Oracle Linux Manager
Installation Guide for Release 2.10

ORACLE®

Contents

Preface

1   Installing and Upgrading Oracle Linux Manager Servers

2   Installing and Upgrading Oracle Linux Manager Proxies

3   Configuring Inter-Server Synchronization for Oracle Linux Manager Servers

4   Troubleshooting Oracle Linux Manager Problems

Preface

Oracle® Linux Manager: Installation Guide describes how to install Oracle Linux Manager 2.10 in Oracle Linux 7servers and proxies. Oracle Linux Manager 2.10 is based on the Spacewalk open source software.

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.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at https://www.oracle.com/corporate/accessibility/.

Access to Oracle Support for Accessibility

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit https://www.oracle.com/corporate/accessibility/learning-support.html#support-tab.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. 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 ongoing and will take time and external cooperation.

1
Installing and Upgrading Oracle Linux Manager Servers

This chapter describes how to install and upgrade Oracle Linux Manager servers.

For information about the types of support that Oracle provides for Oracle Linux Manager 2.10, refer to the About Oracle Linux Manager Server and Client Support section of the Oracle Linux Manager: Release Notes for Release 2.10 .

Oracle Linux Manager Server Requirements

As the primary component in the entire setup, Oracle Linux Manager sever has different sets of requirements to efficiently manage client systems that are registered to the server.

Oracle Linux Requirements

Complete the following requirements for the designated Oracle Linux Manager server:

- Install Oracle Linux 7 by using either the **Minimal** or **Basic Server** profile.
- Before installing Oracle Linux Manager, remove the `jta` package which prevents Oracle Linux Manager services from starting.
- Use 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.
- Update your system with the latest packages from the Oracle Linux yum server.
- **Do not register an Oracle Linux Manager 2.10 server or client with ULN.** Instead, register an Oracle Linux Manager 2.10 server as a client of itself to receive updates.

Memory Requirements

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

In large deployments where Oracle Linux Manager server services and maintains a large number of clients, custom channels, and so on, consider installing 16 GB of RAM. Increasing RAM improves performance in operations such as building repositories, which requires sizeable amounts of memory. See Memory Considerations When Building Repositories in Oracle Linux Manager: Client Life Cycle Management Guide for Release 2.10 .

Storage Requirements

To preserve errata mapping, by default, Oracle Linux Manager maintains all of the available versions of available packages in each software channel that you configure. As a result, the storage requirements for an Oracle Linux Manager 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.

With Oracle Linux Manager 2.10, you can reduce the storage requirements considerably by using the following command when synchronizing packages:

```
sudo spacewalk-repo-sync --latest
```

The server then synchronizes only the latest packages that are available at the time of synchronization. It does not remove older packages from the channel.

> ⚠️ **Caution:**
>
> If the synchronization interval is large, you might miss a particular version of a package. Errata handling, which manages errata that are associated with specific package versions, would be affected. If errata consistency is important to you, Oracle recommends that you do *not* use the `--latest` option. However, using the option with a Ksplice channel is an exception because its packages are always cumulative.

> 🛇 **Important:**
>
> **DO NOT** use the `--latest` option when synchronizing module-enabled channels such as `ol8_AppStream`. The mechanism that underlies this option is not module-aware and if used, will skip required packages.

An Oracle Linux Manager 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 Oracle Linux Manager. 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.

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

Networking Requirements

The following are network requirements to install an Oracle Linux Manager server:

- Static IP address
- Correctly configured forward and reverse DNS host name, with the following specifications:

> **⚠ Caution:**
>
> Noncompliance with these specifications for the server's host name can cause Oracle Linux Manager to fail in proxy communications, inter-server synchronization (ISS), certificate validation, and other areas of operation.

– The host name of the server must **not** contain uppercase letters.

– While the `/etc/hostname` file contains the short name of the host, the `/etc/hosts` file **must** specify the host's FQDN, as shown in bold in the following example:

```
cat /etc/hostname

olmsvr

cat /etc/hosts

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

Note that Oracle Linux Manager does not consider `.local` and `.localdomain` to be valid domain names.

• Port numbers

The following table describes the network ports that an Oracle Linux Manager 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 Oracle Linux Manager clients (if required)
`5269`/tcp	Inbound	Push support to Oracle Linux Manager proxies (if required)

• Configured network time synchronization

Configure Oracle Linux Manager server, proxies, and clients to use a network time synchronization mechanism such as the Network Time Protocol (NTP) or the Precision Time Protocol (PTP). To establish a Secure Socket Layer (SSL) based connection, Oracle Linux Manager requires that the system times on server and client systems be consistent to within 120 seconds.

For more information, see Configuring Network Time in Oracle Linux 7: Setting Up Networking.

Database Requirements and Configuration Instructions

Oracle supports *only* Oracle Database for use with Oracle Linux Manager. Thus, while you can use PostgreSQL with the software, this setup is not covered by Oracle support. Additionally, Oracle does not provide any tools for migrating from an unsupported database.

In general, you should use supported Oracle databases when using Oracle Linux Manager 2.10. For specific supported versions, see Oracle Database Support in Oracle Linux Manager: Release Notes for Release 2.10 . Oracle provides a restricted-use license for the use of Oracle Database Enterprise Edition with Oracle Linux Manager 2.10 for Oracle Linux support customers.

For more information about Oracle licenses, see Oracle Linux 7: Licensing Information User Manual.

> **⊘ Important:**
>
> Providing comprehensive information about operating supported databases is outside the scope of this documentation. For any database operation such as installation, configuration, upgrade, and other related tasks, consult your Oracle Database administrator and the Oracle Database documentation at https://docs.oracle.com/en/database/database.html.

Oracle Database Installation Requirements

Prior to installing Oracle Linux Manager server, you must install an Oracle Database server, make this server available, and ensure that it is operational.

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

The following database installation requirements apply to Oracle Linux Manager server installations:

- For fresh installations of the server, use Oracle Database Enterprise edition 19c or Oracle Database Enterprise edition 12c.

- For upgrades to the server, Oracle **strongly** suggests that you use Oracle Database Enterprise edition 19c.

Database Sizing Requirements

When determining the amount of space Oracle Linux Manager 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 server (typically, 250 KiB per client system).

- Number of channels allocated to each client system (about 500 KiB per channel).

- Number of packages that each channel will contain (approximately 230 KiB per package in the channel. A channel with 5000 packages would require 1.1 GiB).

For example, if you have a large Oracle Linux Manager 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.

Oracle Database Configuration

The following are general guidelines for configuring Oracle Database. You can perform these steps during or after the database installation. Always consult with your Oracle database administrator for matters related to installing or configuring the database for your particular environment.

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

- The database must have an Oracle Linux Manager user.

  For every Oracle Linux Manager server that shares the same database server, you must create a separate Oracle Linux Manager user.

- The Oracle Linux Manager user must be assigned the `CONNECT` and `RESOURCE` roles.

- The Oracle Linux Manager user must have the following system privileges:

  — `ALTER SESSION`

  — `CREATE SYNONYM`

  — `CREATE TABLE`

  — `CREATE TRIGGER`

  — `CREATE VIEW`

  — `UNLIMITED TABLESPACE`

  — `SELECT ON V_$PARAMETER`

Creating an Oracle Linux Manager User on an On-Premise Database

The steps to follow depend on whether you connect to the container database first or directly to the pluggable database.

For all cases, you must log in to your Oracle account first before performing these steps.

- If you are connecting to the container database first, choose one of the following methods:

  — Running the `ALTER SESSION` command before creating the user

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

       ```
       cd $ORACLE_HOME/bin
       sqlplus / as SYSDBA
       ```

    2. Type the following command:

       ```
       SQL> ALTER SESSION SET CONTAINER = DEVPDB;
       ```

    3. For each Oracle Linux Manager user that you need to set up, run the following commands:

       ```
       SQL> create user olm_user identified by olm_passwd;
       SQL> grant connect,resource to olm_user;
       SQL> grant alter session, create synonym, create table, create trigger,
       ```

```
          create view to olm_user;
          SQL> grant select on v_$parameter to olm_user
          SQL> grant unlimited tablespace to olm_user;
```

– Creating the user directly

1. Log in to the container database as a database administrator (typically, SYS or SYSDBA).

```
cd $ORACLE_HOME/bin
sqlplus / as SYSDBA
```

2. For each Oracle Linux Manager user that you need to set up, run the following commands:

> ❗ **Important:**
>
> Make sure to use the required c## prefix for the user name.

```
SQL> create user c##olm_user identified by olm_passwd;
SQL> grant connect,resource to c##olm_user;
SQL> grant alter session, create synonym, create table, create
trigger, create view to olm_user;
SQL> grant select on v_$parameter to olm_user
SQL> grant unlimited tablespace to c##olm_user;
```

• If you are connecting directly to the pluggable database:

1. Log in to the PDB as a database administrator (typically, SYS or SYSDBA).

```
cd $ORACLE_HOME/bin
sqlplus / as SYSDBA
```

2. For each Oracle Linux Manager user that you need to set up, run the following commands:

```
SQL> create user olm_user identified by olm_passwd;
SQL> grant connect,resource to olm_user;
SQL> grant alter session, create synonym, create table, create trigger,
create view to olm_user;
SQL> grant select on v_$parameter to olm_user
SQL> grant unlimited tablespace to olm_user;
```

Installing Oracle Linux Manager Server

Follow these steps to install Oracle Linux Manager server software:

1. Ensure that the Oracle Database is running.

   See Oracle Database Installation Requirements.

2. Install Oracle Instant Client.

   a. Download the latest 18.5 release of the following Instant Client RPM packages.

   • Instant Client Package (Basic)

   • Instant Client Package (SQL*Plus)

The packages can be downloaded from https://www.oracle.com/database/
technologies/instant-client.html.

b. Install the Instant Client packages.

```
sudo yum install oracle-instantclient18.5-basic-18.5.0.0.0-3.x86_64.rpm oracle-
instantclient18.5-sqlplus-18.5.0.0.0-3.x86_64.rpm
```

c. Add the library path to `ldconfig`.

```
echo "/usr/lib/oracle/18.5/client64/lib" | sudo tee /etc/ld.so.conf.d/oracle-
instantclient18.5.conf
sudo ldconfig
```

3. Ensure that the `jta` package is not installed.

a. Remove the `jta` package if it is installed on the system.

```
sudo yum list installed | grep jta
sudo yum remove jta
```

b. To prevent any future accidental installation of the package, do one of the following:

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

```
exclude=jta*
```

- Disable the Oracle Linux 7 `addons` channel (`[ol7_addons]`).

```
sudo yum-config-manager --disable ol7_addons
```

4. Configure the system firewall.

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

5. Install the latest `oracle-release-el7` package.

```
sudo yum install oracle-release-el7
```

If your system is running an Oracle Linux release that is earlier than Oracle Linux 7 Update 7, run the following additional command to make the system use the modular yum repository configuration.

```
sudo /usr/bin/ol_yum_configure.sh
```

6. Install and enable the Oracle Linux Manager yum repository.

```
sudo yum install oracle-linux-manager-server-release-el7
sudo yum-config-manager --enable ol7_optional_latest
```

7. Install the following packages for enabling Oracle Linux Manager server to use Oracle Database.

```
sudo yum install spacewalk-oracle spacecmd spacewalk-utils
```

ORACLE®

> **✎ Note:**
>
> As part of Oracle Linux Manager installation process, all of the Oracle Linux yum server configuration, as well as ULN configuration, are disabled. After the installation, Oracle Linux Manager handles this configuration henceforth.
>
> If you need to re-enable yum repository configuration after an installation, but *before* you have configured any repositories in Oracle Linux Manager, you can temporarily rename any affected yum repository configuration files to enable them again, for example:
>
> ```
> sudo mv /etc/yum.repos.d/oracle-linux-ol7.repo.rpmsave /etc/
> yum.repos.d/oracle-linux-ol7.repo
> ```
>
> Remember to disable the yum repository configuration files again after you have configured repositories within Oracle Linux Manager.

8. Configure Oracle Linux Manager to use the Oracle Database.

```
sudo spacewalk-setup --external-oracle
```

The command initiates an interactive session that prompts you for information about your current database.

Global Database Name or SID
Name of the database when it was set up. If necessary, inquire with your database administrator for the information.

Database hostname [localhost]
FQDN of the database system if that system is separate from Oracle Linux Manager server. Otherwise, this prompt is skipped.

Username and Password
Credentials of the database Oracle Linux Manager user.

> **⚠ Caution:**
>
> The user name you specify must match the name you previously created when following the steps in Oracle Database Configuration. For example, if the name has the `c##` prefix, that name must also be specified here.

Admin Email Address
Email address of the Oracle Linux Manager administrator.

Organization
Name of your Oracle Linux Manager organization.

Organization Unit
Oracle Linux Manager server's FQDN.

Email address

Email address of person managing the certificates, if different from the Admin Email Address.

Location prompts

Information identifying the location of Oracle Linux Manager server.

The following is an example of the interactive session:

```
sudo 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]? olmmanager-db.mydom.com
Username? olm_user
Password? olm_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.
** Package installation: Locking required rpm versions.
* 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
Cname alias of the machine (comma separated)?
Organization? Company Demo
Organization Unit [olmsvr.mydom.com]? olmsvr.mydom.com
Email Address [your.email@domain.com]? my.email@mydom.com
City? city
State? state
Country code (Examples: "US", "JP", "IN", or type "?" to see a list)? country
** 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://olmsvr.mydom.com to create the Oracle Linux Manager administrator
account.
```

9. Verify that Oracle Linux Manager services are running.

In the following example, the status is displayed in bold.

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

● tomcat.service - Apache Tomcat Web Application Container
   Loaded: loaded (/usr/lib/systemd/system/tomcat.service; enabled; vendor
preset: disabled)
   Active: **active (running)** since Thu 2020-01-16 22:37:14 UTC; 18h ago
 Main PID: 29861 (java)
   CGroup: /system.slice/tomcat.service
           └─29861 /usr/lib/jvm/jre/bin/java -ea -Xms256m -Xmx256m -
Djava.awt.headless=true
-Dorg.xml.sax.driver=org.apache.xerces.parsers.SAXParser -
...

● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor
preset: disabled)
   Active: **active (running)** since Thu 2020-01-16 22:37:28 UTC; 18h ago
     Docs: man:httpd(8)
           man:apachectl(8)
 Main PID: 30034 (httpd)
   Status: "Total requests: 2504; Current requests/sec: 0; Current
traffic: 0 B/sec"
   CGroup: /system.slice/httpd.service
           ├─30034 /usr/sbin/httpd -DFOREGROUND
           ├─30036 /usr/sbin/httpd -DFOREGROUND
           ...

● rhn-search.service - Oracle Linux Manager search engine
   Loaded: loaded (/usr/lib/systemd/system/rhn-search.service; enabled;
vendor preset: disabled)
   Active: inactive (dead) since Thu 2020-01-16 22:37:32 UTC; 18h ago
  Process: 30181 ExecStop=/usr/sbin/rhn-search stop (code=exited, status=0/
SUCCESS)
  Process: 30040 ExecStart=/usr/sbin/rhn-search start (code=exited, status=0/
SUCCESS)
 Main PID: 30073 (code=exited, status=0/SUCCESS)

● cobblerd.service - Cobbler daemon
   Loaded: loaded (/usr/lib/systemd/system/cobblerd.service; enabled; vendor
preset: disabled)
   Active: **active (running)** since Thu 2020-01-16 22:37:28 UTC; 18h ago
 Main PID: 30038 (cobblerd)
   CGroup: /system.slice/cobblerd.service
           └─30038 /usr/bin/python2 -s /usr/bin/cobblerd --no-daemonize
...

10. At the completion of the installation, ensure that only the following repositories are enabled on the system:

- UEKR5 or UEKR6

- ol7_latest

- ol7_optional_latest

- ol7_oraclelinuxmanager210_client

- ol7_oraclelinuxmanager210_server

You can verify enabled repositories by running the following command:

```
sudo yum repolist
```

Configuring a Newly Installed Oracle Linux Manager Server

Of the configuration tasks described in this section, configuring the initial organization and the Oracle Linux Manager administrator is mandatory. The other tasks are optional but recommended.

Creating the Initial Organization and Oracle Linux Manager Administrator Account

After completing the installation, you must create an initial organization and the main Oracle Linux Manageradministrator account.

For more information about the concept of *organization*, see Oracle Linux Manager: Concepts Guide for Release 2.10 .

1. Open a browser and access Oracle Linux Manager server's URL, which is the server's FQDN, such as `https://olmsvr.mydom.com`.

2. If prompted, select to trust the SSL certificate.

   The Create Organization page opens automatically.

3. Enter the required values in the appropriate fields to create the organization and its administrator.

4. Click **Create Organization**.

   The administrator you created is automatically logged in and the Overview page is displayed.

   Use the web interface to perform additional configuration tasks. For example, see Setting Up Primary-Worker Configurations With Oracle Linux Manager Web Interface as well as Oracle Linux Manager: Client Life Cycle Management Guide for Release 2.10 .

Replacing a Self-Signed SSL Certificate

You can use certificates for individual Oracle Linux Manager servers or proxies. Alternatively, you can also use wildcard certificates for all Oracle Linux Manager servers or proxies in the domains that the wildcard certificates cover.

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).

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

   ```
   sudo 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:

      a. Send the Certificate Signing Request (CSR) file `/root/ssl-build/`*olmsvr*`/`
         `server.csr` to the CA, where *olmsvr* is the simple name, **not** the FQDN, of Oracle Linux Manager server or the proxy.

         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 a Privacy Enhanced Mail (PEM) format.

     – If your certificate is DER-formatted, convert it to PEM format.

```
sudo openssl x509 -inform der -text -in certificate_file Readable
content
sudo openssl x509 -inform der -in server.cer -out server.pem
```

     – If a PEM-formatted certificate is not generated from a Linux or UNIX based system, remove ^M characters that might exist in that certificate.

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

     As an alternative, you can also run the following command, provided you installed the dos2unix package:

```
sudo dos2unix server.pem
```

   d. Copy the PEM-formatted server certificate file to /root/ssl-build/ _olmsvr_/server.crt.

```
sudo cp server.pem /root/ssl-build/olmsvr/server.crt
```

   This command overwrites the original file in that destination directory.

- Obtain a server certificate using an external tool:

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

   b. If the private key has an existing password, replace that key as follows:

```
sudo openssl rsa -in keyfilewithpasswd.key -out /root/ssl-build/
olmsvr/server.key
```

   This step ensures that Oracle Linux Manager 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:

```
sudo 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. Concateneate the two certificates you just downloaded to /root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT.

   Use the followng command exactly as shown:

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

ORACLE®

- – *intermediate_ca.pem*: intermediate public certificate file of the CA that issued your server certificate
- – *root_ca.pem*: public certificate file of the root CA

In the the chain certificate, the intermediate certificate **must precede** the certificate of the root CA. The CA chain certificate does not work if its component certificates are not in the correct order.

> **✎ Note:**
>
> In the rare case where a root CA signed the server certificate directly, then only the *root_ca.pem* would be contained in the chain certificate:
>
> ```
> sudo cp root_ca.pem /root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT
> ```

4. Validate the server certificate against the CA public certificate.

```
sudo openssl verify -CAfile /root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT /root/ssl-build/olmsvr/server.crt
```

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 Oracle Linux Manager database so that it is available for provisioning client systems.

```
sudo rhn-ssl-dbstore -v --ca-cert=/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. Prepare the web server SSL package for installation:

   a. Generate the web server SSL package., for example:

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

   ...working...

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

   The most current Oracle Linux Manager 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/olmsvr/rhn-org-httpd-ssl-archive-olmsvr-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 Oracle Linux Manager Proxy.
       Presumably 'olmsvr.mydom.com'.
   ```

   b. (Optional) List the files that the packages install.

See the following two examples:

```
sudo rpm -qlp /root/ssl-build/olmsvr/rhn-org-httpd-ssl-key-pair-
olmsvr-1.0-rev.src.rpm

rhn-org-httpd-ssl-key-pair-olmsvr-1.0.tar.gz
rhn-org-httpd-ssl-key-pair-olmsvr.spec

sudo rpm -qlp /root/ssl-build/olmsvr/rhn-org-httpd-ssl-key-pair-
olmsvr-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
```

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

```
sudo yum install /root/ssl-build/olmsvr/rhn-org-httpd-ssl-key-pair-
olmsvr-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, for example:

```
sudo 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.
```

b. (Optional) List the files that the packages install.

The following are two examples:

```
sudo 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

sudo rpm -qlp /root/ssl-build/rhn-org-trusted-ssl-cert-1.0-rev.noarch.rpm

/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT
```

c. If an Oracle Linux Manager server or proxy is also configured as a client, install the public CA certificate `noarch` package on this system.

```
sudo 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`.

    d. 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.

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

    e. Verify that the installed copies of `RHN-ORG-TRUSTED-SSL-CERT` digest in the different locations are identical. The locations are `/root/ssl-build`, `/usr/share`, and `/var/www/html/pub`, for example:

```
sudo 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
```

8. On an Oracle Linux Manager server, stop Oracle Linux Manager services, clear the `jabberd` database, then restart the services.

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

9. On Oracle Linux Manager proxies, restart the proxy services.

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

10. On the remaining Oracle Linux Manager clients, download and install the public CA certificate package.

```
sudo wget https://olmsvr/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.

Configuring a Web Proxy for an Oracle Linux Manager Server

If needed, configure the web proxy by using one of the following methods *after* you have installed Oracle Linux Manager:

- Edit the `/etc/rhn/rhn.conf` file and configure the specific web proxy parameters as shown by the settings in bold:

```
server.satellite.http_proxy = webproxy.mydom.com:80
server.satellite.http_proxy_username = proxy-username
server.satellite.http_proxy_password = proxy-password
```

- In the Oracle Linux Manager web interface, select the **Admin** tab, then **Oracle Linux Manager Configuration**, and enter the appropriate values to the HTTP proxy fields.

Upgrading to Oracle Linux Manager Server

This section provides information for upgrading Spacewalk 2.7 server to Oracle Linux Manager 2.10.

> **NOT_SUPPORTED:**
>
> If you are currently running earlier Spacewalk versions, such as Spacewalk 2.4 or Spacewalk 2.6, you must first upgrade to Spacewalk 2.7 before proceeding with the steps in this section. For instructions, see Upgrading a Spacewalk Server in Spacewalk for Oracle® Linux: Installation Guide for Release 2.7.

Preparing to Upgrade

You must use Oracle databases that are supported in Oracle Linux Manager. For a list of supported databases in Oracle Linux Manager 2.10, see Oracle Database Support in Oracle Linux Manager: Release Notes for Release 2.10 .

Before you upgrade, check the following elements in their respective XML files:

- `<driver>` in the `/etc/jabberd/sm.xml` file

- `<module>` in the `/etc/jabberd/c2s.xml` file

If both elements in the two files specify `sqlite`, you can proceed to Performing the Upgrade. If not, then complete the following steps:

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

   ```
   sudo systemctl stop osa-dispatcher
   sudo systemctl stop jabberd
   ```

2. Specify `sqlite` for the `<driver>` and `<module>` elements in the files as shown:

   - `/etc/jabberd/sm.xml`: `<driver>sqlite</driver>`.

   - `/etc/jabberd/c2s.xml`: `<module>sqlite</module>`.

3. Create the SQLite database.

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

4. Start the `jabberd` and `osa-dispatcher` services.

   ```
   sudo systemctl start jabberd
   sudo systemctl start osa-dispatcher
   ```

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

   ```
   sudo cat /var/log/messages | grep sqlite
   ```

6. On client servers, make the `osad` service re-authenticate to `jabberd`.

If you previously registered client servers on which you then installed the `osad` service, remove the `osad-auth.conf` file first before restarting the service, as follows:

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

Performing the Upgrade

> **Note:**
>
> If your system is already running Spacewalk 2.10, see Switching From Spacewalk 2.10 to Oracle Linux Manager 2.10 for information to convert it to Oracle Linux Manager.

Upgrade to Oracle Linux Manager 2.10 as follows:

1. Backup all current configurations.

   - Back up all of the Spacewalk 2.7 configuration files in the following directories:

     - `/etc/jabberd`

     - `/etc/rhn`

     - `/etc/sysconfig/rhn`

     - `/root/ssl-build`

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

   - Back up the Spacewalk 2.7 database.

     This step is recommended as a precaution in case the upgrade does not complete successfully.

     To use the Recovery Manager (RMAN) to create a backup, refer to your database version's Backup and Recovery User's Guide in https://docs.oracle.com/en/database/oracle/oracle-database/index.html.

2. Change the way the server that is currently running Spacewalk 2.7 Server obtains packages depending on the server's current configuration.

   - If the Spacewalk 2.7 server is registered as a client of itself:

     a. Create an Oracle Linux Manager server channel as a child of the Oracle Linux 7 base channel.

        For more information about configuring channels, see Creating Software Channels and Repositories in Oracle Linux Manager: Client Life Cycle Management Guide for Release 2.10 .

     b. Create an Oracle Linux Manager server repository that accesses the corresponding server channel on the Oracle Linux yum server server (`https://yum.oracle.com/repo/OracleLinux/OL7/oraclelinuxmanager210/server/x86_64/`), by using the same GPG settings as for Oracle Linux 7.

c. Associate Oracle Linux Manager server repository with its corresponding server channel and synchronize the repository's packages from the Oracle Linux yum server.

d. Change the channel subscription from the Spacewalk server to Oracle Linux Manager server.

e. Configure and synchronize the following additional channels:

– Oracle Linux 7 Server Latest

– Oracle Linux 7 Server Optional Latest

– Oracle Instant Client for Oracle Linux 7

– Oracle Linux Manager (formerly Spacewalk) Client 2.10 for Oracle Linux 7

– Oracle Linux Manager (formerly Spacewalk) Server 2.10 for Oracle Linux 7

- If the Spacewalk 2.7 server obtains packages from the Oracle Linux yum server:

a. Disable the Spacewalk server repository for the Spacewalk 2.7 release in the Oracle Linux yum server repository configuration file.

Edit the configuration file and set `enabled=0`. Or, run the following command:

```
sudo yum-config-manager --disable repository
```

b. **Required**: Install the latest `oracle-release-el7` package.

> **⊘ Important:**
>
> You **must** run the following command even if you have recently updated the system, in order to successfully run the `yum swap` command later in this procedure.

```
sudo yum install oracle-release-el7
```

If your system is running an Oracle Linux release that is earlier than Oracle Linux 7 Update 7, run the following additional command to make the system use the modular yum repository configuration:

```
sudo /usr/bin/ol_yum_configure.sh
```

c. Install the `oracle-linux-manager-server-release-el7` package.

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

> **✎ Note:**
>
> The command creates the file `/etc/yum.repos.d/oracle-linux-manager-server-ol7.repo` if that file does not exist.
>
> However, if the file already exists, then the command leaves that file unmodified and instead creates a new file `/etc/yum.repos.d/oracle-linux-manager-server-ol7.repo.rpmnew` that contains new repository entries for Oracle Linux Manager Server. Use the `.rpmnew` file to guide you to make the necessary modifications to the existing `.repo` file.

3. Verify that the correct Oracle Linux Manager repositories are enabled, and earlier Spacewalk versions are disabled.

   The `/etc/yum.repos.d/oracle-linux-manager-server-ol7.repo` file should resemble the following example:

   ```
   [ol7_oraclelinux-manager210_server]
   name=Oracle Linux Manager Server 2.10 for Oracle Linux 7 ($basearch)
   baseurl=https://yum$ociregion.oracle.com/repo/OracleLinux/OL7/
   oraclelinuxmanager210/server/$basearch/
   gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
   gpgcheck=1
   enabled=1

   [ol7_oracle-linux-manager210_client]
   name=Oracle Linux Manager Client 2.10 for Oracle Linux 7 ($basearch)
   baseurl=https://yum$ociregion.oracle.com/repo/OracleLinux/OL7/
   oraclelinuxmanager210/client/$basearch/
   gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
   gpgcheck=1
   enabled=1
   ```

   The `/etc/yum.repos.d/oracle-spacewalk-server-ol7.repo` should resemble the following example:

   ```
   [ol7_spacewalk27_server]
   name=Spacewalk Server 2.7 for Oracle Linux 7 ($basearch)
   baseurl=https://yum$ociregion.oracle.com/repo/OracleLinux/OL7/spacewalk27/
   server/$basearch/
   gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
   gpgcheck=1
   enabled=0

   [ol7_spacewalk26_server]
   name=Spacewalk Server 2.6 for Oracle Linux 7 ($basearch)
   baseurl=https://yum$ociregion.oracle.com/repo/OracleLinux/OL7/spacewalk26/
   server/$basearch/
   gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
   gpgcheck=1
   enabled=0

   [ol7_spacewalk27_client]
   name=Spacewalk Client 2.7 for Oracle Linux 7 ($basearch)
   baseurl=https://yum$ociregion.oracle.com/repo/OracleLinux/OL7/spacewalk27/
   client/$basearch/
   gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
   gpgcheck=1
   enabled=0
   ```

```
[ol7_spacewalk26_client]
name=Spacewalk Client 2.6 for Oracle Linux 7 ($basearch)
baseurl=https://yum$ociregion.oracle.com/repo/OracleLinux/OL7/spacewalk26/
client/$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=0
```

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

```
sudo yum versionlock list
sudo yum versionlock delete cglib c3p0
```

5. Upgrade the Instant Clients.

```
sudo yum swap -- remove oracle-instantclient11.2-basic oracle-
instantclient11.2-sqlplus freemarker velocity-tools -- upgrade oracle-
instantclient18.5-basic oracle-instantclient18.5-sqlplus spacewalk-oracle
```

> **✎ Note:**
>
> The command might generate a `No match for argument` message with references to `freemarker` and `veolcity-tools`. These packages might have existed in the system from an earlier Spacewalk 2.6 installation, but which are no longer required by Oracle Linux Manager 2.10. Thus, in this case, you can ignore the message.

6. Add the library path to `ldconfig`.

```
echo "/usr/lib/oracle/18.5/client64/lib" | sudo tee /etc/ld.so.conf.d/oracle-
instantclient18.5.conf
sudo ldconfig
```

7. Upgrade all the packages.

```
sudo yum upgrade
```

8. Stop Oracle Linux Manager services.

```
sudo /sbin/spacewalk-service stop
```

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

9. Upgrade Oracle Linux Manager's database schema.

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

The process requires intervention at some point in order to continue, as shown in bold in the following example:

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

Please make sure all Oracle Linux Manager services apart from database are
stopped.
...
Schema upgrade: [spacewalk-schema-2.7.28-1.0.2.el7] -> [spacewalk-
schema-2.9.11-1.el7]
Searching for upgrade path: [spacewalk-schema-2.7.28-1.0.2] -> [spacewalk-
```

```
schema-2.9.11-1]
Searching for upgrade path: [spacewalk-schema-2.7.28] -> [spacewalk-schema-2.9.11]
Searching for upgrade path: [spacewalk-schema-2.7] -> [spacewalk-schema-2.9]
The path: [spacewalk-schema-2.7] -> [spacewalk-schema-2.8] -> [spacewalk-
schema-2.9]
Planning to run spacewalk-sql with [/var/log/spacewalk/schema-upgrade/
20200123-165929-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/20200406-174429-to-spacewalk-
schema-2.10.log].
The database schema was upgraded to version [spacewalk-schema-2.10.11-1.el7].
```

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.

10. Upgrade Oracle Linux Manager's configuration for the Oracle Database.

    ```
    sudo spacewalk-setup --external-oracle --upgrade
    ```

    The command initiates an interactive session that prompts you for information about your current database.

11. Restart Oracle Linux Manager services.

    ```
    sudo /sbin/spacewalk-service start
    ```

12. Perform any necessary postinstallation tasks.

    Review the information in Configuring a Newly Installed Oracle Linux Manager Server.

13. If necessary, upgrade your Oracle database.

    a. Back up the Oracle Linux Manager database again.

       This step is recommended as a precaution in case the following step to upgrade the database does not complete successfully.

       To use the Recovery Manager (RMAN) to create a backup, refer to your database version's Backup and Recovery User's Guide in https://docs.oracle.com/en/database/oracle/oracle-database/index.html.

    b. Upgrade the Oracle database.

       As indicated in the Oracle Linux Manager: Release Notes for Release 2.10 , Oracle Linux Manager 2.10 supports only Oracle Database Enterprise edition 12c and Oracle Database Enterprise edition 19c. Oracle **strongly** recommends that you use Oracle Database Enterprise edition 19c.

> **❗ Important:**
>
> If you are upgrading your Oracle database, do **not** use the RPM
> version of the Oracle Database Enterprise edition 19c release.
> Upgrading an OUI-installed Oracle database with the RPM version is
> not supported.

For this step, consult your database administrator and follow the instructions in
your database documentation.

14. Upgrade the Spacewalk Client to Oracle Linux Manager 2.10 Client.

    For instructions, refer to the appropriate section in the chapter Registering Client
    Systems With Oracle Linux Manager in Oracle Linux Manager: Client Life Cycle
    Management Guide for Release 2.10 .

Switching From Spacewalk 2.10 to Oracle Linux Manager 2.10

If you are already using Spacewalk 2.10, you should convert to Oracle Linux Manager
2.10 as the Spacewalk 2.10 repositories are scheduled to be retired. For details, see
Oracle Linux Manager: Release Notes for Release 2.10 .

To switch a Spacewalk 2.10 server to Oracle Linux Manager:

1. Backup all current configurations.

   • Back up all of the Spacewalk 2.10 configuration files in the following
     directories:

     – `/etc/jabberd`

     – `/etc/rhn`

     – `/etc/sysconfig/rhn`

     – `/root/ssl-build`

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

   • Back up the Spacewalk 2.10 database.

     This step is recommended as a precaution in case the switch does not
     complete successfully.

     To use the Recovery Manager (RMAN) to create a backup, refer to your
     database version's Backup and Recovery User's Guide in https://
     docs.oracle.com/en/database/oracle/oracle-database/index.html.

2. Change the way the server that is currently running Spacewalk 2.10 Server
   obtains packages depending on the server's current configuration.

   • If the Spacewalk 2.10 server obtains packages from the Oracle Linux yum
     server, install the `oracle-linux-manager-server-release-el7` package.

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

   • If the Spacewalk 2.10 server is registered as a client of itself, update the
     existing Spacewalk server and client repository URLs to Oracle Linux Manager
     as follows:

Oracle Linux Manager Server

– **Server Repository Label**: `ol7_oraclelinuxmanager210_server`

– **Server Repository Name**: Oracle Linux Manager (formerly Spacewalk) Server 2.10 for Oracle Linux 7

– Yum URL: `https://yum.oracle.com/repo/OracleLinux/OL7/oraclelinuxmanager210/server/x86_64`

Oracle Linux Manager Client (Oracle Linux 7)

– **Client Repository Label**: `ol7_oraclelinuxmanager210_client`

– **Client Repository Name**: Oracle Linux Manager (formerly Spacewalk) Client 2.10 for Oracle Linux 7

– Yum URL: `https://yum.oracle.com/repo/OracleLinux/OL7/oraclelinuxmanager210/client/x86_64`

Oracle Linux Manager Client (Oracle Linux 8)

– **Client Repository Label**: `ol8_oraclelinuxmanager210_client`

– **Client Repository Name**: Oracle Linux Manager (formerly Spacewalk) Client 2.10 for Oracle Linux 8

– Yum URL: `https://yum.oracle.com/repo/OracleLinux/OL8/oraclelinuxmanager210/client/x86_64`

For more information about configuring channels and repositories, see Creating Software Channels and Repositories in Oracle Linux Manager: Client Life Cycle Management Guide for Release 2.10 .

3. Upgrade all the packages.

```
sudo yum upgrade
```

2
Installing and Upgrading Oracle Linux Manager Proxies

This chapter describes how to install or upgrade an Oracle Linux Manager proxy.

An Oracle Linux Manager proxy acts as an intermediary between Oracle Linux Manager clients and an Oracle Linux Manager server. The main purposes of an Oracle Linux Manager proxy are to mitigate the load on Oracle Linux Manager server and reduce the download times for Oracle Linux Manager clients.

Oracle Linux Manager Proxy Requirements

Oracle supports Oracle Linux Manager proxies that are running on Oracle Linux 7 on the x86_64 platform. Note the following requirements to install an Oracle Linux Manager proxy.

Oracle Linux Requirements

The following are additional requirements:

- Install Oracle Linux 7 by using either the **Minimal** or **Basic Server** profile.
- Before installing Oracle Linux Manager, remove the `jta` package, which prevents Oracle Linux Manager services from starting.
- Use 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.
- Update your system with the latest packages from the Oracle Linux yum server.
- **Do not register an Oracle Linux Manager server or client with ULN**. Instead, register an Oracle Linux Manager server as a client of itself to receive updates.

Storage Requirements

The following are the storage requirements for an Oracle Linux Manager proxy:

- An Oracle Linux Manager 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, an Oracle Linux Manager 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.

Networking Requirements

The following are the networking requirements for an Oracle Linux Manager proxy:

- Static IP address for the proxy

- Correctly configured forward and reverse DNS host name, with the following specifications:

> ⚠️ **Caution:**
>
> Noncompliance with these specifications for the server's host name can cause Oracle Linux Manager to fail in its proxy communications, inter-server synchronization (ISS), certificate validation, and other areas of operation.

  – The host name of the server must **not** contain uppercase letters.

  – While the `/etc/hostname` file contains the short name of the host, the `/etc/hosts` file **must** specify the host's FQDN, as shown in bold in the following example:

```
cat /etc/hostname

olmproxy

cat /etc/hosts

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

    Note that Oracle Linux Manager does not consider `.local` and `.localdomain` to be valid domain names.

- Port numbers

  The following table describes the network ports that an Oracle Linux Manager 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 Oracle Linux Manager clients (if required)
`5269`/tcp	Inbound	Push support to Oracle Linux Manager proxies (if required)

- Configured network time synchronization

  Configure Oracle Linux Manager server, proxies, and clients to use NTP or PTP. In order to establish a Secure Socket Layer (SSL) based connection, Oracle Linux Manager requires that the system times on server and client systems be consistent to within 120 seconds.

If required for Oracle Linux Manager proxy, you can configure a web proxy during installation. See Configuring a Web Proxy for an Oracle Linux Manager Server.

Installing an Oracle Linux Manager Proxy

An Oracle Linux Manager should be configured with the full Oracle Linux Manager client and be registered with Oracle Linux Manager server.

1. Ensure that the `jta` package is not installed.

   a. Remove the `jta` package if it is installed on the system.

   ```
   sudo yum list installed | grep jta
   sudo yum remove jta
   ```

   b. To prevent any future accidental installation of the package, do one of the following:

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

     ```
     exclude=jta*
     ```

   - Disable the Oracle Linux 7 `addons` channel (`[ol7_addons]`).

     ```
     sudo yum-config-manager --disable ol7_addons
     ```

2. Configure the system firewall.

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

3. Ensure that the correct channels are configured on the system.

   a. If not already present, create these required software channels for both Oracle Linux Manager and Oracle Linux 7:

   - Oracle Linux 7 Latest (`https://yum.oracle.com/repo/OracleLinux/OL7/latest/`)

   - Oracle Linux 7 Optional Latest (`https://yum.oracle.com/repo/OracleLinux/OL7/optional/latest/`

   - Oracle Linux Manager (formerly Spacewalk) Server 2.10 for Oracle Linux 7 repository (`https://yum.oracle.com/repo/OracleLinux/OL7/oraclemanager210/server/x86_64/`)

   - Oracle Linux Manager (formerly Spacewalk) Client 2.10 for Oracle Linux 7 repository (`https://yum.oracle.com/repo/OracleLinux/OL7/oraclemanager210/client/x86_64/`)

   b. Ensure that all the packages in these channels are properly syncrhonized with the Oracle Linux yum server.

   c. Change the system's channel subscription from the Spacewalk 2.7 server channel to Oracle Linux Manager (formerly Spacewalk) Server 2.10 for Oracle Linux 7 channel.

   d. Subscribe the proxy to Oracle Linux Manager client and server channels.

4. Install Oracle Linux Manager client software and the `openssh-clients` packages.

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

5. Register the system as a client of Oracle Linux Manager server for which it functions as a 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.

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

In a browser tab, navigate to `http://olmsvr_FQDN/pub`, where *olmsvr_FQDN* is the fully qualified domain name of Oracle Linux Manager 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:

```
sudo wget -q -O /usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT http://
olmsvr_FQDN/pub/RHN-ORG-TRUSTED-SSL-CERT
```

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

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

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

i. Verify that `serverURL` is set to Oracle Linux Manager server's URL, for example `https://olmsvr.mydom.com/XMLRPC`:

```
sudo grep ^serverURL= /etc/sysconfig/rhn/up2date
```

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

```
sudo grep ^sslCACert= /etc/sysconfig/rhn/up2date
```

> **Note:**
>
> If the settings are not correct, most likely a mistake was made when registering the system with the `rhnreg_ks` command. Run the `rhnreg_ks` command again to check that you correctly specified the path of the CA certificate and Oracle Linux Manager server's URL. Also, make sure to specify the `--force` option to override the previous settings.

6. Install Oracle Linux Manager proxy installer package.

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

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

```
sudo mkdir /root/ssl-build
```

8. Copy Oracle Linux Manager server's CA key and public certificate files to the proxy server's `/root/ssl-build`. The files to be copied are the following:

   • `RHN-ORG-PRIVATE-SSL-KEY`

   • `RHN-ORG-TRUSTED-SSL-CERT`

   • `rhn-ca-openssl.cnf`

   See the following example:

```
sudo scp 'root@olm_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 Oracle Linux Manager proxy by running the `/usr/sbin/configure-proxy.sh` script.

   The script initiates an interactive configuration, as the following example shows. User input is displayed in bold.

```
sudo /usr/sbin/configure-proxy.sh

Using RHN parent (from /etc/sysconfig/rhn/up2date): olmsvr.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 Oracle Linux
Manager Parent
Server, you will be prompted to generate an SSL certificate.
This SSL certificate will allow client systems to connect to this Oracle Linux
Manager Proxy
securely. Refer to the Oracle Linux Manager Proxy Installation Guide for more
information.
Organization []: Company Demo
Organization Unit [olmproxy.us.mydom.com]: [Enter]
Common Name [olmproxy.us.mydom.com]: [Enter]
City []: Redwood Shores
State []: CA
Country code []: US
Email [my.email@mydom.com]: [Enter]
Cname aliases (separated by space) []: [Enter]
Oracle Linux Manager 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-olmproxy-1.0-1
Create and populate configuration channel rhn_proxy_config_1000010000?
[Y/n]: Y
Oracle Linux Manager username: []: olm_user
Password: olm_passwd
Using server name olmsvr.mydom.com
Creating config channel rhn_proxy_config_1000010000
Config channel rhn_proxy_config_1000010000 created
Using server name olmsvr.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 Oracle Linux Manager 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
```

> **✏ Note:**
>
> The information that you provide is recorded in a file named `proxy-answers.txt.`*UID* , such as `proxy-answers.txt.NtM1Y` in the previous output. You can use this file to automate the configuration of an Oracle Linux Manager 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 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 perform this step from Oracle Linux Manager server.

11. To check that Oracle Linux Manager proxy is running correctly, specify the URL of the proxy when registering an Oracle Linux Manager client, as shown in the following example

    ```
    sudo rhnreg_ks --sslCACert=/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT --
    serverUrl=https://olmproxy_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.

Upgrading a Spacewalk 2.7 Proxy Server

Upgrade a Spacewalk proxy system as follows:

1. If not already present on the Spacewalk 2.7 server, create software channels for both Oracle Linux Manager client and server , then subscribe the proxy system to these channels.

    a. Create an Oracle Linux Manager client channel as a child of the Oracle Linux 7 base channel.

    b. Create an Oracle Linux Manager client repository that accesses the corresponding client channel on the Oracle Linux yum server (`https://yum.oracle.com/repo/OracleLinux/OL7/oraclelinuxmanager210/client/x86_64/`), using the same GPG settings as the Oracle Linux release.

    c. Associate Oracle Linux Manager client repository with the corresponding client channel and synchronize the repository's packages from the Oracle Linux yum server.

    d. Create an Oracle Linux Manager server channel as a child of the Oracle Linux 7 base channel.

    e. Create an Oracle Linux Manager server repository that accesses the corresponding server channel on the Oracle Linux yum server (`https://yum.oracle.com/repo/`

ORACLE

`OracleLinux/OL7/oraclelinuxmanager210/server/x86_64/`), using the same GPG settings as the Oracle Linux release.

f. Associate Oracle Linux Manager (formerly Spacewalk) Server 2.10 for Oracle Linux 7 repository with the corresponding server channel and synchronize the repository's packages from the Oracle Linux yum server.

g. Change the system's channel subscription from the Spacewalk 2.7 server channel to Oracle Linux Manager (formerly Spacewalk) Server 2.10 for Oracle Linux 7 channel.

h. Subscribe the upgraded proxy system to Oracle Linux Manager client and server channels instead of the Spacewalk server and client channels for Release 2.7.

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:

```
sudo cd /root/ssl-build
sudo 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.

```
sudo yum update
```

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

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

5. Configure Oracle Linux Manager 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:

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

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

3

Configuring Inter-Server Synchronization for Oracle Linux Manager Servers

This chapter describes the configuration and synchronization of primary and worker or secondary Oracle Linux Manager systems.

About Primary-Secondary Configurations

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

Typical use cases of this configuration include the following examples:

- 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 Oracle Linux Manager 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. A less typical topology is a directed graph, where several top-level primary servers might exist, and each worker can have more than one primary servver . If a worker has more than one primary server , you can designate one as the default primary server with which the worker synchronizes.

To set up the relationships between primary and worker Oracle Linux Manager servers, you can use the `spacewalk-sync-setup` command, provided that you installed the `spacewalk-utils` package. Otherwise, you would need to use Oracle Linux Manager web interface which enables you to configure each server independently.

Setting a Worker-Only Oracle Linux Manager Server

By default, an Oracle Linux Manager server is configured so that it can act as a primary server. Any worker server that you configure for the primary server can synchronize from that primary server.

You can designate an Oracle Linux Manager server to function only as a worker server by following these steps:

1. Edit `/etc/rhn/rhn.conf` and set the value of `disable_iss` as follows:

   ```
   disable_iss=1
   ```

2. Restart the `httpd` service.

```
sudo systemctl restart httpd
```

To make the server revert to the default behavior, reset `disable_iss` to 0.

Creating Primary-Worker Configurations With the spacewalk-sync-setup Command

This section assumes that you have installed the `spacewalk-utils` package. If not, follow the method in Setting Up Primary-Worker Configurations With Oracle Linux Manager Web Interface instead.

Ensure first that Oracle Linux Manager is running on both the primary and worker servers. Then, on either primary or worker server, run the `spacewalk-sync-setup` command: as follows

```
sudo spacewalk-sync-setup --apply --create-templates --ms=primary_olmsvr_FQDN \
--ml=primary_olmadm --mp=primary_olmadm_passwd --ss=backup_olmsvr_FQDN \
--sl=backup_olmadm --sp=backup_olmadm_passwd

INFO: Connecting to olmadmin@olmsvr.mydom.com
INFO: Connecting to olmadmin@olmsvr2.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/olmsvr.mydom.com_RHN-ORG-TRUSTED-SSL-CERT
http://olmsvr.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/olmsvr.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 Configuring a Primary Oracle Linux Manager Server.

Setting Up Primary-Worker Configurations With Oracle Linux Manager Web Interface

This section describes how to use Oracle Linux Manager Web Interface to configure primary and worker systems and how to create organizations to be included in their synchronization.

Creating Local Organizations

If you intend to include organizations when configuring primary-worker server synchronization, you must create those organizations first. You can create as many organizations as you need.

1. Log in to your Oracle Linux Manager server's URL, such as `https://olmsvr.mydom.com`.

2. Select **Admin**.

3. On the **Organizations** page, click **+ Create Organization**.

4. On the Create Organization page, enter the required values to create the organization and its administrator.

> **Note:**
>
> Each organization you create must have its own administrator acocunt that is different from the Oracle Linux Manager administrator.

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

6. Click **Create Organization**.

Configuring a Primary Oracle Linux Manager Server

Configure a primary Oracle Linux Manager server as follows:

1. On **Admin**, select **ISS Configuration**.

   The **Master Setup** tab is selected by default.

2. 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 primary-worker server 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.

5. Provided that you have already created the organizations, select those organizations that you want to enable to be exported to the worker, then click **Allow Orgs**.

   To create organizations, see Creating Local Organizations.

Configuring a Worker Oracle Linux Manager Server

Configure a worker Oracle Linux Manager server as follows:

1. On a separate browser tab, navigate to `http://`*`primary_olmsvr_FQDN`*`/pub` 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 on a terminal window as follows:

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

2. Switch back to the browser tab that is displaying the ISS Configuration page.

3. Select the **Slave Setup** tab and click **+ Add new master**.

4. On the Details for new Master page, do the following:

   • Type the FQDN of the primary server.

- • Type the absolute path of the downloaded primary's CA certificate (`RHN-ORG-TRUSTED-SSL-CERT-MASTER`).

5. Select if you want the primary server to be the default server with which the worker synchronizes.

6. Click **Add new master**.

   The page refreshes to display a Configure Master-to-Slave Org Mappings section.

7. Choose one of the following steps:

   - • If you do not intend to import any organization, select **NOT MAPPED**.

   - • If you intend to import an organizations, select it from the pull-down menu in the Matching Local Org column.

     This step assumes you have already created the organizations. See Creating Local Organizations.

8. Click **Update**.

Synchronizing Software Channels on an Oracle Linux Manager Worker Server

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

```
sudo satellite-sync [--iss-parent=primary_olmsvr_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, Oracle Linux Manager Default Organization with ID 1 is assumed.

The *primary_olmsvr_FQDN* value specifies the FQDN of the primary Oracle Linux Manager server. If not specified, and the worker server has more than one primary server, the default primary server is assumed.

The following example shows how to use the command to begin the synchronization process.

```
sudo satellite-sync -c oraclelinux6-x86_64-patch

16:16:52 Oracle Linux Manager - live synchronization
16:16:52    url: https://olmsvr.mydom.com
16:16:52    debug/output level: 1
16:16:52    db:  c##olm2/<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
```

4

Troubleshooting Oracle Linux Manager Problems

This chapter describes how to diagnose and fix problems that you might encounter on an Oracle Linux Manager server. For information about other known issues and possible workarounds, see Oracle Linux Manager: Release Notes for Release 2.10 .

Checking the Status of Services

Use the `/usr/sbin/spacewalk-service status` command to identify Oracle Linux Manager services that might be running incorrectly. For Oracle Linux Manager proxy servers, use the `rhn-proxy status` command.

Services that do not start correctly are typically caused by incorrect configuration information that was provided during installation.

For Oracle Linux Manager proxies, verify also that the `/etc/sysconfig/rhn/systemid` file is owned by `root:apache` and that its mode is set to 640.

If required to clear up package provisioning problems on Oracle Linux Manager proxies, clear the proxy cache as follows:

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

   ```
   sudo systemctl stop httpd
   sudo systemctl stop squid
   ```

2. Delete the contents of the cache as follows:

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

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

   ```
   sudo systemctl start squid
   sudo systemctl start httpd
   ```

Checking Logs for Errors

The following Oracle Linux Manager server logs are information sources when errors occur:

/var/log/httpd/*
`httpd` service log files.

/var/log/rhn_satellite_install.log
Installation log file.

/var/log/rhn/reposync/*
Repository synchronization log files.

/var/log/rhn/rhn_server_satellite.log
Synchronization log file.

/var/log/rhn/rhn_server_xmlrpc.log
XML-RPC transaction log file.

/var/log/rhn/rhn_taskomatic_daemon.log
Red Hat Network (RHN) Task Engine (Taskomatic) log messages.

/var/log/tomcat
Tomcat log messages for Oracle Linux.

/var/log/yum.log
Yum log file.

On Oracle Linux Manager proxies, these addiitonal logs are also useful for error checking:

/var/log/rhn/rhn_proxy_broker.log
Proxy brokering service log file.

/var/log/rhn/rhn_proxy_redirect.log
Proxy SSL redirection service log file.

/var/log/squid/*
Squid proxy log files.

> **✎ Note:**
>
> Oracle Linux Manager generates large numbers of log messages, particularly under the `/var/log/httpd` directory. To avoid running out of disk space, adjust the `logrotate` settings to implement more active rotation, compression, and archival of log files.

For more information, see the Oracle Linux 7: Monitoring and Tuning the System.

Issues and Problems

This section describes issues you might encounter with the current Oracle Linux Manager release. It also includes workarounds should these errors occur.

osa-dispatcher Reports a Certificate Verification Failure

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

```
sudo systemctl start osa-dispatcher

Starting osa-dispatcher: Oracle Linux Manager 10611 2015/05/26 17:11:22 +01:00:
('Traceback caught:',)
Oracle Linux Manager 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 Oracle Linux Manager.

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
```

You are prompted for the pass phrase before the key is displayed.

If you typed the correct password, the base64-encoded private key is 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.

    ```
    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://olmsvr.mydom.com/XMLRPC
    ```

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 displayed:

```
Oracle Linux Manager 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.

```
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
```

ORACLE®

> **✎ Note:**
>
> To avoid problems with OSA, you should clear the `jabberd` database at regular intervals.
>
> To avoid database corruption, follow the instructions in Preparing to Upgrade.