



# Upgrading the Integrated EMS

---

## Introduction

Use these procedures to upgrade the Integrated EMS. The upgrades can be through the maintenance release or through the patches.

For more information on installing or upgrading Integrated EMS software, refer to *Integrated EMS Installation Method, 24-1464*.

This section includes the following sections:

- [Upgrading Integrated EMS software](#)
  - [Preparing to upgrade the Integrated EMS](#)
  - [Upgrading Integrated EMS in a simplex configuration](#)
  - [Upgrading Integrated EMS in an HA configuration](#)
  - [Completing the Integrated EMS upgrade](#)
- [Setting up the BootP file on SSPFS](#)
- [Editing and viewing object properties using Java Web Client](#)
- [Editing and viewing object properties using Web Client](#)
- [Downgrading the IEMS software](#)

## Upgrading Integrated EMS software

Upgrading Integrated EMS software involves installing a higher version of Integrated EMS software over the current version of the Integrated EMS. Use this procedure to upgrade Integrated EMS software to higher versions in simplex and HA configurations.

**Note:** If the upgrade of Integrated EMS to the newly installed version of software fails before the upgrade is completed, all the changes done for migrating the data of Integrated EMS revert to the original state.

### Preparing to upgrade the Integrated EMS

The following table contains a summary of required pre-upgrade procedures.

#### Required pre-upgrade procedures

Requirement	Documentation
1. Check the hardware requirements	Refer to "Hardware requirements" of <i>Integrated EMS Basics</i> , NN10329-111
2. Ensure the (I)SN07 Integrated EMS is installed with all patches	Refer to <a href="#">Ensuring (I)SN07 Integrated EMS is installed</a>
3. Backup the SSPFS including the Oracle data.	It is recommended that the user takes a backup image for restore in case the upgrade fails. Refer to backup and restore procedures of <i>ATM/IP Solution-level Fault Management</i> , NN10408-900
4. Ensure the SSPFS software is upgraded	Refer to "Upgrading SSPFS software" of <i>Upgrading a Carrier Voice over IP Network</i> , NN10440-450
5. Ensure the devices supported by Integrated EMS are upgraded to (I)SN07	Refer to the Upgrade document for the device
6. Ensure the user names in (I)SN07 are compliant to (I)SN08 restrictions.	All user names in (I)SN07 must be compliant to the (I)SN08 restrictions. Refer to "Adding New Users" of (I)SN08 <i>Integrated EMS Security and Administration</i> , NN10336-611. If the user names are not compliant to these rules they may be deleted without notice during upgrade.

## Required pre-upgrade procedures

Requirement	Documentation
7. Order of upgrade	Refer to "Component Upgrade order" of <i>Upgrading a Carrier Voice over IP Network</i> , NN10440-450
8. Ensure the DNS is enabled.	Ensure the domain name service (DNS) is enabled on the server. Refer to procedure "Configuring Domain Name Service" in <i>ATM/IP Solution-level Configuration Management</i> , NN10409-500.

### Ensuring (I)SN07 Integrated EMS is installed

The Integrated EMS (I)SN07 Maintenance Release software or Integrated EMS (I)SN07 software with complete patch must be installed in the system or set must be installed. If you want to install Integrated EMS patches, refer to "Carrier Voice over IP Network Patching" of *Upgrading a Carrier Voice over IP Network*, NN10440-450.

## Upgrading Integrated EMS in a simplex configuration

The following procedure is to upgrade Integrated EMS software in NTRX51LC(COAM) simplex and NTRX51LC(COAM) duplex deployment sites.

**To upgrade Integrated EMS to a higher version, follow these steps:**

### *At the Integrated EMS Server system*

- 1 Log in at the console port as the root user at the server where the Integrated EMS Server needs to be upgraded.
- 2 Type the following command and press the Enter key to verify the status of the Integrated EMS Server:

```
# hostname://>servquery -status all
```

The output shows the services running on the unit.

```
APP NAME          STATUS
=====          =====
CINOTIFIER        RUNNING
DATABASE          RUNNING
IS                RUNNING
BOOTP             RUNNING
WEBSERVER         RUNNING
CORBA             RUNNING
OMPUSH           RUNNING
WEBSERVICES       RUNNING
ORA_AUTO_BACKUP   RUNNING
```

DELEGATE	RUNNING
ORA_ARCHIVE_ROTATOR	RUNNING
PROP_SRV	RUNNING
IEMS	RUNNING
SNMP_POLLER	RUNNING
RADSVR	RUNNING

- 3** Use the following table to determine your next step.

---

<b>If you are upgrading from a</b>	<b>Do</b>
CD	follow <a href="#">step 4</a>
directory	follow <a href="#">step 5</a>

---

***At the server***

- 4** Insert the CD that contains the IEMS software into the drive.

***At the server console***

- 5** Execute substep [a](#) or [b](#) according to whether you are upgrading from a CD or a directory.
- a** If you are upgrading from a CD, upgrade the IEMS software by typing
- ```
# cd /cdrom/cdrom0/bin/
```
- and pressing the Enter key.
- Run the appl\_mgr script by typing
- ```
# ./appl_mgr.ksh
```
- and pressing the Enter key.
- Proceed to [step 6](#).
- b** If you are upgrading from a directory, upgrade the CS2M software by typing
- ```
# cd /tmpmnt/bin/
```
- and pressing the Enter key.
- Run the appl\_mgr script by typing
- ```
# ./appl_mgr.ksh
```
- 6** Confirm that you want to continue the upgrade by typing "y" and pressing the Enter key.

The screen output lists the currently installed packages and confirms the upgrade.

The screen output then lists the contents of the Integrated EMS software package to be installed and is similar to the following screen shot:

```

NNaxl      VERSION: 3.25,v1
NNedu      VERSION: 1.3.2,v1
NNjre      VERSION: 1.4.2_04,v1
NNlog4cpp  VERSION: 0.3.4b,v1
NNlog4j    VERSION: 1.2.8,v1
NNnds      VERSION: 5.1_SP2_HF2,v1
NNnssaml   VERSION: 1.1.0,mip0400ac38
NNoro      VERSION: 2.0.7,v1
NNrad      VERSION: 1.1.0,mip0400ac38
NNrogwave  VERSION: sourcePro_6.0,v1
NNslixext  VERSION: 1.1.0,mip0400ac38
NNslix     VERSION: 6.0_SP1,v1
NNsecore   VERSION: 1.1.0,mip0400ac38
NNsecui    VERSION: 1.1.0,mip0400ac38
NNsisclt   VERSION: 1.1.0,mip0400ac38
NNswgmt    VERSION: MIP4.0.0,mip0400ac38
NNxercesc  VERSION: 2.3.0,v1
IEMS      I IEMS_8_45_0
NNCEMS180 18.0.165.0

```

- 7 Confirm the upgrade by typing "y" and pressing the Enter key.

Do you want to upgrade ? (y/n) y

A message appears which is similar to the following screen shot:

**Note:** The upgrade process may take thirty minutes or more depending on the user data.

```

Installing the new security server components...
Done installing the new security server components.

=====
Checking version of IEMS package...

Installing IEMS Package...
Done Installing IEMS Package.

Installing the CEM ...

=====
Upgrade of the IEMS software package completed successfully

Exporting data for migration
Configuring ... this will take 30 minutes or more depending on user data

```

- 8 To make the Integrated EMS patch current, refer to "Carrier Voice over IP Network Patching" of *Upgrading a Carrier Voice over IP Network*, NN10440-450.

- 9** If the Media Server 2000 devices must be managed, set up the BootP file. Refer to "[Setting up the BootP file on SSPFS](#)".

**Note:** Only perform this procedure if the Media Server 2000 is in your network and this set up was not previously executed as part of CMT configuration.

- 10** Verify there are no error logs in the location `/var/sadm/system/logs`.

- 11** Run the Config File Swap script.

If installation is done using CD, use the following command:

```
/cdrom/cdrom0/bin/switch08conf.ksh
```

If installation is done using ISO images, use the following command:

```
/tmpmnt/bin/switch08conf.ksh
```

Confirm the Config File Swap by typing "y" and then pressing the Enter key.

- 12** If the `nscd.conf`, `pam.conf`, and `nsswitch.conf` files were customized for your configuration, you must re-edit the files.

- 13** Run the Integrated EMS cleanup script on the active unit using the following commands:

```
cd /opt/nortel/iems/current/bin
./CleanUpSN07Data.sh
```

- 14** Remove the CD or ISO images associated with the (I)SN08 load installation. Select your next step:

If	Do
you are using a CD	use the <code>eject CD</code> command.
you are using an ISO image	refer to "Unmounting and removing an ISO image from an SSPFS-based server" of <i>Upgrading a Carrier Voice over IP Network</i> , NN10440-450.

- 15** If required, update the CEM documentation. Select your next step.

If	Do
you are using a CD	go to <a href="#">step 18</a>
you are using an ISO image	go to <a href="#">step 20</a>

- 16** Insert the CD that contains the CEM documentation into the drive.

- 17 Upgrade the CEM documentation by typing  

```
# pkgadd -d SScemhelp.pds
```

and pressing the Enter key.
- 18 Repeat [step 14](#) to eject the CD.
- 19 Repeat [step 10](#) and go to [step 17](#).
- 20 Mount the CEM help file. Refer to "Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server" of *Upgrading a Carrier Voice over IP Network*, NN10440-450.
- 21 Upgrade the CEM documentation by typing  

```
# pkgadd -d SScemhelp.pds
```

and pressing the Enter key.  
**Note:** To add the CEM to Integrated EMS, refer to "Integration of Core Element Manager with Integrated EMS" of *Integrated EMS Basics*, NN10329-111.
- 22 Start the Integrated EMS Server by entering the following command:  

```
servstart IEMS
```
- 23 After 3 minutes, issue the following command and check that Integrated EMS Server has started.  

```
servquery -status -group IEMS
```

If the Integrated Server has started, the following message is displayed to indicate that the upgrade was successful and Integrated EMS is in service:  

```
IEMS Instance is UP
```

After installing the (I)SN08 version of Integrated EMS, the migration is done when the Integrated EMS Server is started for the first time. The order of migration is mentioned in [Integrated EMS data migration order](#) section. If the migration fails, all the changes done for migrating the data of Integrated EMS alone revert to the original state as specified in the note on page [2](#).

If the migration fails, you can check for error messages the file IEMSDataMigration.log located under /home/opt/nortel/iems/current/logs.

### Integrated EMS data migration order

Integrated EMS data migration occurs in the following order:

- Security data migration
- Integrated EMS data migration
  - Database schema migration
  - Data migration
  - Configuration migration

### Upgrading Integrated EMS in an HA configuration

Use the following procedure to upgrade Integrated EMS software in Dual N240 (HA) 4G - NTRX51LC deployment sites. In HA and co-residency configurations, upgrades are carried out as follows:

All maintenance release upgrades are performed on the standby node while the active node is providing service. After the standby node of the cluster is upgraded and configured, perform a failover so the standby node becomes active. After determining that both nodes are functional, the newly active node with the maintenance release update can be cloned to the standby node. This ensures both nodes or units of the cluster have the same software and data image.

**To upgrade the Integrated EMS software in an HA configuration, follow these steps:**

#### ***At the Integrated EMS Server system***

- 1 Determine which cluster nodes are in standby so they can be upgraded with the maintenance release. Log into any of the cluster units at the console port as the root user and type the following command:

```
# bash
```

The unit prompt changes showing the unit you have logged into and its status as follows:

```
hostname-unit0(inactive) : />
```

If the unit you have logged into is active, log out and log back in to the other unit.

- 2 To query the status of cluster unit, type the following command:

```
hostname-unit0(inactive) : />ubmstat
```

The state of the ClusterIndicator is either active (ACT) or standby (STBY). Upgrade the unit in STBY mode first.

```
Group State
```

```
-----
ClusterIndicator STBY
```

- 3** Determine whether any applications are running on the STBY unit by typing the following command:

```
hostname-unit0(inactive) :/>servquery -status
all
```

The output shows the services running on the unit.

APP NAME	STATUS
=====	=====
CINOTIFIER	NOT RUNNING
DATABASE	NOT RUNNING
IS	NOT RUNNING
APS	NOT RUNNING
BOOTP	NOT RUNNING
WEBSERVER	NOT RUNNING
CORBA	NOT RUNNING
OMPUSH	NOT RUNNING
SESMService	NOT RUNNING
WEBSERVICES	NOT RUNNING
ORA_AUTO_BACKUP	NOT RUNNING
DELEGATE	NOT RUNNING
ORA_ARCHIVE_ROTATOR	NOT RUNNING
NPM	NOT RUNNING
PROP_SRV	NOT RUNNING
SAM21EM	NOT RUNNING
IEMS	NOT RUNNING
SNMP_POLLER	NOT RUNNING
RADSVR	NOT RUNNING

- 4** If any of the applications are running, stop the application by typing:

```
# servstop
```

and pressing the Enter key.

- 5** To disable failover for the inactive unit, follow the procedure "Removing a node from a cluster" of *Upgrading a Carrier Voice over IP Network*, NN10440-450.

- 6** Use the following table to determine your next step.

If you are upgrading from a	Do
CD	follow <a href="#">step 7</a>

---

<b>If you are upgrading from a</b>	<b>Do</b>
directory	follow <a href="#">step 8</a>

---

***At the server***

- 7 Insert the CD that contains the IEMS software into the drive.

***At the server console***

- 8 Execute substep [a](#) or [b](#) according to whether you are upgrading from a CD or a directory.

- a** If you are upgrading from a CD, upgrade the IEMS software by typing

```
# cd /cdrom/cdrom0/bin/
```

and pressing the Enter key.

Run the appl\_mgr script by typing

```
# ./appl_mgr.ksh
```

and pressing the Enter key.

Proceed to [step 9](#).

- b** If you are upgrading from a directory, upgrade the CS2M software by typing

```
# cd /tmpmnt/bin/
```

and pressing the Enter key.

Run the appl\_mgr script by typing

```
# ./appl_mgr.ksh
```

- 9 Confirm that you want to continue with the upgrade by typing "yes" and pressing the Enter key.

A message similar to the following screen shot appears:

```

NNaxl      VERSION: 3.25,v1
NNedu      VERSION: 1.3.2,v1
NNjre      VERSION: 1.4.2_04,v1
NNlog4cpp  VERSION: 0.3.4b,v1
NNlog4j    VERSION: 1.2.8,v1
NNnds      VERSION: 5.1_SP2_HF2,v1
NNnsssaml  VERSION: 1.1.0,mip0400ac38
NNoro      VERSION: 2.0.7,v1
NNrad      VERSION: 1.1.0,mip0400ac38
NNrogwave  VERSION: sourcePro_6.0,v1
NNs1isext  VERSION: 1.1.0,mip0400ac38
NNs1is     VERSION: 6.0_SP1,v1
NNseccore  VERSION: 1.1.0,mip0400ac38
NNsecui    VERSION: 1.1.0,mip0400ac38
NNsisc1t   VERSION: 1.1.0,mip0400ac38
NNswgmt    VERSION: MIP4.0.0,mip0400ac38
NNxercesc  VERSION: 2.3.0,v1
IEMS      IEMS_8_45_0
NNCEMS180 18.0.165.0

```

- 10 Confirm the upgrade by typing "y" and then pressing the Enter key.

Do you want to upgrade ? (y/n) y

A message appears similar to the following screen shot:

**Note:** The upgrade process may take thirty minutes or more depending on the user data.

```

Installing the new security server components...
Done installing the new security server components.

=====
Checking version of IEMS package...

Installing IEMS Package...
Done Installing IEMS Package.

Installing the CEM ...

=====
Upgrade of the IEMS software package completed successfully

Exporting data for migration
Configuring ... this will take 30 minutes or more depending on user data

```

- 11 To make the Integrated EMS patch current, refer to "Carrier Voice over IP Network Patching" of *Upgrading a Carrier Voice over IP Network*, NN10440-450.

- 12** If the Media Server 2000 devices must be managed, set up the BootP file. Refer to "[Setting up the BootP file on SSPFS](#)".

**Note:** Only perform this procedure if the Media Server 2000 is in your network and this set up was not previously executed as part of CMT configuration.

<b>If the Integrated EMS application</b>	<b>Do</b>
resides on a stand alone server	<a href="#">step 13</a>
resides on the SSPFS-based server with the CS 2000 Management Tools application	<a href="#">step 32</a>

- 13** To enable failover for the inactive unit, follow the procedure "Returning a node to a cluster" of *Upgrading a Carrier Voice over IP Network*, NN10440-450.

- 14** Verify the state of cluster using the procedure "Verifying the state of a cluster" of *Upgrading a Carrier Voice over IP Network*, NN10440-450.

This step should not return any output if everything is fine and ready for the next step. If this step returns any messages, you must contact support.

- 15** Stop the cluster using the procedure "Stopping a cluster" of *Upgrading a Carrier Voice over IP Network*, NN10440-450.

- 16** Verify there are no error logs in the location `/var/sadm/system/logs`.

- 17** Ensure that the Central Security Server is fully configured and running before proceeding to next step.

- 18** Wait for Integrated EMS to connect to the Central Security Server which may take up to twenty minutes.

- 19** Restart the Integrated EMS Server by typing:

```
# servrestart IEMS
```

and pressing the Enter key.

- 20** Run the Config File Swap script as follows:

If installation is done using CD, use the following command:

```
/cdrom/cdrom0/bin/switch08conf.ksh
```

If installation is done using ISO images, use the following command:

```
/tmpmnt/bin/switch08conf.ksh
```

Confirm the Config File Swap by typing "y" and then pressing the Enter key.

- 21** If the `nscd.conf`, `pam.conf`, and `nsswitch.conf` files were customized for your configuration, you must re-edit the files on the active and inactive units.
- 22** Run the Integrated EMS cleanup script on the active unit using the following commands:
- ```
cd /opt/nortel/iems/current/bin
./CleanUpSN07Data.sh
```
- 23** Remove the CD or ISO images associated with the (I)SN08 load installation. Select your next step:
- | If                         | Do                                                                                                                                            |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| you are using a CD         | use the <code>eject CD</code> command.                                                                                                        |
| you are using an ISO image | refer to "Unmounting and removing an ISO image from an SSPFS-based server" of <i>Upgrading a Carrier Voice over IP Network</i> , NN10440-450. |
- 24** If required, update the CEM documentation. Select your next step.
- | If                         | Do                            |
|----------------------------|-------------------------------|
| you are using a CD         | go to <a href="#">step 25</a> |
| you are using an ISO image | go to <a href="#">step 29</a> |
- 25** Insert the CD that contains the CEM documentation into the drive.
- 26** Upgrade the CEM documentation by typing
- ```
# pkgadd -d SScemhelp.pds
```
- and pressing the Enter key.
- 27** Repeat [step 23](#) to eject the CD.
- 28** Repeat [step 16](#) and go to [step 30](#).
- 29** Mount the CEM help file. Refer to "Transferring and mounting an ISO image delivered through ESD onto an SSPFS-based server" of *Upgrading a Carrier Voice over IP Network*, NN10440-450.
- 30** Upgrade the CEM documentation by typing
- ```
# pkgadd -d SScemhelp.pds
```

and pressing the Enter key.

**Note:** To add the CEM to Integrated EMS, refer to "Integration of Core Element Manager with Integrated EMS" of *Integrated EMS Basics*, NN10329-111.

- 31** To clone the inactive node to the active node so both nodes have same image, refer to "Cloning the image of one node in a cluster to the other node" of *Upgrading a Carrier Voice over IP Network*, NN10440-450.

**Note:** Ensure no provisioning activities are in progress, or are scheduled to take place during this step. This includes Integrated EMS Security administration actions that involve changes to the security database.

**Example**

Adding or changing user account information and adding or changing group information.

- 32** Procedure is complete.

After installing the (I)SN08 version of Integrated EMS, the migration is done when the Integrated EMS Server is started for the first time in the upgraded (I)SN08 unit becomes active. The order of migration is mentioned in [Integrated EMS data migration order](#) section. If the migration fails, all the changes done for migrating the data of Integrated EMS alone revert to the original state as specified in the note on page [2](#).

If the migration fails, you can check for error messages the file IEMSDataMigration.log located under /home/opt/nortel/iems/current/logs.

## Completing the Integrated EMS upgrade

The following table contains a summary of required post-upgrade procedures that has to be followed after upgrading to (I)SN08 Integrated EMS.

### Required post-upgrade procedures

| Requirement                                                                                                                                       | Procedure                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Clear the Java Web Start Client cache on client workstation.                                                                                   | Clear the Java Web Start Client cache to properly launch the Integrated EMS Client. To clear the Java Web Start Client cache, refer to "Clearing the JWS cache on a client workstation" in the <i>ATM/IP Solution-level Configuration Management</i> document, NN10409-500.                                                 |
| 2. Check whether the user group and user list are imported correctly.                                                                             | Verify that the user group and user lists have been imported correctly in the Integrated EMS Security and Administration GUI. Refer to "Listing all groups and users" of <i>Integrated EMS Security and Administration</i> , NN10336-611.                                                                                   |
| 3. Edit the object properties in the Integrated EMS for the Integrated SSPFS platform that you just upgraded to reflect the new software version. | Refer to either of the procedures that follow to update the software version in the Device Version field. <ul style="list-style-type: none"> <li>• <a href="#">Editing and viewing object properties using Java Web Client</a></li> <li>• <a href="#">Editing and viewing object properties using Web Client</a></li> </ul> |

---

## Setting up the BootP file on SSPFS

---

### Application

Use this procedure to set up the Succession Server Platform Foundation Software (SSPFS) platform as the bootp master and migrate the bootp entries from the core manager to the SSPFS platform.

**Note:** Only perform this procedure if the CS 2000 SAM21 Manager is in your network.

### Prerequisites

This procedure has the following prerequisites:

- the OpenSSH fileset on the core manager must be APPLIED

**Note:** You can verify whether the OpenSSH fileset is APPLIED using command “sdmmtc details” at the core manager. If it is not applied, refer to procedure “Installing or upgrading OpenSSH” in *Upgrading the CS 2000 Core Manager*, NN10060-461.

- you need the password for the root user on the core manager (SDM)
- you need the IP address of the core manager (SDM)

**Note:** You can obtain the IP address of the core manager (SDM) using command “sdmmtc eth” at the core manager. Use the IP address associated with the host name of the core manager, which is the first one.

## Action

Perform the following steps to complete this procedure.

### *At your workstation*

- 1 Telnet to the CS 2000 Management Tools server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

#### **server**

is the IP address or hostname of the CS 2000 Management Tools server

- 2 When prompted, enter your user ID and password.

- 3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

- 4 When prompted, enter the root password.

- 5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

### *Response*

```
Command Line Interface
```

```
1 - View
```

```
2 - Configuration
```

```
3 - Other
```

```
X - exit
```

```
select -
```

- 6 Configure the IP address of the core manager (SDM) as follows:
  - a Enter the number next to the "Configuration" option in the menu.

*Example response*

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)

X - exit

Select -
```

- b** Enter the number next to the “OAMP Application Configuration” option in the menu.

*Example response*

```
OAMP Application Configuration
1 - sdm_conf (Configure SDM IP Address)
2 - sdm_unconf (Unconfigure SDM IP Address)
3 - sdmuser_conf (Configure SDM User)
4 - sdmuser_unconf (Unconfigure SDM User)
5 - cmClli_rediscovery (Re-discover the CM
  CLLI by SDM IP)
6 - cmClli_conf (Configure CM_CLLI Address)
7 - cmClli_unconf (Unconfigure CM_CLLI IP
  Address)
8 - cm_conf (Configure CM IP Address)
9 - cm_unconf (Unconfigure CM IP Address)

X - exit
```

```
select -
```

- c** Enter the number next to the “sdm\_conf” option in the menu.

*Example response*

```
===Executing "sdm_conf"
```

```
Enter the ip address of the SDM []
```

- d** When prompted, enter the IP address of the core manager (SDM).

*Example response*

```
Retrieving CM CLLI. Please wait...
```

```
SDM IP: 47.152.34.56
CM CLLI: OFFICE3
```

```
Enter "ok" to accept current settings
```

- e** When prompted, confirm the current settings by typing

```
ok
```

and pressing the Enter key.

- 7** Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

- 8 For the SAM21 Manager user, generate the ssh key pair needed for data transmission between the SAM21 Manager and the CS 2000 Core Manager by typing

```
# keygen.sh sam21em
```

and pressing the Enter key.

*Example response*

```
Generating public/private rsa key pair.  
Enter file in which to save the key  
(/export/home/sam21em/.ssh/id_rsa):
```

- 9 When prompted, press the Enter key to accept the default location and filename “/export/home/sam21em/.ssh/id\_rsa” for the key.

**Note 1:** If the default location and filename is not provided, enter “/export/home/sam21em/.ssh/id\_rsa”.

**Note 2:** If the location and filename “/export/home/sam21em/.ssh/id\_rsa” already exists and you wish to overwrite, type **y** and press the Enter key. Otherwise, type **n**.

*Example response*

```
Your identification has been saved in  
/export/home/sam21em/.ssh/id_rsa.  
Your public key has been saved in  
/export/home/sam21em/.ssh/id_rsa.pub.  
The key fingerprint is:  
21:cb:c6:7f:df:05:f8:4a:2f:23:e9:09:c8:37  
bc:1e sam21em@znc0s0j6
```

```
The authenticity of host '47.142.128.16  
(47.142.128.16)' can't be established. RSA key  
fingerprint is  
21:cb:c6:7f:df:05:f8:4a:2f:23:e9:09:c8:37  
bc:1e sam21em@znc0s0j6  
Are you sure you want to continue connecting  
(yes/no)?
```

- 10 When prompted, confirm you want to continue connecting by typing

```
# yes
```

and pressing the Enter key.

*Example response:*

```
Warning: Permanently added '47.142.128.16'  
(RSA) to the list of known hosts.  
root@47.142.128.16's password:
```

- 11** When prompted, enter the password for the SDM root user.
- 12** When prompted, enter the password for the SDM root user again.

*Example response:*

```
Successfully performed bootptab manipulation  
Synchronizing files IF clustered node
```

Once complete, the SAM21 Manager application will have access to the needed directories and files on the core manager.

- 13** You have completed this procedure.

---

## Editing and viewing object properties using Java Web Client

---

### Application

Use this procedure to edit or view the properties of objects that are displayed in the IEMS topology using Java Web Client.

### Prerequisites

None

### Action

#### *At the IEMS workstation*

- 1 Launch the IEMS Java Web Start Client. Refer to Launching IEMS Java Web Start Client in *Integrated EMS Basics*, NN10329-111.
- 2 Select the required object in the Integrated EMS Topologies tree under Applications.

**Note:** The properties of an object from the Inventory panel of Integrated EMS tree can also be viewed. To view the Inventory object properties, select the object in the Integrated Topologies tree under Applications to open the Inventory view. Double-click the required row in the Inventory view.

- 3 Right-click the map symbol and select the **Managed Object Properties** menu item or double-click the map symbol to open the Object Properties window.

**Note:** The object properties displayed can differ for each component.

*A window similar to the following figure opens.*

**Object Properties** ----iems-sf2

**Base Properties**

Name: raghuram-SAM21-Mgr  
 Display Name: raghuram  
 Type: SAM21 Mgr  
 Status: Unknown  
 IP-Address: 192 . 168 . 118 . 160  
 Platform: None  
 Managed:   
 Time Zone: Etc/GMT+12  
 Device Version: 8.0  
 Enable System Unmanage:   
 Fault Interface State: NORMAL

**Other Properties**

Poll Interval (In seconds): 300  
 Status Change Time: Tue Mar 01 07:29:43 GMT+05:30 2005

Back Next  
 Modify Help Close  
 Done

- 4 Modify the object properties listed in the table below if required.

#### Managed object properties in Java Web Client

| Field        | Description                                                            |
|--------------|------------------------------------------------------------------------|
| Name         | Displays a unique name for the object                                  |
| Display Name | Edit the name displayed in the topology for the object                 |
| Type         | Displays the type of object (element manager, EMS, EMS platform or NE) |
| Status       | Displays the status of the object                                      |
| IP-Address   | Edit the IP address of the object                                      |

## Managed object properties in Java Web Client

| Field                                                                                                                                                                                                                                                                                        | Description                                                                                                                                                                                                  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Platform                                                                                                                                                                                                                                                                                     | Select the platform where the object resides from the drop-down list                                                                                                                                         |
| Managed                                                                                                                                                                                                                                                                                      | Indicates whether the object is managed or unmanaged                                                                                                                                                         |
| Time Zone                                                                                                                                                                                                                                                                                    | Select the time zone of the geographical location where the object exists from the drop-down list                                                                                                            |
| Device Version                                                                                                                                                                                                                                                                               | Select the device version of the managed object from the drop-down list                                                                                                                                      |
| Enable System Unmanage                                                                                                                                                                                                                                                                       | Enable or disable the System_Unmanaged state. Refer to the System_Unmanaged state section of Configuring the Message Overload Controller parameters in <i>Integrated EMS Fault Management</i> , NN10334-911. |
| Poll Interval                                                                                                                                                                                                                                                                                | Edit the Poll Interval for status updates                                                                                                                                                                    |
| Status Change Time                                                                                                                                                                                                                                                                           | Displays the last status change time of the object                                                                                                                                                           |
| <p><b>Note:</b> For the following objects, only the Display Name and the Managed field can be modified.</p> <ul style="list-style-type: none"> <li>SDM platform, APS EMS application, CS 2000 Core, Call Agent Core, IMX/CSE MX, Media Proxy, Media Gateway 7480/15000, MSS 15000</li> </ul> |                                                                                                                                                                                                              |

5 Select your next step.

| If                                                                                 | Do                           |
|------------------------------------------------------------------------------------|------------------------------|
| you do not want to modify any other properties                                     | go to <a href="#">step 6</a> |
| you want to view or modify the fault interface or performance interface properties | go to <a href="#">step 8</a> |

6 Click the **Modify** button to update the changes.

7 Go to [step 16](#).

8 Click the **Next** button to proceed to the Fault Interface window.  
*A window similar to the following figure opens.*

- 9 Edit or view the fault interface properties of the object as required.

**Note:** The Details panel dynamically changes according to the fault interface of the EMS/NE.

- 10 Select your next step.

| If                                                              | Do                      |
|-----------------------------------------------------------------|-------------------------|
| you do not want to modify any other properties                  | <a href="#">step 11</a> |
| you want to view or modify the performance interface properties | <a href="#">step 13</a> |

- 11 Click the **Modify** button to update the changes.

- 12 Go to [step 16](#).
- 13 Click the **Next** button to proceed to the Performance Interface window.

*A window similar to the following figure opens.*

Object Properties ---- Nortel

Performance Interface

SNMP Details

Port 161

Community

Version v3

V3 Security Details

Security Level NoAuthNoPriv

User name v3admin Context name saul

Auth Protocol MD5 Auth Password

Privacy Protocol CBC-DES Privacy Password

Back Next

Modify Help Close

Done

- 14 Edit or view the performance interface properties of the object as required.
- 15 Click the **Modify** button to update the changes.
- 16 You have completed this procedure.

---

## Editing and viewing object properties using Web Client

---

### Application

Use this procedure to modify or view the properties of an object in the IEMS topology using Web Client.

### Prerequisites

None

### Action

#### *At the IEMS workstation*

- 1 Launch the IEMS Web Client. Refer to Launching the IEMS Web Client in *IEMS Basics*, NN10329-111.
- 2 Select the **Integrated EMS Topologies** tab.
- 3 Navigate to the required topology node in the Integrated EMS Topologies tree.
- 4 Click the map symbol label to open the **General Information** window.

**Note:** The object properties displayed can differ for each component.

*A window similar to the following figure opens.*

Integrated EMS Topologies → Network Elements

←AMS2 **rajagopal-MS2000**

 General

 Monitoring

 Fault Interface

 Performance Interface

**General Information**

|                |                                                                                           |
|----------------|-------------------------------------------------------------------------------------------|
| Name           | rajagopal-MS2000                                                                          |
| Device Type    | NE-MS2000                                                                                 |
| Status         |  Clear |
| Is Managed ?   | <input checked="" type="radio"/> Yes <input type="radio"/> No                             |
| Display Name   | <input type="text" value="raj"/>                                                          |
| Device Version | <input type="text" value="8.0"/>                                                          |
| IP Address     | <input type="text" value="192.168.113.201"/>                                              |
| Web User Name  | <input type="text" value="rajagopal"/>                                                    |
| Web Password   | <input type="password" value="****"/>                                                     |

- 5 Select each vertical tab and modify the object properties listed in the table below if required.

### Managed object properties in Web Client

| Field          | Description                                                            |
|----------------|------------------------------------------------------------------------|
| <b>General</b> |                                                                        |
| Name           | Displays the unique object name of the managed object                  |
| Device Type    | Displays the type of object (element manager, EMS, EMS platform or NE) |
| Status         | Displays the status of the object                                      |
| Is Managed?    | Indicates whether the object is managed or unmanaged                   |
| Display Name   | Displays the name or label displayed in map symbol                     |
| Device Version | Select the version of the device from the drop-down list               |

**Managed object properties in Web Client**

| <b>Field</b>                   | <b>Description</b>                                                   |
|--------------------------------|----------------------------------------------------------------------|
| IP Address                     | Modify the IP address of the object                                  |
| Web User name                  | Enter your web user name                                             |
| Web Password                   | Enter your web password                                              |
| <b>Monitoring</b>              |                                                                      |
| Last Status Update Time        | Displays the time when the status of the managed object last changed |
| Last Status Change Time        | Displays the time when the status of the managed object last changed |
| Status Polling Interval (secs) | Modify the Poll Interval for status updates                          |

**Managed object properties in Web Client**

| <b>Field</b>                 | <b>Description</b>                                                               |
|------------------------------|----------------------------------------------------------------------------------|
| <b>Fault Interface</b>       | If the details are present for the selected object, the details can be modified. |
| <b>Performance Interface</b> | If the details are present for the selected object, the details can be modified. |

- 6** Click the **Update Object** button to update the changes.
- 7** You have completed this procedure.

## Downgrading the IEMS software

---

This section provides the information required to roll back a software upgrade and revert to the previous release of the software.

**Note:** It is highly recommended that all console and telnet sessions used during rollbacks, be logged to a file to assist in any necessary troubleshooting.

### Downgrading to (I)SN07

Follow the link according to your office configuration.

- [Rollback on Sun Netra t1400 or Sun Netra 240 one-server configuration on page 32](#)
- [Rollback on Sun Netra 240 two-server configuration on page 33](#)

## Rollback on Sun Netra t1400 or Sun Netra 240 one-server configuration



### CAUTION Service interruption

All of the applications on the server will be out of service for the duration of the downgrade. Therefore, it is recommended to involve the proper support groups and explore other options before proceeding with the downgrade.

Use the table below as a checklist during the rollback of the SSPFS and IEMS software to (I)SN07. Place a check (✓) in the ✓ column as you complete each procedure.

### Downgrading a Sun Netra t1400 or Sun Netra 240 (one-server configuration) to (I)SN07

| Activities                                                                                                                                                                                           | ✓ | Procedures                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|----------------------------------------------------------------------------------------------------------|
| 1 Restore the file systems and Oracle data from backup media.                                                                                                                                        |   | Refer to procedure <a href="#">Performing a full system restore on an SSPFS-based server on page 35.</a> |
| 2 Clear the Java™ Web Start (JWS) cache on the client workstation.<br><br><b>Note:</b> Only perform this activity if the IEMS is on the same server as the CS 2000 Management Tools (CS2M) software. |   | Refer to procedure <a href="#">Clearing the JWS cache on a client workstation on page 59.</a>            |

**Note:** Restoring the file systems and Oracle data from backup media, restores your system as it was before the upgrade to (I)SN08.

### Rollback on Sun Netra 240 two-server configuration

Follow the link according to whether only one server in the cluster was upgraded to (I)SN08, or both servers in the cluster were upgraded to (I)SN08.

- [Downgrading the only upgraded server in the cluster on page 33](#)
- [Downgrading both upgraded servers in the cluster on page 34](#)

### Downgrading the only upgraded server in the cluster

Use the table below as a checklist during the rollback of the SSPFS and IEMS software to (I)SN07 on the only upgraded server. Place a check (√) in the √column as you complete each procedure.

### Downgrading the only upgraded server to (I)SN07

| Activities                                                                                  | √ | Procedures                                                                                                   |
|---------------------------------------------------------------------------------------------|---|--------------------------------------------------------------------------------------------------------------|
| 1 Clone the image of the server with the (I)SN07 software onto the other (upgraded) server. |   | Refer to procedure <a href="#">Cloning the image of one node in a cluster to the other node on page 47</a> . |

**Note:** Cloning the image of the (I)SN07 server onto the server that was upgraded, restores the server as it was before the upgrade to (I)SN08.

## Downgrading both upgraded servers in the cluster



### CAUTION Service interruption

All of the applications on the server will be out of service for the duration of the downgrade. Therefore, it is recommended to involve the proper support groups and explore other options before proceeding with the downgrade.

Use the table below as a checklist during the rollback of the SSPFS and IEMS software to (I)SN07 on both upgraded servers. Place a check (√) in the √column as you complete each procedure.

### Downgrading both upgraded servers to (I)SN07

| Activities                                                                                                                                                                                           | √ | Procedures                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|-------------------------------------------------------------------------------------------------------------|
| 1 Restore the file systems and Oracle data from backup media.                                                                                                                                        |   | Refer to procedure <a href="#">Performing a full system restore on an SSPFS-based server on page 35.</a>    |
| 2 Clone the image of the server you just downgraded to (I)SN07, onto the other server.                                                                                                               |   | Refer to procedure <a href="#">Cloning the image of one node in a cluster to the other node on page 47.</a> |
| 3 Clear the Java™ Web Start (JWS) cache on the client workstation.<br><br><b>Note:</b> Only perform this activity if the IEMS is on the same server as the CS 2000 Management Tools (CS2M) software. |   | Refer to procedure <a href="#">Clearing the JWS cache on a client workstation on page 59.</a>               |

**Note:** Restoring the file systems and Oracle data from backup media, restores your system as it was before the upgrade to (I)SN08.

---

## Performing a full system restore on an SSPFS-based server

---

### Application

Use this procedure to perform a full system restore from backup media on a Succession Server Platform Foundation Software (SSPFS)-based server (Sun Netra t1400 or Sun Netra 240).

A full system restore consists of reverting to the previous release of SSPFS, restoring the file systems, and restoring the oracle data.

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager
- Core Billing Manager (CBM)

**Note:** Restoring the oracle data does not apply to the CBM as it does not use an oracle database.

#### ATTENTION

System logs indicating application and database errors generate until the file systems and oracle data are restored on the system using this procedure and procedure [Restoring the oracle data on an SSPFS-based server on page 41](#). No database errors generate on the CBM as it does not use an oracle database.

### Prerequisites

This procedure has the following prerequisites:

- SSPFS CD disk#1 for the release you are reverting to
- tape, CD or DVD on which you backed up the file systems
- tape, CD or DVD on which you backed up the oracle data

## Action

Use one of the methods below according to your office configuration.

- [Simplex configuration \(one server\) on page 36](#)
- [High-availability configuration \(two servers\) on page 38](#)

**Note:** Only the [Simplex configuration \(one server\)](#) uses a full system restore from tape on a Sun Netra t1400 server.

### Simplex configuration (one server)

#### At the server console

- 1 Log in to the server through the console (port A) using the root user ID and password.
- 2 Bring the system to the OK prompt by typing  
# **init 0**  
and pressing the Enter key.
- 3 Insert SSPFS CD disk#1 into the drive.

| If restoring from | Do                     |
|-------------------|------------------------|
| tape              | <a href="#">step 4</a> |
| CD or DVD         | <a href="#">step 5</a> |

- 4 Insert the tape with the backed up file systems into the drive.
- 5 At the OK prompt, restore the system by typing  
OK **boot cdrom - restore**  
and pressing the Enter key.
- 6 When prompted, accept the software license restrictions by typing  
**ok**  
and pressing the Enter key.

The system reboots.

If restoring from CD or DVD, you will be prompted to insert Volume 1 of the backup CD or DVD into the drive. Insert the CD or DVD on which you backed up the file systems. During the restore process, the system will prompt you for additional Volumes if more than one CD or DVD was used during the backup of file systems.

The restore process can take several hours to complete depending on the number and size of the files that are being restored.

**Note:** Although it can appear as if the system is hanging at times, please do not interrupt the restore process. If you suspect an issue with the restore process, please contact your next level of support.

**7** Eject the backup CD or DVD from the drive as follows:

**a** Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

**b** Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

**Note:** If the DVD drive tray does not open (if not busy or being read from or written to), enter the following commands:

```
# /etc/init.d/volmgt stop
```

```
# /etc/init.d/volmgt start
```

Then, press the eject button located on the front of the DVD drive.

**c** Remove the backup CD or DVD from the drive.

**8** Proceed as follows:.

| If                                         | Do                      |
|--------------------------------------------|-------------------------|
| this SSPFS-based server is hosting the CBM | <a href="#">step 12</a> |
| otherwise                                  | <a href="#">step 9</a>  |

**9** List the oracle groups by typing

```
# groups oracle
```

and pressing the Enter key.

| If the output is                       | Do                      |
|----------------------------------------|-------------------------|
| oinstall data dba or oinstall dba data | <a href="#">step 10</a> |
| oinstall dba data                      | <a href="#">step 11</a> |

- 10 Correct the oracle groups by typing  

```
# usermod -g oinstall -G data,dba oracle
```

and pressing the Enter key.
- 11 Restore the oracle data using procedure [Restoring the oracle data on an SSPFS-based server on page 41](#). Once the data restore is complete, continue to [step 12](#).
- 12 Reboot the server by typing  

```
# init 6
```

and pressing the Enter key.
- 13 The procedure is complete.

### High-availability configuration (two servers)

#### *At the console connected to the inactive node*

- 1 Log in to the inactive node through the console (port A) using the root user ID and password.
- 2 Bring the system to the OK prompt by typing  

```
# init 0
```

and pressing the Enter key.

#### *At the console connected to the active node*

- 3 Log in to the active node through the console (port A) using the root user ID and password.
- 4 Access the OK prompt by typing  

```
# init 0
```

and pressing the Enter key.
- 5 Insert SSPFS CD disk#1 into the drive.
- 6 At the OK prompt, restore the system by typing  

```
OK boot cdrom - restore
```

and pressing the Enter key.
- 7 When prompted, accept the software license restrictions by typing  

```
ok
```

and press the Enter key.  
The system reboots.

- 8** When prompted, insert Volume 1 of the CD or DVD on which you backed up the file systems, into the drive.

**Note:** During the restore process, the system will prompt you for additional Volumes if more than one CD or DVD was used during the backup of file systems.

The restore process can take several hours to complete depending on the number and size of the files that are being restored.

**Note:** Although it can appear as if the system is hanging at times, please do not interrupt the restore process. If you suspect an issue with the restore process, please contact your next level of support.

- 9** Eject the backup CD or DVD from the drive as follows:

- a** Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

- b** Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

**Note:** If the DVD drive tray does not open (if not busy or being read from or written to), enter the following commands:

```
# /etc/init.d/volmgt stop
```

```
# /etc/init.d/volmgt start
```

Then, press the eject button located on the front of the DVD drive.

- c** Remove the backup CD or DVD from the drive.

- 10** Use the following table to determine your next step.

| If                                         | Do                      |
|--------------------------------------------|-------------------------|
| this SSPFS-based server is hosting the CBM | <a href="#">step 14</a> |
| otherwise                                  | <a href="#">step 11</a> |

- 11** List the oracle groups by typing  
**# groups oracle**  
and pressing the Enter key.

| If the output is                          | Do                      |
|-------------------------------------------|-------------------------|
| oinstall data dba or oinstall<br>dbs data | <a href="#">step 12</a> |
| oinstall dba data                         | <a href="#">step 13</a> |

- 12** Correct the oracle groups by typing  
**# usermod -g oinstall -G data,dba oracle**  
and pressing the Enter key.
- 13** Restore the data using procedure [Restoring the oracle data on an SSPFS-based server on page 41](#). Once the data restore is complete, execute [step 14](#) and [step 15](#) .
- 14** Reboot the server by typing  
**# init 6**  
and pressing the Enter key.
- 15** Re-image the inactive node using the active node's image. If required, refer to procedure [Cloning the image of one node in a cluster to the other node](#).  
You have completed this procedure.

---

## Restoring the oracle data on an SSPFS-based server

---

### Application

Use this procedure to restore the oracle data from a backup tape, CD or DVD on a Succession Server Platform Foundation Software (SSPFS)-based server (Sun Netra t1400 or Sun Netra 240). Also use this procedure to restore the data that was automatically backed up to a file on the server by the backup restore manager.

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager
- Core Billing Manager (CBM)

**Note:** Restoring the oracle data is not applicable to the CBM as it does not use an oracle database.

### Prerequisites

This procedure requires the oracle data backup tape, CD or DVD. If the data was saved through the backup restore manager, the name of the file located in directory “/data/bkresmgr/backup” is required.

## Action

Perform the following steps to complete this procedure.

### *At the server*

- 1 Insert the tape, CD or DVD containing the oracle data backup into the drive. If restoring the data from a file, start at [step 2](#).

### *At your workstation*

- 2 Log in to the server by typing  

```
> telnet <server>
```

 and pressing the Enter key.  
 where  
     **server**  
     is the IP address or host name of the SSPFS-based server on which you are performing the data restore
- 3 When prompted, enter your user ID and password.
- 4 Change to the root user by typing  

```
$ su - root
```

 and pressing the Enter key.
- 5 When prompted, enter the root password.
- 6 Verify the permissions on the restore log directory (bkslog) by typing  

```
# ls -alrt /var/opt/nortel
```

 and pressing the Enter key.

#### *Example response*

```
total 22
lrwxrwxrwx  1 root  succsn      28 Dec 22  2003 gwc
-> /net/47.141.126.131//swd/gwc
drwxrwxr-x  4 root   other        512 Dec 22  2003 .
drwxr-xr-x  7 root   sys          512 Sep 10 12:41 ..
drwxr-xr-x  2 oracle oinstall    512 Dec  8 15:58 db
drwxrwxrwt  2 root   other        6656 Dec 15 19:56 bkslog
```

| If the permissions of bkslog | Do                     |
|------------------------------|------------------------|
| are drwxrwxrwt               | <a href="#">step 8</a> |
| are not drwxrwxrwt           | <a href="#">step 7</a> |

- 7 Change the permissions of bkslog by typing  
# **chmod 777 /var/opt/nortel/bkslog**
- 8 If not already done, stop the server applications that run on the server.

| For                                              | Refer to                                                       |
|--------------------------------------------------|----------------------------------------------------------------|
| CS 2000 Management Tools server applications     | <i>ATM/IP Security and Administration</i> ,<br>NN10402-600     |
| MG 9000 Manager and mid-tier server applications | the <i>MG9000 Security and Administration</i> ,<br>NN10162-611 |
| Integrated EMS server application                | <i>IEMS Security and Administration</i> ,<br>NN10336-611       |

- 9 Use the following table to determine your next step.

| If                             | Do                        |
|--------------------------------|---------------------------|
| restoring from tape, CD or DVD | substep <a href="#">a</a> |
| restoring from a file          | substep <a href="#">b</a> |

- a Restore the database from backup tape, CD or DVD by typing  
\$ **/opt/nortel/sspfs/bks/rsdata**  
and pressing the Enter key.  
Proceed to [step 10](#).

- b** Restore the database from the backup file by typing

```
$ /opt/nortel/sspfs/bks/rsdata -f  
/data/bkresmgr/backup/<filename>
```

and pressing the Enter key.

*where*

**filename**

is the name of the backup file created by the backup restore manager

Proceed to [step 11](#).

- 10** Remove the tape from the drive, or eject the CD or DVD from the drive as follows:

- a** Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

- b** Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

**Note:** If the DVD drive tray does not open (if not busy or being read from or written to), then enter the following commands:

```
# /etc/init.d/volmgt stop
```

```
# /etc/init.d/volmgt start
```

Press the eject button located on the front of the DVD drive.

- c** Remove the CD or DVD from the drive.

- 11** Verify that the database restored properly.

**12** Start the server applications that run on the server.

| <b>For</b>                                       | <b>Refer to</b>                                                |
|--------------------------------------------------|----------------------------------------------------------------|
| CS 2000 Management Tools server applications     | <i>ATM/IP Security and Administration</i> ,<br>NN10402-600     |
| MG 9000 Manager and mid-tier server applications | the <i>MG9000 Security and Administration</i> ,<br>NN10162-611 |
| Integrated EMS server application                | <i>IEMS Security and Administration</i> ,<br>NN10336-611       |

You have completed this procedure.



## Cloning the image of one node in a cluster to the other node

### Application

Use this procedure to clone the image of the active node in a cluster to the inactive node.

### Prerequisites

This procedure has the following prerequisites:

- you need the root user ID and password
- you need console access to the Inactive node if this is the first time you clone, or if you replaced the Inactive unit or executed a reverse restore (switched unit 0 and 1)

#### ATTENTION

Ensure no provisioning activities are in progress, or are scheduled to take place during this procedure.

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Establish a login session to the Active node using one of the following methods:

| If using          | Do                     |
|-------------------|------------------------|
| telnet (unsecure) | step <a href="#">2</a> |
| ssh (secure)      | step <a href="#">3</a> |

- 2 Log in to the Active node using telnet (unsecure) as follows:
  - a Log in to the Active node by typing
 

```
> telnet <server>
```

 and pressing the Enter key.  
 where  
**server**  
 is the cluster IP address, which automatically defaults to the Active node in the cluster
  - b When prompted, enter your user ID and password.



**5** Determine the server profile as follows:**a** Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

*Example response*

```
Command Line Interface
```

```
1 - View
2 - Configuration
3 - Other
```

```
X - exit
```

```
select -
```

**b** Enter the number next to the “View” option in the menu.*Example response*

```
View
```

```
1 - sspfs_soft (Display Software
Installation Level Of SSPFS)
2 - chk_sspfs (Check SSPFS Processes)
3 - sw_conf (The software configuration of
the wrtypyxp)
4 - cpu_util (Overall CPU utilization)
5 - cpu_util_proc (CPU utilization by
process)
6 - port_util (I/O port utilization)
7 - disk_util (Filesystem utilization)
```

```
X - exit
```

```
select -
```

**c** Enter the number next to the “sspfs\_soft” option in the menu.*Example response*

```
=== Executing "sspfs_soft"
```

```
SSPFS version: 08.0 Build: 200508421 Server
Profile: cbm850
```

```
=== "sspfs_soft" completed successfully
```

d Note the Server Profile.

| If the Server Profile is | Do                      |
|--------------------------|-------------------------|
| cbm850                   | step <a href="#">16</a> |
| anything else            | step <a href="#">6</a>  |

6 Verify that all applications on the server are running by typing

```
# servquery -status all
```

and pressing the Enter key.

*Example response:*

```
APP NAME                STATUS
=====                =====
SNMP_POLLER             RUNNING
DELEGATE                 RUNNING
PROP_SRV                RUNNING
WEBSERVER                RUNNING
DATABASE                 RUNNING
SAM21EM                  RUNNING
SESMSservice            RUNNING
CORBA                    RUNNING
ORA_ARCHIVE_ROTATOR     RUNNING
OMPUSH                   RUNNING
BOOTP                    RUNNING
WEBSERVICES              RUNNING
ORA_AUTO_BACKUP         RUNNING
APS                       RUNNING
NPM                       RUNNING
```

7 Use the following table to determine your next step.

| If                                       | Do                      |
|------------------------------------------|-------------------------|
| all applications are running             | step <a href="#">10</a> |
| one or more applications are not running | step <a href="#">8</a>  |

8 Start each application that is not running by typing

```
# servstart <app_name>
```

and pressing the Enter key.

*where*

**app\_name**

is the name of the application that is not in a “RUNNING” state, for example, SAM21EM

- 9 Use the following table to determine your next step.

| If                                    | Do                                 |
|---------------------------------------|------------------------------------|
| one or more applications do not start | contact your next level of support |
| all applications are running          | step <a href="#">10</a>            |

- 10 Use the following table to determine your next step.

| If this server is            | Do                      |
|------------------------------|-------------------------|
| running the NPM software     | step <a href="#">11</a> |
| not running the NPM software | step <a href="#">13</a> |

**Note:** The Network Patch Manager (NPM) software is running on this server if NPM appeared in the response from step [6](#).

- 11 Verify the Patching Server Element (PSE) server application is running by typing

```
# pse status
```

and pressing the Enter key.

| If PSE is   | Do                      |
|-------------|-------------------------|
| running     | step <a href="#">13</a> |
| not running | step <a href="#">12</a> |

- 12 Start the PSE server application by typing

```
# pse start
```

and pressing the Enter key.

| If PSE         | Do                                 |
|----------------|------------------------------------|
| does not start | contact your next level of support |
| starts         | step <a href="#">13</a>            |

- 13** Use the following table to determine your next step.

| If this server is                                 | Do                      |
|---------------------------------------------------|-------------------------|
| running the CS 2000 Management Tools software     | step <a href="#">14</a> |
| not running the CS 2000 Management Tools software | step <a href="#">16</a> |

- 14** Verify that the SESMservice application is fully functional by typing

```
# ptmctl status
```

and pressing the Enter key.

*Example response:*

```
SESM STATUS
```

```
-----
COMPONENT                STATUS
-----                -
Proxy Agent              RUNNING
RMI Registry             RUNNING
Snmpfactory              RUNNING
MI2 Server               RUNNING
```

```
Current number of SESM processes running: 4 (of 4)
```

```
SESM APPLICATION STATUS: All Applications ready
```

- 15** Use the following table to determine your next step.

| If the SESMService is | Do                                 |
|-----------------------|------------------------------------|
| not fully functional  | contact your next level of support |
| fully functional      | step <a href="#">16</a>            |

- 16 Use the following table to determine your next step.

| If                                                                                                                                                   | Do                      |
|------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| this is the first time you are cloning the unit, or you replaced the unit or executed a reverse restore (i.e. switched unit 0 and unit 1)            | step <a href="#">17</a> |
| this is not the first time you are cloning the unit, and you did not replace the unit or execute a reverse restore (i.e. switched unit 0 and unit 1) | step <a href="#">20</a> |

- 17 Use the following table to determine your next step.

| If you                                                | Do                      |
|-------------------------------------------------------|-------------------------|
| know the Ethernet address of the Inactive unit        | step <a href="#">19</a> |
| do not know the Ethernet address of the Inactive unit | step <a href="#">18</a> |

***At the console connected to the inactive node***

- 18 Determine the Ethernet address of the Inactive node as follows:

- a Log in to the inactive node through the console (port A) using the root user ID and password.

**Note:** Ensure you are on the Inactive server by typing `ubmstat`. If `ClusterIndicatorACT` is displayed in the response, which indicates you are on the Active server, log out of that server and log in to the other server. The response must display `ClusterIndicatorSTBY`, which indicates you are on the Inactive server.

- b Bring the system to the OK prompt by typing

```
# init 0
```

and pressing the Enter key.

- c At the OK prompt, display the Ethernet address of the inactive node by typing

OK **banner**

and pressing the Enter key.

*Example response:*

```
Sun Fire V240, No keyboard
Copyright 1998-2002 Sun Microsystems, Inc.
All rights reserved. OpenBoot 4.8.0.build_04,
2048 MB memory installed, Serial #52964131.
Ethernet address 0:3:ba:28:2b:23, Host ID:
83282b23.
```

- d Take note of the Ethernet address that is displayed.

**At your workstation (login session to the Active node)**

- 19 Start the cloning process by typing

# **startb <Ethernet address>**

and press the Enter key.

where

**Ethernet address**

is the Ethernet address of the Inactive unit

Proceed to step [21](#)

- 20 Start the cloning process by typing

# **startb**

and press the Enter key.

- 21 Use the following table to determine your next step.

| If the system                                               | Do                      |
|-------------------------------------------------------------|-------------------------|
| prompts you to enter the command "boot net - image"         | step <a href="#">22</a> |
| does not prompt you to enter the command "boot net - image" | step <a href="#">26</a> |

- 22 Connect to the console port of the Inactive node.

| If the console displays | Do                      |
|-------------------------|-------------------------|
| the OK prompt           | step <a href="#">25</a> |
| the login prompt        | step <a href="#">23</a> |

***At the console connected to the inactive node***

- 23** Log in using the root user ID and password.
- 24** Bring the system to the OK prompt by typing  
`# init 0`  
and pressing the Enter key.
- 25** At the OK prompt, boot the inactive node from the image of the active node by typing  
`OK boot net - image`  
and press the Enter key.

**Note:** There must be a space between the “-” and “image”.

*Example response:*

```
SC Alert: Host System has Reset
```

```
Sun Fire V240, No Keyboard  
Copyright 1998-2002 Sun Microsystems, Inc. All  
rights reserved. OpenBoot 4.8.0.build_04, 2048  
MB memory installed, Serial #52964131. Ethernet  
address 0:3:ba:28:2b:23, Host ID: 83282b23.
```

```
Rebooting with command: boot net - image
```

```
.  
.
.
```

```
SC Alert: Host System has Reset
```

**At your workstation (login session to the Active node)**

- 26** Monitor the progress of the cloning from the active node. Cloning the inactive node takes approximately one hour to complete.

*Example response:*

```

Waiting for network response from unit1-priv0...
received network response from unit1-priv0...
Waiting for unit1-priv0 to clone data...
waiting...1
waiting...2
waiting...3
unit1-priv0 is cloning: /export/d2
.
.
.
Verifying cluster status of unit1-priv0
waiting for cluster filesystem status to become
normal.
Deleted snapshot 0.
Deleted snapshot 1.
Deleted snapshot 2.
Deleted snapshot 3.
d99: Soft Partition is cleared

```

- 27** Once the cloning is complete, wait approximately 5 minutes before you proceed to the next step.

**At your workstation (login session to the Active node)**

- 28** Verify the status of replicated disk volumes by typing

```
# udstat
```

and pressing the Enter key.

| If all file systems are | Do                                 |
|-------------------------|------------------------------------|
| ACTIVE                  | step <a href="#">29</a>            |
| not ACTIVE              | contact your next level of support |

**At your workstation**

- 29** Establish a login session to the Inactive node using one of the following methods:

| If using          | Do                      |
|-------------------|-------------------------|
| telnet (unsecure) | step <a href="#">30</a> |
| ssh (secure)      | step <a href="#">31</a> |

- 30** Log in to the Inactive node using telnet (unsecure) as follows:
- Log in to the Inactive node by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the physical IP address of the Inactive node in the cluster
  - When prompted, enter your user ID and password.
  - Change to the root user by typing  

```
$ su - root
```

and pressing the Enter key.
  - When prompted, enter the root password.  
Proceed to step [32](#).
- 31** Log in using ssh (secure) as follows:
- Log in to the Inactive node by typing  

```
> ssh -l root <server>
```

and pressing the Enter key.  
where  
**server**  
is the physical IP address of the Inactive node in the cluster  
**Note:** If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter *yes* at the prompt.
  - When prompted, enter the root password.

- 32** Verify the status of replicated disk volumes by typing  
# **udstat**  
and pressing the Enter key.

| If all file systems are | Do                                 |
|-------------------------|------------------------------------|
| ACTIVE                  | step <a href="#">33</a>            |
| not ACTIVE              | contact your next level of support |

***At your workstation (login session to the Active node)***

- 33** Complete the cloning process by typing  
# **finishb**  
and pressing the Enter key.  
You have completed this procedure.

## Clearing the JWS cache on a client workstation

### Application

Use this procedure to clear the Java™ Web Start (JWS) cache on a client workstation.

The JWS cache on a client workstation needs to be cleared after an HTTPS certificate is installed on an existing Sun server that was not previously using a certificate. Clearing the cache allows you to properly launch the CS 2000 Management Tools client applications from your workstation.

### Prerequisites

None

### Action

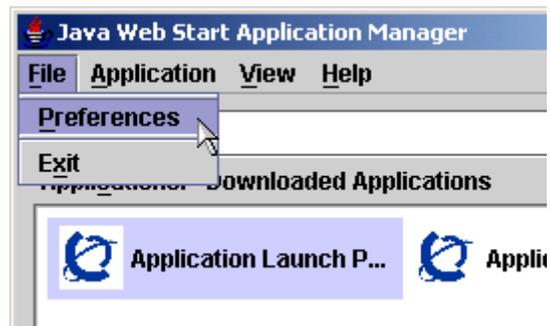
Perform the following steps to complete this procedure.

#### *At your workstation*

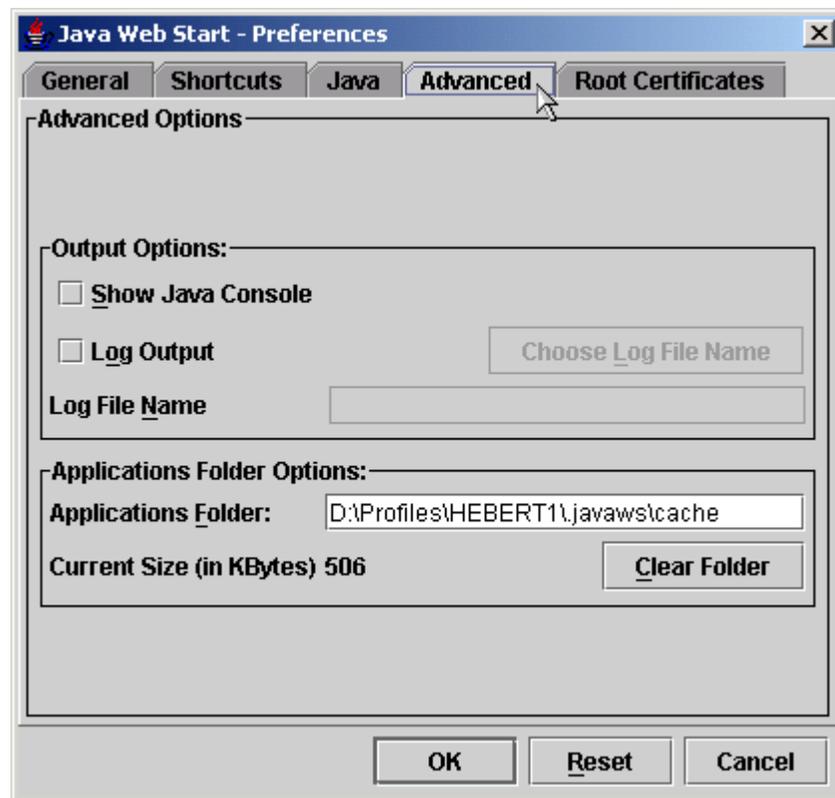
- 1 Access the Java Web Start Application Manager.



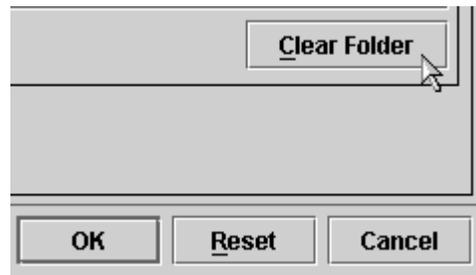
- 2 Click **File->Preferences** to access the Preferences window.



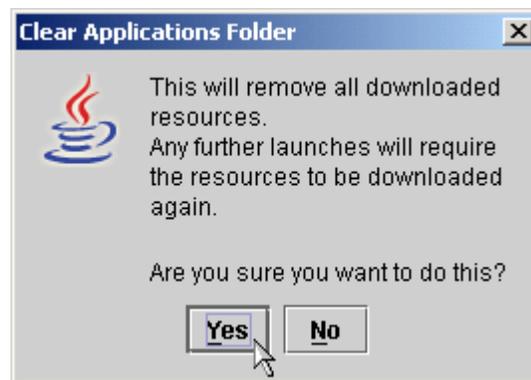
- 3 Click the **Advanced** tab to access the Advanced window.



- 4 Click **Clear Folder** to clear the cache.



- 5 Click **Yes** to confirm you want to clear the cache (remove all downloaded resources).



- 6 Click **OK** to close the Preferences window.
- 7 Exit the Java Web Start Application Manager.  
You have completed this procedure.