Install Manual

Management Center – Application Portal

SMC Application Portal

Install Manual

Printed: April 2010

Table of Contents

1 SMC Application Portal Installation

Introduction

The SMC Application Portal is installed on the master host of the cluster. The "master host" is the computer on which cluster and system management services are run. The installation includes the SMC Application Portal application and supporting third-party applications. The main items installed include:

- SMC Application Portal web application
- JBoss application server
- Java Development Kit
- PostgreSQL Database
- LDAP server

1.1 SMC Application Portal Requirements

The following lists the hardware and software requirements for running the SMC Application Portal on a cluster. Ensure that these requirements are met before beginning the SMC Application Portal installation process.

Hardware requirements for the cluster:

- Master host: x86_64 processor

Note: The "master host" is the computer on which cluster and system management services are run.

- A homogeneous set of compute node(s)
- A Gigabit Ethernet or InfiniBand switch for the high-speed interconnect
- Network accessibility to the master host from the compute node(s)

Software requirements for the cluster:

- SUSE Linux Enterprise Server 11 (any service pack)
- GNU GCC Compiler
- User home directories NFS mounted on to the compute node(s)
- Altair PBS Professional 9.x, or higher, for UNIX batch scheduling (10.2 is required for dynamic provisioning support)
- Password-less RSH and/or SSH between the master host and compute node(s)
- A local or remote lightweight directory access protocol (LDAP) server must be available for user authentication
- Environment module package installed and functional. See http://modules.sourceforge.net, for more information about environment modules.
- The master host must have the following distribution packages installed: PyXML, Python, and OpenSSL.
- If the operating system is SUSE Linux Enterprise Server 11, the `libXerces-c28` package is required (available from the SLES 11 SDK).

The following software packages must be installed and functional for applicable features of the SMC Application Portal to be utilized:

- FLUENT 6.3.x

- Abaqus 6.7-x Standard/Explicit
- ANSYS Multiphysics (ane3fl)
- Intel MPI 3.1 (or later)
- SGI MPT 1.19 (or later)
- Intel C/C++/Fortran Compiler Suite

Web browser requirements for users:

- Firefox 2.0.4 (or later)
- Safari 3.0.4 (or later)
- Microsoft Internet Explorer 6 or 7

SMC Application Portal functionality in other browsers or browser versions is not guaranteed.

1.2 Installation

Installation is performed from a directory containing installation materials. These installation materials may be on a CDROM or downloaded from the SGI web site.

Perform the installation in the order described since later steps depend on prior steps.

Follow the installation instructions using the directory names, user names, and passwords supplied. Failure to do so can result in malfunction of one or more components.

Unless otherwise specified, perform all operations as **root user**.

1.2.1 Package Installation

To install SMC Application Portal on the master host, you can use any front-end for RPM, such as YaST, Yum, and so on.

Add the SMC Application Portal CDROM or ISO image as an installation source, and install the following packages:

- `java-1.5.0-sun-devel`
- `lkSGI`
- `lkSGI-java`
- `postgresql_jwx`
- `jboss`
- `jbossws`
- `portal`

- islepbs
- portalcfg

1.2.2 LDAP Server

The SMC Application Portal uses LDAP to authorize and authenticate users. Your LDAP server must have a "Roles" Organizational Unit (OU) defined, and the users who will be using the SMC Application Portal should belong to the role of "Administrator", "User", or both.

The following instructions will allow you to create a local LDAP server. For troubleshooting or more information about LDAP, see http://openldap.org.

Install Packages

From your Linux distribution CDROM or software repository, install the following packages:

SLES 11:
- openldap2
- openldap2-client
- nss_dap
- pam_ldap

Edit the Configuration File

Edit the OpenLDAP daemon `slapd.conf` configuration file, which is typically located in the `/etc/openldap` or `/etc/ldap directory` (depending upon your Linux distribution). The following is an example of example of a `slapd.conf` file, with comments removed.

Note: The example below uses the directory `/var/run/slapd` for the location of the LDAP `pid` file and `args` files. If your default `slapd.conf` file uses a different location for the "`pidfile`" and "`argsfile`" properties, it is recommended to keep the existing settings for these properties instead of using the version from the example.

```
include     /etc/openldap/schema/core.schema
include     /etc/openldap/schema/cosine.schema
include     /etc/openldap/schema/inetorgperson.schema
include     /etc/openldap/schema/nis.schema

loglevel    256
pidfile     /var/run/slapd/slapd.pid
argsfile    /var/run/slapd/slapd.args

TLSCipherSuite  HIGH
TLSCertificateFile /etc/openldap/ssl/ldapserver.cert
TLSCertificateKeyFile /etc/openldap/ssl/ldapserver.key

access to attrs=userPassword,shadowLastChange
        by dn="cn=Manager,dc=foo,dc=bar,dc=com" write
        by anonymous auth
        by self write
        by * none

access to dn.base="" by * read

access to dn.base="cn=Subschema" by * read
```

```
access to *
        by dn="cn=Manager,dc=foo,dc=bar,dc=com" write
        by * read

database    bdb
suffix      "dc=foo,dc=bar,dc=com"
checkpoint  32  30
rootdn      "cn=Manager,dc=foo,dc=bar,dc=com"
rootpw      {SSHA}pmGNh60VoZ6hcRU+YfODO1DD1gpMhYSD
directory   /var/lib/ldap
index       objectClass     eq
index       cn,sn,mail      eq,sub
index       departmentNumber    eq
```

Change the LDAP administrative password, as follows:

- Run the `slappasswd` command. Enter the desired administrative password for `ldap`. It will return a hashed password, such as `{SSHA}pmGNh60VoZ6hcRU+YfODO1DD1gpMhYSD`

(example is for the password "secret")

- Add this to the `slapd.conf` file for the `rootpw` value

Install a Self-signed SSL Certificate

LDAP needs a Secure Sockets Layer (SSL) Certificate installed (unless you choose not to use to turn off TLS/SSL, which is not recommended.) If you need to use a self-signed certificate, you can run the following commands to create the key and certificate:

```
# mkdir /etc/openldap/ssl
# cd /etc/openldap/ssl
# openssl req -new -x509 -nodes -out ldapserver.cert -keyout ldapserver.key
```

Next, a basic structure for the LDAP database is needed. The code example below is a good starting point for a blank database. It provides the following:

- Creates a top level entry for a server "`foo.bar.com`", whose organizational unit is "`Foo Bar Widgets Emporium`"
- Creates a "`Group`" entry
- Creates a group named "`users`" underneath Group, with a GID of 100 and a user named "`fbarr`" as a member of "`users`"
- Creates a "`People`" entry
- Adds a user named "`fbar`" to "`People`", with UID 1012, and GID of 100
- Creates a "`Roles`" entry
- Adds the roles "`Administrator`" and "`User`" - each having the user "`fbarr`" as a member.

```
dn: dc=foo,dc=bar,dc=com
dc: foo
objectClass: dcObject
objectClass: organizationalUnit
ou: Foo Bar Widgets Emporium
structuralObjectClass: organizationalUnit

dn: ou=Group,dc=foo,dc=bar,dc=com
ou: Group
objectClass: organizationalUnit
entryUUID: a9e43208-96e7-102c-91ff-f7ec5e060c07
```

```
dn: cn=users,ou=Group,dc=foo,dc=bar,dc=com
objectClass: posixGroup
objectClass: top
cn: users
gidNumber: 100
memberUid: fbarr
structuralObjectClass: posixGroup

dn: ou=People,dc=foo,dc=bar,dc=com
ou: People
objectClass: organizationalUnit
structuralObjectClass: organizationalUnit

dn: uid=fbarr,ou=People,dc=foo,dc=bar,dc=com
uid: fbarr
cn: Foux Barr
sn: Barr
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
loginShell: /bin/bash
uidNumber: 1012
gidNumber: 100
homeDirectory: /home/fbarr
gecos: Foux Barr
structuralObjectClass: inetOrgPerson
userPassword:secret

dn: ou=Roles,dc=foo,dc=bar,dc=com
objectClass: organizationalUnit
ou: Roles
structuralObjectClass: organizationalUnit

dn: cn=admin,ou=Roles,dc=foo,dc=bar,dc=com
cn: admin
objectClass: top
objectClass: groupOfUniqueNames
uniqueMember: uid=fbarr,ou=People,dc=foo,dc=bar,dc=com
structuralObjectClass: groupOfUniqueNames

dn: cn=user,ou=Roles,dc=foo,dc=bar,dc=com
cn: user
objectClass: top
objectClass: groupOfUniqueNames
structuralObjectClass: groupOfUniqueNames
uniqueMember: cn=users,ou=Group,dc=foo,dc=bar,dc=com
uniqueMember: uid=fbarr,ou=People,dc=foo,dc=bar,dc=com
```

Note: A sample LDIF file is provided on the installation media under the `docs/` directory, called `sample_ldif.txt`.

To import the LDIF file to your LDAP server, you must meet the following conditions:

- No pre-existing LDAP database.
- The `slapd` daemon must not be active.

Now perform the following steps:

1. As **root user**, execute the following:

```
# slapadd -v -l /path/to/ldif
```

You should see output verifying that the various entries are added.

2. Start up the `slapd` daemon by entering the command:

```
# /etc/init.d/ldap start
```

3. To verify that LDAP is working, perform the following command:

```
# ldapsearch -x -b "dc=foo,dc=bar,dc=com" "objectclass=*"
```

4. Enable the LDAP server to run by entering the following command:

```
# chkconfig --add ldap
```

The LDAP database has now been added.

Login Authentication Using LDAP

In order for jobs to run on the SMC Application Portal properly, the same user you use to log in to the SMC Application Portal should be accessible from Linux also. To do this, perform the following:

- For SLES 11, use YaST to configure Linux to log on using LDAP. Open YaST, go to Network Services, LDAP Client. Check Use LDAP and populate the server name/address and LDAP Base DN. Check LDAP TLS/SSL.

1.2.3 Install the License

You will need to obtain a license key from SGI.
For information about software licensing, refer to the licensing FAQ at http://www.sgi.com/support/licensing/faq.html.

Open the `/etc/lk/keys.dat` file in a text editor. Copy and paste the license string, exactly as given, and save the file.

1.3 Configure the SMC Application Portal

This section describes how to configure the SMC Application Portal using the configuration GUI and set up the dynamic provisioning feature with PBS Professional 10.2 (or higher). It contains these sections:

1.3.1 Configure the SMC Application Portal Using the Configuration GUI

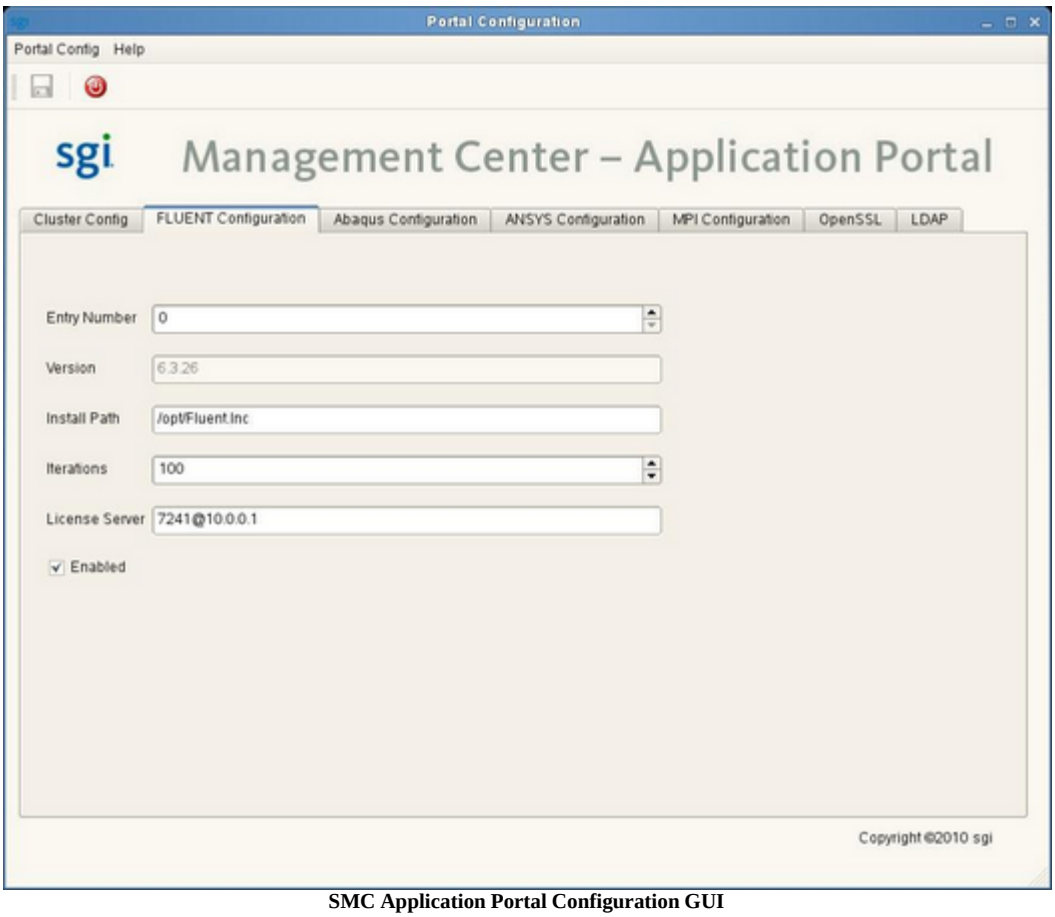
This section describes how to configure the SMC Application Portal.

- Execute the following commands to start the Configuration GUI:

```
# cd /opt/sgi/portal/portalcfg
```

```
# ./portalcfg.py
```

The SGI Management Center - Application Portal Configuration GUI appears. Use the arrow button on the right to view all of the configuration tabs. Use the red button on the left to exit the GUI.



SMC Application Portal Configuration GUI

- On the **Cluster Config** tab, change the "**Maximum Nodes**"

value to match the number of nodes in your cluster. Change the "**Cores/Node**" value to match the number of CPU cores available on each node in your cluster. Choose the default high-speed interconnect for your cluster.

- On the **FLUENT Configuration** tab, you can change the install path, default number of iterations, and License Server value for your FLUENT installation. You can also enable or disable configured versions of FLUENT here.

- On the **Abaqus Configuration** tab, you can set the Abaqus Home, Abaqus Binary and License server for each configured version of Abaqus. You can also enable or disable configured versions of Abaqus here.

- On the **ANSYS Configuration** tab, you can set the ANSYS executable and path, and the ANSYS license server. You can also enable or disable configured versions of ANSYS here.

- On the **MPI Configuration** tab, you can enable and disable configured MPI(s) on the system.

- Click on the **OpenSSL** tab to Generate a **Self-Signed Key**. Use the **Update Portal SSL Config** button to install the certificate.

- On the **LDAP** tab, enter the Search Base DN, LDAP URI, LDAP Admin DN, LDAP Password, Authentication Method, and Roles DN for the LDAP Server that will be providing authentication for the SMC Application Portal.

Note: The If your environment modules or installed Message Passing Interface (MPI) applications differ from the versions supported by SGI, please edit the `/opt/sgi/portal/portal/admin/portal_config.xml` file and review the <*module*> or <*home*> sections for each of your installed MPI(s).

1.3.2 Setting Up Dynamic Provisioning

If you want to use the dynamic provisioning feature with PBS Professional 10.2 (or higher), you must add one or more "`available_os`" entries in the `/opt/sgi/portal/portal/admin/jobworx_config.xml` configuration file. Each `available_os` value corresponds to the name of an image that is available in the SGI Management software for provisioning nodes.

```
<config id="cluster" version="1">
      <entry id="maxnodes" key="maxnodes" value="14"/>
       <entry id="processors" key="processors" value="4"/>
       <entry id="ptype" key="ptype" value="64"/>
      <entry id="interconnect" key="interconnect" value="infiniband"/>
      <entry id="interconnect_install" key="interconnect_install"
          value="ethernet"/>
      <entry id="ibtype" key="ibtype" value="IBV"/>
      <entry id="myrtype" key="myrtype" value="GM"/>
      <entry id="available_os" key="SUSE Linux Enterprise Server"
          value="Compute-SLES11.0"/>
</config>
```

Note: This example is for a configuration with SGI Management Center containing one image named `Compute-SLES11.0`.

Please see the PBS Professional documentation on details about setting up PBS Professional for dynamic provisioning.

1.4 Start SMC Application Portal Services

This section describes how to start the SMC Application Portal services.

As **root** user, start the services by running the following commands:

```
# /etc/init.d/postgres start
# /etc/init.d/jboss start
# /etc/init.d/portal start
# /etc/init.d/islepbs start
```

The following services will be started:

- The `postgres` and JBOSS Services, needed for SMC Application Portal
- The SMC Application Portal Heartbeat daemon
- The `Islepbs` daemon

Once the services have been started, you can verify the operation of SMC Application Portal by loading the URL https://hostname:8443/portal.

You can now log in to the SMC Application Portal using the accounts established in the LDAP server.

1.5 Uninstall the SMC Application Portal

Perform the following commands, to stop the SMC Application Portal services:

NOTE: The "`islepbs`" package only applies if you are using the PBS Professional job scheduler.

```
# /etc/init.d/islepbs stop
# /etc/init.d/portal stop
# /etc/init.d/jboss stop
# /etc/init.d/postgres stop
```

Uninstall the SMC Application Portal by using the following commands:

```
# rpm -e islepbs
# rpm -e portal
# rpm -e jbosssws
# rpm -e jboss
# rpm -e portalcfg
# rpm -e postgresql_jwx
```

Index

- C -

- I -

- M -

- S -

- U -

Technical Publications Library
http://docs.sgi.com