CHAPTER 5

Configuring Cisco DCNM Servers

This chapter describes how to configure Cisco Data Center Network Manager for LAN (DCNM-LAN) servers.

This chapter includes the following sections:

Configuring Secure Client Communications

This section describes how to configure Cisco Data Center Network Manager for LAN (DCNM-LAN) for secure client-server communications.

Note Use the HTTPs option for secured communication between the server and client.

This section includes the following topics:

Information About Secure Client Communications

This section includes the following topics:

Encrypted Client-Server Communications

By default, communication between the Cisco DCNM-LAN client and server is unencrypted; however, you can enable secure client-server communications, which uses Transport Layer Security (TLS), a protocol based on the Secure Sockets Layer (SSL) 3.0 protocol. In particular, communications between the Cisco DCNM-LAN client and the EJB port on the Cisco DCNM-LAN server are encrypted when you enable secure client communications.

Enabling secure client communications does not affect how users download, install, and log into the Cisco DCNM-LAN client.

Firewall Support for Client-Server Communications

Cisco DCNM-LAN supports client-server connections across gateway devices such as a firewall; however, you must configure any gateway devices to allow the connections that the client must open to the Cisco DCNM-LAN server.

By default, the secondary server bind port is assigned a random port number when the Cisco DCNM-LAN server starts. To support client-server communications across a gateway device, you must configure the Cisco DCNM-LAN server to use a specific port for the secondary server bind service.

Configuring Secure Client Communications for Cisco DCNM Release 6.2(5a) and Prior Releases

By default, Cisco DCNM Web Client uses HTTP. If you want to install SSL certificates and use Cisco DCNM Web Client over HTTPS (using TCP port 443 or another custom port), you need a certificate for each external IP address that accepts secure connections. You can purchase these certificates from a well-known Certificate Authority (CA).

To enable SSL, you must set up the keystore to use either a self-signed certificate or a certificate from a trusted third-party company such as VeriSign.

This section includes the following topics:

Creating a Local Certificate

Note This section is applicable to Cisco DCNM Release 6.2(5a) and prior releases only.

Step 1 Set up a keystore to use a self-signed certificate (local certificate). From the command line, enter the following command on windows:

```
%JAVA_HOME%/bin/keytool -genkey -alias tomcat -keyalg RSA -keystore "
C:\Program Files\Cisco
Systems\dcm\jboss-4.2.2.GA\server\fm\conf\fmserver.jks"
```

Step 2 Enter your name, organization, state, and country. Enter **change it** when prompted for a keystore password. If you prefer to use your own password, do not forget to change the keystorepass attribute in the server.xml file. When prompted for a key password, press **Enter** or use the same password as the keystore password.

Note You can now follow the steps in the next section for modifying DCNM Web Client to use SSL.

To obtain a certificate from the Certificate Authority of your choice, you must create a Certificate Signing Request (CSR). The CSR is used by the certificate authority to create a certificate that identifies your website as secure.

Creating a Certificate Request

Note This section is applicable to Cisco DCNM Release 6.2(5a) and prior releases only.

Step 1 Create a local certificate (as described in the previous section).

Note Note You must enter the domain of your website in the fields First and Last name in order to create a working certificate.

Step 2 Create the CSR with this command on windows:

```
keytool -certreq -keyalg RSA -alias tomcat -file certreq.csr -keystore
" C:\Program Files\Cisco
Systems\dcm\jboss-4.2.2.GA\server\fm\conf\fmserver.jks"
```

You must now have a file named certreq.csr. The file is encoded in PEM format. You can submit it to the certificate authority. You can find instructions for submitting the file on the Certificate Authority website.

Step 3 After you have your certificate, you can import it into your local keystore. You must first import a Chain Certificate or Root Certificate into your keystore. You can then import your certificate.

Step 4 Download a Chain Certificate from the Certificate Authority where you obtained the certificate:

- For Verisign.com commercial certificates, go to this URL:

  http://www.verisign.com/support/install/intermediate.html
- For Verisign.com trial certificates, go to this URL:

  http://www.verisign.com/support/verisign-intermediate-ca/Trial_Secure_Server_Root/index.html
- For Trustcenter.de, go to this URL:

  http://www.trustcenter.de/certservices/cacerts/en/en.htm#server
- For Thawte.com, go to this URL:

  http://www.thawte.com/certs/trustmap.html

Step 5 Import the Chain Certificate into your keystore by entering the following command

```
keytool -import -alias root -keystore " C:\Program Files\Cisco
Systems\dcm\jboss-4.2.2.GA\server\fm\conf\fmserver.jks" -trustcacerts
-file filename_of_the_chain_certificate"
```

Step 6 Import the new certificate in X509 format by entering the following command:

```
keytool -import -alias tomcat -keystore " C:\Program Files\Cisco
Systems\dcm\jboss-4.2.2.GA\server\fm\conf\fmserver.jks" -trustcacerts
-file your_certificate_filename"
```

Modifying Cisco DCNM Web Client to Use SSL

Note This section is applicable to Cisco DCNM Release 6.2(5a) and prior releases only.

Step 1 Stop Cisco DCNM Web Client if you have already launched it. If you have installed the Cisco DCNM Web Client on Windows, you can stop the service using Windows Services under Administrative Tools.

Step 2 Use a text editor to open \jboss-4.2.2.GA\server\fm\deploy\jboss-web.deployer\server.xml from the directory where DCNM Web Client is installed. You see the following lines in the beginning after some copyright information:

```
<Connector className="org.apache.catalina.connector.http.HttpConnector"
port="80" minProcessors="5" maxProcessors="75"
enableLookups="false" redirectPort="8443"
acceptCount="10" debug="0" connectionTimeout="60000"/>
<!-- Define an SSL HTTP/1.1 Connector on port 8443 -->
<!--
<Connector className="org.apache.catalina.connector.http.HttpConnector"
port="8443" minProcessors="5" maxProcessors="75"
enableLookups="true"
acceptCount="10" debug="0" scheme="https" secure="true">
<Factory className="org.apache.catalina.net.SSLServerSocketFactory"
clientAuth="false" protocol="TLS"/>
</Connector>
-->
```

Step 3 Comment the first <Connector> element and uncomment the second one. Note that the port changes from 8443 to 443 and keystore and keypass are added. Your file should look like the following example:

```
<!-- A HTTP/1.1 Connector on port 8080
<Connector port="80"
maxThreads="250" protocol="HTTP/1.1" strategy="ms" maxHttpHeaderSize="8192"
emptySessionPath="true"
server="Apache"
enableLookups="false" redirectPort="8443" acceptCount="100"
connectionTimeout="20000" disableUploadTimeout="true" allowTrace="false"/>

-->

<!-- Add this option to the connector to avoid problems with
.NET clients that don't implement HTTP/1.1 correctly
restrictedUserAgents="^.*MS Web Services Client Protocol 1.1.4322.*$"
-->
<!-- A AJP 1.3 Connector on port 9009 -->
```

```
<Connector port="9009"
emptySessionPath="true" enableLookups="false" redirectPort="8443"
protocol="AJP/1.3"/>

<!-- SSL/TLS Connector configuration using the admin devl guide keystore -->
<Connector port="443"
protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
emptySessionPath="true"
server="Apache"
scheme="https" secure="true" clientAuth="false" sslProtocol = "TLS"
securityDomain="java:/jaas/encrypt-keystore-password"
SSLImplementation="org.jboss.net.ssl.JBossImplementation" allowTrace="false"/>
```

Step 4 Save this file.

Step 5 Create a keyword password from the command line by navigating to C:\Program Files\Cisco Systems\dcm\fm\bin, entering Encrypter.bat ssl, and then entering fmserver_1_2_3 as the password.

Step 6 Restart Cisco DCNM Web Client.

Note Note If you restart Cisco DCNM-SAN Server with SSL enabled, you must restart Cisco DCNM Web Client. If you want to stop and restart Cisco DCNM-SAN Server with SSL disabled, you must restart Cisco DCNM Web Client.

Enabling Cisco DCNM-LAN SSL

Install Cisco DCNM on a single or clustered environment as described in the Cisco DCNM installation section.

Note This section is applicable to Cisco DCNM Release 6.2(5a) and prior releases only.

Note Ensure you launch the Cisco DCNM-LAN client atleast once before enabling SSL.

Step 1 From the server machine, copy the certification file .**dcnm/certs**.

Step 2 When HTTPS is not enabled, copy the fmtrust.jks file from the server machine under **<***dcnm-server-install-folder***>\dcm\jboss-4.2.2.GA\server\fm\conf** to the client machine under **.dcnm\certs** (located in user home) folder on the client machine. Once the file is copied, rename the file to **truststore**.

Step 3 When HTTPS is enabled, copy the fmserver.jks from the server machine under <*dcnm-server-install-folder*>**\dcm\jboss-4.2.2.GA\server\fm\conf** to the client machine under **.dcnm\certs** (located in user home) folder on the client machine. Once the file is copied, rename the file to **truststore.**

Step 4 When Cisco DCNM is installed on Microsoft Windows, locate the dcnm-wrapper.conf file under <*dcnm-server-install-folder*>**\dcm\dcnm\config**. You will need to do the following in the dcnm-wrapper.conf file. Replace

```
wrapper.java.additional.10="-Djavax.net.ssl.keyStore=../../jboss-4.2.2.GA/server/dcnm/conf
/cert/keystore" wrapper.java.additional.11="-Djavax.net.ssl.keyStorePassword=admin#1_2_3"
```

with

```
wrapper.java.additional.10="-Djavax.net.ssl.keyStore=../../jboss-4.2.2.GA/server/fm/conf/f
mserver.jks"wrapper.java.additional.11="-Djavax.net.ssl.keyStorePassword=fmserver_1_2_3"
```

Step 5 When Cisco DCNM is installed on Linux, locate the dcnm-run.sh file under <dcnm-server-install-folder>/dcm/ jboss-4.2.2.GA /bin. You will need to do the following in the dcnm-run.sh. Replace

```
JAVA_OPTS="-Djavax.net.ssl.keyStore=$JBOSS_HOME/server/dcnm/conf/cert/keystore
-Djavax.net.ssl.keyStorePassword=admin#1_2_3 $JAVA_OPTS"
```

with

```
JAVA_OPTS="-Djavax.net.ssl.keyStore=$JBOSS_HOME/server/fm/conf/fmserver.jks
-Djavax.net.ssl.keyStorePassword=fmserver_1_2_3 $JAVA_OPTS"
```

Enabling Encrypted Client-Server Communications

You can enable TLS to encrypt client-server communications.

If your Cisco DCNM-LAN deployment is a clustered-server deployment, you must perform this procedure on each server in the cluster.

Note This section is applicable to Cisco DCNM Release 6.2(5a) and prior releases only.

Step 1 Stop the Cisco DCNM-LAN server. If you are enabling secure client communications on a server cluster, use the stop-dcnm-cluster script. For single-server deployments, do one of the following:

- Microsoft Windows—Choose **Start > All Programs > Cisco DCNM Server > Stop DCNM Server**.
- RHEL—Use the Stop_DCNM_Server script.

For more information about stopping Cisco DCNM-LAN, see the *Cisco DCNM Fundamentals Guide, Release 6.x*.

Step 2 In a text editor, open the jboss-service.xml file that is at the following location:

INSTALL_DIR\dcm\jboss-4.2.2.GA\server\dcnm\deploy\ejb3.deployer\META-INF\jboss-service.xml

where *INSTALL_DIR* is the Cisco DCNM installation directory. On Microsoft Windows, the default installation directory is C:\Program Files\Cisco Systems. On RHEL systems, the default installation directory is /usr/local/cisco.

Step 3 Find the following section in the file. Verify that the section you find matches the following lines exactly.

```
<!--mbean code="org.jboss.remoting.transport.Connector"
name="jboss.remoting:type=Connector,transport=SslEjb3Connector,handler=ejb3">
  <depends>jboss.aop:service=AspectDeployer</depends>
  <attribute
name="InvokerLocator">sslsocket://${jboss.bind.address}:${cisco.dcnm.remoting.sslejbport:3
843}</attribute>
  <attribute name="Configuration">
    <handlers>
```

```
      <handler
subsystem="AOP">org.jboss.aspects.remoting.AOPRemotingInvocationHandler</handler>
    </handlers>
  </attribute>
</mbean-->
```

The section is commented out using the standard XML comment markers, <!-- and -->.

Step 4 Uncomment the section as follows:

a. From the first line of the section, remove the following three characters from before mbean:

```
!--
```

The changed line should read as follows:

```
<mbean code="org.jboss.remoting.transport.Connector"
name="jboss.remoting:type=Connector,transport=SslEjb3Connector,handler=ejb3">
```

b. From the last line of the section, remove the following two characters after mbean:

```
--
```

The changed line should read as follows:

```
</mbean>
```

Step 5 Find the following section in the file. Verify that the section you find matches the following lines exactly.

```
<mbean code="org.jboss.remoting.transport.Connector"
name="jboss.remoting:type=Connector,name=DefaultEjb3Connector,handler=ejb3">
        <depends>jboss.aop:service=AspectDeployer</depends>
        <attribute
name="InvokerLocator">socket://${jboss.bind.address}:${cisco.dcnm.remoting.ejbport:3873}</
attribute>
        <attribute name="Configuration">
            <handlers>
                <handler
subsystem="AOP">org.jboss.aspects.remoting.AOPRemotingInvocationHandler</handler>
            </handlers>
        </attribute>
    </mbea
```

The section is not commented. Use the standard XML comment marker to comment.

Step 6 Use the standard XML comment markers to comment out the section, as follows:

a. In the first line of the section, add the following three characters from before mbean:

```
!--
```

The changed line should read as follows:

```
<!--mbean code="org.jboss.remoting.transport.Connector"
name="jboss.remoting:type=Connector,transport=SslEjb3Connector,handler=ejb3">
```

b. In the last line of the section, add the following two characters after mbean:

```
--
```

The changed line should read as follows:

```
</mbean-->
```

Step 7 Save and close the jboss-service.xml file.

Step 8 In a text editor, open the jboss-service.xml file that is at the following location:

INSTALL_DIR\dcm\jboss-4.2.2.GA\server\dcnm\conf\jboss-service.xml

Note This is a different jboss-service.xml file than you opened in Step 2.

Step 9 Find the following section in the file.

```
cisco.dcnm.remoting.transport=socket
cisco.dcnm.remoting.port=3873
cisco.dcnm.remoting.ejbport=3873
cisco.dcnm.remoting.sslejbport=3843
cisco.dcnm.remoting.client.invokerDestructionDelay=0
```

The port numbers at the end of the last three lines may vary from this example, depending upon whether the default port numbers were changed during the Cisco DCNM-LAN server installation.

Step 10 Change the cisco.dcnm.remoting.transport value to sslsocket. The changed line should read as follows:

```
cisco.dcnm.remoting.transport=sslsocket
```

Step 11 Change the cisco.dcnm.remoting.port value to match the value specified for cisco.dcnm.remoting.sslejbport. For example, if the Cisco DCNM-LAN server is configured to use the default SSL port, the cisco.dcnm.remoting.sslejbport value is 3843 and the changed line would read as follows:

```
cisco.dcnm.remoting.port=3843
```

Step 12 Change the cisco.dcnm.remoting.client.invokerDestructionDelay value to 30000. The changed line should read as follows:

```
cisco.dcnm.remoting.client.invokerDestructionDelay=30000
```

Step 13 Save and close the jboss-service.xml file.

Step 14 Do one of the following:

- If your Cisco DCNM-LAN deployment is a clustered-server deployment, repeat this procedure on each server in the cluster and then start the servers, beginning with the master server first. Allow at least one minute between starting each server.
- If your deployment is a single-server deployment, start the Cisco DCNM-LAN server.

For more information about starting a single Cisco DCNM-LAN or a cluster of Cisco DCNM-LAN servers, see the *Cisco DCNM Fundamentals Guide, Release 6.x*.

Disabling Encrypted Client-Server Communications

You can disable secure client communications.

If your Cisco DCNM-LAN deployment is a clustered-server deployment, you must perform the following steps on each server in the cluster.

Note This section is applicable to Cisco DCNM Release 6.2(5a) and prior releases only.

Step 1 Stop the Cisco DCNM-LAN server. If you are disabling secure client communications on a server cluster, use the stop-dcnm-cluster script. For single-server deployments, do one of the following:

- Microsoft Windows—Choose **Start > All Programs > Cisco DCNM Server > Stop DCNM Server**.

- RHEL—Use the Stop_DCNM_Server script.

For more information about stopping Cisco DCNM-LAN, see the *Cisco DCNM Fundamentals Guide, Release 6.x*.

Step 2 In a text editor, open the jboss-service.xml file that is at the following location:

INSTALL_DIR\dcm\jboss-4.2.2.GA\server\dcnm\deploy\ejb3.deployer\META-INF\jboss-service.xml

where *INSTALL_DIR* is the Cisco DCNM installation directory. On Microsoft Windows, the default installation directory is C:\Program Files\Cisco Systems. On RHEL systems, the default installation directory is /usr/local/cisco.

Step 3 Find the following section in the file. Verify that the section you find matches the following lines exactly.

```
<mbean code="org.jboss.remoting.transport.Connector"
name="jboss.remoting:type=Connector,transport=SslEjb3Connector,handler=ejb3">
  <depends>jboss.aop:service=AspectDeployer</depends>
  <attribute
name="InvokerLocator">sslsocket://${jboss.bind.address}:${cisco.dcnm.remoting.sslejbport:3
843}</attribute>
  <attribute name="Configuration">
    <handlers>
      <handler
subsystem="AOP">org.jboss.aspects.remoting.AOPRemotingInvocationHandler</handler>
    </handlers>
  </attribute>
</mbean>
```

The section is commented out using the standard XML comment markers.

Step 4 Use the standard XML comment markers to comment out the section, as follows:

a. To the first line of the section, add the following three characters before mbean:

```
!--
```

The changed line should read as follows:

```
<!--mbean code="org.jboss.remoting.transport.Connector"
name="jboss.remoting:type=Connector,transport=SslEjb3Connector,handler=ejb3">
```

b. To the last line of the section, add the following two characters after mbean:

```
--
```

The changed line should read as follows:

```
</mbean-->
```

Step 5 Find the following section in the file. Verify that the section you find matches the following lines exactly.

```
<mbean code="org.jboss.remoting.transport.Connector"
name="jboss.remoting:type=Connector,name=DefaultEjb3Connector,handler=ejb3">
        <depends>jboss.aop:service=AspectDeployer</depends>
        <attribute
name="InvokerLocator">socket://${jboss.bind.address}:${cisco.dcnm.remoting.ejbport:3873}</
attribute>
        <attribute name="Configuration">
            <handlers>
                <handler
subsystem="AOP">org.jboss.aspects.remoting.AOPRemotingInvocationHandler</handler>
            </handlers>
        </attribute>
    </mbean>
```

The section is not commented out using the standard XML comment markers.

Step 6 Use the standard XML comment markers to comment out the section, as follows:

a. In the first line of the section, add the following three characters from before mbean:

```
!--
```

The changed line should read as follows:

```
<!--mbean code="org.jboss.remoting.transport.Connector"
name="jboss.remoting:type=Connector,transport=SslEjb3Connector,handler=ejb3">
```

b. In the last line of the section, add the following two characters after mbean:

```
--
```

The changed line should read as follows:

```
</mbean-->
```

Step 7 Save and close the jboss-service.xml file.

Step 8 In a text editor, open the jboss-service.xml file that is at the following location:

INSTALL_DIR\dcm\jboss-4.2.2.GA\server\dcnm\conf\jboss-service.xml

Note This is a different jboss-service.xml file than you opened in Step 2.

Step 9 Find the following section in the file.

```
cisco.dcnm.remoting.transport=sslsocket
cisco.dcnm.remoting.port=3843
cisco.dcnm.remoting.ejbport=3873
cisco.dcnm.remoting.sslejbport=3843
cisco.dcnm.remoting.client.invokerDestructionDelay=30000
```

The port numbers at the end of the last three lines may vary from this example, depending upon whether the default port numbers were changed during Cisco DCNM-LAN server installation.

Step 10 Change the cisco.dcnm.remoting.transport value to socket. The changed line should read as follows:

```
cisco.dcnm.remoting.transport=socket
```

Step 11 Change the cisco.dcnm.remoting.port value to match the value specified for cisco.dcnm.remoting.ejbport. For example, if the Cisco DCNM-LAN server is configured to use the default EJB port, the cisco.dcnm.remoting.ejbport value is 3873 and the changed line would read as follows:

```
cisco.dcnm.remoting.port=3873
```

Step 12 Change the cisco.dcnm.remoting.client.invokerDestructionDelay value to 0. The changed line should read as follows:

```
cisco.dcnm.remoting.client.invokerDestructionDelay=0
```

Step 13 Save and close the jboss-service.xml file.

Step 14 Do one of the following:

- If your Cisco DCNM-LAN deployment is a clustered-server deployment, repeat this procedure on each server in the cluster and then start the servers, beginning with the master server first. Allow at least one minute between starting each server.
- If your deployment is a single-server deployment, start the Cisco DCNM-LAN server.

For more information about starting a single Cisco DCNM-LAN or a cluster of Cisco DCNM-LAN servers, see the *Cisco DCNM Fundamentals Guide, Release 6.x*.

Specifying a Secondary Server Bind Port

You can configure a Cisco DCNM-LAN server to use a specific secondary server bind port.

If your Cisco DCNM-LAN deployment is a clustered-server deployment, you must perform this procedure on each server in the cluster.

Note This section is applicable to Cisco DCNM Release 6.2(5a) and prior releases only.

DETAILED STEPS

Step 1 Stop the Cisco DCNM-LAN server. If you are enabling secure client communications on a server cluster, use the stop-dcnm-cluster script. For single-server deployments, do one of the following:

- Microsoft Windows—Choose **Start > All Programs > Cisco DCNM Server > Stop DCNM Server**.
- RHEL—Use the Stop_DCNM_Server script.

For more information about stopping Cisco DCNM-LAN, see the *Cisco DCNM Fundamentals Guide, Release 6.x*.

Step 2 In a text editor, open the remoting-bisocket-service.xml file that is at the following location:

INSTALL_DIR\dcm\jboss-4.2.2.GA\server\dcnm\deploy\jboss-messaging.sar\remoting-bisocket-service.xml

where *INSTALL_DIR* is the Cisco DCNM installation directory. On Microsoft Windows, the default installation directory is C:\Program Files\Cisco Systems. On RHEL systems, the default installation directory is /usr/local/cisco.

Step 3 Find the following section in the file. Verify that the section you find includes the secondaryBindPort line.

```
<!-- Use these parameters to specify values for binding and connecting control connections
to work with your firewall/NAT configuration
<attribute name="secondaryBindPort">48227</attribute>
<attribute name="secondaryConnectPort">48227</attribute>
-->
```

By default, the section is commented out using the standard XML comment markers, <!-- and -->.

If you have previously specified a secondary server bind port, the section is not commented out.

Step 4 If the section is commented out, uncomment the secondaryBindPort line, as follows:

a. At the end of the second line of the section, add the following three characters from after configuration:

```
-->
```

The changed line should read as follows:

```
to work with your firewall/NAT configuration-->
```

b. At the beginning of the fourth line of the section, add the following four characters:

```
<!--
```

The changed line should read as follows:

```
<!-- <attribute name="secondaryConnectPort">abc</attribute>
```

After you uncomment the section, it should read as follows:

```
<!-- Use these parameters to specify values for binding and connecting control connections
to work with your firewall/NAT configuration-->
<attribute name="secondaryBindPort">48227</attribute>
<!--<attribute name="secondaryConnectPort">48227</attribute>
-->
```

Step 5 In the secondaryConnectPort line, specify a port number between the opening and closing attribute elements. For example, if you want to specify port 47900, the secondaryBindPort line should read as follows:

```
<attribute name="secondaryBindPort">47900</attribute>
```

Step 6 Save and close the remoting-bisocket-service.xml file.

Step 7 Do one of the following:

- If your Cisco DCNM-LAN deployment is a clustered-server deployment, repeat this procedure on each server in the cluster and then start the servers, beginning with the master server first. Allow at least one minute between starting each server.
- If your deployment is a single-server deployment, start the Cisco DCNM-LAN server.

For more information about starting a single Cisco DCNM-LAN or a cluster of Cisco DCNM-LAN servers, see the *Cisco DCNM Fundamentals Guide, Release 6.x*.

Configuring Secure Client Communications for Cisco DCNM Release 6.3(1) and Further Releases

This section includes the following topics:

Adding a CA signed SSL Certificate in DCNM

Step 1 From command prompt, navigate to **<DCNM install root>/dcm/java/jre1.7/bin/**

Step 2 Generate the public-private key pair in DCNM keystore

```
keytool -genkeypair -alias <alias-name> -keyalg RSA -keystore
"<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuratio
n\fmserver.jks" -storepass fmserver_1_2_3e\configuration\fmserver.jks"
-storepass fmserver_1_2_3
```

For Example: `keytool -genkeypair -alias mykey -keyalg RSA  -keystore "D:\CiscoSystems\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmser ver.jks" -storepass fmserver_1_2_3`

Step 3 Generate the certificate signing request (CSR) from the public key generated in step 1.

```
keytool -certreq -alias <alias-name-from-Step-1> -file <csr-file-name>
-keystore "<DCNM install
root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks"
-storepass fmserver_1_2_3
```

For Example: `keytool -certreq -alias mykey -file certreq.pem -keystore "D:\CiscoSystems\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks" -storepass fmserver_1_2_3`

Step 4 Submit the CSR to certificate signing authority to digitally sign it and download the certificate along with the root intermediate (if applicable).

Step 5 Import the intermediate certificate first, then the root certificate, and finally the signed certificate by following these steps:

- `keytool -importcert -alias <unique-alias-name> -file <intermediate cert file location> -keystore "<DCNM install root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks" -storepass fmserver_1_2_3`
- `keytool -importcert -alias <unique-alias-name> -file <root cert file location> -keystore "<DCNM install root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks" -storepass fmserver_1_2_3`
- `keytool -importcert -alias  <alias-name-from-Step-1> -file <CA signed cert file location> -keystore "<DCNM install root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks" -storepass fmserver_1_2_3`

For Example:

- `keytool -importcert -alias inter -file inter.pem -keystore "D:\Cisco Systems\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks" -storepass fmserver_1_2_3`
- `keytool -importcert -alias root -file root.pem -keystore "D:\Cisco Systems\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks" -storepass fmserver_1_2_3`
- `keytool -importcert -alias mykey -file mykey.pem -keystore "D:\Cisco Systems\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks" -storepass fmserver_1_2_3`

Step 6 Stop the DCNM services.

Step 7 Open the following files:

- <Install root>/dcm/JBoss- 7.2.0.Final/standalone/configuration/standalone-san.xml
- <Install root>/dcm/JBoss- 7.2.0.Final/standalone/configuration/ standalone-lan.xml

Step 8 Search for **key-alias="sme"** and replace with **key-alias="<key-alias in the Step 1 above>"**

Step 9 Restart the DCNM Services.

Note You must configure the Cisco DCNM Web Port again, after adding a ca signed SSL certificate.

Enabling SSL/HTTPS on Cisco DCNM

Note This section is not applicable from Cisco DCNM Release 6.3(1).

To enable SSL/HTTPS on a OVA setup perform the following:

Step 1 Launch SSH to logon to the server using root user credentials.

Step 2 Stop the DCNM application by using the **appmgr stop dcnm** command.

You can check the status by using the **appmgr status dcnm** command.

Step 3 Update the DCNM by using the **appmgr update dcnm -h true**.

You can check the status by using the **appmgr status all** command.

Step 4 Start the applications in the server by using the **appmgr start dcnm** command.

You must be to logon to the Web Client, SAN Client and the LAN Client using **https://<server-name>//**.

To enable SSL/HTTPS on a RHEL or WINDOWS setup, choose HTTPS upfront, select to run in the HTTPs mode while you execute the installer.

Note To enable CA signed, refer to Adding a CA signed SSL Certificate in DCNM, page 5-12.

Configuring SMTP Servers

This section describes how to configure Cisco Data Center Network Manager for LAN (DCNM-LAN) servers to use SMTP servers.

This section includes the following topics:

Information About SMTP Servers

The Cisco DCNM-LAN client supports a feature where you can specify rising or falling threshold rules for sample variables in collected statistical data. When one of these thresholds has been crossed, you can specify that an e-mail alert be sent. The Cisco DCNM-LAN server can be configured to send e-mail to an SMTP server.

Configuring for SMTP Servers for Cisco DCNM Release 6.2(5a) and Prior Releases

Cisco DCNM-LAN servers are configured to use SMTP servers by setting a property value.

DETAILED STEPS

Step 1 Stop the Cisco DCNM-LAN server. If you are enabling SMTP communications on a server cluster, use the stop-dcnm-cluster script. For single-server deployments, do one of the following:

- Microsoft Windows—Choose **Start > All Programs > Cisco DCNM Server > Stop DCNM Server**.
- RHEL—Use the Stop_DCNM_Server script.

For more information about stopping Cisco DCNM-LAN, see the *Cisco DCNM Fundamentals Guide, Release 6.x*.

Step 2 In a text editor, open the mail-service.xml file at the following location:

INSTALL_DIR\dcm\jboss-4.2.2.GA\server\dcnm\deploy\mail-service.xml

where *INSTALL_DIR* is the Cisco DCNM installation directory. On Microsoft Windows, the default installation directory is C:\Program Files\Cisco Systems. On RHEL systems, the default installation directory is /usr/local/cisco.

Step 3 Find the mail.smtp.host property value and modify it to specify the SMTP gateway server.

For example:

```
<!-- Specify the SMTP gateway server -->
<property name="mail.smtp.host" value="smtp.nosuchhost.nosuchdomain.com"/
```

Step 4 Save and close the mail-service.xml file.

Step 5 Do one of the following:

- If your Cisco DCNM-LAN deployment is a clustered-server deployment, repeat this procedure on each server in the cluster and then start the servers, beginning with the master server first. Allow at least one minute between starting each server.
- If your deployment is a single-server deployment, start the Cisco DCNM-LAN server.

For more information about starting a single Cisco DCNM-LAN or a cluster of Cisco DCNM-LAN servers, see the *Cisco DCNM Fundamentals Guide, Release 6.x*.

Configuring for SMTP Servers for Cisco DCNM Release 6.3(1) and Further Releases

Perform the following steps to configure SMTP server for JBOSS 7.

Step 1 Enter the SMTP server details should be provided in the server configuration file.

Step 2 Edit the DCNM LAN Server Configuration file **$(DCNM_INSTALl_FOLDER)\jboss-as-7.2.0.Final\standalone\configuration\standalone-lan.xml**

Step 3 Navigate to the section of the file:

```
<subsystem xmlns="urn:jboss:domain:mail:1.1">
            <mail-session jndi-name="java:jboss/mail/Default">
                <smtp-server outbound-socket-binding-ref="mail-smtp"/>
            </mail-session>
</subsystem>
```

Step 4 Add the SMTP user related details and thereby change the default configuration as shown below.

```
<subsystem xmlns="urn:jboss:domain:mail:1.1">
<mail-session jndi-name="java:jboss/mail/Default" from="user@domain.com">
                  <smtp-server outbound-socket-binding-ref="mail-smtp"/>
                </mail-session>
</subsystem>
```

Step 5 Search for the socket definition **mail-smtp** and edit the SMTP server details as shown below.

```
<outbound-socket-binding name="mail-smtp">
    <remote-destination host="SERVERIP" port="25"/>
</outbound-socket-binding>
```

Step 6 Provide the appropriate SMTP host (FQN)/IP address.

Step 7 Restart the server.