Oracle® Communications Offline Mediation Controller

System Administrator's Guide

Release 12.0

E91424-01

December 2017

ORACLE®

Oracle Communications Offline Mediation Controller System Administrator's Guide, Release 12.0

E91424-01

Contents

2 Managing Offline Mediation Controller Security

3 Managing Nodes Using NMShell Command-Line Components

4 Backing Up and Restoring Offline Mediation Controller

5 Troubleshooting Offline Mediation Controller

Preface

This guide provides instructions for administrating Oracle Communications Offline Mediation Controller.

Audience

This guide is intended for system administrators, database administrators, and developers who maintain and manage Offline Mediation Controller.

This guide assumes that you:

- Have a working knowledge of the UNIX operating system
- Understand your network configuration and the equipment from which Offline Mediation Controller collects data

Downloading Oracle Communications Documentation

Product documentation is available from Oracle Help Center:

http://docs.oracle.com

Additional Oracle Communications documentation is available from the Oracle software delivery Web site:

https://edelivery.oracle.com

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

1

Configuring Offline Mediation Controller

This chapter explains how to start, stop, and monitor Oracle Communications Offline Mediation Controller components.

Configuring the offline_mediation.conf File

To start, stop, and monitor the Offline Mediation Controller components using the **ProcessControl** script, define the components that are running, the installation they run from, and the ports and IP addresses they use in the **offline_mediation.conf** file. The **ProcessControl** script uses the information in the **offline_mediation.conf** file to start, stop, and monitor multiple servers from multiple Offline Mediation Controller installations.

To configure the **offline_mediation.conf** file:

1. Open the *OMC_home*/**offline_mediation/offline_mediation.conf** file in a text editor, where *OMC_home* is the directory in which Offline Mediation Controller is installed.
2. Specify the Offline Mediation Controller components to start or stop using the following syntax:

   ```
   daemon_name:OMC_home:port:[IP_Address]:{Y|N}
   ```

   where:

   - *daemon_name* is the name for the Offline Mediation Controller component:
     - **admnsvr** (Administration Server)
     - **nodemgr** (Node Manager)
   - *port* is the port on which the server component runs. The port number range is between **49152** and **65535**.
   - *IP_Address* is the IP address for the host computer to start, stop, and monitor multiple servers from multiple Offline Mediation Controller installations.
   - *Y/N* indicates whether this component is started when the system starts or not.

   For example:

   ```
   admnsvr:/OMC_home:55105::Y
   nodemgr:/OMC_home:55109::Y
   ```

3. Save and close the file.

Starting and Stopping Offline Mediation Controller

You can start and stop Offline Mediation Controller by using the following methods:

- The **ProcessControl** script. See "Starting and Stopping Offline Mediation Controller by Using the ProcessControl Script."
- The individual component commands. See:
  - Starting and Stopping Node Manager
  - Starting and Stopping Administration Server

Starting and Stopping Offline Mediation Controller by Using the ProcessControl Script

You can start or stop Offline Mediation Controller by using the **ProcessControl** script. This script preserves the node status when you restart Node Manager.

Important: Before running the **ProcessControl** script, ensure that you have run the **configure** script. For more information, see the discussion about adding Offline Mediation Controller service to system startup in *Offline Mediation Controller Installation Guide*.

To start and stop Offline Mediation Controller by using the **ProcessControl** script:

1. Go to the *OMC_home***/bin** directory.
2. Run the following command, which starts the Offline Mediation Controller components that are defined in the **offline_mediation.conf** file on the appropriate ports:

   ```
   ./ProcessControl start
   ```

3. Run the following command, which stops the Offline Mediation Controller components that are defined in the **offline_mediation.conf** file:

   ```
   ./ProcessControl stop
   ```

Starting and Stopping Node Manager

To start and stop Node Manager:

1. Go to the *OMC_home***/bin** directory.
2. Run the following command, which starts Node Manager:

   ./nodemgr [**-d** | **-f** | **-F** | **-j**] [**-p** *port*] [**-i** *IP_Address*]

   where:

   - **-d** runs Node Manager in the background with debug output redirected to *OMC_home***/log/nodemgr**_*port***.out**.

     This option uses a large amount of the CPU during its processes.
   - **-f** runs Node Manager in the foreground.
   - **-F** runs Node Manager in the foreground with debug output.
   - **-j** runs Node Manager, with the just-in-time (JIT) compiler enabled, in the background with debug output redirected to *OMC_home***/log/nodemgr**_*port***.out**.

- **-p** *port* runs Node Manager on *port*.
- **-i** *IP_Address* specifies the IP address of the host computer on which Node Manager is installed. Use this parameter to start Node Manager installed on multiple computers.

If you run this command with no options, Node Manager starts in the background with no debug output.

3. Run one of the following commands, which stops Node Manager:
   - To shut down Node Manager:

     ```
     ./nodemgr -s [-p port]
     ```

   - To stop the Node Manager process:

     ```
     ./nodemgr -k [-p port]
     ```

Starting and Stopping Administration Server

To start and stop Administration Server:

1. Go to the *OMC_home***/bin** directory.
2. Run the following command, which starts Administration Server:

   ```
   ./adminsvr [-d | -f | -F | -j] [-x][-p port][-i IP_Address]
   ```

   where:
   - **-d** runs Administration Server in the background with debug output redirected to *OMC_home***/log/adminsvr**_*port***.out**.
   - **-f** runs Administration Server in the foreground.
   - **-F** runs Administration Server in the foreground with debug output.
   - **-j** runs Administration Server, with the JIT compiler enabled, in the background with debug output redirected to *OMC_home***/log/adminsvr**_*port***.out**.
   - **-x** disables user authentication.
   - **-p** *port* runs Administration Server on *port*.
   - **-i** *IP_Address* specifies the IP address to be used. It is used for multi-home systems.

   If you run this command with no options, Administration Server starts in the background with no debug output.
3. Run one of the following commands, which stops Administration Server:
   - To shut down Administration Server:

     ```
     ./adminsvr -s [-p port]
     ```

   - To stop the Administration Server process:

     ```
     ./adminsvr -k [-p port]
     ```

Starting Administration Client

To start Administration Client:

1. Go to the *OMC_home*/**bin** directory.
2. Run the following command:

   ```
   ./gui [-d | -f | -F]
   ```

   where:

   - **-d** runs Administration Client in the background with debug output redirected to *OMC_home*/**log/gui**_*port*.**out**.
   - **-f** runs Administration Client in the foreground.
   - **-F** runs Administration Client in the foreground with debug output.

   If you run this command with no options, Administration Client starts in the background with no debug options.

Changing the IP Address of a Mediation Host

You cannot change the IP address of a mediation host. Instead, you must remove the mediation host using that IP address, and reassign the IP address in the the **offline_mediation.conf** file.

To change the IP address of a mediation host:

1. Write down the port number on which Offline Mediation Controller is connected.
2. In the Admin Client, delete the mediation host running on the Offline Mediation Controller workstation. To do so:
   1. Delete nodes from the node chain from left to right; otherwise, the dependence of one node on the previous node may prevent you from removing it.
   2. Delete the mediation host.
3. Stop all Offline Mediation Controller related processes on the workstation.
4. For UNIX machines, modify the /etc/hosts file with the new IP addresses and reboot the workstations. Restart the Offline Mediation Controller processes.
5. Look in the directory *OMC_Home*/offline_mediation for the **offline_mediation.conf** file and replace any occurrences of the old IP address with the new IP address, where *OMC_Home* is the directory in which you installed Offline Mediation Controller. Entering an IP address is optional in this file, so if the field has no value, you can leave it as is.
6. When you log in to the Administration Client, enter the new IP address of the workstation on which the adminsvr will be running.
7. In the Admin Client, add a mediation host for each workstation.
8. Restart the adminsvr and nodemgr processes on the workstation.
9. Restart all nodes on the workstation.
10. Ensure the file SystemModel.cfg in the Administration Server config directory *OMC_Home*/config/adminserver have the new IP addresses and the correct port number.

11. Ensure the files dataflowmap.cfg and nmPort in the Node Manager config directory *OMC_Home*/config/nodemgr have the new IP addresses and the correct port number.

    Note: *OMC_Home* is the directory in which you installed Offline Mediation Controller.

12. Should this fail, stop all nodes, stop all processes (Client, adminsvr, nodemgr) and manually change all the config files that have not been changed to the new IP addresses in the config directories.
13. Restart the adminsvr and nodemgr processes on the primary workstation (nodemgr only on the backup workstation).
14. Restart all the nodes on the primary workstation (for backup workstations, restart the CC node only).

Running the ProcessControl Script to Monitor Offline Mediation Controller Components

You can use the **ProcessControl** script to monitor Offline Mediation Controller components to ensure they are still running and to restart the server.

To run the **ProcessControl** script to monitor Offline Mediation Controller components:

1. Stop all Offline Mediation Controller components.
2. Open the **/etc/inittab** file in a text editor.
3. Add the following entry:

   ```
   NT:3:respawn:/etc/init.d/ProcessControl monitor
   ```

4. Save and close the file.
5. Run the following command, which periodically monitors the status of the Offline Mediation Controller components that are defined in the **offline_mediation.conf** file:

   ```
   ./ProcessControl monitor
   ```

Modifying Attribute Names Displayed in Record Editor

By default, Record Editor uses the name **Network Accounting Record** for each NAR in your system. This means that each NAR will be displayed as **Network Accounting Record** in the left pane of the Record Editor window. When you expand a NAR, the NAR attribute names are listed.

To modify the attribute name:

1. Open the *OMC_home***/datadict/Data_Dictionary.xml** file in a text editor, where *OMC_home* is the directory in which Offline Mediation Controller is installed.
2. Search for the attribute ID.
3. Change the **<Attr>** element to **<Attr tagForName="true">**.

   The **tagForName** option overrides the default attribute name.

4. Set the **<Name>** element to the attribute name you want to display in Record Editor.

   Note: If you leave the **<Name>** element blank, Record Editor displays the attribute ID as the attribute name.

5. Save the file.
6. Restart Record Editor.

Setting System Monitoring Options

This section explains the system-monitoring options for the *OMC_home*/**config/nodemgr/nodemgr.cfg** file. If you do not modify the **nodemgr.cfg** file, Offline Mediation Controller uses the default threshold values.

You can modify **nodemgr.cfg** to manage your threshold options to monitor disk, memory, and CPU usage levels. You can set a warning threshold and an error threshold for these areas. You must decide what action to take if the thresholds are crossed.

- To monitor disk errors, see "Using the Disk Status Monitor".
- To monitor memory errors, see "Using the Memory Monitor".
- To monitor CPU usage levels, see "Using the CPU Usage Monitor".

By default, Offline Mediation Controller generates a single alarm for each error condition, even if the error condition occurs multiple times. To generate an alarm or trap for every error occurrence, open the **nodemgr.cfg** file and change the SUPPRESS_MULTIPLE_ALARMS parameter value to **No**.

Using the Disk Status Monitor

You use the disk status monitor to alert you to potential disk issues, so you can take action to avoid unrecoverable errors.

Note: The disk status monitor runs only on Solaris workstations that have the Sun Solstice DiskSuite **metastat** command installed.

Table 1–1 lists the parameters you can add or modify in the **nodemgr.cfg** file.

Table 1–1 Disk Status Monitor Parameters

Parameter	Description
DISK_STATUS_CMD	The full path to the **metastat** command. The default is **/usr/sbin/metastat**.
DISK_STATUS_POLLTIME	Amount of time to wait between polling intervals.

Using the Memory Monitor

You use the memory monitor to alert you when memory usage exceeds a specified threshold. In addition to the threshold, you can configure the memory monitor to log memory usage statistics.

Table 1–2 lists the parameters you can add or modify in the **nodemgr.cfg** file.

Table 1–2 Memory Monitor Parameters

Parameter	Description
LOG_MEMORY_USAGE	Set to **Y** to log memory usage statistics. The default is **N**.
MEMORY_MAJOR_ THRESHOLD	The level at which a major alarm is raised, as a percentage. The default is **85**.
MEMORY_WARNING_ THRESHOLD	The level at which a warning alarm is raised, as a percentage. The default is **70**.
MEMORY_SAMPLE_TIME	A time interval, in seconds, during which the memory usage must be above a specific threshold level before an alarm is raised. The default is **60**.
MEMORY_SAMPLE_FREQ	The number of polls that are taken during each sample period. The default is **4**.

For example, using the default values for MEMORY_SAMPLE_TIME (60 seconds) and MEMORY_SAMPLE_FREQ (4), the memory usage polls would occur every 15 seconds (60 seconds divided by 4). In this case, an alarm would be generated if the memory usage level was above the specified threshold for 4 consecutive polls.

Using the CPU Usage Monitor

The CPU usage monitor generates a critical or major alarm if the CPU usage level reaches a specified value.

Table 1–3 lists the parameters you can add or modify in the **nodemgr.cfg** file.

Table 1–3 CPU Usage Monitor Parameters

Parameter	Description
CPU_REDTHRESHOLD	The percentage of CPU in use that will generate a critical alarm. The default is **90**.
CPU_ YELLOWTHRESHOLD	The percentage of CPU in use that will generate a major alarm. The default is **80**.
CPU_SAMPLETIME	The period, in seconds, in which to poll a fixed number of times. The default is **60**.
CPU_SAMPLEFREQ	How often to poll during the fixed period. The default is **3**.

For example, using the default values for CPU_SAMPLETIME (60 seconds) and CPU_ SAMPLEFREQ (3), a poll will take place every 20 seconds (60 seconds divided by 3).

Managing Ports

Offline Mediation Controller uses specific ports to send data to and to receive data from external devices and applications. Use the port information in Table 1–4 when you are planning the network and configuring routers and firewalls that communicate between Offline Mediation Controller components.

Table 1–4 Port Information

Application	Protocol	Source	Source Port	Destination	Destination Port
GTP	UDP	GSN	1024 or higher	Offline Mediation Controller	3386
Open FTP and FTP	TCP	MSC, Application Server or Offline Mediation Controller	20 or 21	Application Server or Offline Mediation Controller	20 or 21
SNMP	UDP	Offline Mediation Controller	161	EMS	162
RADIUS	UDP	GSN or RADIUS Server	1814	Offline Mediation Controller	1813
DBSR	TCP	Offline Mediation Controller	1521	Oracle database	1521

Managing Mediation Host Security

By default, all Administration Servers can connect to the mediation host (also called a node manager). You can limit access to a mediation host by using its associated *OMC_home*/**config/nodemgr/nodemgr_allow.cfg** file. The file lists the IP addresses for all Administration Servers that are allowed to connect to the mediation host. You can edit the list at any time to allow or disallow Administration Server access to the mediation host.

Setting Up an Offline Mediation Controller Administration Server Firewall

You can set up a network firewall between the Offline Mediation Controller servers and the corporate intranet or external Internet. Administration Client can connect with and operate the Offline Mediation Controller servers through this firewall.

To set up a firewall, perform the following tasks:

- Defining Administration Server Port Number
- Defining Administration Client Port Numbers

These port numbers are defined during the installation process but can be modified to accommodate your particular firewall configuration.

Defining Administration Server Port Number

To change the default Administration Server's port number for the firewall:

1. Stop all Offline Mediation Controller components.
2. Open the *OMC_home*/**config/adminserver/firewallportnumber.cfg** file in a text editor.
3. Change the value of the following entry:

   AdminServer=*port*

   where *port* is the port on which Administration Server runs. The suggested port number range is between **49152** and **65535**. The default port number in the configuration file is **55110**.

4. Save and close the file.

Defining Administration Client Port Numbers

To change the default firewall port number range values:

1. Stop all Offline Mediation Controller components.
2. Open the *OMC_home*/**config/GUI/firewallportnumber.cfg** file in a text editor.
3. Change the values of the following entries:

   RangeFrom=*port*
   RangeTo=*port*

   where *port* is the port on which Administration Client runs. The suggested port number range is between **49152** and **65535**. The default port number range in the configuration file is **55150** to **55199**.
4. Save and close the file.

Configuring Node Manager Memory Limits

To configure Node Manager memory limits:

> **Note:** The performance of the system can be affected by changing these settings, which by default are optimized for most Offline Mediation Controller applications.

1. Go to the *OMC_home*/**customization** directory and verify that the **nodemgr.var** file exists. On a newly installed system, the **nodemgr.var** file may not yet exist.

   If the file does not exist, run the following command, which creates the file:

   cp *OMC_home*/**config/nodemgr/nodemgr.var.reference** *OMC_home*/**customization/nodemgr.var**
2. Open the **nodemgr.var** file in a text editor.
3. Specify the upper memory size by modifying the NM_MAX_MEMORY parameter. The default is 3500 megabytes.
   - The valid range for a Solaris installation is from **500** to **3500**.
   - The valid range for an Oracle/Red Hat Enterprise Linux installation is from **500** to **3500**.
4. Specify the lower memory size by modifying the NM_MIN_MEMORY parameter. The default is 1024 megabytes.
   - The valid range for a Solaris installation is from **50** to **3500**.
   - The valid range for a Oracle/Red Hat Enterprise Linux installation is from **50** to **3500**.
5. Save and close the file.
6. Restart Node Manager.

Configuring the Java Virtual Machine Memory Usage when Running Administration Client

You can configure the maximum and minimum memory sizes the Java Virtual Machine (JVM) uses when running Administration Client. By configuring the maximum memory size, you can reduce the amount of memory JVM uses when running Administration Client.

To set the maximum and minimum memory sizes:

1. Open the *OMC_Home***/bin/gui** file in a text editor, where *OMC_Home* is the directory in which Administration Client is installed.
2. Add or modify the following entries:

```
InitializeExternalConfig(){
   NM_MIN_MEMORY=value
   NM_MAX_MEMORY=value
}
```

   where *value* is the appropriate value for the respective entry.

   For example:

```
InitializeExternalConfig(){
   NM_MIN_MEMORY=1024
   NM_MAX_MEMORY=3500
}
```

3. Save and close the file.

Configuring the Java Virtual Machine Memory Usage when Running Administration Server

You can configure the maximum and minimum memory sizes the JVM uses when running Administration Server. By configuring the maximum memory size, you can reduce the amount of memory JVM uses when running Administration Server.

To set the maximum and minimum memory sizes:

1. Open the *OMC_Home***/bin/adminsvr** file in a text editor.
2. Add or modify the following entries:

```
InitializeExternalConfig(){
   NM_MIN_MEMORY=value
   NM_MAX_MEMORY=value
}
```

   where *value* is the appropriate value for the respective entry.

   For example:

```
InitializeExternalConfig(){
   NM_MIN_MEMORY=1024
   NM_MAX_MEMORY=3500
}
```

3. Save and close the file.

Using Logs to Monitor Offline Mediation Controller Components

Offline Mediation Controller records system activity in log files. One log file is generated for each Offline Mediation Controller component and for each node on the mediation host. Review the log files daily to monitor your system and detect and diagnose system problems.

Types of Log Files

Offline Mediation Controller generates log files for Offline Mediation Controller components and for the nodes you create.

Log Files for Offline Mediation Controller Components

For Offline Mediation Controller components such as Administration Server, Node Manager, and Administration Client, log files are named *component***.log**; for example, **nodemgr.log**, **adminserver.log**, and **GUI.log**. The closed log files are saved using the Offline Mediation Controller component or cartridge node name, and an incrementing number; for example, **nodemgr.log.1**, **nodemgr.log.2**.

Log Files for Offline Mediation Controller Nodes on the Mediation Host

For each node on the mediation host, the log file is named *nodeID***.log**, where *nodeID* is the unique ID that is assigned by Administration Server when you create a node on a mediation host; for example, if the unique ID of the node is **2ys4tt-16it-hslskvi1**, the log file name is **2ys4tt-16it-hslskvi1.log**.

Location of Log Files

The following are the minimum Offline Mediation Controller log files:

- **nodemgr.log**
- **adminserver.log**
- **GUI.log**

Depending on the number of nodes you create, your installation will have one or more node log files.

Default Log File Locations

The log files for Offline Mediation Controller components are stored in the *OMC_home***/log/***component* directory; for example, the Node Manager log file is in the *OMC_home***/log/nodemgr** directory.

The log files for the nodes are stored in the *OMC_home***/log/***nodeID* directory; for example, if the node ID of the node is **2ys4tt-16it-hslskvi1**, the node log file is in the *OMC_home***/log/2ys4tt-16it-hslskvi1** directory.

Note: Oracle recommends that you not change the default location of the log files. If you change the location of the log files, you cannot access the log information from Administration Client.

Table 1–5 lists the components and their corresponding log file locations:

Table 1–5 Offline Mediation Controller Components and Log File Locations

Component	Log File Locations
Node Manager	*OMC_home*/**log/nodemgr/nodemgr.log**
Administration Server	*OMC_home*/**log/adminserver/adminserver.log**
Administration Client	*OMC_home*/**log/gui/GUI.log**
Node	*OMC_home*/**log/***nodeID*/*nodeID*.**log**

About the Logger Properties Files

Each Offline Mediation Controller component or node has its own logger properties file. When an Offline Mediation Controller component or a node is started for the first time, the logger properties file is dynamically created in the *OMC_home*/**config/***component* directory. By default, the logger properties file is set to the default logging level.

Table 1–6 lists the components and their corresponding logger properties file locations:

Table 1–6 Offline Mediation Controller Components and Logger Properties File Locations

Component	Logger Properties File Locations
Node Manager	*OMC_home*/**config/nodemgr/nodemgrLogger.properties**
Administration Server	*OMC_home*/**config/adminserver/adminserverLogger.properties**
Administration Client	*OMC_home*/**config/GUI/GUILogger.properties**
Node	*OMC_home*/**config/***nodeID*/*nodeID***Logger.properties**

Setting the Reporting Level for Logging Messages

By default, Offline Mediation Controller components report information messages. You can set Offline Mediation Controller to report or to not report information messages. The following levels of reporting are supported:

- **NO** = no logging
- **WARN** = log only warning messages
- **INFO** = (default) log information messages
- **DEBUG** = log debug messages
- **ALL** = log warning, information, and debug messages

> **Important:** To avoid performance degradation, use INFO level logging for debugging.

To change the severity level for logging:

1. Open the logger properties file for the component in a text editor. See "About the Logger Properties Files".
2. Search for the following entry:

   log4j.logger.*componentName*.*component*=*severity*,*component***Appender**

   where:

- *componentName* is the name of the Offline Mediation Controller component.
- *component* is the Offline Mediation Controller component or the node ID.
- *severity* is the current severity level for the logging.

For example:

```
log4j.logger.NodeManager.nodemgr=WARN,nodemgrAppender
```

3. Change the entry to the desired severity level for logging.

   For example, to change the log level from WARN to INFO for Node Manager:

   ```
   log4j.logger.NodeManager.nodemgr=INFO,nodemgrAppender
   ```

4. Save and close the file.

> **Note:** You do not need to restart the running process to enable the changes in the logging level. A predefined delay of two minutes is set before the changed logger configuration takes effect.

Using Server Monitoring

The Offline Mediation Controller server monitoring feature creates log files that report hardware performance at all times, and divides that data into convenient statistical categories.

Statistical Categories

Each statistical category has an entry in the nodemgr.cfg file to indicate if performance logging is desired. The default values are pre-set in this file and you can change them where necessary. The nodemgr.cfg file is located at *OMC_Home*/**config/nodemgr**. The statistical categories are listed in the following sections.

Disk Utilization

This function monitors the percentage of total disk space currently used on the Offline Mediation Controller partition. The corresponding entry in the nodemgr.cfg file is: SERVERMONITOR_DISK_UTILIZATION

The disk utilization log file is located in *OMC_Home*/**serverMonitoring/IP_Port/diskUtilization**

The log file values are as follows:

partition = Offline Mediation Controller installation, used to determine partition being monitored

kbytes= total disk space in partition, measured in kbytes

used= total disk space in partition used, measured in kbytes

available= disk space not in use

capacity= percentage of disk space in used

Here is an example of the disk utilization log file:

```
<poll date="2005/09/27" time="14:44:18" partition="/opt/nm500" kbytes="5886725"
used="5139094" avail="688764" capacity="89%" />
 <poll date="2005/09/27" time="14:49:19" partition="/opt/nm500" kbytes="5886725"
used="5139129" avail="688729" capacity="89%" />
<poll date="2005/09/27" time="14:54:19" partition="/opt/nm500" kbytes="5886725"
```

```
used="5139137" avail="688721" capacity="89%" />
<poll date="2005/09/27" time="14:59:20" partition="/opt/nm500" kbytes="5886725"
used="5139144" avail="688714" capacity="89%" />
<poll date="2005/09/27" time="15:04:20" partition="/opt/nm500" kbytes="5886725"
used="5139150" avail="688708" capacity="89%" />
```

Disk Status

This function monitors the health of the disk containing Offline Mediation Controller using the metastat command. Note: the metastat command must be previously installed on the system to correctly use this feature. The corresponding entry in the nodemgr.cfg file is: SERVERMONITOR_DISK_STATUS

The disk status log file is located in *OMC_Home***/serverMonitoring/IP_Port/diskStatus**

Here is an example of the disk status log file:

```
<poll date="2005/09/27" time="16:26:15" diskHealth="healthy" />
<poll date="2005/09/27" time="16:36:15" diskHealth="healthy" />
<poll date="2005/09/27" time="16:46:15" diskHealth="healthy" />
```

CPU Utilization

This function monitors the percentage of the processor(s) currently in use in the system. The corresponding entry in the nodemgr.cfg file is: SERVERMONITOR_CPU_UTILIZATION

The CPU utilization log file is located in *OMC_Home***/serverMonitoring/IP_Port/cpuUtilization**

The log file values are as follows:

cpuActive = percentage of cpu taken up with user processes

cpuSystem= percentage of cpu taken up with system processes

cpuIdle = percentage of cpu not being used

Here is an example of the CPU utilization log file:

```
<poll date="2005/09/27" time="14:39:46" cpuActive="34" cpuSystem="4" cpuIdle="62"
/>
<poll date="2005/09/27" time="14:40:06" cpuActive="62" cpuSystem="3" cpuIdle="35"
/>
<poll date="2005/09/27" time="14:40:26" cpuActive="38" cpuSystem="4" cpuIdle="58"
/>
<poll date="2005/09/27" time="14:40:46" cpuActive="16" cpuSystem="3" cpuIdle="81"
/>
```

Memory Utilization

This function monitors the percentage of the memory currently in use in the system. The corresponding entry in the nodemgr.cfg file is: SERVERMONITOR_MEMORY_UTILIZATION

The memory utilization log file is located in *OMC_Home***/serverMonitoring/IP_Port/memoryUtilization**

The log file values are as follows:

freeMemory = amount of memory not used in the heap, measured in bytes

maxMemory = memory limit available for process to grow into (-Xmx option), measured in bytes

usedMemory = maxMemory - freeMemory, measured in bytes

memory Utilization = (currently allocated process limit - freeMemory) / maxMemory, measured in bytes

Here is an example of the memory utilization log file:

```
<poll date="2005/09/27" time="14:36:07" memoryUtilization="2.8679903"
usedMemory="5.4105304E7" freeMemory="1.23482E7" maxMemory="6.6453504E7" />
<poll date="2005/09/27" time="14:36:22" memoryUtilization="2.4237578"
usedMemory="5.6333232E7" freeMemory="1.0120272E7" maxMemory="6.6453504E7" />
<poll date="2005/09/27" time="14:36:37" memoryUtilization="2.577369"
usedMemory="5.6435312E7" freeMemory="1.0018192E7" maxMemory="6.6453504E7" />
<poll date="2005/09/27" time="14:36:52" memoryUtilization="2.6964898"
usedMemory="5.6514472E7" freeMemory="9939032.0" maxMemory="6.6453504E7" />
```

Open Files - System File Monitoring

This function tracks the number of files open on the operating system. To enable system file monitoring in Offline Mediation Controller, the open source package "lsof" must be installed in a location accessible from the $PATH variable. The corresponding entry in the nodemgr.cfg file is: SERVERMONITOR_OPEN_FILES

The log file is located in *OMC_Home*/**serverMonitoring/IP_Port/systemFiles**

The log file value "**openFiles**" is the number of open files in the entire system.

Here is an example of the open files log file:

```
<poll date="2005/09/27" time="16:19:55" openFiles="2203" />
<poll date="2005/09/27" time="16:20:58" openFiles="2222" />
<poll date="2005/09/27" time="16:22:02" openFiles="2298" />
<poll date="2005/09/27" time="16:23:05" openFiles="2298" />
<poll date="2005/09/27" time="16:24:09" openFiles="2201" />
<poll date="2005/09/27" time="16:25:12" openFiles="2247" />
<poll date="2005/09/27" time="16:26:15" openFiles="2201" />
```

Log File Information

Log File Format

A server monitor log is an xml file, which tracks performance values gathered at each poll instance. Each log contains a date and timestamp, followed by the statistical values gathered during that period. Each statistical category has its own performance log file. For example:

```
<poll date="04/27/2005" time="13:49:07" cpuActive= "4" cpuIdle= "96" />
<poll date="04/27/2005" time="13:50:07" cpuActive= "6" cpuIdle= "94" />
<poll date="04/27/2005" time="13:51:07" cpuActive= "5" cpuIdle= "95" />
<poll date="04/27/2005" time="13:52:07" cpuActive= "5" cpuIdle= "95" />
```

Log File Duration

A server monitor log file contains performance data spanning a day or month, depending on which value you select in the nodemgr.cfg file. The default value is daily. For example:

SERVERMONITOR_LOG_GRANULARITY 'monthly/daily'

Log File Retention

You can specify the number of performance logs the node manager will retain. The default value of 180 allows for half of a year of data retention. For example:

SERVERMONITOR_LOG_RETENTION '###'

Log File Rollover

As a new day or month begins, the node manager automatically opens a file for the new period. At that time, the node manager also performs post-processing on the xml file from the previous day or month. The post-processing involves adding opening and closing tags to the xml file to ensure the data is well-formed.

CSV File Creation

For each performance log xml file, the node manager creates a corresponding csv file. This command-delimited file mirrors the information present in the performance log xml file, and is suitable for importing into Microsoft Excel. For example:

```
Date,time,cpuActive,cpuIdle
04/27/2005,13:49:07,4,96
04/27/2005,13:49:07,6,94
04/27/2005,13:49:07,5,95
```

Log File Naming

The performance log files (xml and csv), are named according to the statistical category and time period to which they pertain. The datestamp is in the format: YearMonthDay. For example:

```
cpu_utilization_20050431.xml (daily)
cpu_utilization_20050431.csv
cpu_utilization_200504.xml (monthly)
cpu_utilization_200504.csv
```

Using the Offline Mediation Controller Shell Tool

You can use the Offline Mediation Controller Shell (NMShell) tool to access Offline Mediation Controller system information, discover node status, and perform start and stop operations, basic alarm monitoring, traffic monitoring and node configuration changes. The NMShell tool runs on Unix workstations and is useful for low speed connections or for accessing Offline Mediation Controller from behind a firewall that does not allow GUI access.

NMShell navigation is similar to the navigation in a file system. The components of the file system - the admin server, node managers and nodes - make up a tree of contexts you can access with the **cd** command. To list the information available in a specific context, you can use the **ls** command. Certain contexts have other, context-specific commands available. For example, if you execute the **cd** command to access a node manager context, you can then use the start and stop commands for the nodes. If you are starting or stopping more than one node, list the node IDs with a space between each one.

Before accessing the system information, you must use the login command, which logs you on to the admin server. You can then navigate the Offline Mediation Controller system.

The NMShell tool is located in the *OMC_Home***/bin/tools** directory.

The commands for NMShell are shown in the following table:

Component	Command	Description
admin server	**login** [IP address] [port]	Log on to the specified admin server.
	cd [IP address] [port]	Change to the specified node manager. If no node manager is specified, change to the parent admin server.
	ls	Display list of node managers configured for this admin server.
	export [file name]	Export the system configuration to an xml file.
	help	Display list of available commands.
node manager	**cd** [*node ID*]	Change to the specified node. If no node is specified, change to the parent node manager.
	ls	Display list of nodes controlled by this node manager.
	ls [*node ID*]	Display list of configuration parameters for a specific node.
	start [*node ID*]	Start one or more nodes on the node manager. Separate the node IDs with a space.
	startall or **start all**	Start all nodes on this node manager.
	stop [*node ID*]	Stop one or more nodes on the node manager. Separate the node IDs with a space.
	stopall or **stop all**	Stop all nodes on this node manager.
	topalarm	Display the top level node manager alarm.
	perf or **performance**	Display the current node's performance window.
	help	Display list of available commands.
node	**cd**	Return to the parent node manager.
	ls	List the configuration for the node.
all	**exit/quit**	Exit the NMShell tool.
	help	List the available commands for the current context.
	pwd	Show the current context.

Monitoring Node Performance

You can monitor node performance in the Administration client in the following ways:

- For a current view of node performance, use the Node Performance View. This view displays a list of nodes running on the selected host. You can monitor node up time, current NARs, current rate, average rate, and total NARs.
- To get node performance statistics, you can configure statistics reporting: input records, output records, duplicate records, aggregated records and discarded records. You can enable or disable statistics reporting for each node, for all nodes, or for no nodes.

About SNMP Trap Hosts

An SNMP trap host is an IP host designated to receive SNMP trap messages from the Offline Mediation Controller system. Offline Mediation Controller issues SNMP trap messages to notify one or more external SNMP-based network management systems of mediation host and node alarm events. You can view trap message text on an external SNMP management system, such as the Hewlett Packard OpenView system.

Note: The same alarms are visible on the Offline Mediation Controller client and in the host and node log files.

Offline Mediation Controller only supports trap messages defined in the Offline Mediation Controller SNMP trap management information base (MIB) which defines the severity levels and meanings of SNMP trap messages issued by any Offline Mediation Controller host.

To ensure traps are received from both the local and remote node managers, when adding the target host, enter the IP address or the host name of the local machine and not the string "localhost".

Offline Mediation Controller supports the generation of SNMP V1 and V2C traps.

SNMP Trap Definitions MIB

The following contains the Offline Mediation Controller MIB used by the Offline Mediation Controller system to define SNMP trap message descriptions, type of fault, fault severity levels, possible data values, data types, and so on. Refer to this information when you configure SNMP network management workstations to receive, interpret, display, and store SNMP trap messages from Offline Mediation Controller.

```
****************************************************************************

-- NM-SNMP-MIB
--
-- Version 1.0 - February 1, 2002
--
-- Revision History
-- Feb/01/2002  Creation of MIB
--
--
****************************************************************************

NM-SNMP-MIB DEFINITIONS ::= BEGIN

    IMPORTS

        MODULE-IDENTITY,

        OBJECT-TYPE,

        enterprises,

        Counter32

    FROM SNMPv2-SMI

        DisplayString
```

```
    FROM SNMPv2-TC

        MODULE-COMPLIANCE,

        OBJECT-GROUP

    FROM SNMPv2-CONF

        IpAddress

    FROM RFC1155-SMI;

-- Define the associated MIB root

nortel          OBJECT IDENTIFIER  ::=  { enterprises 562  }

udc             OBJECT IDENTIFIER  ::=  { nortel 57 }

PM              OBJECT IDENTIFIER  ::=  { udc 1 }

registration    OBJECT IDENTIFIER  ::=  { udc 2 }


udc-r330-mib MODULE-IDENTITY

    LAST-UPDATED "0202010000Z"    -- February 1st, 2002

    ORGANIZATION "Oracle Communications Software"

    CONTACT-INFO

        "Contact: Oracle Communications Software"

    DESCRIPTION

        "This MIB module defines all of the managed objects

         and traps for Offline Mediation Controller"

  ::= { registration 1 }


--

-- Textual Conventions used in this module

--


--

-- The main MIB branches introduced in this module.

--

udcFaultManagement    OBJECT IDENTIFIER ::= { udc 3 }
```

```
udcFaultNotificationsPrefix OBJECT IDENTIFIER ::= { udcFaultManagement 1 }

udcFaultNotifications OBJECT IDENTIFIER ::= { udcFaultNotificationsPrefix 0 }

udcFaultObjects       OBJECT IDENTIFIER ::= { udcFaultManagement 2 }

--

-- NM Fault Notification definitions

--

udcClearFault NOTIFICATION-TYPE

    OBJECTS      { udcFaultComponentName, udcFaultComponentType,

                 udcFaultHostName, udcFaultSeverity, udcFaultCategory,

                 udcFaultSpecificText, udcFaultAdditionalText,

                 udcFaultTime, udcFaultNotificationId }

    STATUS        current

    DESCRIPTION

        ""

    ::= { udcFaultNotifications 1 }

udcWarningFault NOTIFICATION-TYPE

    OBJECTS      { udcFaultComponentName, udcFaultComponentType,

                 udcFaultHostName, udcFaultSeverity, udcFaultCategory,

                 udcFaultSpecificText, udcFaultAdditionalText,

                 udcFaultTime, udcFaultNotificationId }

    STATUS        current

    DESCRIPTION

        "A non-service affecting condition has occurred.

         The component continues to operate properly."

    ::= { udcFaultNotifications 2 }

udcMinorFault NOTIFICATION-TYPE

    OBJECTS      { udcFaultComponentName, udcFaultComponentType,

                 udcFaultHostName, udcFaultSeverity, udcFaultCategory,

                 udcFaultSpecificText, udcFaultAdditionalText,

                 udcFaultTime, udcFaultNotificationId }
```

```
    STATUS        current
    DESCRIPTION
        "A non-service affecting condition has occurred.
         The component is operating properly, but corrective action
         is required to prevent escalation."
    ::= { udcFaultNotifications 3 }


udcMajorFault NOTIFICATION-TYPE
    OBJECTS      { udcFaultComponentName, udcFaultComponentType,
                udcFaultHostName, udcFaultSeverity, udcFaultCategory,
                udcFaultSpecificText, udcFaultAdditionalText,
                udcFaultTime, udcFaultNotificationId }
    STATUS        current
    DESCRIPTION
        "A service affecting condition has occurred. The component is
         functioning with degraded performance and requires immediate
         operator action."
    ::= { udcFaultNotifications 4 }


udcCriticalFault NOTIFICATION-TYPE
    OBJECTS      { udcFaultComponentName, udcFaultComponentType,
                udcFaultHostName, udcFaultSeverity, udcFaultCategory,
                udcFaultSpecificText, udcFaultAdditionalText,
                udcFaultTime, udcFaultNotificationId }
    STATUS        current
    DESCRIPTION
        "A service affecting condition has occurred. The component is
         out of service and requires immediate operator action."
    ::= { udcFaultNotifications 5 }
--
```

```
-- UDC Fault Notification Objects

--

udcFaultComponentName OBJECT-TYPE

    SYNTAX        DisplayString

    MAX-ACCESS    accessible-for-notify

    STATUS        current

    DESCRIPTION

        "Unique name for the component with the fault condition.

         For example:

            nodemanager10900

            d6hvac-8es-cvfbb830 (a node-id)

         "

    ::= {  udcFaultObjects 1 }

udcFaultComponentType OBJECT-TYPE

    SYNTAX    DisplayString

    MAX-ACCESS    accessible-for-notify

    STATUS    current

    DESCRIPTION

        "The component type at which the fault condition originates."

    ::= { udcFaultObjects 2 }


udcFaultHostName OBJECT-TYPE

    SYNTAX        DisplayString

    MAX-ACCESS    accessible-for-notify

    STATUS        current

    DESCRIPTION

         "The hostname or IP Address (dot notation) where the

          NM component executes"

    ::= { udcFaultObjects 3 }

udcFaultSeverity OBJECT-TYPE
```

```
    SYNTAX INTEGER {
        clear (1),
        warning (2),
        minor (3),
        major (4),
        critical (5)
    }
    MAX-ACCESS    accessible-for-notify
    STATUS    current
    DESCRIPTION
        "Severity of the reported fault condition. This object value
         duplicates the severity of the notification.  For example,
         a udcWarningFault notification must have udcFaultSeverity
         equal to warning"
    ::= { udcFaultObjects 4 }
udcFaultCategory OBJECT-TYPE
    SYNTAX        DisplayString
    MAX-ACCESS    accessible-for-notify
    STATUS        current
    DESCRIPTION
         "The category of fault condition reported reflects the
          general type of the problem."
    ::= { udcFaultObjects 5 }
udcFaultSpecificText OBJECT-TYPE
    SYNTAX        DisplayString
    MAX-ACCESS    accessible-for-notify
    STATUS        current
    DESCRIPTION
         "The specific text describing the fault condition general
          type of the problem. This text can be used as a key to
```

```
            uniquely identify the fault condition in the category.
            This text field will be provided in the corresponding
            clear trap.  This field will not contain any variable
            text."
        ::= { udcFaultObjects 6 }


udcFaultAdditionalText OBJECT-TYPE
        SYNTAX        DisplayString
        MAX-ACCESS    accessible-for-notify
        STATUS        current
        DESCRIPTION
             "Additional text describing the fault condition. This
            text may contain variable information such as:
            IP addresses or hostnames, protocol port numbers,
            file names, or timestamp information that is useful
            to the operator in characterizing the fault condition."
        ::= { udcFaultObjects 7 }
udcFaultTime OBJECT-TYPE
        SYNTAX      DateAndTime
        MAX-ACCESS    accessible-for-notify
        STATUS        current
        DESCRIPTION
            ""
        ::= { udcFaultObjects 8 }
udcFaultNotificationId OBJECT-TYPE
        SYNTAX        Counter32
        MAX-ACCESS    accessible-for-notify
        STATUS        current
        DESCRIPTION
            "Numeric identifier for a specific incidence of this fault
```

```
            condition. This parameter is guaranteed unique for this
            component name during the life of the fault condition.
            The notification identifier will be provided in the
            corresponding clear notification."
        ::= { udcFaultObjects 9 }
    udcFaultReferenceId OBJECT-TYPE
        SYNTAX        DisplayString
        MAX-ACCESS    accessible-for-notify
        STATUS        current
        DESCRIPTION
            "Provides an alpha-numeric key that the network operator can
            use to look up a text message in any suitable language. For
            instance, the key may take the form of an integer, or even
            a URL."
        ::= { udcFaultObjects 10}
    END
```

2

Managing Offline Mediation Controller Security

This chapter describes security fundamentals for Oracle Communications Offline Mediation Controller.

About Offline Mediation Controller Security

Offline Mediation Controller security includes the following aspects:

- Secure communication
- User and password management
- Secure centralized storage for users and user's role information

About Secure Communication Using Secure Sockets Layer

Secure Sockets Layer (SSL) enables secure communication between applications. SSL enables authentication, data integrity, and data encryption. It helps to secure transmitted data using encryption.

By default, Administration Client communicates with Administration Server through SSLs. Administration Server communicates with Node Manager through SSL. During authentication, Administration Server provides the information using a certificate. It also provides data integrity through an integrity check value.

Creating Secure Connections

In Offline Mediation Controller, one-way SSL is used to create secure connections before sharing any data between the components. To use one-way SSL from a client to a server, configure identity for the server and trust store for the client. The trusted Certification authority (CA) certificates need to include the trusted CA certificate that issued the peer's identity certificate. This certificate does not necessarily have to be the root CA certificate.

In the communication between Administration Client and Administration Server, Administration Server has its own certificate in a secure keystore. This certificate will have a private and public key pair. Administration Server will share the certificate containing only the public key with all its known Administration Clients. Administration Client adds the server's certificate to its trust store, indicating that Administration Server is added to the trusted list.

In the communication between Administration Server and Node Manager, Node Manager acts as the server. Node Manager creates the key pair and store in a secure keystore. Node Manager shares its public key to the known Administration Server to

ensure a secure communication. Administration Server adds Node Manager's certificate to its trust store.

To acquire a digital certificate for your server, generate a public key, a private key, and a Certificate Signature Request (CSR), which contains your public key. You send the CSR request to a certificate authority and follow its procedures for obtaining a signed digital certificate.

After you have your private keys, digital certificates, and any additional trusted CA certificates that you may need, store the private keys and certificates in keystores.

See the discussion on creating certificates in *Offline Mediation Controller Installation Guide*.

Enabling and Disabling SSL Mode

By default, Offline Mediation Controller runs in SSL mode, but the provision for enabling and disabling SSL communication is provided in a common configuration parameter.

> **Note:** If one of the Offline Mediation Controller components is running in SSL mode, the other components must be in SSL mode.

To enable or disable SSL mode for Offline Mediation Controller:

1. Open the *OMC_home***/bin/UDCEnvironment** script in a text editor, where *OMC_home* is the directory in which Offline Mediation Controller is installed.
2. Add or modify the following entry:

   ```
   SSL_ENABLED = value
   ```

   where *value* is:

   - **TRUE** to enable SSL mode.
   - **FALSE** to disable SSL mode.
3. Save and close the file.
4. Restart Offline Mediation Controller.

Securely Connecting Administration Server to Other Node Manager Instances

You can securely connect Administration Server to other Node Manager instances or node hosts to collect data from Node Manager instances.

To securely connect Administration Server to other Node Manager instances:

1. Log on to the system on which Administration Server is installed.
2. Securely copy Node Manager's **nodeManager.cer** file from the machine on which Node Manager is installed to a temporary directory.
3. Run the following command:

   ```
   OMC_home/jre/bin/keytool -import -v -trustcacerts -alias alias_name -file File_path -keystore OMC_home/config/adminserver/adminServerTruststore.jks
   ```

   where:

- *alias_name* is the name of the new keystore entry. You must specify a different alias for each Node Manager.
- *File_path* is the path to the temporary directory and **nodeManager.cer** file that you securely copied.

Administration Server's truststore password prompt appears.

4. Enter Administration Server's truststore password.

   The **Trust this certificate** prompt appears.

5. Confirm to trust the certificate.

   The certificate is successfully imported into Administration Server's truststore.

6. Restart Administration Server and Administration Client.

Configuring Session Timeout Between Administration Server and Administration Client

The session timeout depends solely on the type of components between which the connection is established. Only the session between Administration Client and Administration Server supports session timeout after a preconfigured idle time. The session should never expire between an Administration Server and Node Manager, where user intervention is not expected.

To set the session timeout:

1. Open the *OMC_home***/web/htdocs/AdminServerImpl.properties** file in a text editor.
2. Add or modify the following entry:

   `com.nt.udc.admin.server.AdminServerImpl.timeoutVal` *`value`*

   where *value* specifies a timeout value in minutes. The default is **30**.

3. Save and close the file.
4. Restart Administration Server and Administration Client.

About Users in Offline Mediation Controller

You can create, modify, and delete user login accounts through the Offline Mediation Controller administration client. The Offline Mediation Controller software authenticates all users prior to allowing them access to system configuration views.

When a login attempt fails, the system prompts again for the user name and password for authentication. The Administration Server logs all user authentication events.

Offline Mediation Controller provides the following user roles:

- **Administrator:** Can create or delete login accounts and reset user names and passwords. The administrator can also create, modify, and delete all functional components of the system (administration servers, node managers, nodes, node chains, and so on).
- **Designer:** Can perform all of the tasks that an Administrator can, except user-management tasks.
- **Operator:** Can start and stop nodes, view logs and alarms, and edit NARs.
- **Guest:** Can view logs and alarms.

All users can change their own passwords.

Table 2–1 lists the Offline Mediation Controller functions and user access based on the role.

Table 2–1 Role-Based Access to Functions

Functions	Administrator	Designer	Operator	Guest
Change the node/node host configuration	Yes	Yes	No	No
Start or stop any node	Yes	Yes	Yes	No
Create or delete any node host, node chain, or individual node	Yes	Yes	No	No
Add, change, and delete an SNMP host	Yes	Yes	No	No
Add, change, and delete users	Yes	No	No	No
Change own details	Yes	Yes	Yes	Yes
View alarms and alarm's level for both Node Manager and individual node	Yes	Yes	Yes	Yes
View the log details for messages, exceptions, etc.	Yes	Yes	Yes	Yes
Export configurations	Yes	Yes	No	No
Import configurations	Yes	Yes	No	No
Import customizations	Yes	Yes	No	No
Launch Record Editor	Yes	Yes	Yes	No
Manage poll list	Yes	Yes	No	No
Manage statistics reporting	Yes	Yes	No	No
View Administration Server log	Yes	Yes	Yes	Yes
Create or delete or edit routing between the nodes	Yes	Yes	No	No
Clear alarms	Yes	Yes	No	No

Caution: When you start Administration Server with the **-x** parameter, user authentication is disabled and you cannot perform the user management operations in Administration Client.

About Managing Users in Offline Mediation Controller

You manage Offline Mediation Controller users by using Administration Client. The Offline Mediation Controller software authenticates all users prior to allowing them access to system configuration views. The Administration Server logs all user authentication events.

To log in to a newly installed or upgraded Offline Mediation Controller system for the first time, use the default User ID (Admin) and password (admin). Customize your own login profile, and then create user login profiles. Each profile requires a user name and a password.

About Managing the Administrator User Password in Oracle Unified Directory

You can modify the administrator user password by accessing the Oracle Unified Directory server. For information regarding managing users in Oracle Unified Directory, see the Oracle Unified Directory documentation.

Password Management

Passwords are very important for security of the system. So, the provided password should be strong and not hard-coded for users like Administrator.

By default, the password management policy is applied to users in Offline Mediation Controller. Disabling of user authentication is possible by starting Administration Server using the **-x** parameter.

Storage of Passwords

Offline Mediation Controller stores account passwords (for administrator and general users) in encrypted form in Oracle Unified Directory.

The Offline Mediation Controller installer stores account passwords in encrypted form in Oracle Unified Directory.

By default, the passwords in Oracle Unified Directory are encrypted in the salted SHA-256 format.

About the Default Password Policy

When you create a user account in Offline Mediation Controller, it assigns a default password policy to that user account. The default password policy includes the following rules:

- Passwords expire automatically after 90 days.
- The last three passwords cannot be reused during a password change.
- The password must comply with the following standards:
  - Contain at least six characters
  - Contain at least one lowercase letter
  - Contain at least one uppercase letter
  - Contain at least one special character (for example, $)
  - Contain at least one number
- The user is locked out for 10 minutes after three consecutive failed login attempts.
- The user must change the password after the first successful authentication after a password is set or reset by the administrator.

Modifying the Default Password Policies

The default password policy is assigned to user accounts during Offline Mediation Controller installation. You can modify the default password policies for the user accounts by modifying the parameters in the *OMC_home***/bin/createPasswordPolicy** file.

To modify the default password policy:

1. Ensure that the Oracle Unified Directory server instance is running.

2. Open the *OMC_home*/**bin/createPasswordPolicy** file in a text editor.
3. Enter or modify the values in the parameters. See the Oracle Unified Directory documentation for information about the parameters and values in the **createPasswordPolicy** file.
4. Save and close the file.
5. Go to the *OMC_home*/**bin** directory.
6. Run the following command:

   ```
   ./createPasswordPolicy -p OUD_password
   ```

   where *OUD_password* is the Oracle Unified Directory server instance administrator password.
7. Restart Administration Server and Administration Client.

3

Managing Nodes Using NMShell Command-Line Components

This chapter provides an overview of managing nodes using Oracle Communications Offline Mediation Controller NMShell command-line components.

Using NMShell, you can perform the following tasks at the command line:

- Adding Mediation Hosts to Node Manager
- Exporting Node Configuration and Node Customization
- Importing Node Configuration and Node Customization
- Starting All Nodes

Adding Mediation Hosts to Node Manager

Before you import the node configuration or customization into a mediation host, you must first add the mediation host to Node Manager.

To add a mediation host to Node Manager:

1. Start Administration Server and Node Manager daemons. See the discussion about starting component daemons in *Offline Mediation Controller Installation Guide*.
2. Go to *OMC_home*/**bin/tools**, where *OMC_home* is the directory in which Offline Mediation Controller is installed and enter the following command:

   ```
   ./NMShell
   ```

   The prompt changes to **nmsh>**.
3. Enter the following command:

   login *server_hostname port*

   where:

   - *server_hostname* is the IP address or host name of the computer on which Administration Server is running.
   - *port* is the Administration Server port number.
4. When prompted, enter the user name and password.

   You are connected to Administration Server.
5. Enter the following command:

   addhost -n *mediation_name* **-ip** *node_mgr_hostname* **-p** *port*

where:

- *mediation_name* is the name of the mediation host you are adding to Node Manager.
- *node_mgr_hostname* is the IP address or host name of the computer on which Node Manager is running.
- *port* is the port number at which the mediation host communicates with Node Manager.

The mediation host is added to Node Manager.

Exporting Node Configuration and Node Customization

To export the mediation host's node configuration and customization:

1. Start Administration Server and Node Manager daemons. See the discussion about starting component daemons in *Offline Mediation Controller Installation Guide*.
2. Go to *OMC_home*/**bin/tools** and enter the following command:

   ```
   ./NMShell
   ```

   The prompt changes to **nmsh>**.
3. Enter the following command:

   ```
   login server_hostname port
   ```

   where:

   - *server_hostname* is the IP address or host name of the computer on which Administration Server is running.
   - *port* is the Administration Server port number.
4. When prompted, enter the user name and password.

   You are connected to Administration Server.
5. Enter the following command:

   ```
   export [-n ALL | -n mediation_name@host_name:port] -f filename [-c value]
   ```

   where:

   - **-n ALL** specifies to export from all the mediation hosts configured in Node Manager. This is default.

     -n *mediation_name*@*mediation_hostname*:*port* exports the mediation host's node configuration or node customization.

     where:

     – *mediation_name* is the mediation host's name configured in Node Manager.

     – *mediation_hostname* is the mediation host's IP address or host name.

     – *port* is the port number at which the mediation host communicates with Node Manager.

     To export multiple hosts, enter the mediation hosts separated by comma (,).
   - **-f** *filename* specifies the name and path of the output files. Do not include the file extension.

- **-c** *value* specifies whether to export both the node configuration and customization or only the node configuration.

  where *value* is:

  - **Y** to export both the node configuration and node customization. Two files are generated; a *filename***.xml** file with the node configuration and a *filename***.nmx** file with the node customization. This is default.
  - **N** to export only the node configuration. One file is generated: a *filename***.xml** file with the node configuration.

For example:

```
export -n linux1@10.10.10.111:55109,linux2@10.10.10.112:55110 -f export -c N
```

Only the node configuration from the mediation hosts (**linux1@10.10.10.111:55109** and **linux2@10.10.10.112:55110**) is exported to the **export.xml** file.

Importing Node Configuration and Node Customization

To import the mediation host's node configuration and customization:

1. Start Administration Server and Node Manager daemons. See the discussion about starting component daemons in *Offline Mediation Controller Installation Guide*.
2. Go to *OMC_home***/bin/tools** and enter the following command:

   ./NMShell

   The prompt changes to **nmsh>**.
3. Enter the following command:

   login *server_hostname port*

   where:

   - *server_hostname* is the IP address or host name of the computer on which Administration Server is running.
   - *port* is the Administration Server port number.
4. When prompted, enter the user name and password.

   You are connected to Administration Server.
5. Enter the following command:

   import -n *mediation_name***@***mediation_hostname***:***port* **-f** *filename* **-c** *value*

   where:

   - **-n** *mediation_name*@*mediation_hostname*:*port* specifies the mediation host configured in Node Manager.

     where:

     - *mediation_name* is the mediation host's name configured in Node Manager.
     - *mediation_hostname* is the IP address or host name of the mediation host you are importing to.
     - *port* is the port number at which the mediation host you are importing to communicates with Node Manager.

The command verifies whether the mediation host exists in Node Manager. If the mediation host does not exist, the command generates an error.

- **-f** *filename* specifies the name and path of the input file. Use *filename***.xml** file to import the node configuration and use *filename***.nmx** file to import the node customization.
- **-c** *value* specifies whether to import the node customization or the node configuration.

  where *value* is:

  – **Y** to import only the node customization. Use this value with the *filename***.nmx** file.

  – **N** to import only the node configuration. Use this value with the *filename***.xml** file.

The node configuration and node customization are imported into the specified mediation host.

For example:

```
import -n linux1@10.10.10.111:55109 -f import.xml -c N
```

The node configuration is imported from the **import.xml** file into the specified mediation hosts (**linux1@10.10.10.111:55109**).

Starting All Nodes

To start all nodes:

1. Start Administration Server and Node Manager daemons. See the discussion about starting component daemons in *Offline Mediation Controller Installation Guide*.
2. Go to *OMC_home***/bin/tools** and enter the following command:

   ./NMShell

   The prompt changes to **nmsh>**.
3. Enter the following command:

   login *server_hostname port*

   where:

   - *server_hostname* is the IP address or host name of the computer on which Administration Server is running.
   - *port* is the Administration Server port number.
4. When prompted, enter the user name and password.

   You are connected to Administration Server.
5. Enter the following command:

   startNodes

   All the nodes for the currently running mediation host are started.

4

Backing Up and Restoring Offline Mediation Controller

This chapter describes the tasks that you perform to back up and restore Oracle Communications Offline Mediation Controller.

About Backup and Restore Options

After installing or upgrading an Offline Mediation Controller system, perform one or both of the following backups as a safety measure:

- Standard configuration backup
- Complete system backup

Repeat the backups whenever you make incremental changes to the system configuration or rule files.

If you have not backed up the system regularly, reinstall and reconfigure a system corrupted by an operational error such as an AC power interruption or a disk full condition. Reinstalling and reconfiguring eliminates any chance of recovering and reprocessing mediation data transitioning through the system at the time of the operational error.

About Standard Configuration Backups

The standard configuration backup captures the configuration of an entire Offline Mediation Controller host, provided that you have not made any modifications to it other than those possible through Administration Client.

Perform this backup as soon as you have configured Offline Mediation Controller, even if you have performed a complete system backup.

When you complete a standard configuration backup, you can use the backup configuration directory to restore the Offline Mediation Controller system.

You restore an Offline Mediation Controller system by replacing the damaged configuration directory with a copy of the backup configuration directory. In this circumstance, you restore the system with the same node IDs and data directory structure, and with user data retained in **input**, **output**, and **scratch** directories at the time of the operational error.

Note: If you require Offline Mediation Controller technical support, email a copy of your backup configuration directory to your Oracle Global Support representative. If you want to send a copy of your configuration directory, use the UNIX **tar** command to create an archived version of that directory.

About Complete System Backups

The complete system backup backs up the configuration of an Offline Mediation Controller host that you have modified extensively by a means other than Administration Client. For example, you may want to perform this procedure if you modified rule files and applied software patches.

Perform this backup as soon as you have configured Offline Mediation Controller. After you perform this backup, use the resulting **tar** file to fully restore your customized Offline Mediation Controller system. You can use the restoration procedure to restore an existing system or to install the same Offline Mediation Controller system configuration on another host.

For information on complete system backups, refer to your operating system documentation.

Backing Up a Standard Configuration

To back up a standard Offline Mediation Controller system configuration:

Note: This procedure backs up node chain configurations; it does not back up data.

1. Stop all functional nodes in the system:
   a. In Administration Client, select all nodes.
   b. Right-click and select **stop node(s)**.
2. Go to *OMC_home*, where *OMC_home* is the directory in which Offline Mediation Controller is installed.
3. Copy the directory configuration with a new name:

   ```
   cp -r config DirectoryName
   ```

4. Create an archive of the entire directory:

   ```
   tar cvf DirectoryName.tar DirectoryName
   ```

5. Store the backup copy in a location outside of the Offline Mediation Controller system:

   ```
   mv DirectoryName.tar new_directory
   ```

6. Restart the nodes:
   a. In Administration Client, select all nodes.
   b. Right-click and select **start node(s)**.

Backing Up a Complete System

This procedure backs up node chain configurations and data in transit, but it does not back up processed data outside of the installation directory.

To back up a complete system:

1. Ensure the disk partition in which your Offline Mediation Controller system resides has more than 70 percent of its total reserved space still available.
2. Go to *OMC_home*/**bin** and run the following command, which shuts down the entire system:

   ```
   ./ProcessControl stop
   ```

3. Create a copy of the installation directory.

   This operation may take a few minutes to finish.
4. Go to the copy of the installation directory.
5. In the copy of the installation directory, remove the **input**, **output**, and **scratch** subdirectories:

   ```
   rm -r input output scratch
   ```

   This prevents the restoration of old and duplicate billing records when you restore a full installation.
6. Create an archive of the duplicate installation directory.

   This operation may take a few minutes to finish.
7. Store a copy of the **tar** file image of your Offline Mediation Controller system at a different location.
8. Remove the copy of the installation directory.
9. Restart Offline Mediation Controller.

Restoring Offline Mediation Controller

This section outlines how to restore Offline Mediation Controller for standard configuration backups and complete system backups.

> **Note:** You must shut down all Administration Clients before performing a restore operation to ensure the restored configuration is accurate. Failure to shut down Administration Clients before performing a restore operation can result in overwriting the restored configuration.

If you customized any part of Offline Mediation Controller by a means other than Administration Client and the system is corrupt, restore the system as a standard configuration. If that procedure does not restore the system, restore it as a complete system.

If the disk partition in which Offline Mediation Controller resides is full, you must create, at the same level as the existing installation directory, enough space to restore your system. The amount of space that you create depends on whether you need to save data from the **input**, **output**, and **scratch** subdirectories.

- If you do not need to save data from the **input**, **output**, and **scratch** subdirectories, create at least three times the disk space normally occupied by your archived installation directory.
- If you need to save data from the **input**, **output**, and **scratch** subdirectories, create at least three times the disk space collectively occupied by your archived installation directory plus **input**, **output**, and **scratch** subdirectories.

In the following sample system restoration, you must create space within the installation directory **/ocomc**. The archive file containing the installation directory is **ocomcbackup.tar**.

Restoring a Standard System Configuration

To restore a standard system configuration:

1. Obtain the backup copy of your system **/config** directory.
2. If you retrieved a **tar** file copy of the backup configuration directory, extract the configuration directory.

   tar xvf *DirectoryName***.tar**

   The *DirectoryName* directory and structure is created.
3. Go to *OMC_home* and run the following command, which stops Offline Mediation Controller:

   ./ProcessControl stop
4. Go to *OMC_home* and remove the damaged configuration directory:

   rm -r config
5. Copy the backup configuration directory into the system installation directory:

   cp -r *DirectoryName* **config**
6. Restart the Offline Mediation Controller system:

   cd /*OMC_home***/bin**
   ./ProcessControl start

Restoring a Complete System Backup

To restore a full Offline Mediation Controller system:

1. At the command prompt, run the following command to shut down the Offline Mediation Controller system:

   cd /*OMC_home***/bin**
   ./ProcessControl stop
2. Retrieve the backup **tar** file of your system installation directory.
3. Extract from the **tar** file the backup copy of your installation directory:

   tar xvf /ocomcbackup.tar

   The command re-creates the duplicate installation directory, in this example, **/ocomctmp**.
4. To save as much data as possible from Offline Mediation Controller, go to the existing installation directory.

5. If you determine the directory is not corrupt, copy the **input**, **output**, and **scratch** subdirectories into the duplicate installation directory.

```
cp -r input /ocomctmp/
cp -r output /ocomctmp/
cp -r scratch /ocomctmp/
```

> **Note:** Duplicate records may occur because you do not know which records have already been sent to the billing system.

6. Delete or rename the corrupted installation directory.
   - To delete, run the following command:

     ```
     rm -r /ocomc
     ```

   - To rename, run the following command:

     ```
     mv /ocomc /ocomcdata
     ```

7. Rename the restored installation directory:

```
mv /ocomctmp /ocomc
```

8. Go to **/ocomc/bin** directory and run the following command to restart the system:

```
./ProcessControl start
```

9. The system recreates the **input**, **output**, and **scratch** directories in your restored installation directory, unless you have already copied them over.

Preserving Data When No Backup Exists

Oracle does not support any procedure for restoring an Offline Mediation Controller system that has not been backed up. If you have no backup and you want to save as much existing NAR data as possible, Oracle recommends the following procedure.

To preserve data:

1. Stop all functional nodes in the system:
   a. In Administration Client, select all nodes.
   b. Right-click and select **stop node(s)**.
2. Restart one node at a time, beginning with the node at the end of the corrupted chain.

   A node may be unable to read corrupt NARs from its **input** directory and may stall during restart. After you finish observing the behavior of one node, stop it and move on to the next node in the chain.
3. Run the following command:

   ```
   iostat int 1
   ```

   The output resembles the following listing:

   ```
   iostat int 1
   tty sd0 sd1 sd2 cpu
   tin tout Kps tps serv Kps tps serv Kps tps serv us sy wt id
   1 0 1 0 64 0 0 274 0 0 486 0 0 0 100
   ```

```
0 66 0 0 0 0 0 0 0 0 0 0 0 0 100
0 66 0 0 0 0 0 0 0 0 0 0 0 0 100
0 66 0 0 0 0 0 0 0 0 0 0 0 0 100
```

The last column on the right represents the percentage of total CPU idle time. The lower the number in this column, the more CPU time is being used to service functional nodes running in the system. When a node stalls, the CPU idles more frequently, causing the idle percentage value to rise.

4. Periodically list or monitor the number of NAR files in the node input directory by running one of the following commands:

   ```
   ls | wc
   ```

   While a functional node runs, it consumes at least 50 percent of the CPU idle time on a dual processor machine. If the CPU percentage idle is near 100 percent and the number of NAR files in the **input** directory is not going down, then it is possible that the NAR file currently being read by the functional node from its **input** directory is corrupt. The NAR file currently being processed is the one with the oldest time stamp in its name.

5. Stop the node and use the **rm** or **mv** command to remove the suspect NAR file from the **input** directory.

6. Restart the node.

   If the CPU idle percentage number decreases, then there is an increased level of CPU usage for node processing. If you do not observe this, then the NAR file you removed probably was not corrupt. In this case, stop the node, remove the contents of its **scratch** directory, and restart the node. The node resumes processing the NAR files from its **input** directory.

   If the node continues to stall, stop it, and remove the entire contents of its **input** directory. Restart the node and it resumes processing the NAR files from its **input** directory.

7. Repeat these actions for each node in the chain, as necessary, to identify the corrupt NAR files and to restore system operation.

Call Oracle Global Support for further assistance restoring an Offline Mediation Controller system that has not been backed up.

Backing Up and Restoring NAR Files

If an adverse operational event, such as AC power interruption, mediation host failure, or a hardware or software error corrupts NAR data or prevents one or more processed NARs from being delivered to their destinations, you can restore and reprocess the previously backed up NAR files. You can also engage safe mode on an E250 workstation.

The NAR file backup is available for certain nodes and is enabled through the node configuration window.

During a NAR backup, the system moves each processed NAR file from the **input** directory to the backup directory of a node and changes the NAR file extension from **.arch** to **.archbkup**.

When you restore a backed-up NAR file, you change its file extension from **.archbkup** to **.arch** in the backup directory and move or copy the renamed file into the node's **input** directory. Then, the node processes the NAR file and returns it to the backup directory with the file's last-modification date or timestamp intact. The system

processes the NAR files according to their last-modification timestamp, starting with those having the earliest timestamp.

How you restore a backup file determines when the file is reprocessed by the node and the length of time that the file remains in the backup directory after reprocessing.

- If you restore a NAR file by moving it from the backup directory to the **input** directory, the file's last modification time does not change.
- If you restore a NAR file by copying it from the backup directory to the **input** directory, the system creates a new file with a modification time set to the current system time.

Backing Up NAR Files

To restore NAR files backed up for a specific node, you must enable and configure the node's automated NAR file backup feature.

1. After you detect corrupted NAR data in the downstream mediation or OAM system, determine:
   - The time the problem began
   - The effect of the problem on your system
   - The source of the problem if possible
2. Before you restore any NAR files, identify and repair the source of the problem.
3. Clean up any suspect downstream data. You may need to delete some or all of the affected data.
4. Determine which backup NAR files need to be restored by comparing the time the problem began to the timestamp contained in the name of each backup NAR file associated with the affected node chains.

   The NAR file timestamp indicates the moment the backup file was created. The file contains data captured from that time forward, up to the configured NAR file size. Restore the sequence of backup NAR files that covers the full interval during which the problem occurred. See "Restoring Offline Mediation Controller" for more information.

Restoring NAR Files

To restore NAR files:

1. Log on to Administration Client and determine the ID of the node with the NAR file that you want to restore.
2. Select the mediation server on which the node that you want to examine resides.
3. Select the functional node and click **Edit**.

   The Node dialog box opens displaying the node ID.
4. Stop the node.
5. Go to *OMC_home* and run the following command:

   ```
   ls input backup
   ```

   A list of subdirectories named for the ID of each node appears.

   For example:

   ```
   backup:
   ```

```
1hb48pz-8ha-cdyeaz08 1hb48pz-8ha-cdyex5zr 1hb48pz-8ha-cdyf91bt
1hb48pz-8ha-cdyek5tl 1hb48pz-8ha-cdyf5xxu 1hb48pz-8ha-cdyfabet
1hb48pz-8ha-cdyel3we 1hb48pz-8ha-cdyf7gvb 1hb48pz-8ha-cdynof9c
1hb48pz-8ha-cdyetth6 1hb48pz-8ha-cdyf8a5n
input:
1hb48pz-8ha-cdyeaz08 1hb48pz-8ha-cdyex5zr 1hb48pz-8ha-cdyf91bt
1hb48pz-8ha-cdyek5tl 1hb48pz-8ha-cdyf5xxu 1hb48pz-8ha-cdyfabet
1hb48pz-8ha-cdyel3we 1hb48pz-8ha-cdyf7gvb 1hb48pz-8ha-cdynof9c
1hb48pz-8ha-cdyetth6 1hb48pz-8ha-cdyf8a5n
```

6. Go to the **backup** directory that contains a NAR file that you want to restore.

   For example:

   cd 1hb48pz-8ha-cdyeaz08

7. Move or copy the NAR file from the node's backup directory to its **input** directory:

   mv *NAR_file_name* .**archbkup ../input/** *NAR_file_name* **.arch**

8. Rename the file:

   filename.archbkup to *filename***.arch**

9. Start the node.

   The node reprocesses the NAR file.

5

Troubleshooting Offline Mediation Controller

This chapter provides guidelines to help you troubleshoot problems with Oracle Communications Offline Mediation Controller.

Troubleshooting Checklist

When any problems occur, it is best to do some troubleshooting before you contact Oracle Global Support:

- You know your installation better than Oracle Global Support does. You know if anything in the system has been changed, so you are more likely to know where to look first.
- Troubleshooting skills are important. Relying on Oracle Global Support to research and solve all of your problems prevents you from being in full control of your system.

If you have a problem with your Offline Mediation Controller system, ask yourself these questions first, because Oracle Global Support will ask them of you:

- What exactly is the problem? Can you isolate it?

  Oracle Global Support needs a clear and concise description of the problem, including when it began to occur.

- What do the log files say?

  This is the first thing that Oracle Global Support asks for. Check the error log for the Offline Mediation Controller component you are having problems with.

- Has anything changed in the system? Did you install any new hardware or new software? Did the network change in any way? Does the problem resemble another one you had previously? Has your system usage recently jumped significantly?
- Is the system otherwise operating normally? Has response time or the level of system resources changed? Are users complaining about additional or different problems?

Using Error Logs to Troubleshoot Offline Mediation Controller

Offline Mediation Controller error log files provide detailed information about system problems. If you are having a problem with Offline Mediation Controller, look in the log files.

Offline Mediation Controller logs specific details about actions performed in the Offline Mediation Controller GUI in Administration Server log files.

Getting Help for Offline Mediation Controller Problems

If you cannot resolve the Offline Mediation Controller problem, contact Oracle Global Support.

Before you contact Oracle Global Support, try to resolve the problem with the information logged in the log files. If this does not help to resolve the problem, note the following information:

- A clear and concise description of the problem, including when it began to occur.
- Relevant portions of the relevant log files.
- Relevant configuration files.
- Recent changes in your system after which the problem occurred, even if you do not think they are relevant.
- List of all Offline Mediation Controller components and patches installed on your system.

When you are ready, report the problem to Oracle Global Support.

Common Problems and Their Solutions

This section describes common problems found when running Offline Mediation Controller and their solutions.

Problem: ps: illegal option

When you start Node Manager or the Administrative Server, you receive a "ps: illegal option" error message.

Possible Cause

The **ps** script from the **ucb** package is used. You must use the **ps** script in the **/usr/bin** or **/bin** directory.

Solution

In the PATH environment variable, make sure that **/usr/bin** and **/bin** appear before **/usr/ucb**.

Problem: keytool error: java.io.FileNotFoundException While Creating Administration Server Certificate

After installing only Administration Server, when you run the **createAdminSvrCert** script to create Administration Server certificate, you receive the "keytool error: java.io.FileNotFoundException: *OMC_home***/config/GUI/adminClientTruststore.jks** (No such file or directory) " error message, where *OMC_home* is the directory in which Offline Mediation Controller is installed.

Possible Cause

The *OMC_home***/config/GUI/adminClientTruststore.jks** does not exist.

Solution

You must manually import Administration Server's public certificate into Administration Client's truststore.

To manually import Administration Server's public certificate into Administration Client's truststore:

1. Log on to the system on which the Offline Mediation Controller is installed.
2. Run the following command:

   ```
   OMC_home/jre/bin/keytool -import -v -trustcacerts -alias adminServer -file OMC_
   home/config/adminserver/adminServer.cer -keystore OMC_
   home/config/GUI/adminClientTruststore.jks
   ```

   The **Enter keystore password** prompt appears.
3. Enter Administration Client's truststore password.

   The **Trust this certificate** prompt appears.
4. Enter **y**, which trusts the certificate.

   Administration Server's public certificate is imported to Administration Server's truststore.

Problem: keytool error: java.io.FileNotFoundException While Creating Node Manager Certificate

After installing only Node Manager, when you run the **createNodeMgrCert** script to create Node Manager certificate, you receive the "keytool error: java.io.FileNotFoundException: *OMC_home*/**config/adminserver/adminServerTuststore.jks** (No such file or directory) " error.

Possible Cause

The *OMC_home*/**config/adminserver/adminServerTuststore.jks** does not exist.

Solution

You must manually import Node Manager's public certificate into Administration Server's truststore.

To manually import Node Manager's public certificate into Administration Server's truststore:

1. Log on to the system on which the Offline Mediation Controller is installed.
2. Run the following command:

   ```
   OMC_home/jre/bin/keytool -import -v -trustcacerts -alias nodeManager -file OMC_
   home/config/nodemgr/nodeManager.cer -keystore OMC_
   home/config/adminserver/adminServerTuststore.jks
   ```

   The **Enter keystore password** prompt appears.
3. Enter Administration Server's keystore (truststore) password.

   The **Trust this certificate** prompt appears.
4. Enter **y**, which trusts the certificate.

   Node Manager's public certificate is imported to Administration Server's truststore.

Problem: com.maverick.ssh.SshException When FTP is Used in Collection or Distribution Cartridge Pack

When File Transfer Protocol (FTP) is used in the Collection or Distribution cartridge pack installed on Solaris SPARC (64-bit) or Solaris X86 (64-bit), you receive the "com.maverick.ssh.SshException" error.

Possible Cause

All the required security providers are not included in the Java security files.

Solution

You must manually copy the following jar files into the *Java_home*/**jre/lib/ext** directory (where *Java_home* is the directory in which the supported version of Java is installed) and restart the system:

- **bcprov-ext-jdk15on-158.jar**
- **bcprov-jdk15on-158.jar**

To restart the system, see the discussion about starting and stopping Offline Mediation Controller in *Offline Mediation Controller System Administrator's Guide*.

Problem: Error While Starting Node Manager with SSL Enabled

When you start Node Manager with Secure Sockets Layer (SSL) enabled, you receive the following error:

```
Cannot support
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 with currently installed providers
```

Possible Cause

All the required security providers are not included in the Java security files.

Solution

You must manually copy the jars from the **jce_policy-8.zip** file into the *Java_home*/**jre/lib** directory and restart the system. You can download this file from Oracle Technology Network:

http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

To restart the system, see the discussion about starting and stopping Offline Mediation Controller in *Offline Mediation Controller System Administrator's Guide*.

A

Offline Mediation Controller Directory Structure and Contents

This appendix describes the Oracle Communications Offline Mediation Controller diirectory structure and contents.

Directory Structure and Contents

The main install directory for the system contains several sub-directories. Each contains specific types of files for various purposes. This is the list of all the directories used by the system:

- **3rdparty_jars**
- **bin**: Contains script files used to run Offline Mediation Controller
- **config**: Contains the nodes' configuration data. This data is input through the configuration GUI.
- **customization**: Contains the customized classes, rules files, and templates.
- **datadict**: Holds the dictionary of attributes for the entire system. This dictionary is not referenced in real-time by the system. It is a static reference.
- **datafiles**
- **input**: Contain the input directories for all nodes. Collection cartridges may not make use of these input directories.
- **jre**
- **licenses**
- **log**
- **output**: Contains the output directories for all nodes. Distribution cartridges may not make use of these output directories.
- **rules**: The NPL files, also referred to as rule files, reside in this directory. The subdirectories are organized by node type. For example, CC, DC and Processor nodes are referred to as the major node types. Further sub-directories are organized by the minor node types. For example “FlatFileOI”.
- **scratch**: Contains the scratch area for all nodes. The scratch is used as a temporary area for all nodes prior to the data being passed to its output.
- **web**: Contains compiled NPL files, or class files. The subdirectories here are also organized by node types similar to the rules directories.
- **xslt**