Application Server Installation Guide

Cloud Manager 2.0

December 15, 2011

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.
1800 South Novell Place
Provo, UT 84606
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 5

1 Installing Cloud Manager Application Server Components 7

1.1 Installing to SLES 11 . . . 7
1.2 Installing to SLES 10 . . . 8

2 Using the Cloud Manager Application Server Configuration Tool 11

3 Configuring the PostgreSQL Database Connection and Credentials 13

4 Configuring Cloud Manager to Use Authentication Sources 17

4.1 Configuring Authentication to an LDAP Directory . . . 18
4.2 Configuring Authentication through an NCSS Director . . . 20
4.3 Configuring LDAP Plus NCSS Authentication . . . 21
4.3.1 LDAP Plus NCSS Authentication Concepts . . . 22
4.3.2 Configuring LDAP plus NCSS Authentication . . . 23
4.4 Configuring Authentication to Novell Access Manager . . . 25

5 Installing and Configuring Other Cloud Manager Feature Settings 27

5.1 Installing the Cloud Manager Application Console . . . 27
5.2 Configuring the Cloud Manager Web Server (Jetty) . . . 27
5.3 Configuring the Cloud Manager Web Server to Use SSL . . . 28
5.4 Configuring Cloud Manager SMTP Mail Settings . . . 29
5.5 Configuring Cloud Manager System Shell Login Information . . . 30

6 Configuring Secure Authentication Sources to Communicate with Cloud Manager 31

6.1 Configuring Novell Cloud Security Service Connectors for Cloud Manager . . . 31
6.1.1 Creating and Configuring an NCSS Connector for the Cloud Manager Application Console32
6.1.2 Creating and Configuring an NCSS Connector for the Cloud Manager API . . . 35
6.1.3 Creating and Configuring an NCSS Connector for the Cloud Manager Tasks API . . . 35
6.1.4 Creating and Configuring an NCSS Connector for the Cloud Manager App Services API35
6.2 Configuring Novell Access Manager to Work with Cloud Manager . . . 36
6.2.1 Managing a Reverse Proxy for Authentication to Cloud Manager . . . 36

7 What's Next? 43

A Optional Application Server Configuration Tasks 45

A.1 Configuring Cloud Manager to Support Server-Based Rebranding of Mobile Clients . . . 45
A.1.1 Configuring the Jetty.xml File . . . 45
A.1.2 Configuring the Context XML File . . . 46

About This Guide

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

- Chapter 1, "Installing Cloud Manager Application Server Components," on page 7
- Chapter 2, "Using the Cloud Manager Application Server Configuration Tool," on page 11
- Chapter 3, "Configuring the PostgreSQL Database Connection and Credentials," on page 13
- Chapter 4, "Configuring Cloud Manager to Use Authentication Sources," on page 17
- Chapter 5, "Installing and Configuring Other Cloud Manager Feature Settings," on page 27
- Chapter 6, "Configuring Secure Authentication Sources to Communicate with Cloud Manager," on page 31
- Chapter 7, "What's Next?," on page 43
- Appendix A, "Optional Application Server Configuration Tasks," on page 45

Audience

The information in this guide is intended for anyone who needs to install and configure NetIQ Cloud Manager software. This user should be an experienced Linux system administrator who has the following:

- Familiarity with and administrative rights to an authentication LDAP directory (Microsoft Active Directory or Novell eDirectory).
- A working knowledge of PostgreSQL databases.
- An understanding of security issues related to user authentication between services and SSL certificates.
- Experience in Linux and Windows system operation.
- Familiarity with virtual machine technology and data center operations.

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 (http://www.novell.com/documentation/feedback.html) and enter your comments there.

Additional Documentation

For other NetIQ Cloud Manager 2.0 documentation, see the NetIQ Cloud Manager 2.0 documentation Web site (http://www.novell.com/documentation/cloudmanager2/).

1 Installing Cloud Manager Application Server Components

NetIQ Cloud Manager, a WorkloadIQ product from NetIQ, transforms your virtual infrastructure into a true Cloud environment. Built to operate with your existing VMware, Microsoft Hyper-V, or Xen virtual hosts, Cloud Manager accelerates delivery of services through on-demand requesting of workloads and automated provisioning of the workloads.

This section includes information about installing the Cloud Manager RPMs to a server in your data center.

- Section 1.1, “Installing to SLES 11,” on page 7
- Section 1.2, “Installing to SLES 10,” on page 8

1.1 Installing to SLES 11

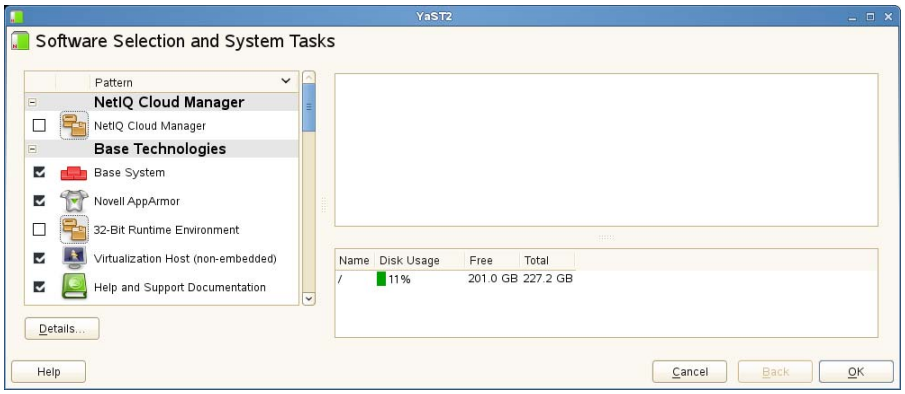
The RPMs in the Cloud Manager install patterns must be installed to a supported version of SUSE Linux Enterprise Server (SLES) 10 or 11. You should install the Application Server on a dedicated server for optimal performance. For more information about the installation requirements for Cloud Manager, see “Cloud Manager System Requirements” in the *NetIQ Cloud Manager 2.0 Installation Planning Guide*.

Some Cloud Manager RPMs have dependencies on SLES patterns that might not have been previously installed on the SLES server. For this reason, we recommend that you mount the SLES install media in a disk drive on the server while you install the Cloud Manager packages, either from another disk drive on the same server or from a downloaded ISO image.

1. Log in to the target SLES server as `root`, then open YaST.
2. From the NetIQ product downloads Web site, download the appropriate NetIQ Cloud Manager ISO to the SLES server.

   or

   Load the NetIQ Cloud Manager DVD on the SLES server.
3. Define the NetIQ 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 license agreement, then click *Next* to display the Software Selection and System Tasks dialog box.



5 Select the *NetIQ Cloud Manager* installation pattern.

6 Click *OK* to install the packages.

7 When package installation is complete, click *OK* to close the Installed Add-On Products dialog box.

1.2 Installing to SLES 10

1 Log in to the target SLES server as `root`, then open YaST.

2 Download the appropriate NetIQ Cloud Manager ISO to the SLES server.

or

Load the NetIQ Cloud Manager DVD on the SLES server.

3 Define the NetIQ Cloud Manager ISO or DVD as an add-on product:

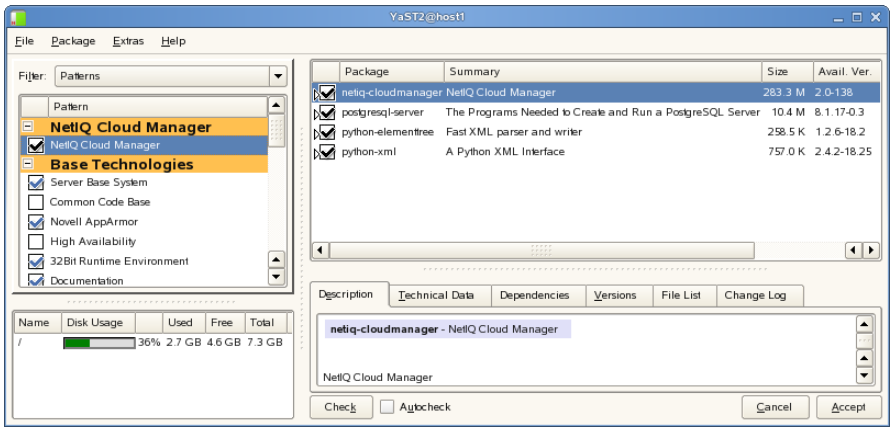
3a In the YaST Control Center, click *Software,* then click *Add-On Products*.

3b In the Add-on Product Media dialog box, do one of the following to select the ISO media (*Local Directory* or *DVD*) to install.

- (Conditional) Select *DVD*, click *Next*, insert the DVD, then click *Continue*.
- (Conditional) Select *DVD*, click *Next*, insert the DVD, then click *Continue*.

4 Read and accept the license agreement, then click *Next* to display YaST2.

5 In YaST2, click the *View* drop-down menu, then select *Patterns* to display the NetIQ Cloud Manager install patterns



6 Select the NetIQ Cloud Manager install pattern, then click *Accept* to install the packages.

2 Using the Cloud Manager Application Server Configuration Tool

After you have installed the NetIQ Cloud Manager Application components, you need to configure the system according to your data center environment architecture and your objectives for using the product. Cloud Manager provides a configuration tool to help you.

The Cloud Manager configuration tool is highly interactive, detecting your SUSE Linux Enterprise Server 11 SP1 operating system and its present configuration. It also detects the installation of the Cloud Manager Orchestration components on the server and gives you the opportunity to configure them by running a separate but related tool.

TIP: In a production environment, we recommend running the Orchestration configuration tool and the Cloud Manager Application configuration tool on different servers.

For more information about the Orchestration configuration tools, see "Configuring Cloud Manager Orchestration Components" in the *NetIQ Cloud Manager 2.0 Orchestration Installation Guide*.

The Cloud Manager Application Server configuration tool also gives you the option to install the product in a demonstration mode, building all of the components (including an embedded ApacheDS LDAP with default users already set up) that you need if you want to demonstrate or conceptualize product functionality. You should not use this "demo mode" if you have installed Cloud Manager in your production environment and you want to configure it there.

This section of the documentation does not discuss the concepts of the demo mode (how to run it or what to observe in it).

The configuration tool includes a script with several segments. Each segment prompts for information and then executes the configuration with the information you provide. The following chapters provide the detail about the segments of the script:

- Chapter 3, "Configuring the PostgreSQL Database Connection and Credentials," on page 13
- Chapter 4, "Configuring Cloud Manager to Use Authentication Sources," on page 17
- Chapter 5, "Installing and Configuring Other Cloud Manager Feature Settings," on page 27

3 Configuring the PostgreSQL Database Connection and Credentials

The NetIQ Cloud Manager installation pattern includes an optional `postgresql-server` package. This package can be installed with Cloud Manager on the local host by default. No matter when it is installed, however, a PostgreSQL ORDBMS is required for Cloud Manager. This product uses a dedicated database in Postgres to store all of its data.

This section helps you to prepare the information you need to configure the Postgres instance you use for Cloud Manager.

1 Make sure you know the information you are prompted to provide during the Postgres configuration:

Information Needed for Configuration	Description
Database server	You need to know the Postgres database server hostname or IP address. Unless you chose not to install the postgres package during the install, the Cloud Manager Application Server installs the packages in this pattern on the same server where you installed Cloud Manager. The default is `localhost`.

Information Needed for Configuration	Description
Autoconfigure an unconfigured Postgres installation?	If you install a Postgres ORDBMS intended for Cloud Manager but you have not yet configured it, Cloud Manager can autoconfigure it for your environment. Autoconfigure sets up the Postgres authentication method, changes the default postgres user password, and configures the database for local connections only. If you choose to autoconfigure, the tool sets up the environment and exits without displaying a summary of the settings it used. If you want to troubleshoot database problems, you can view the settings. Autoconfigure does the following: ◆ Generates a Postgres user password and copies it to `/etc/opt/netiq/cloudmanager/etc/pgusr.in`. ◆ Creates a database and names it `cloudmanager`. ◆ Creates a database user and names it `cmadmin`. ◆ Generates a database password for `cmadmin` and copies it to `/etc/opt/netiq/cloudmanager/etc/com.novell.ncm.backend.connpool.cfg` If you choose not to autoconfigure because your Postgres instance is already configured or because it is remotely located, the tool directs you to supply information for a new database configuration for Cloud Manager. **IMPORTANT**: Running autoconfigure on a Postgres instance that is already configured causes autoconfigure to fail.
Database server port	You need to know the port that your Postgres server uses for outside communication. The default is `5432`. **NOTE**: This documentation does not discuss the configuration for the Postgres server.

Information Needed for Configuration	Description
Create a new Postgres database? (You can choose to use an existing database instead of creating an new one.)	If you want to use Cloud Manager with a fresh database, you can choose to create that database. The configuration tool configures that database with data that you supply when prompted: ◆ **Administrator Name:** An administrative user with permission to create a database. ◆ **Database Administrator Password:** The password that the Administrator designated above uses to log in to the database. ◆ **Database Name:** An arbitrary name you specify to identify the database. The default is `cloudmanager`. ◆ **Database User Name:** A user to be created who must have read/write permissions to the database. The default is `cmadmin`. ◆ **Database User Password:** The password that the database user (designated above) uses to log in to the database.
Use an existing Postgres database	If you want to use an existing Postgres database, that database should not have been used prior for any other purpose. The configuration tool configures that database with authentication data that you supply when prompted: ◆ **Database Name:** An arbitrary name you specify to identify the database. The default is `cloudmanager`. ◆ **Database User Name:** A user to be created who must have read/write permissions to the database. ◆ **Database User Password:** The password that the database user (designated above) uses to log in to the database.

2 At the Cloud Manager Application Server, run the Cloud Manager Application configuration tool:

```
/opt/netiq/cloudmanager/configurator/config
```

The tool displays the first segment of its configuration script:

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

INSTALLATION OPTIONS MENU

Select products to configure

 #   selected  Item
 1)     no     NetIQ Cloud Manager - Server
 2)     no     NetIQ Cloud Manager - Manage Authentication
 3)     no     NetIQ Cloud Manager - Manage Certificates

Select from the following:
  1 - 3)  toggle selection status
       a)  all
       n)  none
       f)  finished making selections
       q)  quit -- exit the program
Selection [f]:
```

3 Specify `1` to configure the Cloud Manager Application Server, then enter `f` to finish the selection and move to the *PostgreSQL Database Connection* segment of the script.

```
POSTGRESQL DATABASE CONNECTION

This segment of the configuration utility lets you provide PostgreSQL
authentication information to be used by NetIQ Cloud Manager (NCM).

If you want to install Postgres to a local database and Postgres has not been
configured, you can choose to configure Postgres automatically.

If you choose to install to an existing Postgres server, you need the
following information:

    -  The Postgres server IP Address and the port where the service is running
    -  A username with permission to create the NCM database and user

       or

       The database name you want to populate, along with a username with write
       permission to that database.

Press <RETURN> to continue...
```

4 Follow the prompts to complete the Postgres configuration. Use the information you collected in Step 1 on page 13 as the script prompts you.

The configuration tool checks the database server and the database instance you specify, using the newly-defined credentials to make sure that the database instance and the database user can be created.

Following the Postgres configuration, continue with Chapter 4, “Configuring Cloud Manager to Use Authentication Sources,” on page 17 to configure the authentication sources you want to use with Cloud Manager.

4 Configuring Cloud Manager to Use Authentication Sources

The instructions in this section assume that you have already used the configuration tool to configure the Postgres database use by the NetIQ Cloud Manager Application Server, as described in Chapter 3, “Configuring the PostgreSQL Database Connection and Credentials,” on page 13.

The Net IQ Cloud Manager Application Server can connect to and search several different kinds of authentication sources to collect information about users in those sources. These are the users that can be authorized, depending on their individual roles, to log into Cloud Manager as Cloud Manager users.

The Cloud Manager Application Server configuration tool includes a segment that displays directly after the Postgres Configuration segment of the script, prompting you to choose an authentication source and asking for specific information that allows Cloud Manager connection to that source.

NOTE: If you configured authentication sources in a previous configuration session, you can manage those configuration settings in a new session. The tool provides a new option (`NetIQ Cloud Manager - Manage Authentication`) that you can select to make authentication configuration changes subsequent to your initial work.

This section discusses the authentication source options in Cloud Manager and how to obtain the data you provide for the tool. The section also includes an explanation of the setup you need to perform, if any, to prepare each of these authentication sources for connection to Cloud Manager.

- Section 4.1, “Configuring Authentication to an LDAP Directory,” on page 18
- Section 4.2, “Configuring Authentication through an NCSS Director,” on page 20
- Section 4.3, “Configuring LDAP Plus NCSS Authentication,” on page 21
- Section 4.4, “Configuring Authentication to Novell Access Manager,” on page 25

4.1 Configuring Authentication to an LDAP Directory

The NetIQ Cloud Manager administrator can choose to authenticate users through a supported Lightweight Directory Access Protocol (LDAP) directory service, either Microsoft Active Directory or Novell eDirectory. Cloud Manager users must have an account in the LDAP directory and must be members of the Cloud Manager user group. In addition, the LDAP user you specify as the read-only user must have All Attribute access to the area of the directory to be used by Cloud Manager.

You can also choose to add the Secure Sockets Layer (SSL) protocol to manage the security of authentication data being passed between Cloud Manager and LDAP. Adding SSL to the authentication process adds encryption and verification the process.

This section helps you to prepare the information you need to configure LDAP for Cloud Manager authentication. If you want to use another authentication service, see Section 4.2, "Configuring Authentication through an NCSS Director," on page 20, Section 4.3, "Configuring LDAP Plus NCSS Authentication," on page 21, or Section 4.4, "Configuring Authentication to Novell Access Manager," on page 25.

1 Make sure you know the information you are prompted to provide during the LDAP configuration:

Information Needed for LDAP Configuration	Description
Do you want to use SSL with LDAP?	If you respond with "yes" to this question, you are asked for an SSL certificate later in the configuration.
LDAP Source	You need to select the LDAP source for use with Cloud Manager, either Novell eDirectory or Microsoft Active Directory.
LDAP host address	This is the address (DNS name or IP address) of the LDAP host that Cloud Manager can connect to for authentication. If you chose to use SSL with LDAP, this address should match the subject of the certificate issued for the LDAP host. The configuration tool immediately validates this address when you specify it.
LDAP port	Designate the port where you want the LDAP server to listen for communication from Cloud Manager. If you are using SSL, the default port is 636. If you chose not to use SSL, the default port is 389.
Path to SSL certificate on LDAP server	This is the file system path to the SSL certificate you previously copied to the LDAP server. The certificate must be in DER format.[1] You need to use this setting only if you want to use SSL with the LDAP authentication.
LDAP read-only user DN	Specify the distinguished name (DN) of an existing LDAP read-only user who has read access to the LDAP directory. This user must have All Attribute read rights to the area of the directory that is to be used for Cloud Manager.

Information Needed for LDAP Configuration	Description
LDAP read-only user's password	Specify the password for the LDAP read-only user. When you specify the user password, the configuration tool immediately attempts an SSL authentication to validate the existence of this user and password.
Cloud Manager LDAP user DN	Specify the DN of an existing LDAP user whom you want to designate as the Cloud Manager administrator. When you specify this LDAP user, the configuration tool immediately attempts to locate the user in LDAP, then asks you to verify that this is the user you want to designate as the Cloud Manager administrator. Make sure that the `mail` attribute is set for this user in LDAP.
LDAP DN of NCM Users	Specify the DN of the LDAP container where the users whom you want to log in to Cloud Manager already exist. This is the parent context of users that will be allowed to log in to the Cloud Manager Application Console. All subdirectories and users are included by default. Make sure that all users, regardless of their context in this container, have their email domain configured prior to logging into the Application Console. **NOTE**: You can use the Cloud Manager Application Console later to import users who do not currently exist in this DN.

[1] Use the following command on a Linux machine to fetch the certificate and then copy it to another machine if needed.

```
echo 'GET / 1.0' | openssl s_client -connect <server_ip_addr_or_dns>:<port>|
sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' >ldap.pem
```

The following command converts the certificate to DER format (required by Cloud Manager):

```
openssl x509 -in ldap.pem -inform PEM -out ldap.cer -outform DER
```

2. Continue running the configuration tool (`/opt/netiq/cloudmanager/configurator/config`). In the configuration segment following the configuration of the Postgres database, the tool displays the following text:

```
Authentication Type

1) LDAP
2) NCSS
3) LDAP plus NCSS
4) NAM

Selection:
```

3. Specify `1` (LDAP) as the authentication type you want to configure.
4. Follow the prompts and use the information you gathered in Step 1 to complete this segment of the configuration.

After the LDAP authentication configuration, continue with Chapter 5, "Installing and Configuring Other Cloud Manager Feature Settings," on page 27.

4.2 Configuring Authentication through an NCSS Director

The NetIQ Cloud Manager administrator can choose to authenticate users logging in with their email addresses through a supported Novell Cloud Security Service (NCSS) server. NCSS should already be installed in your environment.

If you choose to let users authenticate through NCSS, you must also use the Secure Sockets Layer (SSL) protocol with it.

This section helps you to prepare the information you need to configure NCSS for Cloud Manager authentication. If you want to use some other authentication service, see Section 4.1, "Configuring Authentication to an LDAP Directory," on page 18, Section 4.3, "Configuring LDAP Plus NCSS Authentication," on page 21, or Section 4.4, "Configuring Authentication to Novell Access Manager," on page 25.

If you want to learn more about Novell Cloud Security Service, see the Novell Cloud Security Service 1.0 SP2 documentation Web site (http://www.novell.com/documentation/novellcloudsecurityservice/index.html).

1 Make sure you know the information you'll be prompted to provide during the NCSS authentication configuration:

Information Needed to Configure Authentication to NCSS Director	Description
DNS Address of the NCSS Director service	Specify the DNS name of the server that hosts the NCSS Director service. This address should match the address on the SSL certificate that was issued for the server.
Path to the SSL Certificate of the NCSS Director server	Specify the path in the file system where the SSL certificate resides. This certificate must be in DER format. If no SSL certificate exists, you can create one by visiting the NCSS Web page in your browser. You can use your browser tools to export the certificate. Remember that it must be in DER format. For more information, see *Retrieving the Public Certificate of the LDAP Server* (http://www.novell.com/documentation/novellcloudsecurityservice/install/data/bqc05g1.html) in the *Novell Cloud Security Service 1.0 SP2 Installation Guide*.
Cloud Manager Administrator user name	Specify the initial user name that you want to designate as the Cloud Manager administrator. This should be the new administrator's login name or Common Name (CN) and must already exist in your LDAP directory. This value is not validated during the configuration. You must be certain that you specify the value correctly so that users can log in through NCSS.
Cloud Manager Administrator email address	Specify the email address of the user you want to be the Cloud Manager administrator. This email address must already exist as an LDAP attribute of the future administrator. If the user has more than one email address, use the first address in the email attributes list. Cloud Manager uses this email address to determine the administrative permissions to apply to the user.

As you continue running the configuration tool (`/opt/netiq/cloudmanager/configurator/config`) following the configuration of the Postgres database, the tool displays the following text:

```
Authentication Type

1) LDAP
2) NCSS
3) LDAP plus NCSS
4) NAM

Selection:
```

2. Specify `2` (NCSS) as the authentication type you want to configure.
3. Follow the prompts and use the information you gathered in Step 1 to complete this segment of the configuration.

After the NCSS authentication configuration, continue with Chapter 5, "Installing and Configuring Other Cloud Manager Feature Settings," on page 27.

4.3 Configuring LDAP Plus NCSS Authentication

The NetIQ Cloud Manager administrator can choose to authenticate tenant customers through a supported Novell Cloud Security Service (NCSS) server that redirects the customers back to their own LDAP source for authentication credentials.

With this authentication option, Cloud Manager users of various roles store their credentials in the LDAP directory that you specify during configuration. For example, if you are a cloud service provider, you can set up your own enterprise LDAP structure for logging in to Cloud Manager, but your customers can use their own LDAP structures–preconfigured within NCSS–to authenticate to Cloud Manager.

This section helps you to prepare the information you need to configure LDAP plus NCSS for Cloud Manager authentication.

If you want to use another authentication service, see Section 4.1, "Configuring Authentication to an LDAP Directory," on page 18, Section 4.3, "Configuring LDAP Plus NCSS Authentication," on page 21, or Section 4.4, "Configuring Authentication to Novell Access Manager," on page 25.

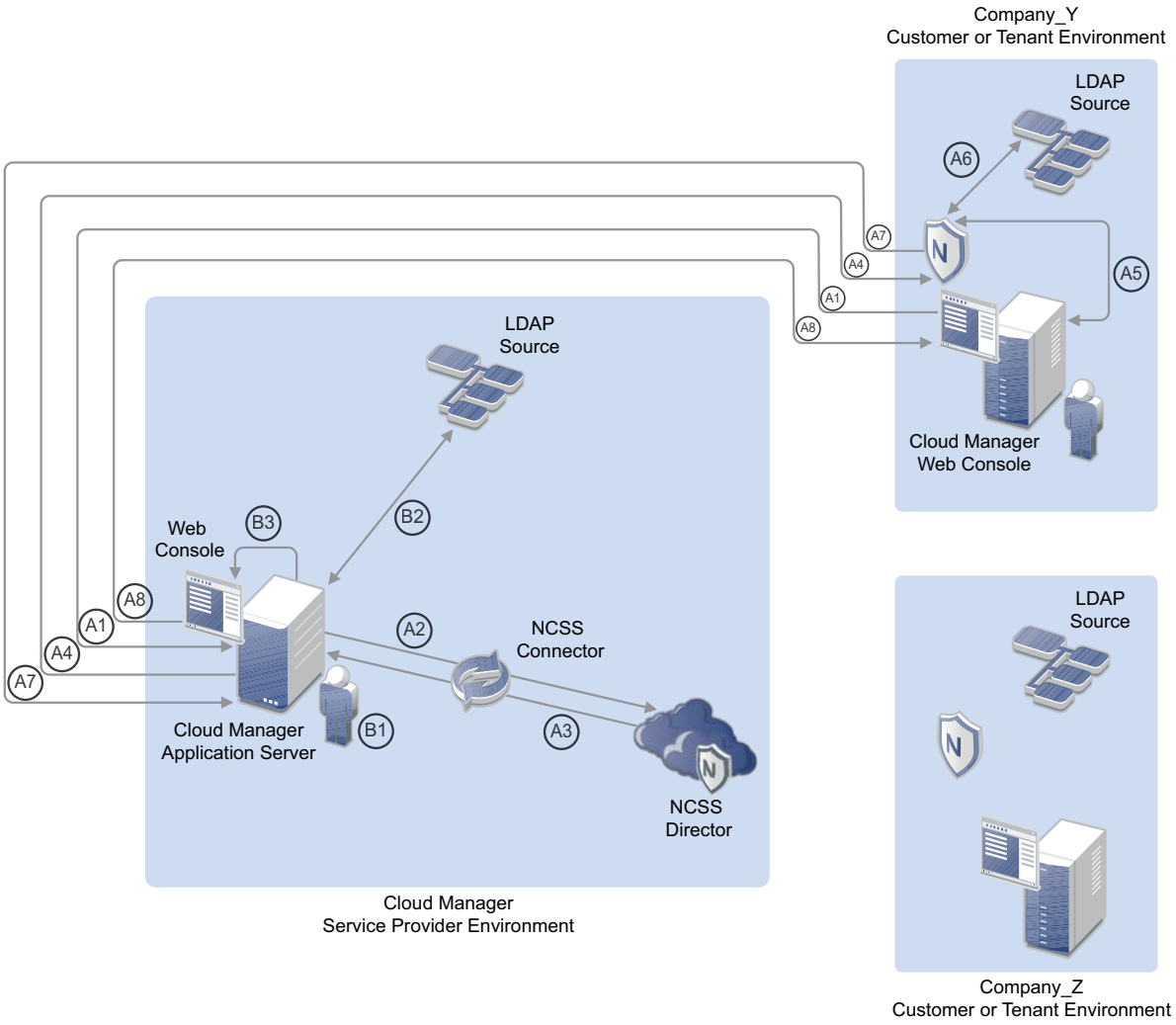
- Section 4.3.1, "LDAP Plus NCSS Authentication Concepts," on page 22
- Section 4.3.2, "Configuring LDAP plus NCSS Authentication," on page 23

If you want to learn more about Novell Cloud Security Service, see the Novell Cloud Security Service 1.0 SP2 documentation Web site (http://www.novell.com/documentation/novellcloudsecurityservice/index.html).

4.3.1 LDAP Plus NCSS Authentication Concepts

The following diagram illustrates the process of LDAP plus NCSS authentication from the perspective of the customer or "tenant" on the Cloud Manager Service Provider after you provide the required configuration information.

Figure 4-1 *LDAP Plus NCSS Authentication*



Customer or "Tenant" Authentication

Stage A1: Customer Steve at Company_Y has bought tenant rights in Jim's Cloud Manager Service Provider environment. Steve opens a Web browser and loads the URL to the Cloud Manager Application Console. Steve's Web browser opens the Cloud Manager Web portal, which connects to the Cloud Manager Application Server.

Stages A2, A3: The Application Server uses a preconfigured NCSS connector to communicate to the NCSS Director. The NCSS Director recognizes the login request and redirects that request back to the Cloud Manager Application Server.

Stage A4: The Application Server sends login requirements to NCSS components that were previously installed in the Company_Y environment and directs the Application Console to display open login fields.

Stage A5: NCSS components at Company_Y recognize that an LDAP login is required and establish a link to the Company_Y LDAP source. Steve at Company_Y sees the login field waiting for input on the Cloud Manager Application Console. He enters his username and password.

Stages A6, A7: NCSS components at Company_Y check the customer's LDAP source to validate Steve's login credentials. The NCSS components send the tested credentials back to the Cloud Manager Server, which validates them through the NCSS Director.

Stage A8: The Cloud Manager Server recognizes the privileges that Steve has, based on the context of the email address information listed in his LDAP Source. The Cloud Manager Server opens the relevant Web page for Steve in its Application Console.

Service Provider Administrator Authentication

Stage B1: Service Provider Jim is the Cloud Manager administrator. He wants to use NetIQ Cloud Manager to provide business services to his customers, including Steve at Company_Y, so he opens a Web browser and loads a special URL provided to him by the Cloud Manager Application Server.

Stage B2: Jim's Web browser opens the Cloud Manager Application Console, which is directly connected to the Cloud Manager Server. The Cloud Manager server recognizes the special URL as a Cloud Manager administrator login request, so it establishes a connection to Jim's LDAP source and directs its Application Console to display open login fields for a potential Cloud Manager Administrator.

Stage B3: Jim sees the login field waiting for input on the Cloud Manager Application Console, so he enters his username and password.

The Cloud Manager Server also recognizes the privileges that Jim has, based on the context of the email address information listed in his LDAP Source. The Cloud Manager Server opens the relevant Web page for Jim in its Application Console.

4.3.2 Configuring LDAP plus NCSS Authentication

1 Make sure you know the information you'll be prompted to provide during the LDAP plus NCSS authentication configuration:

Information Needed to Configure Authentication	Description
NCSS Director Configuration	
DNS Address of the NCSS Director service	Specify the DNS name of the server that hosts the NCSS Director service. This address should match the address on the SSL certificate that was issued for the server.

Information Needed to Configure Authentication	Description
Path to the SSL Certificate of the NCSS Director server	Specify the path in the file system where the SSL certificate resides. This certificate must be in DER format. If no SSL certificate exists, you can create one by visiting the NCSS Web page in your browser. You can use your browser tools to export the certificate. Remember that it must be in DER format.
LDAP Configuration	
Do you want to use SSL with LDAP?	If you respond with “yes” to this question, you are asked for an SSL certificate later in the configuration.
LDAP Source	You need to select the LDAP source for use with Cloud Manager, either Novell eDirectory or Microsoft Active Directory.
LDAP host address	This is the address (DNS name or IP address) of the LDAP host that Cloud Manager can connect to for authentication. If you chose to use SSL with LDAP, this address should match the subject of the certificate issued for the LDAP host. The configuration tool immediately validates this address when you specify it.
LDAP port	Designate the port where you want the LDAP server to listen for communication from Cloud Manager. If you are using SSL, the default port is 636. If you chose not to use SSL, the default port is 389.
Path to SSL certificate on LDAP server	This is the file system path to the SSL certificate you previously copied to the LDAP server. The certificate must be in DER format.
LDAP read-only user DN	Specify the distinguished name (DN) of an existing LDAP read-only user who has read access to the LDAP directory.
LDAP read-only user’s password	Specify the password for the LDAP read-only user. When you specify the user password, the configuration tool immediately attempts an SSL authentication to validate the existence of this user and password.
Cloud Manager LDAP user DN	Specify the DN of an existing LDAP user whom you want to designate as the Cloud Manager administrator. When you specify this LDAP user, the configuration tool immediately attempts to locate the user in LDAP, then asks you to verify that this is the user you want to designate as the Cloud Manager administrator. Make sure that the `mail` attribute is set for this user in LDAP.

Information Needed to Configure Authentication	Description
LDAP DN of NCM Users	Specify the DN of the LDAP container where the users whom you want to log in to Cloud Manager already exist. This is the parent context of users that will be allowed to log in to the Cloud Manager Application Console. All subdirectories and users are included by default. Make sure that all users, regardless of their context in this container, have an email domain configured prior to logging into the Application Console. **NOTE**: You can use the Cloud Manager Application Console later to import users who do not currently exist in this DN.

As you continue running the configuration tool (`/opt/netiq/cloudmanager/configurator/config`) following the configuration of the Postgres database, the tool displays the following text:

```
Authentication Type

1) LDAP
2) NCSS
3) LDAP plus NCSS
4) NAM

Selection:
```

2. Specify `3` (LDAP plus NCSS) as the Authentication Type you want to configure.
3. Follow the prompts and use the information you gathered in Step 1 to complete this segment of the configuration.

After the LDAP plus NCSS authentication configuration, continue with Chapter 5, "Installing and Configuring Other Cloud Manager Feature Settings," on page 27.

4.4 Configuring Authentication to Novell Access Manager

The NetIQ Cloud Manager administrator can choose to authenticate customers through Novell Access Manager (NAM).

This section helps you to prepare the information you need to configure Cloud Manager authentication through Novell Access Manager. If you want to use some other authentication service, see Section 4.1, "Configuring Authentication to an LDAP Directory," on page 18, Section 4.2, "Configuring Authentication through an NCSS Director," on page 20, or Section 4.3, "Configuring LDAP Plus NCSS Authentication," on page 21.

If you want to learn more about Novell Access Manager, see the Novell Access Manager 3.1 SP3 documentation Web site (http://www.novell.com/documentation/novellaccessmanager313/).

1. Make sure you know the information you are prompted to provide during the Access Manager authentication configuration:

Information Needed to Configure Authentication to NAM	Description
Cloud Manager Administrator user name	Specify the initial user name that you want to designate as the Cloud Manager administrator. This should be the new administrator's login name or Common Name (CN) and must already exist in your LDAP directory.
Cloud Manager Administrator email address	Specify the email address of the user you want to be the Cloud Manager administrator. This email address must already exist as an LDAP attribute of the future administrator. If the user has more than one email address, use the first address in the email attributes list. Cloud Manager uses this email address to determine the administrative permissions to apply to the user.

As you continue running the configuration tool (`/opt/netiq/cloudmanager/configurator/config`) following the configuration of the Postgres database, the tool displays the following text:

```
Authentication Type

1) LDAP
2) NCSS
3) LDAP plus NCSS
4) NAM

Selection:
```

2. Specify `4` (NAM) as the Authentication Type you want to configure.
3. Follow the prompts and use the information you gathered in Step 1 on page 25 to complete this segment of the configuration.

After the Novell Access Manager authentication configuration, continue with Chapter 5, "Installing and Configuring Other Cloud Manager Feature Settings," on page 27.

5 Installing and Configuring Other Cloud Manager Feature Settings

When you have completed configuring the NetIQ Cloud Manager Application Server to use your chosen configuration source, you must use the NetIQ Cloud Manager configuration tool to install or configure other Cloud Manager features that help you administer Cloud Manager.

- Section 5.1, “Installing the Cloud Manager Application Console,” on page 27
- Section 5.2, “Configuring the Cloud Manager Web Server (Jetty),” on page 27
- Section 5.3, “Configuring the Cloud Manager Web Server to Use SSL,” on page 28
- Section 5.4, “Configuring Cloud Manager SMTP Mail Settings,” on page 29
- Section 5.5, “Configuring Cloud Manager System Shell Login Information,” on page 30

5.1 Installing the Cloud Manager Application Console

The first feature that the configuration tool can install is the Cloud Manager Application Console. The console is a Web-based user interface that lets you manage your Cloud Manager system. The console’s display layout varies, depending on the role of the user who logs in. We recommend that you install this UI when prompted, unless you choose to create your own customer Web UI.

For more information, see the *NetIQ Cloud Manager 2 Cloud Administrator Guide*.

5.2 Configuring the Cloud Manager Web Server (Jetty)

The Cloud Manager configuration tool lets you decide whether to integrate SSL with the Cloud Manager Web server (Jetty). If you want you configure a secure connection between Cloud Manager Orchestration Server and the Cloud Manager Application Server, you need to answer “yes” to the following question:

```
Choose whether to configure the NetIQ Cloud Manager web server to use SSL.

Use SSL with Jetty? (yes/no):
```

If you choose to use SSL, ensure that you know the information are prompted to provide during the Jetty SSL configuration:

Information Needed to Configure SSL Use with Jetty	Description
Web Console HTTPS Port	Specify the secure port for the Cloud Manager Application Console. By default, this is port 8183, but you can specify any unused secure port.
Web Console HTTP Port	Specify the HTTP (non-secure) port for the Cloud Manager Application Console. If you chose to enable SSL for Jetty, Cloud Manager disables this port in `jetty.xml` for security purposes. You can re-enable the port by uncommenting the relevant section of the file.

5.3 Configuring the Cloud Manager Web Server to Use SSL

If you choose to use SSL with Cloud Manager's Jetty Web server, you need to provide Secure Socket Layer (SSL) information that the Cloud Manager Application Server can use to provide a secure connection.

When the configuration tool displays its SSL configuration segment, it immediately detects the existing DNS name of the server where you are performing the configuration. Because this DNS name must match the subject of the security certificate, you can change the DNS name to match the subject of an existing certificate.

The configuration tool lets you choose to use either a self-signed certificate generated by the server, or an existing certificate that you can import. The configuration is based on the details you provide after that initial determination:

```
Select 'yes' if you want to use an existing certificate for <detected
_dns_hostname>. If you select 'no', NetIQ Cloud Manager will use a self-signed
certificate.

Use existing certificate? (y/n):
```

Make sure you are prepared with the following information you are prompted to provide for configuring the Cloud Manager Web Server to use an imported SSL certificate:

Information Needed to Configure an Imported SSL Certificate	Description
Path to the Cloud Manager Server Certificate	Specify the path to an existing public certificate (in PEM format) that you want to import and use on this server. For example: `/home/jdoe/cloudmgr/newcert.pem` SSL is required if you want to use NCSS with Cloud Manager. If no SSL certificate exists, you can create one by using OpenSSL (http://www.novell.com/communities/node/4048/generating-edirectory-server-certificate-using-openssl-tool) or YaST (http://www.novell.com/documentation/sles11/book_security/data/sec_security_yast_ca_module.html). Use your browser tools to export the certificate.
Path to the Cloud Manager Server Private Key	Specify the path to the private key file of this server. This must be the private key file (in PEM format) that is provided by your trusted certificate authority. For example: `/home/jdoe/cloudmgr/newkey.pem`
Private Keystore Password	Specify the password you want to use for decrypting the private key file exclusively for Cloud Manager. If you don't want to use a password, press Enter when the tool prompts you with this question.

5.4 Configuring Cloud Manager SMTP Mail Settings

Cloud Manager uses SMTP messaging to send notifications about pending or completed system tasks and Business Service status. These notifications are sent from a system-like user account to a Cloud Manager user who receives a preconfigured message appropriate for his or her role and based on conditions or events occurring in the Cloud Manager system.

The Cloud Manager configuration tool lets you decide whether to configure mail settings for the system.

If you choose to use email in this way, you need to answer "yes" to the following question:

```
Configure the SMTP mail settings at this time? (yes/no):
```

If you choose to use e-mail, make sure you know the information you are prompted to provide during the email configuration segment of the configuration:

Information Needed to Configure SMTP Mail Settings	Description
Email Address of Message Source	Specify the email address from which all system notifications are to be sent. This should be a “no-reply” address because the message is automatically generated from the Cloud Manager system.
Cloud Manager SMTP Host	Specify the DNS name of the SMTP host you want to use with Cloud Manager, for example: `smtp.example.test`.
SMTP Port	Specify the port that the SMTP server is listening on. The default setting is port 25, but you can specify another port if you want to.

If your SMTP server requires authentication, you can configure SMTP later in the Cloud Manager Application Console.

5.5 Configuring Cloud Manager System Shell Login Information

As the system administrator, you have access to the inner workings of NetIQ Cloud Manager. You can access the system through an Apache Karaf shell or through the Karaf Web console (`http://<cloud_manager_server_address>:8181/system/console/bundles`). This segment of the configuration tool process lets you establish the login credentials for the Karaf system administrator.

The credentials you are prompted to provide for the system administrator configuration are independent of any other credentials for the Cloud Manager System.

Information Needed to Configure Authentication for the System Shell	Description
System User	Specify the initial user name that you want to designate as the Karaf system user.
System User’s Password	Specify the password of the system user. This doesn’t need to correlate to any directory password. It is stored in the `users.properties` file located in `/etc/opt/netiq/cloudmanager/etc`.

6 Configuring Secure Authentication Sources to Communicate with Cloud Manager

This section discusses configuring Novell Cloud Security Service (NCSS) and Novell Access Manager (NAM) as identity service tools that you can leverage to let your NetIQ Cloud Manager users securely log in to Cloud Manager.

- Section 6.1, "Configuring Novell Cloud Security Service Connectors for Cloud Manager," on page 31
- Section 6.2, "Configuring Novell Access Manager to Work with Cloud Manager," on page 36

6.1 Configuring Novell Cloud Security Service Connectors for Cloud Manager

Novell Cloud Security Service is a Web-based identity and access management gateway that acts as a trusted identity broker between your NetIQ Cloud Manager installation being used as a cloud service provider and the various LDAP infrastructures you might have in place to support and manage your customer's authentication.

Through NCSS Connectors that you configure, your customers can seamlessly become users of Cloud Manager and are enabled to use their accustomed credentials to log in to Cloud Manager with limited access to services specific to their organizations. NCSS and Cloud Manager work in unison to provide this multi-tenant environment where information is separated, secured, and protected. There are four NCSS connectors that you need to configure:

- Section 6.1.1, "Creating and Configuring an NCSS Connector for the Cloud Manager Application Console," on page 32
- Section 6.1.2, "Creating and Configuring an NCSS Connector for the Cloud Manager API," on page 35
- Section 6.1.3, "Creating and Configuring an NCSS Connector for the Cloud Manager Tasks API," on page 35
- Section 6.1.4, "Creating and Configuring an NCSS Connector for the Cloud Manager App Services API," on page 35

The content in this section is not intended as a comprehensive guide to NCSS. You should have already installed NCSS (http://www.novell.com/documentation/novellcloudsecurityservice/install/data/bq5t8g8.html) and you should be familiar with its capabilities so that you understand the context of this section. For more complete information about Novell Cloud Security Service, see the Cloud Security Service documentation Web site (http://www.novell.com/documentation/novellcloudsecurityservice/).

6.1.1 Creating and Configuring an NCSS Connector for the Cloud Manager Application Console

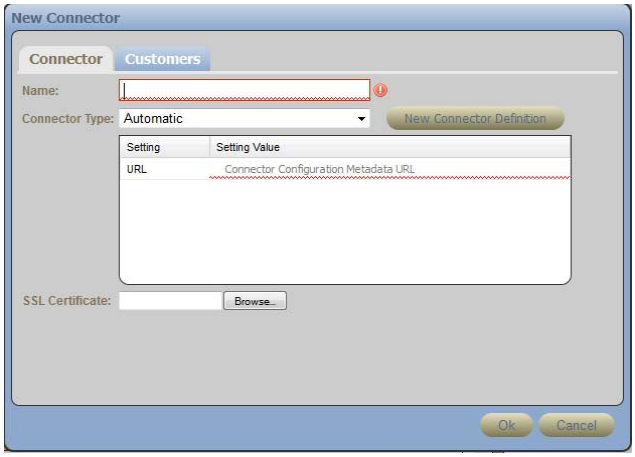
This section includes information about creating and configuring the NCSS connector for the Cloud Manager Application Console.

- "Adding a Connector for the Cloud Manager Application Console" on page 32
- "Adding Customers to the Cloud Manager Application Console Connector" on page 33
- "Configuring the Application Console Connector as a Customer" on page 34

Adding a Connector for the Cloud Manager Application Console

Use the steps in this section is to add a surface connector in NCSS that interacts with Cloud Manager Application Console user interface. Before you follow these steps to configure a connector, make sure that Cloud Manager is running and configured for an NCSS or an LDAP plus NCSS authentication.

1. Log in to the NCSS Provider Console and open the Home page. For more information about logging in to the console, see *"Logging in to the Provider Console"* (http://www.novell.com/documentation/novellcloudsecurityservice/provider/data/br69wb7.html) in the *Novell Cloud Security Service 1.0 SP2 Provider Administration Guide*.
2. In the Connector panel, click *New Connector Definition*.



3. In the *Name* field, specify a name for this connector, identifying it as a connector to the Cloud Manager Application Console.
4. In the *Connector Type* field, select *Automatic*.
5. In the *URL* field, specify the full DNS name of your Cloud Manager Application Server, followed by the SSL port number, followed by `/config`. For example:

   ```
   https://netiq-office.dnsdhcp.city.netiq.com:8183/config
   ```

6. In the *SSL Certificate* field, click *Browse*, then browse to and select the certificate you created for the Cloud Manager Application Server. This certificate must be in DER format for NCSS, so you might need to create another copy converted from PEM format.
7. Click *OK* to create the new connector.

   An error message similar to the following might be displayed:

```
Error Adding Connector, reason: ProxyException starting new Automatic connector
9c31b250-0ea6-4f88-98ac-9ab22f0df391; cause:
com.sun.jersey.api.client.ClientHandlerException:
javax.net.ssl.SSLHandshakeException: com.ibm.jsse2.util.g:
PKIX path building failed: java.security.cert.CertPathBuilderException: unable
to find valid certification path to requested target.
```

The error displays for several minutes in the NCSS console before the connector eventually starts (that is, its icon changes from red to green). You can ignore the message content.

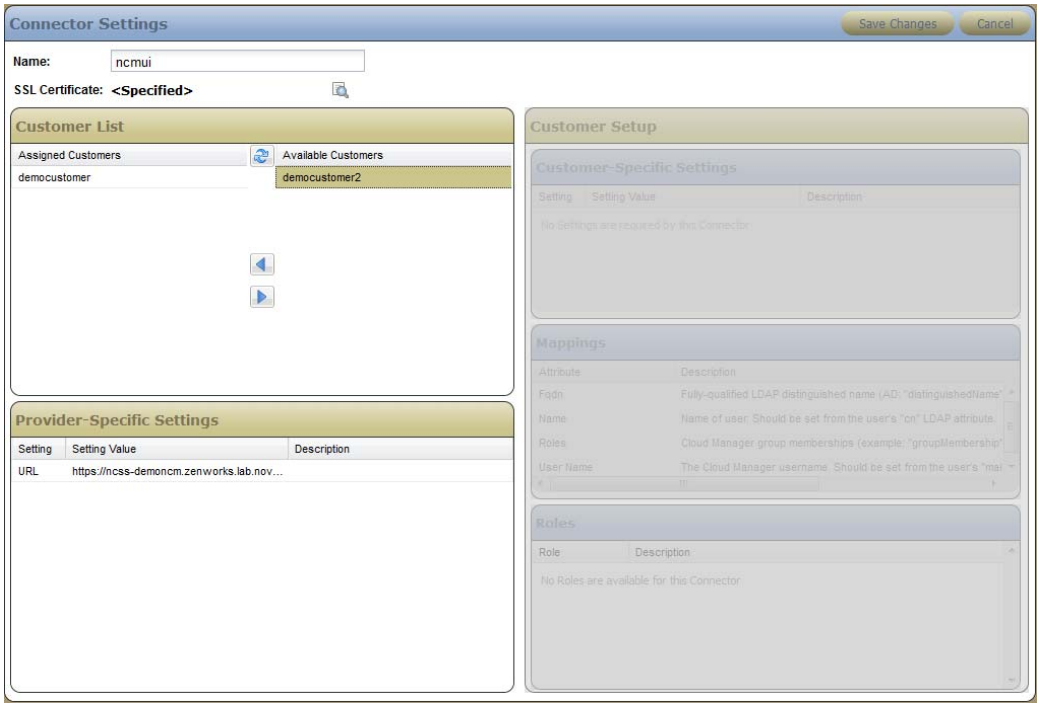
8 Continue with "Adding Customers to the Cloud Manager Application Console Connector" on page 33.

Adding Customers to the Cloud Manager Application Console Connector

After you have created the connector to the Cloud Manager Application Console, you need to establish which NCSS customers can access the Application Console.

1 On the *Home* page of the NCSS provider console, select the active (green) icon of the connector that you created in Adding a Connector for the Cloud Manager Application Console to display the Connectors page of the console.

2 On the *Connector Settings* panel of the *Connectors* page, click *Edit* to enable the edit mode for the *Customer List* subpanel.



3 Allow a customer access to the connector:

3a In the *Available Customers* list, select the customer.

3b Click the arrow icon to move the customer from the *Available Customers* list to the *Assigned Customers* list.

4 Click *Save Changes*.

5 Continue with "Configuring the Application Console Connector as a Customer" on page 34.

Configuring the Application Console Connector as a Customer

Cloud Manager requires that you map a customer's LDAP attributes to attributes defined within NCSS. This is necessary because eDirectory and Active Directory define their attributes in different ways. Without a common mapping, these divergent methods can cause problems for the Cloud Manager system. NCSS lets you map these attributes to a single, common set of definitions. This mapping is usually performed by the customer in the customer login view of NCSS, or you can do it as the NCSS provider administrator.

1. Log in to the NCSS console to open the Customers page. For more information, see *"Logging in to the Customer Console"* (http://www.novell.com/documentation/novellcloudsecurityservice/customer/data/br9x5xh.html) in the *Novell Cloud Security Service 1.0 SP2 Customer Administration Guide* or "*Logging in to the Provider Console*" (http://www.novell.com/documentation/novellcloudsecurityservice/provider/data/br69wb7.html) in the *Novell Cloud Security Service 1.0 SP2 Provider Administration Guide*.
2. (Conditional) If you log in to NCSS as a provider, you must select a customer in the *Customer List* panel of the Customers page. You must change the settings of the customer who will be logging in to the Cloud Manager Application Console.
3. In the *Connector List* panel of the Connectors page, make sure that the connector name of the Cloud Manager Application Console connector you created in Adding a Connector for the Cloud Manager Application Console is selected.
4. In the *Connector Settings* panel of the Connectors page, click *Edit*.
5. Map the attributes for the connector according to the LDAP source (eDirectory or Active Directory) you are using:
   - **5a** Click the *Required Mappings* tab to open the required mappings table.
   - **5b** Select the *Mapping Value* or *Type* column for each attribute. As you browse your LDAP source, consult the information in *Description* column to give you guidance, specify the values for each attribute, then click *Save*.
     - **FQDN:** Specify the fully-qualified LDAP distinguished name. In Active Directory, the value is the distinguishedName LDAP attribute. In eDirectory version 8.8.3 and later, the value is the entryDN LDAP attribute.
     - **Name:** Specify the name of this user. Obtain the value from the user's cn LDAP attribute.
     - **Roles:** Specify this user's group memberships in Cloud Manager. In eDirectory, this value is the groupMembership LDAP attribute. In Active Directory, this is the memberOf LDAP attribute.
     - **User Name:** Specify the Cloud Manager user name. Obtain the value from the user's mail attribute in his or her LDAP entry.
   - **5c** In the *Connector Settings* panel, click *Save Changes*.
6. Select *Security Services* from the toolbar to open the *Identity Brokers* panel, then click *Send Configuration* to send the mappings to the NCSS Secure Bridge.
7. Continue with Section 6.1.2, "Creating and Configuring an NCSS Connector for the Cloud Manager API," on page 35.

6.1.2 Creating and Configuring an NCSS Connector for the Cloud Manager API

To create and configure an NCSS connector for the Cloud Manager API, follow the steps in Section 6.1.1, "Creating and Configuring an NCSS Connector for the Cloud Manager Application Console," on page 32 that you used to create the connector (including its unique name), associating users to the connector, and configuring the connector as a customer.

The unique difference in creating a connector for the Cloud Manager API occurs in Step 5 of the procedure, when you specify the full DNS name of your Cloud Manager Application Server in the *URL* field. For the API connector, use this syntax:

```
https://<ncm_server_address>:<port_if_needed>/cloudmanager-api/config
```

An actual URL might look like this:

```
https://netiq-office.dnsdhcp.city.netiq.com:8183/cloudmanager-api/config
```

When you have completed this process, continue with Section 6.1.3, "Creating and Configuring an NCSS Connector for the Cloud Manager Tasks API," on page 35.

6.1.3 Creating and Configuring an NCSS Connector for the Cloud Manager Tasks API

To create and configure an NCSS connector for the Cloud Manager Tasks API, follow the steps in Section 6.1.1, "Creating and Configuring an NCSS Connector for the Cloud Manager Application Console," on page 32 that you used to create the connector (including its unique name), associating users to the connector, and configuring the connector as a customer.

The unique difference in creating a connector for the Cloud Manager Tasks API occurs in Step 5 of the procedure, when you specify the full DNS name of your Cloud Manager Application Server in the *URL* field. For the Tasks API connector, use this syntax:

```
https://<ncm_server_address>:<port_if_needed>/tasks-api/config
```

An actual URL might look like this:

```
https://netiq-office.dnsdhcp.city.netiq.com:8183/tasks-api/config
```

When you have completed this process, continue with Section 6.1.4, "Creating and Configuring an NCSS Connector for the Cloud Manager App Services API," on page 35.

6.1.4 Creating and Configuring an NCSS Connector for the Cloud Manager App Services API

To create and configure an NCSS connector for the Cloud Manager App Services API, follow the steps in Section 6.1.1, "Creating and Configuring an NCSS Connector for the Cloud Manager Application Console," on page 32 that you used to create the connector (including its unique name), associating users to the connector, and configuring the connector as a customer.

The unique difference in creating a connector for the Cloud Manager App Services API occurs in Step 5 of the procedure, when you specify the full DNS name of your Cloud Manager Application Server in the *URL* field. For the App Services API connector, use this syntax:

```
/app-services-api/config
```

So an actual URL might look like this:

```
https://netiq-office.dnsdhcp.city.netiq.com:8183/app-services-api/config
```

6.2 Configuring Novell Access Manager to Work with Cloud Manager

Novell Access Manager (NAM) provides secure, single sign-on access to trusted NetIQ Cloud Manager users from any location, in spite of the internal technical and organizational boundaries in your enterprise. Novell Access Manager supports multi-factor authentication, role-based access control, data encryption, and SSL VPN services.

The content in this section is not intended as a comprehensive guide to NAM. You should have already installed Novell Access Manager and a Novell Access Manager Access Gateway. You should also have installed NetIQ Cloud Manager, and the Cloud Manager Application Server should be running.

You need to be familiar with Novell Access Manager capabilities so that you understand the context of the content in this section. For more information about Novell Access Manager, see the Access Manager documentation Web site (http://www.novell.com/documentation/novellaccessmanager31/index.html).

- Section 6.2.1, "Managing a Reverse Proxy for Authentication to Cloud Manager," on page 36

6.2.1 Managing a Reverse Proxy for Authentication to Cloud Manager

A reverse proxy acts as the front end to the Cloud Manager Web Server on your Internet. The proxy off-loads frequent requests, thereby freeing up bandwidth. It also increases security because the IP addresses of your Web servers are hidden from the intranet.

You can use an existing reverse proxy and add a new proxy service for Cloud Manager or you can create a new reverse proxy with a service for Cloud Manager. You can configure the authentication settings of the reverse proxy according to the needs of your enterprise.

For information about creating a new reverse proxy, see *"Managing Reverse Proxies and Authentication"* (http://www.novell.com/documentation/novellaccessmanager31/accessgatewayhelp/data/reverselist.html) in the *Novell Access Manager 3.1 SP4 Configuration Guide*.

When the reverse proxy is set up as you want it, you need to perform the other configuration procedures necessary for Novell Access Manager authentication:

- "Creating and Configuring the Proxy Service for the Cloud Manager Reverse Proxy" on page 37
- "Adding and Protecting All Cloud Manager Resources" on page 37
- "Creating an Identity Injection Policy for the New Cloud Manager Protected Resource" on page 39
- "Adding and Configuring an HTML Rewriter Profile for the Proxy Service" on page 41

Creating and Configuring the Proxy Service for the Cloud Manager Reverse Proxy

You must create a unique proxy service for Cloud Manager. Configure the proxy service settings according to the needs of your enterprise.

The first proxy service of a reverse proxy is considered the master (or parent) proxy. Subsequent proxy services can use domain-based, path-based, or virtual multi-homing, relative to the published DNS name of the master proxy service. If you are creating a second proxy service to be used for Cloud Manager on the reverse proxy, see "*Using Multi-Homing to Access Multiple Resource"s (http://www.novell.com/documentation/novellaccessmanager31/accessgatewayhelp/data/b34l8ue.html)* in the *Novell Access Manager 3.1 SP4 Access Gateway Guide*.

Remember that for the *Web Server IP Address* setting of the proxy service, you need to specify the IP Address for the Cloud Manager Web server, and for the *Web Server Host Name* setting of the proxy service, you need to specify the DNS name of the Cloud Manager Web server.

When you have configured the proxy service according to your needs, you can continue with "Adding and Protecting All Cloud Manager Resources" on page 37.

Adding and Protecting All Cloud Manager Resources

A protected resource configuration specifies the directory (or directories) on the Cloud Manager Web server that you want to protect. The protected resource configuration specifies the authorization procedures and the policies that should be used to enforce protection.

You need to group all of the Cloud Manager resources that use the proxy service.

To create a resource that groups all of the Cloud Manager services:

1. Log in to the Access Manager Administration Console. For information about accessing the console, see *"Logging In to the Administration Console"* (http://www.novell.com/documentation/novellaccessmanager31/installation/data/b2euq6u.html) in the *Novell Access Manager 3.1 SP4 Installation Guide.*
2. In the console, select *Devices* > *Access Gateways* to open the Access Gateways page.
3. On the Access Gateways page, select *Edit* for the Gateway Server you want to edit. This displays the Access Gateway Server Configuration page.
4. On the Access Gateway Server Configuration page, select the name of the reverse proxy. This opens the Reverse Proxy configuration page.
5. On the Reverse Proxy page, select the proxy service you want to configure. This opens the Reverse Proxy Service page.
6. On the Reverse Proxy Service page, select the *Protected Resources* tab to open the Protected Resources page.

7 Configure the protected resource.:

7a On the Protected Resources page, select *New*, then specify a display name for the new resource you want to protect. For example, to create a resource that you want to use to represent all Cloud Manager resources, you could name the resource "everything."

When you create the display name, the Overview page for the new resource is displayed.

7b Fill in the fields to configure the resource:

- **Description:** Specify a description for the protected resource. You can use it to briefly describe the purpose for protecting this resource.
- **Authentication Procedure:** Select *Name/Password -Form* from the drop-down list. This specifies a form-based authentication over HTTP or HTTPS, using the Access Manager login form.
- **URL Path:** Select the default path, which is `/*`. This specifies everything on the Cloud Manager Web Server.

7c Click the *Protected Resources* breadcrumb at the top of the Overview page to return to the Protected Resources page.

7d On the Protected Resources page, make sure that the new protected resource is selected as *Enabled*.

8 Continue with "Creating an Identity Injection Policy for the New Cloud Manager Protected Resource" on page 39.

Creating an Identity Injection Policy for the New Cloud Manager Protected Resource

When the Cloud Manager protected resource is created, you need to associate it with an Access Manager identity injection policy to protect it. This policy specifies the information that must be injected into the HTTP header. Because Cloud Manager is configured to detect certain fields in the header, it can deny user authentication or redirect that user to an alternate Web page if it does not find the required information in the header.

1. Log in to the Access Manager Administration Console. For information about accessing the console, see *"Logging In to the Administration Console"* (http://www.novell.com/documentation/novellaccessmanager31/installation/data/b2euq6u.html) in the *Novell Access Manager 3.1 SP4 Installation Guide.*
2. In the Access Manager Administration Console, select *Devices* > *Access Gateways* to open the Access Gateways page.
3. On the Access Gateways page, select *Edit* for the Gateway Server you want to edit. This displays the Access Gateway Server Configuration page.
4. On the Access Gateway Server Configuration page, select the name of the reverse proxy. This opens the Reverse Proxy configuration page.
5. On the Reverse Proxy page, select the proxy service you want to configure. This opens the Reverse Proxy Service page.
6. On the Reverse Proxy Service page, select the *Protected Resources* tab to open the Protected Resources page.
7. On the Protected Resources page, select the display name of the Cloud Manager protected resource to open the properties views, then select *Identity Injection* to open the Identity Injection Policy List.
8. Select *Manage Policies* to open the Policies page.
9. Fill in the fields.
   - **Description:** (Optional) Describe the purpose of this policy. Because Identity Injection policies are customized to match the content of a specific Web server, include the name of the Cloud Manager Web server as part of the description.
   - **Priority:** Specify the order in which a rule is applied in the policy, when the policy has multiple rules. The highest priority is 1 and the lowest priority is 10.
10. In the actions panel of the page, select *New* > *Inject into Custom Header*.

    This inserts custom names with values into a custom header.
11. Configure five custom policy headers for Cloud Manager. You must configure the attributes of the custom headers as specified below. The headers must be created or moved into the order listed. You can use the *Copy Action* icon to copy each header, then you can modify the configurations as needed.

    11a Create the `X-TrustedUser` header, using the following information to populate the fields.:
    - **Custom Header Name:** Specify `X-TrustedUser`.
    - **Value:** Select *LDAP Attribute*. Selecting this option enables the LDAP attribute list box and the Refresh Data Rate list box. For this header, select *cn* as the LDAP attribute, then select *Session* as the refresh rate.
    - **Multi-Value Separator:** Select the semicolon (;) separator from the list box.
    - **DN Format:** Select the *LDAP* option from the list box.

11b Create the `X-TrustedRoles` header, using the following information to populate the fields:

- **Custom Header Name:** Specify `X-TrustedRoles`.
- **Value:** Select *LDAP Attribute*. Selecting this option enables the LDAP attribute list box and the Refresh Data Rate list box. For this header, select *groupMembership* as the LDAP attribute, then select *Session* as the refresh rate.

  NOTE: The *groupMembership* attribute applies if you are using eDirectory. If you are using Active Directory, the attribute is *memberOf*.
- **Multi-Value Separator:** Select the semicolon (;) separator from the list box.
- **DN Format:** Select the *LDAP* option from the list box.

11c Create the `X-TrustedUserFQDN` header, using the following information to populate the fields:

- **Custom Header Name:** Specify `X-TrustedUserFQDN`.
- **Value:** Select *Credential Profile*. Selecting this option enables the Credential Profile list box. For this header, select *LDAP Credentials: LDAP User DN* as the credential profile.
- **Multi-Value Separator:** Select the semicolon (;) separator from the list box.
- **DN Format:** Select the *LDAP* option from the list box.

11d Create the `X-TrustedUserDisplayName` header using the following information to populate the fields.

- **Custom Header Name:** Specify `X-TrustedUserDisplayName`.
- **Value:** Select *LDAP Attribute*. Making this selection enables the LDAP attribute list box and the Refresh Data Rate list box. For this header, select *displayName* as the LDAP attribute, then select *Session* as the refresh rate.
- **Multi-Value Separator:** Select the semicolon (;) separator from the list box.
- **DN Format:** Select the *LDAP* option from the list box.

11e Create the `X-TrustedUserEmail` header using the following information to populate the fields.

- **Custom Header Name:** Specify `X-TrustedUserEmail`.
- **Value:** Select *LDAP Attribute*. Making this selection enables the LDAP attribute list box and the Refresh Data Rate list box. For this header, select *mail* as the LDAP attribute, then select *Session* as the refresh rate.
- **Multi-Value Separator:** Select the semicolon (;) separator from the list box.
- **DN Format:** Select the *LDAP* option from the list box.

12 Click *OK* to save the new policy and display it on the Policies page.

13 On the Policies page, click *Enable* to enable this new policy for the protected resource.

14 Continue with "Adding and Configuring an HTML Rewriter Profile for the Proxy Service" on page 41.

NOTE: Make sure that you always update your configuration when you make changes in Novell Access Manager.

For more information, see *"Configuring an Identity Injection Policy"* (http://www.novell.com/documentation/novellaccessmanager31/policyhelp/data/editpolicyii.html) in the *Novell Access Manager 3.1 SP4 Policy Guide*.

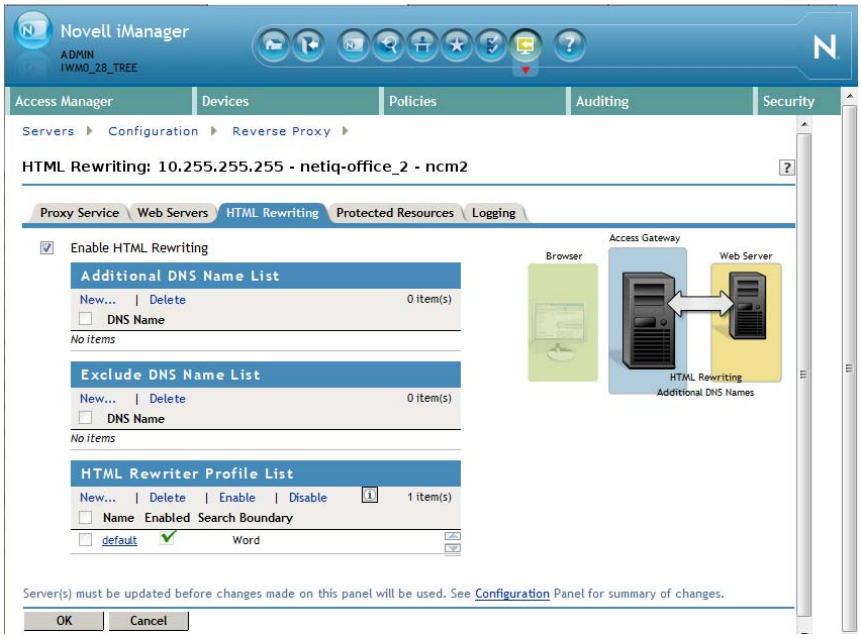
Adding and Configuring an HTML Rewriter Profile for the Proxy Service

The changes you make to the Novell Access Manager Access Gateway configurations for Cloud Manager require HTML rewriting because the Cloud Manager Web server is not aware that the Access Gateway machine is obfuscating its DNS names. URLs contained in its pages must be checked to ensure that these references contain the DNS names that the client browser understands. On the other end, the client browsers are not aware that the Access Gateway is obfuscating the DNS names of the resources they are accessing. The URL requests coming from the client browsers that use published DNS names must be rewritten to the DNS names that the Cloud Manager Web server expects.

The information in *"Understanding the Rewriting Process" (http://www.novell.com/documentation/novellaccessmanager31/accessgatewayhelp/data/b3nqotc.html#b3o4npk)* in the *Novell Access Manager 3.1 SP4 Access Gateway Guide* explains this process more fully.

You need to create and configure a new HTML Rewriter Profile for use with Cloud Manager.

1. Log in to the Access Manager Administration Console. For information about accessing the console, see *"Logging In to the Administration Console"* (http://www.novell.com/documentation/novellaccessmanager31/installation/data/b2euq6u.html) in the *Novell Access Manager 3.1 SP4 Installation Guide.*
2. In the Access Manager Administration Console, select *Devices* > *Access Gateways* to open the Access Gateways page.
3. On the Access Gateways page, select *Edit* for the Gateway Server you want to edit. This displays the Access Gateway Server Configuration page.
4. On the Access Gateway Server Configuration page, select the name of the reverse proxy. This opens the Reverse Proxy configuration page.
5. On the Reverse Proxy page, select the proxy service you want to configure. This opens the Reverse Proxy Service page.
6. On the Reverse Proxy Service page, select the *HTML Rewriting* tab to open the HTML rewriting page.



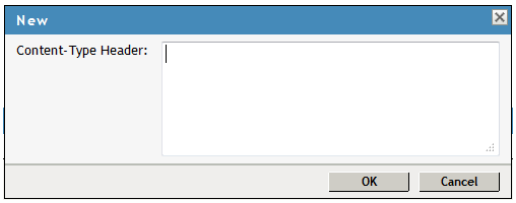
The HTML Rewriting page specifies which DNS names are to be rewritten. The HTML Rewriter Profile specifies which pages to search for DNS names that need to be rewritten.

7 Select *Enable HTML Rewriting*.

This option is enabled by default. When it is disabled, no rewriting occurs. When it is enabled, this option activates the internal HTML rewriter. When data is sent to the browsers, this rewriter replaces the name of the Cloud Manager Web server with the published DNS name. It replaces the published DNS name with the Web Server Host Name when sending data to the Cloud Manager Web server. It also ensures that the proper scheme (HTTP or HTTPS) is included in the URL. This is needed because you can configure the Access Gateway to use HTTPS between itself and client browsers and to use HTTP between itself and the Web servers.

8 Specify a name for the new profile, use the default search boundary, then click *OK* to open the HTML Rewriter configuration page.

9 In the *Content-Type Header* section of the page, click *New* to open a New dialog box.



10 In the dialog box, specify the new content-type header, which is `application/xml`, select the *Rewrite Inbound Headers* check box, then click *OK* to make sure that the new Content-Type Header is enabled for the protected resource.

7 What's Next?

When you complete installation and configuration of your NetIQ Cloud Manager system, as explained in this book, you are ready to start populating your system with the components that enable users to provision their own business services. For information, see the *NetIQ Cloud Manager 2 Cloud Administrator Guide*.

A Optional Application Server Configuration Tasks

This section includes the following information:

- Section A.1, "Configuring Cloud Manager to Support Server-Based Rebranding of Mobile Clients," on page 45

A.1 Configuring Cloud Manager to Support Server-Based Rebranding of Mobile Clients

In order to configure your NetIQ Cloud Manager 2.0 Application Server to support server-based rebranding of the Cloud Manager mobile iPhone and iPad clients, you must make some changes to server configuration.

There are two procedures you need to use to enable this feature:

- Section A.1.1, "Configuring the Jetty.xml File," on page 45
- Section A.1.2, "Configuring the Context XML File," on page 46

NOTE: The paths specified in these instructions have been tested with an RPM upgrade, so if you choose to use a different path, make sure it does not interfere with RPM upgrade.

A.1.1 Configuring the Jetty.xml File

Use these steps to configure `/opt/netiq/cloudmanager/deploy/jetty/etc/jetty.xml`:

1. At the NetIQ Cloud Manager Application Server, find the `ContextDeployer` section of the `jetty.xml` file.
2. Uncomment the entire section in the file that references the ContextDeployer.
3. Change the `configurationDir` definition in the `ContextDeployer` section to a path inside of the `/etc` directory, for example, `/etc/opt/netiq/cloudmanager/etc/webcontext`.
4. Change the `scanInterval` definition (measured in seconds) to the desired frequency.

   Specify `0` if you want to allow scanning after startup.

After you make these changes, the `jetty.xml` file might look like this:

```
<Call name="addLifeCycle">
    <Arg>
        <New class="org.mortbay.jetty.deployer.ContextDeployer">
            <Set name="contexts"><Ref id="Contexts"/></Set>
            <Set name="configurationDir">/etc/opt/netiq/cloudmanager/etc/
webcontext</Set>
            <Set name="scanInterval">0</Set>
        </New>
    </Arg>
</Call>
```

A.1.2 Configuring the Context XML File

1. At the NetIQ Cloud Manager Application Server, add a new file to the path specified in the `configurationDir` definition (that is, `/etc/opt/netiq/cloudmanager/etc/webcontext)` as referenced in Step 3 on page 45.

   Name the file `resources.xml`. The resulting file path is `/etc/opt/netiq/cloudmanager/etc/webcontext/resources.xml`.

2. Create the `resources.xml`file and save it with the following contents:

   ```
   <?xml version="1.0"?>
   <!DOCTYPE Configure PUBLIC "-//Mort Bay Consulting//DTD Configure//EN"
   "http://jetty.mortbay.org/configure.dtd">

   <Configure class="org.mortbay.jetty.handler.ContextHandler">
       <Set name="contextPath">/resources</Set>
       <Set name="resourceBase">/var/opt/netiq/cloudmanager/webres</Set>
       <Call name="addHandler">
           <Arg>
               <New class="org.mortbay.jetty.handler.ResourceHandler"/>
           </Arg>
       </Call>
   </Configure>
   ```

   - The `contextPath` defines the URL context for the client resources.
   - The `resourceBase` defines the file system path for the resource files you want to have available.

3. Create the directory `/var/opt/netiq/cloudmanager/webres`.
4. Create the directory `/var/opt/netiq/cloudmanager/webres/mobile`.
5. Copy your rebranded images to `/var/opt/netiq/cloudmanager/webres/mobile`.
6. Execute the following commands to ensure that the correct file permissions are set:

   ```
   chown root.root /var/opt/netiq/cloudmanager/webres -R
   chmod 644 /var/opt/netiq/cloudmanager/webres/* -R
   chmod 755 /var/opt/netiq/cloudmanager/webres
   chmod 755 /var/opt/netiq/cloudmanager/webres/mobile

   chown root.root /etc/opt/netiq/cloudmanager/etc/webcontext -R
   chmod 755 /etc/opt/netiq/cloudmanager/etc/webcontext
   chmod 644 /etc/opt/netiq/cloudmanager/etc/webcontext/* -R
   ```

7. Use the following command to restart services (making sure to clear the cache):

   ```
   /etc/init.d/netiq-cloudmanager reload
   ```

8. Ensure that your rebranded files are accessible through a Web browser. For example, you could access `login.png` by browsing to `https://<server>:8183/resources/mobile/login.png`.

TIP: If you reference files remotely or from a browser, you must reference them explicitly.

For example, if a file named `test.jpg` resides in the `webres/mobile` folder of your Application Server file system (`/var/opt/netiq/cloudmanager/webres/mobile/test.jpg`), you cannot access that file from a Web browser at home unless you provide an explicit Web address like this:

`https://<server>:8183/resources/mobile/test.jpg`