AUTHORIZED DOCUMENTATION

Installation Guide

Novell®
Cloud Manager

1.1

December 8, 2010

www.novell.com

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

This guide provides instructions for installing and configuring a Novell Cloud Manager 1.1 system. It includes the following sections:

Audience

This information is intended for anyone who needs to install and configure the Novell Cloud Manager software. Consumers of this information should be experienced Linux system administrators who are familiar with and have administrative rights to the authentication LDAP directory (Microsoft Active Directory or Novell eDirectory), have working knowledge of PostgreSQL databases, and understand certificate issues related to secure authentication.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of this guide, visit the Novell Cloud Manager 1.1 documentation Web site (http://www.novell.com/documentation/cloudmanager1).

Additional Documentation

For other Novell Cloud Manager 1.1 documentation, see the Novell Cloud Manager 1.1 documentation Web site (http://www.novell.com/documentation/cloudmanager1).

Installation Checklist

1

To ensure that you successfully install and configure Novell Cloud Manager, you should follow the installation checklist provided below. Each task provides brief information and a reference to where you can find more complete details.

It is assumed that you already completed the tasks in the *Novell Cloud Manager 1.1 Installation Roadmap* (http://www.novell.com/documentation/cloudmanager1/pdfdoc/ncm1_getting_started/ncm1_getting_started.pdf) to implement a virtualization infrastructure and set up PlateSpin Orchestrate.

Task	Details
☐ Review the Cloud Manager requirements and supported environments	See Chapter 2, “System Requirements,” on page 11 and Chapter 3, “Supported Environments,” on page 15
☐ Prepare for installation	Before installing and configuring Cloud Manager, you need to prepare the LDAP directory that Cloud Manager will use to authenticate users. In addition, if you plan to use a remote database for storing Cloud Manager data, you need to prepare the database. See Chapter 4, “Pre-Installation Preparation,” on page 17.
☐ Install the Cloud Manager software	You install Cloud Manager to a supported version of SUSE Linux Enterprise Server (SLES) 10 or 11. See Chapter 5, “Installation,” on page 21.
☐ Configure the Cloud Manager system	After installation, you must complete several configuration tasks before Cloud Manager can be used, including configuring the Cloud Manager application server (GlassFish), connecting to the Cloud Manager database, and configuring the connections between the Cloud Manager Server and the PlateSpin Orchestrate Servers. See Chapter 6, “Configuration,” on page 23.

After you’ve completed the installation and configuration, continue with *Building a Cloud* in the *Novell Cloud Manager 1.1 Administration Guide* to start populating your Cloud Manager system with the components that will enable users to provision their own business services.

System Requirements

2

The requirements for Novell Cloud Manager are listed below.

2.1 PlateSpin Orchestrate

Cloud Manager utilitizes PlateSpin Orchestrate to automate the creation and management of workloads in your virtual infrastructure.

Cloud Manager 1.1 requires PlateSpin Orchestrate 2.6. Cloud Manager 1.1 does not work with any versions of PlateSpin Orchestrate other than version 2.6.

For system requirements and installation instructions for PlateSpin Orchestrate 2.6, see the *PlateSpin Orchestrate 2.6 Installation and Configuration Guide*.

2.2 Server Requirements

The Cloud Manager Server requires the following.

Item	Requirement
Operating System	Any of the following: • **SLES 11 SP1 (64-bit):** SUSE Linux Enterprise Server 11 Service Pack 1 on the 64-bit (x86-64) architecture (Intel and AMD Opteron processors) • **SLES 11 SP1 (32-bit):** SUSE Linux Enterprise Server 11 Service Pack 1 on the 32-bit (x86) architecture (Intel and AMD Opteron processors) • **SLES 11 (64-bit):** SUSE Linux Enterprise Server 11 on the 64-bit (x86-64) architecture (Intel and AMD Opteron processors) • **SLES 11 (32-bit):** SUSE Linux Enterprise Server 11 on the 32-bit (x86) architecture (Intel and AMD Opteron processors) • **SLES10 SP3 (64-bit):** SUSE Linux Enterprise Server 10 Service Pack 3 on the 64-bit (x86-64) architecture (Intel and AMD Opteron processors) • **SLES 10 SP3 (32-bit):** SUSE Linux Enterprise Server 10 Service Pack 3 on the 32-bit (x86) architecture (Intel and AMD Opteron processors)

Item	Requirement
Hardware	**Minimum:** A single-server configuration, with the Cloud Manager Server and PlateSpin Orchestrate Server running on the following minumum supported hardware: ◆ 4 Pentium-class CPU cores ◆ 40 GB disk space ◆ 4 GB RAM **Recommended:** A two-server configuration, with the Cloud Manager Server running on the following hardware: ◆ Xeon dual-core or higher ◆ 20 GB disk space ◆ 4 GB RAM and the PlateSpin Orchestrate Server running on the following hardware: ◆ Xeon dual-core or higher ◆ 20 GB disk space ◆ 3 GB RAM
Database	PostgreSQL (included with SLES)
TCP Ports	The following ports are used by the Cloud Manager Server. The ports (or their substitutes if not using the defaults) must be open for both inbound and outbound communication: ◆ 4848 - Application Server administration port ◆ 5432 - PostgreSQL database port (default) ◆ 7676 - JMS port ◆ 8080 - HTTP port (default) ◆ 8181 - HTTPS port (default) ◆ 8686 - JMX port

2.3 Console Requirements

The Cloud Manager console is a Web-based application that requires the following:

Item	Requirement
Web Browser	Any of the following: ◆ **Internet Explorer 8:** Supported on Windows 7 (32/64-bit), Windows Vista (32/64-bit), and Windows XP (32-bit) ◆ **Mozilla Firefox 3.6:** Supported on Windows 7 (32/64-bit), Windows Vista (32/64-bit), and Windows XP (32-bit) ◆ **Mozilla Firefox 3.5:** Supported on Windows 7 (32/64-bit), Windows Vista (32/64-bit), Windows XP (32-bit), SLED 11 SP1 (32/64-bit)
Display Resolution	1024 x 768 or higher
Pop-Up Blocker	Allow pop-ups from Cloud Manager console to enable Help system

2.4 LDAP Directory Service Requirements

Cloud Manager authenticates users via an LDAP directory. The directory must meet the following requirements:

Item	Requirement
LDAP Directory	Either of the following: ◆ Microsoft Active Directory ◆ Novell eDirectory

Supported Environments

3

Novell Cloud Manager supports the following virtualization environments:

Item	Supported Environment
Hypervisor	◆ VMware vSphere 4.x ◆ Windows Server 2008 R2 Hyper-V ◆ Xen (as part of SLES 10 SP3 or SLES 11 SP1)
Windows workloads (VMs)	◆ Windows Server 2008 (32- and 64-bit) ◆ Windows Server 2003 (32- and 64-bit)
Linux workloads (VMs)	◆ SUSE Linux Enterprise Server 11 ◆ SUSE Linux Enterprise Server 10 ◆ SUSE Linux Enterprise Server 9 ◆ Red Hat Enterprise Linux 5 ◆ Red Hat Enterprise Linux 4

Pre-Installation Preparation

4

Before installing and configuring Novell Cloud Manager, you need to prepare the LDAP directory that Cloud Manager will use to authenticate users. In addition, if you plan to use a remote database for storing Cloud Manager data, you need to prepare the database.

4.1 Preparing the LDAP Directory

Cloud Manager authenticates users via a supported LDAP directory service, either Microsoft Active Directory or Novell eDirectory. Cloud Manager users must have an account in the directory and be a member of the Cloud Manager user group.

4.1.1 Identifying the User Search Base

Cloud Manager requires you to specify a search base for users. When authenticating a user, Cloud Manager checks only the users contained within the search base.

As you identify the search base, consider the following:

- If you plan to use an existing directory for authentication, you will need to set the search base to a container that encompasses the users who require access to Cloud Manager.
- If you plan to set up a new directory, you can structure the directory to maximize efficiency by placing the users in one container (a flat structure) and specifying the container as the search base. If you need to support multiple departments, organizations, or companies, you can create separate containers for each and set the search base above the containers.

You supply the search base when configuring the LDAP connection in Cloud Manager. Make sure you know the DN of the search base (for example, `cn=Users,dc=MyCompany,dc=com`).

4.1.2 Resolving Duplicate User IDs

Cloud Manager does not support user IDs that are the same, even if they are in different containers in the directory. Capitalization does not make a user ID unique. For example, JSmith and jsmith in the directory are the same user in Cloud Manager.

You should ensure that all users have unique user IDs.

4.1.3 Creating the Cloud Manager Group

Access to Cloud Manager is controlled through membership in a Cloud Manager user group. Only users who are members of the group can log in.

1. Create a user group using any valid LDAP name (for example, `CloudManagerGroup` or `ncmusers`).

   Remember the name and the container. During configuration of the LDAP connection, you will need to provide the group's common name and the search base for the group (for example, `cn=Groups,dc=MyCompany,dc=com`)

2. Add users who need access to Cloud Manager.

   Make sure to add yourself and any other individuals who will be Cloud Manager administrators.

   You can add users to the group at any time. To ensure that no users can log in until you've completely set up Cloud Manager, wait to add users (other than yourself) until later.

4.1.4 Creating a Search Account for Cloud Manager

Cloud Manager requires an account that has rights to search and read the following directory containers and objects:

- The user search base container and all containers beneath it.
- The Cloud Manager user group container.

4.2 Preparing a Remote Database

Cloud Manager stores information to a PostgreSQL database. You can use a local database (on the Cloud Manager Server) or a remote database (on another server).

If you use a local database, the installation program installs and configures the database. If you use a remote database, you need to configure it.

To configure a remote database:

1. If the PostgreSQL server has never been started, start it to initialize its database:

   ```
   # rcpostgresql start
   ```

2. Edit `/var/lib/pgsql/data/pg_hba.conf`.

   Add the following line to enable a remote connection from the Cloud Manager Server:

```
host    all    all    server_address    md5
```

   where *server_address* is the Cloud Manager Server IP address in CIDR notation.

3. Edit `/var/lib/pgsql/data/postgresql.conf`.

   Find `listen_addresses = 'localhost'`, make sure the line is uncommented, and add the Cloud Manager Server's IP address to the list. For example, `listen_addresses = 'localhost,123.127.45.9'`.

4. Restart the PostgreSQL server:

   ```
   # rcpostgresql restart
   ```

5 Run the following commands:

```
# su - postgres -c psql
postgres=# CREATE DATABASE ncm;
postgres=# CREATE USER <username> password '<password>';
postgres=# GRANT ALL ON DATABASE ncm to <username>;
postgres=# \c ncm
ncm=# CREATE SCHEMA NOVELL;
ncm=# GRANT ALL on SCHEMA NOVELL to <username>;
ncm=# CREATE SCHEMA SCHDLR;
ncm=# GRANT ALL on SCHEMA SCHDLR to <username>;
ncm=# ALTER USER <username> SET search_path TO novell,public;
ncm=# \q
```

Installation

5

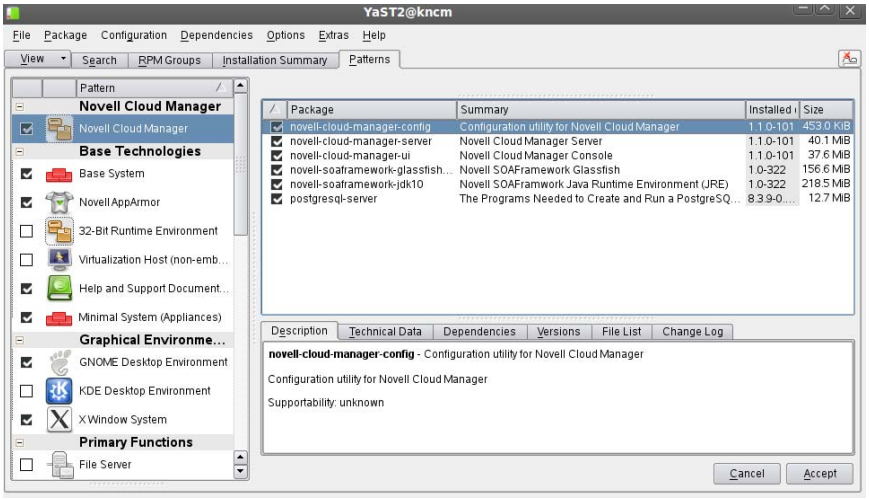
Novell Cloud Manager must be installed to a supported version of SUSE Linux Enterprise Server (SLES) 10 or 11.

5.1 Installing to SLES 11

1. Log in to the target SLES server as `root`, then open YaST.
2. Download the appropriate Novell Cloud Manager ISO to the SLES server.

   or

   Load the Novell Cloud Manager DVD on the SLES server.
3. Define the Novell Cloud Manager ISO or DVD as an add-on product:
   - **3a** In the YaST Control Center, click *Software*, then click *Add-On Products*.
   - **3b** Click Add, select *Local ISO Image* or *DVD*, then follow the prompts to add the product.
4. Read and accept the end-user license agreement (EULA), then click *Next* to display Yast2.
5. In YaST2, click *View*, then select *Patterns* to display the Novell Cloud Manager installation pattern.



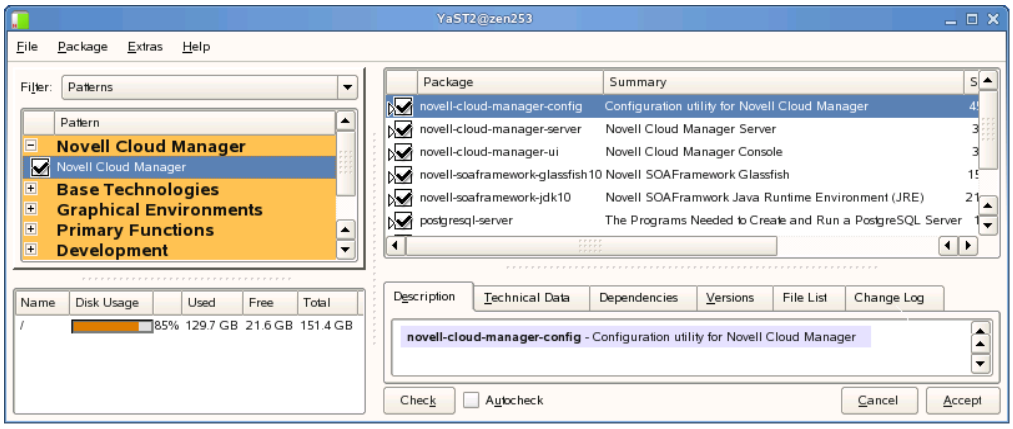
6. Select the Novell Cloud Manager installation pattern.
7. Click *OK* to install the packages.
8. When package installation is complete, click *OK* to close the Installed Add-On Products dialog box.
9. Continue with Chapter 6, “Configuration,” on page 23 to configure the Cloud Manager Server.

5.2 Installing to SLES 10

1. Log in to the target SLES server as `root`, then open YaST.
2. Download the appropriate Novell Cloud Manager ISO to the SLES server.

   or

   Load the Novell Cloud Manager DVD on the SLES server.
3. Define the Novell Cloud Manager ISO or DVD as an add-on product:
   - **3a** In the YaST Control Center, click *Software*, then click *Add-On Products*.
   - **3b** In the Add-on Product Media dialog box, select the ISO media (*Local Directory* or *DVD*) to install.
     - **3b1** (Conditional) Select *DVD*, click *Next*, insert the DVD, then click *Continue*.
     - **3b2** (Conditional) Select *Local Directory*, click *Next*, select the *ISO Image* check box, browse to ISO on the file system, then click *OK*.
4. Read and accept the end-user license agreement (EULA), then click *Next* to display YaST2.
5. In YaST2, click the *View* drop-down menu, then select *Patterns* to display the Novell Cloud Manager install patterns



6. Select the Novell Cloud Manager install pattern, the click *Accept* to install the packages.
7. When package installation is complete, exit YaST and ontinue with Chapter 6, “Configuration,” on page 23 to configure the Cloud Manager Server.

Configuration

6

After you've installed the Novell Cloud Manager software, you need to perform the following tasks to configure the system:

6.1 Configuring GlassFish and the Database Connection

The Cloud Manager Server runs as a set of applications within a GlassFish application server domain. You must run the Cloud Manager configuration utility to create and configure the domain. The utility also configures access to the PostgreSQL database used by the Cloud Manager Server.

1 Make sure you know the information that you will be prompted for during configuration:

GlassFish Application Server	
Administrator username and password	You must provide a username and password to use for the GlassFish administrator. If it ever becomes necessary for you to access the GlassFish application server directly, you can use this name and password. The password must be at least 8 characters.
Administrative port	This port lets you access the application server for administrative purposes The default is 4848. You should use this port unless it is already being used.
HTTP port	This is the non-secure HTTP port. The default is 8080. You should use this port unless it is already being used. If you installed the Cloud Manager Server on the same machine as a PlateSpin Orchestrate Server, port 8080 is used by the Orchestrate Server so you must specify a different port (for example, 8081, 8008, or so forth).
HTTP secure port	This is the secure HTTP port. The default is 8181. You should use this port unless it is already being used.

PostgreSQL Database	
Database server address	The hostname or IP address of the server where the database resides. If the database is local to the Cloud Manager Server, you can use `localhost`.
Database port	This field is displayed only for remote databases. Specify the port on which the remote database listens.
Database username and password	If the database is local, you must provide a name and password that will be used when creating the Cloud Manager database instance. If the database is remote, you must specify the name and password that allows access to database instance that you created when configuring the remote database (see Chapter 4, “Pre-Installation Preparation,” on page 17. The password must be at least 8 characters.

2 At the Cloud Manager Server, run the following command as root to ensure that `boot.clock` is enabled:

```
chkconfig boot.clock on
```

The GlassFish application server has a dependency on `boot.clock`. If boot.clock is not enabled, the Cloud Manager Server cannot run.

3 At the Cloud Manager Server, run the Cloud Manager configuration utility:

```
/opt/novell/cloud-manager/config
```

The configuration utility launches and displays the following:

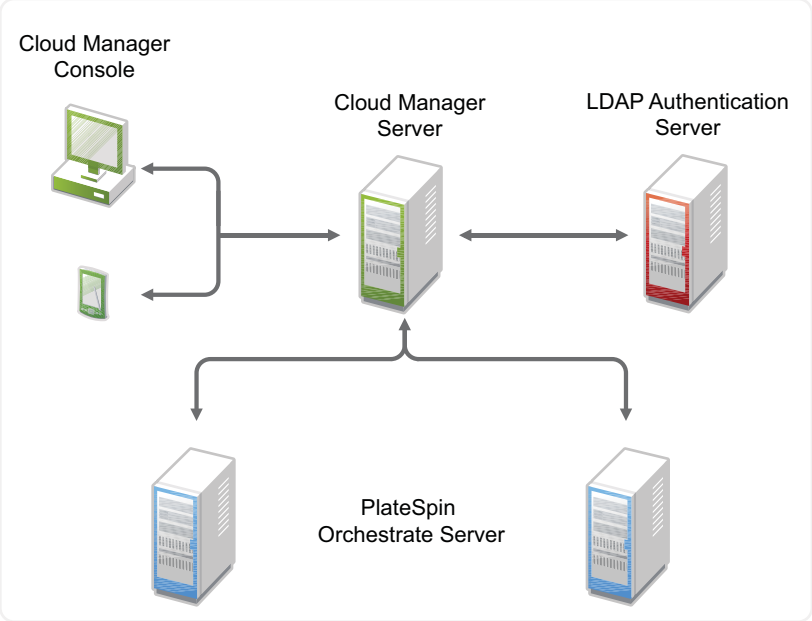
```
Welcome to the Novell Cloud Manager configuration utility.


This utility lets you configure:
    - the GlassFish application server that is installed
      by Cloud Manager
    - the connection to the PostgreSQL database used for
      storing Cloud Manager data

Continue? (y/n) [yes]:
```

4 Follow the prompts.

5 After configuration of the application server and database connection is complete, continue with “Configuring Cloud Manager Server Connections” on page 25.

6.2 Configuring Cloud Manager Server Connections

The Cloud Manager Server communicates with the Cloud Manager Console, the LDAP Server, and all PlateSpin Orchestrate Servers via HTTP connections. The connections can be secure (SSL) or non-secure (no SSL).



The following sections provide configuration instructions for each of the Cloud Manager Server's connections:

- Section 6.2.1, "Configuring the Cloud Manager Console Connection," on page 25
- Section 6.2.2, "Configuring the PlateSpin Orchestrate Server Connections," on page 27
- Section 6.2.3, "Configuring the LDAP Server Connection," on page 29

6.2.1 Configuring the Cloud Manager Console Connection

No configuration is required to use a non-secure connection between the Cloud Manager Server and the Cloud Manager console. If this is the type of connection you want to use, skip to "Configuring the PlateSpin Orchestrate Server Connections" on page 27.

By default, the Cloud Manager Server supports a secure connection with the console. When the server is installed, it creates a self-signed certificate as the server certificate. You can keep the self-signed certificate or replace it with your own trusted certificate so that when users log in the first time, they are prompted to accept your trusted certificate rather than the untrusted, self-signed certificate.

The following sections explain how to replace the self-signed certificate with either an existing or new trusted certificate provided by your Certificate Authority (CA).

- "Using an Existing Certificate" on page 26
- "Generating a New Certificate" on page 26

Using an Existing Certificate

If you already have a certificate for the server where you installed the Cloud Manager Server and you want to use that certificate, complete the following steps.

1. Make sure that your private key and certificate are in .DER format (*key*.der and *cert*.der), that the key is encoded in PKCS#8 format, and that the certificate is encoded in X.509 format.
2. Use the importkey java class (ImportKey.class) to import the private key and certificate into a new java keystore file:

   2a If you don't have the importkey java class, download it from one of the many available sites such as this site (http://www.agentbob.info/agentbob/79-AB.html).

   2b Run the following command:

```
java ImportKey key.der cert.der s1as
```

   This creates a keystore.ImportKey file that contains the private key and certificate stored under an s1as alias.

   Note: The 1 in slas is the number 1 not the letter l.

3. Rename the keystore.ImportKey file to keystore.jks and copy it to the following location to replace the old keystore file:

   ```
   /var/opt/novell/soaframework10/domains/NovellCloudManager/config
   ```

4. Reset the keystore password to changeit:

   ```
   keytool -keystore keystore.jks -storepasswd -new changeit
   ```

   When prompted for the old password, enter importkey.

5. Reset the private key password (identified by the s1as alias) to changeit:

   ```
   keytool -keystore keystore.jks -alias s1as -storepass changeit -keypasswd
   ```

   When prompted for the old password, enter importkey.

6. Restart the Cloud Manager Server:

   ```
   /etc/init.d/novell-soaframework.NovellCloudManager restart
   ```

Generating a New Certificate

The following steps explain how to generate a new certificate for use:

1. On the Cloud Manager Server, change to the directory that contains the keystore.jks file:

   ```
   /var/opt/novell/soaframework10/domains/NovellCloudManager/config
   ```

2. Delete the default self-signed certificate:

```
keytool -delete -alias s1as -keystore keystore.jks -storepass store_password
```

   where *store_password* is the keystore password. If you have not changed the default password after installation of the Cloud Manager Server, the password is changeit.

3. Generate a new key pair and self-signed certificate:

```
keytool -genkey -keyalg keyalg -keystore keystore.jks -validity val_days -
alias s1as
```

   where *keyalg* is the algorithm for generating the key pair (for example, RSA) and *val_days* is the number of days the certificate is valid (for example, 365).

In addition to generating the key pair, the command wraps the public key into a self-signed certificate and stores the certificate and the private key in a new keystore entry identified by the alias (`s1as`).

While generating the key pair and certificate, you need to ensure that the certificate matches the fully-qualified name of your Cloud Manager Server.

4. Generate a certificate signing request (CSR):

```
keytool -certreq -alias s1as -file certreq_file -keystore keystore.jks -
storepass store_password
```

where *`certreq_file`* is the CSR file to create (for example, `slas.csr`) and *`store_password`* is the keystore password (the default is `changeit`).

5. Submit the CSR to a CA to receive a signed server certificate.
6. Store the signed server certificate from the CA including the markers `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` into `s1as.cert` file.
7. Copy the `slas.cert` file to the following Cloud Manager Server directory:

   `/var/opt/novell/soaframework10/domains/NovellCloudManager/config`
8. Replace the original self-signed certificate with the signed certificate from the CA (stored in the `s1as.cert` file):

```
keytool -import -v -alias s1as -file s1as.cert -keystore keystore.jks -
storepass store_password
```

where *`store_password`* is the keystore password (the default is `changeit`).

9. Restart the Cloud Manager Server:

   `/etc/init.d/novell-soaframework.NovellCloudManager restart`

NOTE: We strongly recommend that you change the default password (`changeit`) for the Cloud Manager Server keystore. For instructions, see How to Change the Keystore Password (http://weblogs.java.net/blog/2007/11/19/ssl-and-crl-checking-glassfish-v2#4).

6.2.2 Configuring the PlateSpin Orchestrate Server Connections

The Cloud Manager Server requires a connection to each PlateSpin Orchestrate Server that you plan to define as a Cloud Manager zone.

- “Enabling a Secure Connection” on page 27
- “Enabling a Non-Secure Connection” on page 29

Enabling a Secure Connection

A secure connection requires certificate authentication between the Cloud Manager Server and the PlateSpin Orchestrate Server. To enable a secure connection, you need to generate the public certificate for the PlateSpin Orchestrate Web Server, import the public certificate to the Cloud Manager Server trust store, and configure the secure port for the PlateSpin Orchestrate Web Service. The following sections provide instructions:

- “Generating the PlateSpin Orchestrate Web Service Public Certificate” on page 28

- “Importing the Certificate into the Cloud Manager Server Trust Store” on page 28
- “Configuring the PlateSpin Orchestrate Web Service Secure Port” on page 28

Generating the PlateSpin Orchestrate Web Service Public Certificate

The PlateSpin Orchestrate Web Service is started automatically as part of the PlateSpin Orchestrate Server startup. The first time it starts, the Web Service creates a keystore, generates a public/private key pair, and exports the public key to a certificate.

You should check the public certificate to ensure ensure that it includes the correct information. If it does not, you will need to fix the information issues and regenerate the certificate.

1. On the PlateSpin Orchestrate Server, change to the `/opt/novell/pso-ws/jetty/etc` directory.
2. Verify the certificate:

   ```
   keytool -printcert -file psoserver.cer
   ```

   The CN entry in the certificate must match the FQDN of the host. If it does not, resolve the issue in DNS and then regenerate the `psoserver.cer` file by doing the following:

   - Delete the `keystore` file from the `/opt/novell/pso-ws/jetty/etc` directory.
   - Restart the PlateSpin Orchestrate Web Service:

     ```
     /etc/init.d/novell-pso-ws restart
     ```

     When it is restarted, the PlateSpin Orchestrate Web Service creates a new keystore, generates a public/private key pair, and exports the public key to a certificate.

Importing the Certificate into the Cloud Manager Server Trust Store

1. Copy the `psoserver.cer` file from the `/opt/novell/pso-ws/jetty/etc` directory on the PlateSpin Orchestrate Server to the following directory on the Cloud Manager Server:

   ```
   /var/opt/novell/soaframework10/domains/NovellCloudManager/config
   ```

2. Change to the `/var/opt/novell/soaframework10/domains/NovellCloudManager/config` directory.
3. Import the `psoserver.cer` file into the trust store:

   ```
   /opt/novell/soaframework-jdk10/bin/keytool -import -keystore cacerts.jks
   -alias psoserver -file psoserver.cer
   ```

4. Verify the key import:

   ```
   /opt/novell/soaframework-jdk10/bin/keytool -list -keystore cacerts.jks
   ```

5. Restart the Cloud Manager Server:

   ```
   /etc/init.d/novell-soaframework.NovellCloudManager restart
   ```

Configuring the PlateSpin Orchestrate Web Service Secure Port

By default, the PlateSpin Orchestrate Web Service listens on port 8443. If you want to change this port:

1. On the PlateSpin Orchestrate Server, open the `jetty-ssl.xml` file:

   ```
   /etc/opt/novell/pso-ws/jetty/jetty-ssl.xml
   ```

2 Locate the <Call name =”addConnector”> section. It will look similar to the section shown below:

```
<Call name="addConnector">
  <Arg>
    <New class="org.mortbay.jetty.security.SslSocketConnector">
      <Set name="Port">8443</Set>
      <Set name="maxIdleTime">30000</Set>
      <Set name="handshakeTimeout">2000</Set>
      <Set name="keystore"><SystemProperty name="jetty.home" default="."
        />/etc/keystore</Set>
      <Set name="password">OBF:1vny1zlo1x8e1vnw1vn61x8g1zlu1vn4</Set>
      <Set name="keyPassword">OBF:1u2u1wml1z7s1z7a1wnl1u2g</Set>
      <Set name="truststore"><SystemProperty name="jetty.home"
        default="." />/etc/keystore</Set>
      <Set name="trustPassword">OBF:1vny1zlo1x8e1vnw1vn61x8g1zlu1vn4</Set>
      <Set name="handshakeTimeout">2000</Set>
    </New>
  </Arg>
</Call>
```

3 In the <Set name="Port"> directive, change the port number.

When adding the PlateSpin Orchestrate Server as a zone in Cloud Manager, you specify this port as the server port.

4 Save the jetty-ssl.xml file.

5 Restart the PlateSpin Orchestrate Web Service:

```
/etc/init.d/novell-pso-ws restart
```

Enabling a Non-Secure Connection

1 On the PlateSpin Orchestrate Server, open the jetty.xml file:

```
/etc/opt/novell/pso-ws/jetty/jetty.xml
```

2 Uncomment the <Call name =”addConnector”> section that enables the non-secure port.

3 Change port 8080 to another non-secure port such as 8081, 8082, or 8008.

If port 8080 is not already taken by another service, you can use port 8080. However, more than likely, the port is already taken because both the PlateSpin Orchestrate User Portal and Cloud Manager Server use port 8080 as the default non-secure HTTP port.

When adding the PlateSpin Orchestrate Server as a zone in Cloud Manager, you specify this port as the server port.

4 Save the jetty.xml file.

5 Restart the PlateSpin Orchestrate Web Service:

```
/etc/init.d/novell-pso-ws restart
```

6.2.3 Configuring the LDAP Server Connection

No configuration is required to use a non-secure connection between the Cloud Manager Server and the LDAP Server. If this is the type of connection you want to use, skip this section and continue with Section 6.3, “Connecting to the LDAP Directory,” on page 30.

If you want to use a secure connection from the Cloud Manager Server to the LDAP Server, you need to export the LDAP Server's certificate and import it into the Cloud Manager Server's trust store:

- "Exporting the LDAP Server Certificate" on page 30
- "Importing the Certificate into the Cloud Manager Server Trust Store" on page 30

Exporting the LDAP Server Certificate

Using the certificate management tool available for your LDAP Server, export the server certificate from your LDAP Server in X.509 (.cer) format.

Importing the Certificate into the Cloud Manager Server Trust Store

1. Copy the `.cer` file from the LDAP Server to the following directory on the Cloud Manager Server:

   `/var/opt/novell/soaframework10/domains/NovellCloudManager/config`

2. Change to the `/var/opt/novell/soaframework10/domains/NovellCloudManager/config` directory.

3. Import the `.cer` file into the trust store:

```
/opt/novell/soaframework-jdk10/bin/keytool -import -keystore cacerts.jks  -alias alias -file certificate
```

   where *`alias`* is whatever name you want assigned to this entry in the keystore and *`certificate`* is the name of the LDAP `.cer` file.

4. Verify the key import:

   `/opt/novell/soaframework-jdk10/bin/keytool -list -keystore cacerts.jks`

5. Restart the Cloud Manager Server:

   `/etc/init.d/novell-soaframework.NovellCloudManager restart`

6.3 Connecting to the LDAP Directory

The final required configuration task is to provide the Cloud Manager Server with the information it needs to connect to and search the LDAP directory designated as the authentication source for Cloud Manager users. Before proceeding, make sure you completed the tasks in Section 4.1, "Preparing the LDAP Directory," on page 17.

1. From a supported Web browser, enter the following URL to access the Cloud Manager console:

```
http://domain:port
```

   where *`domain`* is the domain name of the server and *`port`* is the HTTP port (8080 by default) assigned when running the Cloud Manager configuration utility. The port number is not required if you completed the configuration in Section 6.4, "(Optional) Simplifying the Cloud Manager URL," on page 32.

   The console is displayed with only the LDAP configuration page accessible. You must configure and test the connection in order to access the rest of the console.

2. Provide the LDAP Server connection information:

Host: Specify the FQDN (fully qualified domain name) or IP address of the host machine running the LDAP Server. For example, `ldap.mycompany.com` or `123.45.67.8`.

Port: Specify the TCP port (on the host machine) where the LDAP Server is listening for LDAP connections. The standard port for non-SSL connections is 389. The standard port for SSL connections is 636.

Use SSL: Select this option to if you have already configured the Cloud Manager Server to support a secure connection to the LDAP Server (see Section 6.2.3, “Configuring the LDAP Server Connection,” on page 29) and you want to enable the secure connection.

3 Set the search base for the Cloud Manager users and user group:

Search Base DN: Specify the base location where user searches begin. All portions of the LDAP tree located below the base DN are searched. For example, `cn=Users,dc=MyCompany,dc=com`).

User Group: Specify the name of the LDAP user group used for Cloud Manager users. A user must be a member of this group to authenticate to Cloud Manager.

Group Base DN: Specify the base location where the search for the Cloud Manager user group begins. All portions of the LDAP tree located below the base DN are searched. For example, `cn=Groups,dc=MyCompany,dc=com`).

4 Provide an LDAP account that has search rights to the user and group base DNs:

DN: Specify an account that has rights to search the locations defined by the Search Base DN. For example, `cn=Administrator,cn=Users,dc=MyCompany,dc=com`

Password: Specify the password for the account.

Password Confirm: Confirm the password for the account.

5 Click *Test LDAP Configuration* to display the Test LDAP Configuration dialog box.

User Name: Specify the user ID of a Cloud Manager user. This user must exist in the search base DN and be a member of the Cloud Manager user group. This is the user that Cloud Manager will attempt to authenticate to test the configuration settings.

Password: Specify the user’s password.

6 If the test is successful, click *OK* to save the configuration. Otherwise, check the configuration information and repeat the test.

If the test fails, make sure of the following:

- The Novel Cloud Manager user group exists and is located in the specified group base DN.
- The search bind account has sufficient rights to the user search base and group search base.
- The Cloud Manager user you entered to test the configuration exists in the user search base and is a member of the Cloud Manager user group.

At this point, installation and configuration of your Novell Cloud Manager system is complete and you are ready to start populating your system with the components that will enable users to provision their own business services. For instructions, see *Building a Cloud* in the *Novell Cloud Manager 1.1 Administration Guide*.

6.4 (Optional) Simplifying the Cloud Manager URL

The URL to access the Cloud Manager console is:

`http://domain:HTTP_port` (non-secure)

or

`https://domain:secure_HTTP_port` (secure)

where *`domain`* is the domain name of the server, and *`HTTP_port`* and *`secure_HTTP_port`* are the ports assigned when running the Cloud Manager configuration utility (see Section 6.1, “Configuring GlassFish and the Database Connection,” on page 23).

Example URLs using the default ports might be:

`http://cloudmanager.novell.com:8080`

or

`https://cloudmanager.novell.com:8181`

The non-secure URL redirects automatically to the secure URL if the Cloud Manager Server is configured to support secure connections for the console.

If desired, you can eliminate the need to specify the ports by using ports 80 and 443. Because the GlassFish application server used by Cloud Manager does not bind to ports below 1024, you must configure the firewall on the Cloud Manager Server to redirect the ports to the standard 80 and 443 ports.

1. On the Cloud Manager Server, open the `/etc/sysconfig/SuSEfirewall2` file:
2. Locate the `FW_REDIRECT` command and change it to:

   ```
   FW_REDIRECT="0/0,0/0,tcp,80,8080 0/0,0/0,tcp,443,8181"
   ```

   If the Cloud Manager Server is not using the default ports (8080 and 8181), substitute the used ports in the command.
3. Locate the `FW_SERVICES_EXT_TCP` command and change it to:

   ```
   FW_SERVICES_EXT_TCP="443 80 8080 8181"
   ```

   If the Cloud Manager Server is not using the default ports (8080 and 8181), substitute the used ports in the command.
4. In YaST > Firewall, start the firewall and configure it to start automatically at computer startup.

If you go to `http://domain:80`, you are still redirected to `https://domain:8181` because of the GlassFish application server configuration. However, if you go to `https://domain` you never see the port redirection in the URL.

Software Updates

7

In an effort to continually improve your Cloud Manager experience, Novell releases updates to address important issues. Currently, the following update is available for Cloud Manager 1.1:

- Novell Cloud Manager 1.1.2 Update

You can download this update through your Novell Customer Center account. Instructions for applying the update are included in the download.

What’s Next?

8

At this point, installation and configuration of your Novell Cloud Manager system is complete and you are ready to start populating your system with the components that will enable users to provision their own business services. For information, see *Building a Cloud* in the *Novell Cloud Manager 1.1 Administration Guide*.

Uninstall

A

To uninstall the Novell Cloud Manager software:

1. Remove the Cloud Manager Server:

   1a On the Cloud Manager Server, run the Cloud Manager configuration utility:

   ```
   /opt/novell/cloud-manager/config
   ```

   1b When you are prompted to remove the current Cloud Manager domain and continue with the configuration, enter `Yes`.

   This removes the GlassFish application server files and Cloud Manager Server files. If the Cloud Manager database is local, it also removes the database from the PostgreSQL server and removes the Cloud Manager database user.

   1c When you receive the first configuration prompt (*Provide a username for the GlassFish administrator*), press `ctrl+c` to exit the configuration utility.

2. Use YaST to remove the Cloud Manager pattern from the server.

   Removing the pattern deletes the following packages:

   `novell-cloud-manager-config`

   `novell-cloud-manager-server`

   `novell-cloud-manager-ui`

   `novell-soaframework-glassfish10`

   `novell-soaframework-jdk10`

   The `postgresql-server` package is not removed with the pattern. To remove the postgres package, you must select the package for deletion.

3. Delete the `etc/init.d/novell_soaframework.NovellCloudManager` file.

4. If the Cloud Manager database is remote (rather than local to the server), do the following on the remote server:

   4a Clean up the database:

   ```
   # su - postgres -c psql
   postgres=# DROP DATABASE ncm;
   postgres=# DROP USER user;
   ```

   Replace *`user`* with the Cloud Manager database user. If you did not change the default, the user is `admin`.

   4b Edit `/var/lib/pgsql/data/postgresql.conf` to disable Cloud Manager Server access to the database. In the file, find the `listen_addresses = 'localhost'` entry and remove the Cloud Manager Server's IP address from the list of addresses.