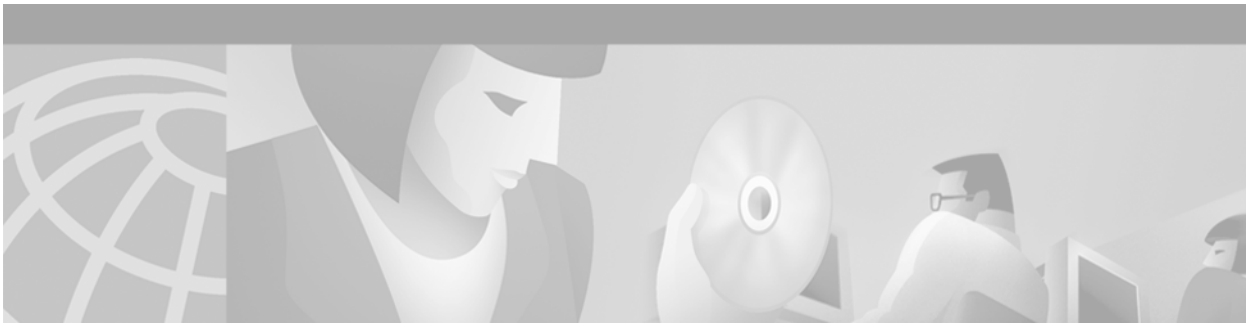

Release Notes for Cisco Media Gateway Controller Node Manager Release 2.1

February 8, 2007

These release notes describe the features and caveats for the Cisco Media Gateway Controller Node Manager version 2.1.

Introduction

Please read this entire document prior to using the Cisco Media Gateway Controller Node Manager (CMNM); as it contains pertinent information about installing, configuring, and using the software. This document provides up-to-date information about the current release of the CMNM from Cisco Systems, Inc.

For more information on the Cisco Media Gateway Controller Node Manager software, please visit Cisco's Web site at:

http://www.cisco.com > Software Center > Voice Software > Cisco Media Gateway Controller Node Manager

Contents

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Software Release History

Release 2.1(1.A) Patch Level 00

- The Backup/Restore feature has been removed. This feature is now supported in VSPT.
- Removal of MGX support. MGX is now supported in CMGM Element Manager.
- Online documentation added.
- CMNM has been enhanced to display performance data for SS7Path.
- A new dialog box has been created for dialplan properties.
- The following bugs were resolved:

Table 46 Resolved in Release 2.1(1.A) Patch Level 00

DDTS Number	Description
CSCuk26527	ST. CMNM fails to get a large dialplan.
CSCuk23874	CMNM. Status of C7IPlink misses first letter.
CSCdv47874	Cannot upload/flow through provision some nas path properties.
CSCdv88044	CMNM fails to bring up the trunkgroup property screen.
CSCdv76921	Change chassis snmp community string not propagated to child.
CSCdv88124	CMNM fails to get operational status of linkset component.
CSCdt11172	Performance data for most of CAS measurement group missing.
CSCdt14890	Discovery of Network through seed file is not complete.
CSCdt28893	VSCs state does not appear correctly in the viewer.
CSCdt28931	CMNM does not show peer port information on c7Ip links.
CSCdt37692	Cannot handle v1 cold start trap from VSC.
CSCdt56464	CMNM's diagnostic tools do not respond if invalid uid/pwd.
CSCdt93960	Import from seed file does not discover signalling.
CSCdu01430	Cleared event in event browser has wrong text.
CSCdt60865	CMNM does not mask out the password during deployment.
CSCdu06927	Some warning messages appear in the log file.
CSCdr30073	Need to get PM data from failed VSC after a switch over.
CSCdu33193	BAMS does not get associated with a MGC Node.
CSCdt92769	Status check for admin states gives invalid information.

Table 46 Resolved in Release 2.1(1.A) Patch Level 00 (continued)

DDTS Number	Description
CSCdv04298	BAMS node does not get discovered when deployed using seedfile.
CSCdt92778	Error with MGC Host Diagnostics status check for linksets.
CSCdv05092	BAMS doing auto-discovery every 1 hour instead of every 6 hours.
CSCdv05146	Unable to launch Xterm application on BAMS phase 3.
CSCdv05182	MML output is messed up.
CSCdv05411	BAMS nodes get reparented incorrectly.
CSCdv08718	BAMS node does not get deployed while deploying BAMS phase 2.
CSCdv08810	trkGrp properties missing in 9.1.5.
CSCdv21607	Installation script stops after backing up DB.
CSCdv22701	Install: The CEMF_PATCH_LEVEL variable was getting set.
CSCdv61793	Upgrade install doesnt remove backup and mgx8260.
CSCdv22720	Install: CMNM packages do not display in cemf show cmd.
CSCdv27591	Manually transitioning VSC fron hung discovery state to active state.
CSCdv35277	All SLT interfaces are shown as unreachable.
CSCdv38256	Install: Remove mgxEM from CSCOcmnm install.
CSCdv39487	Process status diagnostic tool doesnt work on BAMS 3.04.
CSCdv73019	Unable to retrieve node properties for BAMS P2.
CSCdv44635	ST. CMNM cant reboot the MGC host(userdoc).
CSCdv82497	Install: update required CEMF patch version from 1 to 4.
CSCdv77983	SLT device unreachable alarm not cleared.
CSCuk25971	NMS. CMNM does not find VSPT Release 2.1.
CSCuk27716	ST. CMNM cant reboot the MGC host.
CSCdu01987	Reboot operation for SLT requires that SLT be deployed with a userid.
CSCdt68946	The navigation menu for the administration dialog should be removed.
CSCdt40336	cmnmversion command does not display the correct information in Release 2.0.
CSCdt09317	Output of the tool to retrieve admin state has misleading info.

Release 2.1(1.1) Patch Level 00

- Added upgrade option to provide ability to upgrade from Cisco CMNM 1.5 to Cisco CMNM 2.0.

- The following bugs were resolved:

Table 47 Resolved in Release 2.1(1.1) Patch Level 00

DDTS Number	Description
CSCdt40353	Release Notes do not mention upgrade procedure for CMNM 2.0.
CSCdr30073	CMNM need to get performance data from failed VSC after a switch over.
CSCds57400	VSC performance counter units are undefined.
CSCds30084	CMNM need to handle the case when user deploys more than two MGC hosts in a MGC node.
CSCdv22720	CMNM EMs are now displayed with the "cemf show" command.
CSCdv38256	The mgxEM has been removed from CMNM.

Installation Requirements

Detailed installation requirements are documented in Chapter 2 of the *Cisco Media Gateway Controller Node Manager User's Guide*. Review this chapter prior to installing and/or configuring the software. Here are some general installaiton guidelines include the following:

- Sun Ultra 60 workstation with 2 CPUs (360 MHz or faster)
- 1.0 GB of RAM (or greater)
- 4, 6, 8, or 9 GB SCSI drives properly configured. The database drives should be configured as RAW devices and connected to a separate SCSI controller for maximum performance.
- The tmpfs file system must be mounted to /tmp for maximum performance.
- ObjectStore (Cisco Element Management Framework (CEMF) database program) should be configured to use raw file systems

Note Installing drives greater than 9 GB does *not* result in performance gains. The main bottleneck of the CEMF application is hard disk input/output (i/o) speed, not capacity. Maximum performance is achieved using many drives of lower capacity instead of a few, larger capacity drives.

Supported Network Elements

The following network elements have been tested and verified to work with this release of the Cisco CMNM.

Note All other releases of Network Element Software have not been tested and are not supported with this release.

- Cisco Media Gateway (MGX):

  1.1.1, or SCC_r01.01.a04 as reported by release command
- Cisco Virtual Switch Controller (VSC):

7.4(11)
9.0(0)

- BAMS:

  2.63, 2.64, 2.65, 2.67i

- Catalyst 5500:

  5.4(4) (other 5.x code also works)

- Catalyst 2900XL:

  12.0(5)2.XU (other 12.x code also works)

- Catalyst 2600:

  12.0(7)XR

- This release is also compatible with the following releases of Network elements:

  Cisco Virtual Switch Controller (VSC):

  9.0(1), 9.0(2)

Note This release can manage a Release 9.0(1) VSC as a Release 9.0(0) VSC, however it may not support all Release 9.0(1) features. For more information, please see the "Known Issues and Operational Recommendations" section.

Installation Checklist

Before installing the software, read Chapter 2, *Installing CMNM*, of the *Cisco MGC Node Manager User's Guide*. If you are setting up a client/server architecture, then the CEMF and CMNM software must be installed on both the client and server workstations. The CMNM installation software determines whether the client or manager software should be installed.

- Verify that the minimum hardware requirements pertaining to your site have been met
- Ensure that the computer is in DNS
  - Ensure that the computer is using DNS

    The computer must have a valid entry in DNS.
  - If the computer is not using DNS, disable Name Resolution completely (that is, there should be no /etc/resolv.conf file).
- Verify that the CEMF software has been installed and is running (the CEMF software must be running for the Cisco MGCM software to be installed.)

Note Refer to the "Installing CMNM" section in the "Cisco Media Gateway Controller Node Manager Users Guide" for detailed instruction on how to mount the CD-ROM.

Step 1 Become the root user.

Step 2 Place CMNM CD in the CD-ROM drive.

Step 3 Change to the /cdrom/cdrom0 directory

Step 4 Execute the command: **./installCSCOcmnm**.

Step 5 Follow the on-screen prompts.

Step 6 Eject the CD-ROM when the installation is complete.

Upgrade Procedure Checklist

The Cisco CMNM upgrade process enables you to easily upgrade from CMNM Release 1.5. Refer to the "Upgrading from CMNM Release 1.5" section of the "Cisco Media Gateway Controller Node Manager Users Guide" for detailed instructions on how to mount the CD-ROM.

Step 1 Become the root user.

Step 2 Place CMNM CD in the CD-ROM drive.

Step 3 Change to the /cdrom/cdrom0 directory.

Step 4 Execute the command **./installCSCOcmnm -upgrade**.

Step 5 Follow the on-screen prompts.

Step 6 Eject the CD-ROM when the installation is complete.

Patch Procedure

The Cisco CMNM patch process is not incremental. Downloading and installing the latest patch installs all the previous patches. The patch process automatically determines which portions of the Cisco MGC Node Manager need to be patched. In order for you to install a patch, the base Cisco MGC Node Manager software must be installed. Use the following steps to install the latest patches.

Step 1 Verify that the base Cisco MGC Node Manager software is installed.

Step 2 Become the root user.

Step 3 Create a temporary installation directory /opt/cmnm_tmp_install.

Step 4 Download the patched software from its location to the temporary installation directory.

Step 5 Extract the patched software. For example, you can use:

```
zcat CSCOcmnmPatch_0x.tar.Z | tar xvf -
```

Step 6 Execute the command: **./patchCSCOcmnm**

Step 7 Follow the on-screen prompts.

Open Caveats

This section describes open issues and caveats for Cisco Media Gateway Controller Node Manager version 2.1. Table 48 lists resolved caveats sorted by severity, then identifier, then component.Contact your Cisco representative to obtain status on software problem reports (SPRs). For more information on IOS caveats, see the IOS release notes for your platform.

Note Caveats with a severity of 1, 2, and 3 only are listed.

Table 48 Open Caveats

Identifier	Severity	Component	Description	Explanation
CSCdw34451	2	other	Host controller consumes too much memory.	Workaround: None.
CSCdw35337	2	other	Host controller cores when polling the standby VSC.	Workaround: None.
CSCdv26748	3	snmp	SNMP: Research: CIAgent recognize processor state change.	Workaround: None.
CSCdw48034	4	doc	CMNM: Upgrade to CMNM2.1(2) not supported.	This CMNM version requires an upgrade from CEMF 3.1P4 to CEMF 3.2P1. The upgrade has not been tested and hence is not supported for this version. Need to do fresh install of CEMF 3.2P1 and then CMNM 2.1(2.B).
CSCdr13927	2	other	Need to support installing on workstation that is not in DNS.	The CEMF license manager (and Corba) do not work correctly if the workstation's hostname is not in DNS. A resolv.conf exists; the nsswitch.conf file is set with either: files dns or files.

New Features and Enhancements

Country Code Prefix Per Trunk Group Capability

This featurette (CSCdv61281) allows you to send to different carriers for a given destination (on a per trunk group basis) where some carriers use an international format and other carriers use a national format. You can choose to apply or remove a country code and also optionally apply an international prefix.

This featurette introduces four new trunk groups and one new analysis result type which delivers the country code digits used for B-number manipulation. If the analysis result type is retrieved, it supplies the country code digit string that is internally stored until egress trunk group selection. During the final processing stage, the UCM checks to determine whether to prefix the called and calling party numbers with national or international prefixes (0 or 00).

MGC Product Name References

This featurette (CSCdw15883) renames existing code references from VSC, VSC3000, SC, and SC 2200 to a more generic MGC. These changes are applied to customer viewable area such as properties, messages, alarms, measurements and the GUI screen. Internal code references, such as variable names, will not be changed.

Generic Transparency Descriptor Flow-Through Support

This featurette (CSCdw32042) provides generic transparency descriptor (GTD) support. GTD transports ISUP messages and parameters, using a generic format, between the ingress and egress SC2200 Signaling Controllers. To support the GTD protocol, the following changes were made to the SC2200:

- a new component, GTD Parameter was created
- a new property, GtdCapTypeProp for NAS sigpath, was created
- changes were made to mml to provision the GTD parameters

Online Documentation

This featurette (CSCdu80596) provides online documentation support. This documentation is accessible using a button located on the CMNM interface. At this time, a PDF of the CMNM User's Guide is available.

8260 Support

This featurette (CSCdv39570) removes 8260 management support to prevent conflict with other EMS. Seed files from the VSPT, which include 8260 seed information, are also ignored.

Dial Plan Properties: Overdecadic Field

This featurette (CSCdv54344) provides a new dialog box for dialplan properties. This new dialog box displays the dialplan name and the overdecadic property. It can be launched from the dialplan or from the dialplan folder.

Known Issues and Operational Recommendations

This section contains information about known issues and the corresponding workarounds.

Note For more information about Cisco IOS issues and workarounds, see the Cisco IOS release notes for your platform.

CMNM Does Not Correctly Collect Performance Counters

CMNM does not correctly collect performance counters generated by the PGW. Some counters are not collected and others are collected on the wrong type of object.

Upgrade to CMNM 2.1 Not Supported

There is no supported upgrade path to CMNM 2.1.

CMNM Checks for Available Disk Space For Installation

During installation, CMNM detects how much disk space is available for installation. If the system does not have enough available disk space, you are prompted whether you want to continue the installation routine. If you enter 'N' to stop the CMNM installation, the installation continues.

The workaround is to ensure that enough free disk space is available before CMNM is installed. The amount of disk space required is detailed in the CMNM installation guide.

CMNM Does Not Support SNMP Packages Larger Than 2084 Bytes

CEMF Release 3.1 software does not support SNMP packages larger than 2084 bytes. As a result, CMNM does not support SNMP packages larger than 2084 bytes. The workaround is to configure managed devices to use the maximum size of 2084 bytes for SNMP packages.

CMNM Cannot Discover an Interface or IP Address for BAMS

Sometimes CMNM reports that it cannot discover an interface or IP address for BAMS. This might be caused by the mib2agt getting into a *strange* state. You can restart the mib2agt by stopping the current process. The new process mib2agt is restarted automatically.

```
ps -ef | grep mib2agt
kill -9 <PID>
```

CMNM Release 2.0 Does Not Support BAMS Phase 3

CMNM Release 2.0 does not support BAMS phase 3.

CMNM Release 2.0 Does Not Support Some Attributes

Although CMNM Release 2.0 supports MGC host 9.0(1) and 9.0(2), it does not support the following attributes:

Table 49 Unsupported Attributes

Object	Attributes
SessionSet	nextHop1, netMask1, nextHop2, netMask2
SS7SGIpLink	nextHop, netMask
SIPLink	nextHop, netMask

Upload/Download Operation

The Cisco MGC Node Manager (MGCNM) upload operation backs up all the necessary files resulting from a prov-exp:all command on a Cisco Media Gateway Controller (MGC) host. In addition, every device is backed up once every 24 hours.

A download operation transfers only the backed-up configuration files from the specified TFTP server to the MGC host. The configuration is not loaded, nor is it activated.

Use the following steps to restore a MGC host configuration from a MGCNM-initiated backup:

Step 1 Transfer the backup configuration file to the host where the Cisco Voice Services Provisioning Tool (VSPT) is running:

- **a.** Telnet to the host where the VSPT is running.
- **b.** Change to the */tmp* directory.
- **c.** Create a directory under /tmp to copy the configuration file.
- **d.** Change to the new directory created in the previous step.
- **e.** FTP to the TFTP server or other host where the backed up configuration file exists.
- **f.** Change to the directory where the configuration file exists.
- **g.** Get the configuration file (this should be a file with a .tar extension). For example,

  `get mgc21-2001Jan31.tar`.

- **h.** Quit the FTP session.

Step 2 Extract the saved configuration files from the retrieved tar file, for example,

`tar -xvf mgc21-2001Jan31.tar .`

Step 3 Start the Cisco VSPT.

Step 4 Create a new configuration:

- **a.** Select **File > New** to create a new configuration.
- **b.** Enter a name for the new configuration and click OK. The New Configuration Wizard dialog appears.
- **c.** Select the **Perform manual configuration** option and click OK.

Step 5 Import the backed-up configuration files into your new configuration:

a. Import MML Configuration File:

- Select **File > Import** from the menu bar.
- Select **From File** to import configuration information from a file.
- Set the file type to MML Configuration File and click **Select**.
- At the Specify file to import dialog, enter the directory where you transferred the backed up configuration file. Enter the directory name in the File name input field (for example, /tmp/mgc) and click **Open**.

  You should see the original tar file and a new folder. This folder contains the various backed up configuration files.
- Double click the new folder. You should see one or more files with a file extension of .mml and possibly some files with a .dat extension.
- Select the file named config.mml and click **Open.** Click **OK** in the Import Dialog window.

b. Import the trunk group file (if there is one):

- Select **File > Import** from the menu bar.
- Set the file type to Trunk Group File and click **Select** to choose the file to import.
- Select the export_trkgrp.dat file and click **Open** and then **OK** in the Import Dialog window.

c. Import the trunk file (if there is one):

- Select **File > Import** from the menu bar.
- Set the file type to Trunk File and click **Select** to choose the file to import.
- Select the export_trunk.dat file and click **Open** and then **OK** in the Import Dialog window.

d. Import the MML routing file (if there is one):

- Select **File > Import** from the menu bar.
- Set the file type to MML Routing File and click **Select** to choose the file to import.
- Select the file named routing.mml and click **Open** and then **OK** in the Import Dialog window.

e. Import the dialplan file(s) (if there are any):

- Select **File > Import** from the menu bar.
- Set the file type to Dialplan File and click **Select** to choose the file to import.

  If you have a dial plan configured, there might be additional MML files listed other than the config.mml and routing.mml files. If so, repeat steps c, d, and e for each file to import them.

Step 6 Specify MGC host information:

- Select **Unknown MGC** in the tree shown under Number Analysis and enter the required attribute information on the right for the MGC host where you would like to restore the configuration.

  You must enter the MGC host name, login id, and password. After this, click **Import Settings** located toward the bottom right hand corner of the dialog box. This retrieves some of the information from the specified MGC host.
- Click **Modify** at the bottom of the screen to save your settings.

Step 7 Save your configuration:

Select **File > Save > As Working** from the menu bar.

Step 8 Deploy your configuration:

- Select **Tools > Deploy** from the menu bar.
- Enter the name under which you would like to save the configuration on the MGC host to which you are deploying the configuration.
- Select **[NEW]** as the "Based on configuration".
- Select the appropriate VSC deployment action.
- Click **OK** to deploy the configuration.

  A progress window pops up showing each provision command as it is executed on the MGC host. If there are errors, they are listed.

Hints and Tips

Initial CMNM Configuration

CMNM is initially configured with one user:

```
id: admin
password: admin
```

Sample Network Seed File

A sample network seed file is located at: <CEMF Direcory>/samples/seedfile.txt. To access the <CEMF Directory>, enter the following command:

Manager:

```
pkgparam CSCOcemfm BASEDIR
```

Client:

```
pkgparam CSCOcemfc BASEDIR
```

Changing the IP Address or Hostname

If you have installed a CEMF/CMNM client and need to change the IP address/hostname of the CEMF/CMNM server, you must change the client's configuration. Complete the following procedure to select a different server:

Note The following example uses the hostname CMNM and the IP address 10.1.1.1.

Step 1 **#cd <CEMF Directory>/bin**

Step 2 **#./cemf stop**

Step 3 Edit /var/adm/Atlantech/system/info. Change to the correct hostname and ip address:

```
MGRHOSTNAME=rambler
MGRIPADDRESS=10.1.1.1
COREHOSTNAME=rambler
```

Step 4 Edit <CEMF Directory>/config/env/avCore.sh. Change the hostname in the lines below, and save the file.

```
MgrSystemManager=rambler1270; export MgrSystemManager
PortAllocator=rambler1270; export PortAllocator
transRouter=rambler1271; export transRouter;
```

Step 5 #**<CEMF Direcory>/bin/cemf start**

Installing CEMF/CMNM on a Server

If you have installed CEMF/CMNM on a server and need to change the IP address/hostname, you must make the changes shown in the following procedudre:

Note The following example uses the hostname CMNM and the IP address 10.1.1.1.

Step 1 #**cd <CEMF Directory>/bin**

Step 2 #**./cemf stop**

Step 3 Edit /var/adm/Atlantech/system/info to reflect the following hostname and ip address:

```
MGRHOSTNAME=rambler
MGRIPADDRESS=10.1.1.1
COREHOSTNAME=rambler
```

Step 4 Edit <CEMF Directory>/config/env/avCore.sh to reflect the hostname in the lines below, and save the file.

```
MgrSystemManager=rambler1270; export MgrSystemManager
PortAllocator=rambler1270; export PortAllocator
transRouter=rambler1271; export transRouter;
```

Step 5 Edit /var/sadm/pkg/CSCOcemfm/pkginfo to reflect the following values:

```
MGRIPADDRESS=10.1.1.1
MGRHOSTNAME=10.1.1.1
COREHOSTNAME=10.1.1.1
LOCALHOSTNAME=10.1.1.1
```

Step 6 You will also need to make these same changes for each Element Manager. To do so, edit the following files:

```
/var/sadm/pkg/hostEM/pkginfo
/var/sadm/pkg/mgcEM/pkginfo
/var/sadm/pkg/mgxEM/pkginfo
```

Step 7 Rename <CEMF Directory>/ODI/OS5.1/ostore/<hostname>_server_parameter to reflect the new hostname.

Note You must obtain a new CEMF license. For information on obtaining a new CEMF license, refer to "CEMF Licensing" in the "Troubleshooting" section.

Step 8 **<CEMF Direcory>/bin/cemf start**

Configuring the CEMF Software for Maximum Performance

The following are guidelines for installing CEMF:

- Use the primary drive for the Solaris operating system and the ObjectStore transaction log.
- The second drive should contain the CEMF software (that is, /opt/cemf).
- Configure the ObjectStore database for Raw FileSystems. The remaining hard drives should contain the RAW FileSystem partitions for the CEMF database (preferably on a separate SCSI controller).

  Mount the tmpfs file system to /tmp so the ObjectStore cache files can be kept in memory. ObjectStore is the database program included with CEMF. Keeping the cache files in memory provides for an enormous performance boost for CEMF. Here is how the tmpfs line should read in the /etc/vfstab file (the blank areas between the keywords are spaces):

  ```
  swap  -  /tmp  tmpfs  -  yes  -
  ```

Configuring Raw Filesystems in ObjectStore

By default, the CEMF database system (ObjectStore) is configured to use typical cooked file systems (that is, filesystems with readable directory entries) for the database. However, database performance is maximized when ObjectStore is configured to use Raw file systems. To achieve maximum performance, the hard drives containing the Raw file systems should be on a separate SCSI controller (not on the same controller as the primary operating system drive). The following should be noted:

- Partition the hard drives when you install the Solaris operating system.
- Type the command, **/bin/pkgparam CSCOcemfm BASEDIR** to get the installation directory for the CEMF software.
- All Raw partitions must be exactly the same size (in MB). ObjectStore does not use partitions of different sizes.
- The Raw partition names (that is, **/dev/rdsk/c0t1d0s3**) must be available before starting the configuration session.
- Determine the name of the machine (for example,cemfserver).
- Adding, modifying, and/or deleting Raw File systems resets the ObjectStore database and destroys any existing data there.

Complete the following steps to start the ObjectStore and CEMF processes:

Step 1 Log in to the system as the root user.

Step 2 Using the following command, stop the current CEMF processes:

/etc/init.d/cemf stop

Step 3 Shut down ObjectStore:

/etc/rc2.d/S80ostore4 stop

Step 4 Shut down the AV license manager:

/etc/rc2.d/S98avlm stop

Step 5 Start a CEMF shell:

/etc/rc2.d/S99cemf shell

Step 6 Change to the CEMF installation directory:

/opt/<INSTALL_DIR>

Step 7 Change the directory to **./ODI/OS5.1/ostore/etc** (under **/opt/<INSTALL_DIR>**).

Step 8 Edit the hostname server parameter file (**<hostname>_server_parameters**) with the following modifications:

- Put a comment character # at the beginning of the Log File line. This places the transaction log in the Raw partition and improves performance.
- Add an entry for each Raw Partition ObjectStore will use. Each line must begin with PartitionX: (where X is a number, starting with zero and incrementing by one).

Note Don't forget the colon character.

  - Each line must have the word PARTITION as the second element.
  - Each line must have the Raw partition listed as the last element (use the rdsk partition identifier).
  - Example:

```
unix-shell#> cd /opt/CSCOcemf/ODI/OS5.1/ostore/etc
unix-shell#> cat cemfserver_server_parameters

#Log File: /opt/transact.log
Partition0: PARTITION /dev/rdsk/c2t9d0s0
Partition1: PARTITION /dev/rdsk/c2t10d0s0
Partition2: PARTITION /dev/rdsk/c2t12d0s0
Partition3: PARTITION /dev/rdsk/c2t13d0s0

unix-shell#>
```

Step 9 Change directory to <CEMF_INSTALL>/ODI/OS5.1/ostore/lib. For example, /opt/CSCOcemf/ODI/OS5.1/ostore/lib.

Step 10 Run the command **./osserver -i** to reinitialize ObjectStore. Answer **yes** when prompted to reinitialize the database.

Step 11 Run the command **/etc/init.d/cemf reset** to reset the CEMF database. Answer **yes** when prompted.

Step 12 Run the command **/etc/init.d/cemf start** to start the ObjectStore and CEMF processes.

ObjectStore is now using RAW databases.

Troubleshooting

Viewing Core Files Generated by CEMF and CMNM

Use the **/opt/cemf/bin/listCores** command to view all core files generated by CEMF and CMNM.

CEMF Licensing

If you are having problems with CEMF licensing, you might need to stop and restart the license manager daemon. To do so, execute the following commands:

```
#>  /etc/rc2.d/S98alvm stop
#>  /etc/rc2.d/S98alvm start
```

Note The CEMF licenses are fixed for a particular machine. You cannot copy the license file from one machine to another. If you want to install the CEMF software on another machine, you must contact Cisco TAC and ask for a new license. You will need the hostname and hostid of the new machine.

Viewing the Most Recently Changed Log Files

CMNM log files are stored in <CEMF Directory>/logs. You can view the most recently changed log file with **ls -lt** command.

Interesting CMNM Log Files

Some CMNM log files are:

- hostController.log [MGC Host]
- mgcController.log [MGC Node]
- mgxController.log [MGX 8260]

Error Messages That Are Safe to Ignore

Most of the entries in the CMNM log files are created by the CEMF platform and are of limited value. The following error messages are safe to ignore:

- SNMP and MIB parsing errors (which display when an EM controller starts):
  - SNMP : ERROR mib.cc:1283 Mib Object is already on the tree for .
  - SNMP : ERROR mibDependencyMgr.cc:191 mibDependencyMgr.cc:196 Mib . not defined
  - SNMP : ERROR mibParser.y:359 EXPORTS are currently ignored (;, line 8)
  - SNMP : WARN mibParser.y:1154 Name and number form OIDs are not properly implemented ().
- Database warning (which display when an EM controller is first installed):

general : WARN Creating Database /opt/AV3/db/mgcController.db

- General errors (which display when the EM controller starts up):
  - general : ERROR Unable to get event channel ID for channel ' '
  - general : ERROR EventChannelManager : Failed to find location for event channel
  - general : WARN OGManager::OGManager - Unable to get deleteEventChannel from .ini file
  - general : ERROR OGManager::processGroupClass - invalid class id
  - general : ERROR EventChannelManager : Failed to find location for event channel ERROR OGManager::processGroupClass - invalid class id
  - general : ERROR OGChangeEventHandler::process - could not find drep!
  - general : ERROR IdAllocatorOS : Deprecated constructor called
  - Task : WARN PerfPollTask::createGroupsResult : group . already exists.
  - mgcController : WARN Controller::initialiseController Controller is configured NOT to auto populate tech tree on autodiscover
- Other misc errors:
  - general : WARN CommsBuffer::serialize - resizing buffer size
  - general : ERROR PersistentAttributeStore::PersistentAttributeStore() nameInit = 'xxx. is longer than 16 characters. All Objectstore segment comments will be truncated to use the first 16 characters.

Resetting the User Password

If you forget your password, you can reset the CEMF user IDs and passwords. The following command removes all passwords, and resets the admin user ID's password to *admin*.

```
<CEMF Directory>/bin/cemf shell
<CEMF Directory>/bin/partitioningTool -r
```

Backing Up and Restoring the CEMF/CMNM Databases

The following command backs-up the CEMF/CMNM databases. By default the backup files are placed in /opt/AVBackup.

```
/opt/CSCOcemf/bin/cemf stop
/opt/CSCOcemf/bin/cemf backup
/opt/CSCOcemf/bin/cemf start
```

The following command will restore a CEMF/CMNM database.

```
/opt/CSCOcemf/bin/cemf stop
/opt/CSCOcemf/bin/cemf restore -t mm-dd-yyyy
/opt/CSCOcemf/bin/cemf start
```

For more information on backing up and restoring CEMF/CMNM Databases refer to the “Cisco EMF Database Backup and Restore Procedures” section of the *Installing, Licensing, and Configuring Cisco EMF Manual*.

Forcing an Uninstall of an Element Manager

The CEMF daemons must be running for the Element Managers (EMs) to uninstall. There are two ways to force an uninstall of an EM; both cause loss of all CEMF/CMNM data. Before running these commands, it is recommended that you back up your databases.

The uninstallCSCOcmnm script can be invoked with an undocumented option to force the removal of all or one EM. From a command line, as root, type the command:

/opt/CSCOcemf/uninstall/uninstallCSCOcmnm -force [-em <EM>]

You can specify only one EM to remove or all EMs by omitting that parameter. The list of EMs includes hostEM, mgcEM, andmgxEM.

Example:

/opt/CSCOcemf/uninstall/uninstallCSCOcmnm -force -em mgxEM -em mgcEM

After you run this command, the CEMF databases are corrupted. To correct this problem, reset the CEMF databases by running the following command. You must do this before using CEMF again,even using CEMF to reinstall CMNM.

```
/opt/CSCOcemf/bin/cemf stop
/opt/CSCOcemf/bin/cemf reset
/opt/CSCOcemf/bin/cemf start
```

After you have successfully reset the database and restarted CEMF, you must reinstall CMNM. If you want to restore a CEMF/CMNM database after you have reinstalled CMNM, refer to “Backing up and restoring the CEMF/CMNM Databases” in the preceding section.

If the above method doesn't remove the EMs, then you can try another method. When the EMs are installed, Solaris package information is placed in subdirectories of /var/sadm/pkg. The subdirectory is the name of the packge, as specified above (that is, hostEMm, mgcEMm, and so on.). As the root user, complete the following steps for each EM that you want to remove.

```
/opt/CSCOcemf/bin/cemf stop
touch /var/sadm/pkg/<EM>/install/.avload
pkgrm <EM>
/opt/CSCOcemf/bin/cemf reset
/opt/CSCOcemf/bin/cemf start
```

Example:

```
/opt/CSCOcemf/bin/cemf stop
touch /var/sadm/pkg/mgcEMm/install/.avload
pkgrm mgcEMm
/opt/CSCOcemf/bin/cemf reset
/opt/CSCOcemf/bin/cemf start
```

To restore a CEMF/CMNM database after you have reinstalled CMNM, refer to the preceding “*Backing Up and Restoring the CEMF/CMNM Databases*”.

Managing Network Devices Over a Slow Link

If you are managing network devices over a slow link (T1 or slower), you might need to alter SNMP parameters used by CMNM for SNMP Get Requests. You can change these parameters for any existing objects by accessing the States dialog. You can also change these parameters in the Advanced tab of the Seed File Deployment dialog.

The default number of SNMP retries is 2. You might need to increase this value when the CMNM workstation is connected to network devices over a slow link.

The default SNMP timeout value is 5000 milliseconds (5 seconds). You may need to increase this value when the CMNM workstation is connected to network devices over a slow link.

Maximizing Logfile Output

By default CMNM logs only warning and error messages. If you want to turn on debug messages in all log files, complete the following steps, as the root user:

Step 1 **cd <CEMF Direcory>/bin**

Step 2 **./cemf stop**

Step 3 **cd <CEMF Direcory>/config/init**

Step 4 Edit loggercommon.include and add or change the following line:

loggingLevelMask = 12

Step 5 **cd <CEMF Direcory>/bin**

Step 6 **./cemf start**

Step 7 To set the logging level back to warning, add or change the following line:

loggingLevelMask = 10

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

http://www.cisco.com

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support

- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.