Table of Contents

System Administrator Guide for CEMon for EMI-1

1 Installation and Configuration

1.1 Prerequisites

1.1.1 Operating system

A standard 64 bit SL(C)5 distribution is supposed to be properly installed.

1.1.2 Node synchronization

A general requirement for the Grid nodes is that they are synchronized. This requirement may be fulfilled in several ways. One of the most common one is using the `NTP` protocol with a time server.

1.2 Plan how to deploy CEMon

1.2.1 Choose the authorization model

CEMon can be configured to use as authorization system:

- the ARGUS authorization framework

OR

- the grid Java Authorization Framework (gJAF)

In the former case a ARGUS box (usually at site level) where to define policies is needed.

To use ARGUS as authorization system, yaim variable `USE_ARGUS` must be set in the following way:

```
USE_ARGUS=yes
```

In this case it is also necessary to set the following yaim variables:

- `ARGUS_PEPD_ENDPOINTS` The endpoint of the ARGUS box (e.g."https://cream-43.pd.infn.it:8154/authz")
- `CREAM_PEPC_RESOURCEID` The id of the CREAM CE in the ARGUS box (e.g. "http://pd.infn.it/cream-18")

If instead gJAF should be used as authorization system, yaim variable `USE_ARGUS` must be set in the following way:

```
USE_ARGUS=no
```

1.2.2 Repositories

For a successful installation, you will need to configure your package manager to reference a number of repositories (in addition to your OS);

- the EPEL repository
- the EMI middleware repository
- the CA repository

and to **REMOVE (!!!)** or **DEACTIVATE (!!!)**

- the DAG repository

1.2.2.1 The EPEL repository

You can install the EPEL repository, issuing:

```
rpm -Uvh http://download.fedora.redhat.com/pub/epel/5/i386/epel-release-5-4.noarch.rpm
```

1.2.2.2 The EMI middleware repository

The EMI-1 RC4 repository can be found under:

```
http://emisoft.web.cern.ch/emisoft/dist/EMI/1/RC4/sl5/x86_64
```

To use yum, the yum repo to be installed in `/etc/yum.repos.d` can be found at https://twiki.cern.ch/twiki/pub/EMI/EMI-1/rc4.repo

1.2.2.3 The Certification Authority repository

The most up-to-date version of the list of trusted Certification Authorities (CA) is needed on your node. The relevant yum repo can be installed issuing:

```
wget http://repository.egi.eu/sw/production/cas/1/current/repo-files/egi-trustanchors.repo -O /et
```

1.2.2.4 Important note on automatic updates

An update of an RPM not followed by configuration can cause problems. Therefore **WE STRONGLY RECOMMEND NOT TO USE AUTOMATIC UPDATE PROCEDURE OF ANY KIND**.

Running the script available at http://forge.cnaf.infn.it/frs/download.php/101/disable_yum.sh (implemented by Giuseppe Platania, INFN Catania) yum autoupdate will be disabled

1.2.3 Installation of CEMon

In EMI, CEMon is installed as part of the CREAM-CE. So the following instructions refer to the installation of the CREAM CE.

First of all, install the `yum-protectbase` rpm:

```
  yum install yum-protectbase.noarch
```

Then proceed with the installation of the CA certificates:

```
yum install ca-policy-egi-core
```

To proceed the installation, install fSun JDK (`jdk`) or openjdk (`java-1.6.0-openjdk`)

Then install `xml-commons-apis`:

```
yum install xml-commons-apis
```

This is due to a dependency problem within the Tomcat distribution

Then install the CREAM-CE metapackage:

```
yum install emi-cream-ce
```

1.2.4 Installation of the CEMon CLI

The CEMon CLI is part of the EMI-UI. To install it please refer to the Generic Installation & Configuration Guide

1.3 Configuration

1.3.1 Using the YAIM configuration tool

For a detailed description on how to configure the middleware with YAIM, please check the YAIM guide .

The necessary YAIM modules needed to configure a certain node type are automatically installed with the middleware.

1.3.2 Configuration of CEMon using yaim

In EMI, CEMon is installed and configured as part of the CREAM-CE

1.3.2.1 Install host certificate

The CREAM CE node requires the host certificate/key files to be installed. Contact your national Certification Authority (CA) to understand how to obtain a host certificate if you do not have one already.

Once you have obtained a valid certificate:

- hostcert.pem - containing the machine public key
- hostkey.pem - containing the machine private key

make sure to place the two files in the target node into the `/etc/grid-security` directory. Then set the proper mode and ownerships doing:

```
chown root.root /etc/grid-security/hostcert.pem
chown root.root /etc/grid-security/hostkey.pem
chmod 600 /etc/grid-security/hostcert.pem
chmod 400 /etc/grid-security/hostkey.pem
```

1.3.2.2 Configure the siteinfo.def file

Set your `siteinfo.def` file, which is the input file used by yaim. Documentation about yaim variables relevant for CREAM CE is available at
https://twiki.cern.ch/twiki/bin/view/LCG/Site-info_configuration_variables#cream_CE

Be sure that `USE_CEMON` is set to `true`.

1.3.2.3 Run yaim

After having filled the `siteinfo.def` file, run yaim:

```
/opt/glite/yaim/bin/yaim -c -s <site-info.def> -n creamCE
```

1.3.3 Configuration of the CEMon CLI

The CEMon CLI is part of the EMI-UI. To configure it please refer to xxx.

2 Operating the system

2.1 How to start the CEMon service

A site admin can start the CEMon service just starting the tomcat container:

```
/etc/init.d/tomcat5 start
```

To stop the CEMon service, it is just necessary to stop the CEMon container:

```
/etc/init.d/tomcat5 stop
```

2.2 Configuration files

Information about configuration files in the CEMonis available at
http://wiki.italiangrid.org/twiki/bin/view/CEMon/ServiceReferenceCard#Configuration_files_location_wit

2.3 Log files

Information about log files in the CREAM CE is available at
http://wiki.italiangrid.org/twiki/bin/view/CEMon/ServiceReferenceCard#Logfile_locations_and_management

2.4 Network ports

Information about ports used in the CREAM CE is available at
http://wiki.italiangrid.org/twiki/bin/view/CEMon/ServiceReferenceCard#Open_ports

2.5 Security related operations

2.5.1 Security recommendations

Security recommendations relevant for CEMon is available at
http://wiki.italiangrid.org/twiki/bin/view/CEMon/ServiceReferenceCard#Security_recommendations

2.5.2 How to block/ban a user

Information about how to ban users is available at
http://wiki.italiangrid.org/twiki/bin/view/CEMon/ServiceReferenceCard#How_to_block_ban_a_user

2.5.3 How to block/ban a VO

To ban a VO, it is suggested to reconfigure the service via yaim without that VO in the `siteinfo.def`

2.6 How to add/remove sensors

CEMon sensors that must be plugged in CEMon are defined in the CEMon configuration file (`/etc/glite-ce-monitor/cemonitor-config.xml`). Each active sensor is identified by a section that has the following format:

```
 <sensor id=xxx
```

```
...
...
/sensor>
```

By default only the `CREAM job` sensor is enabled.

To enable/disable a specific sensor, it is just necessary to uncomment/comment the sensor definition in the CEMon configuration file. Please note that then it is NOT necessary to restart tomcat

2.7 How to add a static subscription

There are two types of subscriptions:

- subscriptions created by an authorized user (using e.g. the `glite-ce-monitor-subscribe` command)
- static subscriptions, created by the CEMon system administrator

Static subscriptions can be created editing the CEMon configuration file `/etc/glite-ce-monitor/cemonitor-config.xml`.

An example of static subscription settings is this one:

```
<subscription id="subscription-1"
              subscriberId="_C_IT_O_INFN_OU_Personal_Certificate_L_Padova_CN_Massimo_Sgaravatto
              subscriberGroup="dteam"
              monitorConsumerURL="https://cream-47.pd.infn.it:8788"
    sslprotocol="SSLv3"
              retryCount="-1">
  <topic name="CREAM_JOBS">
    <dialect name="CLASSAD" />
  </topic>
  <policy rate="60" />
</subscription>
```

After having added/removed a static subscription, it is NOT necessary to restart tomcat.

-- MassimoSgaravatto - 2011-04-20

This topic: CEMon > SystemAdministratorGuide
Topic revision: r6 - 2012-04-19 - MassimoSgaravatto