Installing Platform RTM

Platform RTM
Version 8.0.2
Release date: October 2011

Platform
Computing

Contents

C H A P T E R

1

About this guide

Platform RTM can be installed on a variety of operating systems. This guide contains all the information required for any installation path. Note that you will not need all the information in this guide. Refer only to those chapters that apply to your selected installation path.

In brief, installing Platform RTM entails the following steps:

1. Prepare to install
2. Install Platform RTM
3. Activate Platform RTM

2

Pre-installation checklist

System sizing depends on a number of factors, the most significant include:

- The number of jobs per day across all clusters
- The number of hosts to be monitored
- The number of clusters to be monitored
- The polling frequencies for each cluster
- The number of concurrent logins to be supported
- The RRDfile data retention desired
- The amount of historical job data to be retained
- Job graph archiving choice

Keep the following tips in mind when sizing up your Platform RTM file system:

Database

- Database sizing depends on number of jobs per day and job detail data retention.
- Assume 4KB per job for this type of file system.
- Length of running jobs is a factor on job usage storage requirements.

Cacti RRDfiles

- Cacti RRDfiles size depends on the data retention.
- The default data retention results in smaller RRDfiles; assume 1-2MB per host, 30MB + per cluster depending on the number of users, projects, or queues.
- This file can be huge depending on customer data retention requirements.

Job Graphs

- Job Graphs, in general, are created on demand. So data storage requirements vary depending on the number of users viewing job graphs.
- Each set of job graphs results in approximately 2MB of file storage. However, if Job Graph archiving is enabled and you have high volume clusters, this can result in TB of RRDfiles. For example, 10,000 Jobs per day results in 20GB of storage required per day for archiving.

Syslog Volume

- The syslog database can become large depending on your per host logging level, the number of hosts, and your discard rules.
- Currently, there is no estimate established for the syslog database sizing.

System requirements

The following are the minimum requirements for Platform RTM installation:

- A system with a minimum of 2GB RAM and 40GB disk.
- A VMware or Xen virtual system may also be used. For Xen, full virtualization environment must be set.

  This minimum specification can support a cluster with:

  - up to 500 hosts
  - average daily 100,000 jobs
  - up to 300 users and 300 user groups

  For larger cluster, refer to performance tuning in the Administration guide.
- If system is on DHCP, configuration is done automatically. If system is not on DHCP, configuration can be made using the default Linux networking tools.
- An LSF cluster must be accessible by Platform RTM.
- The Platform RTM host must be an LSF client of that LSF cluster.
- LSF poller requires a valid license. To obtain a license, contact rtm-support@platform.com.

3

Install Platform RTM

You can install Platform RTM with the following Operating Systems:

- Red Hat Enterprise Linux (RHEL) version 5.2 or above, 6.0, or 6.1.
- CentOS version 5.2 or above
- SuSE Linux Enterprise Server (SLES) version 10 SP2 and 11 SP1

Install Platform RTM on RHEL

For RHEL, Platform RTM supports versions 5.2 or later. This documentation refers to RHEL 5.2 as the operating system with which RTM is installed.

Prepare to install

If you are using RHEL 6.x, as a pre-install step download PHP-SNMP package with RHN.

RHEL 6.0: `php-snmp-5.3.2-6.el6.x86_64.rpm`

RHEL 6.1: `php-snmp-5.3.3-3.el6.x86_64.rpm`

Note:

The `rhel-server-6.x-x86_64-dvd.iso` image does not contain php-snmp package. For proper Platform RTM on RHEL 6.x installation, you need to download this package from the Red Hat official site using Red Hat Network (RHN) account.

If you did not register your RHEL installation with the RHN, create a `yum` repository from the DVD media.

- Query the available `php-snmp` package and run the yum install:

  [root@duderanch lib]# yum list | grep php-snmp

  php-snmp.x86_64 5.3.3-3.el6 @rhel-x86_64-server-optional-6

- Install the plugin called `yum-downloadonly` and run the following command:

  [root@duderanch lib]# yum install yum-downloadonly

- Download the php-snmp package from RHN:

  [root@duderanch opt]# yum install php-snmp --downloadonly

---

1. Run the RHEL 5.2 or above installation program.

   For more information, refer to your Red Hat Enterprise installation documentation.

2. Either you disable the firewall or ensure that port 80 is open, and disable Security Enhanced Linux (SELinux).

   In the Security level field, if you select Enable firewall, you must also select the Web Server (HTTP, HTTPS) field.

   For the Enable SELinux? field, select Disable.

3. Ensure that the following packages are selected by default:

   - @ MySQL Database
   - @ Editors
   - @ System Tools
   - @ Text Internet
   - @ Web Server
   - @ Mail Server

   After you select the packages, the program proceeds with the installation.

4. If you have not disabled SELinux or allowed port 80 during installation, run the following commands:

```
# system-config-securitylevel-tui
# reboot
```

5. Restart the Platform RTM host to complete the installation and log into the host as root.

6. If you did not register your RHEL installation with the Red Hat Network (RHN), create a yum repository from the DVD media.

   - 1. Mount the RHEL 5.2 ISO image (for example, rhel5.2.dvd.iso) by running the following commands:

     ```
     # mkdir -p /mnt/rhel-iso
     # mkdir /mnt/rhel
     # mount -o loop rhel5.2.dvd.iso /mnt/rhel-iso
     # ln -sf /mnt/rhel-iso/Server/ /mnt/rhel
     ```

   2. Create a yum repository by running the following commands:

     ```
     # cd /mnt/rhel/
     # rpm -ivh Server/createrepo*.rpm
     # createrepo -vp .
     ```

   3. Create a /etc/yum.repos.d/rhel.repo text file with the following contents:

     ```
     [RHEL]
     NAME=RHEL
     baseurl=file:///mnt/rhel
     enabled=1
     ```

Install the Platform RTM packages

1. Log into the Platform RTM host as root.

2. Download the Platform RTM installation packages from my.platform.com.

   1. Create a directory to store the installation packages.

      mkdir -p /mnt/rtm

   2. Download all the Platform RTM installation files and copy them into the /mnt/rtm directory.

      For Platform RTM 8.0.2, download all installation files from http://my.platform.com/products/platform-lsf-family/platform-rtm.

3. Verify that the md5sum for the downloaded tar file matches the sum on the website.

4. Uncompress the tar file.

5. Temporarily allow the Platform RTM host to install unsigned packages.

   You need to allow unsigned packages because some of the Platform RTM installation packages are unsigned.

   a) Make a backup copy of the /etc/yum.conf file.

      cp /etc/yum.conf /etc/yum.conf.orig

   b) Edit the /etc/yum.conf file and specify **gpgcheck=0** in the file.

6. Navigate to the RTM installation package directory.

   cd /mnt/rtm

7. Deploy the Platform RTM packages.

   - Install all Platform RTM components. The following command assumes that you accept both the GNU General Public License (GPL) and the Platform End User License Agreement (EULA).

      yum localinstall rtm*.rpm rrdtool*.rpm python-cherrypy*.rpm python-simplejson*.rpm php-json*.rpm

- Only install the open source components.

  yum localinstall rtm-admin-plugin*.rpm rtm-boost-plugin*.rpm rtm-cacti*.rpm rtm-doc*.rpm rtm-extras*.rpm rtm-flexlm*.rpm rtm-release*.rpm rtm-lsfpollerd*.rpm rtm-grid-plugin*.rpm rtm-rtmssh-plugin*.rpm rtm-settings-plugin*.rpm rtm-syslog-plugin*.rpm rtm-thold-plugin*.rpm rrdtool*.rpm python-simplejson*.rpm php-json*.rpm python-cherrypy*.rpm

8. Erase existing databases from your host.

   This is necessary because Platform RTM will tune the MySQL configuration to optimize the database performance based on the specifications of your host. This requires the recreation of the InnoDB log and data files.

   Run the following commands to erase the MySQL databases from your host:

   Note:

   If you have any data that you need on the existing databases, back up the MySQL database (for example, by using mysql dump) before proceeding.

   ```
   service mysqld stop
   rm -f /var/lib/mysql/ibdata*
   rm -f /var/lib/mysql/ib_logfile*
   ```

9. Start the Platform RTM service.

   service rtm start

   The Platform RTM service initializes the Platform RTM database and configuration.

10. Change the method that your host uses to forward log messages in the network from syslogd to rsyslog.

    The Cacti syslog plugin included with Platform RTM requires the use of rsyslog instead of syslogd in order to function correctly.

    Run the following commands to change from syslogd to rsyslog.

    ```
    service syslog stop
    chkconfig syslog off
    chkconfig rsyslog on
    service rsyslog start
    ```

11. Allow the Platform RTM host to accept syslog messages forwarded from other hosts.

    a) Run the iptables command to create a new iptables rule for accepting syslog messages from other hosts.

       iptables -A INPUT -i eth0 -p udp -m state --state NEW --dport 514 -j ACCEPT

    b) Save the current iptables rules to the /etc/sysconfig/iptables file:

       service iptables save

       Important:

       By default, /etc/sysconfig/iptables file does not exist on a fresh installed host. Run service iptables save command to save the current firewall policy to /etc/sysconfig/iptables file.

       The /etc/sysconfig/iptables file can only be saved when the iptables service is running.

       ---

12. Clean up the temporary installation files from the Platform RTM host.

    umount /mnt/rhel-iso

```
rmdir /mnt/rhel-iso
umount /mnt/rtm-iso
rmdir /mnt/rtm-iso
rm -rf /mnt/rtm
rm -rf /mnt/rhel
mv -f /etc/yum.conf.orig /etc/yum.conf
rm -f /etc/yum.repos.d/rhel.repo
rpm -e createrepo
```

Install Platform RTM on CentOS

This documentation refers to CentOS 5.x (5.2 or above) as the operating system with which RTM is installed.

Prepare to install

1. Run the CentOS installation program.

   For more information, refer to your CentOS 5.x installation documentation.

2. Either you disable the firewall or ensure that port 80 is open, and disable Security Enhanced Linux (SELinux).

   In the Security level field, if you select Enable firewall, you must also select the Web Server (HTTP, HTTPS) field.

   For the Enable SELinux? field, select Disable.

3. Ensure that the following packages are selected by default:

   - @ MySQL Database
   - @ Editors
   - @ System Tools
   - @ Text Internet
   - @ Web Server
   - @ Mail Server

   After you select the packages, the program proceeds with the installation.

4. If you have not disabled SELinux or allowed port 80 during installation, run the following commands:

   ```
   # system-config-securitylevel-tui
   # reboot
   ```

5. Restart the Platform RTM host to complete the installation and log into the host as root.

6. If your CentOS installation could not download from a CentOS repository, create a `yum` repository from the DVD media.

   1. Mount the CentOS 5 ISO image (for example, `centos5.dvd.iso`) by running the following commands:

      ```
      mkdir -p /mnt/centos-iso
      mkdir /mnt/centos
      mount -o loop centos5.dvd.iso /mnt/centos-iso
      ln -sf /mnt/centos-iso/CentOS/ /mnt/centos
      ```

   2. Create a `yum` repository by running the following commands:

      ```
      cd /mnt/centos/
      rpm -ivh CentOS/createrepo*.rpm
      createrepo -vp .
      ```

   3. Create a `/etc/yum.repos.d/centos.repo` text file with the following contents:

      ```
      [CENTOS]
      NAME=CENTOS
      baseurl=file:///mnt/centos
      enabled=1
      ```

Install the Platform RTM packages

1. Log into the Platform RTM host as root.

2. Download the Platform RTM installation packages from my.platform.com.

   1. Create a directory to store the installation packages.

      mkdir -p /mnt/rtm

   2. Download all the Platform RTM installation files and copy them into the /mnt/rtm directory.

      For Platform RTM 8.0.2, download all installation files from http://my.platform.com/products/platform-lsf-family/platform-rtm.

3. Verify that the md5sum for the downloaded tar file matches the sum on the website.

4. Uncompress the tar file.

5. Temporarily allow the Platform RTM host to install unsigned packages.

   You need to allow unsigned packages because some of the Platform RTM installation packages are unsigned.

   a) Make a backup copy of the /etc/yum.conf file.

      cp /etc/yum.conf /etc/yum.conf.orig

   b) Edit the /etc/yum.conf file and specify **gpgcheck=0** in the file.

6. Navigate to the RTM installation package directory.

   cd /mnt/rtm

7. Deploy the Platform RTM packages.

   • Install all Platform RTM components. The following command assumes that you accept both the GNU General Public License (GPL) and the Platform End User License Agreement (EULA).

      yum localinstall rtm*.rpm rrdtool*.rpm python-cherrypy*.rpm python-simplejson*.rpm php-json*.rpm

   • Only install the open source components.

      yum localinstall rtm-admin-plugin*.rpm rtm-boost-plugin*.rpm rtm-cacti*.rpm rtm-doc*.rpm rtm-extras*.rpm rtm-flexlm*.rpm rtm-release*.rpm rtm-lsfpollerd*.rpm rtm-grid-plugin*.rpm rtm-rtmssh-plugin*.rpm rtm-settings-plugin*.rpm rtm-syslog-plugin*.rpm rtm-thold-plugin*.rpm rrdtool*.rpm python-simplejson*.rpm php-json*.rpm python-cherrypy*.rpm

8. Erase existing databases from your host.

   This is necessary because Platform RTM will tune the MySQL configuration to optimize the database performance based on the specifications of your host. This requires the re-creation of the InnoDB log and data files.

   Run the following commands to erase the MySQL databases from your host:

   Note:

   If you have any data that you need on the existing databases, back up the MySQL database (for example, by using mysqldump) before proceeding.

   ```
   service mysqld stop
   rm -f /var/lib/mysql/ibdata*
   rm -f /var/lib/mysql/ib_logfile*
   ```

9. Start the Platform RTM service.

   service rtm start

   The Platform RTM service initializes the Platform RTM database and configuration.

10. Change the method that your host uses to forward log messages in the network from syslogd to rsyslog.

The Cacti syslog plugin included with Platform RTM requires the use of rsyslog instead of syslogd in order to function correctly.

Run the following commands to change from syslogd to rsyslog.

```
service syslog stop
chkconfig syslog off
chkconfig rsyslog on
service rsyslog start
```

11. Allow the Platform RTM host to accept syslog messages forwarded from other hosts.

a) Run the iptables command to create a new iptables rule for accepting syslog messages from other hosts.

```
iptables -A INPUT -i eth0 -p udp -m state --state NEW --dport 514 -j ACCEPT
```

b) Save the current iptables rules to the /etc/sysconfig/iptables file:

```
service iptables save
```

Important:

By default, /etc/sysconfig/iptables file does not exist on a fresh installed host. Run service iptables save command to save the current firewall policy to /etc/sysconfig/iptables file.

The /etc/sysconfig/iptables file can only be saved when the iptables service is running.

12. Clean up the temporary installation files from the Platform RTM host.

```
umount /mnt/centos-iso
rmdir /mnt/centos-iso
umount /mnt/rtm-iso
rmdir /mnt/rtm-iso
rm -rf /mnt/rtm
rm -rf /mnt/centos
mv -f /etc/yum.conf.orig /etc/yum.conf
rm -f /etc/yum.repos.d/centos.repo
rpm -e createrepo
```

Install Platform RTM on SLES

This documentation refers to SLES 10 SP2 (64 bit) and SLES 11 SP1 (64 bit) as the operating system with which Platform RTM is installed.

Prepare to install

1. Run the SLES installation program.

   For more information, refer to your SLES installation documentation.

   Follow the **# zypper install -t pattern lamp_server** software steps.

2. Ensure that the following packages are selected by default:

   - @ php5-curl
   - @ php5-snmp
   - @ php5-ldap
   - @ php5-gd
   - @ php5-mysql
   - @ gd
   - @ python-openssl
   - Apart from the listed packages for SLES 10, select @ python-devel
   - Apart from the listed packages for SLES 11, select @ rrdtool, @ perl-DBD-mysql, and @ net-snmp.

   After you select the packages, the program proceeds with the installation.

3. Remove postfix and install sendmail.

   # zypper install sendmail

   Select Solution 2: delete postfix when prompted.

4. Disable Novell AppArmor for Platform RTM to work properly.

   # yast

   Choose Novell AppArmor and select AppArmor Control Panel.

   Uncheck the enable option and choose Done.

5. Configure the firewall.

   1. In YaST, choose Security and Users > Firewall.
   2. Choose Allowed Services tab and select the Advanced option. Ensure that selected zone is External Zone.
   3. Enter following values for the following ports:

      TCP Ports: 22 25 80 113 443 513:1023

      UDP Ports: 514
   4. Proceed to see configuration summary. Review the settings for "Open Services, Ports, and Protocols" and accept the settings.
   5. Choose Security and Users>Firewall.
   6. Select Start-Up > When Booting. Under Switch On and Off, select Start Firewall Now.
   7. Review the settings and then accept it.

6. Configure Apache2 Web Server. Platform RTM uses symbolic link to link to the htdocs folder. Make changes in the following to allow symbolic link:

```
# cd /etc/apache2
```

```
# vim default-server.conf
```

Under the Configure the DocumentRoot section, change Options None to Options FollowSymLinks. Save and exit.

7. Ensure the APACHE_MODULES parameter has php5 in the list. For example,

APACHE_MODULES=actions alias auth_basic authn_file authz_host authz_groupfile authz_default authz_user authn_dbm autoindex cgi dir env expires include log_config mime negotiation setenvif ssl suexec userdir php5

8. Turn on Apache2 and MySQL server

 # chkconfig mysql on

 # chkconfig apache2 on

9. Configure timezone.

Edit /etc/php5/apache2/php.ini and /etc/php5/cli/php.ini, add timezone information under the [Date] section, for example,

[Date]

date.timezone = **Asia/Hong_Kong**

Install the Platform RTM packages

1. Log into the Platform RTM host as root.
2. Download the Platform RTM installation packages from my.platform.com.
   a) Create a directory to store the installation packages.

      mkdir -p /mnt/rtm
   b) Copy all the Platform RTM SLES installation files into the /mnt/rtm directory.
3. Verify that the md5sum for the downloaded tar file matches the sum on the website.
4. Uncompress the tar file.
5. Navigate to the RTM installation package directory.

   cd /mnt/rtm

   # rpm -ivh *.rpm
6. For SLES 11, replace /usr/lib64/python2.6/site-packages/cherrypy/_cpchecker.py with the file in patch directory # cp /mnt/rtm/_cpchecker.py /usr/lib64/python2.6/site-packages/cherrypy/_cpchecker.py
7. Erase existing databases from your host.

   This is necessary because Platform RTM will tune the MySQL configuration to optimize the database performance based on the specifications of your host. This requires the recreation of the InnoDB log and data files.

   Run the following commands to erase the MySQL databases from your host:

   Note:

If you have any data that you need on the existing databases, back up the MySQL database (for example, by using `mysql dump`) before proceeding.

```
service mysql stop
rm -f /var/lib/mysql/ibdata*
rm -f /var/lib/mysql/ib_logfile*
```

8. Start the Platform RTM service.

   service rtm start

   The Platform RTM service initializes the Platform RTM database and configuration.

9. Startup sendmail service.

   # service sendmail start

10. Clean up the temporary installation files from the Platform RTM host.

    ```
    # rm -rf /mnt/rtm
    ```

Install Platform RTM

4

Activate Platform RTM

Prerequisites:

* You have a valid license key for Platform RTM.
* Your local host (that is, the computer that you will use to access the Platform RTM Console) is running a supported web browser.

  Platform RTM supports Firefox 3.6 or later and Internet Explorer (IE) 8 or later.

The following describes the initial post-installation and configuration tasks that you need to perform for Platform RTM to function properly.

1. Log into your local host.
2. Add licenses to your Platform RTM installation.
   a) Use your web browser to launch the Platform RTM Console.

      The URL for the Platform RTM Console is **http://*rtm_host*/cacti** where rtm_host is either the Platform RTM host name or IP address.

      For example, if your Platform RTM host name is $hostA.example.com$ with IP address $192.168.1.5$, you can use either of the following URLs to launch the Platform RTM Console:

      * **http://hostA.example.com/cacti**
      * **http://192.168.1.5/cacti**
   b) Specify the Platform RTM administrator name and password.

      The default administrator name is **admin**, and the default password for this account is **admin**.

      To see the License Info page, click the Admin tab, then the License subtab.
   c) Add the license file to Platform RTM.

      You can add the license file to Platform RTM using one of the following methods:

      * Click Browse and navigate to your license file.
      * Open your license file with a text editor and copy the text to the clipboard, then paste this text to the License Text field in the License Info page.
   d) Click Save to save the license file to Platform RTM.
3. Add LSF clusters for RTM to monitor.

Follow the steps described in `Add or edit LSF clusters for Platform RTM to monitor` in the Platform RTM Administration guide for every LSF cluster that you want Platform RTM to monitor.

4. Add license servers for Platform RTM to monitor.

   Follow the steps described in for every license server that you want Platform RTM to monitor.

5. Optional. Set up the Platform RTM database on a remote host.

   By default, the Platform RTM host runs as the database host. You may choose to set up the database on another host to disperse Platform RTM activity to other machines, or to use a more optimal database host.

   Follow the steps in the Platform RTM Administration guide to set up the Platform RTM database on a remote host.

6. Optional. Click the Admin tab to verify and configure the date and time of your Platform RTM host.

   You can also update or upgrade your Platform RTM license using this tab. For more information on the Admin tab, refer to .

Set time zone

Navigate to the Datetime Edit page by clicking the Admin tab, then the Date & Time subtab. This page defines the time zone, and current date and time. You can also specify an NTP server. After changing any of these settings, RTM restarts the system services.

Note:

If the server is not able to synchronize the date/time, you can manually set the date/time. NTP overrides any manual settings once the server is able to synchronize.

Activate Platform RTM

5

Upgrade Platform RTM to a Newer Version

If you have an existing cluster with Platform RTM and Platform LSF, follow upgrade steps.

Versions supported for upgrade

The following versions are supported for Platform RTM upgrade.

- Platform RTM 2.1.2->Platform RTM 8.0.2 on RHEL 5.2 or above (X86_64), CentOS 5.2 or above (X86_64)
- Platform RTM 8.0->Platform RTM 8.0.2 on RHEL 5.2 (or above) X86_64, CentOS 5.2 (or above) (X86_64), SLES 10(SP2) (X86_64), SLES11(SP1) (X86_64)
- Platform RTM 2.0.1->Platform RTM 8.0.2 on SLES 10(sp2) (X86_64)

Upgrade Platform RTM on RHEL and CENTOS

You must be a RTM administrator.

Note:

Prior to running the upgrade scripts, backup the Platform RTM database. Backup utility can be found at:

Console > Utilities > Grid Utilities > Force Cacti Backup

Or if your Platform RTM 2.1.2 is upgraded from 2.0.x, then **Console > Grid Management > Utilities > Force Cacti Backup**.

Note that the backup process may take a long time for large deployments.

---

1. Log into the Platform RTM host as root.
2. Download the Platform RTM installation packages from my.platform.com.

   * Download the Platform RTM installation tar file and extract them into the `/mnt/rtm` directory.

     For Platform RTM, download all .rpm files from `http:\\my.platform.com\products\platform-lsf-family\platform-rtm`.

   * Extract the Platform RTM installation packages from the Platform RTM ISO image.

     Run the following commands to copy the packages from an ISO image:

     ```
     mkdir -p /mnt/rtm-iso
     mount -o loop /file_path/rtm-version.architecture.iso /mnt/rtm-iso
     mkdir -p /mnt/rtm
     cp -v /mnt/rtm-iso/CentOS/rtm*.rpm /mnt/rtm
     cp -v /mnt/rtm-iso/CentOS/rrdtool*.rpm /mnt/rtm
     cp -v /mnt/rtm-iso/CentOS/python-cherrypy*.rpm /mnt/rtm
     cp -v /mnt/rtm-iso/CentOS/python-simplejson*.rpm /mnt/rtm
     cp -v /mnt/rtm-iso/CentOS/php-json*.rpm /mnt/rtm
     ```

3. Update the `/etc/yum.conf` file and set **gpgcheck=0**.
4. Stop all the Platform RTM services.

   service licpollerd stop

   service lsfpollerd stop

   service advocate stop

   service crond stop

5. Navigate to the RTM installation package directory and update RPMs.

   cd /mnt/rtm

   yum localinstall rtm*.rpm rrdtool*.rpm python-cherrypy*.rpm python-simplejson*.rpm php-json*.rpm

---

Caution:

If you see the following warning, then the config file must have been modified since the last installation.

warning: *<config file path>* created as *<config file path>.rpmnew*

Merge the modifications into the *<config file path>*.rpmnew file and replace the *<config file path>*.rpmnew file with the original *<config file path>*.

diff *<config file path> <config file path>*.rpmnew

cp *<config file path> <config file path>*.bak

vi *<config file path>*.rpmnew

mv *<config file path>*.rpmnew *<config file path>*

6. (Optional) If Platform RTM is using a remote database, refer to the Platform RTM Administration guide and check for the configuration files. Make sure that the database configuration is pointing to the remote database host.

7. Upgrade the Platform RTM pollers, database, and templates.

   For advanced configuration edit /etc/rtm_install.conf. Here you can specify different users or groups for pollers, files, directories, or database.

   For Remote License or LSF Pollers, refer to INSTALL.REMOTE_LICPOLLER or INSTALL.REMOTE_LSFPOLLER README.

   Note:

   If you are upgrading from Platform RTM 8.0, log into cacti database in mysql with root (i.e. mysql -u root cacti) and execute the following SQL statement:

   REPLACE INTO settings (name, value) VALUES ('grid_db_version', '8.0');

   service rtm upgrade

   Note:

   You can refer to /var/log/rtm.upgrade.log for details or errors encountered during the upgrade.

   The upgrade script spawns a background process to upgrade the jobs table. This process will continue even after you have completed the upgrade steps. During this period, the job search will be limited.

   The upgrade script doesn't silently upgrade existing datasource templates, you can log into cacti database in MySQL with root (i.e. mysql -u root cacti) and execute the following SQL statement:

   ```
   UPDATE data_template_rrd SET rrd_maximum=0 WHERE
   data_source_type_id=1 AND rrd_maximum <> 0;
   ```

   Or import cacti_data_template_<datasource-name>.xml from /opt/cacti/templates/upgrade/

8. Restart the Platform RTM services.

   service licpollerd restart

   service lsfpollerd restart

   service advocate restart

   service crond restart

   service sendmail restart

9. Clean up the temporary installation files from the Platform RTM host.

```
umount /mnt/rhel-iso
rmdir /mnt/rhel-iso
rm -rf /mnt/rtm
mv -f /etc/yum.conf.orig /etc/yum.conf
```

10. Upgrade your license file.

   Remember:

   You need to upgrade your license file to enable lsfpoller and
   licpoller feature for server monitoring.

11. After upgrading Platform RTM, log on to the Platform RTM portal and check the LSF Cluster status on the Console > Grid Management > Clusters page.

Upgrade Platform RTM on SLES

You must have Platform RTM installed before you can upgrade it. You must be a RTM administrator.

Note:

Prior to running the upgrade scripts, backup the Platform RTM database. Backup utility can be found at:

Console > Utilities > Grid Utilities > Force Cacti Backup

Or if your Platform RTM 2.1.2 is upgraded from 2.0.x, then **Console > Grid Management > Utilities > Force Cacti Backup**.

Note that the backup process may take a long time for large deployments.

Make sure that you have installed php5-sockets and python-devel packages before you start the upgrade process.

zypper install php5-sockets

zypper install python-devel

Then restart http server.

service apache2 restart

---

1. Log into the Platform RTM host as root.
2. Download the Platform RTM installation packages from my.platform.com. There are separate packages for SLES 10 and SLES11.

   Copy the installation files into the /mnt/rtm directory.

   For Platform RTM, download all .rpm files from http:\\my.platform.com\products \platform-lsf-family\platform-rtm.
3. Stop all the Platform RTM services.

   service licpollerd stop (if this service is available)

   service lsfpollerd stop

   service advocate stop

   service cron stop
4. Navigate to the RTM installation package directory and update RPMs.

   cd /mnt/rtm

   rpm -Uvh python-cherrypy*.rpm

   rpm -Uvh python-simplejson*.rpm

   rpm -Uvh python-pexpect*.rpm

   rpm -Uvh --nopostun rtm*.rpm

Caution:

If you see the following warning, then the config file must have been modified since the last installation.

warning: *<config file path>* created as *<config file path>*. rpmnew

Merge the modifications into the *<config file path>*. rpmnew file and replace the *<config file path>*. rpmnew file with the original *<config file path>*.

diff *<config file path>* *<config file path>*.rpmnew

cp *<config file path>* *<config file path>*.bak

vi *<config file path>*.rpmnew

mv *<config file path>*.rpmnew *<config file path>*

5. (Optional) If Platform RTM is using a remote database, refer to the Platform RTM Administration guide and check for the configuration files. Make sure that the database onfiguration is pointing to the remote database host.

6. Upgrade the Platform RTM pollers, database, and templates.

    service rtm upgrade

    For advanced configuration edit /etc/rtm_install.conf. Here you can specify different users or groups for pollers, files, directories, or database.

    For Remote License Pollers, refer to INSTALL.REMOTE_LICPOLLER README.

    Note:

    You can refer to /var/log/rtm.upgrade.log for details or errors encountered during the upgrade.

    The upgrade script spawns a background process to upgrade the jobs table. This process will continue even after you have completed the upgrade steps. During this period, the job search will be limited.

    The upgrade script doesn't silently upgrade existing datasource templates, you can log into cacti database in MySQL with root (i.e. mysql -u root cacti) and execute the following SQL statement:

    ```
    UPDATE data_template_rrd SET rrd_maximum=0 WHERE
    data_source_type_id=1 AND rrd_maximum <> 0;
    ```

    Or import cacti_data_template_<datasource-name>.xml from /opt/cacti/templates/upgrade/

    ---

7. Restart the Platform RTM services.

    service licpollerd restart

    service lsfpollerd restart

    service advocate restart

    service cron restart

    service sendmail restart

8. Clean up the temporary installation files from the Platform RTM host.

    ```
    umount /mnt/iso
    rmdir /mnt/iso
    rm -rf /mnt/rtm
    ```

9. Upgrade your license file.

    Remember:

You need to upgrade your license file to enable lsfpoller and
licpoller feature for server monitoring.

10. After upgrading Platform RTM, log on to the Platform RTM portal and check the LSF Cluster status
on the Console > Grid Management > Clusters page.

6

Set up Remote License or LSF Pollers (Optional)

Platform RTM is preconfigured with local license or LSF pollers to collect information from license or LSF servers. If you want to use remote license or LSF pollers, you need to set up and configure the remote license pollers to work with Platform RTM. For more details on how to set up and configure remote license or LSF pollers on Platform RTM, refer to the INSTALL.REMOTE_LICPOLLER or INSTALL.REMOTE_LSFPOLLER README.

Set up Remote License or LSF Pollers (Optional)

7

Enable Remote Hosts Syslog Transfer

To enable cluster hosts to appear in the Platform RTM Syslogs page, make sure that the hosts run `syslogd` to forward log messages in the network.

Optional. If you want any hosts in the LSF clusters that Platform RTM monitors to appear in the Platform RTM Syslogs page, you need to enable the hosts to forward logs to the Platform RTM host.

Important:

The `syslog` must be installed on a host where you want system logs to be forwarded to RTM host. The `syslog.conf` file will not exist if the application is not installed.

Perform the following steps on each host that you want to appear on the Platform RTM Syslogs page.

1. Log into a remote host.
2. Edit the `/etc/syslog.conf` file and add the following line to the end of the file:

   . @*rtm_host_ip*

   where *rtm_host_ip* is the IP address of your Platform RTM host.

   For example, if your IP address is 192.168.1.5, add the following to the end of the `syslog.conf` file:

   . @192.168.1.5
3. Restart the `syslog` service to apply your changes.

   service syslog restart

Enable Remote Hosts Syslog Transfer

8

Enable Grid Control on an LSF Cluster

Enable grid control on an LSF cluster to grant Platform RTM access to that cluster. This allows you to run LSF commands on that cluster.

Prerequisites: The LSF cluster and the RTM host must meet the following requirements:

- The LSF master host is a Linux, AIX, HPUX, or Solaris host with sh or bash installed.
- The Platform RTM host is a LSF server, or is added to the LSF cluster as an LSF client.
- The RTM host has rsh or ssh access to the LSF master host.
- The LSF master host uses at least one of the following methods of authentication and meets the corresponding requirements:

    - ssh password authenticaion: You are asked for the password of the LSF master host root user each time you invoke a cluster control action.
    - ssh private key authentication

        - You created an ssh public key pair by running **sshkeygen -t rsa** on the RTM host as root, then adding the public key to the authorized_keys file of the LSF master host root user.
        - The LSF master host has password-less authentication (ssh private key authorization or rsh) available with all other hosts in the LSF cluster.
    - rsh password-less authentication

        - The .rhosts file in the LSF master host specifies the root user of the RTM host.
        - The LSF master host and the RTM host both have the incoming TCP port 514 open.
        - The LSF master host has password-less authentication (ssh private key authorization or rsh) available with all other hosts in the LSF cluster.

The following describes the steps that you need to perform to enable grid control and allow you to control LSF clusters using the Platform RTM Console.

1. Click the Console tab.
2. Enable grid control for each applicable user in the RTM host.
    a) Under the Utilities section of the Console menu bar, click User Management.
    b) Click the name of the user for which you want to enable grid control.
    c) In the Realm Permissions section, select the Cluster Control Management field, if it is currently unchecked.
3. Under the Grid Management section of the Console menu bar, click Clusters.

4. Enable grid control on LSF clusters.

Perform the following for each cluster that you want to control:

a) Click the name of the cluster that you want to control.

The Cluster Edit page displays.

b) Click Control tab.

The User Authentication settings section appears.

c) In the User Authentication settings section, specify the settings for the Primary LSF administrator account in the LSF master host.

To ensure that RTM has access to the appropriate LSF commands, you must consider the following:

- The specified Primary LSF administrator user name is the name of the LSF adminsitrator account in the LSF cluster for which you are enabling grid control. You must specify the username of the Primary LSF Administrator for the LSF machine. You need to set the cluster username before executing cluster via advocate, otherwise, invalid credentials/no username specified error appears.

  This account is used by the Host-, Queue-, and Job-level controls using eauth in the LSF master host to invoke the control actions. After saving these settings, this user name is created as a disabled Unix local account in the RTM host.

- If you are connecting to the LSF master host using ssh private key authentication, you need to provide the private key path pointing to the private key file. As shown in the prerequisites, the public key of this file is added to the authorized_keys file of the LSF master host root user.

- The LSF server top directory is the top-level LSF installation directory (LSF_TOP).

d) Click Save to apply your changes.