Spacewalk for Oracle® Linux

Installation Guide for Release 2.7

ORACLE®

Oracle Legal Notices

About this document

This document describes how to install Spacewalk 2.7 servers and proxies.

Document generated on: 2021-02-05 (revision: 661)

Table of Contents

Preface

Spacewalk for Oracle® Linux: Installation Guide for Release 2.7 describes how to install Spacewalk 2.7 servers and proxies on Oracle Linux 6 and Oracle Linux 7.

Audience

This document is written for system administrators who want to use Spacewalk to manage Oracle Linux systems. It is assumed that readers have a general understanding of the Linux operating system.

Related Documents

The documentation for this product is available at:

Oracle® Linux Manager & Spacewalk for Oracle® Linux Documentation

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle recognizes the influence of ethnic and cultural values and is working to remove language from our products and documentation that might be considered insensitive. While doing so, we are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is an ongoing, long-term process.

Chapter 1 Installing and Upgrading Spacewalk Servers

This chapter describes how to install and upgrade Spacewalk servers and proxies.

> **Note**
>
> This guide provides information and procedures for installing Spacewalk for Oracle Linux Release 2.7. However, Oracle recommends that you install Spacewalk for Oracle Linux Release 2.10 instead. For procedures, see *Spacewalk for Oracle® Linux: Installation Guide for Release 2.10*.

1.1 Oracle Linux Requirements

Oracle supports Spacewalk servers that are running on Oracle Linux 6 (x86_64) or Oracle Linux 7 (x86_64). Oracle recommends that you update your Oracle Linux system with the latest packages that are available on the Oracle Linux yum server.

> **Note**
>
> Do not register a Spacewalk server or client with ULN. You can register a Spacewalk server as a client of itself to receive updates.

You should install Oracle Linux 6 or Oracle Linux 7 by using either the **Minimal** or **Basic Server** software set. If you select additional package groups during installation, remove the `jta` package before installing Spacewalk, as this package causes Spacewalk services to fail to start.

Install Spacewalk by using only the packages that are provided by Oracle from the Oracle Linux yum server at https://yum.oracle.com.

No third-party package repositories are required to install Spacewalk on Oracle Linux 6 or Oracle Linux 7. All of the required packages are available in the Spacewalk repositories on the Oracle Linux yum server.

1.2 Storage Requirements for a Spacewalk Server

A Spacewalk server should have a minimum of 8 GB of memory. If the Spacewalk server also runs the database that stores the Spacewalk repository, this memory requirement is *in addition to* what is required to run the database.

To preserve errata mapping, by default, Spacewalk maintains all available versions of all available packages in each software channel that you configure. As a result, the storage requirements for a Spacewalk server can be significant, depending on the number of major versions and architectures that you choose to support. Typically, the Oracle Linux binary repositories require approximately 60 GB for each combination of Oracle Linux release and architecture. An extra 40 GB is required for source packages and 80 GB is required for Ksplice updates for each combination of Oracle Linux release and architecture.

> **Note**
>
> With Spacewalk 2.7, you can reduce the storage requirements considerably by specifying the `--latest` option to the `spacewalk-repo-sync` command, which causes the server to synchronize only the latest packages that are available at the time of synchronization. It does not remove older packages from the channel. If the synchronization interval is large, you might miss a particular version of a package, which can have implications for errata handling, where errata are associated with specific package versions. If errata consistency is important to you, Oracle

> recommends that you do *not* use `--latest`. However, using `--latest` with a Ksplice channel is an exception because its packages are always cumulative.

⚠️ **Caution**

> Packages are never removed from Oracle Linux repositories so that the space that is required for each repository always increases. You should actively monitor the available disk space on the Spacewalk server.

A Spacewalk server stores the packages that it hosts under the `/var/satellite/redhat` directory hierarchy. You should plan how to best configure the `/var` file system before installing Spacewalk. For example, if you set up `/var` as an `ext4` or `XFS` file system by using Logical Volume Manager (LVM), you can expand the storage when required.

1.3 Networking Requirements for a Spacewalk Server

Prior to installing a Spacewalk server, refer to the following networking requirements and configuration information:

- **Configure a fully qualified domain name**

  You must configure a fully qualified domain name (FQDN) for the Spacewalk server. Note that Spacewalk does not consider `.local` and `.localdomain` to be valid domain names.

  ⚠️ **Caution**

  > The Spacewalk server and clients must be able to resolve the Spacewalk server's FQDN for both forward and reverse lookups in DNS. If these conditions are not met, neither certificate validation nor PXE booting work. In addition, clients cannot register with the Spacewalk server. In particular, a lack of reverse DNS lookup causes Inter-Server Synchronization (ISS) to fail.

  Also, verify that the host name that is returned by the `hostname` command and the value of `HOSTNAME` that is defined in the `/etc/hostname` file (for Oracle Linux 7) or the `/etc/sysconfig/network` file (for Oracle Linux 6) are identical.

  As shown in the following example, the host name must be consistent with the FQDN that is defined for the system in DNS, for both forward and reverse lookups:

```
# hostname
swksvr.mydom.com
# grep HOSTNAME /etc/sysconfig/network
HOSTNAME=swksvr.mydom.com
```

  You can also use the `host` command to verify this information on systems that are running Oracle Linux 6:

```
# host swksvr.mydom.com
swksvr.mydom.com has address 192.168.1.3
# host 192.168.1.3
3.1.168.192.in-addr.arpa domain name pointer swksvr.mydom.com.
```

  You will need to edit the `/etc/hosts` file and configure the actual IP address for the FQDN and host name, but not the loopback address (`127.0.0.1`), as shown in the following example:

```
127.0.0.1       localhost localhost.localdomain localhost4 localhost4.localdomain4
::1             localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.1.3     swksvr.mydom.com swksvr
```

- **Port numbers for a Spacewalk server**

  The following table describes the network ports that a Spacewalk server uses, depending on its configuration.

Port/ Protocol	Direction	Purpose
69/udp	Inbound	TFTP (if PXE provisioning support is required)
80/tcp	Inbound and outbound	HTTP access
443/tcp	Inbound and outbound	HTTPS access
5222/tcp	Inbound	Push support to Spacewalk clients (if required)
5269/tcp	Inbound	Push support to Spacewalk proxies (if required)

- **Configure network time synchronization**

  Configure the Spacewalk server, proxies, and clients to use a network time synchronization mechanism such as the Network Time Protocol (NTP) or the Precision Time Protocol (PTP). In order to establish a Secure Socket Layer (SSL) based connection, Spacewalk requires that the system time on these systems be consistent to within 120 seconds. Furthermore, if the system times (corrected for time zone difference) of the server and a client differ by more than 120 seconds, authentication of the osad service on the client by the jabberd service on the server fails.

  For more information, see *Oracle® Linux 6: Administrator's Guide* or *Oracle® Linux 7: Administrator's Guide*.

1.4 Database Requirements and Configuration Instructions

You can use the following database solutions to store Spacewalk data:

- Oracle Database

- Oracle Database Express Edition (Oracle Database XE)

- PostgreSQL

However, note that Oracle supports *only* Oracle Database for use with Spacewalk and provides a restricted-use license for the use of Oracle Database 12*c* Enterprise Edition for Oracle Linux support customers.

> **Note**
>
> If you are upgrading existing Spacewalk instances that are using Oracle Database 11gR2, and you do not have an Oracle Database license that is currently active, you *must* upgrade to at least Oracle Database 12cR1 prior to upgrading to Spacewalk 2.7

For more information, see *Oracle® Linux 6: Licensing Information User Manual* or *Oracle® Linux 7: Licensing Information User Manual*.

> **Note**
>
> Oracle Database XE (Oracle Database Express Edition) and PostgreSQL and their use is not described in this document. Also, Oracle does not provide any tools for migrating from an unsupported database.

1.4.1 Database Sizing Requirements

When determining the amount of space the Spacewalk database requires, be sure to include sizing estimates in your overall calculation for the following: number of client systems that will be served by the Spacewalk server, number of channels allocated to each client system, as well as the number of packages that each channel will contain.

To more accurately determine how much space the Spacewalk database requires, use the following calculation:

- 250 KiB per client system.

- 500 KiB per channel, plus an additional 230 KiB per package in the channel (a channel with 5000 packages would require 1.1 GiB).

For example, if you have a large Spacewalk server that is serving 10,000 systems, and each system has four channels containing 12,000 packages per-channel, then 2.5 GiB would be required for the clients, and 11 GiB would be required for the channels.

1.4.2 Oracle Database Installation Requirements

You must install an Oracle Database server, make this server available, and ensure that it is up and running *before* installing Spacewalk.

Supported Oracle Database releases include the following:

- Oracle Database 12c.

  You can download the software from Oracle at https://www.oracle.com/database/technologies/oracle-database-software-downloads.html.

- Oracle Database 11gR2, release 11.2.0.3 or later (requires an active Oracle Database license).

  > **Note**
  >
  > Use of this Oracle Database version is in extended support and requires an active, pre-existing Oracle Database license.

  To obtain the correct Oracle Database 11gR2 release, download the software from My Oracle Support (MOS) at https://support.oracle.com.

Consult with your Oracle database administrator for specific details about any prerequisite tasks, as well as specific installation instructions for your environment. For complete information, refer to the Oracle Database documentation at https://docs.oracle.com/en/database/database.html.

1.4.3 Oracle Database Configuration

The following are general guidelines for configuring Oracle Database. You can perform these steps during or after an installation. Consult with your Oracle database administrator to obtain any additional configuration instructions for your particular environment.

- The database must use the `AL32UTF8` character set that supports Unicode.

  > **Note**
  >
  > You can specify the `AL32UTF8` character set if you select **Advanced install** in the Installation GUI, but not if you select the **Typical install** option.
  >
  > If you installed the 12cR2 version of Oracle Database, the `AL32UTF8` character set is the default.

- The database must have a Spacewalk user. You create this user by using SQL*Plus commands, as described in the steps that follow. You can use any name that you choose for the Spacewalk user.

  For example, you could create a user named `spacewalk` for Oracle Database 11gR2. For Oracle Database 12c, if the database is a pluggable database, you might create a user named `c##spacewalk`. Note that if the database is not a pluggable database, the `c##` prefix does not need to be part of the user name.

- If several Spacewalk servers will share the same database server, you must create a separate Spacewalk user for each server. For example, if you intend to set up two Spacewalk servers that share the same database, you could create two users for Oracle Database 11gR2 with the following names: `spacewalk` and `spacewalk2`. For Oracle Database 12c, you could create the `c##spacewalk` and `c##spacewalk2` users.

- The Spacewalk user must be assigned the `CONNECT` and `RESOURCE` roles.

- The Spacewalk user must have the following system privileges:

  - `ALTER SESSION`
  - `CREATE SYNONYM`
  - `CREATE TABLE`
  - `CREATE TRIGGER`
  - `CREATE VIEW`
  - `UNLIMITED TABLESPACE`

Creating a Spacewalk User

Create a Spacewalk user as follows:

1. Log in to the system as a database administrator (typically, `SYS` or `SYSDBA`) on the database server.

   ```
   $ sqlplus / as SYSDBA
   ```

2. Set up the Spacewalk user by running the following SQL*Plus commands:

   ```
   SQL> create user sw_user identified by sw_passwd;
   SQL> grant connect,resource to sw_user;
   SQL> grant alter session, create synonym, create table, create trigger, create view to sw_user;
   SQL> grant unlimited tablespace to sw_user;
   ```

   In the previous command example, `sw_user` and `sw_passwd` are the user name and password that you will use to administer Spacewalk.

Repeat these steps for each Spacewalk user that you need to set up.

1.5 Installing a Spacewalk Server

Before you install the Spacewalk server software, you must do the following:

- Install the Oracle Database and ensure that it is up and running.

  For specific instructions on installing and configuring Oracle Database, consult with your Oracle database administrator. See also the product documentation at https://docs.oracle.com/en/database/database.html.

- Meet all of the requirements and perform any of the prerequisite tasks that are described in this document, as well as those that are specified in the product documentation.

  In particular, make sure you have configured a FQDN for the Spacewalk server, as described in Section 1.3, "Networking Requirements for a Spacewalk Server". The /etc/hosts file should have an FQDN entry for the Spacewalk server.

  > **Caution**
  >
  > The Spacewalk server and clients *must* be able to resolve the Spacewalk server's FQDN for both forward and reverse lookups in DNS. If these conditions are not met, neither certificate validation nor PXE boot will work. In addition, clients cannot register with the Spacewalk server. In particular, a lack of reverse DNS lookup on the Spacewalk server or the clients causes Inter-Server Synchronization (ISS) to fail.

Follow these steps to install the Spacewalk server software:

1. Install Oracle Instant Client release 11.2.0.4.

   a. Download the following Instant Client packages. You can find out more about the Instant Client from:

      https://www.oracle.com/database/technologies/instant-client.html

      - Instant Client Package (Basic)

      - Instant Client Package (SQL*Plus)

      > **Note**
      >
      > Do not download the packages for release 12.1 or later, as these releases are not supported. For additional information, refer to the Instant Client FAQ at https://www.oracle.com/database/technologies/faq-instant-client.html.

   b. Install the Instant Client packages.

      ```
      # yum install oracle-instantclient11.2-basic-11.2.0.4.0-1.x86_64.rpm \
      oracle-instantclient11.2-sqlplus-11.2.0.4.0-1.x86_64.rpm
      ```

   c. Add the library path to ldconfig.

      ```
      # echo /usr/lib/oracle/11.2/client64/lib > /etc/ld.so.conf.d/oracle-instantclient11.2.conf
      # ldconfig
      ```

⚠️ **Caution**

The Spacewalk server configuration fails if the Instant Client is missing. Oracle recommends that you install the latest 11.2.0.4 release of the Instant Client.

2. Ensure that the `jta` package is not installed and prevent it from being installed when you install Spacewalk.

   Check whether the `jta` package is installed as followed:

   ```
   # yum list installed | grep jta
   ```

   To remove the `jta` package:

   ```
   # yum remove jta
   ```

   To prevent the `jta` package from being installed later, do one of the following:

   - Disable the Oracle Linux 6 or Oracle Linux 7 `addons` channels (`[ol6_addons]` or `[ol7_addons]`).

   - Add the `jta` package to the `exclude` directive in the `/etc/yum.conf` file as follows:

     ```
     exclude=jta*
     ```

3. Configure the system firewall.

   For Oracle Linux 6, you would configure the system firewall as follows:

   ```
   # iptables -I INPUT -p udp -m udp --dport 69 -j ACCEPT
   # iptables -I INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
   # iptables -I INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
   # iptables -I INPUT -p tcp -m state --state NEW -m tcp --dport 5222 -j ACCEPT
   # iptables -I INPUT -p tcp -m state --state NEW -m tcp --dport 5269 -j ACCEPT
   # iptables -I OUTPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
   # iptables -I OUTPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
   # service iptables save
   ```

   For Oracle Linux 7, you would configure the system firewall as follows:

   ```
   # firewall-cmd --permanent --add-port=69/udp
   # firewall-cmd --permanent --add-port=80/tcp
   # firewall-cmd --permanent --add-port=443/tcp
   # firewall-cmd --permanent --add-port=5222/tcp
   # firewall-cmd --permanent --add-port=5269/tcp
   # firewall-cmd --reload
   ```

4. Enable access to the repositories that contain the Spacewalk Server packages and any dependent packages on the Oracle Linux yum server at https://yum.oracle.com.

   - For Oracle Linux 6, do the following:

     a. Ensure that your system is up to date and that you have transitioned to use the modular yum repository configuration by installing the `oraclelinux-release-el6` package and running the `/usr/bin/ol_yum_configure.sh` script, for example:

        ```
        # yum install oraclelinux-release-el6
        ```

```
# /usr/bin/ol_yum_configure.sh
```

> **Note**
>
> If the system is already using the new modular yum repository, a message is displayed when you run the `/usr/bin/ol_yum_configure.sh` command. The following message can be safely ignored:
>
> ```
> Missing /etc/yum.repos.d/public-yum-ol7.repo. Exiting
> ```

b. Install the `oracle-spacewalk-server-release-el6` release package to install appropriate yum repository configuration.

```
# yum install oracle-spacewalk-server-release-el6
```

The `ol6_spacewalk27_server` and the `ol6_spacewalk27_client` repositories are enabled by default in the repository configuration file.

- For Oracle Linux 7, do the following:

  a. Ensure that your system is up to date and that you have transitioned to using the modular yum repository configuration by installing the `oraclelinux-release-el7` package and running the `/usr/bin/ol_yum_configure.sh` script, for example:

  ```
  # yum install oraclelinux-release-el7
  # /usr/bin/ol_yum_configure.sh
  ```

  > **Note**
  >
  > On systems that were installed by using Oracle Linux 7.6 media or earlier, a message is displayed when you run the `/usr/bin/ol_yum_configure.sh` command if the system is already using the new modular yum repository. This message can be safely ignored:
  >
  > ```
  > Missing /etc/yum.repos.d/public-yum-ol7.repo. Exiting
  > ```
  >
  > Note that systems that were installed by using Oracle Linux 7.7 or later are automatically configured to use the modular yum configuration during an installation.

  b. Install the `oracle-linux-manager-server-release-el7` release package to install appropriate yum repository configuration. This package reflects the new naming convention but includes the proper information for Spacewalk 2.7.

  ```
  # yum install oracle-linux-manager-server-release-el7
  ```

  c. Enable the correct Spacewalk repositories for Spacewalk 2.7.

  ```
  # yum-config-manager --disable ol7_oracle-linux-manager210_server ol7_oracle-linux-manager210_client
  # yum-config-manager --enable ol7_spacewalk27_server ol7_spacewalk27_client
  ```

  d. Enable the `ol7_optional_latest` repository, which is included in the `oraclelinux-release-el7` package:

  ```
  # yum-config-manager --enable ol7_optional_latest
  ```

5. Install the Spacewalk Server packages that are configured to use Oracle Database.

```
# yum install spacewalk-oracle
```

Note

As part of the Spacewalk installation process, all of the Oracle Linux yum server configuration, as well as ULN configuration, is disabled because Spacewalk handles this configuration going forward.

If you need to re-enable yum repository configuration after an installation, but *before* you have configured any repositories in Spacewalk, you can temporarily rename any affected yum repository configuration files to enable them again, for example:

```
# mv /etc/yum.repos.d/oracle-linux-ol7.repo.rpmsave /etc/yum.repos.d/oracle-linux-ol7.
```

Remember to disable the yum repository configuration files again after you have configured repositories within Spacewalk.

6. (Optional) Install the `spacecmd` and `spacewalk-utils` packages if you want to use commands such as `spacecmd`, `spacewalk-common-channels`, `spacewalk-hostname-rename`, and `spacewalk-sync-setup`.

```
# yum install spacecmd spacewalk-utils
```

`spacecmd`	Enables you to administer Spacewalk from the command line. You can manage activation keys, configuration channels, kickstarts, software channels, systems, and users by using this command.
`spacewalk-common-channels`	Enables you to configure the software channels, public yum repositories, GNU Privacy Guard (GPG) keys, and activation keys for Oracle Linux from the command line.
`spacewalk-hostname-rename`	Enables you to regenerate the SSL certificate if you change the system's host name.
`spacewalk-sync-setup`	Enables you configure a primary-worker (master-slave) relationship between two Spacewalk servers that you want to use in ISS configuration. See Chapter 3, *Configuring Inter-Server Synchronization for Spacewalk Servers*.

Note

You can safely ignore any SELinux `restorecon` messages that are displayed when the packages are installed.

Alternatively, you can install the additional packages at a later time if you register the Spacewalk server as a client of itself and then subscribe it to the appropriate Spacewalk Server channel for Release 2.7.

7. Configure Spacewalk to use the Oracle Database by running the `spacewalk-setup --external-oracle` command.

   The `--external-oracle` option is used because all Oracle databases are external to Spacewalk's setup, regardless of whether the database is running on the same system.

   The following example shows how to run the command to initiate an interactive session where you provide the information that is required to complete the Spacewalk setup.

   When configuring Spacewalk, keep the following key points in mind:

   - The *sw_user* and *sw_passwd* are the Spacewalk user name and password that you specified when you configured the Oracle Database, per Section 1.4.3, "Oracle Database Configuration".

   - The value that is expected for the database service name (SID) is the global database name and *not* the value of `ORACLE_SID`.

   - The `Database hostname [localhost]?` prompt is bypassed if the setup tool detects that the Oracle Database and Spacewalk are co-located on the same host. You are only prompted for this information during the setup if the Oracle Database is on a host other than the host on which Spacewalk is installed.

   - The value that you specify for the Organization Unit must be the same as the FQDN of the server in DNS. Also, this value must match the system's host name.

```
# spacewalk-setup --external-oracle
* Setting up SELinux..
* Setting up Oracle environment.
* Setting up database.
** Database: Setting up database connection for Oracle backend.
Global Database Name or SID (requires tnsnames.ora)? company.mydom.com
Database hostname [localhost]? spacewalk-db.mydom.com
Username? sw_user
Password? sw_passwd
Database: Testing database connection.
** Database: Populating database.
*** Progress: ########################################################
* Configuring tomcat.
* Setting up users and groups.
** GPG: Initializing GPG and importing key.
** GPG: Creating /root/.gnupg directory
You must enter an email address.
Admin Email Address? my.email@mydom.com
* Performing initial configuration.
* Activating Spacewalk.
** Loading Spacewalk Certificate.
** Verifying certificate locally.
** Activating Spacewalk.
* Enabling Monitoring.
* Configuring apache SSL virtual host.
Should setup configure apache's default ssl server for you
                                  (saves original ssl.conf) [Y]? y
** /etc/httpd/conf.d/ssl.conf has been backed up to ssl.conf-swsave
* Configuring jabberd.
* Creating SSL certificates.
CA certificate password? cert_passwd
Re-enter CA certificate password? cert_passwd
Organization? Company Demo
Organization Unit [swksvr.mydom.com]? swksvr.mydom.com
Email Address [your.email@domain.com]? my.email@mydom.com
City? Redwood Shores
State? CA
Country code (Examples: "US", "JP", "IN", or type "?" to see a list)? US
```

```
** SSL: Generating CA certificate.
** SSL: Deploying CA certificate.
** SSL: Generating server certificate.
** SSL: Storing SSL certificates.
* Deploying configuration files.
* Update configuration in database.
* Setting up Cobbler..
Cobbler requires tftp and xinetd services be turned on for PXE provisioning functionality.
Enable these services [Y]? y
* Restarting services.
Installation complete.
Visit https://swksvr.mydom.com to create the Spacewalk administrator account.
```

8. Verify that the Spacewalk services are running.

```
# /usr/sbin/spacewalk-service status
router (pid 5097) is running...
sm (pid 5105) is running...
c2s (pid 5113) is running...
s2s (pid 5121) is running...
tomcat6 (pid 5193) is running...                          [  OK  ]
httpd (pid  5303) is running...
osa-dispatcher (pid  5331) is running...
rhn-search is running (5353).
cobblerd (pid 5392) is running...
RHN Taskomatic is running (5419).
```

The process IDs on your system are likely to be different from those shown in this example.

9. Note the Spacewalk server URL that is mentioned in the output.

You will need the Spacewalk server URL to create the main Spacewalk administrator account and an initial organization, as described in Section 1.6.2, "Configuring a Spacewalk Administrator and an Initial Organization".

After completing the Spacewalk server installation, perform any required or optional post-installation tasks. For instructions, see Section 1.6, "Configuring a Newly Installed Spacewalk Server",

1.6 Configuring a Newly Installed Spacewalk Server

After installing a Spacewalk server, perform the following tasks. Some tasks, although recommended, are optional.

1.6.1 Replacing a Self-Signed SSL Certificate

When you install a Spacewalk server or Spacewalk proxy, you can create a self-signed SSL certificate to use with Spacewalk clients. The following procedure describes how to replace self-signed certificates or expired CA-signed certificates with certificates that have been signed by a Certificate Authority (CA).

You can use certificates for individual Spacewalk servers or Spacewalk proxies, or wildcard certificates for all Spacewalk servers or Spacewalk proxies in the domains that the wildcard certificates cover.

Replace the existing certificate on a Spacewalk server or Spacewalk proxy as follows:

1. Create a backup of the system's existing SSL configuration.

```
# tar -cvf SSLconfig.tar \
  /etc/httpd/conf/ssl.* \
  /etc/pki/spacewalk/jabberd/server.pem \
  /root/ssl-build \
```

```
/var/www/html/pub
```

2. Obtain a server certificate by using one of the following methods:

   • Obtain a server certificate from a CA and install this certificate in the SSL build hierarchy on the system as follows:

   a. Send the Certificate Signing Request (CSR) file `/root/ssl-build/`*`swksvr`*`/server.csr` to the CA.

   > **Note**
   >
   > *swksvr* is the name of the Spacewalk server or Spacewalk proxy that you used to set up the existing SSL configuration, with the domain name removed.

   After validating your request, the CA returns a signed server certificate file.

   b. Create a backup of the signed server certificate file.

   c. If necessary, convert the certificate to Privacy Enhanced Mail (PEM) format.

   A PEM-formatted certificate file is a text file that contains a Base64 encoded certificate section between the BEGIN/END markers, as shown in the following output:

   ```
   -----BEGIN CERTIFICATE-----
   MIIF7DCCBNSgAwIBAgIQbsx6pacDIAm4zrz06VLUkTANBgkqhkiG9w0BAQUFADCB
   ...
   Rs/iGAZeqa6ogZpHFt4MKGwlJ7net4RYxh84HqTEy2Y=
   -----END CERTIFICATE-----
   ```

   A PEM-formatted certificate file usually has a file extension of `.crt` or `.pem`. However, binary DER-formatted certificate files also sometimes have a `.crt` extension.

   A DER-formatted certificate file is a binary file that usually has a file extension of `.cer` or `.der`, but can also have the extension `.cert` or `.crt`.

   Test whether a certificate file is in DER format by typing the following command:

   ```
   # openssl x509 -inform der -text -in certificate_file
   ```

   d. If a certificate file is in DER format, convert the file to a PEM-formatted certificate file by typing the following command:

   ```
   # openssl x509 -inform der -in server.cer -out server.pem
   ```

   If a PEM-formatted certificate file was not generated on a UNIX or a Linux system, the file might contain `^M` carriage return characters.

   e. Use either of the following commands to remove these characters:

   ```
   # sed -i -e 's/\r//' server.pem
   ```

   ```
   # dos2unix server.pem
   ```

   Note that the `dos2unix` command is available in the `dos2unix` package.

   f. Copy the PEM-formatted server certificate file to `/root/ssl-build/`*`swksvr`*`/server.crt`.

   ```
   # cp server.pem /root/ssl-build/swksvr/server.crt
   ```

This command overwrites the original file.

- Obtain a server certificate using an external tool as follows:

  a. Obtain both the private key and the signed certificate from the external tool in PEM format, then copy both to `/root/ssl-build/swksvr`.

  b. If the private key has an existing password, remove it, then replace the key as follows:

  ```
  # openssl rsa -in keyfilewithpasswd.key -out /root/ssl-build/swksvr/server.key
  ```

  This step ensures that Spacewalk services can start unattended.

3. Add the CA public certificate to the `/root/ssl-build` directory as the `RHN-ORG-TRUSTED-SSL-CERT` file by using one of the following methods:

   - If available, obtain the CA chain certificate from the CA that issued the server certificate. Copy this certificate file to `/root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT`:

   ```
   # cp ca_chain.pem /root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT
   ```

   - If the CA chain certificate is not available from the issuing CA, create the CA chain certificate as follows:

     a. Obtain the root CA public certificate and the intermediate CA public certificates from the issuing CA.

     b. Concatenate the chain of CA public certificate files starting with the public certificate file of the CA that issued your server certificate down to the public certificate file of the root CA to `/root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT`:

     ```
     # cat intermediate_ca.pem root_ca.pem > /root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT
     ```

     In the previous command, `intermediate_ca.pem` is the public certificate file of the intermediate CA that signed your server certificate, and `root_ca.pem` is the public certificate file of the root CA that signed the intermediate certificate.

     ⚠ **Caution**

     The order in which the public certificates in a CA chain certificate file appear is critical. The CA chain certificate does not work if its component certificates are not in the correct order.

   - If a root CA signed your server certificate directly (which is unlikely nowadays), only the public certificate of the root CA is required. Copy the root CA public certificate file to `/root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT`:

   ```
   # cp root_ca.pem /root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT
   ```

4. Validate the server certificate against the CA public certificate by typing the following command:

   ```
   # openssl verify -CAfile /root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT \
     /root/ssl-build/swksvr/server.crt
   /root/ssl-build/swksvr/server.crt: OK
   ```

   If the command returns an error, verify that you correctly created `RHN-ORG-TRUSTED-SSL-CERT` and also verify that the date and time on the server are configured correctly.

5. Store the CA public certificate in the Spacewalk database so that it is available for use in provisioning client systems:

```
# rhn-ssl-dbstore -v --ca-cert=/root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT
Public CA SSL certificate:  /root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT
```

If the command returns an error, run the command again, specifying a higher level of debugging, such as `-vvv`, to gather more information about the problem.

6. Generate and install the web server SSL package as follows:

   a. Generate the web server SSL package.

```
# rhn-ssl-tool --gen-server --rpm-only --dir /root/ssl-build

...working...

Generating web server's SSL key pair/set RPM:
    /root/ssl-build/swksvr/rhn-org-httpd-ssl-key-pair-swksvr-1.0-rev.src.rpm
    /root/ssl-build/swksvr/rhn-org-httpd-ssl-key-pair-swksvr-1.0-rev.noarch.rpm

The most current Spacewalk Proxy Server installation process against RHN hosted
requires the upload of an SSL tar archive that contains the CA SSL public
certificate and the web server's key set.

Generating the web server's SSL key set and CA SSL public certificate archive:
    /root/ssl-build/swksvr/rhn-org-httpd-ssl-archive-swksvr-1.0-rev.tar

Deploy the server's SSL key pair/set RPM:
    (NOTE: the Red Hat Satellite or Proxy installers may do this step for you.)
    The "noarch" RPM needs to be deployed to the machine working as a
    web server, or Red Hat Satellite, or Spacewalk Proxy.
    Presumably 'swksvr.mydom.com'.
```

   List the files that the packages install.

```
# rpm -qlp /root/ssl-build/swksvr/rhn-org-httpd-ssl-key-pair-swksvr-1.0-rev.src.rpm
rhn-org-httpd-ssl-key-pair-swksvr-1.0.tar.gz
rhn-org-httpd-ssl-key-pair-swksvr.spec
# rpm -qlp /root/ssl-build/swksvr/rhn-org-httpd-ssl-key-pair-swksvr-1.0-rev.noarch.rpm
/etc/httpd/conf/ssl.crt/server.crt
/etc/httpd/conf/ssl.csr/server.csr
/etc/httpd/conf/ssl.key/server.key
/etc/pki/spacewalk/jabberd/server.pem
```

   b. Install the web server SSL `noarch` package.

```
# yum install /root/ssl-build/swksvr/rhn-org-httpd-ssl-key-pair-swksvr-1.0-rev.noarch.rpm
```

7. Generate the public CA certificate package and make both the package and the CA public certificate file available to clients.

   a. Generate the public CA certificate package.

```
# rhn-ssl-tool --gen-ca --dir=/root/ssl-build --rpm-only

...working...
Generating CA public certificate RPM:
    /root/ssl-build/rhn-org-trusted-ssl-cert-1.0-rev.src.rpm
    /root/ssl-build/rhn-org-trusted-ssl-cert-1.0-rev.noarch.rpm

Make the public CA certificate publicly available:
    (NOTE: the Red Hat Satellite or Proxy installers may do this step for you.)
    The "noarch" RPM and raw CA certificate can be made publicly accessible
```

```
   by copying it to the /var/www/html/pub directory of your Red Hat Satellite or
   Proxy server.
```

List the files that the packages install.

```
# rpm -qlp /root/ssl-build/rhn-org-trusted-ssl-cert-1.0-rev.src.rpm
rhn-org-trusted-ssl-cert-1.0.tar.gz
rhn-org-trusted-ssl-cert.spec
# rpm -qlp /root/ssl-build/rhn-org-trusted-ssl-cert-1.0-rev.noarch.rpm
/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT
```

b. If a Spacewalk server or proxy is also configured as a client, install the public CA certificate `noarch` package on this system.

```
# yum install /root/ssl-build/pub/rhn-org-trusted-ssl-cert-1.0-rev.noarch.rpm
```

The public CA certificate is installed as `/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT`.

c. Copy the `rhn-org-trusted-ssl-cert-1.0-rev.noarch.rpm` package and CA public certificate file to `/var/www/html/pub` for access by clients.

```
# cp /root/ssl-build/rhn-org-trusted-ssl-cert-1.0-rev.noarch.rpm /var/www/html/pub
# cp /root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT /var/www/html/pub
```

Note

If you do not copy the updated `RHN-ORG-TRUSTED-SSL-CERT` to `/var/www/html/pub`, the `osa-dispatcher` service fails to start.

Verify that the installed copies of `RHN-ORG-TRUSTED-SSL-CERT` are identical by comparing their digest values as follows:

```
# sha1sum /root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT \
   /usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT \
   /var/www/html/pub/RHN-ORG-TRUSTED-SSL-CERT
74380a372bfa55d8ab7579bf01502c874b8aae84
                      /root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT
74380a372bfa55d8ab7579bf01502c874b8aae84
                      /usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT
74380a372bfa55d8ab7579bf01502c874b8aae84
                      /var/www/html/pub/RHN-ORG-TRUSTED-SSL-CERT
```

The `rhn-org-trusted-ssl-cert-1.0-rev.src.rpm` package is usually not made available to clients.

8. On a Spacewalk server, stop the Spacewalk services, clear the `jabberd` database, then restart Spacewalk.

```
# /usr/sbin/spacewalk-service stop
# rm -Rf /var/lib/jabberd/db/*
# /usr/sbin/spacewalk-service start
```

On a Spacewalk proxy, restart the Spacewalk proxy services.

```
# /usr/sbin/rhn-proxy restart
```

9. On the remaining Spacewalk clients, download and install the public CA certificate package.

```
# wget https://swksvr.mydom.com/pub/rhn-org-trusted-ssl-cert-1.0-rev.noarch.rpm
--2015-06-05 15:15:44--  https://swksvr.mydom.com/pub/rhn-org-trusted-ssl-cert-1.0-rev.noarch.rpm
Resolving swksvr.mydom.com... 192.168.1.3
Connecting to swksvr.mydom.com|192.168.1.3|:443... connected.
```

```
HTTP request sent, awaiting response... 200 OK
Length: 4840 (4.7K) [application/x-rpm]
Saving to: "rhn-org-trusted-ssl-cert-1.0-2.noarch.rpm"

100%[=====================================>] 4,840        --.-K/s   in 0s

2015-06-05 15:15:44 (57.5 MB/s) - "rhn-org-trusted-ssl-cert-1.0-rev.noarch.rpm" saved [4840/4840]

# yum install /root/ssl-build/pub/rhn-org-trusted-ssl-cert-1.0-rev.noarch.rpm
```

> **Note**
>
> If you subsequently replace the server certificate because it is revoked or
> expired, you do not need to update the public CA certificate on the clients unless
> you change the CA that signs the server certificate.

1.6.2 Configuring a Spacewalk Administrator and an Initial Organization

After installing a Spacewalk server and connecting to the Oracle Database, you must create the main Spacewalk administrator account and an initial organization. Follow these steps:

1. Open a browser and access the URL that is specified in the Step of 7 in Section 1.5, "Installing a Spacewalk Server".

    As shown in the following example, the server that is shown in the output is `swksvr.mydom.com`, which is the host name that you provided when you configured the Oracle Database:

    ```
    Installation complete.
    Visit https://swksvr.mydom.com to create the Spacewalk administrator account.
    ```

    Because Spacewalk uses a self-signed certificate by default, you will be prompted to trust this certificate the first time you launch the Spacewalk user interface by using a web browser, unless you have replaced the SSL certificate. See Section 1.6.1, "Replacing a Self-Signed SSL Certificate".

2. On the Create Organization page (located under Create First User), enter the required values in the appropriate fields.

3. Accept any of the default values that are provided for you.

4. If you are prompted to provide additional configuration details, click the link to be taken to a General Configuration page, where you can enter any additionally required values.

5. Save the changes and then log in to the Spacewalk web interface.

    The Overview page for the Spacewalk web interface is displayed

    See *About the Spacewalk Web Interface* in *Spacewalk for Oracle® Linux: Client Life Cycle Management Guide for Release 2.7*.

1.6.3 Replacing the jabberd/osa Database on Spacewalk Servers or Spacewalk Proxies

You might need to replace the `jabberd`/`osa` database on a Spacewalk server or proxy if you encounter any of the following errors:

*   OSA status shows "offline as of unknown" for client servers.

*   `osa-dispatcher` errors in `/var/log/mesasges` on the Spacewalk server or proxy.

- "db: corruption detected! close all jabberd processes and run db_recover" message in `/var/log/messages` on the Spacewalk server or proxy.

This problem occurs because the default Berkeley database format does not support transactions, and as a result, can become damaged when too many clients attempt to update at the same time. Switching to SQLite provides transactional support for the `jabberd` database and can handle significantly more downstream clients.

Follow these steps to resolve the problem:

1. Stop the `osa-dispatcher` and `jabberd` services.

   If you are running Oracle Linux 7, use the `systemctl` command:

   ```
   # systemctl stop osa-dispatcher
   # systemctl stop jabberd
   ```

   If you are running Oracle Linux 6, use the `service` command:

   ```
   # service osa-dispatcher stop
   # service jabberd stop
   ```

2. Edit the `/etc/jabberd/sm.xml` file and change "<driver>db</driver>" to "<driver>sqlite</driver>".

3. Edit the `/etc/jabberd/c2s.xml` file and change "<module>db</module>" to "<module>sqlite</module>".

4. Create the SQLite database as follows:

   ```
   # sqlite3 /var/lib/jabberd/db/sqlite.db < /usr/share/jabberd/db-setup.sqlite
   # chown jabber:jabber /var/lib/jabberd/db/sqlite.db
   ```

5. Start the `jabberd` and `osa-dispatcher` services again.

   For Oracle Linux 7, type the following commands:

   ```
   # systemctl start jabberd
   # systemctl start osa-dispatcher
   ```

   For Oracle Linux 6, type the following commands:

   ```
   # service jabberd start
   # service osa-dispatcher start
   ```

6. Check `/var/log/messages` to ensure that SQLite is being used.

   ```
   # cat /var/log/messages | grep sqlite
      Feb 24 12:46:18 sw24 jabberd/sm[15196]: loading 'sqlite' storage module
      Feb 24 12:46:18 sw24 jabberd/sm[15196]: initialised storage driver 'sqlite'
      Feb 24 12:46:18 sw24 c2s: Fri Feb 24 12:46:18 2017 [info] loading 'sqlite' authreg module
      Feb 24 12:46:18 sw24 c2s: Fri Feb 24 12:46:18 2017 [notice] initialized auth module 'sqlite'
      Feb 24 12:46:18 sw24 jabberd/c2s[15199]: [sirius.lot209.com] configured; realm=, authreg=sqlite,
      registration enabled, using PEM:/etc/pki/spacewalk/jabberd/server.pem
   ```

7. Reset and restart the `osad` service on the client servers.

   If you previously registered client servers and installed the `osad` service on those servers, you will need to remove the `osad-auth.conf` file and then restart the `osad` service on these systems after the database has been switched.

   For Oracle Linux 7, type the following commands:

```
# systemctl stop osad
# rm -f /etc/sysconfig/rhn/osad-auth.conf
# systemctl start osad
```

For Oracle Linux 6, type the following commands:

```
# service osad stop
# rm -f /etc/sysconfig/rhn/osad-auth.conf
# service osad start
```

Running these commands triggers the osad client on each server to re-authenticate to jabberd.

1.6.4 Configuring a Web Proxy for a Spacewalk Server

If the Spacewalk server needs to connect though a web proxy, you can configure the web proxy by using one of the following methods *after* you have installed Spacewalk:

- Edit the /etc/rhn/rhn.conf file and provide the web proxy configuration settings for the server.satellite.http_proxy, server.satellite.http_proxy_username, and server.satellite.http_proxy_password parameters, as shown in the following example:

```
server.satellite.http_proxy = webproxy.mydom.com:80
server.satellite.http_proxy_username = another
server.satellite.http_proxy_password = examplepass
```

- In the Spacewalk web interface, do the following:

  1. Select the **Admin** tab, then **Spacewalk Configuration**, and then **General**.

  2. Provide the web proxy configuration settings in the fields **HTTP proxy**, **HTTP proxy username**, **HTTP proxy password**, and **Confirm HTTP proxy password**, and then click **Update**.

1.7 Upgrading a Spacewalk Server

Upgrade a Spacewalk server for Release 2.6 to Spacewalk server for Release 2.7 as follows:

Note

If you upgrading existing Spacewalk instances that are using Oracle Database 11gR2, you *must* upgrade to at least Oracle Database 12cR1 prior to upgrading to Spacewalk Release 2.7. For more information, see Section 1.4, "Database Requirements and Configuration Instructions".

The following procedure assumes that you have set up the Spacewalk repository for Release 2.7.

Note

Make sure you do not use the jpackage repository, as that package is obsoleted in this version of Spacewalk. Either disable the package or remove the /etc/yum.repos.d/jpackage-generic.repo file.

1. Back up the all of the Spacewalk configuration files in the following directories:

   - /etc/jabberd

   - /etc/rhn

   - /etc/sysconfig/rhn

2. Back up the Server SSL build directory, typically `/root/ssl-build`.

   For example, you could create a backup by running a command similar to the following:

   ```
   # tar -cvf preSWupgrade.tar /etc/jabberd /etc/rhn /etc/sysconfig/rhn /root/ssl-build
   ```

3. Back up the Spacewalk database.

   For more information about using the Recovery Manager (RMAN) to create a backup, refer to the following documents:

   - Getting Started with RMAN (Oracle Database 11gR2)

   - Getting Started with RMAN (Oracle Database 12c)

4. Disable access to the Spacewalk Server packages for previous Spacewalk releases and enable access to the packages for Spacewalk 2.7.

   - If the Spacewalk server is registered as a client of itself, do the following:

     a. Create a Spacewalk Server channel as a child of the Oracle Linux 6 base channel.

     b. Create a Spacewalk Server repository that accesses the Spacewalk Server channel on the Oracle Linux yum server (`https://yum.oracle.com/repo/OracleLinux/OL6/spacewalk27/server/x86_64/`), using the same GPG settings as for Oracle Linux 6.

     c. Associate the Spacewalk Server repository with the Spacewalk Server channel and synchronize the repository's packages from the Oracle Linux yum server.

     d. Enable the `ol7_optional_latest` repository, which is included in the `oraclelinux-release-el7` package:

        ```
        # yum-config-manager --enable ol7_optional_latest
        ```

        Note that packages in this repository are required to perform an upgrade from Spacewalk 2.6 to Spacewalk 2.7.

     e. Change the channel subscription of the Spacewalk server in Spacewalk from the previous version to the Spacewalk Server channel for Release 2.7.

   - If the Spacewalk server is configured to obtain Spacewalk Server 2.4 or 2.6 packages from the Oracle Linux yum server, do the following:

     a. Disable the Spacewalk Server 2.4 or 2.6 repository in the Oracle Linux yum server repository configuration file. Or, delete your Spacewalk Server 2.4 or 2.6 `.repo` file.

     b. Ensure that your system is up to date and that you have transitioned to using the modular yum repository configuration by installing the `oraclelinux-release-el6` or `oraclelinux-release-el7` package and running the `/usr/bin/ol_yum_configure.sh` script. For example, on Oracle Linux 7, you would run the following command:

        ```
        # yum install oraclelinux-release-el7
        # /usr/bin/ol_yum_configure.sh
        ```

        Note

        On systems that were installed by using Oracle Linux 7.6 media or earlier, a message is displayed when you run the `/usr/bin/`

> `ol_yum_configure.sh` command if the system is already using the new modular yum repository. This message can be safely ignored:
>
> ```
> Missing /etc/yum.repos.d/public-yum-ol7.repo. Exiting
> ```
>
> Note that systems that were installed by using Oracle Linux 7.7 media or later are automatically configured to use the modular yum configuration during installation.

    c. Install the appropriate yum repository configuration.

- For Oracle Linux 6, install the `oracle-spacewalk-server-release-el6` package. The `ol6_spacewalk27_server` and the `ol6_spacewalk27_client` repositories are enabled by default in the repository configuration file.

  ```
  # yum install oracle-spacewalk-server-release-el6
  ```

- For Oracle Linux 7, install the `oracle-linux-manager-server-release-el7` package. This package reflects the new naming convention but includes the proper information for Spacewalk 2.7.

  ```
  # yum install oracle-linux-manager-server-release-el7
  ```

  Then enable the correct Spacewalk repositories for Spacewalk 2.7.

  ```
  # yum-config-manager --disable ol7_oracle-linux-manager210_server ol7_oracle-linux-manager210_client
  # yum-config-manager --enable ol7_spacewalk27_server ol7_spacewalk27_client
  ```

5. Check for any version-locked packages and delete them, for example:

   ```
   # yum versionlock list
   # yum versionlock delete cglib c3p0
   ```

6. Upgrade the Spacewalk packages.

   ```
   # yum upgrade
   ```

7. Stop the Spacewalk services.

   ```
   # /usr/sbin/spacewalk-service stop
   Shutting down spacewalk services...
   Stopping RHN Taskomatic...
   Stopped RHN Taskomatic.
   Stopping cobbler daemon:                                   [  OK  ]
   Stopping rhn-search...
   Stopped rhn-search.
   Shutting down osa-dispatcher:                              [  OK  ]
   Stopping httpd:                                            [  OK  ]
   Stopping tomcat6:                                          [  OK  ]
   Terminating jabberd processes ...
   Stopping s2s:                                              [  OK  ]
   Stopping c2s:                                              [  OK  ]
   Stopping sm:                                               [  OK  ]
   Stopping router:                                           [  OK  ]
   Done.
   ```

   You can safely ignore any SELinux `restorecon` messages that are displayed when the packages are installed.

8. Upgrade the Spacewalk database schema by typing the following command on the Spacewalk server:

   ```
   # /usr/bin/spacewalk-schema-upgrade
   ```

```
Please make sure all Spacewalk services apart from database are stopped.
Schema upgrade: [spacewalk-schema-2.6.17-1.0.1.el6] -> [spacewalk-schema-2.7.28-1.el6]
Searching for upgrade path: [spacewalk-schema-2.6.17-1.0.1] -> [spacewalk-schema-2.7.28-1]
Searching for upgrade path: [spacewalk-schema-2.6.17] -> [spacewalk-schema-2.7.28]
Searching for upgrade path: [spacewalk-schema-2.6] -> [spacewalk-schema-2.7]
The path: [spacewalk-schema-2.6] -> [spacewalk-schema-2.7]
Planning to run spacewalk-sql with [/var/log/spacewalk/schema-upgrade/20180125-085549-script.sql]

Please make sure you have a valid backup of your database before continuing.

Hit Enter to continue or Ctrl+C to interrupt:
Executing spacewalk-sql, the log is in [/var/log/spacewalk/schema-upgrade/20180125-085549-to-spacewalk-
The database schema was upgraded to version [spacewalk-schema-2.7.28-1.el6].
```

The output of the `spacewalk-schema-upgrade` command confirms whether or not the schema upgrade was successful.

In the event of a failure, do the following:

- Check the log files in the `/var/log/spacewalk/schema-upgrade` directory to determine the cause.

- Restore the database from backup.

- Fix the cause of the problem, for example, by extending the tablespaces if there is insufficient space.

- Upgrade the database schema.

9. Upgrade the Spacewalk configuration for the Oracle Database.

```
# spacewalk-setup --external-oracle --upgrade
```

> **Note**
>
> This step resets the `jabberd-dispatcher`/`osa-dispatcher` configuration back to the default. If you have switched to using SQLite, you will need to manually edit the configuration.

10. Restart the Spacewalk services.

```
# /usr/sbin/spacewalk-service start
Starting spacewalk services...
Initializing jabberd processes ...
Starting router:                                        [  OK  ]
Starting sm:                                            [  OK  ]
Starting c2s:                                           [  OK  ]
Starting s2s:                                           [  OK  ]
Starting tomcat6:                                       [  OK  ]
Waiting for tomcat to be ready ...
Starting httpd:                                         [  OK  ]
Starting osa-dispatcher:                                [  OK  ]
Starting rhn-search...
Starting cobbler daemon:                                [  OK  ]
Starting RHN Taskomatic...
Done.
```

11. Perform any necessary post-installation tasks.

Review the information in Section 1.6, "Configuring a Newly Installed Spacewalk Server".

1.8 Troubleshooting Spacewalk Server Problems

The following information describes how to diagnose and fix problems that you might encounter on a Spacewalk server. For information about other known issues and possible workarounds, see *Spacewalk for Oracle® Linux: Release Notes for Release 2.7*.

Use the `/usr/sbin/spacewalk-service status` command to verify whether any Spacewalk services are not running correctly. If a service does not start correctly, the problem is usually caused by incorrect configuration information being provided during installation.

Check the following log files for errors:

`/var/log/httpd/*`	Are `httpd` service log files.
`/var/log/rhn_satellite_install.log`	Is the installation log file.
`/var/log/rhn/reposync/*`	Are the repository synchronization log files.
`/var/log/rhn/rhn_server_satellite.log`	Is the synchronization log file.
`/var/log/rhn/rhn_server_xmlrpc.log`	Is the XML-RPC transaction log file.
`/var/log/rhn/rhn_taskomatic_daemon.log`	Is the Red Hat Network (RHN) Task Engine (Taskomatic) log messages.
`/var/log/tomcat6`	Is the Tomcat log messages for Oracle Linux 6.
`/var/log/tomcat`	Is the Tomcat log messages for Oracle Linux 7.
`/var/log/yum.log`	Is the yum log file.

1.8.1 Managing Spacewalk Logging

Spacewalk generates large numbers of log messages, particularly under the `/var/log/httpd` directory. To avoid running out of disk space, you might need to adjust the `logrotate` settings to implement more active rotation, compression, and archival of log files.

For more information, see *Oracle® Linux 6: Administrator's Guide* and *Oracle® Linux 7: Administrator's Guide*.

1.8.2 osa-dispatcher Reports a Certificate Verification Failure

When you manually start the `osa-dispatcher` service, you might encounter an error message similar to the following:

```
$ sudo systemctl start osa-dispatcher
Starting osa-dispatcher: Spacewalk 10611 2015/05/26 17:11:22 +01:00: ('Traceback caught:',)
Spacewalk 10611 2015/05/26 17:11:22 +01:00: ('Traceback (most recent call last):\n
    File "/usr/share/rhn/osad/jabber_lib.py", line 631, in connect\n
    ssl.do_handshake()\nError: [(\'SSL routines\', \'SSL3_GET_SERVER_CERTIFICATE\',
    \'certificate verify failed\')]\n',)
                                                  [FAILED]
```

This error usually indicates that the system's host name does not match its FQDN in DNS, or that you specified an incorrect FQDN for the name of the Organization Unit when you installed Spacewalk.

Resolving the issue involves regenerating the SSL certificate. However, if the system's host name has been changed over time, then regenerating the certificate requires you to provide the certificate password. To prepare, verify first that you know the correct password. Type the following command:

```
$ sudo openssl rsa -in /root/ssl-build/RHN-ORG-PRIVATE-SSL-KEY
Enter pass phrase for /root/ssl-build/RHN-ORG-PRIVATE-SSL-KEY: cert_passwd
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAvYQ/Enqo+T3WByuXiOQCpIh7eBFdqWt/e+cm3pfvGYBqi/lg
...
+rEs1ZK2mCoofnPzg2o097oPj5v4IHYh8Bmlssbk9BHvQ2ZQckSA
-----END RSA PRIVATE KEY-----
```

If you typed the correct password, the base64-encoded private key would be displayed. Otherwise, the command generates the error message `unable to load Private Key`.

After verification, proceed to the following steps:

1. Issue the following command to regenerate the certificate:

   ```
   $ sudo /usr/sbin/spacewalk-hostname-rename IP_address --ssl-orgunit=FQDN
   ```

2. If prompted for the password, type the same password that you used when you created the existing certificate previously.

3. Type the following commands to clear the `jabberd` database.

   - For Oracle Linux 6:

     ```
     $ sudo service jabberd stop
     $ sudo service osa-dispatcher stop
     $ sudo rm -Rf /var/lib/jabberd/db/*
     $ sudo service jabberd start
     $ sudo service osa-dispatcher start
     ```

   - For Oracle Linux 7:

     ```
     $ sudo systemctl stop jabberd
     $ sudo systemctl stop osa-dispatcher
     $ sudo rm -Rf /var/lib/jabberd/db/*
     $ sudo systemctl start jabberd
     $ sudo systemctl start osa-dispatcher
     ```

4. On every client that is registered with the server, verify that the value of `serverURL` in the `/etc/sysconfig/rhn/up2date` file is configured with the correct server host name or IP value, for example:

   ```
   serverURL=https://swksvr.mydom.com/XMLRPC
   ```

1.8.3 osa-dispatcher Reports an Invalid Password

If the `osa-dispatcher` service starts correctly, but later stops unexpectedly, you might see a log error similar to the following:

```
Spacewalk 2316 2015/06/05 20:38:47 +01:00: ('Invalid password',)
```

This error can occur if the `jabberd` database contains invalid entries.

To clear the error, stop the `jabberd` and `osa-dispatcher` services, clear the `jabberd` database, then restart the `jabberd` and `osa-dispatcher` services.

For Oracle Linux 6, type the following commands:

```
# service jabberd stop
# service osa-dispatcher stop
# rm -Rf /var/lib/jabberd/db/*
# service jabberd start
# service osa-dispatcher start
```

For Oracle Linux 7, type the following commands:

```
# systemctl stop jabberd
# systemctl stop osa-dispatcher
# rm -Rf /var/lib/jabberd/db/*
# systemctl start jabberd
# systemctl start osa-dispatcher
```

Note

To avoid problems with OSA, you should clear the `jabberd` database at regular intervals.

To avoid database corruption, follow the instructions in Section 1.6.3, "Replacing the jabberd/osa Database on Spacewalk Servers or Spacewalk Proxies".

1.8.4 Tomcat Does Not Start

If the Tomcat service does not start, most likely the `jta` package was installed instead of the `geronimo-jta-1.1-api` package.

To resolve the issue, remove the `jta` package and install the `geronimo-jta-1.1-api` package.

Restart the Spacewalk services.

```
# /usr/sbin/spacewalk-service restart
```

1.8.5 Tomcat Runs Out of Memory

If you see messages such as `OutOfMemoryError: Java heap space` in the Tomcat logs, increase the maximum amount of memory that is available to the Tomcat service for its heap as follows:

1. Edit the `/etc/sysconfig/tomcat6` file on Oracle Linux 6 or `/etc/sysconfig/tomcat` file on Oracle Linux 7, and increase the argument to `-Xmx` in the `JAVA_OPTS` setting.

    For example, `-Xmx1024m` increases the maximum size of the heap to 1 GB.

2. Restart the Spacewalk services.

    ```
    # /usr/sbin/spacewalk-service restart
    ```

Chapter 2 Installing and Upgrading Spacewalk Proxies

A Spacewalk proxy acts as an intermediary between Spacewalk clients and a Spacewalk server. The main purposes of a Spacewalk proxy are to mitigate the loading on the Spacewalk server and reduce the download times for Spacewalk clients.

This chapter describes how to install or upgrade a Spacewalk proxy.

2.1 Spacewalk Proxy Requirements

Oracle supports Spacewalk proxies that are running on Oracle Linux 6 (x86_64) or Oracle Linux 7 (x86_64). Oracle recommends that you update Oracle Linux with the latest packages that are available on the Oracle Linux yum server.

> **Note**
>
> Do not register a Spacewalk proxy with ULN. You can register a Spacewalk proxy as a client of itself or as a client of a Spacewalk server to receive updates.

Note the following additional requirements:

* You can install Oracle Linux 6 or Oracle Linux 7 by using the **Minimal** or **Basic Server** software set. If you select additional package groups during installation, remove the `jta` package before installing Spacewalk, as this package causes Spacewalk services to fail to start.

* Install Spacewalk by using only those packages that are provided by Oracle from the Oracle Linux yum server at https://yum.oracle.com.

* No third-party package repositories are required to install Spacewalk on Oracle Linux 6 or Oracle Linux 7. All of the required packages are available in the Spacewalk repository on the Oracle Linux yum server.

2.2 Storage Requirements for a Spacewalk Proxy

The following are the storage requirements for a Spacewalk proxy:

* A Spacewalk proxy should have a minimum of 4 GB of memory.

* Typically, the proxy cache requires 10 GB of storage for each combination of Oracle Linux release and architecture.

* By default, a Spacewalk proxy caches packages under the `/var/spool/squid` directory hierarchy and is limited to using up to 60% of the free space in the file system that contains this directory hierarchy.

2.3 Networking Requirements for a Spacewalk Proxy

The following are the networking requirements for a Spacewalk proxy:

* **Configure a fully qualified domain name**

  You must configure a fully qualified domain name (FQDN) for the Spacewalk proxy. Spacewalk does not consider `.local` and `.localdomain` to be valid domain names. Spacewalk clients must be able to resolve the Spacewalk proxy's FQDN for both forward and reverse lookups in DNS. If these conditions are not met, certificate validation and PXE booting do not work and clients cannot register with the Spacewalk server.

Verify that the host name returned by the `hostname` command and the value of `HOSTNAME` defined in `/etc/sysconfig/network` are identical and that this host name is consistent with the FQDN defined for the system in DNS for both forward and reverse lookups, as shown in the following example

```
# hostname
swkproxy.us.mydom.com
# grep HOSTNAME /etc/sysconfig/network
HOSTNAME=swkproxy.us.mydom.com
```

For Oracle Linux 6, you can also use the `host` command to verify this information:

```
# host swkproxy.us.mydom.com
swkproxy.us.mydom.com has address 10.0.0.24
# host 10.0.0.24
24.0.0.10.in-addr.arpa domain name pointer swkproxy.us.mydom.com.
```

Edit the `/etc/hosts` file and configure the actual IP address for the FQDN and host name and not the loopback address (`127.0.0.1`), as shown in the following example:

```
127.0.0.1       localhost localhost.localdomain localhost4 localhost4.localdomain4
::1             localhost localhost.localdomain localhost6 localhost6.localdomain6
10.0.0.24       swkproxy.us.mydom.com swkproxy
```

- **Port numbers for a Spacewalk proxy**

  The following table describes the network ports that a Spacewalk proxy uses, depending on its configuration.

Port/ Protocol	Direction	Purpose
80/tcp	Inbound and outbound	HTTP access
443/tcp	Inbound and outbound	HTTPS access
5222/tcp	Inbound	Push support to Spacewalk clients (if required)
5269/tcp	Inbound	Push support to Spacewalk proxies (if required)

- **Configure a web proxy**

  If the Spacewalk proxy needs to connect though a web proxy, you can configure the web proxy during installation.

- **Configure network time synchronization**

  Configure the Spacewalk server, proxies, and clients to NTP or PTP. Spacewalk requires that the system time on these systems are consistent to within 120 seconds in order to establish an SSL-based connection.

2.4 Installing a Spacewalk Proxy

> **Note**
>
> A Spacewalk Proxy should be configured with the full Spacewalk client and be registered to the Spacewalk server.

Install the Spacewalk Proxy software as follows:

1. Ensure that the `jta` package is not installed and prevent it from being installed when you install Spacewalk.

   Check whether the `jta` package is installed:

   ```
   # yum list installed | grep jta
   ```

   Remove the `jta` package:

   ```
   # yum remove jta
   ```

   To prevent the `jta` package from being installed later, either disable the Oracle Linux 6 or Oracle Linux 7 Add-ons channel (`[ol6_addons]` or `[ol7_addons]`), or add the `jta` package to the `exclude` directive in the yum configuration file, `/etc/yum.conf`, for example:

   ```
   exclude=jta*
   ```

2. Configure the system firewall.

   The following example shows how you would configure the system firewall for Oracle Linux 6:

   ```
   # iptables -I INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
   # iptables -I INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
   # iptables -I INPUT -p tcp -m state --state NEW -m tcp --dport 5222 -j ACCEPT
   # iptables -I INPUT -p tcp -m state --state NEW -m tcp --dport 5269 -j ACCEPT
   # iptables -I OUTPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
   # iptables -I OUTPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
   # iptables -I OUTPUT -p tcp -m state --state NEW -m tcp --dport 4545 -j ACCEPT
   # service iptables save
   ```

   For Oracle Linux 7, you would configure the system firewall as follows:

   ```
   # firewall-cmd --permanent --add-port=80/tcp
   # firewall-cmd --permanent --add-port=443/tcp
   # firewall-cmd --permanent --add-port=5222/tcp
   # firewall-cmd --permanent --add-port=5269/tcp
   # systemctl reload firewalld
   ```

3. If not already present on the Spacewalk server, create software channels for the Spacewalk Client and the Spacewalk Server, then subscribe the Spacewalk proxy system to these channels as follows:

   a. Create a Spacewalk Client channel as a child of either the Oracle Linux 6 or Oracle Linux 7 base channel, for the installed version of Oracle Linux.

   b. Create a Spacewalk Client repository that accesses the appropriate Spacewalk Client channel on the Oracle Linux yum server (https://yum.oracle.com/repo/OracleLinux/OL6/spacewalk27/client/x86_64/ or https://yum.oracle.com/repo/OracleLinux/OL7/spacewalk27/client/x86_64/) by using the same GPG settings as for Oracle Linux 6 or Oracle Linux 7.

c. Associate the Spacewalk Client repository with the Spacewalk Client channel and synchronize the repository's packages from the Oracle Linux yum server.

d. Create a Spacewalk Server channel as a child of either the Oracle Linux 6 or Oracle Linux 7 base channel, as appropriate, to the installed version of Oracle Linux.

e. Create a Spacewalk Server repository that accesses the appropriate Spacewalk Server channel on the Oracle Linux yum server (`https://yum.oracle.com/repo/OracleLinux/OL6/spacewalk27/server/x86_64/` or `https://yum.oracle.com/repo/OracleLinux/OL7/spacewalk27/server/x86_64/`), by using the same GPG settings as the settings for Oracle Linux 6 or Oracle Linux 7.

f. Associate the Spacewalk Server repository with the Spacewalk Server channel and synchronize the repository's packages from the Oracle Linux yum server.

g. Change the channel subscription of the Spacewalk server in Spacewalk from the previous version to the Spacewalk Server channel for Release 2.7.

h. Subscribe the Spacewalk Proxy to the Spacewalk Client and Server channels.

4. Install the Spacewalk Client software and the `openssh-clients` packages.

```
# yum install rhn-client-tools rhn-check rhn-setup rhnsd \
m2crypto yum-rhn-plugin openssh-clients
```

5. Register the system as a client of the Spacewalk server for which it will act as a Spacewalk proxy.

> **Note**
>
> Before you can register a server, you must have already created a client activation key. If enabled, a universal default key can be used. However, using a specific activation key is better.
>
> The following steps use SSL to encrypt all communication between the client and the Spacewalk server. This configuration is *mandatory.* The Proxy must use SSL to communicate to the server. Otherwise, `jabberd` will not work.

a. Download the CA certificate file `RHN-ORG-TRUSTED-SSL-CERT` to the server.

In a browser tab, navigate to **http://*swksvr_FQDN*/pub**, where *swksvr_FQDN* is the fully qualified domain name of the Spacewalk server, and download the CA certificate file `RHN-ORG-TRUSTED-SSL-CERT` to `/usr/share/rhn`.

Alternatively, you can use `wget` from the command line, for example:

```
# wget -q -O /usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT \
http://swksvr_FQDN/pub/RHN-ORG-TRUSTED-SSL-CERT
```

b. Register the system with Spacewalk by using the `rhnreg_ks` command, with the `--sslCACert` option to specify the path of the CA certificate.

```
# rhnreg_ks --sslCACert=/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT \
```

```
--serverUrl=https://swksvr_FQDN/XMLRPC --activationkey=activation_key
```

Specify the Spacewalk server or proxy by its fully qualified domain name.

c. Verify that the settings in the `/etc/sysconfig/rhn/up2date` file that are used to access the Spacewalk server are correct.

   i. Verify that `serverURL` is set to the Spacewalk server's URL, for example `https://swksvr.mydom.com/XMLRPC`:

   ```
   # grep ^serverURL= /etc/sysconfig/rhn/up2date
   serverURL=https://swksvr.mydom.com/XMLRPC
   ```

   ii. Verify that `sslCACert` is set to the correct CA certificate file, for example `/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT`:

   ```
   # grep ^sslCACert= /etc/sysconfig/rhn/up2date
   sslCACert=/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT
   ```

   Note

   If the settings are not correct, you most likely made a mistake when registering the system by using the `rhnreg_ks` command. Run the `rhnreg_ks` command again, checking that you correctly specify the path of the CA certificate and the Spacewalk server's URL. Also, make sure to specify the `--force` option to override the previous settings.

6. Install the Spacewalk Proxy installer package.

   ```
   # yum -y install spacewalk-proxy-installer
   ```

7. Create the `/root/ssl-build` directory.

   ```
   # mkdir /root/ssl-build
   ```

8. Copy the Spacewalk server's CA key and public certificate files to `/root/ssl-build`.

   ```
   # scp 'root@spacewalk_server:/root/ssl-build/{RHN-ORG-PRIVATE-SSL-KEY,\
   RHN-ORG-TRUSTED-SSL-CERT,rhn-ca-openssl.cnf}' /root/ssl-build
   RHN-ORG-PRIVATE-SSL-KEY                      100% 1751 1.7KB/s   00:00
   RHN-ORG-TRUSTED-SSL-CERT                     100% 5316 5.2KB/s   00:00
   rhn-ca-openssl.cnf                           100% 2186 2.1KB/s   00:00
   ```

9. Configure the Spacewalk proxy by running the `/usr/sbin/configure-proxy.sh` script.

   The following example shows an interactive configuration:

   ```
   # /usr/sbin/configure-proxy.sh
   Using RHN parent (from /etc/sysconfig/rhn/up2date): swksvr.mydom.com
   Using CA Chain (from /etc/sysconfig/rhn/up2date): /usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT
   HTTP Proxy []: [Enter]
   Proxy version to activate [2.7]: [Enter]
   Traceback email []: my.email@mydom.com
   Use SSL [Y/n]: Y
   Regardless of whether you enabled SSL for the connection to the Spacewalk Parent
   Server, you will be prompted to generate an SSL certificate.
   This SSL certificate will allow client systems to connect to this Spacewalk Proxy
   securely. Refer to the Spacewalk Proxy Installation Guide for more information.
   Organization []: Company Demo
   Organization Unit [swkproxy.us.mydom.com]: [Enter]
   Common Name [swkproxy.us.mydom.com]: [Enter]
   City []: Redwood Shores
   ```

```
State []: CA
Country code []: US
Email [my.email@mydom.com]: [Enter]
Cname aliases (separated by space) []: [Enter]
Spacewalk Proxy successfully activated.
Loaded plugins: rhnplugin
This system is receiving updates from RHN Classic or Red Hat Satellite.
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package spacewalk-proxy-management.noarch... will be installed
...
Transaction Summary
================================================================================
Install     42 Package(s)

Total download size: 13 M
Installed size: 32 M
Is this ok [y/N]: y
Downloading Packages:
(1/42): apr...                        | 122 kB     00:00
...
Using CA key at /root/ssl-build/RHN-ORG-PRIVATE-SSL-KEY.
Generating distributable RPM for CA public certificate:
Copying CA public certificate to /var/www/html/pub for distribution to clients:
Generating SSL key and public certificate:
CA password: cert_passwd
Installing SSL certificate for Apache and Jabberd:
Preparing packages for installation...
rhn-org-httpd-ssl-key-pair-swkproxy-1.0-1
Create and populate configuration channel rhn_proxy_config_1000010000? [Y/n]: Y
Spacewalk username: []: sw_user
Password: sw_passwd
Using server name swksvr.mydom.com
Creating config channel rhn_proxy_config_1000010000
Config channel rhn_proxy_config_1000010000 created
Using server name swksvr.mydom.com
Pushing to channel rhn_proxy_config_1000010000:
Local file /etc/httpd/conf.d/ssl.conf -> remote file /etc/httpd/conf.d/ssl.conf
Local file /etc/rhn/rhn.conf -> remote file /etc/rhn/rhn.conf
Local file /etc/squid/squid.conf -> remote file /etc/squid/squid.conf
Local file /etc/httpd/conf.d/cobbler-proxy.conf -> remote file /etc/httpd/conf.d/cobbler-proxy.conf
Local file /etc/httpd/conf/httpd.conf -> remote file /etc/httpd/conf/httpd.conf
Local file /etc/jabberd/c2s.xml -> remote file /etc/jabberd/c2s.xml
Local file /etc/jabberd/sm.xml -> remote file /etc/jabberd/sm.xml
Enabling Spacewalk Proxy.
Shutting down rhn-proxy...
Terminating jabberd processes ...
Stopping s2s:                                     [FAILED]
Stopping c2s:                                     [FAILED]
Stopping sm:                                      [FAILED]
Stopping router:                                  [FAILED]
Stopping httpd:                                   [FAILED]
Stopping squid:                                   [FAILED]
Done.
Starting rhn-proxy...
init_cache_dir /var/spool/squid... Starting squid: .      [  OK  ]
Starting httpd:                                   [  OK  ]
Initializing jabberd processes ...
Starting router:                                  [  OK  ]
Starting sm:                                      [  OK  ]
Starting c2s:                                     [  OK  ]
Starting s2s:                                     [  OK  ]
Done.
There were some answers you had to enter manually.
Would you like to have written those into file
formatted as answers file? [Y/n]: Y
```

```
Writing proxy-answers.txt.NtM1Y
```

The Spacewalk user name and password (`sw_user` and `sw_passwd`) are the Spacewalk server administrator's user name and password.

> **Note**
>
> The information that you provide is optionally recorded in a file named `proxy-answers.txt.UID`, where `UID` is a unique identifier. You can use this file to automate the configuration of a Spacewalk proxy, as shown in the following example:
>
> ```
> # configure-proxy.sh --non-interactive --answer-file=proxy-answers.txt.NtM1Y
> ```

10. If you want to use third-party CA-signed SSL certificate instead of the self-signed SSL certificate, follow the procedure described in Section 1.6.1, "Replacing a Self-Signed SSL Certificate".

> **Note**
>
> Oracle recommends that you replace the self-signed SSL certificate before registering any clients. Otherwise, you must log on separately to each existing client and configure it to use the new SSL certificate. You cannot do this from the Spacewalk server.

11. To check that the Spacewalk proxy is running correctly, specify the URL of the proxy when registering a Spacewalk client, as shown in the following example

```
rhnreg_ks --sslCACert=/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT \
  --serverUrl=https://swkproxy_FQDN/XMLRPC --activationkey=activation_key
```

After registering the client, subscribe it to software channels on the server and verify that you can update packages from the client.

2.5 Upgrading a Spacewalk Proxy

Upgrade a Spacewalk proxy as follows:

1. If not already present on the Spacewalk server, create software channels for the Spacewalk Client and the Spacewalk Server for Release 2.7, then subscribe the Spacewalk proxy system to these channels as follows:

    a. Create a Spacewalk Client channel as a child of either the Oracle Linux 6 base channel.

    b. Create a Spacewalk Client repository that accesses the Spacewalk Client channel on the Oracle Linux yum server (`https://yum.oracle.com/repo/OracleLinux/OL6/spacewalk27/client/x86_64/`), using the same GPG settings as for Oracle Linux 6.

    c. Associate the Spacewalk Client repository with the Spacewalk Client channel and synchronize the repository's packages from the Oracle Linux yum server.

    d. Create a Spacewalk Server channel as a child of the Oracle Linux 6 base channel.

    e. Create a Spacewalk Server repository that accesses the Spacewalk Server channel on the Oracle Linux yum server (`https://yum.oracle.com/repo/OracleLinux/OL6/spacewalk27/server/x86_64/`), using the same GPG settings as for Oracle Linux 6.

    f. Associate the Spacewalk Server repository with the Spacewalk Server channel and synchronize the repository's packages from the Oracle Linux yum server.

g. Change the channel subscription of the Spacewalk server in Spacewalk from the previous release to the Spacewalk server channel for Release 2.7.

h. Subscribe the Spacewalk proxy to the Spacewalk Client and Spacewalk Server channels for Release 2.7 instead of the Spacewalk Server and Client channels for Release 2.6.

2. Back up the CA key, SSL certificate and the openSSL configuration file in `/root/ssl-build`.

   For example, you could use the `tar` command as follows to create a backup:

   ```
   # cd /root/ssl-build
   # tar -cvf /tmp/sslcerts.tar RHN-ORG-PRIVATE-SSL-KEY RHN-ORG-TRUSTED-SSL-CERT rhn-ca-openssl.cnf
   ```

3. Run the `yum update` command to update all of the packages on the system.

   ```
   # yum update
   ```

4. If necessary, extract the CA key, SSL certificate, and openSSL configuration file from your backup file to `/root/ssl-build`:

   ```
   # cd /root/ssl-build
   # tar -xvf /tmp/sslcerts.tar
   ```

5. Configure the Spacewalk proxy by running the `configure-proxy.sh` script.

   The following example uses the `proxy-answers.txt.UID` file that was saved from a previous installation to perform the configuration:

   ```
   # configure-proxy.sh --non-interactive --answer-file=proxy-answers.txt.NtM1Y
   ```

   You can also run this command interactively by omitting any command-line options.

2.6 Troubleshooting Spacewalk Proxy Installation Problems

The following information describes how to diagnose and fix problems that you might encounter on a Spacewalk proxy.

For information about other known issues and possible workarounds, see *Spacewalk for Oracle® Linux: Release Notes for Release 2.7*.

Use the `rhn-proxy status` command to find out which Spacewalk proxy services are not running correctly. If a service does not start correctly, the problem is usually caused by incorrect configuration information being provided during installation.

Verify that the `/etc/sysconfig/rhn/systemid` file is owned by `root:apache` and that its mode is set to 640.

Check the following log files for errors:

`/var/log/httpd/*`	Are the `httpd` service log files.
`/var/log/rhn/` `rhn_proxy_broker.log`	Is the proxy brokering service log file.
`/var/log/rhn/` `rhn_proxy_redirect.log`	Is the proxy SSL redirection service log file.
`/var/log/squid/*`	Are the squid proxy log files.

`/var/log/yum.log`   Is the yum log file.

2.6.1 Clearing the Proxy Cache

If required to clear up package provisioning problems, you can clear the proxy cache as follows:

1. Stop the `httpd` and `squid` services.

    For Oracle Linux 6, type the following commands:

    ```
    # service httpd stop
    # service squid stop
    ```

    For Oracle Linux 7, type the following commands:

    ```
    # systemctl stop httpd
    # systemctl stop squid
    ```

2. Delete the contents of the cache as follows:

    ```
    # rm -Rf /var/cache/rhn/*
    ```

3. Restart the `squid` and `httpd` services.

    For Oracle Linux 6, type the following commands:

    ```
    # service squid start
    # service httpd start
    ```

    For Oracle Linux 7, type the following commands:

    ```
    # systemctl start squid
    # systemctl start httpd
    ```

Chapter 3 Configuring Inter-Server Synchronization for Spacewalk Servers

You can configure ISS to synchronize channel content, channel permissions, and organizational trust settings between Spacewalk servers. The configuration of local non-content settings for users and organizations is not affected. One Spacewalk server acts as a *primary* to provide content to any number of *worker* Spacewalk servers.

Typical use cases include the following:

- Content on the worker servers is regularly synchronized with the primary server to obtain the latest maintenance releases.

- Content is developed and tested on the primary server before distribution to the worker servers.

- Worker servers have local content that is additional to that synchronized from the primary server.

You can configure primary servers that are themselves workers of a higher-level primary Spacewalk server. The usual ISS topology is a tree-like hierarchy, where there is one top-level primary server and each worker has only one primary server, rather than a directed graph, where there might be several top-level primary servers and each worker can have more than one primary server. If a worker has more than one primary server, you can designate one to be the default primary server with which the worker synchronizes.

You can use the `spacewalk-sync-setup` command to set up the relationships between primary server and worker Spacewalk servers, or you can use the Spacewalk web interface to configure each server independently.

3.1 Enabling or Disabling Worker Synchronization Support for a Spacewalk Server

By default, a Spacewalk server is configured so that it can act as a primary server. Any worker servers that you configure for the primary server will be able to synchronize from it. The following steps are not usually necessary unless you want to disable this feature on a Spacewalk server that acts only as a worker server.

Enable or disable support for worker synchronization on a Spacewalk server as follows:

1. To disable ISS support, edit `/etc/rhn/rhn.conf` and set the value of `disable_iss` to 1:

   ```
   disable_iss=1
   ```

   To enable ISS support, edit `/etc/rhn/rhn.conf` and set the value of `disable_iss` to 0:

   ```
   disable_iss=0
   ```

2. Restart the `httpd` service.

   For Oracle Linux 6, type the following command:

   ```
   # service httpd restart
   ```

   For Oracle Linux 7, type the following command:

   ```
   # systemctl restart httpd
   ```

3.2 Configuring Primary and Worker Spacewalk Servers With the spacewalk-sync-setup Command

> **Note**
>
> Before you can configure ISS, Spacewalk must be installed and running on both the primary and worker servers.

The `spacewalk-sync-setup` command is available in the `spacewalk-utils` package.

On either of the Spacewalk servers, run the `spacewalk-sync-setup` command.

```
# spacewalk-sync-setup --apply --create-templates \
  --ms=primary_swksvr_FQDN --ml=primary_swadm --mp=primary_swadm_passwd \
  --ss=worker_swksvr_FQDN --sl=worker_swadm --sp=worker_swadm_passwd
```

In the previous example, `primary_swksvr_FQDN` is the fully qualified domain name of the Spacewalk server that will act as the primary server and the `primary_swadm` and `primary_swadm_passwd` values specify the Spacewalk administrator's user name and password for that server.

The `worker_swksvr_FQDN` value is the fully qualified domain name of the Spacewalk server that will act as the worker server and the `worker_swadm` and `worker_swadm_passwd` values specify the Spacewalk administrator's user name and password for that server.

The following is the typical output that is displayed when running this command:

```
# spacewalk-sync-setup --apply --create-templates \
  --ms=swksvr.mydom.com --ml=swadm --mp=swpass \
  --ss=swksvr2.mydom.com --sl=swadm2 --sp=swpass2
INFO: Connecting to swadmin@swksvr.mydom.com
INFO: Connecting to swadmin@swksvr2.mydom.com
INFO: Generating master-setup file /root/.spacewalk-sync-setup/master.txt
INFO: Generating slave-setup file /root/.spacewalk-sync-setup/slave.txt
INFO: About to wget master CA cert: [wget -q -O
/usr/share/rhn/swksvr.mydom.com_RHN-ORG-TRUSTED-SSL-CERT
http://swksvr.mydom.com/pub/RHN-ORG-TRUSTED-SSL-CERT]
INFO: Applying master-setup /root/.spacewalk-sync-setup/master.txt
INFO: Applying slave-setup /root/.spacewalk-sync-setup/slave.txt
```

A copy of the primary server's CA certificate is stored on the worker as `/usr/share/rhn/swksvr.mydom.com_RHN-ORG-TRUSTED-SSL-CERT`.

You can then map local organizations on the worker server to organizations that the primary server exports. See Section 3.5, "Mapping a Local Organization to an Exported Organization by Using the Spacewalk Web Interface".

3.3 Configuring a Primary Spacewalk Server by Using the Spacewalk Web Interface

Configure a primary Spacewalk server as follows:

1. Go to **Admin**, select **ISS Configuration**, and then select the **Master Setup** tab.

2. On the Known Slave Instances page, click **+ Add new slave**.

3. On the Edit Slave Details page, type the FQDN of the worker server and select or deselect the check boxes that configure worker and organization synchronization.

For example, you might want to enable the worker to synchronize from the primary server, but not want to synchronize all organizations to the worker.

4. Click Create.

    When the page refreshes, you are able to select which organizations can be exported. By default, no organizations are selected.

5. Select the organizations that you want to enable to be exported to the worker, then click **Allow Orgs**.

3.4 Configuring a Worker Spacewalk Server by Using the Spacewalk Web Interface

Configure a worker Spacewalk server as follows:

1. In a browser tab, navigate to `http://primary_swksvr_FQDN/pub`, where `primary_swksvr_FQDN` is the FQDN of the primary Spacewalk server, and download the CA certificate file `RHN-ORG-TRUSTED-SSL-CERT` as `RHN-ORG-TRUSTED-SSL-CERT-MASTER`.

    Alternatively, you can use the `wget` command as follows:

    ```
    # wget -q -O /usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT-MASTER \
    http://primary_swksvr_FQDN/pub/RHN-ORG-TRUSTED-SSL-CERT
    ```

2. In the Spacewalk web interface, go to **Admin**, select **ISS Configuration** and then select the **Slave Setup** tab.

3. On the Known Master Instances page, click **+ Add new master**.

4. On the Details for new Master page, type the FDQN of the primary server and the absolute path name of the primary's CA certificate that you downloaded (`RHN-ORG-TRUSTED-SSL-CERT-MASTER`), then select whether the primary will be the default one with which the worker synchronizes.

5. Click **Add new master**.

    The page refreshes to display a Configure primary-to-Slave Org Mappings section that enables you to configure local names for the organizations that the primary exports. When you synchronize content, access permissions that you have configured for channels on the primary server propagate to the worker server. You can choose which organizations, and any associated channel permissions, to map to a worker server.

    If necessary, create the local organizations to be mapped to the organizations that the primary server exports as follows:

    a. Go to **Admin**, select **Organizations** and click **+ create new organization**.

    b. On the Create New Organization page, provide the details for the organization, including its name and the login details of its administrator.

    > **Note**
    >
    > You must create a new user to act as the organization's administrator, as the Spacewalk administrator cannot perform this role.

    c. Click **Create Organization**.

     d. To return to the Configure Master-to-Slave Org Mappings section for the primary server instance, go to **Admin**, select **ISS Configuration**. Then, select the **Slave Setup** tab and click the name of the primary server instance.

6. In the Configure Master-to-Slave Org Mappings section, select the local organizations that map to the organizations that the primary server exports.

7. For each exported organization in the Master Org Name column, use the pull-down menu in the Matching Local Org column to select the local organization that should map to the export organization.

    If you do not want to import an organization, select **NOT MAPPED**.

8. Click **Update**.

3.5 Mapping a Local Organization to an Exported Organization by Using the Spacewalk Web Interface

Map local organizations on a worker server to organizations exported by a primary server as follows:

1. On the worker server, to view the organizations that a primary server exports, go to **Admin**, select **ISS Configuration**, select the **Slave Setup** tab, and click the name of the primary server instance.

2. On the worker server, create the local organizations that you want to map to the organizations that the primary server exports.

    Create a local organization as follows:

    a. Go to **Admin**, select **Organizations** and click **+ create new organization**.

    b. On the Create New Organization page, provide the details for the organization, including its name and the login details of its administrator.

> **Note**
>
> You must create a new user to act as the organization's administrator, as the Spacewalk administrator cannot perform this role.

    c. Click **Create Organization**.

    d. To return to the Configure Master-to-Slave Org Mappings section for the primary server instance, go to **Admin**, select **ISS Configuration**. Then, select the **Slave Setup** tab and click the name of the primary server instance.

3. In the Configure Master-to-Slave Org Mappings section, select the local organizations that map to the organizations that the primary server exports.

    For each exported organization in the Master Org Name column, use the pull-down in the Matching Local Org column to select the local organization that should map to the export organization. If you do not want to import the organization, select **NOT MAPPED**.

4. Click **Update**.

3.6 Synchronizing Software Channels on a Spacewalk Worker Server

You synchronize a software channel by running the `satellite-sync` command on the worker server as follows:

```
# satellite-sync [--iss-parent=primary_swksvr_FQDN] [--orgid=N] -c channel_label
```

In the previous command, `channel_label` specifies the label of the software channel to synchronize from the primary server.

The argument to the `--orgid` option specifies the ID of the organization on the worker into which the channel is synchronized. If not specified, the Spacewalk Default Organization with ID 1 is assumed.

The `primary_swksvr_FQDN` value specifies the FQDN of the primary Spacewalk server. If not specified, and the worker server has more than one primary, the default primary server is assumed.

Output that is similar to the following is displayed when you perform an initial synchronization of a software channel on a worker server from the Spacewalk Default Organization on the default primary server:

```
# satellite-sync -c oraclelinux6-x86_64-patch
16:16:52 Spacewalk - live synchronization
16:16:52    url: https://swksvr.mydom.com
16:16:52    debug/output level: 1
16:16:52    db:  c##spacewalk2/<password>@//odbsvr.mydom.com/company.mydom.com
16:16:52
16:16:52 Retrieving / parsing orgs data
16:16:52 orgs data complete
16:16:52
16:16:52 Retrieving / parsing channel-families data
16:16:52 channel-families data complete
16:16:52
16:16:52 Retrieving / parsing product names data
16:16:52 product names data complete
16:16:52
16:16:52 Retrieving / parsing arches data
16:16:53 arches data complete
16:16:53
16:16:53 Retrieving / parsing additional arches data
16:16:53 additional arches data complete
16:16:53
16:16:53 Retrieving / parsing channel data
16:16:54    p = previously imported/synced channel
16:16:54    . = channel not yet imported/synced
16:16:54    base-channels:
16:16:54        NONE RELEVANT
16:16:54    oraclelinux6-x86_64:
16:16:54      . oraclelinux6-x86_64-patch   1367    full import from Fri Jul 10 13:02:52 2015
16:16:54
16:16:54 Channel data complete
16:16:54
16:16:54 Retrieving short package metadata (used for indexing)
16:16:54    Retrieving / parsing short package metadata: oraclelinux6-x86_64-patch (1367)
16:17:01 Diffing package metadata (what's missing locally?): oraclelinux6-x86_64-patch

        _____
Diffing:    ##################################### - complete
16:17:04
16:17:04 Downloading package metadata
16:17:04    Retrieving / parsing *relevant* package metadata: oraclelinux6-x86_64-patch (1357)
16:17:04    * WARNING: this may be a slow process.

        _____
Downloading:##################################### - complete
16:42:30
```

```
16:42:30 Downloading rpm packages
16:42:30    Fetching any missing RPMs: oraclelinux6-x86_64-patch (1357)
16:42:53    Total size: 5.31 GiB
16:47:53 Processing rpm packages complete
16:47:53
16:47:53 Importing package metadata
16:47:53    Importing *relevant* package metadata: oraclelinux6-x86_64-patch (1357)
            _____
Importing:  ######################################## - complete
18:06:44
18:06:44 Linking packages to channels
18:07:02
18:07:02 Downloading errata data
18:07:02    Retrieving / parsing errata data: oraclelinux6-x86_64-patch (216)
            _____
Downloading:######################################## - complete
18:07:06 Downloading errata data complete
18:07:06
18:07:06 Downloading kickstartable trees metadata
18:07:06    Retrieving / parsing kickstart data: oraclelinux6-x86_64-patch (NONE RELEVANT)
18:07:06
18:07:06 Downloading kickstartable trees files
18:07:06    Retrieving / parsing kickstart tree files: oraclelinux6-x86_64-patch (NONE RELEVANT)
18:07:06
18:07:06 Importing channel errata
18:07:13    Importing *relevant* errata: oraclelinux6-x86_64-patch (468)
            _____
Downloading:######################################## - complete
18:07:31    No new kickstartable tree to import
    Import complete:
        Begin time: Fri Jul 10 16:16:51 2015
        End time:   Fri Jul 10 18:07:31 2015
        Elapsed:    1 hours, 50 minutes, 40 seconds
```