

SUSE Manager

1.2

www.novell.com

February 21, 2011

Installation Guide



Installation Guide

Copyright © 2011 Novell, Inc.

Copyright © 2011 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution-Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at <http://creativecommons.org/licenses/by-sa/3.0/>. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, MetaMatrix, Fedora, the Infinity Logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries. Linux® is the registered trademark of Linus Torvalds in the United States and other countries. Java® is a registered trademark of Oracle and/or its affiliates. XFS® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries. MySQL® is a registered trademark of MySQL AB in the United States, the European Union and other countries. All other trademarks are the property of their respective owners.

For Novell trademarks, see the Novell Trademark and Service Mark list <http://www.novell.com/company/legal/trademarks/tmlist.html>. Linux* is a registered trademark of Linus Torvalds. All other third party trademarks are the property of their respective owners. A trademark symbol (®, ™ etc.) denotes a Novell trademark; an asterisk (*) denotes a third party trademark.

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	v
1 Conceptual Overview	1
2 Example Topologies	5
2.1 Single SUSE Manager Topology	5
2.2 Multiple SUSE Manager Horizontally Tiered Topology	6
2.3 SUSE Manager-Proxy Vertically Tiered Topology	7
3 Requirements	9
3.1 External Database Requirements	9
3.2 Additional Requirements	11
3.3 Additional Documentation	13
4 Installation	15
4.1 Summary of Steps	15
5 Troubleshooting	19
5.1 Log Files	19
5.2 General Problems	21
5.3 Host Not Found/Could Not Determine FQDN	22
5.4 Connection Errors	23
5.5 SUSE Manager Debugging	24

6	Maintenance	27
6.1	Managing SUSE Manager with spacewalk-service	27
6.2	Updating SUSE Manager	28
6.3	Backing Up SUSE Manager	29
6.4	Using DB Control	31
6.5	Cloning SUSE Manager with the embedded database	35
6.6	Establishing Redundant SUSE Manager server with stand-alone database	36
6.7	Changing the SUSE Manager Hostname	38
6.8	Conducting SUSE Manager-Specific Tasks	38
6.9	Automating Synchronization	41
6.10	Implementing PAM Authentication	42
6.11	Enabling Push to Clients	43

About This Guide

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

This guide is intended for system administrators.

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

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

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

NOTE: Obtaining the Release Notes

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

1 Available Documentation

The following manuals are available on this product:

Quick Start (↑Quick Start)

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

Installation Guide (page 1)

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

Client Configuration Guide (↑Client Configuration Guide)

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

Reference Guide (↑Reference Guide)

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

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

2 Feedback

Several feedback channels are available:

Bugs and Enhancement Requests

For services and support options available for your product, refer to <http://www.novell.com/services/>.

To report bugs for a product component, please use <http://support.novell.com/additional/bugreport.html>.

Submit enhancement requests at <https://secure-www.novell.com/rms/rmsTool?action=ReqActions.viewAddPage&return=www>.

User Comments

We want to hear your comments and suggestions about 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.novell.com/documentation/feedback.html> and enter your comments there.

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 shown in uppercase as on a keyboard
- *File*, *File > Save As*: menu items, buttons
- **► amd64 em64t**: This paragraph is only relevant for the specified architectures. The arrows mark the beginning and the end of the text block. **◄**
- *Dancing Penguins* (Chapter *Penguins*, ↑Another Manual): This is a reference to a chapter in another manual.

Conceptual Overview

SUSE Manager provides a solution to organizations requiring absolute control over and privacy of the maintenance and package deployment of their servers. It allows customers the greatest flexibility and power in keeping servers secure and updated.

Two types of SUSE Manager are available: One with a stand-alone database on a separate machine and one with an embedded database installed on the same machine as SUSE Manager. This guide describes the installation of both types of SUSE Manager.

Although the two types of SUSE Manager are functionally similar, some differences do exist. These variations are primarily isolated to hardware requirements, installation steps, and maintenance activities. They may also appear during troubleshooting. This guide identifies distinctions between the SUSE Manager types by marking the differing instructions as either *Stand-Alone Database* or *Embedded Database*.

SUSE Manager consists of the following components:

- Database — for the stand-alone, remote database, this may be the organization's existing database or, preferably, a separate machine. For a list of supported database versions, refer to the system requirements section. For the embedded database, the database comes bundled with SUSE Manager server and is installed on the same machine as SUSE Manager during the installation process.
- SUSE Manager — core “business logic” and entry point for the update agent running on client systems (either Red Hat Update Agent on Red Hat Enterprise Linux clients or zypper on SUSE Linux Enterprise clients). The SUSE Manager server also includes an Apache HTTP Server (serving XML-RPC requests).

- SUSE Manager Web interface — advanced system, system group, user, and channel management interface.
- RPM Repository — repository for default packages (and custom RPM packages identified by the organization).
- Management Tools:
 - Database and file system synchronization tools
 - RPM importing tools
 - Channel maintenance tools (Web-based)
 - Patch management tools (Web-based)
 - User management tools (Web-based)
 - Client system and system grouping tools (Web-based)
 - An update agent on the client systems

The update agent on the client systems must be reconfigured to retrieve updates from the organization's internal SUSE Manager server. After this one-time reconfiguration, client systems may retrieve updates locally using the update agent, or system administrators may schedule actions through the SUSE Manager website.

IMPORTANT: Latest Updates on Client Systems

It is strongly recommended to install the latest system updates on any client system connected to SUSE Manager to ensure proper connectivity.

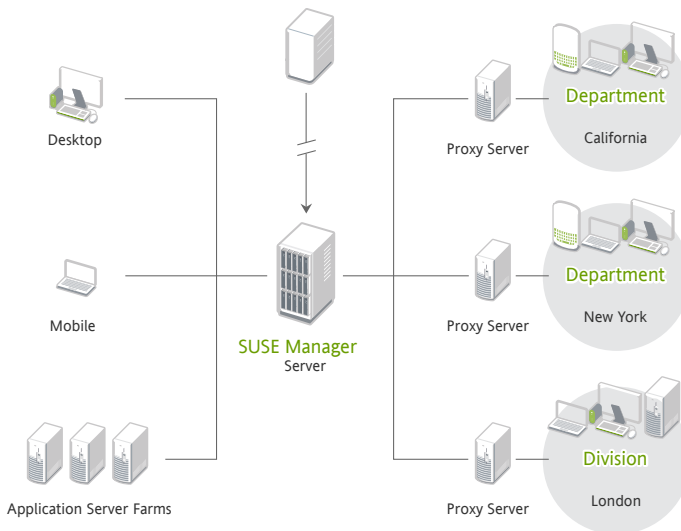
When a client requests updates, the organization's internal SUSE Manager server queries its database, authenticates the client system, identifies the updated packages available for the client system, and sends the requested RPMs back to the client system. Depending upon the client's preferences, the package may also be installed. If the packages are installed, the client system sends an updated package profile to the SUSE Manager database; those packages are removed from the list of outdated packages for the client.

The organization can configure the website for the SUSE Manager server to be accessible from the local area network only or from both the local area network and the Internet. Both setups allow full control over client systems, system groups, and users.

The SUSE Manager management tools are used to synchronize the SUSE Manager database and package repository with Novell Customer Center. The SUSE Manager import tool allows the system administrator to include custom RPM packages in the package repository.

SUSE Manager can be used in conjunction with a SUSE Manager Proxy Server to deliver a distributed, self-contained deployment for the organization. For example, an organization can maintain one SUSE Manager in a secure location. Any client systems with local network access to the SUSE Manager can connect to it. Other remote offices can maintain SUSE Manager proxy server installations that connect to the SUSE Manager server. The different locations inside the organization must be networked, but this can be a private network; an Internet connection is not required for any of the systems.

Figure 1.1 *Using SUSE Manager and SUSE Manager Proxy Server Together*



For an explanation of key terms in the SUSE Manager context, refer to Glossary (↑Reference Guide).

Example Topologies

SUSE Manager can be configured in multiple ways. Select one method depending on the following factors:

- The total number of client systems to be served by SUSE Manager.
- The maximum number of clients expected to connect *concurrently* to .
- The number of custom packages and channels to be served by SUSE Manager.
- The number of SUSE Managers being used in the customer environment.

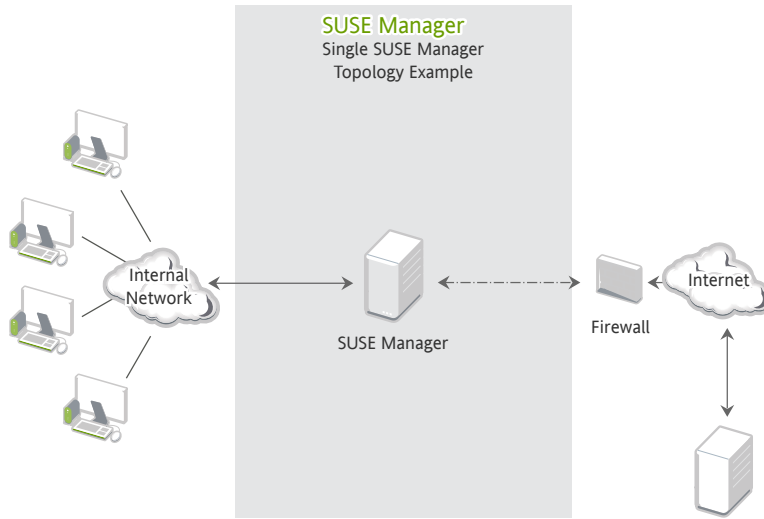
The rest of this chapter describes possible configurations and explains their benefits.

2.1 Single SUSE Manager Topology

The simplest configuration is to use a single SUSE Manager to serve your entire network. This configuration is adequate to service a medium-size group of clients and network.

The disadvantage of using one SUSE Manager is that performance will be compromised as the number of clients requesting packages grows.

Figure 2.1 *Single SUSE Manager Topology*

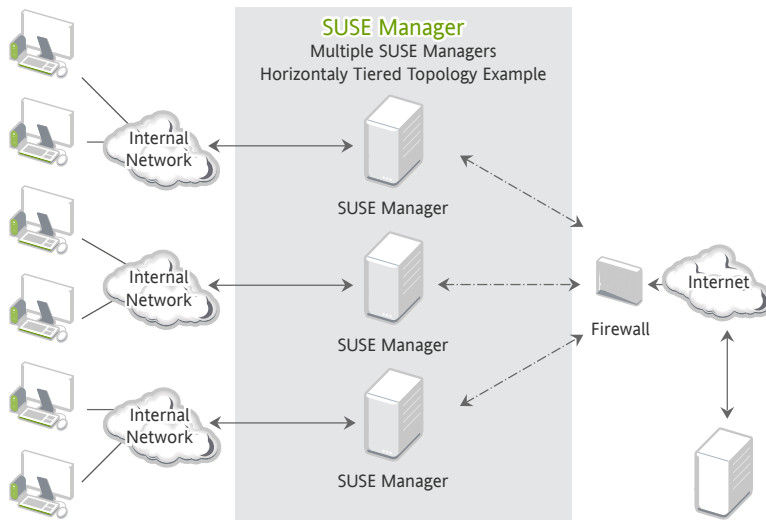


2.2 Multiple SUSE Manager Horizontally Tiered Topology

For very large networks, a more distributed method may be needed, such as having multiple SUSE Managers in a horizontally tiered configuration and balancing the load of client requests.

Additional maintenance is the biggest disadvantage of this horizontal structure.

Figure 2.2 *Multiple SUSE Manager Horizontally Tiered Topology*



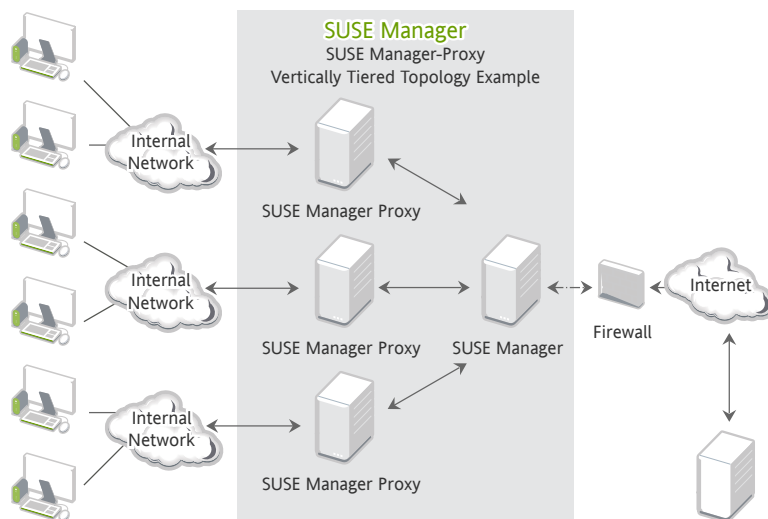
2.3 SUSE Manager-Proxy Vertically Tiered Topology

An alternative method to balance load is to install SUSE Manager Proxy Servers below a SUSE Manager. These Proxies connect to the SUSE Manager for RPMs from Novell Customer Center and custom packages created locally. In essence, the Proxies act as clients of the SUSE Manager.

This vertically tiered configuration requires that channels and RPMs be created only on the SUSE Manager. In this manner, the Proxies inherit and then serve packages from a central location.

Similarly, you should make the Proxies' SSL certificates clients of the SUSE Manager while also setting them to serve the client systems. This process is described in the Client Configuration Guide.

Figure 2.3 *SUSE Manager-Proxy Vertically Tiered Topology*



Requirements

For requirements and prerequisites to be met before installation, refer to Section “System Requirements” (↑Quick Start) and Section “Prerequisites” (↑Quick Start). If you want to use SUSE Manager with an external database, refer to Section 3.1, “External Database Requirements” (page 9).

3.1 External Database Requirements

This section applies only to SUSE Manager if used in conjunction with a stand-alone database as the requirements for the embedded database are included in Section “System Requirements” (↑Quick Start). The stand-alone Database must not run on the same server as the SUSE Manager.

A single 6 GB tablespace is recommended as more than sufficient for most installations. It is possible for many customers to function with a smaller tablespace. An experienced Oracle database administrator (DBA) will be necessary to assess sizing issues. However, keep in mind that the exact size of the database depends on many factors, like number of systems managed, numbers of packages installed on the average system, and numbers of packages imported. If you have 1000 packages this needs approximately 100 MB in the database. Due to these factors, database storage may grow rapidly.

Although you should be generous in your database sizing estimates, you must consider that size affects the time to conduct backups and adds load to other system resources. If the database is shared, its hardware and spacing are entirely dependent on what else is using it.

Additionally, block sizes must be a minimum of 8 KB for SUSE Manager to install properly.

The Oracle database should have a user assigned to SUSE Manager with full DDL and DML access to that user's default tablespace. The user needs standard connection information for the database at the time of installation.

The precise access levels required by the Oracle user are as follows:

- ALTER SESSION
- CREATE SEQUENCE
- CREATE SYNONYM
- CREATE TABLE
- CREATE VIEW
- CREATE PROCEDURE
- CREATE TRIGGER
- CREATE TYPE
- CREATE SESSION

Additional database requirements include:

- Security Identifier (SID)
- Listener Port
- Username
- UTF-8 character set

Two additional *suggested* recommendation for user's default tablespace include:

- Uniform Extent Size
- Auto Segment Space Management

NOTE

Ensure that the NLS/charset setting is set to "UTF8" when using an external database, not 'AL32UTF8' or other charsets. Using other charsets may lead to problems later.

The disk layout on the database machine is independent of SUSE Manager and entirely up to the customer.

3.2 Additional Requirements

The following additional requirements must be met before the SUSE Manager installation:

IMPORTANT: Network Setup

For correct installation and setup of SUSE Manager, make sure the following requirements are fulfilled:

Fully Qualified Domain Name (FQDN)

The system on which to install SUSE Manager must resolve its own FQDN properly. If this is not the case, cookies will not work properly on the Web interface.

Hostname and IP Address

To guarantee that SUSE Manager's domain name can be resolved by its clients, the server and the client machines must be linked to a working Domain Name Server (DNS) server in the customer environment.

The hostname of the SUSE Manager server must not contain uppercase letters as this might cause `jabberd` to fail.

- Full Access

Client systems need full network access to the SUSE Manager solution's services and ports.

- Firewall Rules

We strongly recommend firewalling the SUSE Manager solution from the Internet.

- Synchronized System Times

The connection to the Web server via Secure Sockets Layer (SSL) requires correct timing of both server and clients. For this reason, SUSE Manager server and all client systems must use NTP. If SUSE Manager is used in conjunction with a stand-alone database, the machine of the separate database must be set to the same time zone as SUSE Manager.

- An Novell Customer Center Account

For using SUSE Manager, you need an account at the Novell Customer Center (NCC) where your purchased products and product subscriptions are defined.

- Backups of login information in multiple secure places

Record all relevant usernames, passwords and other login information. For SUSE Manager, this includes usernames and passwords for the Organization Administrator account, the primary administrator account on SUSE Manager itself, SSL certificate generation, and database connection (which also requires a SID, or net service name). We strongly recommend this information be copied onto two separate electronic media, printed out on paper, and stored in a fireproof safe.

In addition to these requirements, it is recommended to configure SUSE Manager in the following manner:

- The entire SUSE Manager solution should be protected by a firewall if the SUSE Manager server accesses or is accessed via the Internet. An Internet connection is not required for SUSE Manager servers running in completely disconnected environments.
- All unnecessary ports should be firewalled off. Client systems connect to SUSE Manager over ports 80, 443, and 4545 (if monitoring is enabled). In addition, if you plan to enable the pushing of actions from SUSE Manager to client systems, as described in Section 6.11, “Enabling Push to Clients” (page 43), you must allow inbound connections on port 5222. Finally, if SUSE Manager will also push to a SUSE Manager proxy, you must also allow inbound connections on port 5269.
- No system components should be directly, publicly available. No user other than the system administrators should have shell access to these machines.

- All unnecessary services should be disabled using `chkconfig`.
- The `httpd` service should be enabled.
- If SUSE Manager serves monitoring-entitled systems and you wish to acknowledge via email the alert notifications you receive, you must have installed and configured a mail transfer agent such as `sendmail` or `postfix` to properly handle incoming mail. This can be done with YaST.

3.3 Additional Documentation

Apart from this Installation Guide, more documentation is available (as a reference or tailored to specific administration tasks). For an overview, refer to About This Guide (page v).

Installation

SUSE Manager is a management server application combined with an operating system (appliance). It can be deployed on industry hardware or in a virtual environment and used in conjunction with an embedded or a stand-alone database.

If your future SUSE Manager server is connected to the Internet, it will receive any updates directly from the Novell Customer Center. For a disconnected setup scenario, configure SUSE Manager to receive any updates from an internal update server (like SMT) instead.

Installation and basic configuration of SUSE Manager is covered in Quick Start (↑Quick Start). It is task-based and guides you through all required steps, from basic installation and setup through basic configuration.

4.1 Summary of Steps

The following overview lists the installation and setup scenarios covered in the Quick Start. The overview includes all required steps for basic installation, setup and configuration of SUSE Manager. Additionally, it covers a list of common administration tasks that you might need afterward.

4.1.1 Installation and Setup

Setup From Scratch—With Internet Connection

For installation and initial setup, you need to execute the following basic steps:

1. If using a stand-alone database: Preparing your database instance according to the formula provided in Chapter 3, *Requirements* (page 9).
2. Procedure “Installing the Appliance” (↑Quick Start)
3. Procedure “Setting Up SUSE Manager” (↑Quick Start)

Setup From Scratch—Without Internet Connection

For installation and initial setup, execute the same basic steps as listed above, but skip the registration of the product at NCC. For details, see Step 10 (↑Quick Start) in Procedure “Installing the Appliance” (↑Quick Start).

During basic configuration, the setup of Novell channels differs from the standard procedure: Instead of importing channels from NCC, you need to create custom channels, and add repositories to be synchronized with the custom channel. For details, refer to Section “Channels” (↑Reference Guide) and the section called “*Manage Software Channels > Manage Repositories*” (↑Reference Guide), respectively.

Migration from a Satellite Server

Instead of setting up a SUSE Manager server from scratch, you can also migrate from an existing Satellite server. For details, refer to Section “Server Migration” (↑Quick Start).

4.1.2 Basic Configuration

To complete the basic SUSE Manager configuration, you need to execute the following steps:

1. Procedure “Creating the SUSE Manager Administrator Account” (↑Quick Start)
2. Procedure “Importing Novell Channels from NCC” (↑Quick Start)

In case of disconnected setup with an internal update server like SMT, you need to create custom channels, and add repositories to be synchronized with the custom channels.

3. Procedure “Creating Activation Keys” (↑Quick Start)
4. Procedure “Generating the Bootstrap Script” (↑Quick Start)

5. Procedure “Editing the Bootstrap Script and Registering Clients” (↑Quick Start)

The following tasks are not part of the initial installation, setup, and configuration but they represent common tasks for basic administration and further configuration:

- Section “Organization Management” (↑Quick Start)
- Section “Management of System and Software Entitlements” (↑Quick Start)
- Section “User Management” (↑Quick Start)

After SUSE Manager is populated with standard channels and packages and all clients are connected to it, you may begin creating and serving custom channels and packages. Once the custom RPMs are developed, you can import them into SUSE Manager using `mgrpush`. In the SUSE Manager Web interface, add custom channels in which to store them.

As can be seen from the overview above, implementing a fully functional SUSE Manager requires more than installing software and a database. Many tasks extending beyond the basic installation and setup are covered in detail in other guides. For a full list of available documentation for this product, refer to About This Guide (page v).

Troubleshooting

This chapter provides tips for determining the cause of and resolving the most common errors associated with SUSE Manager. For services and support options available for your product, refer to <http://www.novell.com/services/>.

In addition, you may package configuration information and logs from SUSE Manager and send them to Novell for further diagnosis. Refer to Section 5.5, “SUSE Manager Debugging” (page 24) for instructions.

5.1 Log Files

Virtually every troubleshooting step should start with a look at the associated log file or files. These provide invaluable information about the activity that has taken place on the device or within the application that can be used to monitor performance and ensure proper configuration. See Table 5.1, “Log Files” (page 20) for the paths to all relevant log files:

NOTE

There may be numbered log files (such as `/var/log/rhn/rhn_satellite_install.log.1`, `/var/log/rhn/rhn_satellite_install.log.2`, etc.) within the `/var/log/rhn/` directory. These are *rotated* logs, which are log files created with a `.<NUMBER>` extension when the current `rhn_satellite_install.log` file fills up to a size as specified by the `logrotate(8)` daemon and the contents written to a rotated log file. For example, the `rhn_satellite_install.log.1`

contains the oldest rotated log file, while `rhn_satellite_install.log` .4 contains the most recently rotated log.

Table 5.1 *Log Files*

Component/Task	Log File Location
Apache Web server	<code>/var/log/httpd/</code> directory
SUSE Manager	<code>/var/log/rhn/</code> directory
SUSE Manager Installation	<code>/var/log/susemanager_setup.log</code>
Database installation (<i>Embedded Database</i>)	<code>/var/log/rhn/install_db.log</code>
Database population	<code>/var/log/rhn/populate_db.log</code>
SUSE Manager Synchronization Tool	<code>/var/log/rhn/mgr-ncc-sync.log</code>
Monitoring infrastructure	<code>/var/log/nocpulse/</code> directory
Monitoring notifications	<code>/var/log/notification/</code> directory
Task Engine (taskomatic)	<code>/var/log/messages</code>
yum	<code>/var/log/yum.log</code>
zypper	<code>/var/log/zypper.log</code>
XML-RPC transactions	<code>/var/log/rhn/rhn_server_xmlrpc.log</code>

5.2 General Problems

To begin troubleshooting general problems, examine the log file or files related to the component exhibiting failures.

A common issue is full disk space. An almost sure sign of this is the appearance of halted writing in the log files. If logging stopped during a write, such as mid-word, you likely have filled disks. To confirm this, run this command and check the percentages in the *Use%* column:

```
df -h
```

In addition to log files, you can obtain valuable information by retrieving the status of your SUSE Manager and its various components. This can be done with the command:

```
/usr/sbin/spacewalk-service status
```

In addition, you can obtain the status of components such as the Apache Web server and the Task Engine individually. For instance, to view the status of the Apache Web server, run the command:

```
rcapache2 status
```

If the Apache Web server is not running, entries in your `/etc/hosts` file may be incorrect. Refer to Section 5.3, “Host Not Found/Could Not Determine FQDN” (page 22) for a description of this problem and possible solutions.

To obtain the status of the Task Engine, run the command:

```
rctaskomatic status
```

To obtain the status of SUSE Manager's embedded database, if it exists, run the command:

```
service oracle status
```

To determine the version of your database schema, run the command:

```
rhn-schema-version
```

To derive the character set types of your SUSE Manager's database, run the command:

```
rhn-charsets
```

If the administrator is not getting email from SUSE Manager, confirm the correct email addresses have been set for `traceback_mail` in `/etc/rhn/rhn.conf`.

If the traceback mail is marked from `susemanager@suse.de` and you would like the address to be valid for your organization, include the `web.default_mail_from` option and appropriate value in `/etc/rhn/rhn.conf`.

If importing a channel fails and you cannot recover it in any other way, run this command to delete the cache:

```
rm -rf temporary-directory
```

Next, restart the importation .

If `zypper up`) or the push capability of SUSE Manager ceases to function, it is possible that old log files may be at fault. Stop the `jabberd` daemon before removing these files. To do so, issue the following commands as root:

```
rcjabberd stop
cd /var/lib/jabberd
rm -f *_db*
rcjabberd start
```

5.3 Host Not Found/Could Not Determine FQDN

Because SUSE Manager configuration files rely exclusively on fully qualified domain names (FQDN), it is imperative key applications are able to resolve the name of the SUSE Manager server into an IP address. Red Hat Update Agent, , and the Apache Web server are particularly prone to this problem with the applications issuing errors of "host not found" and the Web server stating "Could not determine the server's fully qualified domain name" upon failing to start.

This problem typically originates from the `/etc/hosts` file. You may confirm this by examining `/etc/nsswitch.conf`, which defines the methods and the order by which domain names are resolved. Usually, the `/etc/hosts` file is checked first, followed by Network Information Service (NIS) if used, followed by DNS. One of these has to succeed for the Apache Web server to start and the client applications to work.

To resolve this problem, identify the contents of the `/etc/hosts` file. It may look like this:

```
127.0.0.1 this_machine.example.com this_machine localhost.localdomain \
localhost
```

In a text editor, remove the offending machine information:

```
127.0.0.1 localhost.localdomain.com localhost
```

Save the file and attempt to re-run the client applications or the Apache Web server. If they still fail, explicitly identify SUSE Manager server's IP address in the file, such as:

```
127.0.0.1 localhost.localdomain.com localhost
123.45.67.8 this_machine.example.com this_machine
```

Replace the value here with the actual IP address of the SUSE Manager server. This should resolve the problem. Keep in mind, if the specific IP address is stipulated, the file will need to be updated when the machine obtains a new address.

5.4 Connection Errors

A common connection problem, indicated by `SSL_CONNECT` errors, is the result of a SUSE Manager server being installed on a machine whose time had been improperly set. During the installation process, SSL certificates are created with inaccurate times. If the time on SUSE Manager is then corrected, the certificate start date and time may be set in the future, making it invalid.

To troubleshoot this, check the date and time on the clients and on SUSE Manager with the following command:

```
date
```

The results should be nearly identical for all machines and within the "notBefore" and "notAfter" validity windows of the certificates. Check the client certificate dates and times with the following command:

```
openssl x509 -dates -noout -in /usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT
```

Check the SUSE Manager server certificate dates and times with the following command:

```
openssl x509 -dates -noout -in /etc/httpd/conf/ssl.crt/server.crt
```

By default, the server certificate has a one-year life while client certificates are good for 10 years. If you find the certificates are incorrect, you can either wait for the valid start time, if possible, or create new certificates, preferably with all system times set to GMT.

The following measures can be used to troubleshoot general connection errors:

- Attempt to connect to SUSE Manager's database at the command line using the correct connection string as found in `/etc/rhn/rhn.conf`:

```
sqlplus username/password@sid
```

- Ensure SUSE Manager is using Network Time Protocol (NTP) and set to the appropriate time zone. This also applies to all client systems and the separate database machine in SUSE Manager (if used with a stand-alone database).
- Confirm the correct package:

```
rhn-org-httpd-ssl-key-pair-MACHINE_NAME-VER-REL.noarch.rpm
```

is installed on SUSE Manager and the corresponding `rhn-org-trusted-ssl-cert-*.noarch.rpm` or raw CA SSL public (client) certificate is installed on all client systems.

- Verify the client systems are configured to use the appropriate certificate.
- If also using one or more SUSE ManagerProxy Servers, ensure each Proxy's SSL certificates are prepared correctly. The Proxy should have both its own server SSL key-pair and CA SSL public (client) certificate installed, since it will serve in both capacities. Refer to Chapter 3, *SSL Infrastructure* (↑Client Configuration Guide) for specific instructions.
- Make sure client systems are not using firewalls of their own, blocking required ports.

5.5 SUSE Manager Debugging

If you have exhausted the troubleshooting steps above and need more help, contact the Novell support with an aggregation of SUSE Manager's configuration parameters, log files, and database information.

SUSE Manager provides a command line tool explicitly for this purpose. Log in to your SUSE Manager server as `root` and execute the following command:

```
spacewalk-debug
```

It collects several pieces of information and stored them in a tarball:

```
Collecting and packaging relevant diagnostic information.
```

```
Warning: this may take some time...
```

```
* copying configuration information
* copying logs
* copying cobbler files
* copying monitoring moc logs
* copying monitoring scout logs
* copying ssl-build
* copying /etc/sudoers
* copying apache, oracle, tomcat, ncpulse entries from /etc/passwd
* copying apache, oracle, tomcat, ncpulse entries from /etc/group
* querying RPM database (versioning of Spacewalk, etc.)
* querying schema version, database charactersets and database
* get disk space available
* get database statistics
* get schema statistics
* copying audit.log
* timestamping
* creating tarball (may take some time): /tmp/spacewalk-debug.tar.bz2
* removing temporary debug tree
```

```
Debug dump created, stored in /tmp/spacewalk-debug.tar.bz2
```


Maintenance

Because of SUSE Manager's unique environment, its users are provided with abilities not available to any other Novell Customer Center customers. In addition, SUSE Manager itself also requires maintenance. This chapter discusses the procedures that should be followed to carry out administrative functions outside of standard use, as well as to apply patches to SUSE Manager.

6.1 Managing SUSE Manager with `spacewalk-service`

Since SUSE Manager consists of a multitude of individual components, Novell provides a command-line tool that allows you to stop, start, or retrieve status information from the various services in the appropriate order: `spacewalk-service`. This tool accepts all of the typical commands:

```
/usr/sbin/spacewalk-service start
/usr/sbin/spacewalk-service stop
/usr/sbin/spacewalk-service restart
/usr/sbin/spacewalk-service reload
```

```
/usr/sbin/spacewalk-service enable
/usr/sbin/spacewalk-service disable
```

```
/usr/sbin/spacewalk-service status
```

Use `spacewalk-service` to shut down and bring up the entire SUSE Manager and retrieve status messages from all of its services at once.

6.2 Updating SUSE Manager

If any critical updates are made to SUSE Manager, they will be released in the form of a patch for SUSE Manager. Find a generic description on how to apply patches in Procedure 6.1, “Updating a SUSE Manager Server” (page 28). Note that specific instructions may apply depending on the patch.

For SUSE Manager systems that may be connected to the Internet, the best method for applying these patches is using `zypper` or YaST Online Update. Proper registration at Novell Customer Center is mandatory for the system to receive updates. For details, refer to Section “Installation and Setup” (↑Quick Start). SUSE Manager systems that may not be connected to the Internet (disconnected setup) will receive updates from an internal update server instead.

Procedure 6.1 *Updating a SUSE Manager Server*

As soon as SUSE Manager is up and running and the database is configured, updating the server requires more than executing `zypper patch` (or running YaST Online Update alternatively).

The steps below describe the generic procedure, but depending on the patch, specific instructions may apply.

WARNING: Read Patch Advisory

Before applying any updates, make sure to read the patch advisory. Additional configuration steps may be required to apply certain updates, especially if they involve the database. In such cases, the advisory will contain specific and detailed information about necessary steps that may be required.

1 Log in as `root` user to the SUSE Manager server.

2 Stop the Spacewalk service:

```
spacewalk-service stop
```

If the SUSE Manager database is running on the same machine as the SUSE Manager server, this command also stops the SUSE Manager database instance.

- 3 Apply the patch using either `zypper patch` or YaST Online Update. For more information about `zypper` or YaST Online Update, refer to Section “Updating Packages on SLE” (↑Reference Guide).
- 4 If the patch includes an update of the database schema, proceed as follows (otherwise skip the substeps below):

- 4a If the SUSE Manager database is running on the same machine as your SUSE Manager server, start the database instance with

```
/etc/init.d/oracle-xe start
```

- 4b Upgrade the database schema with

```
spacewalk-schema-upgrade
```

- 5 Start the Spacewalk service:

```
spacewalk-service start
```

IMPORTANT: Restart of Services and Applications

Services affected by a package update are not automatically restarted after the update—you need to restart them manually to avoid failures.

Also execute `zypper ps` to check for any applications that still use old code. Restart those applications.

6.3 Backing Up SUSE Manager

Backing up SUSE Manager can be done in several ways. Regardless of the method chosen, the associated database also needs to be backed up. For the stand-alone database, consult your organization's database administrator. For the embedded database, refer to Section 6.4, “Using DB Control” (page 31) for a complete description of this process and the options available.

Here are the minimum files and directories Novell recommends backing up:

- `/rhnsat/` - embedded database only (never to be backed up while the database is running - refer to Section 6.4.2, “Backing up the Database” (page 33))
- `/etc/sysconfig/rhn/`
- `/etc/rhn/`
- `/etc/sudoers`
- `/etc/tnsnames.ora`
- `/srv/www/htdocs/pub/`
- `/var/pacewalk/packages/1` - custom RPMs
- `/root/.gnupg/`
- `/root/ssl-build/`
- `/etc/dhcp.conf`
- `/tftpboot/`
- `/var/lib/cobbler/`
- `/var/lib/rhn/kickstarts/`
- `/srv/www/cobbler`
- `/var/lib/nocpulse/`

If possible, back up `/var/pacewalk/`, as well. In case of failure, this will save lengthy download time. Since `/var/pacewalk/` (specifically `/var/pacewalk/packages/NULL/`) is primarily a duplicate of the package repository, it can be regenerated with `mgr-ncc-sync`. Novell recommends the entire `/var/pacewalk/` tree be backed up. In the case of disconnected satellites, `/var/pacewalk/` *must* be backed up.

Backing up only these files and directories would require reinstalling the SUSE Manager ISO RPMs and re-registering SUSE Manager. In addition, packages would need to be resynchronized using the `mgr-ncc-sync` tool. Finally, you would have to reinstall the `/root/ssl-build/\ rhn-org-httpd-ssl-key-pair-MACHINE_NAME-VER-REL.noarch.rpm`.

Another method would be to back up all of the files and directories mentioned above but reinstall the SUSE Manager without re-registering it. During the installation, cancel or skip the registration and SSL certificate generation sections.

The final and most comprehensive method would be to back up the entire machine. This would save time in downloading and re-installing but would require additional disk space and back up time.

NOTE

Regardless of the back-up method used, when you restore SUSE Manager from a back-up, you must run the following command to schedule the recreation of search indexes the next time the `rhn-search` service is started:

```
rcrhn-search cleanindex
```

6.4 Using DB Control

SUSE Manager with embedded database requires a utility for managing that database: DB Control. This command line utility allows you to do everything from make, verify, and restore backups to obtain database status and restart it when necessary. You *must* be the `oracle` user to invoke DB Control. To begin, switch to the `oracle` user:

```
su - oracle
```

Next, issue the following command:

```
db-control option
```

6.4.1 DB Control Options

DB Control offers many command line options. To use them, as user `oracle` insert the option and the appropriate value, if needed, after the `db-control` command.

Table 6.1 *DB Control Options*

Option	Description
<code>help</code>	Lists these <code>db-control</code> options with additional details.
<code>backup DIRNAME</code>	Backs up the database to the directory specified.
<code>examine DIRNAME</code>	Examines the contents of a backup directory. Returns the timestamp of backup creation and reports on its contents.
<code>extend</code>	Increase the tablespace
<code>gather-stats PCT</code>	Gather statistics on the database objects. <i>PCT</i> is the percentage of rows to estimate (the default is 15%).
<code>report</code>	Reports on current usage of database space.
<code>report-stats</code>	Reports on segments with stale or empty statistics.
<code>restore DIRNAME</code>	Restores the database from backup kept in <i>DIRNAME</i> . Database must be stopped for this command to run successfully.
<code>start</code>	Starts the database instance. This can also be accomplished by issuing the <code>service oracle start</code> command as root.
<code>shrink-segments</code>	Shrinks SUSE Manager Oracle database segments with significant amounts of free space.
<code>status</code>	Shows the current status of the database, either "running" or "offline".

Option	Description
<code>stop</code>	Stops the database instance. This can also be accomplished by issuing the <code>service oracle stop</code> command as root.
<code>tablesizes</code>	Show space report for each table
<code>verify DIRNAME</code>	Verifies the contents of the backup kept in DIRNAME. This command runs a checksum of each of the files kept in the backup.

NOTE

Database statistics are collections of data that describe more details about the database and the objects in the database. These statistics are used by the query optimizer to choose the best execution plan for each SQL statement. Because the objects in a database can be constantly changing, statistics must be regularly updated so that they accurately describe these database objects. Statistics are maintained automatically by Oracle. However, if your database has performance issues after a significant amount of data changes, consider performing manual gathering of statistics.

NOTE

After deleting large amount of data, use the `segment-shrink` feature to reclaim fragmented free space in an Oracle Database segment. The benefits of `segment-shrink` are compaction of data that leads to better cache utilization and the compacted data requires fewer blocks to be scanned in full table scans, which both lead to better performance.

6.4.2 Backing up the Database

It is recommended performing nightly backups of the embedded database and moving the resulting directory to another system via NFS, SCP, FTP, etc. Preferably, this backup system resides off-site. To conduct a backup, shut down the database and related services first by issuing the following command as root:

```
/usr/sbin/spacewalk-service stop
```

Then switch to the `oracle` user and issue this command to initiate the backup:

```
db-control backup DIRNAME
```

Backup files are stored in the directory specified. Note that this is a cold backup; the database must be stopped before running this command. This process takes several minutes. The first backup is a good indicator of how long subsequent backups will take.

Once the backup is complete, return to `root` user mode and restart the database and related services with the following command:

```
/usr/sbin/spacewalk-service start
```

You should then copy that backup to another system using `rsync` or another file-transfer utility. It is strongly recommended scheduling the backup process automatically using cron jobs. For instance, back up the system at 3 a.m. and then copy the backup to the separate repository (partition, disk, or system) at 6 a.m.

6.4.3 Verifying the Backup

Backing up the embedded database is useful only if you can ensure the integrity of the resulting backup. DB Control provides two methods for reviewing backups, one brief, one more detailed. To conduct a quick check of the backup's timestamp and determine any missing files, issue this command as `oracle`:

```
db-control examine DIRNAME
```

To conduct a more thorough review, including running a checksum of each of the files in the backup, issue this command as `oracle`:

```
db-control verify DIRNAME
```

6.4.4 Restoring the Database

DB Control makes embedded database restoration a relatively simple process. As in the creation of backups, you will need to shut down the database and related services first by issuing the following commands in this order as `root`:

```
/usr/sbin/spacewalk-service stop
```

Then switch to the oracle user and issue this command, including the directory containing the backup, to begin the restoration:

```
db-control restore DIRNAME
```

This not only restores the embedded database but first verifies the contents of the backup directory using checksums. Once the restoration is complete, return to `root` user mode and restart the database and related services with these commands in this order:

```
/usr/sbin/spacewalk-service start
```

6.5 Cloning SUSE Manager with the embedded database

You may limit outages caused by hardware or other failures by cloning SUSE Manager with Embedded Database in its entirety. The secondary server can be prepared for use if the primary fails. To clone SUSE Manager, perform these tasks:

1. Install SUSE Manager with embedded database on a separate machine, skipping the SSL Certificate generation step.
2. Back up the primary SUSE Manager database daily using the commands described in Section 6.4.2, “Backing up the Database” (page 33). If this is done, only changes made the day of the failure will be lost.
3. Establish a mechanism to copy the backup to the secondary SUSE Manager and keep these repositories synchronized using a file transfer program such as `rsync`. If you're using a SAN, copying isn't necessary.
4. Use DB Control's `restore` option to import the duplicate data.
5. If the primary SUSE Manager fails, transfer the SSL key pair RPM package in `/root/ssl-build` from the primary to the secondary SUSE Manager, and install the package. This ensures that clients can authenticate with and securely connect to the secondary server.

6. Change DNS to point to the new machine or configure your load balancer appropriately.

6.6 Establishing Redundant SUSE Manager server with stand-alone database

In keeping with the cloning option available to SUSE Manager with embedded database, you may limit outages on SUSE Manager servers with stand-alone database by preparing redundant SUSE Manager servers. Unlike cloning a SUSE Manager with embedded database, redundant SUSE Manager servers with stand-alone database may be run as active, as well as standby. This is entirely up to your network topology and is independent of the steps listed here.

To establish this redundancy, first install the primary SUSE Manager server normally, except the value specified in the Common Name field for the SSL certificate must represent your high-availability configuration, rather than the hostname of the individual server. Then:

1. Prepare the stand-alone database for failover using Oracle's recommendations for building a fault-tolerant database. Consult your database administrator.
2. Install SUSE Manager with stand-alone database on a separate machine, skipping the database configuration, database schema, SSL certificate, and bootstrap script generation steps. Include the same Novell Customer Center account and database connection information provided during the initial SUSE Manager install and register the new SUSE Manager server.

If your original SSL certificate does not take your high-availability solution into account, you may create a new one with a more appropriate Common Name value now. In this case, you may also generate a new bootstrap script that captures this new value.

3. After installation, copy the following files from the primary to the secondary SUSE Manager:

- `/etc/rhn/rhn.conf`

- `/etc/tnsnames.ora`

4. Copy and install the server-side SSL certificate RPMs from the primary SUSE Manager to the secondary. Refer to the Sharing Certificates section of the Client Configuration Guide for precise instructions. Remember, the Common Name value must represent the combined SUSE Manager solution, not a single machine's host-name.

If you generated a new SSL certificate during SUSE Manager installation that included a new Common Name value, copy the SSL certificate RPMs from the secondary to the primary server and redistribute the client-side certificate. If you also created another bootstrap script, you may use this to install the certificate on client systems.

5. If you did not create a new bootstrap script, copy the contents of `/srv/www/htdocs/pub/bootstrap/` from the primary server to the secondary. If you did generate a new one, copy that directory's contents to the primary SUSE Manager.
6. Turn off the Task Engine on the secondary server with the following command:

```
rtaskomatic stop
```

You may use custom scripting or other means to establish automatic start-up/failover of the Task Engine on the secondary server. Regardless, it will need to be started upon failover.

7. Share channel package data (by default located in `/var/spacewalk`) between the SUSE Manager servers over some type of networked storage device. This eliminates data replication and ensures a consistent store of data for each SUSE Manager.
8. Share cache data (by default located in `/var/cache/rhn`) between the SUSE Manager servers over some type of networked storage device. This eliminates data replication and ensures a consistent store of cached data for each server.
9. Make the various SUSE Manager servers available on your network via Common Name and a method suiting your infrastructure. Options include round-robin DNS, a network load balancer, and a reverse-proxy setup.

6.7 Changing the SUSE Manager Hostname

If you need to change the hostname or IP address of the SUSE Manager server, the `spacewalk-utils` package contains the `spacewalk-hostname-rename` script.

To use the `spacewalk-hostname-rename` script, you must first ensure that you know your SSL CA passphrase by performing the following command:

```
openssl rsa -in path/RHN-ORG-PRIVATE-SSL-KEY
```

Then enter passphrase when prompted.

`spacewalk-hostname-rename` requires one mandatory argument, which is the IP address of the SUSE Manager server, regardless of whether the IP address will change along with the hostname or not.

The usage of `spacewalk-hostname-rename` is as follows:

```
spacewalk-hostname-rename <ip address> [ --ssl-country=<country> \
--ssl-state=<state> --ssl-org=<organization/company>\
--ssl-orgunit=<department> --ssl-email=<email address> \
--ssl-ca-password=<password>]
```

Changing the hostname requires to generate a new SSL certificate. If not all necessary options are passed at the command-line (as in the above example), they will be asked interactively via series of prompts.

6.8 Conducting SUSE Manager-Specific Tasks

6.8.1 Deleting Users

Because of the isolated environment in which SUSE Manager operates, SUSE Manager customers have been granted the ability to delete users. To access this functionality,

click *Users* in the top navigation bar of the SUSE Manager website. In the resulting User List, click the name of the user to be removed. This takes you to the *User Details* page. Click the *delete user* link at the top-right corner of the page.

Figure 6.1 *User Deletion*

The screenshot shows the SUSE Manager web interface. The top navigation bar includes links for Documentation, User Admin, Organization, Spacewalk, Default Organization, Preferences, and Sign Out. Below this is a green header with the SUSE Manager logo and a search bar. The main navigation bar has tabs for Overview, Systems, Patches, Channels, Configuration, Schedule, Users, Monitoring, Admin, and Help. The Users tab is selected. On the left, there is a sidebar with 'User List' and sub-links for 'Active', 'Deactivated', and 'All'. The main content area shows the 'User Details' for a user named 'tuxpenguin'. The user's profile includes fields for Username, Prefix, First Name, Last Name, Position, Password, Confirm Password, and Email. The user's email is 'tux@example.org'. There are links for 'delete user' and 'deactivate user' in the top right corner of the user details section.

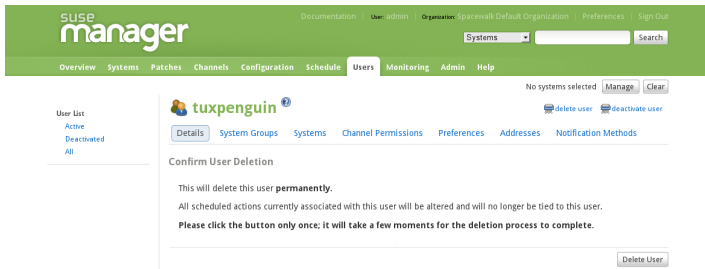
A confirmation page appears explaining that this removal is permanent. To continue, click Delete User at the bottom-right corner of the page.

NOTE

The Organization Administrator role must be removed from the user's profile before deleting the user from SUSE Manager. Failing to do so causes the delete operation to fail.

The Organization Administrator role may be removed by any Organization Administrator (provided they are not the sole Organization Administrator for the organization) by clicking on the *Users* tab and then visiting the *Details* sub-tab.

Figure 6.2 *User Delete Confirmation*



6.8.2 Configuring SUSE Manager Search

SUSE Manager administrators may want to configure certain search options to customize search results for their own optimization requirements.

SUSE Manager search results can be customized via the `/etc/rhn/search.rhn-search.conf` file. The following list defines the search configuration and their default values in parentheses.

- `search.index_work_dir` : Specifies where Lucene indexes are kept (`/usr/share/rhn/search/indexes`)
- `search.rpc_handlers` : semi-colon separated list of classes to act as handlers for XMLRPC calls.

```
(filename>index:com.redhat.satellite.search.rpc.handlers.IndexHandler,  
db:com.redhat.satellite.search.rpc.handlers.DatabaseHandler,  
admin:com.redhat.satellite.search.rpc.handlers.AdminHandler)
```
- `search.max_hits_returned` : maximum number of results which will be returned for the query (500)
- `search.connection.driver_class` : JDBC driver class to conduct database searches (`oracle.jdbc.driver.OracleDriver`)
- `search.score_threshold` : minimum score a result needs to be returned back as query result (.10)

- `search.system_score_threshold` : minimum score a system search result needs to be returned back as a query result (`.01`)
- `search.errata_score_threshold` : minimum score a patch search result needs to be returned back as a query result (`.20`)
- `search.errata.advisory_score_threshold` : minimum score a patch advisory result needs to be returned back as a query result (`.30`)
- `search.min_ngram` : minimum length of n-gram characters. Note that any change to this value requires `clean-index` to be run, and `doc-indexes` need to be modified and rebuilt (`1`)
- `search.max_ngram` : maximum length of n-gram characters. Note that any change to this value requires `clean-index` to be run, and `doc-indexes` need to be modified and rebuilt (`5`)
- `search.doc.limit_results` : type **true** to limit the number of results both on `search.score_threshold` and restrict max hits to be below `search.max_hits_returned`; type **false** means to return all documentation search matches (`false`)
- `search.schedule.interval` : input the time in milliseconds to control the interval with which the SearchServer polls the database for changes; the default is 5 minutes (`300000`).
- `search.log.explain.results` : used during development and debugging. If set to true, this will log additional information showing what influences the score of each result. (`false`)

6.9 Automating Synchronization

Manually synchronizing the SUSE Manager repository with Novell Customer Center can be a time-intensive task. United States business hours tend to be the peak usage time for Novell Customer Center, so synchronization at that time may be slow. For these reasons, Novell encourages you to automate synchronization at other times to better balance load and ensure quick synchronization. Continental United States business hours are roughly 8:00 AM to 9:00 PM EST (UTC -5), due to four time zones, Monday

through Friday. These hours may vary seasonally by one hour. *Further, Novell strongly recommends that synchronization occur randomly for best performance.*

This automation can be set easily by the addition of a simple cron job. To do this, edit the crontab as root:

```
crontab -e
```

This opens the crontab in a text editor, by default Vi. Another editor can be used by first changing the `EDITOR` variable, like so: `export EDITOR=emacs`.

Once opened, use the first five fields (minute, hour, day, month, and weekday) to schedule the synchronization. Remember, hours use military time. Edit the crontab to include random synchronization, like so:

```
0 1 * * * perl -le 'sleep rand 9000' && mgr-ncc-sync >/dev/null \
2>/dev/null
```

This particular job will run randomly between 1:00 a.m. and 3:30 a.m. system time each night and redirect `stdout` and `stderr` from `cron` to prevent duplicating the more easily read message from `mgr-ncc-sync`. Options other than `--email` can also be included. Once you exit from the editor, the modified crontab is installed immediately.

6.10 Implementing PAM Authentication

As security measures become increasingly complex, administrators must be given tools that simplify their management. For this reason, SUSE Manager supports network-based authentication systems via Pluggable Authentication Modules (PAM). PAM is a suite of libraries that helps system administrators integrate SUSE Manager with a centralized authentication mechanism, thus eliminating the need for remembering multiple passwords.

SUSE Manager supports LDAP, Kerberos, and other network-based authentication systems via PAM. To enable SUSE Manager to use PAM and your organization's authentication infrastructure, follow the steps below.

NOTE

To ensure that PAM authentication functions properly, install the `pam-devel` package.

Set up a PAM service file (usually `/etc/pam.d/susemanager`) and have SUSE Manager use it by adding the following line to `/etc/rhn/rhn.conf`:

```
pam_auth_service = susemanager
```

This assumes the PAM service file is named `susemanager`.

To enable a user to authenticate against PAM, select the checkbox labeled *Pluggable Authentication Modules (PAM)*. It is positioned below the password and password confirmation fields on the *Create User* page.

As an example, for a Red Hat Enterprise Linux 5 i386 system, to authenticate against Kerberos one could put the following in `/etc/pam.d/susemanager`:

```
##PAM-1.0
auth      required      pam_env.so
auth      sufficient    pam_krb5.so no_user_check
auth      required      pam_deny.so
account   required      pam_krb5.so no_user_check
```

Please note that changing the password on the SUSE Manager website changes only the local password on the SUSE Manager, which may not be used at all if PAM is enabled for that user. In the above example, for instance, the Kerberos password will not be changed.

6.11 Enabling Push to Clients

In addition to allowing client systems to regularly poll SUSE Manager for scheduled actions, you may enable it to immediately initiate those tasks on provisioning-entitled systems. This bypasses the typical delay between scheduling an action and the client system checking in to retrieve it. This support is provided by the OSA dispatcher (`osad`).

OSA dispatcher is a service that periodically runs a query that checks the SUSE Manager server to see if there are any commands to be executed on the client. If there are, it sends a message through `jabberd` to the `osad` instances running on the clients.

IMPORTANT

SSL must be employed between SUSE Manager and its clients systems for this feature to work. If the SSL certificates are not available, the daemon on the client system fails to connect.

To take advantage of this feature, you must first configure your firewall rules to allow connections on the required port(s), as described in Section 3.2, “Additional Requirements” (page 11).

Then you must install the `osa-dispatcher` package, which can be found in the SUSE Manager software channel. Once installed, start the service on as `root` using the command:

```
rcosa-dispatcher start
```

Finally, install the `osad` package on all *client* systems to receive pushed actions. The package can be found within the Tools child channel for the systems on SUSE Manager.

WARNING

Do *not* install the `osad` package on the SUSE Manager server, as it will conflict with the `osa-dispatcher` package.

Once installed, start the service on the client systems as `root` using the command:

```
rcosad start
```

Like other services, `rcosa-dispatcher` and `rcosad` accept `stop`, `restart`, and `status` commands, as well.

Keep in mind, this feature depends on the client system recognizing the fully qualified domain name (FQDN) of SUSE Manager. This name and not the IP address of the server must be used when configuring the YaST Online Update.

Now when you schedule actions from SUSE Manager on any of the push-enabled systems, the task will begin immediately rather than wait for the system to check in.