for including built-in security SSL and GNU Privacy Guard (GPG) features, both of which are advised. In addition, you may enable remote command acceptance and remote configuration management of the systems to be bootstrapped here. Both features are useful for completing client configuration. Finally, if you are using an HTTP proxy server, fill in the related fields. When finished, click *Generate Bootstrap Script*.

4.11.2.5 *Admin > SUSE Manager Configuration > Organizations*

The *SUSE Manager Configuration > Organizations* page contains details about the organizations feature of SUSE Manager, as well as links to quickly get started creating and configuring organizations. For more information about configuring organizations, refer to Chapter 6, *Multiple Organizations* (page 187).

4.11.2.6 *Admin > SUSE Manager Configuration > Restart*

The *SUSE Manager Configuration > Restart* page contains the final step in configuring SUSE Manager. Click the *Restart* button to restart SUSE Manager and incorporate all of the configuration options added on the previous screens. It will take between four and five minutes for the restart to finish.

4.12 Help

The *Help* pages provide access to the full suite of documentation and support available to SUSE Manager users. Click *Help* in the *Overview* category to see a list of options available to you.

4.12.1 SUSE Manager Quick Start

The *SUSE Manager Quick Start* explains how to install and set up SUSE Manager and how to get started with the most important tasks such as channel configuration or client registration.

4.12.2 SUSE Manager Proxy Quick Start

SUSE Manager Proxy Server is a package-caching mechanism that reduces the bandwidth requirements. Proxy customers cache RPMs, such as Patch Updates from SUSE or custom RPMs generated by their organization, on an internal, centrally-located server. Client systems then receive these updates from the Proxy rather than by accessing the SUSE Manager server individually. The *SUSE Manager Proxy Quick Start* explains how to install and set up a SUSE Manager Proxy Server.

4.12.3 SUSE Manager Reference Guide

The *Reference Guide* page takes you to the document you're reading right now. It provides the most comprehensive set of instructions for using SUSE Manager. Note that links to other technical guides may also appear in the left navigation bar, depending on the entitlement level and product offering of the account with which you logged in.

4.12.4 SUSE Manager Installation Guide

The Installation Guide provides detailed information regarding SUSE Manager server and its installation and initial configuration. Implementing a fully functional SUSE Manager requires more than installing software and a database. Client systems must be configured to use SUSE Manager. Custom packages and channels should be created for optimal use. Since these tasks extend beyond the basic installation, they are covered in detail in other guides, as well as the *SUSE Manager Installation Guide*.

4.12.5 SUSE Manager Client Configuration Guide

By default, all SUSE Linux Enterprise client systems are configured to communicate with Novell Customer Center. When connecting clients to SUSE Manager, many of these settings must be altered. Changing client settings for a system or two may be relatively simple. A large enterprise environment containing hundreds or thousands of systems will benefit from the mass reconfiguration steps described in the SUSE Manager Client Configuration Guide.

The *Client Configuration Guide* is a best practices manual intended to help customers of SUSE Manager configure their client systems.

4.12.6 Release Notes

The *Release Notes* page lists the notes accompanying every recent release of SUSE Manager. All significant changes occurring in a given release cycle, from major enhancements to the user interface to minor changes to the related documentation are documented here.

4.12.7 Search

The *Documentation Search* page features a robust search engine that indexes and searches SUSE Manager documentation.

Figure 4.20 *Documentation Search*

Users can search the available online documentation and filter them according to the following choices in the *What to Search* drop-down menu:

- *Content & Title* — Search both the title heading or body content of all available documents.

- *Free Form* — Search documents and indices for any keyword matches, which broadens search results.

- *Content* — Search only the body content of documentation for more specific matches.

- *Title* — Search only the title headings of the documentation for targeted, specific search results.

The *Free Form* field additionally allows you to search using field names that you prepend to search queries and filter results in that field.

For example, if you wanted to search all of the SUSE Manager manuals for the word `Virtualization` in the title and `install` in the content, type the following in the *Free Form* field:

```
title:Virtualization and content:install
```

Other supported field names for documentation search include:

- `url` — Search the URL for a particular keyword.

- `title` — Search titles for a particular keyword.

- `content` — Search the body of the documentation for a particular keyword.

If there are several pages of search results, you can limit the amount of visible results shown on one page by clicking the *Display quantity items per page* drop-down menu, which offers between 10 and 500 results per page.

To move between pages, click the right or left angle brackets (> to go forward or < to go backward).

5

Monitoring

The monitoring entitlement allows you to perform a actions designed to keep your systems running properly and efficiently. Keep close watch on system resources, network services, databases, standard and custom applications.

Monitoring provides both real-time and historical state-change information, as well as specific metric data. You are not only notified of failures immediately and warned of performance degradation before it becomes critical, you also receive the information necessary to conduct capacity planning and event correlation. For instance, the results of a probe recording CPU usage across systems would prove invaluable in balancing loads on those systems.

Monitoring entails establishing notification methods, installing probes on systems, regularly reviewing the status of all probes, and generating reports displaying historical data for a system or service. This chapter describes common tasks associated with the Monitoring entitlement. Virtually all changes affecting your Monitoring infrastructure must be finalized by updating your configuration, via the *Scout Config Push* page.

5.1 Prerequisites

Before starting to set up monitoring for your infrastructure, ensure you have all the necessary prerequisites in place:

- Monitoring entitlements — These entitlements are required for all systems to be monitored. Monitoring is supported on all target platforms.

- SUSE Manager with monitoring — Monitoring systems must be connected to SUSE Manager with a base operating system of SUSE Linux Enterprise 11. Refer to the SUSE Manager Installation Guide via *Help* for installation instructions.

- Monitoring administrator — This role must be granted to users installing probes, creating notification methods, or altering the monitoring infrastructure in any way. The SUSE Manager administrator automatically inherits the abilities of all other roles within an organization and can therefore carry out these tasks as well. Assign this role via the *User Details* page to other user.

- SUSE Manager monitoring daemon — This daemon, along with the SSH key for the scout, must be running on all systems to be monitored for the internal process monitors to be executed. You may be able to run these probes using the systems' existing SSH daemon (`sshd`). Refer to Section 5.2, "SUSE Manager Monitoring Daemon (rhnmd)" (page 172) for installation instructions and a quick list of probes requiring this secure connection. Refer to Appendix B, *Probes* (page 251) for the complete list of available probes.

5.2 SUSE Manager Monitoring Daemon (rhnmd)

To get the most out of your monitoring entitlement, we suggest installing the SUSE Manager monitoring daemon on your client systems. Based on OpenSSH, `rhnmd` enables SUSE Manager to communicate securely with the client system to access internal processes and retrieve probe status.

The SUSE Manager monitoring daemon requires monitored systems to allow connections on port `4545`. You may avoid opening this port and installing the daemon altogether by using `sshd` instead. Refer to Section 5.2.3, "Configuring SSH" (page 174) for details.

5.2.1 Probes requiring the daemon

An encrypted connection, either via the SUSE Manager monitoring daemon or `sshd`, is required on client systems for the following probes to run:

- Linux::CPU Usage

- Linux::Disk IO Throughput

- Linux::Disk Usage

- Linux::Inodes

- Linux::Interface Traffic

- Linux::Load

- Linux::Memory Usage

- Linux::Process Counts by State

- Linux::Process Count Total

- Linux::Process Health

- Linux::Process Running

- Linux::Swap Usage

- Linux::TCP Connections by State

- Linux::Users

- Linux::Virtual Memory

- LogAgent::Log Pattern Match

- LogAgent::Log Size

- Network Services::Remote Ping

- Oracle::Client Connectivity

- General::Remote Program

- General::Remote Program with Data

Note that all probes in the Linux group have this requirement.

5.2.2 Installing the SUSE Manager Monitoring Daemon

Install the SUSE Manager monitoring daemon to prepare systems for monitoring with the probes identified in Section 5.2.1, "Probes requiring the daemon" (page 172). Note that the steps in this section are optional if you intend to use `sshd` to allow secure connections between the monitoring infrastructure and the monitored systems. Refer to Section 5.2.3, "Configuring SSH" (page 174) for instructions.

The `rhnmd` package is available from the `client tools` channel for all SUSE Linux Enterprise distributions. To install it:

1. Subscribe the systems to be monitored to the `client tools` channel associated with the system. This can be done individually through the *System Details > Channels > Software* subtab or for multiple systems at once through the *Channel Details > Target Systems* tab.

2. Once subscribed, open the *Channel Details > Packages* tab and find the `rhnmd` package (under 'R').

3. Click the package name to open the *Package Details* page. Go to the *Target Systems* tab, select the desired systems, and click *Install Packages*.

4. Install the SSH public key on all client systems to be monitored, as described in Section 5.2.4, "Installing the SSH key" (page 175).

5. Start the SUSE Manager monitoring daemon on all client systems using the command:

```
rcrhnmd start
```

6. When adding probes requiring the daemon, accept the default values for *RHNMD User* and *RHNMD Port*: `nocpulse` and `4545`, respectively.

5.2.3 Configuring SSH

If you wish to avoid installing the SUSE Manager monitoring daemon and opening port 4545 on client systems, you may configure `sshd` to provide the encrypted connection required between the systems and SUSE Manager. This may be especially desirable

if you already have `sshd` running. To configure the daemon for monitoring follow these instructions:

1. Ensure the SSH package is installed on all systems to be monitored:

   ```
   rpm -qi openssh
   ```

2. Identify the user to be associated with the daemon. This can be any user available on the system as long as the required SSH key can be put in the user's `~/.ssh/authorized_keys` file.

3. Identify the port used by the daemon, as identified in its `/etc/ssh/sshd_config` configuration file. The default is port 22.

4. Install the SSH public key on all client systems to be monitored, as described in Section 5.2.4, "Installing the SSH key" (page 175).

5. Start the `sshd` on all client systems using the command:

   ```
   service sshd start
   ```

6. When adding probes requiring the daemon, insert the values derived from steps 2 and 3 in the *RHNMD User* and *RHNMD Port* fields.

5.2.4 Installing the SSH key

Whether you use `rhnmd` or `sshd`, you must install the SUSE Manager monitoring daemon public SSH key on the systems to be monitored to complete the secure connection:

1. Navigate to the *Monitoring > Scout Config Push* page on the SUSE Manager interface and click the name of the Scout that will monitor the client system. The SSH `id_dsa.pub` key is visible on the resulting page.

2. Copy the character string beginning with `ssh-dss` and ending with the hostname of the SUSE Manager server.

3. Select the systems you want to send the key to from the *Systems* page, then select *Systems* from the left menu, click the checkbox next to the systems you want to send the SSH key, then click the *Manage* button at the top.

4. On the *System Set Manager* page, click *Run remote commands*, then in the *Script* text box, type the following line:

```
#!/bin/sh
cat <<EOF >> ~nocpulse/.ssh/authorized_keys
```

Then, press Enter and paste the SSH Key. The result looks similar to the following:

```
#!/bin/sh
cat <<EOF >> ~nocpulse/.ssh/authorized_keys
ssh-dss AABBAB3NzaC3kc3MABCCBAJ4cmyf5jt/ihdtFbNE1YHsT0np0SYJz7xk
hzoKUUWnZmOUqJ7eXoTbGEcZjZLppOZgzAepw1vUHXfa/L9XiXvsV8K5Qmcu70h0
1gohBIder/1I1QbHMCgfDVFPtfV5eedau4AAACAc99dHbWhk/dMPiWXgHxdI0vT2
SnuozIox2klmfbTeO4Ajn/Ecfxqgs5diat/NIaeoItuGUYepXFoVv8DVL3wpp45E
02hjmp4j2MYNpc6Pc3nPOVntu6YBv+whB0VrsVzeqX89u23FFjTLGbfYrmMQflNi
j8yynGRePIMFhI= root@example.com
EOF
```

5. Set the date and time you want the action to take place, then click *Schedule Remote Command*.

Once the key is in place and accessible, all probes that require it should allow ssh connections between the Monitoring infrastructure and the monitored system. Now you can schedule probes requiring the monitoring daemon to run on the newly configured systems.

5.3 mysql package

If your SUSE Manager serves monitoring-entitled client systems on which you run MySQL probes, you must configure the mysql package on the SUSE Manager. Refer to Appendix B, *Probes* (page 251) for a listing of all available probes.

Subscribe the SUSE Manager to the SUSE Linux Enterprise base channel and install the mysql package either with zypper up or YaST.

Once finished, you can schedule MySQL probes with SUSE Manager.

5.4 Notifications

In addition to viewing probe status in the SUSE Manager interface, you can receive notifications whenever a probe changes state. This is especially important for mission-critical production systems.

To enable probe notifications in SUSE Manager, you must have identified a mail exchange server and mail domain during installation of your SUSE Manager and configured a mail transfer agent (such as postfix or sendmail) to properly handle incoming mail.

5.4.1 Creating Notification Methods

Notifications are sent via a notification method, an e-mail or pager address associated with a specific SUSE Manager user. Although the address is tied to a particular user account, it may serve multiple administrators through an alias or mailing list. Each user account can contain multiple notification methods. To create a notification method:

1. Log into the SUSE Manager website as either a SUSE Manager administrator or monitoring administrator.

2. Navigate to the *User Details > Notification Methods* tab and click *create new method*.

3. Enter an intuitive, descriptive label for the method name, such as `DBA day e-mail`, then provide the correct e-mail or pager address. Remember, the labels for all notification methods are available in a single list during probe creation, so they should be unique to your organization.

4. Select the checkbox if you desire abbreviated messages to be sent to the pager. This shorter format contains only the probe state, system hostname, probe name, time of message, and Send ID. The standard, longer format displays additional message headers, system and probe details, and instructions for response.

5. When finished, click *Create Method*. The new method shows up in the *User Details > Notification Methods* tab and the *Notification* page under the top *Monitoring* category. Click its name to edit or delete it.

6. While adding probes, select the *Probe Notifications* checkbox and select the new notification method from the resulting dropdown menu. Notification methods assigned to probes cannot be deleted until they are disassociated from the probe.

5.4.2 Receiving Notifications

If you create notification methods and associate them with probes, you must be prepared to receive them. These notifications come in the form of brief text messages sent to either e-mail or pager addresses. Here is an example of an email notification:

As you can see, the longer e-mail notifications contain virtually everything you would need to know about the associated probe. In addition to the probe command, run time, system monitored, and state, the message contains the Send ID, which is a unique character string representing the precise message and probe. In the above message, the Send ID is `01dc8hqw`.

Pager notifications, by necessity, contain only the most important details, namely the subject of the e-mail message (containing state, system, probe, and time) and the Send ID. Here is an example pager notification:

5.4.3 Redirecting Notifications

Upon receiving a notification, you may redirect it by including advanced notification rules within an acknowledgment e-mail. Just reply to the notification and include the desired option. These are the possible redirect options, or filter types:

- ACK METOO — Sends the notification to the redirect destination(s) *in addition to* the default destination.

- ACK SUSPEND — Suspends the notification method for a specified time period.

- ACK AUTOACK — Does not change the destination of the notification, but auto-matically acknowledges matching alerts as soon as they are sent.

- ACK REDIR — Sends the notification to the redirect destination(s) *instead of* the default destination.

The format of the rule should be `filter_type probe_type duration email_address` where `filter_type` indicates one of the previous advanced commands, `probe_type` indicates probe or system, `duration` indicates the length of time for the redirect, and `email_address` indicates the intended recipient. For example:

```
ACK METOO system 1h boss@domain.com
```

Capitalization is not required. Duration can be listed in minutes (m), hours (h), or days (d). Email addresses are needed only for redirects (REDIR) and supplemental (METOO) notifications.

The description of the action contained in the resulting e-mail defaults to the command entered by the user. The reason listed is a summary of the action, such as `email ack redirect by user@domain.com` where user equals the sender of the email.

NOTE

You can halt or redirect almost all probe notifications by replying to a notification e-mail with a variation of the command `ack suspend host`. However, you cannot halt SUSE Manager probe notifications by responding to a probe with `ack suspend host` or other redirect responses. These probes require you to change the notifications within the SUSE Manager web interface.

5.4.4 Filtering Notifications

Since notifications can be generated whenever a probe changes state, simple changes in your network can result in a flood of notifications. The creation, cancellation, and application of Notification filters is discussed in detail in Section 4.10.3.1, "*Notification > Filters*" (page 161).

5.4.5 Deleting Notification Methods

Theoretically, removing notification methods should be as easy as creating them. After all, you must populate no fields to conduct the deletion and a button exists for this explicit purpose. However, existing relationships between methods and probes can complicate this process. Follow these steps to remove a notification method:

1. Log into the SUSE Manager website as a SUSE Manager administrator or monitoring administrator.

2. Navigate to the *Monitoring > Notifications* page and click the name of the method to be removed.

3. On the *User Details > Notification Methods* tab, click *delete method*. If the method is not associated with any probes, you are presented with a confirmation page. Click *Confirm Deletion*. The notification method is removed.

> **NOTE**
>
> Since both the notification method name and address can be edited, consider updating the method rather than deleting it. This redirects notifications from all probes using the method without having to edit each probe and create a new notification method.

4. If the method is associated with one or more probes, you are presented with a list of the probes using the method and the systems to which the probes are attached instead of a confirmation page. Click the probe name to go directly to the *System Details > Probes* tab.

5. On the *System Details > Probes* tab, select another notification method and click *Update Probe*.

6. You may now return to the *Monitoring > Notifications* page and delete the notification method.

5.5 Probes

Now that the SUSE Manager monitoring daemon has been installed and notification methods have been created, you can install probes on your monitoring-entitled systems. If a system is entitled to monitoring, a *Probes* tab appears within its *System Details* page. This is where you will conduct most probe-related work.

5.5.1 Managing Probes

To add a probe to a system, the system must be entitled to monitoring. Further, you must have access to the system itself, either as the system's root user, through the system group administrator role, or as the SUSE Manager administrator. Then:

1 Log into the SUSE Manager website as either a SUSE Manager administrator or the system group administrator for the system.

2 Navigate to the *System Details > Probes* tab and click *create new probe*.

3 On the *System Probe Creation* page, complete all required fields. First, select the probe command group. This alters the list of available probes and other fields and requirements. Refer to Appendix B, *Probes* (page 251) for the complete list of probes by command group. Remember that some probes require the SUSE Manager monitoring daemon to be installed on the client system.

4 Select the desired probe command and the monitoring scout. Enter a brief but unique description for the probe.

5 Select the *Probe Notifications* checkbox to receive notifications when the probe changes state. Use the *Probe Check Interval* dropdown menu to determine how often notifications should be sent. Selecting `1 minute` (and the *Probe Notification* checkbox) means you will receive notifications every minute the probe surpasses its CRITICAL or WARNING thresholds. Refer to Section 5.4, "Notifications" (page 177) to find out how to create notification methods and acknowledge their messages.

6 Use the *RHNMD User* and *RHNMD Port* fields, if they appear, to force the probe to communicate via `sshd`, rather than the SUSE Manager monitoring daemon. Refer to Section 5.2.3, "Configuring SSH" (page 174) for details. Otherwise, accept the default values of `nocpulse` and `4545`, respectively.

7 If the *Timeout* field appears, review the default value and adjust to meet your needs. Most but not all timeouts result in an UNKNOWN state. If the probe's metrics are time-based, ensure the timeout is not less than the time allotted to thresholds. Otherwise, the metrics serve no purpose, as the probe will time out before any thresholds are crossed.

8 Use the remaining fields to establish the probe's alert thresholds, if applicable. These CRITICAL and WARNING values determine at what point the probe changes state. Refer to Section 5.5.2, "Establishing Thresholds" (page 182) for best practices regarding these thresholds.

9 When finished, click *Create Probe*. Remember, you must commit your monitoring configuration change on the *Scout Config Push* page for this to take effect.

To delete a probe, navigate to its *Current State* page (by clicking the name of the probe from the *System Details > Probes* tab), and click *delete probe*. Finally, confirm the deletion.

5.5.2 Establishing Thresholds

Many of the probes offered by SUSE Manager contain alert thresholds that, when crossed, change the state of the probe. For instance, the Linux::CPU Usage probe allows you to set CRITICAL and WARNING thresholds for the percent of CPU used. If the monitored system reports 75 percent of its CPU used, and the WARNING threshold is set to 70 percent, the probe will go into a WARNING state. Some probes offer a multitude of such thresholds.

In order to get the most out of your monitoring entitlement and avoid false notifications, it is recommended to run your probes without notifications for a time to establish baseline performance for each of your systems. Although the default values provided for probes may suit you, every organization has a different environment that may require altering thresholds.

5.5.3 Monitoring the SUSE Manager Server

In addition to your client systems, you may also monitor your SUSE Manager server. Select a system monitored by the server and go to that system's *System Details > Probes* tab.

Click *create new probe* and select the `SUSE Manager` probe command group. Next, complete the remaining fields as you would for any other probe. Refer to Section 5.5.1, "Managing Probes" (page 180) for instructions.

Although the SUSE Manager server appears to be monitored by the client system, the probe is actually run from the server on itself. Thresholds and notifications work normally.

> **NOTE**
>
> Any probes that require SUSE Manager monitoring daemon connections cannot be run on a SUSE Manager or a SUSE Manager proxy server on which monitoring software is running. This includes most probes in the Linux command group as well as the log agent probes and the remote program probes. Use the SUSE Manager command group probes to monitor SUSE Manager and SUSE Manager proxy servers. In the case of proxy scouts, the probes are listed under the system for which they are reporting data.

5.6 Troubleshooting

Though all monitoring-related activities are conducted through the SUSE Manager Web interface, SUSE provides access to some command line diagnostic tools that may help you determine the cause of errors. To use these tools, you must be able to become the `nocpulse` user on the SUSE Manager server conducting the monitoring.

First log into the SUSE Manager server as root. Then switch to the `nocpulse` user with the following command:

```
su - nocpulse
```

You may now use the diagnostic tools described in the rest of this section.

5.6.1 Examining Probes with rhn-catalog

To thoroughly troubleshoot a probe, you must first obtain its probe ID. You may obtain this information by running `rhn-catalog` on the SUSE Manager server as the `nocpulse` user. The output will resemble:

```
2 ServiceProbe on exa1.example.com (199.168.36.245): test 2
3 ServiceProbe on exa2.example.com (199.168.36.173): rhel2.1 test
4 ServiceProbe on exa3.example.com (199.168.36.174): SSH
5 ServiceProbe on exa4.example.com (199.168.36.175): HTTP
```

The probe ID is the first number, while the probe name (as entered in the SUSE Manager web interface) is the final entry on the line. In the above example, the probe ID `5` corresponds to the probe named `HTTP`.

Pass the `--commandline` (`-c`) and `--dump` (`-d`) options along with a probe ID to `rhn-catalog` to obtain additional details about the probe:

```
rhn-catalog --commandline --dump 5
```

The `--commandline` option yields the command parameters set for the probe, while `--dump` retrieves everything else, including alert thresholds and notification intervals and methods.

The command above will result in output similar to:

```
5 ServiceProbe on exa4.example.com (199.168.36.175):
linux:cpu usage
```

```
       Run as: Unix::CPU.pm --critical=90 --sshhost=199.168.36.175
--warn=70 --timeout=15 --sshuser=nocpulse
--shell=SSHRemoteCommandShell --sshport=4545
```

Use the ID with `rhn-runprobe` to examine the probe's output. Refer to Section 5.6.2, "Viewing the output of rhn-runprobe" (page 184) for instructions.

5.6.2 Viewing the output of rhn-runprobe

Now that you have obtained the probe ID with `rhn-catalog`, use it with `rhn-runprobe` to examine the complete output of the probe. Note that by default, `rhn-runprobe` works in test mode, meaning no results are entered in the database. The following options are available:

Table 5.1   *rhn-runprobe Options*

Option	Description
`--help`	List the available options and exit.
`--probe=PROBE_ID`	Run the probe with this ID.
`--prob_arg=PARAMETER`	Override any probe parameters from the database.
`--module=PERL_MODULE`	Package name of alternate code to run.
`--log=all=LEVEL`	Set log level for a package or package prefix.
`--debug=LEVEL`	Set numeric debugging level.
`--live`	Execute the probe, enqueue data and send out notifications (if needed).

Always include the `--probe` option, the `--log` option, and values for each. The `--probe` option takes the probeID as its value and the `--log` option takes the value "all" (for all run levels) and a numeric verbosity level as its values. Here is an example:

```
rhn-runprobe --probe=5 --log=all=4
```

The above command requests the probe output for probeID 5, for all run levels, with a high level of verbosity.

Provide the command parameters derived from `rhn-catalog`:

```
rhn-runprobe --probe=5 --log=all=4 --sshuser=nocpulse --sshport=4545
```

This yields verbose output depicting the probe's attempted execution. Errors are clearly identified.

Multiple Organizations

6

With SUSE Manager you can create and manage multiple organizations. Divide systems, content, and subscriptions in different organizations or specific groups, for example to reflect departments, teams or projects. This chapter guides you through basic setup tasks and explains the concepts of multiple organization, as well as their creation and management with SUSE Manager.

During installation and setup, SUSE Manager automatically creates a default administrative organization. It gets the organization ID `1` and the organization name that you entered in Step 5a (↑Quick Start) in Procedure "Setting Up SUSE Manager" (↑Quick Start).

6.1 Recommended Models for Using Multiple Organizations

The following examples detail two possible scenarios using the multiple organizations (or multi-org) feature. There's no need to figure out and plan all necessary organizations on your SUSE Manager up front. Start using organizations at whatever pace makes the most sense for you. It may be a good idea to create an additional organization for a limited set of systems and users to experiment with and fully understand the impact of a multi-org SUSE Manager on your processes and policies, before you design the best setup for your purposes.

6.1.1 Centrally-Managed SUSE Manager for a Departmental Organization

In this first scenario, SUSE Manager is maintained by a central group of administrators within a business or other organization (refer to Figure 6.1, "Centralized SUSE Manager Management for a Departmental Organization" (page 189)). The SUSE Manager administrator treats `organization 1` as a staging area for software and system subscriptions and entitlements.

The SUSE Manager administrator's responsibilities include the configuration of SUSE Manager (any tasks available under the *Admin* area of the Web interface), the creation and deletion of additional SUSE Manager organizations, and the allocation and removal of software and system subscriptions and entitlements.

Additional organizations in this example are mapped to departments within a company. One way to divide the various departments in an organization is to consider which departments purchase subscriptions and entitlements for use with SUSE Manager. To maintain centralized control over all organizations in SUSE Manager, create an organization administrator account in each new organization and assign the role to yourself for full access.

Figure 6.1 *Centralized SUSE Manager Management for a Departmental Organization*
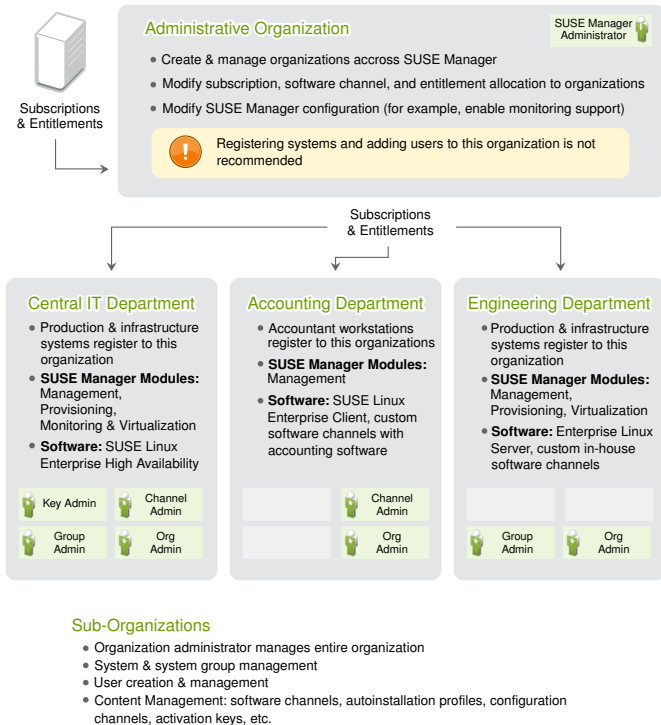
6.1.2 Decentralized Management of Multiple Third Party Organizations

In this example, SUSE Manager is maintained by a central group, but each organization is treated separately without relations or ties between the different organizations on SUSE Manager. Let's assume each organization is a customer of your company. You manage the SUSE Manager application itself while other administrators take care of their respective organizations.

While a SUSE Manager consisting of sub-organizations that are all part of the same company may be more tolerant of sharing systems and content between organizations,

in this decentralized example sharing is not tolerable. Administrators can allocate entitlements in specific amounts to each organization. Each organization will have access to all SUSE content synced to SUSE Manager if the organization has software channel entitlements for the content.

However, if one customer pushes custom content to their organization, it will not be available to other organizations. You as the SUSE Manager administrator would have to push the content to all or selected organizations if you have the necessary access rights.

In this scenario, it might make sense for SUSE Manager administrators to reserve an account in each organization (by adding the organization administrator role for the respective organization). For example, if you are using SUSE Manager to provide managed hosting services to external parties, you might need to access systems in that organization and push content.

Figure 6.2 *Decentralized SUSE Manager Management for Multi-Department Organization*
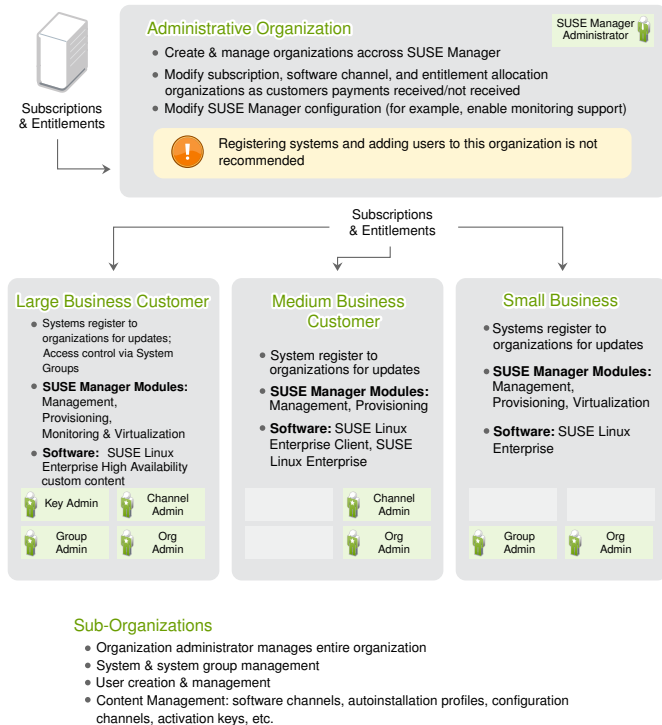
6.1.3 General Tips for Multi-Org Usage

Regardless of which scenario you choose in the management of your multi-org SUSE Manager, the following best practices tips can help.

NOTE: Use of Default Administrative Organization

For managing multiple organization, create new, dedicated organizations within SUSE Manager. The default administrative organization receives special treatment with regards to subscriptions and entitlements. Therefore do *not* use the default administrative organization for registering client systems and

creating users in a multi-organization setup. However, in the following cases it is unproblematic to do so:

- If you use SUSE Manager in a single-organization setup.

- During the migration from a single-organization setup to a multi-organization setup.

The administrative organization is intended to be a staging area for subscriptions and entitlements. When you associate SUSE Manager with a new certificate, any new entitlements will be granted to this organization by default. In order to make those new entitlements available to other organizations on SUSE Manager, you will need to explicitly allocate those entitlements to the other organizations from the administrative organization. Vice versa, if you remove entitlements from other organizations, they will automatically be re-assigned to the default organization.

6.1.3.1 Certificate Has Less Entitlements Than I Am Using

If you have issued a new SUSE Manager certificate and it contains less entitlements than the systems in the organizations of your SUSE Manager are consuming, you cannot activate this new certificate. You will get an error stating that there are insufficient entitlements in the certificate.

There are a few ways you can reduce SUSE Manager entitlement usage in order to activate your new certificate. Evaluate each organization's entitlement usage and decide which organizations can relinquish some entitlements and still function properly. Contact each organization administrator directly and request that they unentitle or delete the system profiles of any extraneous systems in their organizations. If you also have the organization administrator role for these organizations, you can do this yourself. Logged in as a SUSE Manager administrator, you cannot decrement the allocated entitlements to an organization below the number of entitlements associated with system profiles.

There are some situations in which you need to free entitlements and do not have a lot of time to do so, and may not have access to each organization in order to do this yourself. In this case, proceed as described below:

1 Open the `/etc/rhn/rhn.conf` file and adjust set the `web.force_unentitlement` variable as follows:

```
web.force_unentitlement=1
```

Setting this parameter to `1` allows to decrement an organization's allocated entitlements below what they are using. If an organization has more entitlements than are being actively used, you do not need to change this variable to remove entitlements.

2 Restart SUSE Manager:

```
spacewalk-service restart
```

3 Log in to the SUSE Manager default organization in the SUSE Manager Web interface:

4 Reduce the allocated entitlements either via each organization's *Subscriptions* tab or via individual entitlement's *Organizations* tabs.

5 A number of systems in the organization should now be in an *unentitled* state. These are the systems most recently registered with the organization. The number of unentitled systems is equal to the difference between the total number of entitlements you removed from the organization and the number of entitlements the organization did not have applied to the systems.

For example, if you removed 10 entitlements from the organization in Step 4 (page 193), and the organization has four entitlements that were not in use by systems, then 6 systems in the organization will be unentitled.

After you have a sufficient number of entitlements, you should be able to activate your new SUSE Manager certificate.

6.1.3.2 Certificate Has More Entitlements Than I Am Using

If you are issued a new SUSE Manager certificate and it has more entitlements than are being consumed on your SUSE Manager, any extra entitlements will be assigned to the administrative organization. If you log into the Web interface as the SUSE Manager administrator, you will then be able to allocate these entitlements to other organizations. The previously-allocated entitlements to other organizations will be unaffected.

6.2 *Admin > Organizations*

The *Organizations* page in the Web interface allows administrators to view, create, and manage multiple organizations across SUSE Manager. Administrators can allocate software and system entitlements across various organizations, as well as control an organization's access to systems management tasks.

Figure 6.3 *Admin*
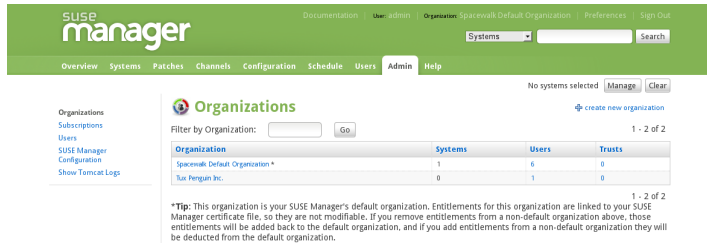
The *Organizations* page lists organizations across the SUSE Manager, with both user and system counts assigned to each organization. The *Organizations* page also features a *Trusts* page for any organizational trusts established. Refer to Section 6.6, "Organizational Trusts" (page 201) for more information about establishing organizational trusts.

6.2.1 *Admin > Organizations > Details*

Clicking on an organization displays the *Details* page, where administrators are provided with a summary of various aspects of the organization.

• *Active Users* — The number of users in the organization.

• *Systems* — The number of systems subscribed to the organization.

• *System Groups* — The number of groups subscribed to the organization.

• *Activation Keys* — The number of activation keys available to the organization.

• *Autoinstallation Profiles* — The number of autoinstallation profiles available to the organization.

- *Configuration Channels* — The number of Configuration Channels available to the organization.

On this page, you can delete an organization by clicking the *Delete Organization* link.

The *Details* page also contains three subtabs: *Users*, *Subscriptions*, and *Trusts*.

6.3 Managing Organizations

Administrators can create new organizations and assign entitlements, groups, systems, and users to it. This enables organizations to perform administrative tasks on their own without affecting other organizations. During creation of a new organization, you also need to create an (initial) organization administrator account. SUSE Manager administrators should reserve the initial organization administrator for themselves to be able to log into this organization when necessary.

NOTE: PAM Accounts

If your SUSE Manager is configured for PAM authentication, avoid using PAM accounts for the organization administrator account in new organizations. Instead, create a SUSE Manager-local account for organization administrators. Reserve PAM-authenticated accounts for SUSE Manager logins with less elevated privileges.

For more information about PAM, see Section "Implementing PAM Authentication" (Chapter 6, *Maintenance*, ↑Installation Guide).

Procedure 6.1 *Creating and Deleting Organizations*

1 Log in to the Web interface as SUSE Manager administrator or organization administrator.

2 To create an organization:

    2a Switch to the *Admin* tab to see a list of all *Organizations* within SUSE Manager.

    2b Click the *Create New Organization* link at the top right corner.

2c Enter an *Organization Name*.

2d To create the initial organization administrator for the new organization, enter the *Desired Login* and the *Desired Password* for the new user and confirm the password.

TIP: Login Names

For the organization administrator account use a login name that can easily be matched with the organization, for example: `orgadmin-mktg` or `eng-dept-admin`.

Figure 6.4   *Create New Organization*

2e Enter the first and last name and the e-mail address of the new user.

2f To finish, click *Create Organization*. Once the new organization is created, the *Organizations* page will list the new organization.

3 To delete an organization:

3a On the *Admin* tab, select *Organizations* from the left navigation bar.

3b Click the desired organization to see the organization details.

3c Click the *Delete Organization* link at the upper right corner and confirm by clicking the *Delete Organization* button.

6.4 Managing Entitlements

One important task after creating a new organization is to assign entitlements to the new organization. There are two types of entitlements that are important:

System Entitlements
> Various categories of system entitlements are available: management, provisioning, monitoring, and virtualization entitlements. Having management entitlements is a base requirement for an organization to function in SUSE Manager. The maximum number of systems that may register with an organization in SUSE Manager depends on the number of management entitlements allocated to that organization—regardless of the number of software entitlements available. For example, if there are 100 SUSE Linux Enterprise client entitlements but only 50 management system entitlements to an organization, only 50 systems are able to register with that organization.

Software Channel Entitlements
> Apart from system entitlements, software channel entitlements are needed for each organization. For example, you must grant `client tools` channel entitlements to each organization (as this channels contains client software required for extended SUSE Manager functionality, such as AutoYaST or Kickstart or virtualization support).

From the *Admin* tab in the Web interface you can manage and assign both types of entitlements by selecting either *Subscription > Software Channel Entitlements* or *Subscription > System Entitlements* from the left navigation bar. For a detailed description of those pages in the Web interface, refer to Section 6.4.1, "*Admin > Subscriptions > Software Channel Entitlements*" (page 199) and Section 6.4.2, "*Admin > Subscriptions > System Entitlements*" (page 200).

The default organization automatically gets the needed system and software entitlements during the synchronization with `mgr-ncc-sync`. To transfer the respective entitlements from the default organization to any newly created organization, proceed as described in Procedure 6.2, "Assigning Entitlements to an Organization" (page 198).

Procedure 6.2 *Assigning Entitlements to an Organization*

1 Log in to the SUSE Manager Web interface as SUSE Manager administrator.

2 Switch to the *Admin* tab and from the left navigation bar, select *Organizations*.

3 Select the organization for which to assign or change entitlements and select the *Subscriptions* subtab.

4 To set any system entitlements for the selected organization:

> **4a** Click the *System Entitlements* subtab to view the *System Entitlements Counts*.
>
> **4b** Set the total number of *Management (Base)* entitlements for the current organization by entering a value in the *Proposed Total* field.
>
> **4c** Similarly, set total numbers for any other entitlements you may need (like monitoring, provisioning, virtualization).
>
> **4d** Click *Update Organization* to confirm your changes.

5 To set software channel entitlements for the selected organization:

> **5a** Click the *Software Channel Entitlements* subtab to view the *Software Channel Entitlements Counts*.
>
> **5b** For any channel that should be available to the client systems of the current organization, enter the desired number of entitlements for this channel in the *Regular Proposed Total* field.
>
> **5c** Click *Update Organization* to confirm your changes.

Any number of system or software entitlements assigned to an organization are deducted from the total number of system or software entitlements.

To view the total number of software entitlements across all organizations in SUSE Manager, switch to the *Admin* tab and select *Subscriptions > Software Channel Entitlements*.

6.4.1 *Admin > Subscriptions > Software Channel Entitlements*

The *Software Channel Entitlements Across SUSE Manager* page lists all entitlements on SUSE Manager across all organizations, as well their usage. Click on an *Entitlement Name* for a more detailed view.

The *Details* subtab for the software channel entitlement contains information about the software channel access granted by the entitlement.

The *Organizations* subtab allows SUSE Manager administrators to adjust the number of software channels available to each organization. Type in the number (within the range listed in *Possible Values*) and click the *Update* button for that organization.

NOTE: Custom Channels and Organizational Trusts

When organization administrators create a custom channel, they can use that channel only within their organization unless an organizational trust is established between the organizations that want to share the channel. For more information about organizational trusts, refer to Section 6.6, "Organizational Trusts" (page 201).

The *Organizations* subtab also contains broad usage information in the *System-Wide Entitlement Usage* section, including:

- *Total* — The total number of channel entitlements for SUSE Manager.

- *Available* — The number of entitlements currently available for allocation.

- *Usage* — The number of entitlements currently in use by all organizations (aside from the default organization), compared to the total number of entitlements allocated.

For example, if the *Total* column is 100 and the *Available* column is 70, that means 30 entitlements are allocated to organizations. The *Usage* column shows how many of those 30 allocated entitlements are in use by organizations besides the default organization. So if the *Usage* column reads `24 of 30 (80%)`, that means 24 channel entitlements out of the 30 allocated are distributed to SUSE Manager organizations.

6.4.2 *Admin > Subscriptions > System Entitlements*

The *System Entitlements Across SUSE Manager* page lists all system entitlements on this SUSE Manager, across all organizations, as well as their usage. Click on the entitlement's name for more details.

System entitlements include *Management*, *Provisioning*, *Monitoring*, and *Virtualization*. Enter the number of allocations of each system entitlement in the text box, not to exceed the limit indicated in the *Possible Values*.

The *Details* subtab for the system entitlement contains information about the entitlement and what access it grants.

The *Organizations* subtab allows SUSE Manager administrators to adjust the number of system entitlement allocations available to each organization. Type in the number (within the range listed in *Possible Values*) and click the *Confirm Changes* button for that organization.

The *Organizations* subtab for the system entitlement also contains usage information in the SUSE Manager-wide entitlement usage section, including:

- *Total Allocated* — The number of total entitlements available for the entire SUSE Manager.

- *Entitlement Usage* — The number of entitlements currently being used.

- *Organization Usage* shows the number of organizations that have access to the entitlement.

6.5 Configuring Systems in an Organization

After a new organization has been created and requisite entitlements assigned to it, you can assign systems to each organization.

There are two basic ways to register a system with a particular organization:

1. Registering Using Login and Password — If you provide a login and password created for a specific organization, the system will be registered with that organization. For example, if `user-123` is a member of the *Central IT* organization on SUSE Manager, the following command would register that system with the *Central IT* organization on your SUSE Manager:

   ```
   mgrreg_ks --username=user-123 --password=foobaz
   ```

2. Registering Using An Activation Key — You can also register a system with an organization using an activation key from the organization. Activation keys will register systems with the organization in which the activation key was created. Activation keys are a good registration method to use if you want to allow users to register systems with an organization without providing them login access to that organization. If you want to move systems between organizations, you may also automate the move with scripts using the activation keys. The prefix of the activation key indicates which organization (by ID number) owns the activation.

6.6 Organizational Trusts

Organizations can share their resources with each other by establishing an organizational trust in SUSE Manager. An organizational trust is bi-directional, meaning that once a SUSE Manager administrator establishes a trust between two or more organizations, the organization administrator from each organization is free to share as much or as little of their resources as they need to. It is up to each organization administrator to determine what resources to share, and what shared resources from other organizations in the trust to use.

NOTE

Only organization administrators have the rights to share their custom content. The SUSE Manager administrator role is limited to allocating system and software entitlements to each organization.

6.6.1 Establishing an Organizational Trust

A SUSE Manager administrator can create a trust between two or more organizations. To do this, click the *Organizations* link in the side menu on the *Admin* main page.

Click the name of one of the organizations and within the *Details* page, click the *Trusts* subtab.

On the *Trusts* subtab, there is a listing of all the other trusts on SUSE Manager. Here you may use the *Filter by Organization* text box to narrow down a long list of organizations to a specific subset.

Figure 6.5 *Organizational Trusts*
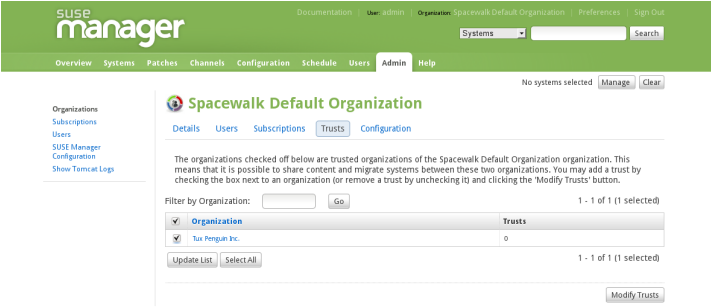
Click the checkbox next to the names of the organizations you want to be in the organizational trust with the current organization and click the *Modify Trusts* button.

6.6.2 Sharing Content Channels between Organizations in a Trust

Once an organizational trust has been established, organizations can now share content such as custom software channels with the other organizations in the trust. There are also three levels of channel sharing that can be applied to each channel for finer-grained channel access control.

NOTE

Organizations cannot share SUSE channels because they are available to all organizations that have entitlements to those channels.

To share a custom channel with another organization, perform the following steps:

1 Login to SUSE Manager with the username of the organization administrator.

2 Click on the *Channels* tab.

3 On the side menu, click *Manage Software Channels*.

4 Click the custom channel that you want to share with the other organizations.

5 From the *Channel Access Control* section of the *Details* page, there are three choices in *Organizational Sharing*.

- *Private* — Make the channel private so that it cannot be accessed by any organizations except the channel's owner.

- *Protected* — Allow the channel to be accessed by specific trusted organizations of your choice.

  NOTE

  If you choose *Protected* sharing, a separate page prompts you to confirm that you are granting channel access to the selected organizations by clicking *Grant Access and Confirm*.

- *Public* — Allow all organizations within the trust to access the custom channel.

  Click the radio button next to your selection and click *Update Channel*.

Now, any other organization administrators within the trust for which you have granted access to your custom channel can allow their client systems to install and update packages from the shared channel.

NOTE

If you have a system subscribed to a shared channel, and the organization administrator of the shared channel changes access rights removing your organization, your system loses that channel. If it was used as base channel, your system will no longer have a base channel on the *Systems* page and will not receive updates.

6.6.3 Migrating Systems from One Trusted Organization to Another

In addition to sharing software channels, organizations in a trust can migrate systems to other trusted organizations by using a utility called `migrate-system-profile`.

`migrate-system-profile` usage is based on the command-line, and uses systemIDs and orgIDs as arguments to specify what is being moved and its destination organization.

To use the `migrate-system-profile` command, you must have the `spacewalk-utils` package installed. You do not need to be logged into the SUSE Manager server to use `migrate-system-profile`; however, if you do not log in, you will need to specify the hostname or IP address of the server as a command-line argument.

> **NOTE**
>
> When an organization migrates a system with the `migrate-system-profile` command, the system does not carry any of the previous entitlements or channel subscriptions from the source organization. However, the system's history is preserved, and can be accessed by the new organization administrator in order to simplify the rest of the migration process, which includes subscribing to a base channel and granting entitlements.

6.6.3.1 Using migrate-system-profile

To use `migrate-system-profile` you need to ascertain the ID of the system to be migrated, the ID of the organization the system will migrate to, and the hostname or IP address of the SUSE Manager server if you are running the command from another machine.

The usage from the command line is the following:

```
migrate-system-profile --satellite {SUSE Manager HOSTNAME OR IP} -
--systemId={SYSTEM ID} --to-org-id={DESTINATION ORGANIZATION ID}
```

In the following example, the Finance department (created as an organization in SUSE Manager with OrgID 2) wants to migrate a workstation (with SystemID 10001020) from the Engineering department, but the Finance organization administrator does not

have shell access to the SUSE Manager server. The SUSE Manager hostname is *sat-server.example.com.*

The finance organization administrator would type the following command into a shell:

```
migrate-system-profile --satellite satserver.example.com --systemId=10001020 -
--to-org-id=2
```

The finance organization administrator is then prompted for the username and password (unless they are specified by using `--username=` and `--password=` at the command-line).

The system now shows up in the *Systems* page of the finance organization in the SUSE Manager Web interface. The finance organization administrator can finish the migration process by assigning a base channel and granting entitlements to the client. Check the system's *History* page in the *Events* subtab to see previous subscriptions and entitlements.

Figure 6.6 *System History*
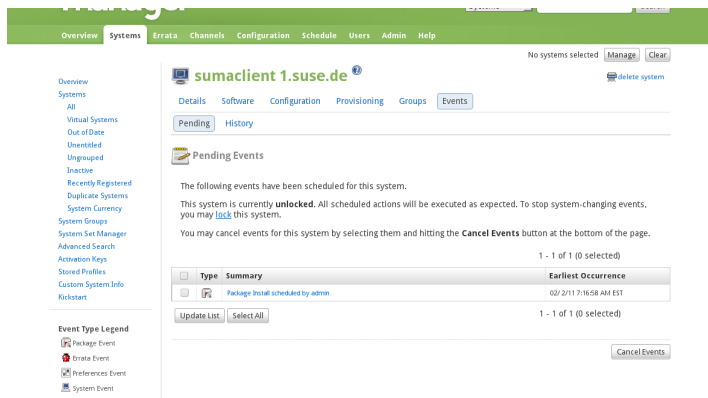
NOTE

The SUSE Manager administrator can migrate a system from one trusted organization to any other in the trust. However, organization administrators can only migrate a system from their own organization to another in the trust.

To migrate several systems at once, SUSE Manager administrators can use the `--csv` option of `migrate-system-profile` to automate the process using a simple comma-separated list of systems to migrate.

A line in the CSV file should contain the ID of the system to be migrated as well as the destination organization's ID in the following format:

```
systemId,to-org-id
```

The `systemId`, for example could be `1000010000`, while the `to-org-id` could be `4`. A compatible CSV might look like this:

```
1000010000,3
1000010020,1
1000010010,4
```

For more information about using `migrate-system-profile` refer to the manual page by typing `man migrate-system-profile` or for a basic help screen type `migrate-system-profile -h`.

6.7 *Admin > Users*

The *Users Across SUSE Manager* page contains a list of all users on the SUSE Manager, throughout all organizations.

> **NOTE**
>
> You are only able to modify the details of organization users if you are logged in as the responsible organization administrator.

Clicking the *Username* displays the *User Details* page. Refer to Section 4.9, "Users — [Mgmt]" (page 150) for more information on user configuration.

6.7.1 *Admin > Organizations > Details > Users*

The *Users* subtab lists the users assigned to the organization, including their real names, email address, and a check mark indicating whether the user is an administrator of the organization.

If you are the organization administrator, you can click the username to display the *User Details* page for the user. For instructions regarding user management, refer to Section 4.9.1.1, "*User List > Active > User Details* — [Mgmt]" (page 152).

NOTE

You must be logged in as the organization administrator to edit the User details for an organization. The SUSE Manager administrator cannot edit user details for organization users.

Virtualization

7

SUSE Manager allows to autoinstall and manage Xen and KVM VM Guests on a registered VM Host Server or integrate with SUSE Studio. In order to autoinstall a VM Guest, an autoinstallable distribution and an autoinstallation profile (AutoYaST or Kickstart for example) need to exist on SUSE Manager. VM Guests registered with SUSE Manager can be managed like "regular" machines. In addition, basic VM Guest management tasks such as (re)starting and stopping or changing processor and memory allocation can be carried out using SUSE Manager.

Autoinstalling and managing VM Guests via SUSE Manager is limited to Xen and KVM guests. SUSE Manager uses `libvirt` for virtual machine management. Currently, virtual machines from other virtualization solutions such as VMware* or VirtualBox*, are recognized as VM Guests, but cannot be managed from within SUSE Manager.

7.1 Autoinstalling VM Guests

With SUSE Manager you can automatically deploy Xen and KVM VM Guests using AutoYaST or Kickstart profiles. It is also possible to automatically register the VM Guests, so they can immediately be managed by SUSE Manager.

7.1.1 Requirements on SUSE Manager

Setting up and managing VM Guests with SUSE Manager does not require special configuration options. However, you need to provide activation keys for the VM Host Server and the VM Guests, an autoinstallable distribution and an autoinstallation profile.

In order to automatically register VM Guests with SUSE Manager, a bootstrap script is needed.

7.1.1.1 Activation Keys

Just like any other client, VM Host Server and VM Guests need to be registered with SUSE Manager using activation keys. Find details on how to setup activation keys at Procedure "Creating Activation Keys" (↑Quick Start). While there are no special requirements for a VM Guest key, the following minimum requirements must be met for the VM Host Server activation key.

VM Host Server Activation Key: Minimum Requirements

- Entitlements: Provisioning, Virtualization Platform

- Packages:`rhn-virtualization-host`,`osad`

  If you would like to be able to manage the VM Host Server system itself from SUSE Manager (e.g. by executing remote scripts), the package `rhncfg-actions` needs to be installed as well.

7.1.1.2 Setting up an Autoinstallable Distribution

In order to autoinstall clients from SUSE Manager you need to provide an "autoinstallable distribution", also referred to as autoinstallable tree, or installation source. This installation source needs to be made available through the filesystem of the SUSE Manager host. It can for example be a mounted local or remote directory or a "loop-mounted" iso image. It must match the following requirements:

- Kernel and initrd location:

  ### RedHat / Generic RPM

  - images/pxeboot/vmlinuz

    images/pxeboot/initrd.img

  ### SUSE

  - boot/*arch*/loader/initrd

boot/*arch*/loader/linux

- The *Base Channel* needs to match the autoinstallable distribution.

IMPORTANT: Autoinstallation package sources

There is a fundamental difference between RedHat and SUSE systems regarding the package sources for autoinstallation. The packages for a RedHat installation are being fetched from the *Base Channel*. Packages for installing SUSE systems are being fetched from the autoinstallable distribution.

As a consequence, the autoinstallable distribution for a SUSE system has to be a complete installation source (same as for a regular installation).

---

1 Make sure an installation source is available from a local directory. The data source can be any kind of network resource, a local directory or an iso image (which has to be loop-mounted). Files and directories must be world readable.

2 Login to the SUSE Manager web interface and open *System > Autoinstallation > Distributions > Create New Distribution*.

3 Fill out the form *Create Autoinstallable Distribution* as follows:

Distribution Label
Choose a unique name for the distribution. Only letters, numbers, hyphens, periods, and underscores are allowed; the minimum length is 4 characters. This field is mandatory.

Tree Path
Absolute local disk path to installation source. This field is mandatory.

Base Channel
Channel matching the installation source. This channel is the package source for non-SUSE installations. This field is mandatory.

Installer Generation
Operating system version matching the installation source. This field is mandatory.

Kernel Options
> Options passed to the kernel when booting for the installation. There is no need to specify the `install=` parameter, since it will automatically be added. This field is optional.

Post Kernel Options
> Options passed to the kernel when booting the installed system for the first time. This field is optional.

4 Save your settings by clicking *Update Autoinstallable Distribution*.

In order to edit an existing *Autoinstallable Distribution*, go to *System > Autoinstallation > Distributions* and click on a *Label*. Make the desired changes and save your settings by clicking *Update Autoinstallable Distribution*.

7.1.1.3 Providing an Autoinstallation Profile

Autoinstallation profiles (AutoYaST or Kickstart files) contain all the installation and configuration data needed to install a system without user intervention. The may also contain scripts that will be executed after the installation has completed.

All profiles can be uploaded to SUSE Manager and be edited afterwards. Kickstart profiles can also be created from scratch with SUSE Manager.

A minimalist AutoYaST profile including a script for registering the client with SUSE Manager is listed in Appendix C, *Minimalist AutoYaST Profile for Automated Installations* (page 323). For more information, examples and HOWTOs on AutoYaST profiles, refer to http://www.suse.de/~ug/. For more information on Kickstart profiles, refer to your RedHat documentation.

Uploading an Autoinstallation Profile

1 Login to the SUSE Manager web interface and open *System > Autoinstallation > Profiles > Upload New Kickstart/AutoYaST File*.

2 Choose a unique name for the profile. Only letters, numbers, hyphens, periods, and underscores are allowed; the minimum length is 6 characters. This field is mandatory.

3 Choose an *Autoinstallable Tree* from the drop-down menu. If no *Autoinstallable Tree* is available, you need to add an Autoinstallable Distribution. Refer to Section 7.1.1.2, "Setting up an Autoinstallable Distribution" (page 210) for instructions.

4 Choose a *Virtualization Type* from the drop-down menu. KVM and Xen (para-virtualized and fully-virtualized) are available. Do not choose *Xen Virtualized Host* here.

5 Scroll down to the end of the web page to the *File to Upload* dialog. Either manually enter the path to to the profile file or use the *Browse* button to select it. Click *Upload File*.

6 The uploaded file will be displayed in the *File Contents* section, where you can edit it.

7 Click *Create* to store the profile.

In order to edit an existing profile, go to *System > Autoinstallation > Profiles* and click on a *Label*. Make the desired changes and save your settings by clicking *Create*.

NOTE: Editing existing Kickstart profiles

If you are changing the *Virtualization Type* of an existing Kickstart profile, it may also modify the bootloader and partition options, potentially overwriting any user customizations. Be sure to review the *Partitioning* tab to verify these settings when changing the *Virtualization Type*.

Creating a Kickstart Profile

NOTE

Currently it is only possible to create autoinstallation profiles for RHEL systems. If installing a SUSE Linux Enterprise Server system, you need to upload an existing AutoYaST profile as described in Section "Uploading an Autoinstallation Profile" (page 212).

---

1 Login to the SUSE Manager web interface and open *System > Autoinstallation > Profiles > Create New Kickstart File*.

2 Choose a unique name for the profile. The minimum length is 6 characters. This field is mandatory.

3 Choose a *Base Channel*. This channel is the package source for non-SUSE installations and must match the *Autoinstallable Tree*. This field is mandatory.

4 Choose an *Autoinstallable Tree* from the drop-down menu. If no *Autoinstallable Tree* is available, you need to add an Autoinstallable Distribution. Refer to Section 7.1.1.2, "Setting up an Autoinstallable Distribution" (page 210) for instructions.

5 Choose a *Virtualization Type* from the drop-down menu. KVM and Xen (para-virtualized and fully-virtualized) are available. Do not choose *Xen Virtualized Host* here.

6 Click the *Next* button to continue to Step 2.

7 Select the location of the distribution files for the installation of your VM Guests. There should already be a *Default Download Location* filled out and selected for you on this screen. Click the *Next* button to continue to Step 3.

8 Choose a `root` password for the VM Guests. Click the *Finish* button to generate the profile.

   This completes Kickstart profile creation. After completing Step 3, you are taken to the newly-created Kickstart profile. You may browse through the various tabs of the profile and modify the settings as you see fit, but this is not necessary as the default settings should work well for the majority of cases.

Adding a Registration Script to the Autoinstallation Profile

A VM Guest that is autoinstalled does not get automatically registered. Adding a section to the autoinstallation profile that invokes a bootstrap script for registration will fix this. The following procedure describes adding a corresponding section to an AutoYaST profile. Refer to your RedHat Enterprise Linux documentation for instructions on adding scripts to a Kickstart file.

1 First, provide a bootstrap script on the SUSE Manager:

   1a Create a bootstrap script for VM Guests on the SUSE Manager as described in Procedure "Generating the Bootstrap Script" (↑Quick Start).

   1b Login as `root` to the konsole of SUSE Manager and go to `/srv/www/htdocs/pub/bootstrap`. Copy `bootstrap.sh` (the bootstrap script

created in the previous step) to e.g. `bootstrap_vm_guests.sh` in the same directory.

1c Edit the newly created file according to your needs. The minimal requirement is to include the activation key for the VM Guests (see Section 7.1.1.1, "Activation Keys" (page 210) for details). We strongly recommend to also include one or more GPG keys (for example, your organization key, and package signing keys).

2 Login to the SUSE Manager Web interface and go to *Systems > Autoinstallation > Profiles*. Click on the profile that is to be used for autoinstalling the VM Guests to open it for editing.

Scroll down to the *File Contents* section where you can edit the AutoYaST XML file. Add the following snippet at the end of the XML file right before the closing `</profile>` tag and replace the given IP address with the address of the SUSE Manager server. See Appendix C, *Minimalist AutoYaST Profile for Automated Installations* (page 323) for an example script.

```
<scripts>
  <init-scripts config:type="list">
    <script>
      <interpreter>shell </interpreter>
      <location>
        http://192.168.1.1/pub/bootstrap/bootstrap_vm_guests.sh
      </location>
    </script>
  </init-scripts>
</scripts>
```

IMPORTANT: Only one `<scripts>` section allowed

If your AutoYaST profile already contains a `<scripts>` section, do not add a second one, but rather place the `<script>` part from above within the existing `<scripts>` section!

---

3 Click *Update* to save the changes.

7.1.2 VM Host Server Setup

A VM Host Server system serving as an target for autoinstalling VM Guests from SUSE Manager must be capable of runing guest operating systems. This requires either KVM or Xen being properly set up. For installation instructions for SUSE Linux Enterprise Server systems refer to the guides *SLES 11 Virtualization with KVM Administration Guide* or *SLES 11 Virtualization with Xen Administration Guide* available from http://www.novell.com/documentation/sles11/. For instructions on setting up a RedHat VM Host Server refer to your RedHat Enterprise Linux documentation.

Since SUSE Manager uses `libvirt` for VM Guest installation and management, the `libvirtd` needs to run on the VM Host Server. The default `libvirt` configuration is sufficient to install and manage VM Guests from SUSE Manager. However, in case you want to access the VNC console of a VM Guest as a non-`root` user, you need to configure `libvirt` appropriately. Configuration instructions for `libvirt` on SUSE Linux Enterprise Server are available in the *SLES 11 Virtualization with KVM Administration Guide* available from http://www.novell.com/documentation/sles11/. For instructions for a RedHat VM Host Server refer to your RedHat Enterprise Linux documentation.

Apart from being able to serve as a host for KVM or Xen guests which are managed by `libvirt`, a VM Host Server must be registered with SUSE Manager.

1 Make sure either KVM or Xen is properly set up.

2 Make sure the `libvirtd` is running.

3 Register the VM Host Server with SUSE Manager:

> **3a** Create a bootstrap script on the SUSE Manager as described in Procedure "Generating the Bootstrap Script" (↑Quick Start).

> **3b** Download the bootstrap script from susemanager.example.com/pub/bootstrap/bootstrap.sh to the VM Host Server.

> **3c** Edit the bootstrap script according to your needs. The minimal requirement is to include the activation key for the VM Host Server (see Section 7.1.1.1,

"Activation Keys" (page 210) for details). We strongly recommend to also include one or more GPG keys (for example, your organization key, and package signing keys).

3d Execute the bootstrap script to register the VM Host Server.

4 Once the registration process is finished and all packages have been installed, replace the `rhnsd` (Spacewalk query daemon) with the `osad` (Open Source Architecture Daemon). On a SUSE Linux Enterprise Server system this can be achieved by running the following commands as user `root`:

```
rcrhnsd stop
insserv -r rhnsd
insserv osad
rcosad start
```

> **IMPORTANT: `osad` vs. `rhnsd`**
>
> The `rhnsd` daemon checks for scheduled actions every four hours, so it can take up to four hours before a scheduled action is carried out. When having registered many clients with SUSE Manager this behavior ensures a certain level of load balancing, since not all clients act upon a scheduled action at the same time.
>
> However, when managing VM Guests, you usually want actions like rebooting a VM Guest to be carried out immediately. Replacing `rhnsd` with `osad` ensures just this. The `osad` daemon receives commands over the jabber protocol from SUSE Manager and commands are instantly executed. Alternatively you may schedule actions to be carried out at a fixed time in the future (whereas with `rhnsd` you can only schedule for a time in the future plus up to four hours).

7.1.3 Autoinstalling VM Guests

Once all requirements on the SUSE Manager and the VM Host Server are met, you can start to autoinstall VM Guests on the host. Note that VM Guests will not be automatically registered with SUSE Manager, therefore we strongly recommend to modify the autoinstallation profile as described in Section "Adding a Registration Script to the

Autoinstallation Profile" (page 214). VM Guests need to be registered in order to manage them with SUSE Manager. Proceed as follows to autoinstall a VM Guest;.

IMPORTANT: No parallel Autoinstallations on VM Host Server

It is not possible to install more than one VM Guest at a time on a single VM Host Server. When scheduling more than one autoinstallation with SUSE Manager make sure to choose a timing, that starts the next installation after the previous one has finished. If a guest installation starts, while another one is still running, the running installation will be cancelled.

---

1 Login to the SUSE Manager web interface and click on the *Systems* tab.

2 Click on the VM Host Server's name to open it's *System Status* page.

3 Open the form for creating a new VM Guest by clicking *Virtualization > Provisioning*. Fill out the form by choosing an autoinstallation profile and by specifying a name for the VM Guest (must not already exist on VM Host Server). Choose a proxy if applicable and enter a schedule. In order to change the VM Guest's hardware profile and configuration options, click *Advanced Options*.

4 Finish the configuration by clicking *Schedule Autoinstallation and Finish*. The *Session Status* page opens, where you can monitor the autoinstallation process.

NOTE: Checking the Installation Log

An installation log is available when clicking *Events > History* on the *Session Status* page. This opens the *System History Event* page where you can click on a *Summary* entry to view a detailed log.

In case an installation has failed, you can *Reschedule* it from this page once you have corrected the problem. Doing so, you do not have to configure the installation again.

If the event log does not contain enough information to locate a problem, log in to the VM Host Server console and read the logfile `/var/log/up2date`. If you are using the `rhnsd`, you may alternatively immediately trigger any scheduled actions by calling `rhn_ckeck` on the VM Host Server. Increase the command's verbosity by using the options $-v$, $-vv$, or $-vvv$, respectively.

7.2 Managing VM Guests

Basic VM Guest management actions such as restarting or shutting down a virtual machine as well as changing the CPU and memory allocation can be carried out from the SUSE Manager web interface when the following requirements are met:

- VM Host Server must be a KVM or Xen host

- `libvirtd` must be running on VM Host Server

- VM Host Server and VM Guest must be registered with SUSE Manager

All actions can be carried out from the SUSE Manager web interface from the *Virtualization* page of the VM Host Server. Navigate to this page by clicking on the *Systems* tab. On the resulting page, click on the VM Host Server's name and then on *Virtualization*. This page lists all VM Guests for this host known to SUSE Manager.

7.2.1 Displaying a VM Guest's Profile

Click on the name of a VM Guest on the VM Host Server's *Virtualization* page to open it's profile page with detailed information about this guest. For details refer to Section 4.4.2, "Systems" (page 62).

A profile page for a virtual system dopes not differ from a regular system's profile page and you may perform the same actions from it (e.g. installing software or changing it's configuration) as for a regular system.

7.2.2 Starting, Stopping, Suspending and Resuming a VM Guest

In order to start, stop, restart, suspend or resume a VM Guest, navigate to the VM Host Server's *Virtualization* page. Check one or more *Guests* from the table and scroll down to the bottom of the page. Choose an action from the drop-down list next to *Apply Action* and click *Apply Action*. *Confirm* the action on the next page.

> **NOTE: Automatically restarting a VM Guest**
>
> Automatically restarting a VM Guest when the VM Host Server reboots is not enabled by default on VM Guests and cannot be configured from SUSE Manager. Please refer to your KVM or Xen documentation. Alternatively, you may use `libvirt` to enable automatic reboots.

7.2.3 Changing the CPU or RAM allocation of a VM Guest

To change the CPU or RAM allocation of a VM Guest navigate to the VM Host Server's *Virtualization* page. Check one or more *Guests* from the table and scroll down to the bottom of the page. Choose an action from the *Set* drop-down list and provide a new value. Confirm with *Apply Changes* followed by *Confirm*.

The memory allocation can be changed on the fly, provided the memory ballooning driver is installed on the VM Guest. If this is not the case, or if you want to change the CPU allocation, you need to shutdown the guest first. Refer to Section 7.2.2, "Starting, Stopping, Suspending and Resuming a VM Guest" (page 219) for details.

7.2.4 Deleting a VM Guest

To delete a VM Guest you must first shut it down as described at Section 7.2.2, "Starting, Stopping, Suspending and Resuming a VM Guest" (page 219). Wait at least two minutes to allow the shutdown to finish and then choose *Delete Systems* followed by *Apply Action* and *Confirm*.

7.3 Integrating SUSE Studio Onsite Appliances into SUSE Manager

SUSE Manager allows you to integrate your appliances built with SUSE Studio Onsite and to create virtual hosts based on one of your appliances. The guest can be started, stopped, resumed

7.3.1 Requirements

In order to integrate your SUSE Studio Onsite appliances in SUSE Manager, make sure you have fulfilled the following requirements:

- Real hardware which is not virtualized.

- Have installed the package `rhn-virtualization-host` on your client (see Section 7.3.1.1, "Needed Packages" (page 221)).

- Have an account either on the SUSE Studio Onsite Web site at http://susestudio.com, or you have your own SUSE Studio Onsite service.

- Your activation key contains the Virtualization entitlement (see Section 7.3.1.2, "Activation Keys" (page 222)).

- Have set the SUSE Studio Onsite credentials in SUSE Manager (see Section 7.3.1.3, "Getting your SUSE Studio Onsite API Key" (page 222)).

- Have built your appliance as either in Xen or KVM output (see Section 7.3.1.4, "Providing the Correct Formats" (page 222)).

7.3.1.1 Needed Packages

In order to start deploying virtual appliances, install the package `rhn-virtualization-host` on your client. The package is distributed in the following channels:

Table 7.1   *Channels Distributing rhn-virtualization-host*

Product	Architecture (i586/x86_64/s390x)
SLES11 SP1	Parent channel: `sles11-sp1-pool-ARCH` `sles11-sp1-suse-manager-tools-ARCH`

Product	Architecture (i586/x86_64/s390x)
SLES11 SP2	Parent channel: `sles11-sp1-pool -ARCH` `sles11-sp2-suse-manager -tools-ARCH`

7.3.1.2 Activation Keys

To enable virtualization for SUSE Studio Onsite check the virtualization entitlement flag as follows:

1 Log in to SUSE Manager.

2 Go to *Systems > Activation Keys* to get a list of all keys.

3 Create a new key or select an existing key.

4 Scroll down and enable the *Virtualization Platform* entitlements.

5 Finish with *Update Activation Key*.

7.3.1.3 Getting your SUSE Studio Onsite API Key

The SUSE Studio Onsite API key is needed to associate your SUSE Studio Onsite credentials with your SUSE Manager account. Log in to SUSE Manager, go to *Overview > Your Account > Credentials* and add your user name, API key, and your SUSE Studio Onsite instance.

The API key can be found in SUSE Studio Onsite when you select your user name in the main tab and go to *API & hook*.

7.3.1.4 Providing the Correct Formats

SUSE Studio Onsite offers a couple of formats to output your appliance. At the moment, SUSE Manager supports only deploying KVM or Xen formats. Log into SUSE Studio

Onsite, select your appliance, and go to the *Build* tab. Build a new version and choose as default format *VMware/VirtualBox KVM (.vmdk)* or *Xen guest*. After the build has succeeded, you can build additional formats.

Additionally, SUSE Studio Onsite allows you to build your appliance with support for SUSE Manager. To activate it, do the following:

1 Log in to SUSE Studio Onsite.

2 Create a new appliance or click an existing appliance link.

3 Go to *Configuration > Appliance*.

4 Enable the *Integrate with SUSE Manager* checkbox.

5 Enter the hostname or the IP address of your SUSE Manager server and the name of the bootstrap script.

6 Rebuild your appliance.

When you start your appliance the first time, it will be register on your SUSE Manager server.

7.3.2 Setting Up SUSE Manager

In order to add virtualization support to one of your SUSE Manager clients, proceed as follows:

1 Check if you have all fulfilled all requirements from Section 7.3.1, "Requirements" (page 221).

2 Prepare your SUSE Manager client:

2a Start a shell and log into your SUSE Manager client which you turn on virtualization support.

2b Start YaST in your console and go to *Virtualization > Install Hypervisor and Tools*.

2c Choose your hypervisor, be it KVM (recommended) or Xen. After you have selected your preferred hypervisor, YaST will perform the following actions:

1. Installing the necessary packages.

2. Creating a network bridge.

3. Rebooting your client.

2d After the reboot is finished, login again into your SUSE Manager client and start YaST.

3 Log into SUSE Manager.

4 Go to *Systems* tab and select one of your machines which should run the KVM or Xen appliance.

5 Go to the *Virtualization > Images* subtab. SUSE Manager prints a list of all your available appliances which provides a KVM or Xen type.

6 Choose from the list of your appliances and click the link.

7 If needed, change any values, like number of virtual CPUs, proxy server, memory, etc.

8 Click *Schedule Deployment* to start the image deployment process.

If you want to stop, resume, or interact with the guest, select the checkbox of your guest, choose one of the options from the popup menu, and click *Apply Action*. The same actions can be performed on the commandline by using `virsh` (KVM, see `http://www.suse.com/documentation/sles11/book_kvm/data/book_kvm.html`) or `xm` (Xen, see `http://www.suse.com/documentation/sles11/book_xen/data/book_xen.html`).

Cobbler

8

SUSE Manager features the Cobbler server that allows administrators to centralize their system installation and provisioning infrastructure. Cobbler is an installation server that collects the various methods of performing unattended system installations, whether it be server, workstation, or guest systems in a full or para-virtualized setup.

Cobbler offers several tools to assist in pre-installation guidance, automated installation file management, installation environment management, and more. Features of Cobbler include:

* installation environment analysis using the `cobbler check` command,

* multi-site installation server configuration with `cobbler replicate`,

* virtual machine guest installation automation with the `koan` client-side tool.

8.1 Cobbler Requirements

To use Cobbler as a PXE boot server, you should heed the following guidelines:

* If you plan to use Cobbler to install systems using PXE, you must have a TFTP server installed and configured.

* If you plan to use Cobbler to PXE boot systems for installation, you must either set up a DHCP server for Cobbler PXE booting or have access to your network DHCP

server `/etc/dhcp.conf` to change `next-server` to the hostname or IP address of your Cobbler server.

8.1.1 Configuring Cobbler with /etc/cobbler/settings

Cobbler configuration is mainly done in the `/etc/cobbler/settings` file. Most of the settings can keep the default value for Cobbler to run as intended. For more information about configuring Cobbler settings, consult the `/etc/cobbler/settings` file, which documents each setting in detail.

8.1.2 Cobbler and DHCP

Cobbler supports bare-metal automated installation of systems configured to perform network boots using a PXE boot server. To properly implement a Cobbler installation server, administrators need to either have administrative access to the network's DHCP server or set up DHCP on the Cobbler server itself.

8.1.2.1 Configuring an Existing DHCP Server

If you have a DHCP server deployed on another system in the network, you will need administrative access to the DHCP server in order to edit the DHCP configuration file so that it points to the Cobbler server and PXE boot image.

As root on the DHCP server, edit the `/etc/dhcpd.conf` file and append a new class with options for performing PXE boot installation. For example:

```
allow booting;
allow bootp; ❶
class "PXE" ❷ {
match if substring(option vendor-class-identifier, 0, 9) = "PXEClient"; ❸
next-server 192.168.2.1; ❹
filename "pxelinux.0"; ❺
}
```

Step by step explanation:

❶   Enable network booting with the `bootp` protocol.

❷   Create a class called `PXE`.
❸   A system that is configured to have PXE first in its boot priority, identifies itself
      as `PXEClient.`
❹   As a result, the DHCP server directs the system to the Cobbler server at
      `192.168.2.1.`
❺   The DHCP server retrieves the `pxelinux.0` bootloader file.

8.1.3 Xinetd and TFTP

SUSE Manager uses the `atftpd` daemon, but it can also operate with Xinetd/TFTP.
The `atftpd` is installed per default and the recommended method for providing PXE
services. Usually you do not have to change its configuration, but if you have to, use
the YaST Sysconfig Editor.

Xinetd is a daemon that manages a suite of services, including TFTP, the FTP server
used for transferring the boot image to a PXE client.

To configure TFTP, you must first enable the service via Xinetd. To do this, edit the
`/etc/xinetd.d/tftp` as root and change the `disable = yes` line to `disable
= no`.

Before TFTP can serve the `pxelinux.0` boot image, you must start the Xinetd service.
Start YaST and use *System > System Services (Runlevel)* to configure the Xinetd daemon.

8.1.4 Syncing and Starting the Cobbler
        Service

Once all the prerequisites specified in `cobbler check` are configured to your needs,
start the Cobbler service.

Start the SUSE Manager server with the following command:

```
/usr/sbin/spacewalk-service start
```

WARNING

Do not start or stop the `cobblerd` service independent of the SUSE Manager service, as doing so may cause errors and other issues.

Always use `/usr/sbin/spacewalk-service` to start or stop SUSE Manager.

8.2 Adding a Distribution to Cobbler

When all Cobbler prerequisites are met and Cobbler is running, you can use the Cobbler server as an installation source for a distribution: Make installation files such as the kernel image and the initrd image available on the Cobbler server. Then add a distribution to Cobbler, using either the Web interface or the command line tools.

For information about creating and configuring AutoYaST or Kickstart distributions from the SUSE Manager interface, refer to Section 4.4.9.8, "Autoinstallation > Distributions — [Prov]" (page 123).

To create a distribution from the command line, use `cobbler` as follows:

```
cobbler distro add --name=string --kernel=path --initrd=path
```

The `--name=string` option is a label used to differentiate one distribution choice from another (for example, `sles11server`)

The `--kernel=path` option specifies the path to the kernel image file

The `--initrd=path` option specifies the path to the initial ramdisk (initrd) image file.

8.3 Adding a Profile to Cobbler

Once you have configured a distribution for Cobbler, add profiles.

Cobbler profiles associate a distribution with additional options, like AutoYaST or Kickstart files. Profiles are the core unit of provisioning and there must be at least one Cobbler profile for every distribution added. For example, two profiles might be created

for a web server and a desktop configuration. While both profiles use the same distribution, the profiles are for different installation types.

For information about creating and configuring Kickstart and AutoYaST profiles in the SUSE Manager interface, refer to Section 4.4.9.3, "Autoinstallation Profiles (Kickstart and AutoYaST)" (page 113).

Use `cobbler` to create profiles on the command line:

```
cobbler profile add --name=string --distro=string [--kickstart=url] -
[--virt-file-size=gigabytes] [--virt-ram=megabytes]
```

The `--name=`*string* is the unique label for the profile, such as `sles11webserver` or `sles11workstation`.

The `--distro=`*string* option specifies the distribution that will be used for this particular profile. Distributions were added in Section 8.2, "Adding a Distribution to Cobbler" (page 228).

The `--kickstart=`*url* option specifies the location of the Kickstart file (if available).

The `--virt-file-size=`*gigabytes* option allows you to set the size of the virtual guest file image. The default is 5 gigabytes.

The `--virt-ram=`*megabytes* option specifies how many megabytes of physical RAM a virtual guest can consume. The default is 512 megabytes.

8.4 Adding a System to Cobbler

Once the distributions and profiles for Cobbler have been created, add systems to Cobbler. System records map a piece of hardware on a client with the cobbler profile assigned to run on it.

NOTE

If you are provisioning via `koan` and PXE menus alone, it is not required to create system records, though they are useful when system-specific Kickstart templating is required or to establish that a specific system should always get

a specific content installed. If a client is intended for a specific role, system records should be created for it.

For information about creating and configuring automated installation from the SUSE Manager interface, refer to Section "System Details > Provisioning — [Prov]" (page 80).

The following command adds a system to the Cobbler configuration:

```
cobbler system add --name=string --profile=string --mac=AA:BB:CC:DD:EE:FF
```

The `--name=`*`string`* is the unique label for the system, such as `engineering_server` or `frontoffice_workstation`.

The `--profile=`*`string`* specifies one of the profile names added in Section 8.3, "Adding a Profile to Cobbler" (page 228).

The `--mac=`*`AA:BB:CC:DD:EE:FF`* option allows systems with the specified MAC address to automatically be provisioned to the profile associated with the system record if they are being installed.

For more options, such as setting hostname or IP addresses, refer to the Cobbler manpage (`man cobbler`).

8.5 Cobbler Templates

The SUSE Manager Web interface facilitates creating variables for use with Kickstart distributions and profiles. To create a Kickstart profile variable, refer to Section "Autoinstallation Details > Variables" (page 117).

Kickstart variables are a part of an infrastructural change in SUSE Manager to support templating in Kickstart files. Kickstart templates are files describing how to build actual Kickstart files, rather than creating specific Kickstarts.

These templates are shared by various profiles and systems that have their own variables and corresponding values. These variables modify the templates and a template engine parses the template and variable data into a usable Kickstart file. Cobbler uses an advanced template engine called Cheetah that provides support for templates, variables, and snippets.

Advantages of using templates include:

- Robust features that allow administrators to create and manage large amounts of profiles or systems without duplication of effort or manually creating Kickstarts for every unique situation.

- While templates can become complex and involve loops, conditionals and other enhanced features and syntax, you can keep them simply by creating Kickstart files without such complexity.

8.5.1 Using Templates

Kickstart templates can have static values for certain common items such as PXE image filenames, subnet addresses, and common paths such as `/etc/sysconfig/network -scripts/`. However, templates differ from standard Kickstart files in their use of variables.

For example, a standard Kickstart file may have a networking section similar to the following:

```
network --device=eth0 --bootproto=static --ip=192.168.100.24 -
--netmask=255.255.255.0 --gateway=192.168.100.1 --nameserver=192.168.100.2
```

In a Kickstart template file, the networking section would rather look like this:

```
network --device=$net_dev --bootproto=static --ip=$ip_addr -
--netmask=255.255.255.0 --gateway=$my_gateway --nameserver=$my_nameserver
```

These variables will be substituted with the values set in your Kickstart profile variables or in your system detail variables. If there are the same variables defined in both the profile and the system detail, then the system variable takes precedence.

For more information about Kickstart templates, refer to the Cobbler project page at:

https://fedorahosted.org/cobbler/wiki/KickstartTemplating

8.5.2 Kickstart Snippets

If you have common configurations across all Kickstart templates and profiles, you can use the Snippets feature of Cobbler to take advantage of code reuse.

Kickstart snippets are sections of Kickstart code that can be called by a `$SNIPPET()` function that will be parsed by Cobbler and substituted with the contents of the snippet.

For example, you might have a common hard drive partition configuration for all servers, such as:

```
clearpart --all
part /boot --fstype ext3 --size=150 --asprimary
part / --fstype ext3 --size=40000 --asprimary
part swap --recommended

part pv.00 --size=1 --grow

volgroup vg00 pv.00
logvol /var --name=var vgname=vg00 --fstype ext3 --size=5000
```

Save this snippet of the configuration to a file like `my_partition` and place the file in `/var/lib/cobbler/snippets/` where Cobbler can access them.

Use the snippet by callin the `$SNIPPET()` function in your Kickstart templates. For example:

```
$SNIPPET('my_partition')
```

Wherever you invoke that function, the Cheetah parser will substitute the function with the snippet of code contained in the `my_partition` file.

For more information about Kickstart snippets, refer to the Cobbler project page at:

https://fedorahosted.org/cobbler/wiki/KickstartSnippets

8.6 Using Koan

Whether you are provisioning guests on a virtual machine or re-installing a new distribution on a running system, koan works in conjunction with Cobbler to provision systems on the fly.

8.6.1 Using Koan to Provision Virtual Systems

If you have created a virtual machine profile as documented in Section 8.3, "Adding a Profile to Cobbler" (page 228), you can use `koan` to initiate the installation of a virtual guest on a system.

For example, create a Cobbler profile with the following command:

```
cobbler add profile --name=virtualfileserver --distro=sless11-x86_64-server -
--virt-file-size=20 --virt-ram=1000
```

This profile is for a fileserver running SUSE Linux Enterprise Server 11 with a 20GB guest image size and allotted 1GB of system RAM.

To find the name of the virtual guest system profile, run the following `koan` command:

```
koan --server=hostname --list-profiles
```

This command lists all the available profiles created with `cobbler profile add`.

Start creating the image file and the installation of the virtual guest system.

```
koan --virt --server=cobbler-server.example.com --profile=virtualfileserver -
--virtname=marketingfileserver
```

The command specifies that a virtual guest system be created from the Cobbler server (hostname `cobbler-server.example.com`) using the `virtualfileserver` profile. The `virtname` option specifies a label for the virtual guest, which by default is the system's MAC address.

Once the installation of the virtual guest is complete, it can be used as any other virtual guest system.

8.6.2 Using Koan to Re-install Running Systems

`koan` can replace a still running system with a new installation from the available Cobbler profiles by executing the following command *on the system to be re-installed*:

```
koan --replace-self --server=hostname --profile=name
```

This command, running on the system to be replaced, will start the provisioning process and replace its own system using the profile in `--profile=name` on the Cobbler server specified in `--server=hostname`.

Command Line Config Management Tools

<div style="text-align: right; font-size: 2em; font-weight: bold;">A</div>

In addition to the SUSE Manager Web interface, SUSE Manager offers two command line tools for managing system configuration files: the Configuration Client and the Configuration Manager. There is a complementary Actions Control tool that is used to enable and disable configuration management on client systems. If you do not yet have these tools installed, they can be found in the *SUSE Manager Tools* child channel for your operating system (package names are: `rhncfg-client`, `rhncfg-management`, and `rhncfg-actions`).

NOTE: Tip

Keep in mind, whenever a configuration file is deployed via SUSE Manager, a backup of the previous file including its full path is made in the `/var/lib/rhncfg/backups/` directory on the affected system. The backup retains its filename but has a `.rhn-cfg-backup` extension appended.

A.1 Actions Control

The Actions Control (`mgr-actions-control`) application is used to enable and disable configuration management on a system. Client systems cannot be managed in this fashion by default. This tool allows SUSE Manager Administrators to enable or disable specific modes of allowable actions such as: *deploying* a configuration file on the system, *uploading* a file from the system, *diffing* what is currently managed on a system with what is available, or running *remote commands*. These various modes are enabled/disabled by placing/removing files and directories in the `/etc/sysconfig/`

rhn/allowed-actions/ directory. Due to the default permissions of the /etc/
sysconfig/rhn/ directory, Actions Control will most likely have to be run by
someone with root access.

A.1.1 General command line options

There is a manpage available, as there are for most command line tools, though the use
of this tool is simple enough to describe here briefly. First, decide what scheduled actions
should be enabled for use by system administrators. The following options enable the
various scheduled action modes:

Table A.1   *mgr-actions-control options*

Option	Description
--enable-deploy	Allow mgrcfg-client to deploy files.
--enable-diff	Allow mgrcfg-client to diff files.
--enable-upload	Allow mgrcfg-client to upload files.
--enable-mtime-upload	Allow mgrcfg-client to upload mtime (file modification time).
--enable-all	Allow mgrcfg-client to do everything.
--enable-run	Enable running scripts.
--disable-deploy	Disable deployment.
--disable-diff	Prohibit diffing.
--disable-upload	No file uploads allowed.
--disable-mtime-upload	Disable mtime upload.
--disable-all	Disable all options
--disable-run	No scripts allowed to run.

Option	Description
--report	Report whether modes are enabled or disabled.
-f, --force	Force the operation without asking first.
-h, --help	Show help message and exit.

Once a mode is set—and for many `mgr-actions-control --enable-all` is common—your system is ready for configuration management through SUSE Manager.

A.2 Configuration Client

As the name implies, the Configuration Client (`mgrcfg-client`) is installed on and run from an individual client system to gain knowledge about how SUSE Manager deploys configuration files to the client.

The Configuration Client offers these primary modes: list, get, channels, diff, and verify.

A.2.1 Listing Config Files

To list the configuration files for the machine and the labels of the config channels containing them, issue the command:

```
mgrcfg-client list
```

The output resembles the following list ("DoFoS" is a shortcut for "D or F or S", which means "Directory", "File", or "Something else"(?)):

```
DoFoS   Config Channel      File
F       config-channel-17   /etc/example-config.txt
F       config-channel-17   /var/spool/aalib.rpm
F       config-channel-14   /etc/rhn/rhn.conf
```

These configuration files apply to your system. However, there may be duplicate files present in other channels. For example, issue the following command:

```
mgrcfg-manager list config-channel-14
```

and observe the following output:

```
Files in config channel 'config-channel-14'
/etc/example-config.txt /etc/rhn/rhn.conf
```

You may wonder why the second version of /etc/example-config.txt in config-channel-14 does not apply to the client system. The rank of the /etc/example-config.txt file in config-channel-17 was higher than that of the same file in config-channel-14. As a result, the version of the configuration file in config-channel-14 is not deployed for this system, therefore mgrcfg-client command does not list the file.

A.2.2 Getting a Config File

To download the most relevant configuration file for the machine, issue the command:

```
mgrcfg-client get /etc/example-config.txt
```

You should see output resembling:

```
Deploying /etc/example-config.txt
```

You may then view the contents of the file with less or another pager. Note that the file is selected as the most relevant based upon the rank of the config channel containing it. This is accomplished within the *Configuration* tab of the *System Details* page. Refer to Section 4.4.2.10, "System Details" (page 66) for instructions.

A.2.3 Viewing Config Channels

To view the labels and names of the config channels that apply to the system, issue the command:

```
mgrcfg-client channels
```

You should see output resembling:

```
Config channels:
Label               Name
-----               ----
config-channel-17   config chan 2
config-channel-14   config chan 1
```

The following table lists the options available for `mgrcfg-client get`:

Table A.2 *mgrcfg-client get options*

Option	Description
--topdir=TOPDIR	Make all file operations relative to this string.
-h, --help	Show help message and exit.

A.2.4 Differentiating between Config Files

To view the differences between the config files deployed on the system and those stored by SUSE Manager, issue the command:

```
mgrcfg-client diff
```

The output resembles the following:

```
--- /tmp/@3603.0.rhn-cfg-tmp 2004-01-13 14:18:31.000000000 -0500
+++ /etc/example-config.txt 2003-12-16 21:35:32.000000000 -0500
@@ -1,3 +1,5 @@
+additional text
```

In addition, you may include the `--topdir` option to compare config files with those located in an arbitrary (and unused) location on the client system, like this:

```
# mgrcfg-client diff --topdir /home/test/blah/
/usr/bin/diff: /home/test/blah/etc/example-config.txt: No such file or -
directory
/usr/bin/diff: /home/test/blah/var/spool/aalib.rpm: No such file or directory
```

A.2.5 Verifying Config Files

To quickly determine if client configuration files are different from those associated with it via SUSE Manager, issue the command:

```
        mgrcfg-client verify
```

The output resembles the following:

```
modified /etc/example-config.txt /var/spool/aalib.rpm
```

The file `example-config.txt` is locally modified, while `aalib.rpm` is not.

The following table lists the options available for `mgrcfg-client verify`:

Table A.3   *mgrcfg-client verify options*

Option	Description
-v, --verbose	Increase the amount of output detail. Displays differences in the mode, owner, and group permissions for the specified config file.
-h, --help	Show help message and exit.

A.3 Configuration Manager

The Configuration Manager (`mgrcfg-manager`) is designed to maintain SUSE Manager's central repository of config files and channels, not those located on client systems. This tool offers a command line alternative to the configuration management features in the SUSE Manager Web interface. Additionally, some or all of the related maintenance tasks can be scripted.

To use the command line interface, Config Administrators require a SUSE Manager account (username and password) with the appropriate permission set. The username may be specified in `/etc/sysconfig/rhn/rhncfg-manager.conf` or in the [rhncfg-manager] section of `~/.rhncfgrc`.

When the Configuration Manager is run as root, it attempts to pull in needed configuration values from the Red Hat Update Agent. When run as a user other than root, you may have to change the `~/.rhncfgrc` configuration file. The session file is cached in `~/.rhncfg-manager-session` to avoid having to log in for every command.

The default timeout for the Configuration Manager is 30 minutes. To alter this, add the `server.session_lifetime` option and a new value to the `/etc/rhn/rhn`

`.conf` file on the server running the manager, for example set the time out to 120 minutes:

```
server.session_lifetime = 120
```

The Configuration Manager offers these primary modes: add, create-channel, diff, diff-revisions, download-channel, get, list, list-channels, remove, remove-channel, revisions, update, and upload-channel.

Each mode offers its own set of options, which can be displayed by issuing the following command:

```
mgrcfg-manager mode --help
```

Replace *mode* with the name of the mode whose options you'd like to see:

```
mgrcfg-manager diff-revisions --help
```

Find a list of options for the add mode at Table A.4, "`mgrcfg-manager add` options" (page 242).

A.3.1 Creating a Config Channel

To create a config channel for your organization, issue the command:

```
mgrcfg-manager create-channel channel-label
```

If prompted for your SUSE Manager username and password, provide them.

Once you have created a config channel, use the remaining modes listed above to populate and maintain that channel.

A.3.2 Adding Files to a Config Channel

To add a file to a config channel, specify the channel label and the local file to be uploaded:

```
mgrcfg-manager add --channel=channel-label/path/to/file
```

In addition to the required channel label and the path to the file, you may use the available options for modifying the file during its addition. For instance, you may alter the path and file name by including the `--dest-file` option in the command, like:

```
mgrcfg-manager add --channel=channel-label \
--dest-file=/new/path/to/file.txt/path/to/file
```

The output resembles the following:

```
Pushing to channel example-channel
Local file >/path/to/file -> remote file /new/path/to/file.txt
```

The following table lists the options available for `mgrcfg-manager add`:

Table A.4 *mgrcfg-manager add options*

Option	Description
-cCHANNEL --channel=CHANNEL	Upload files in this config channel
-dDEST_FILE --dest-file=DEST_FILE	Upload the file as this path
--delim-start=DELIM_START	Start delimiter for variable interpolation
--delim-end=DELIM_END	End delimiter for variable interpolation
-h, --help	show help message and exit

NOTE

By default, the maximum file size for configuration files is 128KB. If you need to change that value, find or create the following line in the `/etc/rhn/rhn.conf` file:

```
web.maximum_config_file_size=128
```

Change the value from 128 to whatever limit you want in bytes.

A.3.3 Differentiating between Latest Config Files

To view the differences between the config files on disk and the latest revisions in a channel, issue the command:

```
          mgrcfg-manager diff --channel=channel-label -
--dest-file=/path/to/file.txt \
/local/path/to/file
```

You should see output resembling:

```
/tmp/dest_path/example-config.txt /home/test/blah/hello_world.txt
--- /tmp/dest_path/example-config.txt config_channel: example-channel -
revision: 1
+++ /home/test/blah/hello_world.txt 2003-12-14 19:08:59.000000000 -0500
@@ -1 +1 @@
-foo
+hello, world
```

The following table lists the options available for `mgrcfg-manager diff`:

Table A.5   *mgrcfg-manager diff options*

Option	Description
-cCHANNEL, --channel=CHANNEL	Get file(s) from this config channel
-rREVISION, --revision=REVISION	Use this revision
-dDEST_FILE, --dest-file=DEST_FILE	Upload the file as this path
-tTOPDIR, --topdir=TOPDIR	Make all files relative to this string
-h, --help	Show help message and exit

A.3.4 Differentiating between Various Versions

To compare different versions of a file across channels and revisions, use the −r flag to indicate which revision of the file should be compared and the −n flag to identify the two channels to be checked. Refer to Section A.3.11, "Determining the Number of File Revisions" (page 247) for related instructions. Specify only one file name here, since you are comparing the file against another version of itself. For example:

```
mgrcfg-manager diff-revisions -
-n=channel-label1-r=1-n=channel-label2-r=1/path/to/file.txt
```

The output resembles the following:

```
--- /tmp/dest_path/example-config.txt 2004-01-13 14:36:41 \
config channel: example-channel2 revision: 1
--- /tmp/dest_path/example-config.txt 2004-01-13 14:42:42 \
config channel: example-channel3 revision: 1
@@ -1 +1,20 @@
-foo
+blaaaaaaaaaaaaaaah
+-----BEGIN PGP SIGNATURE-----
+Version: GnuPG v1.0.6 (GNU/Linux)
+Comment: For info see http://www.gnupg.org
+
+iD8DBQA9ZY6vse4XmfJPGwgRAsHcAJ9ud9dabUcdscdcqB8AZP7e0Fua0NmKsdhQCeOWHX
+VsDTfen2NWdwwPaTM+S+Cow=
+=Ltp2
+-----END PGP SIGNATURE-----
```

The following table lists the options available for mgrcfg-manager diff-revisions:

Table A.6 *mgrcfg-manager diff-revisions options*

Option	Description
-cCHANNEL, --channel=CHANNEL	Use this config channel
-rREVISION, --revision=REVISION	Use this revision
-h, --help	Show help message and exit

A.3.5 Downloading All Files in a Channel

To download all the files in a channel to disk, create a directory and issue the following command:

```
mgrcfg-manager download-channel channel-label --topdir .
```

The output resembles the following:

```
Copying /tmp/dest_path/example-config.txt -> \
blah2/tmp/dest_path/example-config.txt
```

The following table lists the options available for `mgrcfg-manager download-channel`:

Table A.7   *mgrcfg-manager download-channel options*

Option	Description
-tTOPDIR, --topdir=TOPDIR	Directory to which all the file paths are relative. This option must be set.
-h, --help	Show help message and exit.

A.3.6 Getting the Contents of a File

To direct the contents of a particular file to stdout, issue the command:

```
        mgrcfg-manager get --channel=channel-label \
/tmp/dest_path/example-config.txt
```

You should see the contents of the file as output.

A.3.7 Listing All Files in a Channel

To list all the files in a channel, issue the command:

```
mgrcfg-manager list channel-label
```

You should see output resembling:

```
Files in config channel `example-channel3':
/tmp/dest_path/example-config.txt
```

The following table lists the options available for `mgrcfg-manager get`:

Table A.8   *mgrcfg-manager get options*

Option	Description
-cCHANNEL, --channel=CHANNEL	Get file(s) from this config channel
-tTOPDIR, --topdir=TOPDIR	Make all files relative to this string
-rREVISION, --revision=REVISION	Get this file revision
-h, --help	Show help message and exit

A.3.8 Listing All Config Channels

To list all of your organization's configuration channels, issue the command:

```
mgrcfg-manager list-channels
```

The output resembles the following:

```
Available config channels:
example-channel example-channel2 example-channel3 config-channel-14 -
config-channel-17
```

Note that this does not list `local_override` or `server_import` channels.

A.3.9 Removing a File from a Channel

To remove a file from a channel, issue the command:

```
        mgrcfg-manager remove --channel=channel-label -
/tmp/dest_path/example-config.txt
```

If prompted for your SUSE Manager username and password, provide them.

The following table lists the options available for `mgrcfg-manager remove`:

Table A.9 *mgrcfg-manager remove options*

Option	Description
-cCHANNEL, --channel=CHANNEL	Remove files from this config channel
-tTOPDIR, --topdir=TOPDIR	Make all files relative to this string
-h, --help	Show help message and exit

A.3.10 Deleting a Config Channel

To remove a config channel in your organization, issue the command:

```
        mgrcfg-manager remove-channel channel-label
```

The output resembles the following:

```
Removing config channel example-channel Config channel example-channel removed -
```

A.3.11 Determining the Number of File Revisions

To find out how many revisions (from 1 to N where N is an integer greater than 0) of a file/path are in a channel, issue the following command:

```
        mgrcfg-manager revisions channel-label -
/tmp/dest_path/example-config.txt
```

The output resembles the following:

```
Analyzing files in config channel example-channel \
/tmp/dest_path/example-config.txt: 1
```

A.3.12 Updating a File in a Channel

To create a new revision of a file in a channel (or to add the first revision to that channel if none existed before for the given path), issue the following command:

```
          mgrcfg-manager update \
--channel=channel-label \
--dest-file=/path/to/file.txt/local/path/to/file
```

The output resembles the following:

```
Pushing to channel example-channel:
Local file example-channel /tmp/local/example-config.txt -> \
remote file /tmp/dest_path/example-config.txt
```

The following table lists the options available for `mgrcfg-manager update`:

Table A.10   *mgrcfg-manager update options*

Option	Description
-cCHANNEL, --channel=CHANNEL	Upload files in this config channel
-dDEST_FILE, --dest-file=DEST_FILE	Upload the file to this path
-tTOPDIR, --topdir=TOPDIR	Make all files relative to this string
--delim-start=DELIM_START	Start delimiter for variable interpolation
--delim-end=DELIM_END	End delimiter for variable interpolation
-h, --help	Show help message and exit

A.3.13 Uploading Multiple Files at Once

To upload multiple files to a config channel from a local disk at once, issue the command:

```
mgrcfg-manager upload-channel --topdir=topdirchannel-label
```

The output resembles the following:

```
Using config channel example-channel4 Uploading /tmp/ola_world.txt from -
blah4/tmp/ola_world.txt -
```

The following table lists the options available for `mgrcfg-manager upload-channel`:

Table A.11 *mgrcfg-manager upload-channel options*

Option	Description
-tTOPDIR, --topdir=TOPDIR	Directory all the file paths are relative to
-cCHANNEL, --channel=CHANNEL	List of channels the config info will be uploaded into. Channels delimited by ','. Example: --channel=foo,bar,baz
-h, --help	Show help message and exit

Probes

<div style="text-align: right; font-size: xx-large; font-weight: bold;">B</div>

As described in Section 4.10, "Monitoring — [Mon]" (page 157), monitoring-entitled systems can have probes applied to them that constantly confirm their health and full operability. This appendix lists the available probes sorted by command group, such as Apache.

Many probes that monitor internal system aspects (such as the Linux::Disk Usage probe) rather than external aspects (such as the Network Services::SSH probe) require the installation of the SUSE Manager monitoring daemon (`rhnmd`). This requirement is noted in the individual probe reference.

Each probe has its own reference in this appendix that identifies required fields (marked with *), default values, and the thresholds that may be set to trigger alerts. The beginning of each command group's section contains information applicable to all probes in that group. Section B.1, "Probe Guidelines" (page 252) covers general guidelines; the remaining sections examine individual probes.

NOTE

Nearly all of the probes use Transmission Control Protocol (TCP) as their transport protocol. Exceptions to this are noted within the individual probe references.

B.1 Probe Guidelines

The following general guidelines outline the meaning of each probe state, and provide guidance in setting thresholds for your probes.

Unknown
> State of probes that cannot collect the metrics needed to determine probe state. Probes in this state may be configured incorrectly. Most (though not all) probes enter this state when exceeding their timeout period.

Pending
> State of probes whose data has not been received by SUSE Manager. It is normal for new probes to be in this state. However, if all probes move into this state, your monitoring infrastructure may be failing.

OK
> State of probes that have run successfully without error. This is the desired state for all probes.

Warning
> State of probes that have crossed their WARNING thresholds.

Critical
> State of probes that have crossed their CRITICAL thresholds or reached a critical status by some other means. Some probes become critical when exceeding their timeout period.

While adding probes, select useful thresholds. When these thresholds are crossed, the probe notifies you and your administrators of problems within your infrastructure. Timeout periods are entered in seconds unless otherwise indicated. Exceptions to these rules are noted in the individual probe references.

IMPORTANT

Some probes have thresholds based on time. In order for such CRITICAL and WARNING thresholds to work as intended, their values cannot exceed the amount of time allotted to the timeout period. Otherwise, an UNKNOWN status is returned in all instances of extended latency, thereby nullifying the thresholds.

> For this reason, it is strongly recommended to ensure that timeout periods exceed all timed thresholds.

It is recommended to run your probes without notifications for a time to establish baseline performance for each of your systems. Although the default values provided for probes may suit your needs, every organization has a different environment that may require altering thresholds.

B.2 Apache 1.3.x and 2.0.x

The probes in this section may be applied to instances of the Apache Web server. Although the default values presume you will apply these probes using standard HTTP, you may also use them over secure connections by changing the application protocol to `https` and the port to `443`.

B.2.1 Apache::Processes

The Apache::Processes probe monitors the processes running on an Apache Web server and collects the following metrics:

- Data Transferred Per Child — Records data transfer information only for individual child processes. A child process is created by another process (parent).

- Data Transferred Per Slot — The cumulative amount of data transferred by a child process that restarts. The number of slots is configured in the `httpd.conf` file using the `MaxRequestsPerChild` setting.

The `ExtendedStatus` directive in the `httpd.conf` file of the Web server must be set to `On` for this probe to function properly.

Table B.1 *Apache::Processes settings*

Field	Value
Application Protocol*	http
Port*	80

Field	Value
Pathname*	/server-status
UserAgent*	NOCpulse-ApacheUptime/1.0
Username	
Password	
Timeout*	15
Critical Maximum Megabytes Transferred Per Child	
Warning Maximum Megabytes Transferred Per Child	
Critical Maximum Megabytes Transferred Per Slot	
Warning Maximum Megabytes Transferred Per Slot	

B.2.2 Apache::Traffic

The Apache::Traffic probe monitors the requests on an Apache Web server and collects the following metrics:

- Current Requests — The number of requests being processed by the server at probe runtime.

- Request Rate — Number of server accesses per second since the probe last ran.

- Traffic — Kilobytes of traffic per second the server has processed since the probe last ran.

The ExtendedStatus directive in the httpd.conf file of the Web server must be set to On for this probe to function properly.

Table B.2   *Apache::Traffic settings*

Field	Value
Application Protocol*	http
Port*	80
Pathname*	/server-status
UserAgent*	NOCpulse-ApacheUptime/1.0
Username	
Password	
Timeout*	15
Critical Maximum Current Requests (number)	
Warning Maximum Current Requests (number)	
Critical Maximum Request Rate (events per second)	
Warning Maximum Request Rate (events per second)	
Critical Maximum Traffic (kilobytes per second)	
Warning Maximum Traffic (kilobytes per second)	

B.2.3 Apache::Uptime

The Apache::Uptime probe stores the cumulative time since the Web server was last started. No metrics are collected by this probe, which is designed to help track service level agreements (SLAs).

Table B.3 *Apache::Uptime settings*

Field	Value
Application Protocol*	http
Port*	80
Pathname*	/server-status
UserAgent*	NOCpulse-ApacheUptime/1.0
Username	
Password	
Timeout*	15

B.3 BEA WebLogic 6.x and higher

The probes in this section (with the exception of JDBC Connection Pool) can be configured to monitor the properties of any BEA WebLogic 6.x and higher server (administration or managed) running on a given host, even in a clustered environment. Monitoring of a cluster is achieved by sending all SNMP queries to the administration server of the domain and then querying its Managed Servers for individual data.

In order to obtain this higher level of granularity, the *BEA Domain Admin Server* parameter must be used to differentiate between the administration server receiving SNMP queries and the Managed Server undergoing the specified probe. If the host to be probed is the Administration Server, then the *BEA Domain Admin Server* parameter can be left blank, and both the SNMP queries and the probe will be sent to it only.

If the host to be probed is a managed server, then the IP address of the administration server should be provided in the *BEA Domain Admin Server* parameter, and the managed server name should be included in the *BEA Server Name* parameter and appended to the end of the *SNMP Community String* field. This causes the SNMP queries to be sent to the administration server host, as is required, but redirects the specific probe to the managed server host.

Note that the community string needed for probes run against managed server hosts should be in the form of `community_prefix@managed_server_name` for the SNMP query to return results. SNMP must be enabled on each monitored system. SNMP support can be enabled and configured via the WebLogic console.

Refer to the documentation for your BEA server or information on the BEA website for more details about BEA's community string naming conventions: `http://e-docs.bea.com/wls/docs70/snmpman/snmpagent.html`

B.3.1 BEA WebLogic::Execute Queue

The BEA WebLogic::Execute queue probe monitors the WebLogic execute queue and provides the following metrics:

- Idle Execute Threads — The number of execution threads in an idle state.

- Queue Length — The number of requests in the queue.

- Request Rate — The number of requests per second.

This probe's transport protocol is User Datagram Protocol (UDP).

Table B.4   *BEA WebLogic::Execute Queue settings*

Field	Value
SNMP Community String*	public
SNMP Port*	161
SNMP Version*	1

Field	Value
BEA Domain Admin Server	
BEA Server Name*	myserver
Queue Name*	default
Critical Maximum Idle Execute Threads	
Warning Maximum Idle Execute Threads	
Critical Maximum Queue Length	
Warning Maximum Queue Length	
Critical Maximum Request Rate	
Warning Maximum Request Rate	

B.3.2 BEA WebLogic::Heap Free

The BEA WebLogic::Heap Free probe collects the following metric:

• Heap Free — The percentage of free heap space.

This probe's transport protocol is User Datagram Protocol (UDP).

Table B.5   *BEA WebLogic::Heap Free settings*

Field	Value
SNMP Community String*	public
SNMP Port*	161

Field	Value
SNMP Version*	1
BEA Domain Admin Server	
BEA Server Name*	myserver
Critical Maximum Heap Free	
Warning Maximum Heap Free	
Warning Minimum Heap Free	
Critical Minimum Heap Free	

B.3.3 BEA WebLogic::JDBC Connection Pool

The BEA WebLogic::JDBC Connection Pool probe monitors the Java Database Connection (JDBC) pool on a domain admin server only (no managed servers) and collects the following metrics:

- Connections — The number of connections to the JDBC.

- Connections Rate — The connections per second to the JDBC.

- Waiters — The number of sessions waiting to connect to the JDBC.

This probe's transport protocol is User Datagram Protocol (UDP).

Table B.6   *BEA WebLogic::JDBC Connection Pool settings*

Field	Value
SNMP Community String*	public
SNMP Port*	161
SNMP Version*	1

Field	Value
BEA Domain Admin Server	
BEA Server Name*	myserver
JDBC Pool Name*	MyJDBC Connection Pool
Critical Maximum Connections	
Warning Maximum Connections	
Critical Maximum Connection Rate	
Warning Maximum Connection Rate	
Critical Maximum Waiters	
Warning Maximum Waiters	

B.3.4 BEA WebLogic::Server State

The BEA WebLogic::Server state probe monitors the current state of a BEA WebLogic Web server. If the probe is unable to make a connection to the server, a CRITICAL status results.

This probe's transport protocol is User Datagram Protocol (UDP).

Table B.7 *BEA WebLogic::Server State settings*

Field	Value
SNMP Community String*	public
SNMP Port*	161
SNMP Version*	1

Field	Value
BEA Domain Admin Server	
BEA Server Name*	

B.3.5 BEA WebLogic::Servlet

The BEA WebLogic::Servlet probe monitors the performance of a particular servlet deployed on a WebLogic server and collects the following metrics:

- High Execution Time — The highest amount of time in milliseconds that the servlet takes to execute since the system was started.

- Low Execution Time — The lowest amount of time in milliseconds that the servlet takes to execute since the system was started.

- Execution Time Moving Average — A moving average of the execution time.

- Execution Time Average — A standard average of the execution time.

- Reload Rate — The number of times the specified servlet is reloaded per minute.

- Invocation Rate — The number of times the specified servlet is invoked per minute.

This probe's transport protocol is User Datagram Protocol (UDP).

Table B.8 *BEA WebLogic::Servlet settings*

Field	Value
SNMP Community String*	public
SNMP Port*	161
SNMP Version*	1
BEA Domain Admin Server	

Field	Value
BEA Server Name*	myserver
Servlet Name*	
Critical Maximum High Execution Time	
Warning Maximum High Execution Time	
Critical Maximum Execution Time Moving Average	
Warning Maximum Execution Time Moving Average	

B.4 General

The probes in this section are designed to monitor basic aspects of your systems. When applying them, ensure their timed thresholds do not exceed the amount of time allotted to the timeout period. Otherwise, the probe returns an UNKOWN status in all instances of extended latency, thereby nullifying the thresholds.

B.4.1 General::Remote Program

The General::Remote Program probe allows you to run any command or script on your system and obtain a status string. Note that the resulting message will be limited to 1024 bytes.

Requirements — The SUSE Manager monitoring daemon (rhnmd) must be running on the monitored system to execute this probe.

Table B.9 *General::Remote Program settings*

Field	Value
Command*	
OK Exit Status*	0
Warning Exit Status*	1
Critical Exit Status*	2
Timeout	15

B.4.2 General::Remote Program with Data

The General::Remote Program with Data probe allows you to run any command or script on your system and obtain a value, as well as a status string. To use this probe, you must include XML code in the body of your script. This probe supports the following XML tags:

- `perldata perldata`

- `hash hash`

- `hash key="..." hash`

The remote program will output some iteration of the following code to STDOUT:

```
<perldata>
  <hash>
    <item key="data">10</item>
    <item key="status_message">status message here</item>
  </hash>
</perldata>
```

The required value for `data` is the data point to be inserted in the database for time-series trending. The `status_message` is optional and can be whatever text string is desired with a maximum length of 1024 bytes. Remote programs that do not include a `status_message` still report the value and status returned.

Requirements — The SUSE Manager monitoring daemon (`rhnmd`) must be running on the monitored system to execute this probe. XML is case-sensitive. The `data` item key name cannot be changed and it must collect a number as its value.

Table B.10   *General::Remote Program with Data settings*

Field	Value
Command*	
OK Exit Status*	0
Warning Exit Status*	1
Critical Exit Status*	2
Timeout	15

B.4.3 General::SNMP Check

The General::SNMP Check probe tests your SNMP server by specifying a single object identifier (OID) in dotted notation (such as `1.3.6.1.2.1.1.1.0`) and a threshold associated with the return value. It collects the following metric:

• Remote Service Latency — The time in seconds for the SNMP server to answer a connection request.

Requirements — SNMP must be running on the monitored system to perform this probe. Only integers can be used for the threshold values.

This probe's transport protocol is User Datagram Protocol (UDP).

Table B.11   *General::SNMP Check settings*

Field	Value
SNMP OID*	
SNMP Community String*	public

Field	Value
SNMP Port*	161
SNMP Version*	2
Timeout*	15
Critical Maximum Value	
Warning Maximum Value	
Warning Minimum Value	
Critical Minimum Value	

B.4.4 General::TCP Check

The General::TCP Check probe verifies your TCP server can connect to a system via the specified port number. It collects the following metric:

- Remote Service Latency — The time it takes in seconds for the TCP server to answer a connection request.

The probe passes the string specified in the *Send* field when connecting. The probe anticipates a response from the system, which should include the substring specified in the *Expect* field. If the expected string is not found, the probe returns a CRITICAL status.

Table B.12   *General::TCP Check settings*

Field	Value
Send	
Expect	
Port*	1

Field	Value
Timeout*	10
Critical Maximum Latency	
Warning Maximum Latency	

B.4.5 General::UDP Check

The General::UDP Check probe tests your UDP server by verifying that it can connect to a system via the specified port number. It collects the following metric:

- Remote Service Latency — The time in seconds the UDP server takes to answer a connection request.

The probe passes the string specified in the *Send* field when connecting. The probe anticipates a response from the system, which should include the substring specified in the *Expect* field. If the expected string is not found, the probe returns a CRITICAL status.

This probe's transport protocol is User Datagram Protocol (UDP).

Table B.13   *General::UDP Check settings*

Field	Value
Port*	1
Send	
Expect	
Timeout*	10
Critical Maximum Latency	
Warning Maximum Latency	

B.4.6 General::Uptime (SNMP)

The General::Uptime (SNMP) probe records the time since the device was last started. It uses the SNMP object identifier (OID) to obtain this value. The only error status it will return is UNKNOWN.

Requirements — SNMP must be running on the monitored system and access to the OID must be enabled to run this probe.

This probe's transport protocol is User Datagram Protocol (UDP).

Table B.14 *General::Uptime (SNMP) settings*

Field	Value
SNMP Community String*	public
SNMP Port*	161
SNMP Version*	2
Timeout*	15

B.5 Linux

The probes in this section monitor essential aspects of your Linux systems, from CPU usage to virtual memory. Apply them to mission-critical systems to receive warnings before systems might fail.

Unlike other probe groups, which may or may not require the SUSE Manager monitoring daemon, every Linux probe requires the `rhnmd` daemon to be running on the monitored system.

B.5.1 Linux::CPU Usage

The Linux::CPU Usage probe monitors the CPU utilization on a system and collects the following metric:

- CPU Percent Used — The five-second average of the percentage of CPU used at probe execution.

Requirements — The SUSE Manager monitoring daemon must be running on the monitored system to run this probe.

Table B.15 *Linux::CPU Usage settings*

Field	Value
Timeout*	15
Critical Maximum CPU Percent Used	
Warning Maximum CPU Percent Used	

B.5.2 Linux::Disk IO Throughput

The Linux::Disk IO Throughput probe monitors a given disk and collects the following metrics:

- Read Rate — Kilobytes read per second.

- Write Rate — Kilobytes written per second.

To obtain the value for the required *Disk number or disk name* field, run iostat on the system to be monitored and see what name has been assigned to the disk you want to keep tabs on. The default value of 0 usually refers to the first hard drive connected to the system.

Requirements — The SUSE Manager monitoring daemon (rhnmd) must be running on the monitored system to execute this probe. Also, the *Disk number or disk name* parameter must match the format of the iostat command. If the format is not identical, the configured probe enters an UNKNOWN state.

Table B.16   *Linux::Disk IO Throughput settings*

Field	Value
Disk number or disk name*	0
Timeout*	15
Critical Maximum KB read/second	
Warning Maximum KB read/second	
Warning Minimum KB read/second	
Critical Minimum KB read/second	
Critical Maximum KB written/second	
Warning Maximum KB written/second	
Warning Minimum KB written/second	
Critical Minimum KB written/second	

B.5.3 Linux::Disk Usage

The Linux::Disk Usage probe monitors the disk space on a specific file system and collects the following metrics:

- File System Used — The percentage of the file system currently in use.

- Space Used — The currently used file system size in megabytes.

- Space Available — The size of the currently available file system in megabytes.

Requirements — The SUSE Manager monitoring daemon (`rhnmd`) must be running on the monitored system to execute this probe.

Table B.17 *Linux::Disk Usage settings*

Field	Value
File system*	/dev/hda1
Timeout*	15
Critical Maximum File System Percent Used	
Warning Maximum File System Percent Used	
Critical Maximum Space Used	
Warning Maximum Space Used	
Warning Minimum Space Available	
Critical Minimum Space Available	

B.5.4 Linux::Inodes

The Linux::Inodes probe monitors the specified file system and collects the following metric:

• Inodes — The percentage of inodes currently in use.

An inode holds meta data (like ownership and permissions) about a file or folder in a Linux file system. There is an inode for each file, each inode is identified by a number.

Requirements — The SUSE Manager monitoring daemon (rhnmd) must be running on the monitored system to execute this probe.

Table B.18   *Linux::Inodes settings*

Field	Value
File system*	/
Timeout*	15
Critical Maximum Inodes Percent Used	
Warning Maximum Inodes Percent Used	

B.5.5 Linux::Interface Traffic

The Linux::Interface Traffic probe measures the amount of traffic into and out of the specified interface (such as eth0) and collects the following metrics:

- Input Rate — The traffic in bytes per second going into the specified interface.

- Output Rate — The traffic in bytes per second coming out of the specified interface.

Requirements — The SUSE Manager monitoring daemon must be running on the monitored system to execute this probe.

Table B.19   *Linux::Interface Traffic settings*

Field	Value
Interface*	
Timeout*	30
Critical Maximum Input Rate	
Warning Maximum Input Rate	
Warning Minimum Input Rate	

Field	Value
Critical Minimum Input Rate	
Critical Maximum Output Rate	
Warning Maximum Output Rate	
Warning Minimum Output Rate	
Critical Minimum Output Rate	

B.5.6 Linux::Load

The Linux::Load probe monitors the CPU of a system and collects the following metric:

• Load — The average load on the system CPU over various periods.

Requirements — The SUSE Manager monitoring daemon must be running on the monitored system to execute this probe.

Table B.20 *Linux::Load settings*

Field	Value
Timeout*	15
Critical CPU Load 1-minute average	
Warning CPU Load 1-minute average	
Critical CPU Load 5-minute average	
Warning CPU Load 5-minute average	
Critical CPU Load 15-minute average	
Warning CPU Load 15-minute average	

B.5.7 Linux::Memory Usage

The Linux::Memory Usage probe monitors the memory on a system and collects the following metric:

- RAM Free — The amount of free random access memory (RAM) in megabytes on a system.

You can also include the reclaimable memory in this metric by entering `yes` or `no` in the *Include reclaimable memory* field.

Requirements — The SUSE Manager monitoring daemon must be running on the monitored system to execute this probe.

Table B.21 *Linux::Memory Usage settings*

Field	Value
Include reclaimable memory	no
Timeout*	15
Warning Maximum RAM Free	
Critical Maximum RAM Free	

B.5.8 Linux::Process Counts by State

The Linux::Process Counts by State probe identifies the number of processes in the following states:

- Blocked — A process that has been switched to the waiting queue and whose state has been set to `waiting`.

- Defunct — A process that has terminated (either because it has been killed by a signal or because it has called `exit()`) and whose parent process has not yet received notification of its termination by executing some form of the `wait()` system call.

- Stopped — A process that has been stopped before its execution was completed.

- Sleeping — A process that is in the `Interruptible` sleep state and can later resume execution where it left off.

Requirements — The SUSE Manager monitoring daemon (`rhnmd`) must be running on the monitored system to execute this probe.

Table B.22   *Linux::Process Counts by State settings*

Field	Value
Timeout*	15
Critical Maximum Blocked Processes	
Warning Maximum Blocked Processes	
Critical Maximum Defunct Processes	
Warning Maximum Defunct Processes	
Critical Maximum Stopped Processes	
Warning Maximum Stopped Processes	
Critical Maximum Sleeping Processes	
Warning Maximum Sleeping Processes	
Critical Maximum Child Processes	
Warning Maximum Child Processes	

B.5.9 Linux::Process Count Total

The Linux::Process Count Total probe monitors a system and collects the following metric:

- Process Count — The total number of processes currently running on the system.

Requirements — The SUSE Manager monitoring daemon must be running on the monitored system to execute this probe.

Table B.23 *Linux::Process Count Total settings*

Field	Value
Timeout*	15
Critical Maximum Process Count	
Warning Maximum Process Count	

B.5.10 Linux::Process Health

The Linux::Process Health probe monitors user-specified processes and collects the following metrics:

- CPU Usage — The CPU usage rate for a given process in milliseconds per second. This metric reports the `time` column of `ps` output, which is the cumulative CPU time used by the process. This makes the metric independent of probe interval, allows sane thresholds to be set, and generates usable graphs (i.e. a sudden spike in CPU usage shows up as a spike in the graph).

- Child Process Groups — The number of child processes spawned from the specified parent process. A child process inherits most of its attributes, such as open files, from its parent.

- Threads — The number of running threads for a given process. A thread is the smallest unit of CPU utilization, and consists of a program counter, a register set, and a stack space. A thread is also called a lightweight process.

- Physical Memory Used — The amount of physical memory (or RAM) in kilobytes used by the specified process.

- Virtual Memory Used — The amount of virtual memory in kilobytes used by the specified process, or the size of the process in real memory plus swap.

Specify the process by its command name or process ID (PID). Entering a PID overrides the entry of a command name. If no command name or PID is entered, the error `Command not found` is displayed and the probe will be set to a CRITICAL state.

Requirements — The SUSE Manager monitoring daemon (`rhnmd`) must be running on the monitored system to execute this probe.

Table B.24 *Linux::Process Health settings*

Field	Value
Command Name	
Process ID (PID) file	
Timeout*	15
Critical Maximum CPU Usage	
Warning Maximum CPU Usage	
Critical Maximum Child Process Groups	
Warning Maximum Child Process Groups	
Critical Maximum Threads	
Warning Maximum Threads	
Critical Maximum Physical Memory Used	
Warning Maximum Physical Memory Used	
Critical Maximum Virtual Memory Used	

Field	Value
Warning Maximum Virtual Memory Used	

B.5.11 Linux::Process Running

The Linux::Process running probe verifies that the specified process is functioning properly. It counts either processes or process groups, depending on whether the *Count process groups* checkbox is selected.

By default, the checkbox is selected, thereby indicating that the probe should count the number of process group leaders independent of the number of children. This allows you, for example, to verify that two instances of the Apache Web server are running regardless of the (dynamic) number of child processes. If it is not selected, the probe conducts a straightforward count of the number of processes (children and leaders) matching the specified process.

Specify the process by its command name or process ID. (PID). Entering a PID overrides the entry of a command name. If no command name or PID is entered, the error `Command not found` is displayed and the probe enters a CRITICAL state.

Requirements — The SUSE Manager monitoring daemon (`rhnmd`) must be running on the monitored system to execute this probe.

Table B.25   *Linux::Process Running settings*

Field	Value
Command name	
PID file	
Count process groups	(checked)
Timeout*	15
Critical Maximum Number Running	

Field	Value
Critical Minimum Number Running	

B.5.12 Linux::Swap Usage

The Linux::Swap Usage probe monitors the swap partitions used on a system and reports the following metric:

• Swap Free — The percentage of swap memory that is currently free.

Requirements — The SUSE Manager monitoring daemon (`rhnmd`) must be running on the monitored system to execute this probe.

Table B.26 *Linux::Swap Usage settings*

Field	Value
Timeout*	15
Warning Minimum Swap Free	
Critical Minimum Swap Free	

B.5.13 Linux::TCP Connections by State

The Linux::TCP Connections by State probe counts the total number of TCP connections and the number of connections in the following states:

• TIME_WAIT — The socket is waiting after close for remote shutdown transmission. It may handle packets still in the network.

• CLOSE_WAIT — The remote side has been shut down and is now waiting for the socket to close.

• FIN_WAIT — The socket is closed, and the connection is now shutting down.

• ESTABLISHED — The socket has a connection established.

- SYN_RCVD — The connection request has been received from the network.

This probe can help to find and isolate network traffic to specific IP addresses or to examine network connections into the monitored system.

Filter parameters allow you to narrow the probe's scope. This probe uses the netstat -ant command to retrieve data. The *Local IP address* and *Local port* parameters use values in the *Local Address* column of the output; the *Remote IP address* and *Remote port* parameters use values in the *Foreign Address* column of the output for reporting.

Requirements — The SUSE Manager monitoring daemon (rhnmd) must be running on the monitored system to execute this probe.

Table B.27   *Linux::TCP Connections by State settings*

Field	Value
Local IP address filter pattern list	
Local port number filter	
Remote IP address filter pattern list	
Remote port number filter	
Timeout*	15
Critical Maximum Total Connections	
Warning Maximum Total Connections	
Critical Maximum TIME_WAIT Connections	
Warning Maximum TIME_WAIT Connections	
Critical Maximum CLOSE_WAIT Connections	

Field	Value
Warning Maximum CLOSE_WAIT Connections	
Critical Maximum FIN_WAIT Connections	
Warning Maximum FIN_WAIT Connections	
Critical Maximum ESTABLISHED Connections	
Warning Maximum ESTABLISHED Connections	
Critical Maximum SYN_RCVD Connections	
Warning Maximum SYN_RCVD Connections	

B.5.14 Linux::Users

The Linux::Users probe counts users logged in to a system and reports the following metric:

• Users — The number of users currently logged in.

Requirements — The SUSE Manager monitoring daemon (rhnmd) must be running on the monitored system to execute this probe.

Table B.28   *Linux::Users settings*

Field	Value
Timeout*	15

Field	Value
Critical Maximum Users	
Warning Maximum Users	

B.5.15 Linux::Virtual Memory

The Linux::Virtual Memory probe monitors the total system memory and collects the following metric:

• Virtual Memory — The percentage of total free system memory - random access memory (RAM) plus swap.

Requirements — The SUSE Manager monitoring daemon (rhnmd) must be running on the monitored system to execute this probe.

Table B.29   *Linux::Virtual Memory settings*

Field	Value
Timeout*	15
Warning Minimum Virtual Memory Free	
Critical Minimum Virtual Memory Free	

B.6 LogAgent

The probes in this section monitor the log files on your systems. You can use them to query logs for certain expressions and track the sizes of files. For LogAgent probes to run, the nocpulse user must be granted read access to your log files.

Note that data from the first run of these probes is not measured against the thresholds to prevent spurious notifications caused by incomplete metric data. Measurements will begin on the second run.

B.6.1 LogAgent::Log Pattern Match

The LogAgent::Log Pattern Match probe uses regular expressions to match text located within the monitored log files and collects the following metrics:

• Regular Expression Matches — The number of matches that have occurred since the probe last ran.

• Regular Expression Match Rate — The number of matches per minute since the probe last ran.

Requirements — The SUSE Manager monitoring daemon (`rhnmd`) must be running on the monitored system to execute this probe. For this probe to run, the `nocpulse` user must be granted read access to your log files.

In addition to the name and location of the log file to be monitored, you must provide a regular expression to be matched against. The expression must be formatted for `egrep`, which is equivalent to `grep-E` and supports extended regular expressions. This is the regular expression set for `egrep`:

```
^ beginning of line
$ end of line
. match one char
* match zero or more chars
[] match one character set, e.g. '[Ff]oo'
[^] match not in set '[^A-F]oo'
+ match one or more of preceding chars
? match zero or one of preceding chars
| or, e.g. a|b
() groups chars, e.g., (foo|bar) or (foo)+
```

WARNING

Do not include single quotation marks (`'`) in the expression. Doing so causes `egrep` to fail silently and the probe to time out.

Table B.30   *LogAgent::Log Pattern Match settings*

Field	Value
Log file*	/var/log/messages
Basic regular expression*	
Timeout*	45
Critical Maximum Matches	
Warning Maximum Matches	
Warning Minimum Matches	
Critical Minimum Matches	
Critical Maximum Match Rate	
Warning Maximum Match Rate	
Warning Minimum Match Rate	
Critical Minimum Match Rate	

B.6.2 LogAgent::Log Size

The LogAgent::Log Size probe monitors log file growth and collects the following metrics:

- Size — The size increase of the log file in bytes since the probe last ran.

- Output Rate — The number of bytes per minute the log file has grown since the probe last ran.

- Lines — The number of lines written to the log file since the probe last ran.

- Line Rate — The number of lines written per minute to the log file since the probe last ran.

Requirements — The SUSE Manager monitoring daemon (rhnmd) must be running on the monitored system to execute this probe. For this probe to run, the nocpulse user must be granted read access to your log files.

Table B.31   *LogAgent::Log Size settings*

Field	Value
Log file*	/var/log/messages
Timeout*	20
Critical Maximum Size	
Warning Maximum Size	
Warning Minimum Size	
Critical Minimum Size	
Critical Maximum Output Rate	
Warning Maximum Output Rate	
Warning Minimum Output Rate	
Critical Minimum Output Rate	
Critical Maximum Lines	
Warning Maximum Lines	
Warning Minimum Lines	
Critical Minimum Lines	
Critical Maximum Line Rate	

Field	Value
Warning Maximum Line Rate	
Warning Minimum Line Rate	
Critical Minimum Line Rate	

B.7 MySQL 3.23 - 3.33

The probes in this section monitor aspects of the MySQL database using the `mysqladmin` binary. No special user privileges are needed for these probes.

Note that the `mysql-server` package must be installed on the system conducting the monitoring for these probes to complete. Refer to the MySQL Installation section of the *SUSE Manager Installation Guide* for instructions.

B.7.1 MySQL::Database Accessibility

The MySQL::Database Accessibility probe tests connectivity through a database account that has no database privileges. If no connection is made, a CRITICAL status results.

Table B.32   *MySQL::Database Accessibility settings*

Field	Value
Username*	
Password	
MySQL Port	3306
Database*	mysql
Timeout	15

B.7.2 MySQL::Opened Tables

The MySQL::Opened Tables probe monitors the MySQL server and collects the following metric:

- Opened Tables — The tables opened since the server was started.

Table B.33   *MySQL::Opened Tables settings*

Field	Value
Username	
Password	
MySQL Port*	3306
Timeout	15
Critical Maximum Opened Objects	
Warning Maximum Opened Objects	
Warning Minimum Opened Objects	
Critical Minimum Opened Objects	

B.7.3 MySQL::Open Tables

The MySQL::Open Tables probe monitors the MySQL server and collects the following metric:

- Open Tables — The number of tables open when the probe runs.

Table B.34   *MySQL::Open Tables settings*

Field	Value
Username	

Field	Value
Password	
MySQL Port*	3306
Timeout	15
Critical Maximum Open Objects	
Warning Maximum Open Objects	
Warning Minimum Open Objects	
Critical Minimum Open Objects	

B.7.4 MySQL::Query Rate

The MySQL::Query Rate probe monitors the MySQL server and collects the following metric:

- Query Rate — The average number of queries per second per database server.

Table B.35 *MySQL::Query Rate settings*

Field	Value
Username	
Password	
MySQL Port*	3306
Timeout	15
Critical Maximum Query Rate	
Warning Maximum Query Rate	

Field	Value
Warning Minimum Query Rate	
Critical Minimum Query Rate	

B.7.5 MySQL::Threads Running

The MySQL::Threads Running probe monitors the MySQL server and collects the following metric:

• Threads Running — The total number of running threads within the database.

Table B.36   *MySQL::Threads Running settings*

Field	Value
Username	
Password	
MySQL Port*	3306
Timeout	15
Critical Maximum Threads Running	
Warning Maximum Threads Running	
Warning Minimum Threads Running	
Critical Minimum Threads Running	

B.8 Network Services

The probes in this section monitor various services integral to a functioning network. When applying them, ensure that their timed thresholds do not exceed the amount of

time allotted to the timeout period. Otherwise, an UNKNOWN status is returned in all instances of extended latency, thereby nullifying the thresholds.

B.8.1 Network Services::DNS Lookup

The Network Services::DNS Lookup probe uses the `dig` command to see if it can re-solve the system or domain name specified in the *Host or Address to look up* field. It collects the following metric:

- Query Time — The time in milliseconds required to execute the `dig` request.

Use this probe to monitor the status of your DNS servers. Supply a well-known host/domain name, such as a large search engine or corporate Web site.

Table B.37 *Network Services::DNS Lookup settings*

Field	Value
Host or Address to look up	
Timeout*	10
Critical Maximum Query Time	
Warning Maximum Query Time	

B.8.2 Network Services::FTP

The Network Services::FTP probe uses network sockets to test FTP port availability. It collects the following metric:

- Remote Service Latency — The time in seconds the FTP server takes to answer a connection request.

This probe supports authentication. Provide a username and password in the appropriate fields to use this feature. The optional *Expect* value is the string to be matched against after a successfully connecting to the FTP server. If the expected string is not found, the probe returns a CRITICAL state.

Table B.38 *Network Services::FTP settings*

Field	Value
Expect	FTP
Username	
Password	
FTP Port*	21
Timeout*	10
Critical Maximum Remote Service Latency	
Warning Maximum Remote Service Latency	

B.8.3 Network Services::IMAP Mail

The Network Services::IMAP Mail probe checks if it can connect to the IMAP 4 service on the monitored system. Specifying an optional port will override the default port 143. It collects the following metric:

• Remote Service Latency — The time it takes in seconds for the IMAP server to answer a connection request.

The required *Expect* value is the string to be matched against after a successfully connecting to the IMAP server. If the expected string is not found, the probe returns a CRITICAL state.

Table B.39 *Network Services::IMAP Mail settings*

Field	Value
IMAP Port*	143

Field	Value
Expect*	OK
Timeout*	5
Critical Maximum Remote Service Latency	
Warning Maximum Remote Service Latency	

B.8.4 Network Services::Mail Transfer (SMTP)

The Network Services::Mail Transfer (SMTP) probe checks if it can connect to the SMTP port on the monitored system. Specifying an optional port number overrides the default port 25. It collects the following metric:

- Remote Service Latency — The time it takes in seconds for the SMTP server to answer a connection request.

Table B.40   *Network Services::Mail Transfer (SMTP) settings*

Field	Value
SMTP Port*	25
Timeout*	10
Critical Maximum Remote Service Latency	
Warning Maximum Remote Service Latency	

B.8.5 Network Services::Ping

The Network Services::Ping probe determines if the SUSE Manager server can `ping` the monitored system or a specified IP address. It also checks the packet loss and compares the round trip average against the Warning and Critical threshold levels. The required *Packets to send* value allows you to control how many ICMP ECHO packets are sent to the system. This probe collects the following metrics:

- Round-Trip Average — The time it takes in milliseconds for the ICMP ECHO packet to travel to and from the monitored system.

- Packet Loss — The percentage of data lost in transit.

The *IP Address* field is essential when collecting metrics for systems that have multiple IP addresses. For instance, if the system is configured with multiple virtual IP addresses or uses Network Address Translation (NAT) to support internal and external IP addresses, this option may be used to check a secondary IP address rather than the primary address associated with the hostname.

Note that this probe conducts the `ping` from a SUSE Manager server and not the monitored system. Populating the IP address field does not test connectivity between the system and the specified IP address but between the SUSE Manager server and the IP address. Therefore, entering the same IP address for Ping probes on different systems accomplishes precisely the same task. To conduct a `ping` from a monitored system to an individual IP address, use the Remote Ping probe instead. Refer to Section B.8.7, "Network Services::Remote Ping" (page 294).

Table B.41   *Network Services::Ping settings*

Field	Value
IP Address (defaults to system IP)	
Packets to send*	20
Timeout*	10
Critical Maximum Round-Trip Average	

Field	Value
Warning Maximum Round-Trip Average	
Critical Maximum Packet Loss	
Warning Maximum Packet Loss	

B.8.6 Network Services::POP Mail

The Network Services::POP Mail probe determines if it can connect to the POP3 port on the system. A port number must be specified; specifying another port number overrides the default port 110. This probe collects the following metric:

- Remote Service Latency — The time in seconds it takes the POP server to answer a connection request.

The required *Expect* value is the string to be matched against after a successful connection is made to the POP server. The probe looks for the string in the first line of the response from the system. The default is +OK. If the expected string is not found, the probe returns a CRITICAL state.

Table B.42 *Network Services::POP Mail settings*

Field	Value
Port*	110
Expect*	+OK
Timeout*	10
Critical Maximum Remote Service Latency	
Warning Maximum Remote Service Latency	

B.8.7 Network Services::Remote Ping

The Network Services::Remote Ping probe determines if the monitored system can `ping` a specified IP address. It also monitors the packet loss and compares the round trip average against the Warning and Critical threshold levels. The required *Packets to send* value allows you to control how many ICMP ECHO packets are sent to the address. This probe collects the following metrics:

- Round-Trip Average — The time it takes in milliseconds for the ICMP ECHO packet to travel to and from the IP address.

- Packet Loss — The percentage of data lost in transit.

The *IP Address* field identifies the precise address to be pinged. Unlike with the standard ping probe, this field is required for remote ping. The monitored system directs the ping at the specified IP address rather than at the SUSE Manager server. To conduct pings from the SUSE Manager server to a system or IP address, use the standard Ping probe instead. Refer to Section B.8.5, "Network Services::Ping" (page 292).

Requirements — The SUSE Manager monitoring daemon (`rhnmd`) must be running on the monitored system to execute this probe.

Table B.43   *Network Services::Remote Ping settings*

Field	Value
IP Address*	
Packets to send*	20
Timeout*	10
Critical Maximum Round-Trip Average	
Warning Maximum Round-Trip Average	
Critical Maximum Packet Loss	

Field	Value
Warning Maximum Packet Loss	

B.8.8 Network Services::RPCService

The Network Services::RPCService probe tests the availability of remote procedure call (RPC) programs on a given IP address. It collects the following metric:

- Remote Service Latency — The time in seconds the RPC server takes to answer a connection request.

RPC server programs, which provide function calls via a RPC network, register themselves with the RPC network by declaring a program ID and a program name. NFS is an example of a service that works via the RPC mechanism.

Client programs that wish to use the resources of RPC server programs do so by asking the machine on which the server program resides to provide access to RPC functions within the RPC program number or program name. These conversations can occur over either TCP or UDP (but are almost always UDP).

This probe allows you to test simple program availability. You must specify the program name or number, the protocol over which the conversation occurs, and the usual timeout period.

Table B.44 *Network Services::RPCService settings*

Field	Value
Protocol (TCP/UDP)	udp
Service Name*	nfs
Timeout*	10
Critical Maximum Remote Service Latency	

Field	Value
Warning Maximum Remote Service Latency	

B.8.9 Network Services::Secure Web Server (HTTPS)

The Network Services::Secure Web Server (HTTPS) probe determines the availability of the secure Web server and collects the following metric:

• Remote Service Latency — The time it takes in seconds for the HTTPS server to answer a connection request.

This probe checks if it can connect to the HTTPS port on the specified host and retrieve the specified URL. If no URL is specified, the probe fetches the root document. The probe looks for a HTTP/1 message from the system unless you alter that value. Specifying another port number overrides the default port of 443.

This probe supports authentication. Provide a username and password in the appropriate fields to use this feature. Unlike most other probes, this probe returns a CRITICAL status if it cannot contact the system within the timeout period.

Table B.45 *Network Services::Secure Web Server (HTTPS) settings*

Field	Value
URL Path	/
Expect Header	HTTP/1
Expect Content	
UserAgent*	NOCpulse-check_http/1.0
Username	

Field	Value
Password	
Timeout*	10
HTTPS Port*	443
Critical Maximum Remote Service Latency	
Warning Maximum Remote Service Latency	

B.8.10 Network Services::SSH

The Network Services::SSH probe determines the availability of SSH on the specified port and collects the following metric:

- Remote Service Latency — The time it takes in seconds for the SSH server to answer a connection request.

After successfully contacting the SSH server and receiving a valid response, the probe displays the protocol and server version information. If the probe receives an invalid response, it displays the message returned from the server and generates a WARNING state.

Table B.46   *Network Services::SSH settings*

Field	Value
SSH Port*	22
Timeout*	5
Critical Maximum Remote Service Latency	

Field	Value
Warning Maximum Remote Service Latency	

B.8.11 Network Services::Web Server (HTTP)

The Network Services::Web Server (HTTP) probe determines the availability of the Web server and collects the following metric:

• Remote Service Latency — The time it takes in seconds for the HTTP server to answer a connection request.

This probe check if it can connect to the HTTP port on the specified host and retrieve the specified URL. If no URL is specified, the probe will fetch the root document. The probe looks for a HTTP/1. message from the system, unless you alter that value. Specifying another port number will override the default port of 80. Unlike most other probes, this probe will return a CRITICAL status if it cannot contact the system within the timeout period.

This probe supports authentication. Provide a username and password in the appropriate fields to use this feature. Also, the optional Virtual Host field can be used to monitor a separate documentation set located on the same physical machine presented as a standalone server. If your Web server is not configured to use virtual hosts (which is typically the case), you should leave this field blank. If you do have virtual hosts configured, enter the domain name of the first host here. Add as many probes as necessary to monitor all virtual hosts on the machine.

Table B.47 *Network Services::Web Server (HTTP) settings*

Field	Value
URL Path	/
Virtual Host	
Expect Header	HTTP/1

Field	Value
Expect Content	
UserAgent*	NOCpulse-check_http/1.0
Username	
Password	
Timeout*	10
HTTP Port*	80
Critical Maximum Remote Service Latency	
Warning Maximum Remote Service Latency	

B.9 Oracle 8i, 9i, 10g, and 11g

The probes in this section may be applied to instances of the Oracle database matching the versions supported. Oracle probes require the configuration of the database and associations made by running the following command:

```
$ORACLE_HOME/rdbms/admin/catalog.sql
```

In addition, for these probes to function properly, the Oracle user configured in the probe must have minimum privileges of CONNECT and SELECT_CATALOG_ROLE.

Some Oracle probes are specifically aimed at tuning devices for long-term performance gains, rather than avoiding outages. Therefore, it is recommended to schedule them to occur less frequently, between every hour and every two days. Longer intervals provide a better statistical representation. Anomalies can easily be recognized as such. This applies to the following probes: Buffer Cache, Data Dictionary Cache, Disk Sort Ratio, Library Cache, and Redo Log.

The values for CRITICAL and WARNING thresholds based on time cannot exceed the amount of time allotted to the timeout period. Otherwise, an UNKNOWN status is returned in all cases of extended latency, thereby nullifying the thresholds. For this reason, ensure that timeout periods exceed all timed thresholds. This applies specifically to the probe TNS Ping.

Finally, customers using these Oracle probes against a database using Oracle's Multi-Threaded Server (MTS) must add respective entries to the SUSE Manager server's `/etc/hosts` file to ensure that the DNS name is resolved correctly.

B.9.1 Oracle::Active Sessions

The Oracle::Active Sessions probe monitors an Oracle instance and collects the following metrics:

- Active Sessions — The number of active sessions based on the value of `V$PARAMETER.PROCESSES`.

- Available Sessions — The percentage of active sessions that are available based on the value of `V$PARAMETER.PROCESSES`.

Table B.48   *Oracle::Active Sessions settings*

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout*	30
Critical Maximum Active Sessions	
Warning Maximum Active Sessions	

Field	Value
Critical Maximum Available Sessions Used	
Warning Maximum Available Sessions Used	

B.9.2 Oracle::Availability

The Oracle::Availability probe determines the availability of the database from SUSE Manager.

Table B.49   Oracle::Availability settings

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout*	30

B.9.3 Oracle::Blocking Sessions

The Oracle::Blocking Sessions probe monitors an Oracle instance and collects the following metric:

• Blocking Sessions — The number of sessions preventing other sessions from committing changes to the Oracle database, as determined by the required *Time Blocking* value you provide. Only those sessions that have been blocking for this duration, which is measured in seconds, are counted as blocking sessions.

Table B.50 *Oracle::Blocking Sessions settings*

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Time Blocking (seconds)*	20
Timeout*	30
Critical Maximum Blocking Sessions	
Warning Maximum Blocking Sessions	

B.9.4 Oracle::Buffer Cache

The Oracle::Buffer Cache probe computes the Buffer Cache Hit Ratio to optimize the system global area (SGA) Database Buffer Cache size. It collects the following metrics:

- Db Block Gets — The number of blocks accessed via single block gets (not through the consistent get mechanism).

- Consistent Gets — The number of accesses made to the block buffer to retrieve data in a consistent mode.

- Physical Reads — The cumulative number of blocks read from disk.

- Buffer Cache Hit Ratio — The rate at which the database goes to the buffer instead of the hard disk to retrieve data. A low ratio suggests more RAM should be added to the system.

Table B.51   *Oracle::Buffer Cache settings*

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port	1521
Timeout*	30
Warning Minimum Buffer Cache Hit Ratio	
Critical Minimum Buffer Cache Hit Ratio	

B.9.5 Oracle::Client Connectivity

The Oracle::Client Connectivity probe determines if the database is up and capable of receiving connections from the monitored system. This probe opens an rhnmd connection to the system and issues a sqlplus connect command on the monitored system.

The *Expected DB name* parameter is the expected value of V$DATABASE.NAME. This value is case-insensitive. A CRITICAL status is returned if this value is not found.

Requirements — The SUSE Manager monitoring daemon (rhnmd) must be running on the monitored system to execute this probe. For this probe to run, the nocpulse user must be granted read access to your log files.

Table B.52   *Oracle::Client Connectivity settings*

Field	Value
Oracle Hostname or IP address*	

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
ORACLE_HOME*	/opt/oracle
Expected DB Name*	
Timeout*	30

B.9.6 Oracle::Data Dictionary Cache

The Oracle::Data Dictionary Cache probe computes the Data Dictionary Cache Hit Ratio to optimize the SHARED_POOL_SIZE in init.ora. It collects the following metrics:

- Data Dictionary Hit Ratio — The ratio of cache hits to cache lookup attempts in the data dictionary cache. In other words, the rate at which the database goes to the dictionary instead of the hard disk to retrieve data. A low ratio suggests more RAM should be added to the system.

- Gets — The number of blocks accessed via single block gets (not through the consistent get mechanism).

- Cache Misses — The number of accesses made to the block buffer to retrieve data in a consistent mode.

Table B.53   *Oracle::Data Dictionary Cache settings*

Field	Value
Oracle SID*	

Field	Value
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout*	30
Warning Minimum Data Dictionary Hit Ratio	
Critical Minimum Data Dictionary Hit Ratio	

B.9.7 Oracle::Disk Sort Ratio

The Oracle::Disk Sort Ratio probe monitors an Oracle database instance and collects the following metric:

• Disk Sort Ratio — The rate of Oracle sorts that were too large to be completed in memory and were instead sorted using a temporary segment.

Table B.54 *Oracle::Disk Sort Ratio settings*

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout*	30

Field	Value
Critical Maximum Disk Sort Ratio	
Warning Maximum Disk Sort Ratio	

B.9.8 Oracle::Idle Sessions

The Oracle::Idle Sessions probe monitors an Oracle instance and collects the following metric:

• Idle Sessions — The number of Oracle sessions that are idle, as determined by the required *Time Idle* value you provide. Only those sessions that have been idle for this duration, which is measured in seconds, are counted as idle sessions.

Table B.55   *Oracle::Idle Sessions settings*

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Time Idle (seconds)*	20
Timeout*	30
Critical Maximum Idle Sessions	
Warning Maximum Idle Sessions	

B.9.9 Oracle::Index Extents

The Oracle::Index Extents probe monitors an Oracle instance and collects the following metrics:

- Allocated Extents — The number of allocated extents for any index.

- Available Extents — The percentage of available extents for any index.

The required *Index Name* field contains a default value of % that matches any index name.

Table B.56 *Oracle::Index Extents settings*

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Index Owner*	%
Index Name*	%
Timeout*	30
Critical Maximum of Allocated Extents	
Warning Maximum of Allocated Extents	
Critical Maximum of Available Extents	
Warning Maximum of Available Extents	

B.9.10 Oracle::Library Cache

The Oracle::Library Cache probe computes the Library Cache Miss Ratio to optimize the SHARED_POOL_SIZE in `init.ora`. It collects the following metrics:

- Library Cache Miss Ratio — The rate at which a library cache pin miss occurs. This happens when a session executes a statement that it has already parsed but finds that the statement is no longer in the shared pool.

- Executions — The number of times a pin was requested for objects of this namespace.

- Cache Misses — The number of pins of objects with previous pins since the object handle was created that must now retrieve the object from disk.

Table B.57   *Oracle::Library Cache settings*

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout*	30
Critical Maximum Library Cache Miss Ratio	
Warning Maximum Library Cache Miss Ratio	

B.9.11 Oracle::Locks

The Oracle::Locks probe monitors an Oracle database instance and collects the following metric:

- Active Locks — The current number of active locks as determined by the value in the v$locks table. Database administrators should be aware of high numbers of locks present in a database instance.

Locks are used so that multiple users or processes updating the same data in the database do not conflict. This probe is useful for alerting database administrators when a high number of locks are present in a given instance.

Table B.58 *Oracle::Locks settings*

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout*	30
Critical Maximum Active Locks	
Warning Maximum Active Locks	

B.9.12 Oracle::Redo Log

The Oracle::Redo Log probe monitors an Oracle database instance and collects the following metrics:

- Redo Log Space Request Rate — The average number of redo log space requests per minute since the server has been started.

- Redo Buffer Allocation Retry Rate — The average number of buffer allocation retries per minute since the server was started.

The metrics returned and the thresholds they are measured against are numbers representing the rate of change in events per minute. The rate of change for these metrics should be monitored because fast growth can indicate problems requiring investigation.

Table B.59 *Oracle::Redo Log settings*

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout*	30
Critical Maximum Redo Log Space Request Rate	
Warning Maximum Redo Log Space Request Rate	
Critical Maximum Redo Buffer Allocation Retry Rate	
Warning Maximum Redo Buffer Allocation Retry Rate	

B.9.13 Oracle::Table Extents

The Oracle::Table Extents probe monitors an Oracle database instance and collects the following metrics:

• Allocated Extents-Any Table — The total number of extents for any table.

• Available Extents-Any Table — The percentage of available extents for any table.

In Oracle, table extents allow a table to grow. When a table is full, it is extended by an amount of space configured when the table is created. Extents are configured on a per-table basis, with an extent size and a maximum number of extents.

For example, a table that starts with 10 MB of space and that is configured with an extent size of 1 MB and max extents of 10 can grow to a maximum of 20 MB (by being extended by 1 MB ten times). This probe can be configured to alert by (1) the number of allocated extents (e.g. "go critical when the table has been extended 5 or more times"), or (2) the table is extended past a certain percentage of its max extents (e.g. "go critical when the table has exhausted 80% or more of its max extents").

The required *Table Owner* and *Table Name* fields contain a default value of % that matches any table owner or name.

Table B.60   *Oracle::Table Extents settings*

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Table Owner*	%
Table Name*	%
Timeout*	30
Critical Maximum Allocated Extents	
Warning Maximum Allocated Extents	
Critical Maximum Available Extents	
Warning Maximum Available Extents	

B.9.14 Oracle::Tablespace Usage

The Oracle::Tablespace Usage probe monitors an Oracle database instance and collects the following metric:

- Available Space Used — The percentage of available space in each tablespace that has been used.

Tablespace is the shared pool of space in which a set of tables live. This probe alerts the user when the total amount of available space falls below the threshold. Tablespace is measured in bytes, so extents do not factor into it directly (though each extension removes available space from the shared pool).

The required *Tablespace Name* field is case insensitive and contains a default value of % that matches any table name.

Table B.61   *Oracle::Tablespace Usage settings*

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Tablespace Name*	%
Timeout*	30
Critical Maximum Available Space Used	
Warning Maximum Available Space Used	

B.9.15 Oracle::TNS Ping

The Oracle::TNS Ping probe determines if an Oracle listener is alive and collects the following metric:

- Remote Service Latency — The time it takes in seconds for the Oracle server to answer a connection request.

Table B.62   *Oracle::TNS Ping settings*

Field	Value
TNS Listener Port*	1521
Timeout*	15
Critical Maximum Remote Service Latency	
Warning Maximum Remote Service Latency	

B.10 SUSE Manager

The probes in this section may be applied to the SUSE Manager itself to monitor its health and performance. Since these probes run locally, no specific application or transport protocols are required.

B.10.1 SUSE Manager::Disk Space

The SUSE Manager::Disk Space probe monitors the free disk space on a SUSE Manager server and collects the following metrics:

- File System Used — The percentage of the file system currently in use.

- Space Used — The size of the currently used file system.

• Space Available — The size of free space available on the file system.

Table B.63   *SUSE Manager::Disk Space settings*

Field	Value
Device Pathname*	/dev/hda1
Critical Maximum File System Used	
Warning Maximum File System Used	
Critical Maximum Space Used	
Warning Maximum Space Used	
Critical Maximum Space Available	
Warning Maximum Space Available	

B.10.2 SUSE Manager::Execution Time

The SUSE Manager::Execution Time probe monitors the execution time for probes run from a SUSE Manager and collects the following metric:

• Probe Execution Time Average — The seconds required to fully execute a probe.

Table B.64   *SUSE Manager::Execution Time settings*

Field	Value
Critical Maximum Probe Execution Time Average	
Warning Maximum Probe Execution Time Average	

B.10.3 SUSE Manager::Interface Traffic

The SUSE Manager::Interface Traffic probe monitors the interface traffic on a SUSE Manager and collects the following metrics:

- Input Rate — The amount of traffic in bytes per second the device receives.

- Output Rate — The amount of traffic in bytes per second the device sends.

Table B.65   *SUSE Manager::Interface Traffic settings*

Field	Value
Interface*	eth0
Timeout (seconds)*	30
Critical Maximum Input Rate	
Critical Maximum Output Rate	

B.10.4 SUSE Manager::Latency

The SUSE Manager::Latency probe monitors the latency of probes on SUSE Manager and collects the following metric:

- Probe Latency Average — The lag in seconds between the time a probe becomes ready to run and the time it is actually run. Under normal conditions, this is generally less than a second. When SUSE Manager is overloaded (because it has too many probes with respect to their average execution time), the number goes up.

Table B.66   *SUSE Manager::Latency settings*

Field	Value
Critical Maximum Probe Latency Average	

Field	Value
Warning Maximum Probe Latency Average	

B.10.5 SUSE Manager::Load

The SUSE Manager::Load probe monitors the CPU load on a SUSE Manager and collects the following metric:

- Load — The load average on the CPU for a 1-, 5-, and 15-minute period.

Table B.67   *SUSE Manager::Load settings*

Field	Value
Critical Maximum 1-minute Average	
Warning Maximum 1-minute Average	
Critical Maximum 5-minute Average	
Warning Maximum 5-minute Average	
Critical Maximum 15-minute Average	
Warning Maximum 15-minute Average	

B.10.6 SUSE Manager::Probe Count

The SUSE Manager::Probe Count probe monitors the number of probes on SUSE Manager and collects the following metric:

- Probes — The number of individual probes running on SUSE Manager.

Table B.68   *SUSE Manager::Probe Count settings*

Field	Value
Critical Maximum Probe Count	
Warning Maximum Probe Count	

B.10.7 SUSE Manager::Process Counts

The SUSE Manager::Process Counts probe monitors the number of processes on SUSE Manager and collects the following metrics:

- Blocked — The number of processes that have been switched to the waiting queue and waiting state.

- Child — The number of processes spawned by another process already running on the machine.

- Defunct — The number of processes that have terminated (either because they have been killed by a signal or have called `exit()`) and whose parent processes have not yet received notification of their termination by executing some form of the `wait()` system call.

- Stopped — The number of processes that have stopped before their executions could be completed.

- Sleeping — A process that is in the `Interruptible` sleep state and can later resume execution.

Table B.69   *SUSE Manager::Process Counts settings*

Field	Value
Critical Maximum Blocked Processes	
Warning Maximum Blocked Processes	
Critical Maximum Child Processes	

Field	Value
Warning Maximum Child Processes	
Critical Maximum Defunct Processes	
Warning Maximum Defunct Processes	
Critical Maximum Stopped Processes	
Warning Maximum Stopped Processes	
Critical Maximum Sleeping Processes	
Warning Maximum Sleeping Processes	

B.10.8 SUSE Manager::Processes

The SUSE Manager::Processes probe monitors the number of processes on SUSE Manager and collects the following metric:

• Processes — The number of processes running simultaneously on the machine.

Table B.70   *SUSE Manager::Processes settings*

Field	Value
Critical Maximum Processes	
Warning Maximum Processes	

B.10.9 SUSE Manager::Process Health

The SUSE Manager::Process Health probe monitors customer-specified processes and collects the following metrics:

• CPU Usage — The percentage of CPU used for a given process.

- Child Process Groups — The number of child processes spawned from the specified parent process. A child process inherits most of its attributes, such as open files, from its parent.

- Threads — The number of running threads for a given process. A thread is the basic unit of CPU utilization, and consists of a program counter, a register set, and a stack space. A thread is also called a lightweight process.

- Physical Memory Used — The amount of physical memory in kilobytes being used by the specified process.

- Virtual Memory Used — The amount of virtual memory in kilobytes being used by the specified process, or the size of the process in real memory plus swap.

Specify the process by its command name or process ID. (PID). Entering a PID overrides the entry of a command name. If no command name or PID is entered, the error `Command not found` is displayed and the probe is set to a CRITICAL state.

Table B.71   *SUSE Manager::Process Health settings*

Field	Value
Command Name	
Process ID (PID) file	
Timeout*	15
Critical Maximum CPU Usage	
Warning Maximum CPU Usage	
Critical Maximum Child Process Groups	
Warning Maximum Child Process Groups	
Critical Maximum Threads	

Field	Value
Warning Maximum Threads	
Critical Maximum Physical Memory Used	
Warning Maximum Physical Memory Used	
Critical Maximum Virtual Memory Used	
Warning Maximum Virtual Memory Used	

B.10.10 SUSE Manager::Process Running

The SUSE Manager::Process Running probe verifies that a certain process is running. Specify the process by its command name or process ID. (PID). Entering a PID overrides the entry of a command name. A Critical status results if the probe cannot verify the command or PID.

Table B.72   *SUSE Manager::Process Running settings*

Field	Value
Command Name	
Process ID (PID) file	
Critical Number Running Maximum	
Critical Number Running Minimum	

B.10.11 SUSE Manager::Swap

The SUSE Manager::Swap probe monitors the percentage of free swap space available on SUSE Manager. A CRITICAL status results if the value falls below the Critical threshold. A WARNING status results if the value falls below the Warning threshold.

Table B.73 *SUSE Manager::Swap settings*

Field	Value
Critical Minimum Swap Percent Free	
Warning Minimum Swap Percent Free	

B.10.12 SUSE Manager::Users

The SUSE Manager::Users probe monitors the number of users currently logged into SUSE Manager. A CRITICAL status results if the value exceeds the Critical threshold. A WARNING status results if the value exceeds the Warning threshold.

Table B.74 *SUSE Manager::Users settings*

Field	Value
Critical Maximum Users	
Warning Maximum Users	

Minimalist AutoYaST Profile for Automated Installations

C

The following AutoYaST profile will install a SUSE Linux Enterprise Server system with all default installation options including a default network configuration with DHCP. After the installation is completed, a bootstrap script located on the SUSE Manager server will be executed in order to register the freshly installed system with susemgr;. You need to adjust the IP address of the SUSE Manager server, the name of the bootstrap script and the `root` password according to your needs in the following lines:

```
<user>
...
 <username>root</username>
  <user_password>linux</user_password>
</user>

<location>http://192.168.1.1/pub/bootstrap/my_bootstrap.sh</location>
```

The complete AutoYaST file:

```
<?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>
   <confirm config:type="boolean">false</confirm>
  </mode>
 </general>
 <networking>
  <keep_install_network config:type="boolean">true</keep_install_network>
 </networking>
 <software>
  <install_recommended config:type="boolean">true</install_recommended>
   <patterns config:type="list">
```

```
      <pattern>base</pattern>
    </patterns>
  </software>
  <users config:type="list">
   <user>
    <encrypted config:type="boolean">false</encrypted>
    <fullname>root</fullname>
    <gid>0</gid>
    <home>/root</home>
    <password_settings>
     <expire></expire>
     <flag></flag>
     <inact></inact>
     <max></max>
     <min></min>
     <warn></warn>
    </password_settings>
    <shell>/bin/bash</shell>
    <uid>0</uid>
    <username>root</username>
    <user_password>linux</user_password>
   </user>
  </users>
  <scripts>
   <init-scripts config:type="list">
    <script>
     <interpreter>shell</interpreter>
     <location>http://192.168.1.1/pub/bootstrap/my_bootstrap.sh</location>
    </script>
   </init-scripts>
  </scripts>
</profile>
```

About SUSE Manager and Spacewalk

D

SUSE® Manager's main purpose is to efficiently manage a set of Linux systems and keep them up-to-date. You can register both SUSE® Linux Enterprise and Red Hat Enterprise Linux client systems with the SUSE Manager server.

SUSE Manager is based on the Spacewalk project, `http://spacewalk.redhat.com/`. This allows for seamless migration when switching from Red Hat Network Satellite or a Spacewalk server to SUSE Manager. Both user experience and tools are mostly unchanged, which means that you can use the known commands and the scripts that may already exist on your systems.

However, as SUSE Manager is deployed as an appliance based on SUSE Linux Enterprise, some differences exist regarding environments and tools:

Reporting and Downloading Software Packages
> Instead of connecting to Red Hat Network, SUSE Manager connects to Novell Customer Center (NCC) (`http://www.novell/center`) to receive updates and patches. NCC also provides the entitlements for enabling specific SUSE Manager functionality.

Automatic Deployment
> Automated installation on Red Hat Enterprise Linux client systems is done with Kickstart. For SUSE Linux Enterprise client systems, SUSE Manager uses Auto-YaST.

Software Management
> Is done with `yum` on Red Hat Enterprise Linux client systems. For SUSE Linux Enterprise client systems, SUSE Manager uses `zypper`.

Command Line Tools

The Spacewalk command line tools also work for SUSE Manager. Additionally, symbolic links have been added for a number of commands. For example, `rhn-profile-sync` is also available as `mgr-profile-sync.`

Package Names

Some SUSE Manager package names are different from the original Spacewalk ones.

D.1 Overview Command Line Tools

Table D.1 *Command Line Tools*

Description	Spacewalk	SUSE Manager
Client registration tool	`sm-register`	`mgr-register`
Synchronization tool	`satellite-sync`	`mgr-ncc-sync`
Channel configuration tool	`rhncfg-manager`	`mgrcfg-manager`
Client configuration tool	`rhncfg-client`	`mgrcfg-client`
SUSE Manager service tool	`rhn-satellite`	`spacewalk-service`
Package installer	~~`system-config-packages`~~	`yast sw_single`
Update packages	`up2date`	`zypper up`
Configuration actions for clients	`rhncfg-actions`	`mgrcfg-actions`
Program for identifying clients	`rhn_check`	`mgr_check`
Update system information	`rhn-profile-sync`	`mgr-profile-sync`

Description	Spacewalk	SUSE Manager
Non-interactive program for registering systems	`rhnreg_ks`	`mgrreg_ks`
XML im- and exporter between identical SUSE Manager servers	~~rhn-satellite-exporter~~	`mgr-exporter`

Glossary

Action
> A task that is scheduled by a system administrator using SUSE Manager to be performed on one or more client systems. For example, an action can be scheduled to update the kernel packages on all the systems in a selected group.

Activation Key
> SUSE Manager Management and Provisioning customers can generate activation keys through the SUSE Manager Web site. Each unique key can then be used to "activate" (register) a client system (either SLE or RHEL), entitle the system to SUSE Manager, subscribe the system to specific channels, and subscribe the system to SUSE Manager system groups through the command line utility rhnreg_ks from the bootstrap script.

Base Channel
> A base channel is a type of Channel (page 329) that consists of a list of packages for a specific architecture and SUSE release. For example, all the packages in SUSE Linux Enterprise Server 11 SP1 for the x86 architecture make a base channel.

Bug Fix Alert
> A Patch Alert (page 331) that pertains to a bug fix.

Bugzilla
> Bugzilla is an online application (http://bugzilla.novell.com) that allows users to communicate directly with the developers. In Bugzilla, users can submit bug reports and feature requests for SUSE Linux Enterprise and related open source packages.

Certificate Authority
> A Certificate Authority distributes digital signatures to users as part of a public key infrastructure for encrypted authentication and communication.

Channel
> A channel is a list of software packages. There are two types of channels: base channels and child channels. Channels are used to choose packages to be installed on client systems. Every client system must be subscribed to one Base Channel (page 329) and can be subscribed to one or more Child Channel (page 330).

Channel Administrator

A user role with full access to channel management capabilities. Users with this role can of create channels, assign packages to channels, clone and delete channels. This role can be assigned by an organization administrator through the *Users* tab of the Web interface.

Child Channel

A child channel is a Channel (page 329) associated with a Base Channel (page 329) but contains extra packages.

Client System

A system that is registered with SUSE Manager. Also known as registered system.

Digital Certificate

A client component in XML format that is stored in the `/etc/sysconfig/rhn/systemid` file on registered systems. SUSE Manager verifies this certificate to authenticate the registered system before each connection. This certificate is issued by SUSE and passed to the system as part of the registration process. It includes unique information about the registered system to avoid fraudulent use.

E-mail Notification

Similar to a Patch Alert (page 331) , except the information is delivered via e-mail. If the e-mail notifications option is selected, notifications are sent for every Patch Alert (page 331). The e-mail includes the type of patch alert, summary of the patches, description of the patch, and a list of systems affected by the alert.

Enhancement Alert

A Patch Alert (page 331) that pertains to a package enhancement request.

Management

One of SUSE's service level offerings. It has more features than the update service level, including user management, system groups, and enhanced system details.

Notification Method

An e-mail address to which SUSE Manager monitoring messages will be sent.

Organization Administrator

A user role with the highest level of control over an organization's SUSE Manager account. Organization administrators can add users, systems, and system groups to the organization as well as remove them. They can also edit details of their orga-

nization's users, for example, to grant them certain permissions by assigning roles. Each organization must have at least one organization administrator.

Package

All software in SUSE Linux Enterprise is divided into software packages. Software updates are released in the form of RPM packages that can be installed on a SUSE Linux Enterprise system.

Package Updater

A client application for Red Hat Enterprise Linux client systems that allows users to retrieve and install all updated packages for the client system on which the application is run. From Red Hat Enterprise Linux 5 on, this application replaces the Red Hat Update Agent (`up2date`) that was shipped with former Red Hat Enterprise Linux versions.

Patches

SUSE provides fixes for security issues and bugs as well as package enhancements for SUSE Linux Enterprise Server in the form of patches. These contain a topic, Bugzilla bug IDs, relevant releases/architectures, and the solutions including required RPMs, and file checksums for verification. Each SUSE Patch Alert (page 331) is based on the SUSE Linux Enterprise patch list.

Security issues and bugs are reported by SUSE engineers and the Linux community via Bugzilla which generates a bug report for each issue. SUSE engineering evaluates the reports, resolves the bugs, and generates new RPM packages. After the SUSE quality assurance team has tested new packages, they are placed on the SUSE public file server and a patch is generated.

Patch Alert

An alert that updated packages containing SUSE patches are available for one or more systems within an organization. There are three types of patch alerts: security alerts, bug fix alerts, and enhancement alerts.

Probe

A set of criteria that is either a template or a set of values assigned to a system that is used to measure the performance of a system.

Probe State

The measure of a probe's adherence to its defined criteria. States include: OK, Warning, Critical, Pending, Unknown

Probe Suite

Collection or group of SUSE Manager monitoring probes.

Provisioning

One of the Novell Customer Center service level offerings. It has more features than the Management service level, including autoinstalling, reconfiguring, tracking, and reverting systems.

pup

See Package Updater (page 331).

Red Hat Update Agent

A client application for Red Hat Enterprise Linux client systems that allows users to retrieve and install all updated packages for the client system on which the application is run. The application also includes functionality to register the client with SUSE Manager. Use the Red Hat Update Agent Configuration Tool to configure its preferences.

Registered System

See Client System (page 330).

RPM

A software package manager that was developed by Red Hat Inc. It can be used to build, install, query, verify, update, and uninstall software packages. All software updates from SUSE Manager are delivered in RPM format.

RPM Database

Each SUSE Linux Enterprise system has an RPM database that stores information about all the RPM packages installed on the system. This information includes the version of the package, which files were installed with the package, a brief description of the package, the installation date, and more.

RPM Update

Deliver the RPM packages based on the Patch Alert (page 331) list to a client system without user intervention. If this feature is selected, packages are delivered through the SUSE Manager Daemon (page 333) running on the client system.

Security Alert

A Patch Alert (page 331) that pertains to system security.

Service Level

A SUSE subscription service. Different service levels offer different features of SUSE Manager. There are three paid service levels currently available: update, management, and provisioning.

Sibling

Siblings are virtual guests running on the same host. Virtual guests that run on separate hosts are not siblings.

Software Manager

The name of the first Service Level (page 333) offering for SUSE Manager.

SUSE Manager Administrator

A user role that has the highest level of control in the SUSE Manager Web interface. A SUSE Manager administrator can assign the SUSE Manager administrator role to other users. However, without also having the role of an organization administrator, a SUSE Manager administrator cannot edit user details for organization users. An organization must have at least one SUSE Manager administrator assigned.

SUSE Manager Bootstrap Script

The bootstrap script (`bootstrap.sh`) is a script on your SUSE Manager server which has to be enabled in *Admin > SUSE Manager Configuration > Bootstrap Script* before its initial use. It is executed on clients and collects all information needed by the SUSE Manager server like System Profile (page 333) and Digital Certificate (page 330). The script establishes a connection to your server and registers the clients.

SUSE Manager Daemon

The SUSE Manager client daemon (`rhnsd`) that periodically polls for scheduled actions.

System ID

A unique string of characters and numbers that identifies a registered system. It is stored in the system's Digital Certificate (page 330).

System Profile

Contains hardware and software information about the client system. The profile is created during the registration process and stored on the SUSE Manager server. The software information is a list of RPM packages and their versions installed on

the client system. The system profile is used to determine every Patch
Alert (page 331) relevant to each client system.

System Set Manager
Interface that allows users to perform actions on multiple systems. Actions include
applying patch updates, upgrading packages, and adding/removing systems to/from
system groups.

Update
One of the Novell Customer Center service level offerings.

Traceback
A traceback is a detailed description of "what went wrong" that is useful for trou-
bleshooting SUSE Manager. Tracebacks are automatically generated when a critical
error occurs and are mailed to the individual(s) designated in the SUSE Manager's
configuration file.

up2date
See Red Hat Update Agent (page 332).

Virtual Guest
Any of the virtual instances running on the virtual host, under the control of the
hypervisor. Also referred to as domain U or domU.

Virtual Host
The physical system on which the hypervisor and all guest systems are running.
The virtual host may also be referred to as domain 0, or dom0.

YaST Online Update
A graphical user interface for updating software packages on SUSE Linux Enterprise
systems.

Yellowdog Updater Modified
A command line tool on Red Hat Enterprise Linux client systems, used to retrieve
and install new or updated packages.

`yum`
See Yellowdog Updater Modified (page 334).

Zypper
A command line tool on SUSE Linux Enterprise systems. Use Zypper to install, update, or remove software packages, and to manage repositories.