Dialogic® IP Media Server

Upgrading from Release 2.4.0 to 2.5.0 on Red Hat Enterprise Linux Platforms

April 2009 64-0440-01

www.dialogic.com

Copyright and Legal Disclaimer

All contents of this document are furnished for informational use only and are subject to change without notice and do not represent a commitment on the part of Dialogic Corporation or its subsidiaries ("Dialogic"). Reasonable effort is made to ensure the accuracy of the information contained in the document. However, Dialogic does not warrant the accuracy of this information and cannot accept responsibility for errors, inaccuracies or omissions that may be contained in this document.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH DIALOGIC® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN A SIGNED AGREEMENT BETWEEN YOU AND DIALOGIC, DIALOGIC ASSUMES NO LIABILITY WHATSOEVER, AND DIALOGIC DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF DIALOGIC PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHT OF A THIRD PARTY.

Dialogic products are not intended for use in medical, life saving, life sustaining, critical control or safety systems, or in nuclear facility applications.

Due to differing national regulations and approval requirements, certain Dialogic products may be suitable for use only in specific countries, and thus may not function properly in other countries. You are responsible for ensuring that your use of such products occurs only in the countries where such use is suitable. For information on specific products, contact Dialogic Corporation at the address indicated below or on the web at *www.dialogic.com*.

It is possible that the use or implementation of any one of the concepts, applications, or ideas described in this document, in marketing collateral produced by or on web pages maintained by Dialogic Corporation or its subsidiaries may infringe one or more patents or other intellectual property rights owned by third parties. Dialogic Corporation or its subsidiaries do not provide any intellectual property licenses with the sale of Dialogic products other than a license to use such product in accordance with intellectual property owned or validly licensed by Dialogic Corporation or its subsidiaries. More detailed information about such intellectual property is available from Dialogic Corporation's legal department at 9800 Cavendish Blvd., 5th Floor, Montreal, Quebec, Canada H4M 2V9.

Dialogic Corporation encourages all users of its products to procure all necessary intellectual property licenses required to implement any concepts or applications and does not condone or encourage any intellectual property infringement and disclaims any responsibility related thereto. These intellectual property licenses may differ from

This document discusses one or more open source products, systems and/or releases. Dialogic is not responsible for your decision to use open source in connection with Dialogic products (including without limitation those referred to herein), nor is Dialogic responsible for any present or future effects such usage might have, including without limitation effects on your products, your business, or your intellectual property rights.

Hardware Limited Warranty

Warranty for Hardware Products: Dialogic Corporation or its subsidiary that originally sold the hardware product to you ("Dialogic") warrants to the original purchaser ("Purchaser") of this hardware product ("Product"), that at the time of delivery the Product supplied hereunder will be free from defects in material and workmanship. This warranty is for the standard period for such Product set out on Dialogic's website at http://www.dialogic.com/warranties at the date of purchase, provided the Product remains unmodified, is operated under normal and proper conditions in accordance with its published specifications and documentation, and the system is not opened by unauthorized personnel. The warranty is also void if the defect has resulted from accident, misuse, abuse or misapplication. Any Product which becomes defective during the warranty period and is returned by Purchaser to Dialogic's Authorized Service Center shipping prepaid with a Return Material Authorization (RMA) number (which must be obtained from Dialogic before any return) within thirty (30) days after discovery of the defect, with a written description of the defect, will be repaired or replaced at Dialogic's option. Dialogic will not accept C.O.D. shipments. Dialogic reserves the right to refuse to repair or replace any Product which shows signs of abuse, misuse, neglect or has been altered in any way, including but not limited to Products which have been (i) used in environments which exceed operating tolerances such as supplied voltages and signals or (ii) stored under improper temperature or humidity conditions or (iii) used with equipment, software or interfacing not furnished by Dialogic or (iv) improperly packaged or shipped or (v) harmed by Purchaser or its agents' fault or negligence or (vi) repaired or modified without Dialogic's prior written consent . Purchaser must exercise proper electrostatic discharge (ESD) precautions and pack the Product and the other returned diagnostic information **in the original Dialogic packaging, including the antistatic bag/container and an ESD foam-filled cardboard box. Purchaser may void the warranty if the Product is improperly packaged or shipped**. Dialogic will bear the cost to return the repaired or replaced Product to the location specified on the Return Material Authorization (RMA) form by a method it chooses. If the Purchaser desires a specific form of conveyance, the Purchaser must bear the cost of shipment. All risk of loss shall be with the Purchaser during any and all shipments of the Product. Duties and import fees are the responsibility of the Purchaser.

Additional Exclusions: Dialogic will have no obligation to make repairs or replacements to the Product due to causes beyond the control of Dialogic, including, but not limited to, power or air conditioning failure, acts of God, improper interface with other units, or malfunction of any equipment or software used with the Dialogic Product(s). If Dialogic is requested and agrees to make repairs or replacements necessitated by any such causes, Purchaser will pay for such service or replacement at Dialogic's then prevailing rates.

No Other Warranties: DIALOGIC DISCLAIMS AND PURCHASER WAIVES ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY AGAINST LATENT DEFECTS, WITH RESPECT TO ANY DIALOGIC PRODUCT.

No Liability for Damages: IN NO EVENT SHALL DIALOGIC OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, INTERRUPTION OF ACTIVITIES, LOSS OF INFORMATION OR OTHER PECUNIARY LOSS AND DIRECT OR INDIRECT, CONSEQUENTIAL, INCIDENTAL, ECONOMIC OR PUNITIVE DAMAGES) ARISING OUT OF THE USE OF OR INABILITY TO USE ANY DIALOGIC PRODUCT.

Limitation of Liability: DIALOGIC'S MAXIMUM CUMULATIVE LIABILITY SHALL BE LIMITED TO THE AMOUNTS ACTUALLY PAID BY PURCHASER TO DIALOGIC FOR THE SPECIFIC PRODUCT BEING THE OBJECT OF THE CLAIM. PURCHASER RELEASES DIALOGIC FROM ALL AMOUNTS IN EXCESS OF THE LIMITATION. PURCHASER ACKNOWLEDGES THAT THIS CONDITION IS ESSENTIAL AND THAT DIALOGIC WOULD NOT SUPPLY TO PURCHASER IF IT WERE NOT INCLUDED. THIS WARRANTY EXPRESSLY DOES NOT APPLY TO ANYONE OTHER THAN PURCHASER.

Upgrading on Red Hat Enterprise Linux

This document provides information and instructions for upgrading from the Dialogic® IP Media Server Release 2.4.0 to Dialogic® IP Media Server Release 2.5.0 on platforms running Red Hat Enterprise Linux. It also includes instructions for downgrading from 2.5.0 to 2.4.0 in the event that you need to restore your previous configuration.

Introduction

This document describes the procedure for upgrading your Red Hat Enterprise Linux system from Dialogic® IP Media Server Release 2.4.0 to 2.5.0. Also included is the procedure for downgrading your system from MS 2.5.0 to 2.4.0.

(The Dialogic® IP Media Server is also referred to herein as the “IP Media Server” or “MS”.)

The matrix below defines the specific versions of Red Hat Enterprise Linux and the default VXML version associated with each IP Media Server release.

Table 1. Software Versions

Dialogic® IP Media Server	Red Hat	VXML
2.4.0	Red Hat EL 4 Update 5	VG-2.0
2.5.0	Red Hat EL 4 Update 5 Red Hat EL 5 Update 1	2.0

⚠ **Note: Important**: Use the IP Media Server Web UI to save a copy of your current configuration before starting the upgrade process.

Backup and Restore Scripts

As part of the upgrade process, certain file systems need to be backed up on the system. In the event that you need to downgrade to Release 2.4.0 after the upgrade, these backup files can be restored. Command shell scripts that enable you to back up and restore the necessary file systems are available on the Dialogic Technical Support Website:

http://www.dialogic.com/support/

You may need to contact Dialogic Technical Support for a username and password to access the Website.

Requirements

Red Hat Enterprise Linux

You must have the Red Hat Enterprise Linux 5 Update 1 (RHEL5_U1) CDs if you choose to upgrade your operating system. This is a five CD set available from Red Hat. Red Hat also provides the ISO images online. You can contact Dialogic Technical Support if you need assistance in acquiring these CDs.

Software only customers of the IP Media Server should have these CDs since they are required to purchase the RHEL4_U5 or RHEL5_U1 distribution.

File Systems

The IP Media Server contains 3 file systems that are backed up and restored as part of the upgrade process: ***root***, ***boot***, and ***var***. The following table describes the file systems, the nature of the backup, and the dump file locations.

File System	Backup	Description
root	full	Backup the entire ***root*** filesystem to /var/snowshore/root.dump.
boot	full	Backup the entire ***boot*** filesystem to /var/snowshore/boot.dump.
var	partial	Backup the ***var*** filesystem (excluding the /var/snowshore directory) to /var/snowshore/var.dump.

Note: The backup and restore shell scripts have the ability to copy the dump files across the network to/from a remote system. However, Anaconda does not work on the current version of the RHEL4_U5 Linux Rescue CD, so the network will not come up and therefore network file transfers are currently not possible.

Determining Software Versions

To determine whether the appropriate versions of the Red Hat, Dialogic® IP Media Server, and VXML software packages are installed, use the following commands:

Command	Description
rpm –qa	Lists the complete set of software packages installed.
uname –a	Lists the operating system version information.
df –T	Lists the file systems and supporting disk devices.

Upgrading from Dialogic® IP Media Server 2.4.0 to Dialogic® IP Media Server 2.5.0

To upgrade from MS 2.4.0 to MS 2.5.0, do the following:

1. Determine the block (disk) devices that support the root, boot, and var file systems (page 9).
2. Backup the IP Media Server 2.4.0 root, boot, and var file systems (page 10).
3. Install required Red Hat packages (page 12).
4. Upgrade the IP Media Server packages (page 12).

Determine Block Device

Determine the block device (i.e., disk) that supports the root, boot, and var filesystems. From the Linux command shell (on a running IPMS system), use the **df** command as follows:

```
df –T
```

```
Filesystem   Type1K-blocks   Used         Available  Use%      Mounted on
/dev/sda2    ext3 10080520   1070148      8498304    12%       /
/dev/sda1    ext3101086      11303        84564      12%       /boot
none         tmpfs517328     0            517328     0%        /dev/shm
/dev/sda5    ext323086712    142136       21771836   1%        /var
```

The output from **df** command shows that on this particular system the:

- **root** file system is on device **/dev/sda2**.
- **boot** file system is on device **/dev/sda1**.
- **var** file system is on device **/dev/sda5**.

The block device information is required by the IP Media Server backup and restore procedures.

Note: The block device names (e.g., /dev/sda) employed on your system may be different.

Backup using Dump

This section describes how to use the **dump** command to backup the IPMS ***root***, ***boot*** and ***var*** file systems. The dump files are saved in the ***var*** file system (i.e., within the **/var/snowshore** directory).

Before you backup the file systems, you must first determine and record which block device supports the **root**, **boot**, and **var** filesystems, as described in the previous section ("Determine Block Device" (page 9)).

The ***backup*** and ***restore*** procedures are performed from a *command shell* which you create using the Linux Rescue CD.

Note: The backup and restore shell scripts are installed with the IP Media Server software in the `/opt/snowshore/bin` directory.

Go to Command Shell using Linux Rescue Procedure

The backup and restore procedures are performed from the command shell that is established through the use of the Linux Rescue CD. The ISO image for the Red Hat EL Rescue CD (RHEL4-U5-i386-ES-disc1.iso or RHEL-5.1-server-i386-disc1.iso) is available from Technical Support, and must be burned onto a CD-ROM.

This procedure describes how to establish a command shell using the Linux Rescue CD.

1 Starting the Linux Rescue

Insert the Red Hat EL Rescue CD into the system's CD-ROM drive, log onto the system and type:
`reboot <ENTER>`

2 Red Hat Enterprise Linux

When the ***boot:*** prompt appears on the system monitor, enter "linux rescue", for example:
boot: **linux rescue <ENTER>**
See boot in progress messages on system monitor…

3 Choose a Language

Choose **English**, select **OK** and press <ENTER>.

4 Keyboard Type

Choose **us**, select **OK** and press <ENTER>.
"Searching for linux installations" messages appears on the system monitor.

5 Set Up Networking

Select **No** and press <ENTER>.

Note: Until the issue with Anaconda is resolved, answer **No** so that networking is not set up.
When the issue with Anaconda is resolved, enter **Yes** to setup networking, and then specify that DHCP is to be used by eth0 and eth1. You will then have the ability to transfer files over the network via FTP or SCP. In addition, the **backup** and **restore** shell scripts will be capable of transferring the dump files to/from remote systems.

6 Rescue

Choose **Skip** and press <ENTER> to go directly to the command shell.
-/bin/sh-3.00#

IPMS Backup

The following procedure is used to backup your IPMS system (i.e., ***root***, ***boot*** and ***var*** file systems). This procedure is performed from a *command shell* that is established using the Linux Rescue CD.

For detailed information regarding the use and capabilities of the MS Backup shell script (ms_backup.sh), see “Appendix A: ms_backup.sh Shell Script” (page 18).

1 Create a command shell using the Linux Rescue Procedure. For directions on how to create a command shell, see the section “Go to Command Shell using Linux Rescue Procedure” (page 10).

-/bin/sh-3.00#

2 The backup and restore scripts are installed with the IP Media Server software in the `/opt/snowshore/bin` directory. To make them available for use, do the following:

```
-/bin/sh-3.00# mkdir /mnt/rd
-/bin/sh-3.00# mount –t ext3 /dev/sda2 /mnt/rd
-/bin/sh-3.00# cp /mnt/rd/opt/snowshore/bin/ms_backup.sh /
-/bin/sh-3.00# chmod 777 /ms_backup.sh
-/bin/sh-3.00# umount /mnt/rd
```

Note: When the Anaconda network issue is resolved, you can use FTP or SCP from the command line to transfer the backup and restore shell scripts from a remote system. Until that time, the backup and restore shell scripts are available in the /var/snowshore directory.

3 Run the backup shell script in order to dump the contents of the root, boot, and var filesystems.

You will need to specify the block device (disk) used by your system.

```
-/bin/sh-3.00# ./ms_backup.sh /dev/sda
```

Note: You will see activity on the system console while the backup shell script runs.

4 Remove the Linux Rescue CD.

5 Exit the command shell to reboot the system when the backup shell script completes.

```
-/bin/sh-3.00# exit
```

Dump File Information

The size of the dump files is approximately 6MB for the boot file system (boot.dump), 1.3GB for the root file system (root.dump), and 64MB for the var file system (var.dump).

The *md5sum.dump* file contains the MD5 (128-bit) checksums for root, boot, and var dump files.

```
-rw-r--r--  1 root root    6580224 Mar 11 09:33
/var/snowshore/boot.dump
-rw-r--r--  1 root root        131 Mar 11 09:34
/var/snowshore/md5sum.dump
-rw-r--r--  1 root root 1905039360 Mar 11 09:33
/var/snowshore/root.dump
-rw-r--r--  1 root root   39868416 Mar 11 09:33
/var/snowshore/var.dump
6444   /var/snowshore/boot.dump
8      /var/snowshore/md5sum.dump
1862220/var/snowshore/root.dump
38984  /var/snowshore/var.dump
```

Upgrade to Red Hat EL 5 Update 1

If you choose to upgrade your operating system to RHEL5.1, Dialogic suggests you properly install RHEL5.1 and then install the IPMS 2.5 software or you use the Dialogic IP Media Server 2.5 Recovery CD for Red Hat Enterprise Linux Server 5.1. See the document entitled *Red Hat 5.0 and IPMS 2.5* for more information. Contact Dialogic Support for help with this process or access to the software media.

Installing Required Red Hat Packages

Before upgrading to the IPMS 2.5.0 release, there are required Red Hat packages that you must install. You must obtain the RPMs from the Red Hat installation CDs, Red Hat Technical Support, or Dialogic Technical Support and perform the following steps:

1 Obtain the following rpm files for **Red Hat EL 4 Update 5**:

kernel-devel-2.6.9-55.EL.i686.rpm
libjs-1.5-0.pm.9.i586.rpm
postgresql-docs-7.4.16-1.RHEL4.1.i386.rpm
seamonkey-nspr-1.0.8-0.2.el4.i386.rpm

Xerces-c-2.3.0-37.i586.rpm

Obtain the following rpm files for **Red Hat EL 5 Update 1**:

giflib-utis-4.1.3-7.el5.1
kernel-devel-2.6.18-53.el5.i686.rpm
libjs-1.5-0.pm.9.i586.rpm
php-cli-5.1.6-15.el5
php-common-5.1.6-15.el5.i386.rpm
php-pdo-5.1.6-15.el5.i386.rpm
postgresql-docs-8.1.9-1.el5.i386.rpm
Xerces-c-2.3.0-37.i586.rpm

For a complete list of the necessary Red Hat packages, see the documents entitled *Red Hat 4.0 and IPMS 2.5* or *Red Hat 5.0 and IPMS 2.5*.

2. Copy the relevant files locally on your Media server and run the following command for each rpm listed above:

   ```
   rpm -ivh <packagename.rpm>
   ```

3. Contact Dialogic Technical Support if you have any issues installing these packages.

Upgrading to MS 2.5.0

To upgradethe IP Media Server (Dialogic® software packages) from 2.4.0 to 2.5.0, perform the following steps:

1. Obtain the G2MS 2.5.0 build from Dialogic Technical Support.
2. Copy the G2MS 2.5.0 tar.gz file (e.g., SNOWG2PKG-2.5.0-<DATE>A.EL4.0.rpm.tar.gz or SNOWG2PKG-2.5.0-<DATE>A.EL5.0.rpm.tar.gz) to your NFS server.
3. Use the IP Media Server Web UI to obtain the MS 2.5.0 software package from your NFS server.
4. Click RETRIEVE UPDATES, and then enter the URL, directory path, user name, and password required by your NFS server.

   If you do not have an NFS server, you can copy the G2MS 2.5.0 build (tar.gz file) to the /opt/snowshore/rpm directory on your IP Media Server.
5. Use the IP Media Server Web UI to install the G2MS 2.5.0 software package:

   a. Select SYSTEM->SOFTWARE UPDATES, and then click on the INSTALL tab associated with the MS Release 2.5.0 rpm package listed there.

   b. Click OK to verify the install. This will take a few minutes and requires a system reboot.

c. Check the system configuration after the system reboots. Do not restore from saved configuration files.

Note: The password for the administrator user of the Web UI is blank once Release 2.5.0 is installed.

Accounting Configuration

To enable accounting you must postgress database action.

For example:

- chkconfig posgres on
- service start postgres

Downgrading to MS 2.4.0

This section describes how to downgrade an MS 2.5.0 system back to MS 2.4.0. This assumes you used:

- **df** to determine the block device that correspond to the root, boot, and var file systems. See "Determine Block Device" (page 9).
- the backup shell script to save the contents of the IPMS root, boot and var file systems. See "Backup and Restore Scripts" (page 7).

Use the following procedure to restore your IPMS system (i.e., root, boot and var file systems). For a copy of the restore shell script, see "Appendix B: ms_restore.sh Shell Script" (page 22).

This procedure is performed from a command shell that is established by using the Linux Rescue CD.

Customers are required to backup their vital information (e.g., data, scripts, applications) before using the downgrade procedure. The downgrade procedure restores the contents of the root, boot, and var file systems to their previous state, as contained in the dump files. All files or data created since the dump file were generated will be LOST.

1. Create a command shell using the Linux Rescue Procedure. For directions on how to create a command shell, see "Go to Command Shell using Linux Rescue Procedure" (page 10).

   ```
   -/bin/sh-3.00#
   ```

2. The backup and restore scripts are installed with the IP Media Server software in the `/opt/snowshore/bin` directory. To make them available for use, do the following:

   ```
   -/bin/sh-3.00# mkdir /mnt/rd
   -/bin/sh-3.00# mount -t ext3 /dev/sda2 /mnt/rd
   -/bin/sh-3.00# cp /mnt/rd/opt/snowshore/bin/ms_restore.sh /
   -/bin/sh-3.00# chmod 777 /ms_restore.sh
   -/bin/sh-3.00# umount /mnt/rd
   ```

   Note: When the Anaconda network issue is resolved, you can use FTP or SCP from the command line to transfer the backup and restore shell scripts from a remote system. Until that time, the backup and restore shell scripts will be available in the /var/snowshore directory.

3 Run the restore shell script in order to restore the contents of the root, boot, and var filesystems.

You will need to specify the block device (disk) used by your system.

```
-/bin/sh-3.00# ./ms_restore.sh /dev/sda
```

Note: You will see activity on the system monitor while the restore shell script runs.

4 Remove the Linux Rescue CD.

5 Exit the command shell to reboot the system when the restore shell script completes.

```
-/bin/sh-3.00# exit
```

6 When the system reboots, Release 2.4.0 of the IP Media Server will be running.

Appendix A: ms_backup.sh Shell Script

```
#! /bin/sh

# FILE NAME: ms_backup.sh
#
# SYNOPSIS:  Media Server Backup Procedure
#
# VERSION:   2.5
#
# SYNTAX:    ./ms_backup.sh  disk  [user@host:/dir]
#
#   Required Argument:
#       disk = block device  (e.g., /dev/sda (Intel),
#                                   /dev/hda (IBM),
#                                   /dev/cciss/c0d0p (HP))
#
#    Optional Arguments (all or nothing):
#       user = user login name (e.g., root)
#       host = host name or IP address (e.g., 192.168.12.209)
#       dir  = directory (e.g., /backup).
#
# SHELL SCRIPT ARGUMENTS:
#
#   $1 = disk  (REQUIRED)
#   $2 = user@host:/dir  [OPTIONAL]
#
# DESCRIPTION:
#
#   This shell script is used to backup a Media Server system.
#
#   The script dumps the contents of the root, boot, and var filesystems
#   to the dump files contained in the local /var/snowshore directory.
#   The contents of the /var/snowshore directory are not backed up.
#
#   The md5sum application is used to compute MD5 (128-bit) checksums
#   (as described in RFC 1321) for each dump file.  The checksums are
#   save in the /var/snowshore/md5sum.dump text file.
#
#   If the optional [user@host:/dir] command line argument is specified,
#   scp is used to copy all dump files over the network to a remote system.
#   You will be asked by scp for the password to the remote system.
#
#   Red Hat EL 4.0
#     The RHEL4_U4 Rescue CD (RHEL4-U4-i386-ES-disc1.iso) is use to
#     establish the command shell in which this shell script is executed.
#
#
#   This shell script assumes the following to be true:
#   a) There exist root, boot, and var filesystems, supported by
#      block special files corresponding to disk volumes 2, 1, 5.
#
#   Filesystem  Volume  Intel        IBM            HP
#   ----------  ------    -----        ---            --
#      root       2/dev/sda2   /dev/hda2   /dev/cciss/c0d0p2
#      boot       1/dev/sda1   /dev/hda1   /dev/cciss/c0d0p1
#      var        5/dev/sda5   /dev/hda5   /dev/cciss/c0d0p5
#
#   b) The root, boot, and var filesystems are intact (i.e., not corrupted).
#
#   WARNING: This shell script does not check the validity of the optional
#            [user@host:/dir] argument, it simply uses what was supplied.
#


# Display shell script usage message on error.
usage () {
  cat <<EOF

   SYNTAX:
      ./ms_backup.sh  disk [user@host:/dir]

      Required Argument:
         disk = block device  (e.g., /dev/sda (Intel),
                                     /dev/hda (IBM),
                                     /dev/cciss/c0d0p (HP))

     Optional Arguments (all or nothing):
         user = user login name (e.g., root)
         host = host name or IP address (e.g., 192.168.12.209)
         dir  = directory (e.g., /backup).

   EXAMPLES:
      Intel (w/o network copy):
         ./ms_backup.sh /dev/sda

      IBM (w/o network copy):
         ./ms_backup.sh /dev/hda

      HP (w/o network copy):
         ./ms_backup.sh /dev/cciss/c0d0p

      Intel (w/network copy):
         ./ms_backup.sh /dev/sda root@192.168.12.209:/backup

EOF
  exit 1
}


# (1) Verify existence of block device (i.e., required command line argument).
if [ “$#” != “1” ] && [ “$#” != “2” ] ; then
   echo “Error: invalid number of command line arguments ($# given)!”
   usage
fi
if test ! -b $11 ; then
   echo “Error: [$11] bad block device!”
   usage
fi

# (2) Create mount points and mount root, boot, and var filesystems (separately).
echo “Mounting all filesystems.”
cd /mnt
mkdir -p  root boot var
chmod 777 root boot var
mount -t ext3 $12 /mnt/root
mount -t ext3 $11 /mnt/boot
mount -t ext3 $15 /mnt/var

df -T

# (3) Check if the filesystem dump files exist locally in /var/snowshore.
dumpFiles=0
if test -e /mnt/var/snowshore/root.dump; then
   echo “Found local dump file [/var/snowshore/root.dump].”
   dumpFiles=1
fi
if test -e /mnt/var/snowshore/boot.dump; then
   echo “Found local dump file [/var/snowshore/boot.dump].”
   dumpFiles=2
fi
if test -e /mnt/var/snowshore/var.dump; then
   echo “Found local dump file [/var/snowshore/var.dump].”
   dumpFiles=3
fi

# If so, ask the user for permission to over-write the existing dump files.
if  [ $dumpFiles != 0 ] ; then
   echo “Do you want to over-write the local dump files? <yes:no>”
   overWrite=no
   read overWrite

   if [ $overWrite != yes ]; then
      echo “$0 script exiting: local dump files have not been unmodified...”
      exit 1
   fi
fi

# (4) Remove the log files and recordings in the /var/snowshore directory
#     to make space for the dump files.
```

```
echo “Removing snowshore log files and recordings.”
rm -f /mnt/var/snowshore/log/*
rm -f /mnt/var/snowshore/rec/*


# (5) Backup the root filesystem.
echo “Backup root filesystem.”
cd /mnt/root
dump -0 -b 126 -d 141000 -s 11500 -f /mnt/var/snowshore/root.dump .


# (6) Backup the boot filesystem.
echo “Backup boot filesystem.”
cd /mnt/boot
dump -0 -b 126 -d 141000 -s 11500 -f /mnt/var/snowshore/boot.dump .


# (7) Backup the var filesystem (excluding the /var/snowshore directory).
#     Use ls command to obtain inode number of /var/snowshore directory.
#     Use the dump command to make a backup of the var file system.
#     Exclude the contents of the /var/snowshore directory by specifying
#     the “-e inode_numbers” command line option to dump command.
echo “Backup the var filesystem.”
cd /mnt/var
dump -0 -e “$(ls -ild /mnt/var/snowshore | cut -f1 -d’ ‘)” -b 126 -d 141000 -s 11500 -f
  /mnt/var/snowshore/var.dump .


# (8) Compute MD5 (128-bit) checksums for root, boot, and var dump files.
echo “Compute MD5 checksums for all dump files.”
cd /mnt/var/snowshore
md5sum *.dump > md5sum.dump


# (9) If optional [user@host:/dir] command line argument was specified,
#     copy dump files (via scp) over the network to the remote system.
if [ “$2” != ““ ] ; then
   echo “ “
   echo “Copying local dump files to remote system [$2]”
   echo “ “
   scp *.dump $2
fi


# (10) Umount the root, boot, and var filesystems.
echo “Umount root, boot, and var filesystems.”
cd /
sync
umount /mnt/boot /mnt/root /mnt/var


# (11) Exit the command shell to reboot the system
#exit 0
```

Appendix B: ms_restore.sh Shell Script

```
#! /bin/sh

# FILE NAME: ms_restore.sh
#
# SYNOPSIS:  Media Server Restore Procedure
#
# VERSION:   2.5
#
# SYNTAX:    ./ms_backup.sh  disk  [user@host:/dir]
#
#   Required Argument:
#       disk = block device  (e.g., /dev/sda (Intel),
#                                   /dev/hda (IBM),
#                                   /dev/cciss/c0d0p (HP))
#
#    Optional Arguments (all or nothing):
#       user = user login name (e.g., root)
#       host = host name or IP address (e.g., 192.168.12.209)
#       dir  = directory (e.g., /backup).
#
# SHELL SCRIPT ARGUMENTS:
#
#   $1 = disk  (REQUIRED)
#   $2 = user@host:/dir  [OPTIONAL]
#
# DESCRIPTION:
#
#   This shell script is used to downgrade a Media Server system
#   from Release 2.5.0 back to 2.4.0.
#
#   The script restores the contents of the root, boot, and var filesystems
#   from the dump files contained in the local /var/snowshore directory.
#   The contents of the /var/snowshore directory are not backed up.
#
```

```
#   If the optional [user@host:/dir] command line argument was specified,
#   the dump files are copied (via scp) from the remote system to the
#   local /var/snowshore directory.  You will be asked by scp for the
#   password to the remote system.
#
#   The dump files MD5 (128-bit) checksums are contained in the
#   /var/snowshore/md5sum.dump text file.  The md5sum application
#   can be used to validate the integrity of the dump files.
#
#   Red Hat EL 4.0
#     The RHEL4_U5 Rescue CD (RHEL4-U5-i386-ES-disc1.iso) is use to
#     establish the command shell in which this shell script is executed.
#
#
#   This shell script assumes the following to be true:
#   a) There exist root, boot, and var filesystems, supported by
#      block special files corresponding to disk volumes 2, 1, 5.
#
#   Filesystem  Volume    Intel        IBM            HP
#   ----------  ------    -----        ---            --
#      root       2     /dev/sda2   /dev/hda2   /dev/cciss/c0d0p2
#      boot       1     /dev/sda1   /dev/hda1   /dev/cciss/c0d0p1
#      var        5     /dev/sda5   /dev/hda5   /dev/cciss/c0d0p5
#
#   b) The root, boot, and var filesystems are intact (i.e., not corrupted).
#
#
#   NOTE: The script does not remake the filesystems, whereby negating
#         any problems regarding the proper labeling of the filesystems
#         or filesystem geometry.
#
#   WARNING: This shell script does not check the validity of the optional
#            [user@host:/dir] argument, it simply uses what was supplied.
#


# Display shell script usage message on error.
usage () {
  cat <<EOF

   SYNTAX:
      ./ms_restore.sh  disk [user@host:/dir]

      Required Parameter:
         disk = block device  (e.g., /dev/sda (Intel),
                                     /dev/hda (IBM),
                                     /dev/cciss/c0d0p (HP))

     Optional Parameters (all or nothing):
         user = user login name (e.g., root)
         host = host name or IP address (e.g., 192.168.12.209)
         dir  = directory (e.g., /backup).

   EXAMPLES:
      Intel (w/o network copy):
         ./ms_restore.sh /dev/sda
      IBM (w/o network copy):
         ./ms_restore.sh /dev/hda

      HP (w/o network copy):
         ./ms_restore.sh /dev/cciss/c0d0p

      Intel (w/network copy):
         ./ms_restore.sh /dev/sda root@192.168.12.209:/backup

EOF
  exit 1
}


# (1) Verify existence of block device (i.e., required command line argument).
if [ “$#” != “1” ] && [ “$#” != “2” ] ; then
   echo “Error: invalid number of command line parameters ($# given)!”
   usage
fi
if test ! -b $11 ; then
   echo “Error: [$11] bad block device!”
   usage
fi


# (2) Create mount points and mount the root, boot, and var filesystems (separately).
echo “Mounting filesystems”
cd /mnt
mkdir -p  root boot var
chmod 777 root boot var
mount -t ext3 $12 /mnt/root
mount -t ext3 $11 /mnt/boot
mount -t ext3 $15 /mnt/var

df -T


# (3) Check if filesystem dump files exist locally in /var/snowshore.
dumpFiles=0
if test -e /mnt/var/snowshore/root.dump; then
   echo “Found /var/snowshore/root.dump.”
   dumpFiles=1
fi
if test -e /mnt/var/snowshore/boot.dump; then
   echo “Found /var/snowshore/boot.dump.”
   dumpFiles=2
fi
if test -e /mnt/var/snowshore/var.dump; then
   echo “Found /var/snowshore/var.dump.”
   dumpFiles=3
fi


# (4) If the [user@host:/dir] command line argument was specified,
#     copy dump files (via scp) over the network from remote system.
if [ “$2” != ““ ] ; then
```

```
   # If dump files already exist locally, ask the user for permission to
   # over-write the local dump files with those from the remote system.
   if  [ $dumpFiles != 0 ] ; then
      echo “Do you want to over-write local dump files with those from $2? <yes:no>”
      overWrite=no
      read overWrite

      if [ $overWrite != yes ]; then
         echo “$0 script exiting: local dump files have not been unmodified...”
         exit 1
      fi
   fi

   echo “ “
   echo “Copying dump files from remote system [$2] to /var/snowshore.”
   echo “ “
   cd /mnt/var/snowshore
   scp $2/*.dump .
fi

# (5) Ensure that dump files exist locally for all filesystems being restored.
echo “Verify dump files exist locally for all filesystems being restored.”
if test ! -e /mnt/var/snowshore/root.dump; then
   echo “$0 script terminating: Missing /var/snowshore/root.dump”
   exit 1
fi
if test ! -e /mnt/var/snowshore/boot.dump; then
   echo “$0 script terminating: Missing /var/snowshore/boot.dump”
   exit 1
fi
if test ! -e /mnt/var/snowshore/var.dump; then
   echo “$0 script terminating: Missing /var/snowshore/var.dump”
   exit 1
fi


# (6) Restore the contents of the boot filesystem.
echo “Restore the boot filesystem.”
cd /mnt/boot
rm -rf *
sync
restore -r -v -b 126 -f /mnt/var/snowshore/boot.dump
rm restoresymtable


# (7) Restore the contents of the root filesystem.
echo “Restore the root filesystem.”
cd /mnt/root
rm -rf *
sync
restore -r -v -b 126 -f /mnt/var/snowshore/root.dump
rm restoresymtable


# (8) Restore the contents of the var filesystem.
# Use the rm command to remove all files and directories in var filesystem
# (except for the snowshore directory which contains the dump files).
```

```
echo “Restore the var filesystem.”
cd /mnt/var
rm -rf a* c* d* e* f* l* m* n* o* p* r* snowshore/log/* snowshore/rec/* spool t* v* w* y*
restore -r -v -b 126 -f /mnt/var/snowshore/var.dump
rm restoresymtable


# (9) Mount boot and var filesystems under root.
echo “Mount boot and var filesystems under root.”
cd /
sync
umount /mnt/boot /mnt/var
mount -t ext3 $11 /mnt/root/boot
mount -t ext3 $15 /mnt/root/var


# (10) Reinstall the GRand Unified Bootloader (GRUB).
echo “Install GRUB.”
/mnt/root/sbin/grub --batch <<EOF
root (hd0,0)
find /grub/stage1
setup (hd0)
EOF


# (11) Umount the root, boot, and var filesystems.
echo “Umount root, boot, and var filesystems.”
cd /
sync
umount /mnt/root/boot /mnt/root/var /mnt/root


# (12) Exit the command shell to reboot the system.
# exit


# (13) Upon reboot Media Server 2.4 will be running.
```