Reference Guide

SUSE Manager 2.1

Reference Guide

SUSE Manager 2.1

Publication date: Sep 21 2015

SUSE Linux Products GmbH
Maxfeldstr. 5
90409 Nürnberg
GERMANY
http://www.suse.com/documentation

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

Contents

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 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.suse.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.suse.com/documentation/suse_manager/ ↗.

1 Available Documentation

The following manuals are available on this product:

Installation & Troubleshooting Guide, *Installation & Troubleshooting Guide*

Lists installation scenarios and example topologies for different SUSE Manager setups. Guides you step by step through the installation, setup and basic configuration of SUSE Manager. Also contains detailed information about SUSE Manager maintenance and troubleshooting.

Proxy Quick Start, *Proxy Quick Start*

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

User Guide, *User Guide*

Guides through common use cases and explains the Web interface.

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

Reference documentation that covers administration topics like registering and updating client systems, configuring the SUSE Manager daemon, 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, go to https://scc.suse.com/support/requests ↗, log in, and click *Create New*.

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/doc/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.

- 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.

1 SUSE Manager Overview

SUSE Manager is a 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 Web interface, whether this is hosted by a SUSE Manager or fed through a proxy server,
- SUSE Manager daemon.

SUSE Manager daemon enables channel subscription, package installs, and management of system profiles.

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* for further information). This daemon is necessary in order to schedule updates or other actions through the Web interface.

Find out more about SUSE Manager at http://www.suse.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 on 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 Web interface, 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 applying them to each system individually, work with members of a predefined system group, or work with an ad-hoc collection of systems. With a single action, install software packages on each system in the set, subscribe the systems to a new channel, or apply all patches to them.

- 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— to 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 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 on 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 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 a 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 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.

2 Package Update Tools (SLE and RHEL)

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

To update SUSE Manager server, additional steps might be required. Refer to Section “Updating SUSE Manager”, Chapter 8, *Maintenance*, *Installation & Troubleshooting 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”*.

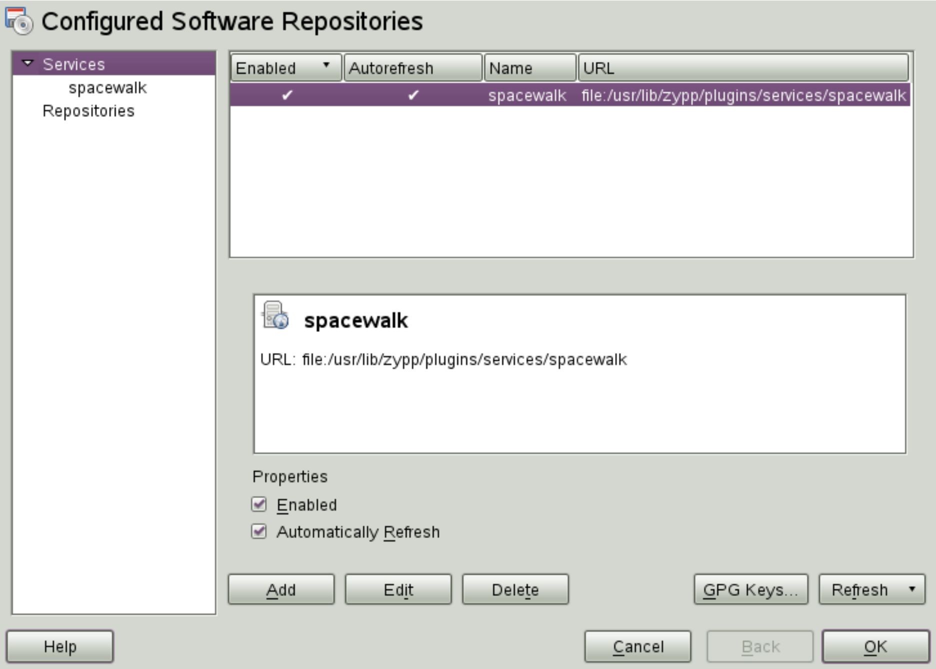
Use `zypper` if you prefer to manage software updates on the command line. For more information, refer to *Section 2.1.2, “Updating Packages from the Command Line with Zypper”*.

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, *User Guide*.

2.1.1 Using YaST Online Update

Novell offers a continuous stream of software security updates for your products. 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.



Enabled	Autorefresh	Name	URL
✓	✓	spacewalk	file:/usr/lib/zypp/plugins/services/spacewalk

spacewalk

URL: file:/usr/lib/zypp/plugins/services/spacewalk

Properties

☑ Enabled

☑ Automatically Refresh

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"*) and you can use YaST to install software updates on the client system. For more information about client activation, refer to Section "Client Setup", Chapter 4, *Installation*, *Installation & Troubleshooting Guide* and Section "Activation Keys — [Mgmt]", Chapter 3, *Systems*, *User Guide*.

SUSE 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

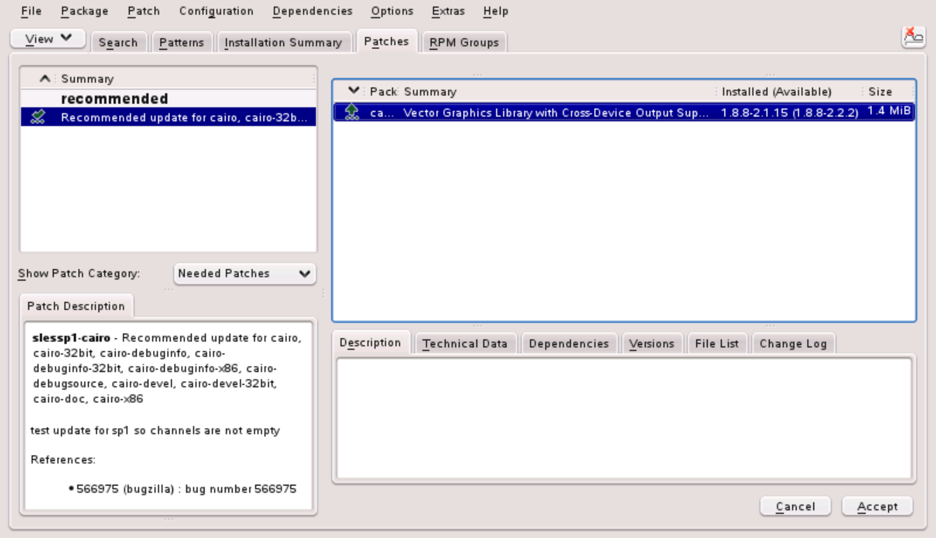
1. Run *Software* › *Online Update* in YaST

2. All new patches (except optional ones) currently available for your system are already marked for installation. Confirm the selection to automatically install these patches.

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.



Summary
recommended
Recommended update for cairo, cairo-32b...

Show Patch Category: Needed Patches

Pack	Summary	Installed (Available)	Size
ca...	Vector Graphics Library with Cross-Device Output Sup...	1.8.8-2.1.15 (1.8.8-2.2.2)	1.4 MiB

slessp1-cairo - Recommended update for cairo, cairo-32bit, cairo-debuginfo, cairo-debuginfo-32bit, cairo-debuginfo-x86, cairo-debugsource, cairo-devel, cairo-devel-32bit, cairo-doc, cairo-x86

test update for sp1 so channels are not empty

References:

- 566975 (bugzilla) : bug number 566975

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 been fulfilled (because the relevant packages have already been updated from another source).

All Patches

All patches available for the client system.

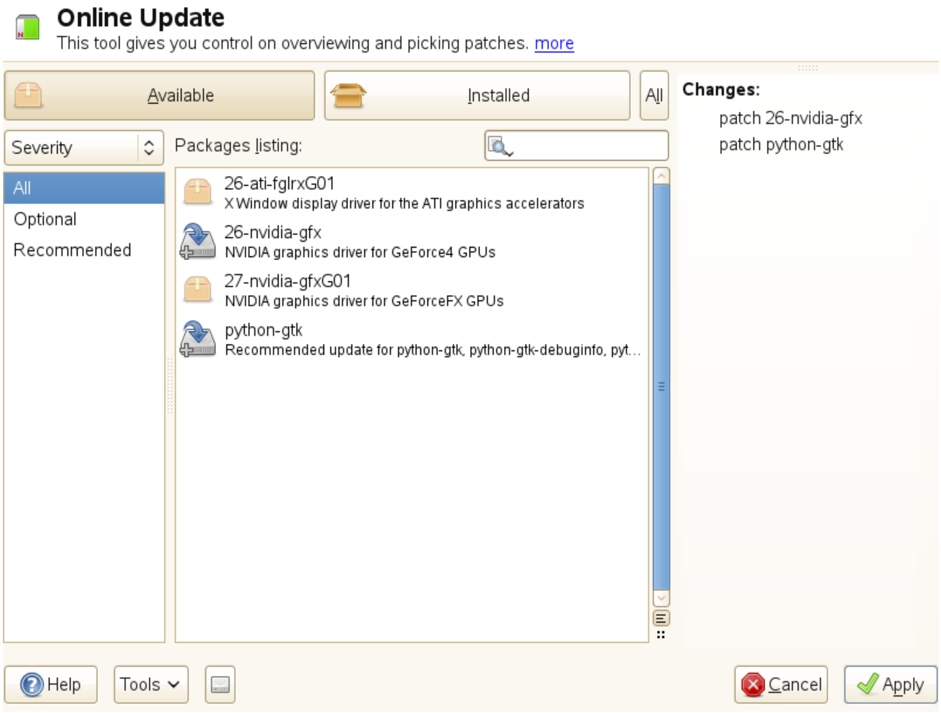
A list entry consists of a symbol and the patch name. For a list of possible symbols, press `Shift`–`F1`. Actions required by `Security` and `Recommended` patches are automatically preset. These actions are *Autoinstall*, *Autoupdate* and *Autodelete*. Actions for `Optional` patches are not preset—right-click 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. If so, 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 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 made once you *Apply* them.



Online Update

This tool gives you control on overviewing and picking patches. more

Severity: All

Changes:
patch 26-nvidia-gfx
patch python-gtk

Packages listing:

26-ati-fglrxG01
X Window display driver for the ATI graphics accelerators

26-nvidia-gfx
NVIDIA graphics driver for GeForce4 GPUs

27-nvidia-gfxG01
NVIDIA graphics driver for GeForceFX GPUs

python-gtk
Recommended update for python-gtk, python-gtk-debuginfo, pyt…

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 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 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. In that case, 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 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 patches:

```
zypper search -t patch
```

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

```
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 be useful to find 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:

For example, if you want 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 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.

2.1.2.2.1 Installing Source Packages

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

```
zypper source-install package_name
```

This command will also install the build dependencies of the specified package. To avoid 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”* for details on repository management.

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

```
zypper search -t srcpackage
```

2.1.2.2.2 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. Do not use the latter (**`zypper dist-upgrade`**) for migrating SUSE Manager 1.7 to version 2.1. Instead use YaST Wagon as described in Section “Online Migration with YaST *Wagon*”, Chapter 8, *Maintenance*, *Installation & Troubleshooting Guide*.

2.1.2.3.1 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 available 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
```

2.1.2.3.2 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: Updating packages to newer versions with `zypper update`

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.

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
```

2.1.2.4.1 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/openSUSE:Libzypp_URIs for details). The *`Alias`* is a shorthand and unique identifier of the repository. You can freely choose it as long as it is 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.

2.1.2.4.2 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
```

2.1.2.4.3 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 its 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 change 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 want 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 and 6

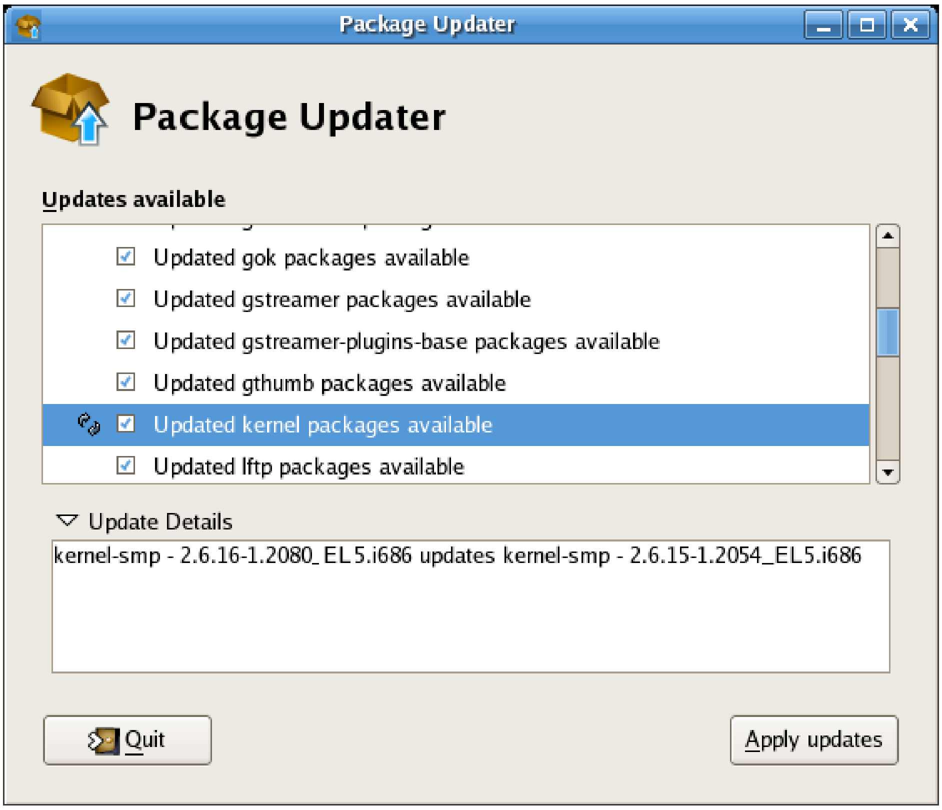
Depending on your version of Red Hat Enterprise Linux, systems registered with SUSE Manager can update client systems directly, using various tools and applications installed on the system. For Red Hat Enterprise Linux 5 and 6, you can use the Package Updater (**`pup`**), the updater applet, and **`yum`** tools to keep systems up-to-date.

The Package Updater (**`pup`**) is the desktop update application for Red Hat Enterprise Linux 5 and later. 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.



☑ Updated gok packages available

☑ Updated gstreamer packages available

☑ Updated gstreamer-plugins-base packages available

☑ Updated gthumb packages available

☑ Updated kernel packages available

☑ Updated lftp packages available

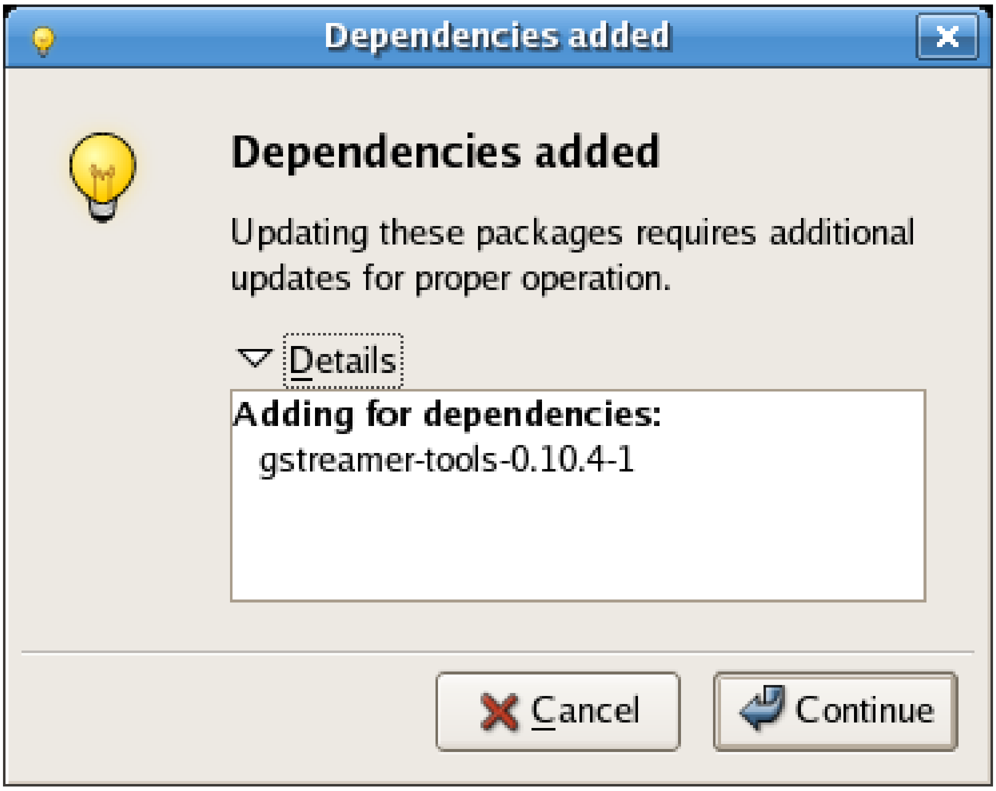
kernel-smp - 2.6.16-1.2080_EL5.i686 updates kernel-smp - 2.6.15-1.2054_EL5.i686

FIGURE 2.4: PACKAGE UPDATER INTERFACE

If there are multiple package updates, they will be listed with pre-selected check boxes 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 resolve any dependencies and notify you if a package must be installed to meet a dependency for an updated package.



Dependencies added

Updating these packages requires additional updates for proper operation.

Adding for dependencies:
gstreamer-tools-0.10.4-1

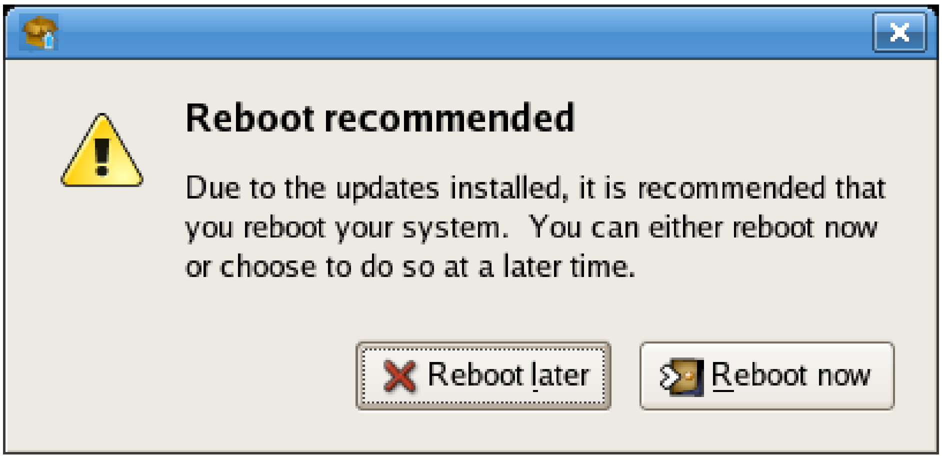
FIGURE 2.5: PACKAGE DEPENDENCY

Click *Continue* to accept the dependency and resume the update.

If this is the first time you are using the Package Updater, the program will prompt you to import 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.



Reboot recommended

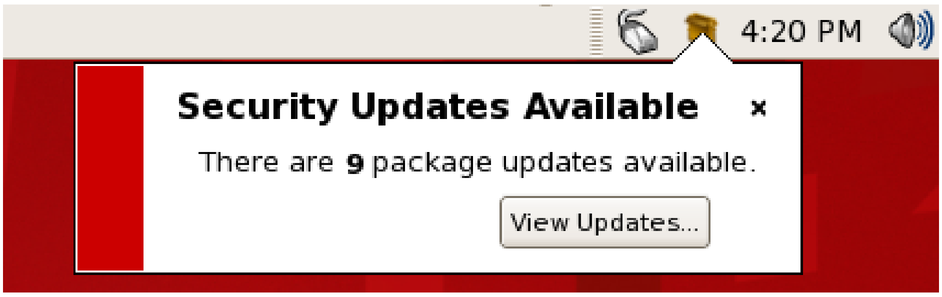
Due to the updates installed, it is recommended that you reboot your system. You can either reboot now or choose to do so at a later time.

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 and later features an applet on the graphical desktop panel that periodically checks for updates from the SUSE Manager server and alerts users when updates are available.



Security Updates Available

There are **9** package updates available.

FIGURE 2.7: PACKAGE UPDATER APPLET

The Package Updater applet stays in the notification tray of the desktop panel and periodically checks for updates. The applet also facilitates various package maintenance tasks. Click the notification icon and choose from the following actions:

- *Refresh*: checks SUSE Manager for new updates.
- *View Updates*: launches the Package Updater application and displays available updates in more detail. Configure the updates to your specifications.

- *Apply Updates*: downloads and installs all updated packages.
- *Quit*: closes 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 dependencies so they may be installed together in an effort to alleviate dependency issues. Red Hat Enterprise Linux 5 and 6 use **yum** to fetch and install packages.

> **Note**
>
> **up2date** is no longer available on Red Hat Enterprise Linux 5 and later versions. The entire stack of update and installation tools is now based on Yum.

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.

3 SUSE Manager Daemon

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 establishes 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.

Warning

When new packages or updates are installed on the client via SUSE Manager, any licenses (EULAs) requiring agreement before installation are automatically accepted.

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 `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. To find out, run:

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

4 Monitoring

The monitoring entitlement allows you to perform 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 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 proves invaluable in balancing loads on those systems.

Monitoring consists of two components: the monitoring system and the monitoring scout. The monitoring system is installed on the SUSE Manager and performs backend functions such as storing monitoring data and acting on it. The monitoring scout runs all the probes and collects monitoring data. The scout can be enabled to run on a SUSE Manager or Proxy system. Using a monitoring scout on a proxy allows you to offload work from the SUSE Manager and provide scalability for probes.

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.

4.1 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 users.

- 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 4.1.1, "SUSE Manager Monitoring Daemon (rhnmd)"* for installation instructions and a quick list of probes requiring this secure connection. Refer to *Appendix B, Probes* for the complete list of available probes.

PROCEDURE 4.1: ENABLING MONITORING IN THE WEB INTERFACE

1. Log in as the administrator and click *Admin* › *SUSE Manager Configuration*.

2. In the *General* tab check *Enable Monitoring*.

3. Then, to make the SSH key available via the Web interface, open the *Monitoring* tab and check *Enable Monitoring Scout*. For more information on SSH key handling, see *Section 4.1.2, "Installing the SUSE Manager Monitoring Daemon"*.

4. Finally, restart SUSE Manager by opening the *Restart* tab, check *Restart SUSE Manager?*, and confirm this dialog with the *Restart* button.

Note: SSH Key on the SUSE Manager Server

Find the SSH key on the SUSE Manager file system here:

```
/var/lib/nocpulse/.ssh/nocpulse-identity.pub
```

4.1.1 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 4.1.3, "Configuring SSH"* for details.

Some probes require 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.

4.1.2 Installing the SUSE Manager Monitoring Daemon

Install the SUSE Manager monitoring daemon to prepare systems for monitoring with the probes listed in *Section 4.1.1, “SUSE Manager Monitoring Daemon (rhnmd)”*. 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 4.1.3, “Configuring SSH”* 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. For a list of client tools channels, see *Appendix E, List of Client Tools Channels*. 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 4.1.4, “Installing the SSH key”*.

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.

4.1.3 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 specified 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 4.1.4, “Installing the SSH key”*.

5. Start `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.

4.1.4 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 check box 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 and add EOF. The result should 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.

4.2 Configuring the MySQL Package for Probes

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* for a listing of all available probes.

Subscribe 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.

4.3 Enabling 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.

4.3.1 Creating Notification Methods

Notifications are sent via a notification method to an email 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 have multiple notification methods associated. To create a notification method:

1. Log into the SUSE Manager Web interface as either a SUSE Manager administrator or monitoring administrator.

2. Navigate to *User* and select the username. On the *User Details* › *Notification Methods* tab, click *create new method*.

3. Enter an intuitive, descriptive label for the method name, such as `DBA day email`, then provide the correct email 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 check box if you desire abbreviated messages to be sent to the email address. 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* check box 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.

4.3.2 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 the specified email address.

The longer email 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.

> ### Note
>
> Since notifications can be generated whenever a probe changes state, simple changes in your network can result in a flood of notifications. Notifications may be redirected to a specific inbox for notifications to avoid issues with higher priority mail. The next section discusses redirecting notifications.

4.3.3 Redirecting Notifications

When receiving a notification, you can redirect it by including advanced notification rules within an acknowledgment email. *Enable email reply* redirects by opening `/etc/aliases` and adding the following line:

```
rogerthat01:    "| /etc/smrsh/ack_queuer.pl"
```

Once the parameter has been set, reply to the notification email 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 automatically 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 email 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 email 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.

4.3.4 Deleting Notification Methods

Existing relationships between methods and probes can complicate the process of deleting notification methods. Follow these steps to remove a notification method:

1. Log into the SUSE Manager Web interface 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. Select another notification method and click *Update Probe*.

6. Return to the *Monitoring* › *Notifications* page and delete the notification method.

4.4 About 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.

4.4.1 Managing Probes

Probes are created on the SUSE Manager, then propagated to the specified monitoring-entitled systems. Follow the steps below to add a probe to SUSE Manager:

1. Log into the SUSE Manager Web interface 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* 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* check box 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* check box) means you will receive notifications every minute the probe surpasses its CRITICAL or WARNING thresholds. Refer to *Section 4.3, "Enabling Notifications"* 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 4.1.3, "Configuring SSH"* for details. Otherwise, accept the default values of `nocpulse` and `4545`, respectively.

7. If the *Timeout* field appears, review the default value and adjust according to your needs. Most but not all timeouts result in an UNKNOWN state. If the probe's metrics are time-based, ensure the timeout is no 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 4.4.2, "Establishing Thresholds"* 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 on the *System Details* › *Probes* tab and click *delete probe*. Finally, confirm the deletion.

4.4.2 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 percentage 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.

4.4.3 Monitoring the SUSE Manager Server

In addition to your client systems, you may also monitor your SUSE Manager or proxy 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 4.4.1, “Managing Probes”* for instructions.

Although the SUSE Manager or proxy server now appears to be monitored by the client system, the server runs the probe on itself. Thresholds and notifications work as usual.

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.

4.5 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.

4.5.1 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 4.5.2, “Viewing the output of rhn-runprobe”* for instructions.

4.5.2 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 4.1: `rhn-runprobe` OPTIONS

Option	Description
`--help`	List the available options and exit.
`--probe=PROBE_ID`	Run the probe with the specified 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 describing the probe's attempted execution. Errors are clearly identified.

5 Managing Multiple Organizations

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 concept 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 5.a, *Installation & Troubleshooting Guide* in Procedure “Setting Up SUSE Manager”, *Installation & Troubleshooting Guide*.

5.1 Recommended Models for Using Multiple Organizations

The following examples detail two possible scenarios using the multiple organizations (or multi-org) feature. 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.

5.1.1 Centrally-Managed SUSE Manager for a Multi-Department Organization

In this first scenario, SUSE Manager is maintained by a central group of administrators within a business or other organization (refer to *Figure 5.1, “Centralized SUSE Manager Management for a Departmental Organization”*). 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.

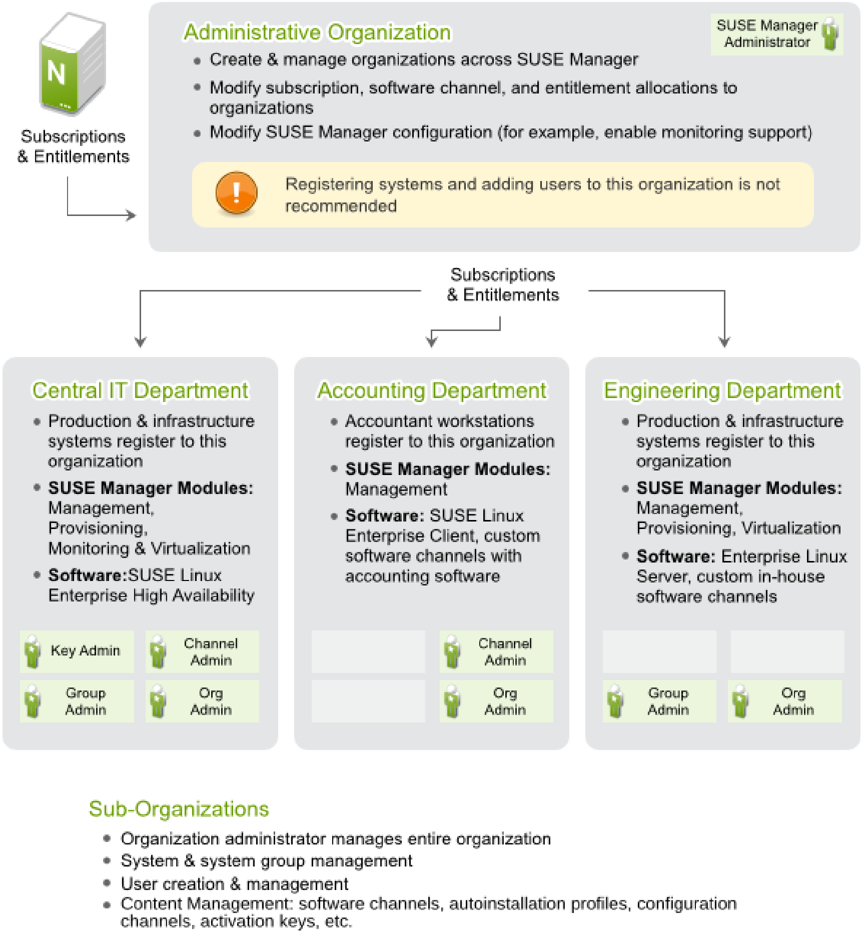

Subscriptions & Entitlements
Administrative Organization
SUSE Manager Administrator
Create & manage organizations across SUSE Manager
Modify subscription, software channel, and entitlement allocations to organizations
Modify SUSE Manager configuration (for example, enable monitoring support)
Registering systems and adding users to this organization is not recommended
Subscriptions & Entitlements
Central IT Department
Production & infrastructure systems register to this organization
SUSE Manager Modules: Management, Provisioning, Monitoring & Virtualization
Software:SUSE Linux Enterprise High Availability
Key Admin
Channel Admin
Group Admin
Org Admin
Accounting Department
Accountant workstations register to this organization
SUSE Manager Modules: Management
Software: SUSE Linux Enterprise Client, custom software channels with accounting software
Channel Admin
Org Admin
Engineering Department
Production & infrastructure systems register to this organization
SUSE Manager Modules: Management, Provisioning, Virtualization
Software: Enterprise Linux Server, custom in-house software channels
Group Admin
Org Admin
Sub-Organizations
Organization administrator manages entire organization
System & system group management
User creation & management
Content Management: software channels, autoinstallation profiles, configuration channels, activation keys, etc.

FIGURE 5.1: CENTRALIZED SUSE MANAGER MANAGEMENT FOR A DEPARTMENTAL ORGANIZATION

5.1.2 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 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.

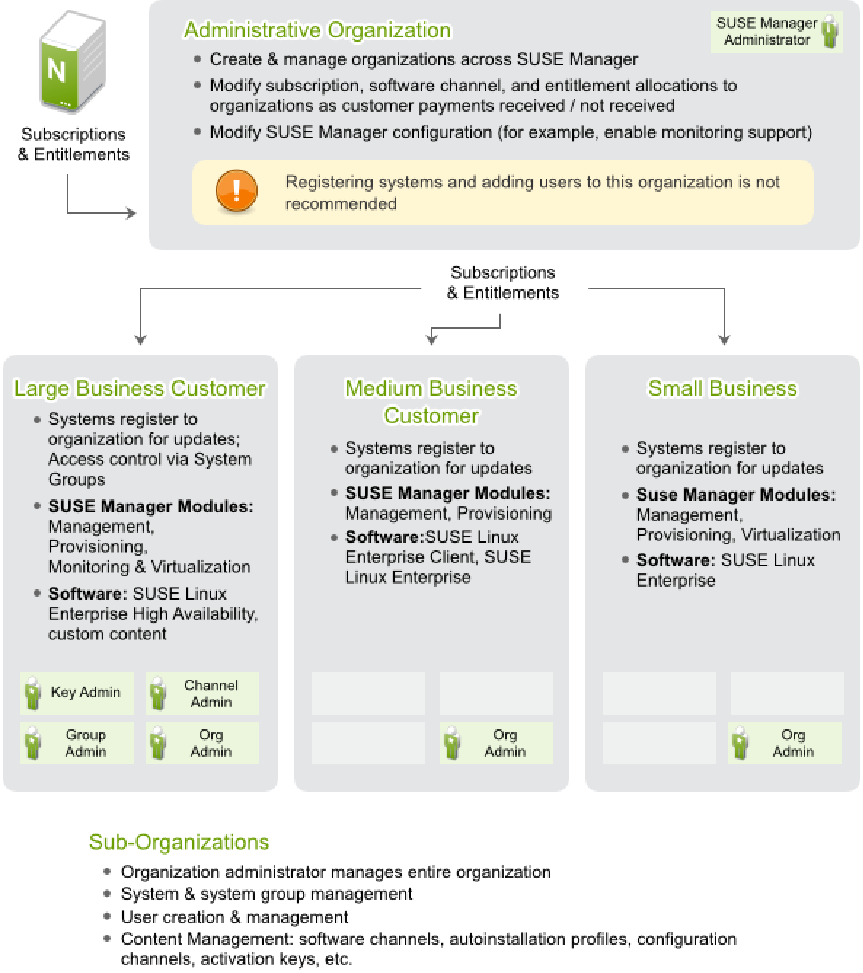

Subscriptions & Entitlements
Administrative Organization
SUSE Manager Administrator
Create & manage organizations across SUSE Manager
Modify subscription, software channel, and entitlement allocations to organizations as customer payments received / not received
Modify SUSE Manager configuration (for example, enable monitoring support)
Registering systems and adding users to this organization is not recommended
Subscriptions & Entitlements
Large Business Customer
Systems register to organization for updates; Access control via System Groups
SUSE Manager Modules: Management, Provisioning, Monitoring & Virtualization
Software: SUSE Linux Enterprise High Availability, custom content
Key Admin
Channel Admin
Group Admin
Org Admin
Medium Business Customer
Systems register to organization for updates
SUSE Manager Modules: Management, Provisioning
Software:SUSE Linux Enterprise Client, SUSE Linux Enterprise
Org Admin
Small Business
Systems register to organization for updates
Suse Manager Modules: Management, Provisioning, Virtualization
Software: SUSE Linux Enterprise
Org Admin
Sub-Organizations
Organization administrator manages entire organization
System & system group management
User creation & management
Content Management: software channels, autoinstallation profiles, configuration channels, activation keys, etc.

FIGURE 5.2: DECENTRALIZED SUSE MANAGER MANAGEMENT FOR MULTI-DEPARTMENT ORGANIZATION

5.1.3 Recommendations for Using Multiple Organizations

Regardless of which scenario you choose for managing 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 regard 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 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. To make these new entitlements available to other organizations on SUSE Manager, you will need to explicitly allocate these entitlements to 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.

5.1.3.1 Certificate Has Less Entitlements Than Are Used

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 might need to free entitlements quickly and may not have access to each organization. There is an option in multi-org SUSE Managers that allows the server administrators to reduce an organization's entitlement count below usage. In this case, log in to the administrative organization and proceed as described below:

1. In the `/etc/rhn/rhn.conf` file set the `web.force_unentitlement` variable to `1`:

   ```
   web.force_unentitlement=1
   ```

This setting 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*, and the organization has four entitlements that were not in use by systems, then 6 systems in the organization will be unentitled.

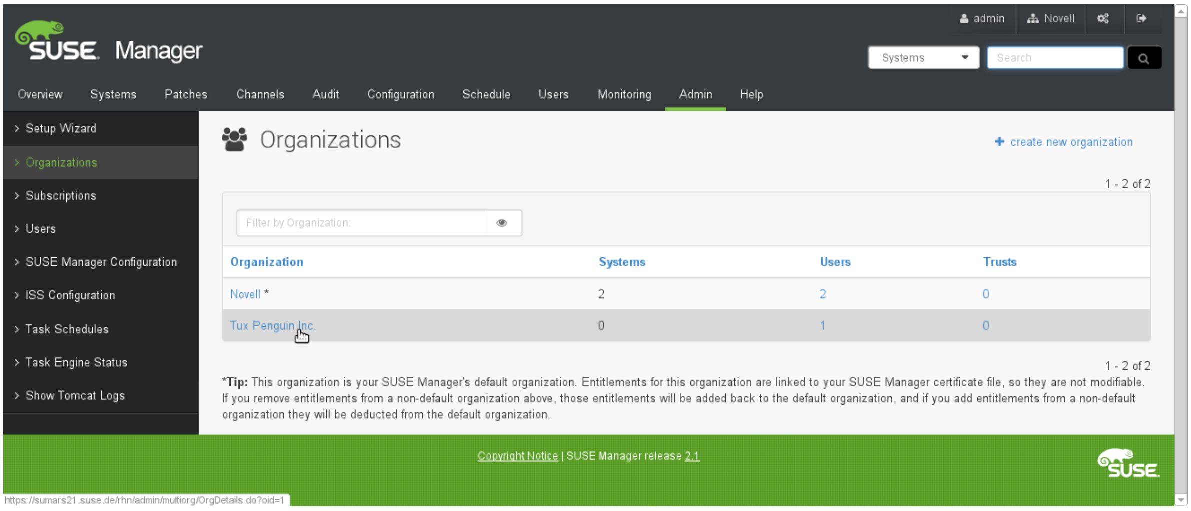
After you have a sufficient number of entitlements, you should be able to activate your new SUSE Manager certificate. Note that modifying the `web.force_unentitlement` variable is only necessary to reduce an organization's allocated entitlements below what they are using. If an organization has more entitlements than are being actively used, you do not need to set this variable to remove them.

5.1.3.2 Certificate Has More Entitlements Than Are Used

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 be able to allocate these entitlements to other organizations. Entitlements previously allocated to other organizations will be unaffected.

5.2 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.



Organization	Systems	Users	Trusts
Novell *	2	2	0
Tux Penguin Inc.	0	1	0

1 - 2 of 2

*Tip: This organization is your SUSE Manager's default organization. Entitlements for this organization are linked to your SUSE Manager certificate file, so they are not modifiable. If you remove entitlements from a non-default organization above, those entitlements will be added back to the default organization, and if you add entitlements from a non-default organization they will be deducted from the default organization.

FIGURE 5.3: 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 5.6, “Organizational Trusts”* for more information about establishing organizational trusts.

5.2.1 *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 also delete an organization by clicking the *Delete Organization* link.

The *Details* page also contains three subtabs: *Users*, *Subscriptions*, and *Trusts*.

5.3 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 main 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 8, *Maintenance, Installation & Troubleshooting Guide*.

PROCEDURE 5.1: CREATING AND DELETING ORGANIZATIONS

1. Log in to the Web interface as SUSE Manager administrator or organization administrator.

2. Procedure to create an organization:

   a. Switch to the *Admin* tab to see a list of all *Organizations* within SUSE Manager.

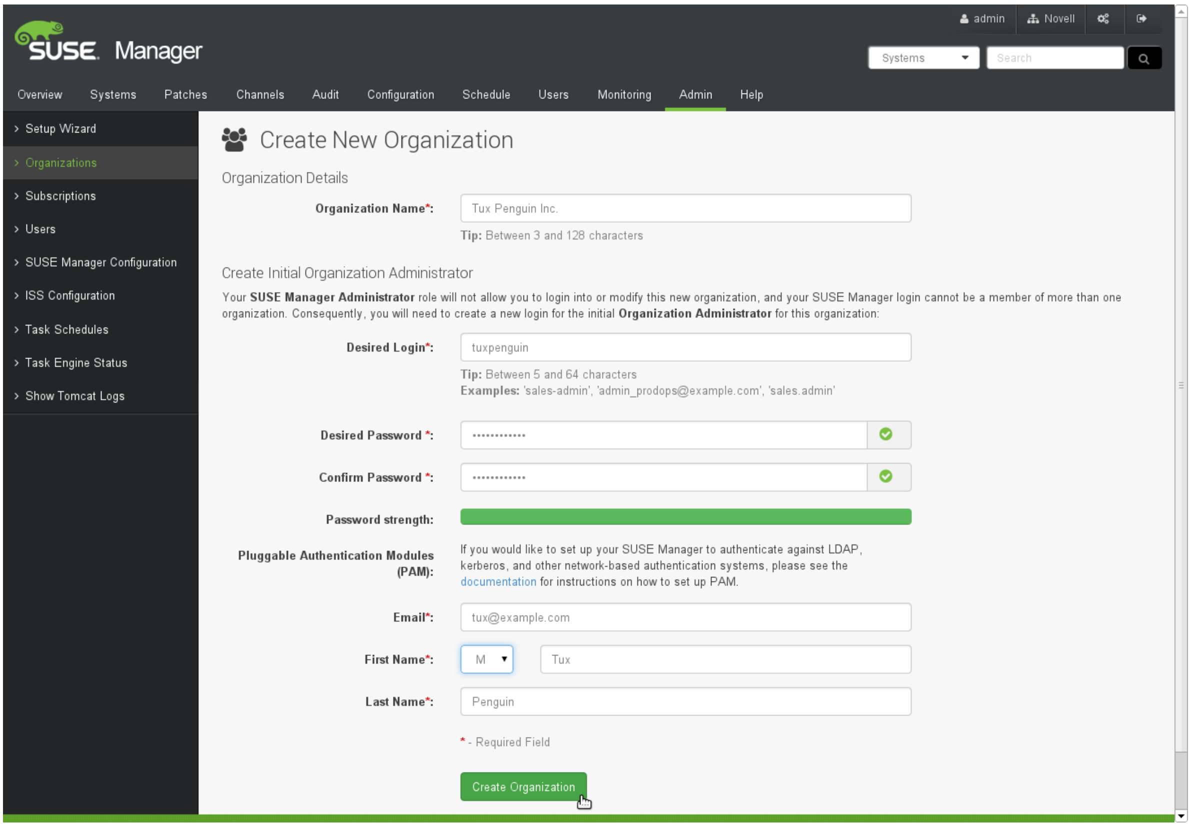
   b. Click the *Create New Organization* link at the top right corner.

   c. Enter an *Organization Name*.

   d. 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`.



Create New Organization

Organization Details

Organization Name*: Tux Penguin Inc.

Tip: Between 3 and 128 characters

Create Initial Organization Administrator

Your **SUSE Manager Administrator** role will not allow you to login into or modify this new organization, and your SUSE Manager login cannot be a member of more than one organization. Consequently, you will need to create a new login for the initial **Organization Administrator** for this organization:

Desired Login*: tuxpenguin

Tip: Between 5 and 64 characters
Examples: 'sales-admin', 'admin_prodops@example.com', 'sales.admin'

Desired Password *: ••••••••••••

Confirm Password *: ••••••••••••

Password strength:

Pluggable Authentication Modules (PAM): If you would like to set up your SUSE Manager to authenticate against LDAP, kerberos, and other network-based authentication systems, please see the documentation for instructions on how to set up PAM.

Email*: tux@example.com

First Name*: M Tux

Last Name*: Penguin

* - Required Field

FIGURE 5.4: CREATE NEW ORGANIZATION

e. Enter the first and last name and the email address of the new user.

f. To finish, click *Create Organization*. Once the new organization is created, the *Organizations* page will list the new organization.

3. Procedure to delete an organization:

a. On the *Admin* tab, select *Organizations* from the left navigation bar.

b. Click the desired organization to see the organization details.

c. Click the *Delete Organization* link at the upper right corner and confirm by clicking the *Delete Organization* button.

5.4 Managing Organization 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 Entitlement - Management

Management entitlements are 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 can register with that organization. Provisioning is also recommended, especially for systems managed in organizations.

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 5.4.1, “Admin > Subscriptions > Software Channel Entitlements”* and *Section 5.4.2, “Admin > Subscriptions > System Entitlements”*.

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 5.2, “Assigning Entitlements to an Organization”*.

PROCEDURE 5.2: 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:

    a. Click the *System Entitlements* subtab to view the *System Entitlements Counts*.

    b. Set the total number of *Management (Base)* entitlements for the current organization by entering a value in the *Proposed Total* field.

    c. Similarly, set total numbers for any other entitlements you may need (like monitoring, provisioning, or virtualization).

    d. Click *Update Organization* to confirm your changes.

5. To set software channel entitlements for the selected organization:

    a. Click the *Software Channel Entitlements* subtab to view the *Software Channel Entitlements Counts*.

    b. 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.

    c. 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*.

5.4.1 *Admin > Subscriptions > Software Channel Entitlements*

The *Software Channel Entitlements Across SUSE Manager* page lists all entitlements on SUSE Manager across all organizations, as well as 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.

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 5.6, “Organizational Trusts”*.

5.4.2 *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. Allocations of each system entitlement can be changed in the text box.

- *Bootstrap (Add-On)*: system can be configured via bootstrap. For more details, see Chapter 5, *Using Bootstrap*, *Client Configuration Guide*.
- *Management (Base)*: a base requirement for all organizations to function correctly. The number of management entitlements allocated to an organization is equivalent to the maximum number of systems that can register to that organization, regardless of the number of software entitlements available.
- *Monitoring (Add-On)*: enables the tracking of monitoring data for a system. For more details on monitoring, refer to Chapter 11, *Monitoring — [Mon]*, *User Guide*.
- *Provisioning (Add-On)*: allows various advanced functionality such as autoinstallation and configuration file provisioning. Recommended especially for systems managed in organizations.
- *Virtualization (Add-On)*: not used in SUSE Manager.
- *Virtualization Platform (Add-On)*: applied to a VM Host Server system with unlimited guest management enabled.

5.5 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:

   ```
   rhnreg_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.

5.6 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, it is up to each organization's administrator to determine what resources to share, and what shared resources from other organizations in the trust to use. With trust established, it is possible to share content and migrate systems between these two organizations.

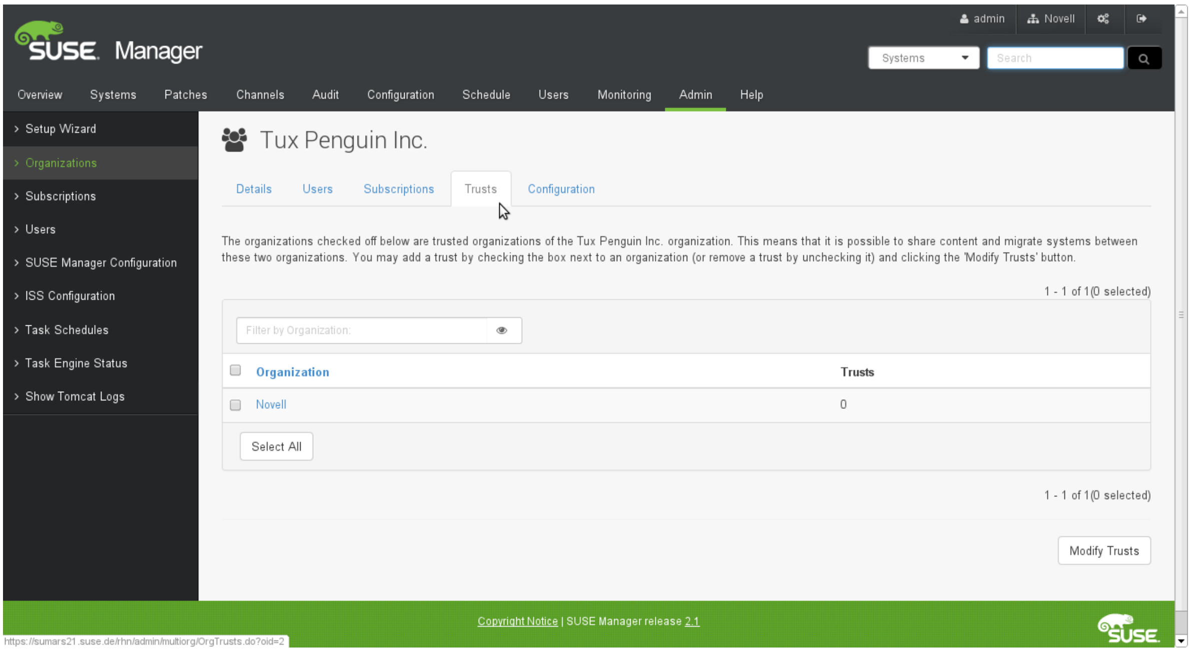
> **Note**
>
> Only organization administrators have the rights to share their custom content. The SUSE Manager administrator role is limited to allocating system and software entitlements to each organization.

5.6.1 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.



The organizations checked off below are trusted organizations of the Tux Penguin Inc. organization. This means that it is possible to share content and migrate systems between these two organizations. You may add a trust by checking the box next to an organization (or remove a trust by unchecking it) and clicking the 'Modify Trusts' button.

□	Organization	Trusts
□	Novell	0

FIGURE 5.5: ORGANIZATIONAL TRUSTS

Click the check box 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.

5.6.2 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, 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.

5.6.3 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 via the SUSE Manager web interface or by using a utility called **`migrate-system-profile`**.

Note

The SUSE Manager administrator can migrate a system from one trusted organization to any other within the trust. However, organization administrators can only migrate a system from their own organization to another in the trust.

Using the web interface to migrate systems, click *Systems* › *Systems*. Click on the system name. On the subtab *Details* › *Migrate*, choose the organization the system needs to migrate to. Click *Migrate System*. The system is successfully migrated to the target organization.

The command-line tool **`migrate-system-profile`** 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.

Verify the ID of the system to be migrated, the ID of the organization the system will migrate to (available in the web interface or use the **`spacewalk-report`** tool), and the hostname or IP address of the SUSE Manager server if you are running the command from another machine.

Use the following command:

```
migrate-system-profile --satellite {SUSE Manager HOSTNAME OR IP} --systemId={SYSTEM
 ID} --to-org-id={DESTINATION ORGANIZATION ID}
```

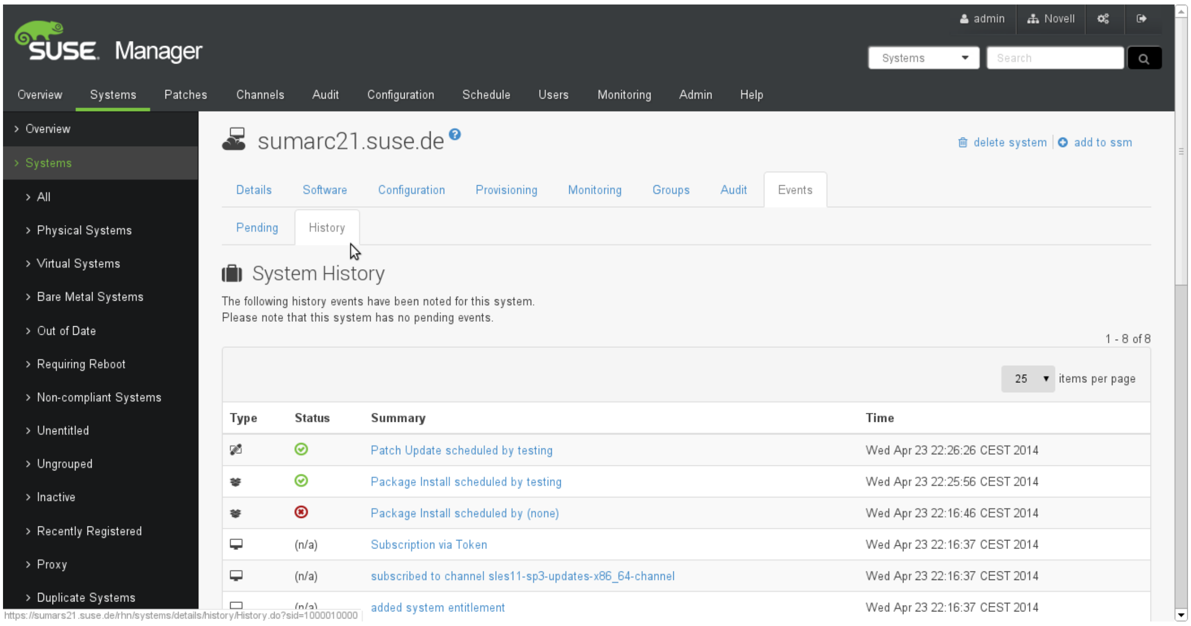
In the following example, the Finance department (created as an organization in SUSE Manager with OrgID 2) wants to migrate a workstation (with SystemID 10001020) from the Engineering department, but the Finance organization administrator does not have shell access to the SUSE Manager server. The SUSE Manager hostname is *satserver.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.



sumarc21.suse.de

System History

The following history events have been noted for this system.
Please note that this system has no pending events.

1 - 8 of 8

25 ▾ items per page

Type	Status	Summary	Time
🩹	✓	Patch Update scheduled by testing	Wed Apr 23 22:26:26 CEST 2014
📦	✓	Package Install scheduled by testing	Wed Apr 23 22:25:56 CEST 2014
📦	⊗	Package Install scheduled by (none)	Wed Apr 23 22:16:46 CEST 2014
🖥	(n/a)	Subscription via Token	Wed Apr 23 22:16:37 CEST 2014
🖥	(n/a)	subscribed to channel sles11-sp3-updates-x86_64-channel	Wed Apr 23 22:16:37 CEST 2014
🖥	(n/a)	added system entitlement	Wed Apr 23 22:16:37 CEST 2014

FIGURE 5.6: SYSTEM HISTORY

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
```

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`**.

5.7 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 Chapter 10, *Users — [Mgmt]*, *User Guide* for more information on user configuration.

5.7.1 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 “*User List > Active > User Details* — [Mgmt]”, Chapter 10, *Users — [Mgmt]*, *User Guide*.

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.

6 Virtualization

SUSE Manager allows to autoinstall and manage Xen and KVM VM Guests on a registered VM Host Server or integrate with SUSE Studio. To autoinstall a VM Guest, an autoinstallable distribution and an autoinstallation profile (AutoYaST or Kickstart) 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.

6.1 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.

6.1.1 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. To automatically register VM Guests with SUSE Manager, a bootstrap script is needed.

6.1.1.1 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”, *Installation & Troubleshooting Guide*. While there are no special requirements for a VM Guest key, at least the following 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 want to manage the VM Host Server system from SUSE Manager (e.g. by executing remote scripts), the package `rhncfg-actions` needs to be installed as well.

6.1.1.2 Setting up an Autoinstallable Distribution

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 file system 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. Log in to the SUSE Manager Web interface and navigate to *Systems* › *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*.

To edit an existing *Autoinstallable Distribution*, go to *Systems* › *Autoinstallation* › *Distributions* and click on a *Label*. Make the desired changes and save your settings by clicking *Update Autoinstallable Distribution*.

6.1.1.3 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. They 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 and Useful Enhancements*. 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.

6.1.1.3.1 Uploading an Autoinstallation Profile

1. Log in to the SUSE Manager Web interface and open *Systems* › *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 6.1.1.2, “Setting up an Autoinstallable Distribution”* 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 *File to Upload* dialog, click *Browse* to select it, then 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.

To edit an existing profile, go to *Systems* › *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*.

6.1.1.3.2 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 6.1.1.3.1, “Uploading an Autoinstallation Profile”*.

1. Log in to the SUSE Manager Web interface and go to *Systems* › *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 6.1.1.2, “Setting up an Autoinstallable Distribution”* 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.

6.1.1.3.3 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:

   a. Create a bootstrap script for VM Guests on the SUSE Manager as described in Procedure “Generating the Bootstrap Script”, *Installation & Troubleshooting Guide*.

   b. Log in 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.

   c. Edit the newly created file according to your needs. The minimal requirement is to include the activation key for the VM Guests (see *Section 6.1.1.1, “Activation Keys”* for details). We strongly recommend to also include one or more GPG keys (for example, your organization key and package signing keys).

2. Log in 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 and Useful Enhancements* 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 above within the existing `<scripts>` section!

3. Click *Update* to save the changes.

6.1.2 VM Host Server Setup

A VM Host Server system serving as a target for autoinstalling VM Guests from SUSE Manager must be capable of running 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.suse.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.suse.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:

    a. Create a bootstrap script on the SUSE Manager as described in Procedure “Generating the Bootstrap Script”, *Installation & Troubleshooting Guide*.

    b. Download the bootstrap script from `susemanager.example.com/pub/bootstrap/bootstrap.sh` to the VM Host Server.

c. Edit the bootstrap script according to your needs. The minimal requirement is to include the activation key for the VM Host Server (see *Section 6.1.1.1, “Activation Keys”* for details). We strongly recommend to also include one or more GPG keys (for example, your organization key and package signing keys).

d. 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. If many clients are registered with SUSE Manager, this long interval ensures a certain level of load balancing since not all clients act on 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 that. 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).

6.1.3 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 6.1.1.3.3, “Adding a Registration Script to the Autoinstallation Profile”*. VM Guests need to be registered 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. Log in to the SUSE Manager Web interface and click on the *Systems* tab.
2. Click on the VM Host Server's name to open its *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. 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 for you to monitor the autoinstallation process.

Note: Checking the Installation Log

To view the installation log, click *Events* › *History* on the *Session Status* page. On the *System History Event* page you can click 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. 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 log file `/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.

6.2 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 in the SUSE Manager Web interface if 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 triggered in 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.

6.2.1 Displaying a VM Guest's Profile

Click on the name of a VM Guest on the VM Host Server's *Virtualization* page to open its profile page with detailed information about this guest. For details refer to Section “Systems”, Chapter 3, *Systems*, *User Guide*.

A profile page for a virtual system does not differ from a regular system's profile page. You can perform the same actions (e.g. installing software or changing its configuration).

6.2.2 Starting, Stopping, Suspending and Resuming a VM Guest

To start, stop, restart, suspend, or resume a VM Guest, navigate to the VM Host Server's *Virtualization* page. Check one or more *Guests* listed in the table and scroll down to the bottom of the page. Choose an action from the drop-down list 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. Refer to your KVM or Xen documentation. Alternatively, you may use `libvirt` to enable automatic reboots.

6.2.3 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 6.2.2, “Starting, Stopping, Suspending and Resuming a VM Guest”* for details.

6.2.4 Deleting a VM Guest

To delete a VM Guest you must first shut it down as described in *Section 6.2.2, “Starting, Stopping, Suspending and Resuming a VM Guest”*. Wait at least two minutes to allow the shutdown to finish and then choose *Delete Systems* followed by *Apply Action* and *Confirm*.

6.3 Integrating SUSE Studio Onsite Appliances into SUSE Manager

SUSE Manager allows you to integrate your appliances built with SUSE Studio Onsite and create virtual hosts based on one of your appliances. The guest can be started, stopped, resumed.

6.3.1 Requirements

To integrate your SUSE Studio Onsite appliances in SUSE Manager, make sure you have fulfilled the following requirements:

- Physical hardware which is not virtualized.
- The package `rhn-virtualization-host` must be installed on your client (see *Section 6.3.1.1, “Needed Packages”*).
- An account at the SUSE Studio Onsite Web site at http://susestudio.com ↗ or your own SUSE Studio Onsite service.
- Your activation key contains the Virtualization entitlement (see *Section 6.3.1.2, “Activation Keys”*).

- The SUSE Studio Onsite credentials must be set in SUSE Manager (see *Section 6.3.1.3, “Getting your SUSE Studio Onsite API Key”*).

- Your appliance must have been built as either Xen or KVM output (see *Section 6.3.1.4, “Providing the Correct Formats”*).

6.3.1.1 Needed Packages

To start deploying virtual appliances, install the package `rhn-virtualization-host` on your client. The package is distributed in the SUSE Manager Tools channel.

6.3.1.2 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*.

6.3.1.3 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*.

6.3.1.4 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 in to 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* check box.
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 registered with your SUSE Manager server.

6.3.2 Setting Up SUSE Manager

To add virtualization support to one of your SUSE Manager clients, proceed as follows:

1. Check if you have fulfilled all requirements from *Section 6.3.1, “Requirements”*.
2. Prepare your SUSE Manager client:
    a. Start a shell, log into your SUSE Manager client and turn on virtualization support.
    b. Start YaST in your console and go to *Virtualization* › *Install Hypervisor and Tools*.
    c. 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.

    d. After the reboot is finished, log in to your SUSE Manager client again and start YaST.

3. Log in to SUSE Manager.

4. Go to the *Systems* page and select the machine to 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 check box of your guest, choose one of the options from the popup menu, and click *Apply Action*. The same actions can be performed on the command line 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).

7 Cobbler

SUSE Manager features the Cobbler server that allows administrators to centralize their system installation and provisioning infrastructure. Cobbler is an installation server that provides 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. This section explains supported features of Cobbler, which 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,
- building installation ISOs with PXE-like menus using the **`cobbler buildiso`** command for SUSE Manager systems with x86_64 architecture.

We only support those Cobbler functions that are either listed within our formal documentation or available via the Web Interface and API.

7.1 Cobbler Requirements

To use Cobbler as a PXE boot server, you should heed the following guidelines:

- To use Cobbler for system installation with PXE, you must have a TFTP server installed and configured. By default, SUSE Manager installs such a TFTP server.
- 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's DHCP server. Edit `/etc/dhcp.conf` to change `next-server` to the hostname or IP address of your Cobbler server.

7.1.1 Configuring Cobbler with /etc/cobbler/settings

Cobbler configuration is mainly done in the `/etc/cobbler/settings` file. With the default settings unchanged, Cobbler should run as intended. Still, all configurable settings are explained in detail in the `/etc/cobbler/settings` file with regard to how they affect functionality of Cobbler and whether it is recommended for users to adjust values to their environment.

7.1.2 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.

7.1.2.1 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 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 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`.

5 The DHCP server retrieves the `pxelinux.0` bootloader file.

7.1.3 Xinetd and TFTP

SUSE Manager uses the `atftpd` daemon, but it can also operate with Xinetd/TFTP. The `atftpd` is installed by default as 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` file 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.

7.1.4 Syncing TFTP Contents to SUSE Manager Proxies

With SUSE Manager 1.7 and later it is possible to sync cobbler generated TFTP contents to SUSE Manager Proxies to perform PXE booting via these proxies.

7.1.4.1 Installation

On the SUSE Manager Server, install the package `susemanager-tftpsync`:

```
zypper install susemanager-tftpsync
```

On the SUSE Manager Proxy systems, install the package `susemanager-tftpsync-recv`:

```
zypper install susemanager-tftpsync-recv
```

7.1.4.2 Configuring SUSE Manager Proxy

Execute `configure-tftpsync.sh` on the SUSE Manager Proxy systems.

This setup script asks for hostnames and IP addresses of the SUSE Manager server and the proxy. Additionally, it asks for the `tftpboot` directory on the proxy. For more information, see the output of **`configure-tftpsync.sh --help`**.

7.1.4.3 Configuring SUSE Manager Server

Execute `configure-tftpsync.sh` on SUSE Manager Server:

```
configure-tftpsync.sh proxy1.example.com proxy2.example.com
```

Execute **`cobbler sync`** to initially push the files to the proxy systems. This will succeed if all listed proxies are properly configured.

> **Note: Changing the List of Proxy Systems**
>
> You can call **`configure-tftpsync.sh`** to change the list of proxy systems. You must always provide the full list of proxy systems.

> **Note: Reinstalling a Configured Proxy**
>
> In case you reinstall an already configured proxy and want to push all files again you must remove the cache file `/var/lib/cobbler/pxe_cache.json` before you can call **`cobbler sync`** again.

7.1.4.4 Requirements

The SUSE Manager Server must be able to access the SUSE Manager Proxy systems directly. Push via proxies is not possible.

7.1.5 Syncing and Starting the Cobbler Service

Before starting the cobbler service, run a check on the cobbler service to make sure that all the prerequisites are configured according to the organization's needs with the command: **`cobbler check`**.

If content, 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. Doing so may cause errors and other issues.

> Always use `/usr/sbin/spacewalk-service` to start or stop SUSE Manager.

7.2 Adding a Distribution to Cobbler

If all Cobbler prerequisites have been 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 “Autoinstallation > Distributions — [Prov]”, Chapter 3, *Systems*, *User Guide*.

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 ram disk (initrd) image file.

7.3 Adding a Profile to Cobbler

Once you have added a distribution to Cobbler, you can 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 “Autoinstallation Profiles (Kickstart and AutoYaST)”, Chapter 3, *Systems*, *User Guide*.

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 7.2, “Adding a Distribution to Cobbler”*.

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 GB.

The `--virt-ram=megabytes` option specifies how many MB of physical RAM a virtual guest can consume. The default is 512 MB.

7.4 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. They are useful when system-specific Kickstart templating is required or to establish that a specific system should always get specific content installed. If a client is intended for a certain 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]”, Chapter 3, *Systems*, *User Guide*.

The following command adds a system to the Cobbler configuration:

```
cobbler system add --name=string --profile=string --mac-address=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 the name of one of the profiles added in *Section 7.3, “Adding a Profile to Cobbler”*.

The `--mac-address=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`**).

7.5 Using 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”, Chapter 3, *Systems*, *User Guide*.

Kickstart variables are 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 simple by creating Kickstart files without such complexity.

7.5.1 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 the same variables are defined in both the profile and the system detail, then the system variable takes precedence.

Note

The template for the autoinstallation has syntax rules, using punctuation symbols. To avoid clashes, they need to be properly treated.

In case the autoinstallation scenario contains any shell script using variables like `$(example)`, its content should be escaped by using the backslash symbol: `\$(example)`.

If the variable named **`example`** is defined in the autoinstallation snippet, the templating engine will evaluate **`$example`** with its content. If there is no such variable, the content will be left unchanged. Escaping the `$` symbol will prevent the templating engine to perform its evaluation as an internal variable. Long scripts or strings can be escaped by wrapping them with the **`#raw`** and **`#end raw`** directives. For example:

```
#raw
#!/bin/bash
for i in {0..2}; do
 echo "$i - Hello World!"
done
#end raw
```

Also, pay attention to similar scenarios like the following:

```
#start some section (this is a comment)
echo "Hello, world"
#end some section (this is a comment)
```

Any line with a # symbol followed by a whitespace is treated as a comment and is therefore not evaluated.

For more information about Kickstart templates, refer to the Cobbler project page at:

https://fedorahosted.org/cobbler/wiki/KickstartTemplating

7.5.2 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 it.

Use the snippet by calling 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.

7.6 Using Koan

Whether you are provisioning guests on a virtual machine or reinstalling a new distribution on a running system, koan works in conjunction with Cobbler to provision systems.

7.6.1 Using Koan to Provision Virtual Systems

If you have created a virtual machine profile as documented in *Section 7.3, “Adding a Profile to Cobbler”*, 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 allocated 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.

7.6.2 Using Koan to Reinstall 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 reinstalled*:

```
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`.

7.7 Building ISOs with Cobbler

Some environments might lack PXE support. The cobbler buildiso command provides functionality to create a boot ISO image containing a set of distributions and kernels, and a menu similar to PXE network installations. Define the name and output location of the boot ISO using the **`--iso`** option.

```
    cobbler buildiso --iso=/path/to/boot.iso
```

The boot ISO includes all profiles and systems by default. Limit these profiles and systems using the **`--profiles`** and **`--systems`** options.

```
    cobbler buildiso --systems="system1,system2,system3" \
    --profiles="profile1,profile2,profile3"
```

Note

Building ISOs with the **`cobbler buildiso`** command is supported for all architectures except the s390x architecture.

A Command Line Configuration Management Tools

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 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-manager`, and `rhncfg-actions`).

Note: Tip

Whenever a configuration file is deployed via SUSE Manager, a backup of the previous file including its full path is stored 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 (`mgr-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, using the **`diff`** command to find out 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 has to be run by someone with root access.

A.1.1 General command line options

There is a manpage available, as for most command line tools. First, decide which scheduled actions should be enabled for use by system administrators. The following options enable the various scheduled action modes:

`--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 diff use.

`--disable-upload`

No file uploads allowed.

`--disable-mtime-upload`

Disable mtime upload.

`--disable-all`

Disable all options.

`--disable-run`

No scripts allowed to run.

`--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, your system is ready for configuration management through SUSE Manager. A common option is **`mgr-actions-control --enable-all`**.

A.2 Configuration Client (`mgrcfg-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
```

View the contents of the file with **`less`** or another pager. Note that the file is selected as the most relevant based on the rank of the config channel containing it. This is accomplished within the *Configuration* tab of the *System Details* page. Refer to Section “System Details”, Chapter 3, *Systems*, *User Guide* 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 list of options available for **`mgrcfg-client get`**:

`--topdir=TOPDIR`

Make all file operations relative to this string.

`--exclude=EXCLUDE`

Exclude a file from being deployed with **`get`**. May be used multiple times.

`-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:

```


rhncfg-client diff
--- /etc/test
+++ /etc/test 2013-08-28 00:14:49.405152824 +1000
@@ -1 +1,2 @@
This is the first line
+This is the second line added
```

In addition, you can 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 list of the options available for **`mgrcfg-client verify`**:

`-v, --verbose`

Increase the amount of output detail. Display differences in the mode, owner, and group permissions for the specified config file.

`-o, --only`

Only show differing files.

`-h, --help`

Show help message and exit.

A.3 Configuration Manager (**`mgrcfg-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, configuration 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 want to see:

```
mgrcfg-manager diff-revisions --help
```

Find a list of options for the add mode in *Section A.3.2, “Adding Files to a Config Channel”*.

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 can use the available options for modifying the file during its addition. For instance, you can alter the path and file name by including the `--dest-file` option in the command:

```
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 list of options available for **`mgrcfg-manager add`**:

`-c CHANNEL --channel=CHANNEL`
: Upload files in this config channel.

`-d DEST_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.

`-i, --ignore-missing`
: Ignore missing local files.

`-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 kilo 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 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 list of options available for **`mgrcfg-manager diff`**:

`-c CHANNEL, --channel=CHANNEL`

Get file(s) from this config channel.

`-r REVISION, --revision=REVISION`

Use this revision.

`-d DEST_FILE, --dest-file=DEST_FILE`

Upload the file at this path.

`-t TOPDIR, --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”* 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
+blah
+-----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 list of options available for **`mgrcfg-manager diff-revisions`**:

`-c CHANNEL, --channel=CHANNEL`

Use this config channel.

`-r REVISION, --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 list of options available for **`mgrcfg-manager download-channel`**:

`-t TOPDIR, --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 list of the options available for **`mgrcfg-manager get`**:

`-c CHANNEL, --channel=CHANNEL`

Get file(s) from this config channel.

`-t TOPDIR, --topdir=TOPDIR`

Directory to which all files are relative.

`-r REVISION, --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 list of the options available for **`mgrcfg-manager remove`**:

`-c CHANNEL, --channel=CHANNEL`

Remove files from this config channel.

`-t TOPDIR, --topdir=TOPDIR`

Directory to which all files are relative.

`-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 list of the options available for **`mgrcfg-manager update`**:

`-c CHANNEL, --channel=CHANNEL`

Upload files in this config channel.

`-d DEST_FILE, --dest-file=DEST_FILE`

Upload the file to this path.

`-t TOPDIR, --topdir=TOPDIR`

Directory to which all files are relative.

`--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=topdir channel-label
```

The output resembles the following:

```
Using config channel example-channel4
Uploading /tmp/ola_world.txt from blah4/tmp/ola_world.txt
```

The list of the options available for **`mgrcfg-manager upload-channel`**:

`-t TOPDIR, --topdir=TOPDIR`

Directory all the file paths are relative to.

`-c CHANNEL, --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.

A.4 Syncing SUSE Manager Repositories from SCC (mgr-sync)

mgr-sync is the new tool replacing **mgr-ncc-sync**. **mgr-sync** must be used, if SUSE Manager is connected to SUSE Customer Center (SCC). With **mgr-sync** you add or synchronize products and channels. It also enables and refreshes SCC data. This tool requires that SCC is enabled by running **mgr-sync enable-scc** first.

mgr-sync has a new command structure using sub-commands similar to **git** or **osc**. For a complete list of command line option, see the mgr-sync manpage (**man mgr-sync**). Basic actions are:

```
mgr-sync enable-scc


mgr-sync list channel(s)|product(s)|credentials
mgr-sync add  channel(s)|product(s)|credentials
mgr-sync delete  credentials


mgr-sync refresh [--refresh-channels] [--from-mirror MIRROR]
```

Here are some usage examples. List channels:

```
mgr-sync list channels
```

Add a channel:

```
mgr-sync add channel LABEL
```

List products:

```
mgr-sync list products
```

Add a product:

```
mgr-sync add product
```

Refresh the data:

```
mgr-sync refresh
```

Refresh the data and schedule reposync of all installed vendor channels:

```
mgr-sync refresh --refresh-channels
```

`mgr-sync` now requires username/password of a “SUSE Manager administrator”. Most of the functions are available as a public API now.

List SCC credentials:

```
mgr-sync list credentials
```

Add new SCC credentials:

```
mgr-sync add credentials
```

To add SCC primary credentials:

```
mgr-sync add credentials --primary
```

There can be one primary credential only. This is username/password used first when retrieving the list of available channels and packages.

Delete SCC credentials:

```
mgr-sync delete credentials
```

A.5 Syncing SUSE Manager Repositories from NCC (`mgr-ncc-sync`)

The now deprecated `mgr-ncc-sync` command helps with selecting repositories or channels and triggering their synchronization from NCC. NCC is now replaced with SUSE Customer Center (SCC); for more information, see *Section A.4, “Syncing SUSE Manager Repositories from SCC (`mgr-sync`)”*.

Note: Switching to SUSE Customer Center (SCC)

At the moment, you can still work with `mgr-ncc-sync` and NCC, but switching to SUSE Customer Center SCC is highly recommended. Switching to SCC and the new `mgr-sync` tool is mandatory, if you want to use SLE 12 repositories.

The list of options available for `mgr-ncc-sync`:

`-l, --list-channels`

List all the base channels available to you and child channels of already synced base channels. Use additionally the `--all-childs` option to see all available child channels.

`--list-products`

List all the products which are available for you.

`--list-products-xml`

The same as `--list-products` but in XML format.

`--add-product`

Add all mandatory channels of a product [interactive].

`-c CHANNEL, --channel=CHANNEL`

Add a new channel and trigger a reposync.

`--all-childs`

Show also child channels if the parent is not synced yet.

`--no-optional`

Do not list optional channels.

`--filter=FILTER`

Show only labels, which contains the filter word (case-insensitive). This is a new option.

`-r, --refresh`

Refresh product, channel, and subscription information without triggering any reposyncs.

`-m, --migrate_res`

Migrate to RES subscriptions.

`-q, --quiet`

Print no output, only log output.

`-d DEBUG, --debug=DEBUG`

Debugging.

`-D DUMPPATH, --dump=DUMPPATH`

Dump NCC XML data into the given directory.

`--from-dir=FROMDIR`

Read data from directory instead of NCC.

A.6 Configuring SUSE Manager's Database (smdba)

SUSE Manager provides the **`smdba`** command for managing the installed database. It is the successor of **`db-control`**, which is not supported anymore.

The **`smdba`** command works on local databases only, not remote. This utility allows you to do several administrative tasks like backing up and restoring the database, everything from creating, verifying, and restoring backups to obtaining the database status, and restart the database if necessary. The **`smdba`** command supports PostgreSQL and Oracle databases.

Find basic information about **`smdba`** in the `smdba` manpage.

Note: Restart Spacewalk Services When Connection is Lost

If you have stopped or restarted the database, it can happen that the Spacewalk services lost their connections. In such a case, run the following command:

```
spacewalk-service restart
```

A.6.1 Control Options

Depending on the database installed, **`smdba`** provides several subcommands:

EXAMPLE A.1: AVAILABLE OPTIONS ON A MACHINE WITH AN ORACLE DATABASE

```
backup-list        List of available backups.
backup-restore     Restore the SUSE Manager Database from backup.
db-start           Start SUSE Manager database.
db-status          Get SUSE Database running status.
db-stop            Stop SUSE Manager database.
listener-restart   Restart SUSE Database Listener.
listener-start     Start the SUSE Manager Database listener.
listener-status    Show database status.
listener-stop      Stop the SUSE Manager Database listener.
space-overview     Show database space report.
```

```
space-reclaim     Free disk space from unused object in tables
                  and indexes.
space-tables      Show space report for each table.
stats-overview    Show tables with stale or empty statistics.
stats-refresh     Gather statistics on SUSE Manager Database
                  database objects.
system-check      Common backend healthcheck.
```

EXAMPLE A.2: AVAILABLE OPTIONS ON A MACHINE WITH A POSTGRESQL DATABASE

```
backup-check            Check the consistency of the backup.
backup-hot              Perform hot backup on running database.
backup-list             List of available backups.
backup-purge            Purge all backups. Useful after successfull reliable
                        recover from the disaster.
backup-restore          Restore the SUSE Manager database from backup.
db-check                Check full connection to the database.
db-start                Start SUSE Manager database.
db-status               Display SUSE Manager database runtime status.
db-stop                 Stop SUSE Manager database.
listener-restart        Restart SUSE Manager database listener.
listener-start          Start the SUSE Manager database listener.
listener-status         Show database status.
listener-stop           Stop the SUSE Manager database listener.
space-overview          Show database space report.
space-reclaim           Free disk space from unused object in tables and
                        indexes.
space-tables            Show space report for each table.
stats-overview          Show tables with stale or empty statistics.
stats-refresh           Gather statistics on SUSE Manager database objects.
system-check            Common backend healthcheck.
```

For a list of available commands on your particular appliance, call **`smdba help`**. Each subcommand can contain different options depending on the database used. To display the help message for a specific subcommand, call **`smdba`** *`COMMAND`* **`help`**.

A.6.2 Starting and Stopping the Database

There are three commands to start, stop, or get the status of the database. These commands work with both databases. Use the following commands:

```
# smdba db-status
Checking database core...       online
# smdba db-stop
Stopping the SUSE Manager database...
Stopping listener:     done
Stopping core:         done
# smdba db-status
Checking database core...       offline
# smdba db-start
Starting listener:     done
Starting core...       done
```

B Probes

As described in Chapter 11, *Monitoring — [Mon]*, *User Guide*, monitoring-entitled systems can have probes applied that constantly check 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"* 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 might 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. 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.

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 different 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
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 other 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.

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 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 oracle website for more details about BEA's community string naming conventions: http://docs.oracle.com/cd/E13222_01/wls/docs81/snmpman/snmpagent.html#1072184↗.

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
BEA Domain Admin Server	
BEA Server Name*	myserver
Queue Name*	default
Critical Maximum Idle Execute Threads	
Warning Maximum Idle Execute Threads	

Field	Value
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
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
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
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	
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 UNKNOWN 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
Timeout*	10
Critical Maximum Latency	

Field	Value
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	
Critical Minimum Input Rate	

Field	Value
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()`**) while the 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	

Field	Value
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	

Field	Value
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	
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* check box is selected.

By default, the check box 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	
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 closing 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	

Field	Value
Critical Maximum CLOSE_WAIT Connections	
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
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	

Field	Value
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	

Field	**Value**
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	
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. See 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	
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

Field	Value
Timeout	15
Critical Maximum Query Rate	
Warning Maximum Query Rate	
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 state 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 resolve 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 after 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 after 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
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"*.

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	
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 a different port number than `110` overrides this default port. 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

Field	Value
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”*.

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

Field	Value
Critical Maximum Round-Trip Average	
Warning Maximum Round-Trip Average	
Critical Maximum Packet Loss	
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 an 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	
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	
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	
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 checks 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 an `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 state 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
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*	

Field	Value
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*	

Field	Value
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*	
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
ORACLE_HOME*	/opt/oracle
Expected DB Name*	

Field	Value
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*	
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
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

Field	Value
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	

Field	Value
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 that must now retrieve the object of the disk. These pins are made up of objects with previous pins from the time the object handle was created .

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

Field	Value
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	
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	
Warning Maximum Threads	
Critical Maximum Physical Memory Used	
Warning Maximum Physical Memory Used	

Field	Value
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	

C Minimalist AutoYaST Profile for Automated Installations and Useful Enhancements

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 SUSE Manager. 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>
```

Use the following enhancement fragment to add child channels:

```
<add-on>
 <add_on_products config:type="list">
  <listentry>
   <ask_on_error config:type="boolean">true</ask_on_error>
   <media_url>http://$c_server/ks/dist/child/channel-label/distribution-label</
media_url>
   <name>$c_name</name>
   <product>$c_product</product>
   <product_dir>/</product_dir>
  </listentry>
...
 </add_on_products>
</add-on>
```

Replace *`channel-label`* and *`distribution-label`* with actual labels such as `sles11-sp1-updates-x86_64` and `sles11-sp2-x86_64`, and set the variables (`$c_server`, etc.) according to your environment. For information about variable, see Section “Autoinstallation > Distributions > Variables”, Chapter 3, *Systems*, *User Guide*.

D About SUSE Manager and Spacewalk

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 Satellite or a Spacewalk server to SUSE Manager. 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 AutoYaST.

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	**yum update**	**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**
XML im- and exporter between identical SUSE Manager servers	**rhn-satellite-exporter**	**mgr-exporter**

E List of Client Tools Channels

This section contains a list of currently (2015) available Client Tools Channels.

```
SLES for SAP 11 SP1: sles11-sp1-suse-manager-tools-x86_64-sap-aio
SLES for SAP 11 SP2: sles11-sp2-suse-manager-tools-x86_64-sap-aio
SLES for SAP 11 SP3: sles11-sp3-suse-manager-tools-x86_64-sap-sp3
SLES for SAP 11 SP4 <arch>: sles11-sp4-suse-manager-tools-<arch>-sap-sp4

studioonsite-1.3: sles11-sp2-suse-manager-tools-x86_64-studio13

SLED11 SP2 i586:   sled11-sp2-suse-manager-tools-i586
SLED11 SP2 x86_64: sled11-sp2-suse-manager-tools-x86_64

SLED11 SP3 i586:   sles11-sp3-suse-manager-tools-i586-sled-sp3
SLED11 SP3 x86_64: sles11-sp3-suse-manager-tools-x86_64-sled-sp3

SLED11 SP4 i586:   sles11-sp4-suse-manager-tools-i586-sled-sp4
SLED11 SP4 x86_64: sles11-sp4-suse-manager-tools-x86_64-sled-sp4

SLES10 SP3 <arch>: sle10-sp3-suse-manager-tools-<arch>
SLES10 SP4 <arch>: sle10-sp4-suse-manager-tools-<arch>

SLES11 SP1 <arch>: sles11-sp1-suse-manager-tools-<arch>
SLES11 SP2 <arch>: sles11-sp2-suse-manager-tools-<arch>
SLES11 SP3 <arch>: sles11-sp3-suse-manager-tools-<arch>
SLES11 SP4 <arch>: sles11-sp4-suse-manager-tools-<arch>

SUSE Manager Proxy 1.2: sles11-sp1-suse-manager-tools-x86_64-proxy
1.7 and 2.1 have the client tools packages included in the Proxy-Pool

RES5 i386:   res5-suse-manager-tools-i386
RES5 x86_64: res5-suse-manager-tools-x86_64

RES6 i386:   res6-suse-manager-tools-i386
RES6 x86_64: res6-suse-manager-tools-x86_64
```

```
RES7 x86_64: res7-suse-manager-tools-x86_64

SLES12 <arch>: sle-manager-tools12-pool-<arch> +
               sle-manager-tools12-updates-<arch>

     optional: sle-manager-tools12-debuginfo-pool-<arch>
               sle-manager-tools12-debuginfo-updates-<arch>
```

F Changes

F.1 Changes from Version 1.7 to Version 2.1

Version 2.1 of SUSE Manager adds the following new features:

- **Base system upgrade to SUSE Linux Enterprise Server 11 SP3:** The underlying SUSE Linux Enterprise Server 11 base system has been upgraded to Service Pack 3 (including updates).

- **Upgrade to upstream Spacewalk 2.1:** The SUSE Manager code has been updated to reflect the 2.1 release of the upstream Spacewalk project (including updates).

- **Non-compliant systems:** The semantics of non-compliant systems have changed. A system is considered non-compliant if it has packages installed which are not available in a channel. A non-compliant system cannot be reinstalled. The old semantics looked for packages in all available channels. The new semantics look for packages only in channels assigned to the system.

- **Channel synchronization logging:** Logging of channel synchronization, triggered by **`mgr-ncc-sync`**, was done per channel and sync run. Every new sync created a new log file. A cron job was used to clean up older log files. With SUSE Manager 2.1 there is only one log file per channel. All synchronization runs for a specific channel log to the same file. Older log files are rotated and compressed now, using logrotate.

- **Inter-Server Sync between 1.7 (master) and 2.1 (slave):** An inter-server synchronization (ISS) between a SUSE Manager 1.7 Server as master and a SUSE Manager 2.1 Server as client will succeed but generate an error mail to the administrator. The error email is harmless and can be deleted.

- **Embedded Oracle DB needs extra permission:** When upgrading a SUSE Manager Server with Database 1.7 (using embedded Oracle DB), an additional permission (create role) will be added.

- **New package `pgtcl`:** Stored procedures in PostgreSQL can now be written in the TCL language. The package `pgtcl` will be added on upgrade.

- **Reboot action status is reflected immediately in the Web interface:** The status of a rebooted client is now updated immediately. In the past, there was a delay in the status update.

G Documentation Updates

This section contains information about documentation content changes made to the *Reference Guide*.

This document was updated on the following dates:

- *Section G.1, “September 25, 2015”*
- *Section G.2, “February 12, 2015”*
- *Section G.3, “December 5, 2014”*
- *Section G.5, “May 7, 2014”*
- *Section G.6, “April 1, 2014”*
- *Section G.7, “March 28, 2014”*
- *Section G.8, “November 22, 2013”*
- *Section G.9, “September 9, 2013”*
- *Section G.10, “August 23, 2013”*
- *Section G.11, “January 25, 2013”*
- *Section G.12, “November 28, 2012”*

G.1 September 25, 2015

Updates were made to the following section. The changes are explained below.

Appendix E, List of Client Tools Channels

New appendix.

G.2 February 12, 2015

Updates were made to the following section. The changes are explained below.

Section A.6.1, "Control Options"

Enhance list for PostgreSQL.

G.3 December 5, 2014

Updates were made to the following section. The changes are explained below.

Section 7.1, "Cobbler Requirements"

Remove misleanding statement about `cobbler-loaders`.

Section A.4, "Syncing SUSE Manager Repositories from SCC (`mgr-sync`)"

New section.

Section A.5, "Syncing SUSE Manager Repositories from NCC (`mgr-ncc-sync`)"

Switching to SUSE Customer Center (SCC) and **`mgr-sync`** is recommended.

G.4 May 9, 2014

Updates were made to the following sections. The changes are explained below.

Glossary

Several new entries in the glossary.

G.5 May 7, 2014

Updates were made to the following sections. The changes are explained below.

Section F.1, "Changes from Version 1.7 to Version 2.1"

Changes in SUSE Manager 2.1.

G.6 April 1, 2014

Updates were made to the following sections. The changes are explained below.

Section 5.4.2, “Admin > Subscriptions > System Entitlements”

Entitlement descriptions have been added to the multi-org chapter.

G.7 March 28, 2014

The Web Interface chapter has been moved from the Reference Guide to the new User Guide.

G.8 November 22, 2013

Updates were made to the following sections. The changes are explained below.

Section 2.1.2, “Updating Packages from the Command Line with Zypper”

Use a `zypper` option as an example that is less confusing in the context of this product.

Section “System Details > Software > SP Migration — [Mgmt] ”, Chapter 3, *Systems*, *User Guide*

Add warning about one-way migration procedure.

Section “ System Details > Provisioning > Snapshots — [Prov]”, Chapter 3, *Systems*, *User Guide*

Add background information about snapshots.

Rolling back an SP migration is not supported.

Section “Autoinstallation > Autoinstallation Snippets — [Prov]”, Chapter 3, *Systems*, *User Guide*

Add more information about autoinstallation snippets.

Section 7.1, “Cobbler Requirements”

SUSE Manager provides the required TFTP server by default.

Appendix C, Minimalist AutoYaST Profile for Automated Installations and Useful Enhancements

Add information about listing child channels in AutoYaST profiles.

Section 4.1, “Prerequisites”

New procedure about enabling monitoring.

G.9 September 9, 2013

Updates were made to the following sections. The changes are explained below.

Section “OpenSCAP”, Chapter 6, *Audit*, *User Guide*

Add a pointer to Chapter 7, *System Security via OpenSCAP*, *User Guide*.

Chapter 7, *System Security via OpenSCAP*, *User Guide*

New chapter.

G.10 August 23, 2013

Updates were made to the following sections. The changes are explained below.

G.10.1 SUSE Manager Web Interface

Section “Categories and Pages”, Chapter 2, *Web Interface — Navigation and Overview*, *User Guide*

Add new pages.

Section “Your Preferences”, Chapter 2, *Web Interface — Navigation and Overview*, *User Guide*

Add *CVS Files*.

Chapter 6, *Audit*, *User Guide*

New section with Section “CVE Audit”, Chapter 6, *Audit*, *User Guide*.

Section “Configuration Files”, Chapter 8, *Configuration*, *User Guide*

Clarify the location of configuration files.

Section “*Admin > SUSE Manager Configuration*”, Chapter 12, *Admin*, *User Guide*

The section about *Certificate* uploading is gone. SUSE Manager does not support this feature, because it does not need it.

Section “*Admin > SUSE Manager Configuration > Cobbler*”, Chapter 12, *Admin*, *User Guide*

New section.

G.10.2 Monitoring

Section 4.3, “Enabling Notifications”

Change wording for clarity.

G.10.3 Cobbler

Section 7.1.4, “Syncing TFTP Contents to SUSE Manager Proxies”

This section is new.

G.10.4 Command Line Configuration Management Tools

Appendix A, Command Line Configuration Management Tools

Fix white-space issues in command listings.

Section A.5, “Syncing SUSE Manager Repositories from NCC (`mgr-ncc-sync`)”

This section is new.

Section A.6, “Configuring SUSE Manager's Database (smdba)”

This section is new. Contents taken over from Section “Configuring SUSE Manager's Database (smdba)”, Chapter 8, *Maintenance*, *Installation & Troubleshooting Guide*.

G.10.5 Changes

Appendix F, Changes

This appendix is new. Contents taken over from Chapter 4, *Installation*, *Installation & Troubleshooting Guide*.

G.11 January 25, 2013

Updates were made to the following sections. The changes are explained below.

G.11.1 SUSE Manager Web Interface

Section “Actions List”, Chapter 9, *Schedule*, *User Guide*

This section is new.

Section “Introduction to AutoYaST”, Chapter 3, *Systems*, *User Guide*

Better formatting for clarity.

Section “*Admin > SUSE Manager Configuration > General*”, Chapter 12, *Admin*, *User Guide*

Mention proxy configuration option.

G.12 November 28, 2012

Updates were made to the following sections. The changes are explained below.

G.12.1 SUSE Manager Web Interface

Section “System Details > Software > SP Migration — [Mgmt] ”, Chapter 3, *Systems*, *User Guide*

This section is new.

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.

Activation Key Administrator

The activation key administrator manages the collection of activation keys. A user with this role assigned can modify and delete any key within the organization.

Base Channel

A base channel is a type of *Channel* 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* 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* and can be subscribed to one or more *Child Channel*.

Channel Administrator

A user role with full access to channel management capabilities. Users with this role can 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* associated with a *Base Channel* 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.

Email Notification

Similar to a *Patch Alert* , except the information is delivered via email. If the email notifications option is selected, notifications are sent for every *Patch Alert*. The email includes the type of the patch alert, summary of the patches, description of the patch, and a list of systems affected by the alert.

Enhancement Alert

A *Patch Alert* 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.

Monitoring

Monitoring consists of two components: the monitoring system and the monitoring scout. The monitoring system is installed on the SUSE Manager and performs backend functions such as storing monitoring data and acting on it. The monitoring scout runs all the probes and collects monitoring data.

Monitoring Administrator

Users with this role assigned can schedule probes and supervise the monitoring infrastructure (only available on monitoring-enabled systems).

Notification Method

An email 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 organization'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* 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 tracks the bug reports 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, the patch is complete and is placed on the SUSE file server for distribution and installation.

Patch Alert

An alert updates packages containing SUSE patches 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 system's adherence to a probe's 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*.

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*.

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* list to a client system without user intervention. If this feature is selected, packages are delivered via the *SUSE Manager Daemon* running on the client system.

Security Alert

A *Patch Alert* 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.

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* and *Digital Certificate*. 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 Group Administrator

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.

System ID

A unique string of characters and numbers that identifies a registered system. It is stored in the system's *Digital Certificate*.

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* 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.

Traceback

A traceback is a detailed error message for troubleshooting SUSE Manager. SUSE Manager automatically generates tracebacks when a critical error occurs and sends mails the individual(s) designated in the SUSE Manager configuration file.

Update

One of the Novell Customer Center service level offerings.

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*.

`Zypper`

A command line tool on SUSE Linux Enterprise systems. Use `zypper` to install, update, or remove software packages, and to manage repositories from the command line.