Oracle® Communications Session Delivery Manager

Installation Guide
Release 7.3
Formerly Net-Net Central

January 2014

ORACLE

Notices

Contents

About this guide - NNC73 - Installation Guide ORACLE

The Oracle Communications Session Delivery Manager Installation Guide explains how to install the Session Delivery Management Suite, which provides advanced management applications and services.

NNC File and Directory Names

This guide supports Session Delivery Manager Version 7.3 and subsequent 7.3 maintenance releases. File names and directories include “xx” to denote the possible presence of alphanumeric characters for maintenance releases. If you are not running a Session Delivery Manager maintenance release, you can disregard the “xx”.

Below is an example of a file name for releases 7.3 and 7.3M1:

NNC73Linux64bit.tar.gz

Session Delivery Manager 7.3:

- NNC73Linux64bit.tar.gz

Session Delivery Manager 7.3M1:

- NNC73M1Linux64bit.tar.gz

Related Documentation

The following table lists the members that comprise the documentation set for this release:

Document Name	Document Description
Acme Packet 4500 System Hardware Installation Guide (400-0101-00)	Contains information about the components and installation of the Acme Packet 4500 system.
Acme Packet 3800 Hardware Installation Guide (400-0118-00)	Contains information about the components and installation of the Acme Packet 3800 system.
Release Notes	Contains information about the current documentation set release, including new features and management changes.
ACLI Configuration Guide	Contains information about the administration and software configuration of the SBC.
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Maintenance and Troubleshooting Guide	Contains information about logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
MIB Reference Guide	Contains information about Management Information Base (MIBs), Acme Packet’s enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Accounting Guide	Contains information about accounting support, including details about RADIUS accounting.

Document Name	Document Description
HDR Resource Guide	Contains information about the Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Administrative Security Essentials	Contains information about support for its Administrative Security license.

Revision History

Date	Revision Number	Description
October 2013	Revision 1.00	Initial Release
December 2013	Revision 1.01	Updates Net-Net Central Install directory requirements
January 2014	Revision 1.02	Updates Linux configuration for the pre-installation procedure

1

Installing the Session Delivery Manager

Overview

This document explains how to install Session Delivery Manager in a Linux operating system and how to migrate data from Net-Net EMS 6.x and Net-Net Route Manager Central 1.x. This release of Session Delivery Manager supports the following.

Hardware Support

The following hardware platforms are supported:

- nn3800
- nn4250
- nn4500
- nn9200
- nn2600
- Net-Net 7000 series, including the Net-Net 7250
- Net-Net 17000 series, including the Net-Net 7350 blade server

Net-Net SBC Support

For a comprehensive list of Net-Net SBC OS support in this release of Session Delivery Manager, please consult the Release Notes.

Limited Support

For the Net-Net 2600, Session Delivery Manager supports trap as events and alarms in Fault Management. For performance statistics and configuration management, Net-Net Centra will redirected the user to the Net-Net 2600 onboard GUI.

Before You Start

This section contains the information you should review before you start the installation process.

System Requirements

Oracle has certified the following hardware and software server platforms; and client requirements for use with Session Delivery Manager Vesrion 7.3.

Note: Other hardware configurations might work with Session Delivery Manager, but Oracle has verified the configurations listed here.

Linux

- CPU: 4-core 2.1 GHz processor or better
- 16 GB RAM minimum
- 195 GB hard drive, 300 GB hard drive recommended

  Note: 150 GB of hard drive space is required for each licensed application. For example, if Session Delivery Manager is licensed with Element Manager, Route Manager, and Report Manager, the recommended disk space is 450 GB.
- Linux Red Hat Fedora Core 13 64 bit or Red Hat Enterprise Linux 6.2 64 bit

  Note: RHEL 5.5 is supported in Session Delivery Manager 7.3, but not be supported in future releases.

Network Manager with Fedora Core 13

Fedora Core 13 installs an application called Network Manager by default. Network Manager is used to configure network connections. It executes automatically when you start your session and it is visible as an applet icon. You need to check your system to see if Fedora Core 13 installed Network Manager on your system. If installed you need to remove it and then turn on the network services.

1. Login as root.
2. Check for Network Manager.

   ```
   service NetworkManager status
   ```
3. Shutdown the Network Manager.

   ```
   service NetworkManager stop
   ```
4. Remove Network Manager using the following command:

   ```
   yum remove NetworkManager
   ```
5. Turn on network services using the following command:

   ```
   chkconfig network on
   service network start
   ```

   Note: You should also ensure that the option Controlled by NetworkManager in Network Configuration is unchecked on your system.

OpenSSL

Most Linux distributions include OpenSSL as part of the OS installation. You can check the version on your system by using the following command:

```
openssl version
OpenSSL 0.9.7d Mar 27 2004
```

Client Requirements

- Internet Explorer versions 9.0 and higher or Mozilla Firefox versions 3.0 and higher or Google Chrome versions 23.0 or higher
- Flash player compatible with your browser installed locally
- If the server is not part of your DNS domain, the hosts file on each client must be edited to include the hostname and IP address of the Session Delivery Manager server. The client host file is usually located in the following directory:

windows\system32\drivers\etc

Using the DNS Database

All Session Delivery Manager servers and clients should be configured to use the DNS database for host name lookups. Session Delivery Manager servers should be defined in the DNS database.

If you are not using the DNS service, you must ensure the hosts file on all Session Delivery Manager servers and clients contain entries for the Session Delivery Manager server.

Note: If you want to connect to an Session Delivery Manager server over a Secure Sockets Layer (SSL) connection, you must have administrator privileges on the client system.

Information You Need

Ensure that you have identified the following information before you install:

- Hostname and IP address/netmask of the Session Delivery Manager server, as well as the IP addresses of its gateway, subnet mask, and DNS server
- IP address for each Net-Net SBC
- SNMP community strings for each Net-Net SBC

Net-Net Central Components Required

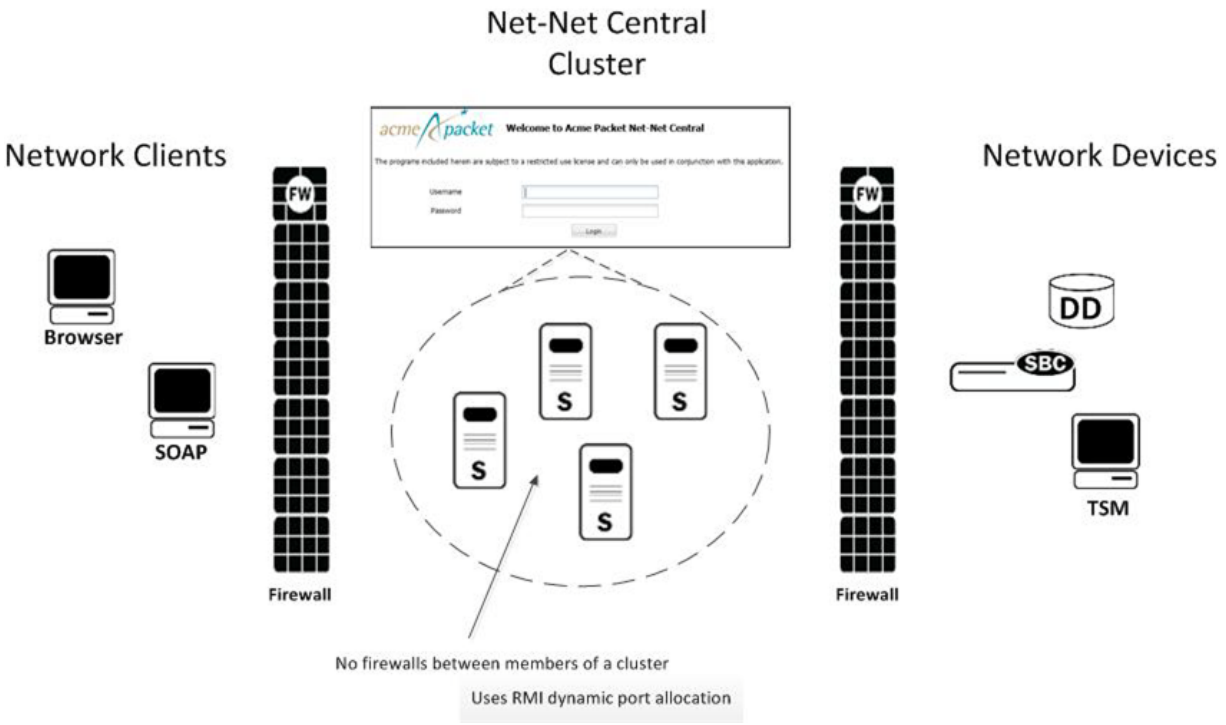
To install Session Delivery Manager, you need to obtain the appropriate tar.gz file for your environment from your Oracle representative.

- NNC73Linux64bit.tar.gz for Linux RHEL v5.5 64 bit installation
- NNC73FC1364bit.tar.gz for Linux Fedora Core 13 64 bit installation
- NNC73RHEL64bit.tar.gz for CentOS 6.2 and CentOS NNC-VM installation

You also need the AcmePacketNetNetCentral.xml license file.

Opening Ports on the Firewall

When setting up Session Delivery Manager in your network, you may have a firewall between the clients (browsers, SOAP, etc.) and the Session Delivery Manager cluster, and a firewall between the Session Delivery Manager cluster and other devices (Net-Net SBCs, Data Domain (DD), Terminal Server Manager (TSM)). See the following illustration.



Note: You cannot have firewalls between the servers in a cluster.

If firewalls exist on either side of the Session Delivery Manager cluster, ensure the ports listed in the following table are open. If your OS system comes with a firewall, you need to apply the same criteria. You must switch off the firewall in your OS, or ensure these ports are available.

Port Number	Protocol	Service	Configurable	Affects Firewall?	Purpose
Between Session Delivery Manager Cluster and Network Clients					
8443	TCP/SSL	HTTPS	N	Y	Apache port. HTTPS port for client/server communication.
8080	HTTP	HTTP	N	Y	HTTP port for client/server communication.
Between Session Delivery Manager Cluster and Network Devices					
161	UDP	SNMP	N	Y	SNMP read/write requests between the Net-Net Central server and the Net-Net SBC.
162	UDP	SNMP	N	Y	SNMP trap reporting from the Net-Net SBC to the Session Delivery Manager server.
22/21	SFTP/FTP				Used for file transfer (such as Route Manager and LRT updates).
8080	HTTP	AMI	N	Y	Used by Session Delivery Manager to communicate with Net-Net 9200 devices via AMI.
5060	TCP		N	Y	Used for Session Delivery Manager Trunk Manager (SIPTX) to communicate with SP-SBC.

Port Number	Protocol	Service	Configurable	Affects Firewall?	Purpose
3001/ 3000		ACP/ACLI			Used by Session Delivery Manager to communicate with all versions of Net-Net SBC except for the Net-Net 9200.
Between Session Delivery Manager Servers in the Cluster					
1098	TCP/SSL	RMI	N	Y	RMI Communication between host members in a cluster. Note: SSL is not supported when HTTPS is enabled.
1099	TCP/SSL	RMI Lookup	N	Y	RMI registry port. Used for the RMI communication between host members in a cluster. Note: SSL is not supported when HTTPS is enabled.
5701	TCP	Hazelcast	N		Used by Hazelcast communication for distributed data structures, peer-to-peer collective data distribution.
5801	TCP	Hazelcast	N	Y	Used by the Hazelcast management console port for the Session Delivery Manager distributed scheduler service.
8005	TCP	HTTP	N	Y	Tomcat shutdown port used by the shutdown script. Can be blocked on a firewall because it is local to the Session Delivery Manager server.
8009	TCP	Apache	N	Y	Tomcat port.
9000	TCP	Berkeley	N	Y	Berkeley database.
61616	TCP	Apache	N	Y	Message broker.
22	SFTP	ActiveMQ	N	Y	Used to transfer files between Session Delivery Manager servers.

Either port 8080 (HTTP) or port 8443 (HTTPS) must be open on the firewall, depending on which port you choose between the network client and Session Delivery Manager server. If installing on a Linux system, the Linux firewall must also have either 8080 (HTTP) or port 8443 (HTTPS) open.

Note:

For iptables/ipf, communication is open between Session Delivery Manager servers in a cluster if the ports listed above are open and there is no firewall deployed between the servers, as ports are assigned dynamically (Remote Method Invocation (RMI) dynamic port allocation).

Before a New Installation

This section explains how to configure your operating system before you install Session Delivery Manager for the first time. You should contact your Oracle systems engineer for a copy of the latest Session Delivery Manager Best Current Practices document. It contains instructions on how to install the Linux operating systems.

Note: You do not have to complete this process if you are using the NNC-VM. Linux is configured automatically using the sysprep utility as part of the NNC-VM installation process.

Configuring Linux

To configure Linux:

- Include the Linux host name
- Disable the default http daemon

Including the Linux Hostname

You must configure the Linux system hostname during the installation of the operating system. You can determine the hostname by using the hostname command on the Linux system. For example:

```
[bash]$ hostname
nncsvr
```

You need to edit the /etc/hosts file to include the Linux system hostname in the following format:

<IP address>	<hostname>	<hostname>.local domain

The following example shows the inclusion of a server named nncsvr with an IP address of 10.0.0.252:

```
[bash]$ cat /etc/hosts
#Do not remove the following line, or various programs
# that require network functionality will fail.
```

10.0.0.252	nncsvr	nncsvr.localdomain
127.0.0.1	localhost	localhost.localdomain

Disabling the Default HTTP Daemon

You need to disable the default http daemon process on the Session Delivery Manager server.

To disable the http daemon:

1. Log in as root user and open a Terminal window.
2. Stop the httpd daemon if it is running:

   ```
   sbin/service httpd stop
   ```
3. Disable the http daemon from restarting a system reboot:

   ```
   chkconfig httpd off
   ```
4. Verify the httpd daemon is not running:

   ```
   sbin/service httpd status
   ```

   The following message appears:

   ```
   httpd is stopped
   ```

Setting the System Locale

You must set the system locale to en_US.UTF-8 in order for Session Delivery Manager to install properly.

To set the locale:

1. Log in as root.
2. Run the following command to set the locale to en_US.UTF-8:

   ```
   export LC_ALL=en_US.UTF-8
   ```

OpenSSL Required for HTTPS

If you plan to use HTTPS, you need OpenSSL installed on the Session Delivery Manager server before you install Session Delivery Manager. Check the version using the following command:

```
openssl version
```

Downloading OpenSSL

If not already installed, download the following OpenSSL file from www.openssl.org/source/:

openssl-0.9.7e.tar.gz

Follow the directions supplied by OpenSSL to install the files.

Displaying Shared Libraries

You need to display the shared libraries and check that they are connected. If any libraries are not connected, you can create soft links for them. For example, in Fedora Core 13 you might need to create soft links for two libraries.

To display shared libraries:

1. As root user, change to the httpserver bin directory. For example:

   ```
   cd /opt/AcmePacket/NNC73/Apache/httpserver/bin
   ```

2. Run the following command to display the shared libraries:

   ```
   ldd httpd
   ```

   Output similar to the following for Fedora Core 13 appears:

   ```
   linux-vdso.so.1 =>  (0x00007fff9e8b0000)
   libm.so.6 => /lib64/libm.so.6 (0x0000003b7f400000)
   libaprutil-1.so.0 => /usr/lib64/libaprutil-1.so.0 (0x00007f85607ea000)
   libexpat.so.0 => (file not found)
   libuuid.so.1 => /lib64/libuuid.so.1 (0x0000003b83800000)
   librt.so.1 => /lib64/librt.so.1 (0x0000003b80400000)
   libcrypt.so.1 => /lib64/libcrypt.so.1 (0x0000003b8fe00000)
   libpthread.so.0 => /lib64/libpthread.so.0 (0x0000003b7fc00000)
   libdl.so.2 => /lib64/libdl.so.2 (0x0000003b7f800000)
   libc.so.6 => /lib64/libc.so.6 (0x0000003b7f000000)
   libdb-4.8.so => /lib64/libdb-4.8.so (0x0000003b95200000)
   /lib64/ld-linux-x86-64.so.2 (0x0000003b7e800000)
   libfreebl3.so => /lib64/libfreebl3.so (0x0000003b90200000)
   ```

   One of the shared libraries libexpat.so.0 is not found. A soft link must be created for it.

Creating Soft Links

You can create soft links for any shared libraries that are not connected.

To create soft links:

1. As root user, change directory to /usr/lib64.
2. Create links for any unlinked shared libraries. For example:

   ```
   ln -s libexpat.so.1.5.2 libexpat.so.0
   ln -s libexpat.so.1.5.2 ../../lib64/libexpat.so.0
   ```

Setting the Maximum Shared Memory in FC13

The default maximum shared memory on Fedora Core 13 is set to 33M by default. Oracle reccomends setting the maximum shared memory to at least 15% of the total system memory.

To set the maximum shared memory in FC13:

1. Login as root.
2. See what the current value for maximum shared memory is by entering the following line:

   ```
   more /proc/sys/kernel/shmmax
   ```

3. See what hte available system memory in bytes is by entering the following line:

   ```
   free -b
   ```

4. Set the new value by enterting the following lines:

```
sysctl -w kernel.shmmax=26000000000
sysctl -p /etc/sysctl.conf
```

Note: The value entered is required to be greater than 15% and no more than 50% of the total system memory.

5. Verify the changes were saved by entering the following line:

```
more /proc/sys/kernel/shmmax
```

Creating nncentral Group and User

For security reasons, you can create an account named nncentral and a group named nncentral. You also must install the UNIX sudo facility and define sudo privileges. After the Session Delivery Manager installation, all the installed files are owned by nncentral. The main Session Delivery Manager process has to run as sudo user in order to have access to port 162.

Creating nncentral Group and User

To create nncentral group and user:

1. Login as root.
2. Enter the following lines:
   - For RedHat 5.5 and CentOS 5.5:

     ```
     groupadd nncentral
     useradd -m -g nncentral -d /home/nncentral -s /usr/bin/bash nncentral
     passwd nncentral
     ```
   - For RedHat 6.2 and CentOS 6.2:

     ```
     groupadd nncentral
     useradd -m -g nncentral -d /home/nncentral -s /bin/bash nncentral
     passwd nncentral
     ```

Editing the sudoer Configuration File

You need to use the visudo tool to make edits to the sudoer configuration. The visudo tool is based on vi editor; you can use all vi editor commands. The Session Delivery Manager administrator needs to provide a sudo password when starting Session Delivery Manager.

1. Login as root.
2. Execute visudo.
   - For RHEL 5.5 or CentOS 5.5:

     ```
     cd /usr/sbin/visudo
     ```
   - For RHEL 6.2 or CentOS 6.2:

     ```
     visudo -f /etc/sudoers.d/nncentral
     ```
3. Add the following lines to the sudoer configuration and issue a save using vi commands:

   ```
   root ALL=(ALL)ALL
   Defaults:ALL timestamp_timeout=0
   nncentral ALL=/opt/AcmePacket/NNC*/jre/bin/java -Dlog4j.configuration=* -cp
   * com.acmepacket.ems.server.services.snmp.TrapRelay.TrapRelay *
   ```

   The following example shows the lines added using the hostname mynnchost:

   ```
   root mynnchost=(ALL)ALL
   Defaults:ALL timestamp_timeout=0
   nncentral ALL=/opt/AcmePacket/NNC*/jre/bin/java -Dlog4j.configuration=* -cp
   * com.acmepacket.ems.server.services.snmp.TrapRelay.TrapRelay *
   ```
4. Execute the following command if you are running RHEL 6.2 or CentOS 6.2:

   ```
   # chmod 0440 /etc/sudoers.d/nncentral
   # chown root:root /etc/sudoers.d/nncentral
   ```

Installing Net-Net Central

This section explains how to install and setup Session Delivery Manager on the Session Delivery Manager server. The steps are the same for all supported operating systems.

To install Session Delivery Manager, you need to obtain the appropriate tar.gz file for your environment and the AcmePacketNetNetCentral.xml license file from your Oracle representative. You explode the tar file contents on your server and run the setup script to configure Session Delivery Manager.

Installing Net-Net Central

To install Session Delivery Manager:

1. Obtain the appropriate tar.gz file from the Oracle customer portal. The tar.gz files include the following:
   - NNC73FC1364bit.tar.gz for Linux Fedora Core 13 64 bit installation
   - NNC73Linux64bit.tar.gz for Linux RHEL v5.5 64 bit installation
   - NNC73RHEL62.tar.gz for RHEL v6.2 64 bit, CentOS v6.2, and the NNC-VM installation
2. FTP the tar.gz file to your system. Place the file in the directory where you want the Session Delivery Manager software to reside after you unzip the tar.gz file. For example, FTP the tar file to the /opt directory.

   Note: You cannot install an older version of Session Delivery Manager in the same directory as a newer version.
3. Unzip the *.tar.gz file.

   ```
   gunzip <filename>.tar.gz
   ```
4. Extract the files using one of the following commands:

   ```
   tar -xvf <filename>.tar
   ```

   From here you run setup to configure Session Delivery Manager.

Running Setup

The following steps show running setup on a Linux system.

To run setup:

1. Login as root user.
2. Navigate to the bin directory. For example:

   ```
   cd /opt/AcmePacket/NNC73/bin
   ```
3. Run setup.sh.

   ```
   ./setup.sh
   ```

   A Welcome message appears and initialization processes occur. Setup checks that minimal system requirements are met and checks system port availability for Session Delivery Manager components.

   This process may take several minutes to complete. Do not kill the setup.sh process during this time or you will risk corrupting the system.

   ```
   [root@nms-vm4 opt]# cd AcmePacket/NNC73/bin/
   [root@nms-vm4 bin]# ./setup.sh
   ============================================================
   Welcome to Session Delivery Manager Setup application
   Version : NNCMainB11
   OS : Linux : amd64 : 2.6.18-194.el5xen
   ============================================================
   Please wait while application loads
   Checking environment and setting permissions.
   Please wait ....
   100%[==================================================]
   ```

```
=============================================================
System Physical Memory Diagnostics
Total System Physical Memory = 16384 MB
Total System Free Physical Memory = 15057 MB
Dynamic memory allocation in progress
Previous database cache 262144000
New database cache 2907701248
Previous JVM Xmx size 1024
New JVM Xmx size 8092
=============================================================
System Disk Space Diagnostics
Total System Disk Space = 127 GB
Free System Disk Space = 117 GB
WARNING: Disk space is insufficient for running this application.
The recommended total disk space that should be available is = 300 GB
=============================================================
System Port Availability Diagnostics : Session Delivery Manager Required
Ports
The following port is available [ 5000 ]
The following port is available [ 8080 ]
The following port is available [ 61616 ]
The following port is available [ 9000 ]
The following port is available [ 8443 ]
The following port is available [ 1099 ]
The following port is available [ 8009 ]
The following port is available [ 1098 ]
The following port is available [ 8005 ]
=============================================================
```

Note: A warning message appears if you have less than the recommended minimum physical memory. Proceeding without the recommended minimum physical memory may result in performance degradation.

After the diagnostics, the setup options appear.

```
Set up options
TYPICAL      : This setup procedure walks the user through
               the minimal setup configuration required to
               configure Net-Net server.
CUSTOM       : This setup procedure provides the user with
               a set of options to manually pick and
               choose from.
[X] 1 - Typical : Runs through most common set up options. (Recommended)
[Default]
[ ] 2 - Custom  : Allows manual customization. (Advanced users)
[ ] 3 - Quit    : Finish and quit setup.
Please select an option [1]
```

Choose the Typical setup option if you are new to Session Delivery Manager or just want to create the minimal configuration required by the Session Delivery Manager server. Choose Custom if you are a more advanced user or are licensed for applications hosted on Session Delivery Manager. The Custom setup also includes the options available on the Typical setup.

You can run the setup repeatedly to change existing configuration values and to access any new Custom options as a result of licensing additional applications.

Typical Setup

The Typical setup performs the minimal configuration required by the Session Delivery Manager server in order to run properly. If this is your first time installing Session Delivery Manager, you will need to exercise all options in the Typical Setup to fully configure the Session Delivery Manager server.

To perform a typical setup:

1. Press Enter to accept the default value 1 for a typical setup. You are prompted about continuing.

2. Enter Y and press Enter to continue. The list of Typical configuration options appears.

```
Do you want to continue Yes/No?Y
============================================================
============================================================
Typical Configuraiton
will walk through basic configuraiton options.
[X]  1 - Check and Apply License   [Default]
[ ]  2 - HTTP/HTTPS configuration
[ ]  3 - Fault Management configuration
[ ]  4 - Mail Server configuration
[ ]  5 - Quit setup
Please select an option[1]
```

3. Verify with your system administrator that you have the correct sudo password before continuing.
4. Press Enter to accept the default value of 1 for checking and applying the Session Delivery Manager license. You are prompted about continuing.
5. Enter Y and press Enter to continue. The license options appear.

```
Do you want to continue Yes/No?Y

============================================================

Check and Apply License
This option allows the end user to validate an existing license,
provide a license or re-apply a Acme Packet Net-Net Central license

Acme Packet Net-Net Central management
Acme Packet Net-Net Central license will be checked, applied and validated.

Please choose to quit license management or apply new license
[X]  1 - Quit   [Default]
[ ]  2 - Apply new license


Please select an option [1]
```

Applying the License

You need a valid license to be able to start the Session Delivery Manager servers. You can apply a new license or check an existing license and accept that.

To apply the license:

1. Enter 2 and press Enter. You are prompted about continuing.
2. Enter Y and press Enter to continue. You are prompted for the license directory and filename.

```
Do you want to continue Yes/No?Y

Please specify the source directory and file name of Acme Packet Net-Net license
Source Directory [        ]
```

3. Enter the name of the directory where the license file is located and the name of the license file and press Enter. For example:

```
/opt/AcmePacketNetNetCentral.xml
```

The license is located and the details appear on the screen.You are prompted about accepting the license.

```
Please specify the source directory and file name of Acme Packet Net-Net license
Source Directory [        ] /opt/AcmePacketNetNetCentral.xml
Source Directory [/opt/AcmePacketNetNetCentral.xml]

License Details
License number                  : -1002
ClientName                      : AcmePacket-Internal
LicenseType                     : permanent
IssuedDate                      : Thu Sep 30 11:43:00 EDT 2010
Key                             : 2.0.1
StartDate                       : 2010-09-30
ExpirationDate                  :
Cluster                         : Enabled

Applications
Application                     Number of licensed devices
RouteManager                    : 8000


Accepting this license will replace an existing license
[X]  1 - Accept license   [Default]
[ ]  2 - Do not accept license


Please select an option [1] ▉
```

4. Press Enter to accept the default and accept the license. You are prompted about continuing.
5. Enter Y and press Enter to continue. The license is accepted and the list of setup options appears.

```
Do you want to continue Yes/No?Y
[ ]  1 - Check and Apply License   [Default]
[X]  2 - HTTP/HTTPS configuration
[ ]  3 - Fault Management configuration
[ ]  4 - Mail Server configuration
[ ]  5 - Quit setup
```

6. Please select an option[2]

   The next setup option is for configuring the Apache load balancer to run in either HTTP or HTTPS mode. The Apache load balancer is responsible for distributing the load by redirecting traffic to the front end servers.

HTTP

To configure HTTP mode:

Note: You cannot use the value root for either the user or group name.

1. Press Enter to accept the default. You are prompted about continuing.
2. Enter Y and press Enter to continue. The HTTP/HTTPS options appear.

```
Do you want to continue Yes/No?Y

============================================================

HTTP/HTTPS configuration
Set up HTTP or HTTPS configuration
[X]  1 - HTTP mode - Configure server to run in HTTP mode   [Default]
[ ]  2 - HTTPS mode - Configure server to run in HTTPS mode


Please select an option [1] ▉
```

3. Press Enter to accept the default to configure HTTP. You are prompted about continuing.
4. Enter Y and press Enter to continue. You are prompted for the username of the server process.

```
Do you want to continue Yes/No?Y

HTTP mode
Configure server to run in HTTP mode

Enter the user name of the server process which determines what files the server is allowed to access. Any fi
les inaccessible to this user are also inaccessible to clients connecting to the Apache HTTP Server.
Apache User [nncentral]
```

5. Press Enter to accept the default value nncentral. You are prompted for the group name.

```
Enter the group name of the Apache HTTP Server processes
Apache Group [nncentral]
```

6. Press Enter to accept the default value nncentral. You are prompted for the port number.

```
Enter the port number that the Apache HTTP Server should listen on
Apache Port Number (1024-65535) [8080]
```

7. Press Enter to accept the default value 8080. The list of Typical setup options appears.

```
Apache Port Number (1024-65535) [8080]
```

Note: You cannot use a port number reserved for Session Delivery Manager components.

HTTPS

To configure HTTPS mode:

1. Enter 2 to configure HTTPS and press Enter. You are prompted about continuing.

```
Please select an option [1] 2


[ ]  1 - HTTP mode - Configure server to run in HTTP mode   [Default]
[X]  2 - HTTPS mode - Configure server to run in HTTPS mode


Do you want to continue Yes/No?
```

2. Enter Y and press Enter to continue. You are prompted for the user name for the server process.

```
Do you want to continue Yes/No?
HTTPS mode
Configure server to run in HTTPS mode
Enter the user name of the server process which determines what files the
server is allowed to access. Any files inacces
sible to this user are also inaccessible to clients connecting to the
Apache HTTP Server.
Apache User [nncentral]
Enter the group name of the Apache HTTP Server processes
Apache Group [nncentral]
```

3. Press Enter to retain the default nncentral. You are prompted for the group name.

```
Apache User [nncentral]

Enter the group name of the Apache HTTP Server processes
Apache Group [nncentral]
```

4. Press Enter to retain the default nncentral. You are prompted for the port number the server should listen on.

```
Enter the port number that the Apache HTTP Server should listen on
Apache Port Number (1024-65535) [8443]
```

Note: You cannot use a port number reserved for Net-Net Central components.

5. Press Enter to retain the default 8443. You are prompted for the server's DNS name.

```
The server name(DNS name of this server)
Server name []
```

6. Enter the DNS name of the server and press Enter. You are prompted about creating a self-signed certificate.

```
Would you like to create a self signed certificate?
[ ]  1 - Yes
[X]  2 - No   [Default]


Please select an option [2] ▉
```

Skip to Creating Self-Signed Certificate to create a self-signed certificate.

No Self-Signed Certificate

1. Retain the default value No if you do not want to create a self-signed certificate.
2. Press Enter. You are prompted about continuing.
3. Enter Y to continue and press Enter. You are prompted for the private key file.

```
Do you want to continue Yes/No?Y

The private key file
Private key file [] ▉
```

4. Enter the file name, including the path, and press Enter. You are prompted for the certificate file.
5. Enter the file name, including the path, and click Enter. You are prompted about intermediate certificates.
6. Press Enter to accept the default. You are prompted about continuing.
7. Enter Yes to continue. You are prompted for the alias name for the certificate in the truststore.
8. Press Enter to accept the default or enter a different alias name and press Enter. You are prompted for the trustore password.
9. Press Enter to accept the default or enter a different password and press Enter.

Creating Self-Signed Certificate

To create a self-signed certificate:

1. Enter 1 if you want to create a self-signed certificate and press Enter. You are prompted about continuing.

```
Please select an option [2] 1


[X]  1 - Yes
[ ]  2 - No   [Default]


Do you want to continue Yes/No?Y
```

2. Enter Y to continue and press Enter. You are prompted for the common name (DNS name) of the server.
3. Enter the DNS name of the server and press Enter. You are prompted for the certificate alias name in the trustore.
4. Retain the default or enter a different alias name and press Enter. You are prompted for the trustore password.
5. Enter the trustore password and press Enter. The Typical install list of options appears.

```
[ ]  1 - Check and Apply License   [Default]
[ ]  2 - HTTP/HTTPS configuration
[X]  3 - Fault Management configuration
[ ]  4 - Mail Server configuration
[ ]  5 - Quit setup
```

From here you configure fault management.

Note: Verify with your system administrator that you have the correct sudo password before continuing.

Fault Management Configuration

To configure fault management:

1. Press Enter to accept the default. You are prompted about continuing.
2. Enter Y and press Enter. Two options appear.

```
Do you want to continue Yes/No? Y
================================================

Fault Management configuration
This option is used to confiure the fault management settings.

[x] 1 - Configure SNMP trap settings  [Default]
[ ] 2 - Quit out of fault management configuration

Please select an option [1]
```

3. Press Enter to accept the default value Configure SNMP trap settings. You are prompted about continuing.
4. Enter Y and press Enter. You are prompted for the port number the Trap Relay should listen on. The valid range is 1-65525. The default is 162.

```
Do you want to continue Yes/No? Y

Enter the port number that Trap Relay should listen on: (1-65535) [162]
```

Configuring the sudo Password

Session Delivery Manager requires the sudo password to configure Trap Relay on ports 1024 and under. You set the sudo password to match the sudo password that has been defined by the system administrator. Installation automatically skips these steps if you select a port 1025 or higher.

To configure a sudo password:

1. You are prompted for the sudo password.

```
Session Delivery Manager requires entry of the sudo password in order to
support internal components that require sudo user privileges.
The password you supply will be securely encrypted.

Enter sudo password: []
```

   Enter the sudo password for user account nncentral and press Enter. You are prompted to confirm the password.

2. Enter the password again and press Enter. The confirmation message appears.

```
Confirm sudo password:  []
Sudo password entered and encrypted successfully!
[ ]  1 - Check and Apply License   [Default]
[ ]  2 - HTTP/HTTPS configuration
[ ]  3 - Fault Management configuration
[X]  4 - Mail Server configuration
[ ]  5 - Quit setup
Please select an option [4]
```

Custom Setup

Custom setup options are for the more advanced user or for those users who are licensed for separate applications. The setup options for those applications are found are included in Custom. For example, if you are licensed for Route Manager, options for Route Manager Central and SAML Single sign on appear in the list.

What appears on the list of setup options can differ depending on what applications you are licensed for. One setup option for the Mail Server always appears on the list but is only applicable if you have a license for Element Manager. This section includes the instructions for all currently supported applications. What you see can be different depending on your licenses.

You can run the setup.sh script repeatedly to access the Custom setup options. Please note that you must run all setup options of Typical Setup before configuring Custom setup options.

Accessing Custom Options

The following instructions are based on configuring setup options on a Linux system.

To access custom setup options:

1. Login as root user.
2. Navigate to the bin directory. For example:

```
cd /opt/AcmePacket/NNC73/bin
```

3. Run setup.sh.

```
./setup.sh
```

A Welcome message appears and initialization processes occur. Setup checks that minimal system requirements are met and checks system port availability for Session Delivery Manager components.

Note: A warning message appears if you have less than the minimum recommended physical memory. Proceeding without hte minimum recommended memory may result in performance degradation.

After the diagnostics, the setup options appear.

```
Set up options
TYPICAL   : This setup procedure walks the user through
            the minimal setup configuration required to
            configure Net-Net server.
CUSTOM    : This setup procedure provides the user with
            a set of options to manually pick and
            choose from.

[x] 1 - Typical : Runs through most common setup options. (Recommended)
[Default]
[ ] 2 - Custom  : Allows manual customization. (Advanced users)
[ ] 3 - Quit    : Finish and quit setup.

Please select an option [1] 2
```

4. Enter 2 for Custom and press Enter. You are prompted about continuing.
5. Enter Y and press Enter. The custom setup options appear.

```
[ ] 1 - Typical : Runs through most common set up options.
[X] 2 - Custom : Allows manual customization.
[ ] 3 - Check : Finish and quit setup.
Do you want to continue Yes/No?Y
=======================================================
[X] 1 - Check and Apply License [Default]
[ ] 2 - HTTP/HTTPS configuration
[ ] 3 - Fault Management configuration
[ ] 4 - Session Delivery Manager cluster management
[ ] 5 - Route Manager Central configuration
[ ] 6 - SAML Single sign on configuration
[ ] 7 - Mail Server configuration
[ ] 8 - Trunk Manager configuration
[ ] 9 - Quit setup
Please select an option [1] 1
```

See the information in Typical Setup for details about the following options:

- Check and Apply License
- HTTP/HTTPS configuration
- Fault Management configuration

See the following sections for details about the custom options.

Cluster Management

If you are licensed for Element Manager, the Session Delivery Manager cluster management option appears. Access this option to configure and manage a cluster of Session Delivery Manager servers for High Availability (HA). See the Session Delivery Manager High Availability Guide for more information about HA and clusters.

Note: Ensure you synchronize time on each server with NTP before adding it to a cluster.

To configure clusters:

1. Enter 4 and press Enter. You are prompted about continuing.
2. Enter Y and press Enter. The cluster management options appear.

```
Do you want to continue Yes/No?Y

============================================================

Net-Net Central cluster management.
This option is used to configure NNC as part of a cluster

Management options
The host machine can run as a standalone or member of a Net-Net Central cluster.

Please choose to quit cluster management or apply new configuration
[X]  1 - Configure and manage members in cluster   [Default]
[ ]  2 - Run current host as a standalone
[ ]  3 - Quit out of cluster configuration


Please select an option [1]
```

Manage Cluster Members

1. Press Enter to configure and manage members in a cluster. You are prompted about continuing.
2. Enter Yes and press Enter. The cluster member management options appear.

```
Do you want to continue Yes/No?Yes
Host name               | DB    | MOM   | Web Worker
                        | Port  | Port  | Port
localhost               | 9000  | 61616 | 8009

Use the following options to add or remove members from cluster.
[ ]  1 - Add a new member
[ ]  2 - Remove all remote members
[ ]  3 - Apply new cluster configuration
[X]  4 - Cancel out and do not apply changes   [Default]


Please select an option [4]
```

Adding New Members

To add new member to a cluster:

1. Enter 1 and press Enter. You are prompted about continuing.
2. Enter Y and press Enter. You are prompted for the IP address of the host you want to add.

```
Do you want to continue Yes/No?Y
Host name          | DB    | MOM   | Web Worker
             | Port  | Port  | Port
localhost          | 9000  | 61616 | 8009
Provide the IP address of the Host requiring membership to the cluster.
Member host name [ ]
```

3. Enter the IP address for the host you are adding to the cluster and press Enter. A confirmation message appears and the options appear again.

```
Provide the IP address of the Host requiring membership to the cluster.
Member host name [ ]172.30.80.19
Valid remote member has been added
Host name          | DB    | MOM   | Web Worker
             | Port  | Port  | Port
localhost          | 9000  | 61616 | 8009
============= Remote members =============
172.1.30.185          | 9000  | 61616 | 8009
172.30.80.19          | 9000  | 61616 | 8009
Use the following options to add or remove members from cluster.
[ ]  1 - Add a new member
[ ]  2 -
[X]  3 - Apply new cluster configuration
[ ]  4 - Cancel out and do not apply changes [Default]
```

4. Repeat steps to add additional hosts to the cluster. When you are done adding hosts to the cluster you can apply the new cluster configuration.
5. Press Enter to accept the default 3 Apply new cluster configuration. (Or you can cancel out of creating a cluster without applying your changes.) You are prompted about continuing.
6. Enter Yes and press Enter. The cluster members are displayed and the cluster management options appear.

```
Do you want to continue Yes/No?Y
Host name               | DB    | MOM   | Web Worker
                        | Port  | Port  | Port
172.30.1.185            | 9000  | 61616 | 8009

============= Remote members ==============
172.30.80.19            | 9000  | 61616 | 8009
172.30.80.9             | 9000  | 61616 | 8009
172.30.80.198           | 9000  | 61616 | 8009

Please choose to quit cluster management or apply new configuration
[X]  1 - Configure and manage members in cluster   [Default]
[ ]  2 - Run current host as a standalone
[ ]  3 - Quit out of cluster configuration


Please select an option [1] ▉
```

7. Enter 3 and press Enter to quit out of the cluster configuration. You are prompted about continuing.
8. Enter Y and press Enter. The Configure sftp information options appear and your are prompted about your host being a member of a Session Delivery Manager cluster.

```
Please select an option [1] 3


[ ]  1 - Configure and manage members in cluster   [Default]
[ ]  2 - Run current host as a standalone
[X]  3 - Quit out of cluster configuration


Do you want to continue Yes/No?Y

Configure sftp information
Make sure to configure sftp properties if there are members in the cluster

Will this machine be a member of a Net-Net Central cluster?
[ ]  1 - Yes
[X]  2 - No   [Default]


Please select an option [2] ▯
```

9. Press Enter to retain the default value No or enter 1 to add your current host to the cluster. See the following section for instructions.

Adding Current Host to Cluster

You can include the host on which you are running setup in the cluster.

1. Enter Y to continue when prompted. A prompt appears for the username to use to SFTP files from the host.

```
Please select an option [2] 1


[X]  1 - Yes
[ ]  2 - No   [Default]


Do you want to continue Yes/No?Y

Please enter the username to use to sftp files off of this machine
Username []
```

2. Enter the username you want to use to SFTP files and press Enter. You are prompted for the password.
3. Enter the password to use to SFTP files and press Enter. The Custom setup options appear.

```
Please enter the username to use sftp files off of this machine
Username [] nncentral
Please enter the password for the username
Password []
[ ] 1 - Check and Apply License [Default]
[ ] 2 - HTTP/HTTPS configuration
[ ] 3 - Fault Management configuration
[ ] 4 - Session Delivery Manager cluster management
[X] 5 - Route Manager Central configuration
[ ] 6 - SAML Single sign on configuration
[ ] 7 - Mail Server configuration
[ ] 8 - Trunk Manager configuration
[ ] 9 - Quit setup
Please select an option [5]
```

Removing Members from Cluster

There are two reasons why you would remove all members from a cluster. Either you are eliminating the cluster or you want to retain the cluster but remove a member. Both of these require you remove all members from the cluster. If you are eliminating the cluster, you are done. If you are removing a member, you need to re-add the members you want to retain to the cluster.

To remove members from the cluster:

1. Enter 4 and press Enter to choose Session Delivery Manager cluster management. You are prompted about continuing.
2. Enter Y and press Enter to continue. The cluster management options appear.
3. Press Enter to retain the default value. You are prompted about continuing.
4. Enter Y and press Enter to continue. The add and remove members options appear.

```
Do you want to continue Yes/No?Y
Host name               | DB    | MOM   | Web Worker
                        | Port  | Port  | Port
172.30.1.185            | 9000  | 61616 | 8009

============= Remote members ==============
172.1.30.185            | 9000  | 61616 | 8009
172.30.80.19            | 9000  | 61616 | 8009
172.30.80.9             | 9000  | 61616 | 8009

Use the following options to add or remove members from cluster.
[ ]  1 - Add a new member
[ ]  2 - Remove all remote members
[ ]  3 - Apply new cluster configuration
[X]  4 - Cancel out and do not apply changes   [Default]


Please select an option [4]
```

5. Enter 2 to choose Remove all remote members and press Enter. You are prompted about continuing.
6. Enter Y to continue and press Enter. You are prompted that the operation removes all remote members from the edition configuration session. By default, the Cancel out of clear operation option is selected.

```
Do you want to continue Yes/No?Y

This operation will remove all remote members from the edition configuration session.
[ ]  1 - Proceed with removing all remote members
[X]  2 - Cancel out of clear operation   [Default]


Please select an option [2] 1
```

7. Enter 1 to choose Proceed with removing all remote members. You are prompted about continuing.
8. Enter Y and press Enter to continue. All remote nodes are removed and only the host you on which you are running Session Delivery Manager is visible. The cluster management options also appear.

```
Do you want to continue Yes/No?Y
Host name               | DB    | MOM   | Web Worker
                        | Port  | Port  | Port
172.30.1.185            | 9000  | 61616 | 8009

Use the following options to add or remove members from cluster.
[ ]  1 - Add a new member
[ ]  2 - Remove all remote members
[ ]  3 - Apply new cluster configuration
[X]  4 - Cancel out and do not apply changes   [Default]


Please select an option [4]
```

9. Enter 3 to apply the new cluster configuration to apply your changes. You are prompted about continuing.
10. Enter Y and press Enter to continue.

Run Current Server as Standalone

You can configure the current server as a standalone to remove it from a cluster. All other members of the cluster are removed as well. You need to re-add any members you want to retain in the cluster.

1. Enter 2 and press Enter. You are prompted about continuing.
2. Enter Y and press Enter to continue. The cluster member list appears with a warning that the server is part of a cluster and configuring it as a standalone removes it from the cluster. (All other members are removed as well and need to be re-added to the cluster if you want to retain them.)
3. Press Enter to continue configuring the server as a standalone. You are prompted about continuing.

4. Enter Y to continue and press Enter. All members of the cluster are removed and the current server is now considered a standalone.

```
Do you want to continue Yes/No?Y
Host name               | DB    | MOM   | Web Worker
                        | Port  | Port  | Port
localhost               | 9000  | 61616 | 8009

Please choose to quit cluster management or apply new configuration
[X]  1 - Configure and manage members in cluster   [Default]
[ ]  2 - Run current host as a standalone
[ ]  3 - Quit out of cluster configuration


Please select an option [1] ▉
```

5. Press Enter to configure and manage members in cluster if you want to retain the other members. You need to re-add them to recreate the cluster. Or enter 3 and press Enter to quit the cluster configuration.
6. Enter Y to continue and press Enter.

Route Management Central

If you are licensed for the Route Manager application, you can access the Net-Net Route Management Central configuration setup option. If you are not licensed for Route Manager, this setup option will not be visible.

1. Enter 5 and press Enter. You are prompted about continuing.
2. Enter Y and press Enter to continue. You are prompted for the maximum number of route set backups.

```
Do you want to continue Yes/No?

=========================================================

Route Manager Central configuration
Configure Route Manager Central properties

Configure number of route set backups per route set/backup type combination
Route Manager Central

Please enter the maximum number of route set backups per route set/backup type c
ombination
# of backups (1-500) [10]
```

3. Enter a value within range or press Enter to accept the default value. The Custom setup list of options appears. You can now configure SAML single sign-on.

Configuring SAML Single Sign-On

If you are licensed for the Route Manager application, you can access the SAML single signon configuration setup option. If you are not licensed for Route Manager, this setup option will not be visible.

The Route Manager application supports login through an external server using SAML single sign-on. You enter a username and password used in the request to the external server for authentication. If using self-signed certificates, you can import them into the Route Manager certificates file (cacerts).

To configure SAML single sign-on:

1. Press Enter to accept the default value 6. You are prompted about continuing.
2. Enter Y and press Enter. You are prompted for the username,

```
SAML Single sign on configuration
Provides SAML Single sign on authentication.

SAML Single sign on
Configure SAML Single sign on

Please enter the username for basic authentication to SAML Responder
Username [] ▉
```

3. Enter the username for basic authentication and press Enter. You are prompted for the password.

```
Please enter the password for basic authentication to SAML Responder
Password [] ▉
```

4. Enter the password required for basic authentication and press Enter. You are prompted about the connection timeout.

```
Please enter the connection timeout to the SAML Responder
Connection timeout (seconds) (5-60) [5] ▉
```

5. Retain the default value 5. You are prompted about importing a certificate.

```
Would you like to import a certificate?
[ ]  1 - Yes
[X]  2 - No   [Default]


Please select an option [2] ▉
```

   If you do want to import a certificate, see the following section for details.

6. Press Enter to retain the default value No. You are done configuring SAML single sign-on.
7. Press Enter to quit setup. You are prompted about continuing.
8. Enter Y and press Enter to quit the setup program.

Importing Certificates

To import certificates:

1. Enter 1 and press Enter to import certificates. You are prompted about continuing.

```
Please select an option [2] 1


[X]  1 - Yes
[ ]  2 - No   [Default]


Do you want to continue Yes/No?▉
```

2. Enter Y and press Enter. You are prompted for the import method.

```
Choose the import method
[X]  1 - File   [Default]
[ ]  2 - HTTP mode


Please select an option [1] ▉
```

3. Press Enter to accept the default File. (If you choose the HTTP mode instead, you need to enter the same information.) You are prompted about continuing.
4. Enter Y and press Enter to continue. You are prompted for the alias name of the imported certificate.

```
Do you want to continue Yes/No?Y

Please enter the alias name for the imported certificate
Alias name [] ▉
```

5. Enter the alias name and press Enter. For example, acmep.csr. You are prompted for the certificate file.

```
Please enter the alias name for the imported certificate
Alias name [] acmep.csr

Please enter the certificate file
File [] ▌
```

6. Enter the name of the certificate file and press Enter. For example, apkt.cer. The loading process occurs and the certificate is added to the keystore using the alias. You are prompted about adding another.
7. Press Enter to accept the default value No. (Or Enter 1 to continue and repeat the steps for adding more.) You are prompted about continuing.
8. Enter Y to continue and press Enter.

Mail Server

The Mail server setup option is visible even if you are not licensed for Element Manager or Report Manager. If you are licensed for Report Manager, you can setup the mail server credientials to enable the sending of emails to a targeted Microsoft Exchange and Gmail server.

To configure the mail server:

1. Press Enter to accept the default of 7 for Mail Server configuration setup. You are prompted about continuing.

```
============================================================

[ ] 1 - Check and Apply License [Default]
[ ] 2 - HTTP/HTTPS configuration
[ ] 3 - Fault Management configuration
[ ] 4 - Session Delivery Manager cluster management
[ ] 5 - Route Manager Central configuration
[ ] 6 - SAML Single sign on configuration
[X] 7 - Mail Server configuration
[ ] 8 - Trunk Manager configuration
[ ] 9 - Quit setup

Please select an option [7]

Do you want to continue Yes/No?
```

2. Enter Y and press Enter. The mail server configuration options appear.

```
Mail Server configuration
This option is used to configure mail server
Configure mail server
Mail server configuration can be used for trap notification.
Please choose to quit mail server configuration or apply new configuration
[X]  1 - Configure mail server   [Default]
[ ]  2 - Quit out of mail server configuration
Please select an option [1]
```

3. Press Enter to configure the mail server. You are prompted to continue.
4. Enter Y and press Enter to continue. The status of the mail server indicates it is not configured and the mail server host options appear.

```
Do you want to continue Yes/No?
Mail server: Not configured

Use the following options to configure mail server host.
[X] 1 - Configure mail server host
[ ] 2 - Apply new mail server configuration  [Default]
[ ] 3 - Cancel out and do not apply changes


Please select an option [1]
```

5. Press Enter to configure the mail server host. You are prompted to continue.
6. Enter Y to continue. You are prompted for the server DNS name.

```
Do you want to continue Yes/No?Y
Mail server: Not configured

Provide the DNS name.
Host name [ ]
```

7. Enter the DNS name and press Enter. For example, mail.acmepacket.com. If configuring a Gmail server you might enter smtp.gmail.com. The mail server name is changed and the mail server configuration options appear.

```
Do you want to continue Yes/No?Y
Mail server: Not configured

Provide the DNS name.
Host name [ ] mail.acmepacket.com
Mail server host name has been changed
Mail from: Not configured

Use the following options to configure mail from.
[X]  1 - Configure mail from
[ ]  2 - Apply new mail server configuration
[ ]  3 - Cancel out and do not apply changes   [Default]


Please select an option [1]
```

8. Press Enter to configure the From address you want to use. You are prompted about continuing.
9. Enter Y and press Enter to continue. You are prompted for the mail from address.
10. Enter the address you want used for the From address and press Enter. For example, if sending to Microsoft Exchange account mailadmin@acmepacket.com. If sending to a Gmail account, mailadmin@gmail.com. You are prompted about the mail server properties.

```
Provide the mail from.
Mail from [ ] mailadmin@acmepacket.com
Mail from has been changed
Mail server propertiesNot configured
Configure Mail server properties
[X]  1 - Configure Mail server properties
[ ]  2 - Apply new mail server configuration
[ ]  3 - Cancel out and do not apply changes   [Default]
Please select an option [1]
```

11. Press Enter to configure mail properties. You are prompted about continuing.
12. Enter Y and press Enter to continue.
13. Enter the mail server properties for your mail server.

```
Do you want to continue Yes/No?
Mail server propertiesNot configured
Provide the server properties if needed.
Mail server properties [ ] mail.smtp.starttls.enable:true
Mail server properties have been changed
Mail logon required: Not configured
```

Note: The format for entering multiple mail server properties is:

```
property1:value1;property2:value2;property3:value3
```

14. Press Enter to continue. You are prompted whether to configure whether the mail logon is required.
15. Press Enter if logon is not required. Or enter true and press Enter. If false, the mail server host configuration options appear. If true, the mail logon user configuration options appear.

```
Provide the mail logon required.
Mail logon required true/false [false] true
Mail logon required has been changed
Mail logon user: Not configured

Use the following options to configure mail logon user.
[X]  1 - Configure mail logon user
[ ]  2 - Apply new mail server configuration
[ ]  3 - Cancel out and do not apply changes   [Default]


Please select an option [1] ▌
```

16. Press Enter to configure the mail logon user. You are prompted about continuing.
17. Enter Y and press Enter to continue. You are prompted for the mail logon user.
18. Enter the username and press Enter. For example, if sending to a Microsoft Exchange server mailrecipient@acmepacket.com. Or for Gmail, mailrecipient@gmail.com. The mail logon user status changes and the configuration options appear.

```
Do you want to continue Yes/No?Y
Mail logon user: Not configured

Provide the mail logon user.
Mail logon user [ ] mailrecipient@acmepacket.com
Mail logon user has been changed
Mail logon user password: Not configured

Use the following options to configure mail logon user password.
[X]  1 - Configure mail logon user password
[ ]  2 - Apply new mail server configuration
[ ]  3 - Cancel out and do not apply changes   [Default]


Please select an option [1] ▌
```

19. Press Enter to configure the mail logon user password. You are prompted about continuing.
20. Enter Y to continue and press Enter. You are prompted for the password.
21. Enter the password the user enters when they logon and press Enter. (Nothing displays on the screen when you enter the password.) The logon user password status changes and the configure mail server host options appears.

```
Do you want to continue Yes/No?
Mail logon user password: Not configured

Provide the mail logon user password.
Mail logon user password [ ]
Mail logon user password has been changed
Mail server: abc

Use the following options to configure mail server host.
[ ] 1 - Configure mail server host
[X] 2 - Apply new mail server configuration  [Default]
[ ] 3 - Cancel out and do not apply changes


Please select an option [2]
```

22. You can cancel the configuration without applying the changes or press Enter to apply the changes to the mail server configuration. You are prompted about continuing.
23. Enter Y to continue and press Enter. You are prompted to either apply the new configuration or quit.

```
Please choose to quit mail server configuration or apply new configuration
[X]  1 - Configure mail server   [Default]
[ ]  2 - Quit out of mail server configuration
Please select an option [1] 2
```

```
[ ]  1 - Configure mail server   [Default]
[X]  2 - Quit out of mail server configuration
```

24. Press Enter to quit the mail server configuration. You are asked if you wish to continue.

Installing Other Licensed Applications

If you hold a license for other Session Delivery Manager applications, you can use the Custom Installation procedure to install the application.

To install your licensed application:

At the following prompt, enter the number associated with the licensed application you are installing (for example, Trunk Manager), and press Enter.

==========

[ ] 1 - Check and Apply License [Default]

[ ] 2 - HTTP/HTTPS configuration

[ ] 3 - Fault Management configuration

[ ] 4 - Session Delivery Manager cluster management

[ ] 5 - Route Manager Central configuration

[ ] 6 - SAML Single sign on configuration

[ ] 7 - Mail Server configuration

[X] 8 - Trunk Manager configuration

[ ] 9 - Quit setup

Please select an option [1] 8

==========

Follow the on-screen prompts to install the Session Delivery Manager licensed application. For more information about your licensed application, see the respective Guide. For Trunk Manager installation procedures, see the Net-Net SIP Trunk Xpress for Service Providers Guide.

Exiting Setup

You can quit the setup utility after completing the custom snstallation procedure.

To exit the setup utility:

1. Enter 9 and press Enter to quit setup.

==========

[ ] 1 - Check and Apply License [Default]

[ ] 2 - HTTP/HTTPS configuration

[ ] 3 - Fault Management configuration

[ ] 4 - Session Delivery Manager cluster management

[ ] 5 - Route Manager Central configuration

[ ] 6 - SAML Single sign on configuration

[ ] 7 - Mail Server configuration

[ ] 8 - Trunk Manager configuration

[X] 9 - Quit setup

Please select an option [1] 9

```
==========================================================
```

2. Enter Y and press Enter to quit the setup program.

```
==========================================================

Do you want to continue Yes/No? y

==========================================================
```

Starting the NNC Server

Before starting the Session Delivery Manager server, you must exit out of root. This is necessary in order for the Postgres database to startup for the Report Manager.

To start the server:

1. Exit out of root.
2. Change to the bin directory. For example:

```
cd /opt/AcmePacket/NNC73/bin
```

3. Execute the startnnc.sh script.

```
./startnnc.sh
```

Checking Running Processes

After you run startnnc.sh, you can verify that Session Delivery Manager is up and running by entering the report process status command on the system. Depending on your hardware specifications it may take a few minutes for Session Delivery Manager to start.

Execute the report process status command on the server.

```
ps -eaf | grep AcmePacket
```

When Session Delivery Manager is successfully running, you should see:

- Several httpd processes
- Three Java processes
- On some systems, you may see a fourth java process run from sudo. This is normal.

Below is an example of the system output:

```
nncentra 2494 2448 0 12:07:57 ? 0:00 httpd -d /apps/AcmePacket/NNC73/
Apache/httpserver -k start
nncentra 2504 2448 0 12:09:57 ? 0:00 httpd -d /apps/AcmePacket/NNC73/
Apache/httpserver -k start
root 2437 1 0 11:52:49 syscon 1:36 /apps/AcmePacket/NNC73/jre/bin/amd64/
java -Dlog4j.configuration=file:/apps/
root 2448 1 0 11:54:25 ? 0:00 httpd -d /apps/AcmePacket/NNC73/Apache/
httpserver -k start
root 2468 1 0 11:54:26 syscon 0:40 /apps/AcmePacket/NNC73/jre/bin/java -
Djava.util.logging.config.file=/apps/A
nncentra 2502 2448 0 12:09:56 ? 0:00 httpd -d /apps/AcmePacket/NNC73/
Apache/httpserver -k start
nncentra 2542 2533 0 14:11:24 pts/2 0:00 grep Acme
nncentra 2501 2448 0 12:09:53 ? 0:00 httpd -d /apps/AcmePacket/NNC73/
Apache/httpserver -k start
nncentra 2507 2448 0 12:12:11 ? 0:00 httpd -d /apps/AcmePacket/NNC73/
Apache/httpserver -k start
root 2443 1 0 11:54:20 syscon 0:00 sudo -S /apps/AcmePacket/NNC73/jre/bin/
java -Dlog4j.configuration=file:/app
nncentra 2505 2448 0 12:10:00 ? 0:00 httpd -d /apps/AcmePacket/NNC73/
Apache/httpserver -k start
nncentra 2500 2448 0 12:09:48 ? 0:00 httpd -d /apps/AcmePacket/NNC73/
```

```
Apache/httpserver -k start
nncentra 2508 2448 0 12:12:11 ? 0:00 httpd -d /apps/AcmePacket/NNC73/
Apache/httpserver -k start
root 2445 2443 0 11:54:20 syscon 0:03 /apps/AcmePacket/NNC73/jre/bin/java
-Dlog4j.configuration=file:/apps/AcmePa
```

Shutting down the NNC Server

There are three procedures for shutting down Session Delivery Manager depending upon your current configuration. Please refer to the applicable section below for the correct instructions.

Standalone System

To shut down a standalone system:

1. Change directory to /NNC700/bin. For example:

   ```
   cd /opt/AcmePacket/NNC700/bin
   ```

2. Execute the shutdownnnc.sh script.

   ```
   ./shutdownnnc.sh
   ```

Cluster System for NNC 7.0

Manual Clean Cluster Shutdown

To perform a manual clean cluster shutdown:

In order to avoid unnecessary database elections, first shutdown the servers running the replica databases, and then shutdown the server running the master.

1. Login to the other servers that are running replica databases first and run the shutdownnnc.sh script on each.
2. Login to the server running the master database and run the shutdownnnc.sh script once the replicated servers have shutdown.

Master Node Determination

To determine the master node for the Session Delivery Manager 7.0x cluster:

1. Login to the Session Delivery Manager GUI client and access the Health Monitor to identify the server with the master database.

   Note: All cluster nodes must be up and running.

2. Identify the master database in one of two ways:

   - In the Heartbeat console, the server that is running the master database has (master) next to the IP address.
   - Search the logs/DbService.log file for a line that looks like this:

     2011-06-14 16:52:16,266 INFO [com.acmepacket.ems.server.services.database.ReplicatedXMLDatabaseManagerImpl] - Method: [setCurrentState] Thread: [Thread-16:74]

     Msg:[Current State = unknown, New State = master]

     2011-06-14 16:52:16,295 INFO [com.acmepacket.ems.server.services.database.ReplicatedXMLDatabaseManagerImpl] - Method: [initDbEnv] Thread: [DatabaseService:20]

     Msg:[Replicated Database environment initialization complete. Role = master, IPAddress = 172.30.80.19]

Cluster System for NNC 7.1+

To perform a cluster shutdown on Session Delivery Manager 7.1+:

1. Change directory to /NNC73/bin. For example:

```
cd /opt/AcmePacket/NNC73/bin
```

2. Execute the shutdownnnc.sh script. The script detects whether the existing instalation is a standalone or clustered system and prompts you with the option to shut down the entire cluster.

Note: You can script an option ahead of time by adding -local for single nodes and -cluster to shutdown an entire cluster.

```
[root@nms-vm12 bin]# ./shutdownnnc.sh
Shutdown back-end server
Do you wish to shut down the entire cluster (Yes/No)?Y
Shutting down cluster.....
```

3. Enter Y to continue and press Enter to shut down the cluster.

Configuring the Net-Net SBC for Net-Net Central Interaction

This section provides an example of how to configure the trap receiver and SNMP community in the Net-Net SBC to point to the Session Delivery Manager server. You need to configure these objects to enable Session Delivery Manager to provide fault management (SNMP traps), performance management statistics, and inventory control (SNMP) for this specific Net-Net SBC. If managing Net-Net 9000 SBCs, you need to create a virtual management interface to enable SOAP/XML (SNMP traps will also be sent to this virtual address).

You need to have Superuser privilege to configure your Net-Net SBC through a terminal by way of a local or remote connection.

Configuring the SNMP Interface

To configure the SNMP interface:

1. Connect to the Net-Net SBC and login.
2. Enable Superuser mode. For example:

```
User Access Verification
Password: <User Mode password>
ACMEPACKET> enable
Password: <Superuser Mode password>
ACMEPACKET#
```

3. Execute the configure terminal command.

```
ACMEPACKET# configure terminal
```

4. Execute the system command.

```
ACMEPACKET(configure)# system
```

5. Execute the trap-receiver command.

```
ACMEPACKET(system)# trap-receiver
```

6. Enter the following information:

   - ip-address <Session Delivery Manager server IP address>
   - filter-level <value>
   - community-name <value>

   For example:

```
ACMEPACKET(trap-receiver)# ip-address 10.0.0.1
ACMEPACKET(trap-receiver)# filter-level all
ACMEPACKET(trap-receiver)# community-name acme
```

7. Create a trap receiver for each Session Delivery Manager server.
8. Enter done. For example:

```
ACMEPACKET(trap-receiver)# done
```

9. Enter exit to return to the system level.

```
ACMEPACKET(trap-receiver)# exit
```

10. Execute the snmp-community command.

```
ACMEPACKET(system)# snmp-community
```

11. Enter the following information:

    - ip-address <Session Delivery Manager server IP address> or a list of IP addresses. For Net-Net 9000, ip-addresses add
    - community-name <value>
    - access-node <value> (leave at its default value)

    For example:

```
ACMEPACKET(snmp-community)# ip-address 10.0.0.1
ACMEPACKET(snmp-community)# community-name acme
```

12. Enter done. For example:

```
ACMEPACKET(snmp-community)# done
```

13. Enter exit to return to the system level.

```
ACMEPACKET(snmp-community)# exit
```

14. Execute the system-config command.

```
ACMEPACKET(system)# system-config
```

15.
16. Enter the following information:

```
ACMEPACKET(system-config)# snmp-enabled enabled
```

17. Enter done. For example:

```
ACMEPACKET(system-config)# done
```

18. Verify the information.
19. Execute the save-config command (for Net-Net 9000, use the save config command).

```
ACMEPACKET(snmp-community)# save-config
```

20. Execute the activate-config command to ensure SNMP is enabled (for Net-Net 9000, use the activate command).

```
ACMEPACKET# activate-config
```

21. Enter the reboot command for Net-Net 4000 SBC (no need to reboot Net-Net 9000).

```
ACMEPACKET(snmp-community)# reboot
```

    After the Net-Net SBC system restarts, execute the show running-config command. The output should contain a trap receiver and SNMP community objects with the information you just configured.

Starting the Net-Net Central Client and Connecting to the Server

Follow the instructions in this section to start the Session Delivery Manager client and log in to the server.

If logging into Session Delivery Manager when third-party X.509 certificates are used for HTTPS access, specify the hostname in DNS name format. Otherwise, the HTTPS you will have to click through security warnings about hostname mismatch between common name in the certificate and the IP address specified in the JNLP.

Note: You might experience difficulty connecting to Session Delivery Manager because of your network's proxy support. If you have trouble connecting, check the proxy settings for both your browser. See Verifying the Client System Settings for more information.

Verifying the Client System Settings

You should verify the client system has the required settings to connect to the Session Delivery Manager server. You need to have the Session Delivery Manager files from the distribution media at hand while verifying the client settings.

Verifying the Internet Explorer Browser Settings

If using Internet Explorer as your browser, you need to verify the following settings.

1. Open the Internet Explorer browser.
2. Choose the Tools menu and click Internet options.
3. Choose the Security tab.
4. Choose the Local intranet option and click Custom Level.
5. Enable the following options (if not already enabled) then click OK.
   - Run ActiveX controls and plug-ins under ActiveX controls and plug-ins
   - Active Scripting and Scripting of Java applets under Scripting
6. Choose the Internet option on the Security tab and click Custom Level. (This step is required if the client system accesses the Session Delivery Manager server via the Internet.)
7. Enable the following options (if not already enabled,) then click OK.
   - Run ActiveX controls and plug-ins under ActiveX controls and plug-ins
   - Active Scripting and Scripting of Java applets under Scripting

   If you are running Internet Explorer 8, follow steps 8-12. If not, procede to the final step.
8. Choose the Trusted Sites option on the Security tab and click Custom Level.
9. Enable the following options (if not already enabled,) then click OK.
   - Automatic prompting for file downloads under Downloads
10. Choose the Trusted Sites option on the Security tab and click the Sites button.
11. Add this website to the zone— Enter the Session Delivery Manager server address in this field.
12. Click Add and then click Close.
13. Click OK on the Internet options window to close it.

Disabling Proxy Server (Optional)

Follow these steps if your client system is configured as a proxy server and you do not want to use it for connecting with the Session Delivery Manager server.

1. Open the Internet Explorer browser.
2. Choose the Tools menu and click Internet options.
3. Click the Connections tab on the Internet options screen.
4. Click LAN Settings and then click Advanced.
5. Enter the Session Delivery Manager server IP address in the Exceptions panel.
6. Click OK.
7. Click OK on the Internet options window to close it.

Starting the Net-Net Central Client

You can start the Session Delivery Manager client by using either the HTTP or HTTPS login:

```
http://<Session Delivery Manager server IP address>:8080
https://<Session Delivery Manager server IP address>:8443 (self-signed
certificates)
https://<domain name>:8443 (third-party X.509 certificates)
```

Note: If using third-party X.509 certificates, use the DNS name of the host such as nncserver.acmepacket.com instead of the IP address. Then it matches the common name in the certificate.

2

Migrating Data to the Session Delivery Manager

EMS 6.x to Net-Net Central 7.3

The instructions below follow data migration from Net-Net EMS 6.x or Route Manager 1.x to Session Delivery Manager 7.3, and earlier versions of Session Delivery Manager to Session Delivery Manager 7.3.

You can migrate the following information from EMS 6.x to Session Delivery Manager 7.3:

- User profile
- Alarms and events
- Device list and Net-Net SBC node information: IP addresses and passwords.
- Banner text
- Audit trail logs

Note: Configuration data is not migrated.

Migration Process

Data migration from Net-Net EMS 6.x to Session Delivery Manager 7.3 is launched and handled by the data migration tool, ensuring data from fault management, user security, and devices is migrated.

The data migration tool retrieves data from the old databases, saving it to different categories of intermediate XML files that are compliant with the Berkeley DB XML (dbxml) files on the embedded Session Delivery Manager database. When you run Session Delivery Manager, the migrated data is available.

Requirements

The requirements for migrating data from Net-Net EMS 6.x include:

- Net-Net EMS 6.x database running
- Host name of the MySQL server
- MySQL port number
- Database user account with permissions allowing execution of SQL query
- User name and password of database user account
- Database name of Net-Net EMS data stored

Before You Migrate Data

Before you migrate data, you must make sure that Session Delivery Manager is not running and execute the setup.sh script to configure the Session Delivery Manager database and environment.

See Shutting down the Session Delivery Manager Server for more information.

To run setup:

1. Obtain the appropriate tar.gz file from the Oracle customer portal. The tar.gz files include the following:
   - NNC73Linux64bit.tar.gz for Linux RHEL v5.5 64 bit installation
   - NNC73FC1364bit.tar.gz for Linux Fedora Core 13 64 bit installation
2. FTP the tar.gz file to your system. Place the file in the opt/AcmePacket directory where you have previously installed Session Delivery Manager software.
3. Unzip the *.tar.gz file.

   ```
   gunzip <filename>.tar.gz
   ```
4. Extract the files using one of the following command:

   ```
   tar -xvf <filename>.tar
   ```
5. Change directory to NNC73/bin. For example:

   ```
   cd /opt/AcmePacket/NNC73/bin
   ```
6. Run the setup.sh script.

   ```
   ./setup.sh
   ```

   The migration tool detects any previous versions of Session Delivery Manager and prompts you based on whether the existing instalation is a standalone or clustered system.

   You can apply the Session Delivery Manager license and complete the Session Delivery Manager installation in standalone or cluster mode.

   If you try to migrate data without running setup first, the following message appears.

   ```
   Starting Migration Application 2011-05-25 14:11:27,086
           Please run Session Delivery Manager setup first. 2011-05-25
   14:11:52,377
   ```

Migrating Data from EMS 6.x to Net-Net Central 7.3

To migrate data from Net-Net EMS 6.x:

Ensure you have run setup.sh first and have shutdown Session Delivery Manager before you migrate data.

The default user groups Admin, Monitor, and Provisoner are not migrated. Session Delivery Manager creates those default groups with different names. Users are migrated but their passwords are reset to their usernames. When users login for the first time, they need to change their passwords.

1. Login as root.
2. Change directory to NNC73/bin. For example:

   ```
   cd /opt/AcmePacket/NNC73/bin
   ```
3. Run the dataMigration.sh script to start the migration.

   ```
   ./dataMigration.sh
   ```

   The migration options appear.

   ```
   Migration Options:
   1 EMS 6.x     :   Migrating data from EMS 6.x to NNC 7.x
   2 RMC 1.x     :   Migrating data from RMC 1.x to NNC 7.x
   3 Quit.
   Select [1]
   ```

4. Press Enter to accept the default and migrate data from Net-Net EMS 6.x. You are prompted for the hostname or IP address.

```
Hostname or IP (required):
```

5. Enter the DNS name of the host or the IP address and press Enter. You are prompted for the port number.

```
Port [3306]:
```

6. Press Enter to accept the default value 3306 or enter an new port number and press Enter. You are prompted for the user name.

```
User [root]:
```

7. Press Enter to accept the default value or enter your username. You are prompted for the password.

```
Password:
```

8. Enter the password and press Enter. The data migration starts and the status appears on the screen.

```
Connected to database 2011-05-24 17:49:19,602
Migrating alarms data ... 2011-05-24 17:49:19,603
Migrating events data ... 2011-05-24 17:49:19,734
Migrating device groups data ... 2011-05-24 17:49:19,801
Migrating fault data ... 2011-05-24 17:49:19,907
Migrating ems details data ... 2011-05-24 17:49:19,934
Migrating device details data ... 2011-05-24 17:49:20,103
Migrating user security data ... 2011-05-24 17:49:20,142
Migrating audit trail logging data ... 2011-05-24 17:49:21,843
Start to load data into database 2011-05-24 17:49:22,104
Loading: alarms.xml into database ... 2011-05-24 17:49:22,530
Loaded: alarms.xml into database successfully. 2011-05-24 17:49:22,596
Loading: events.xml into database ... 2011-05-24 17:49:22,596
Loaded: events.xml into database successfully. 2011-05-24 17:49:22,640
Loading: AuditTrail.xml into database ... 2011-05-24 17:49:22,640
Loaded: AuditTrail.xml into database successfully. 2011-05-24 17:49:22,695
Loading: EMSDetails.xml into database ... 2011-05-24 17:49:22,949
Loaded: EMSDetails.xml into database successfully. 2011-05-24 17:49:23,031
Loading: Fault.xml into database ... 2011-05-24 17:49:23,032
Loaded: Fault.xml into database successfully. 2011-05-24 17:49:23,053
Loading: DeviceGroup.xml into database ... 2011-05-24 17:49:23,054
Loaded: DeviceGroup.xml into database successfully. 2011-05-24 17:49:23,093
Loading: DeviceDetails.xml into database ... 2011-05-24 17:49:23,093
Loaded: DeviceDetails.xml into database successfully. 2011-05-24
17:49:23,128
Loading: UserSecurity.xml into database ... 2011-05-24 17:49:23,128
Loaded: UserSecurity.xml into database successfully. 2011-05-24 17:49:23,227
Loaded data into database successfully 2011-05-24 17:49:23,227
Disconnected from database 2011-05-24 17:49:23,229
Completed data migration successfully! 2011-05-24 17:49:23,230
[nncentral@cosmo bin]#
```

Any new rules and attributes required by Session Delivery Manager are added during the migration process.

Migrating Net-Net Route Manager Central Data

You can migrate the following information from the Route Management database.

- User profile
- Route Sets
- Device list and Net-Net node information: IP addresses and passwords. Configuration data is not migrated.
- Banner text
- Audit trail logs

Migration Process

Data migration from Route Manager 1.x to Session Delivery Manager 7.3 is launched and handled by the data migration tool, ensuring data from fault management, user security, and devices is migrated.

The data migration tool retrieves data from the old databases, saving it to different categories of intermediate XML files that are compliant with the Berkeley DB XML (dbxml) files on the embedded Session Delivery Manager database. When you run Session Delivery Manager, the migrated data is available.

Requirements

The requirements for migrating data from Net-Net Route Manager Central 1.x include:

- Path to database entry folder. For example, on Linux:

  ```
  opt/ACMEPacket/rmc/db
  ```
- Stopping Route Manage Central

Before You Migrate Data

Before you migrate data, you must make sure that Route Manager Central and Session Delivery Manager are not running and execute the setup.sh script to configure the Session Delivery Manager database and environment.

To run setup:

1. Obtain the appropriate tar.gz file from the Oracle customer portal. The tar.gz files include the following:
   - NNC73Linux64bit.tar.gz for Linux RHEL v5.5 64 bit installation
   - NNC73FC1364bit.tar.gz for Linux Fedora Core 13 64 bit installation
2. FTP the tar.gz file to your system. Place the file in the opt/AcmePacket directory where you have previously installed Session Delivery Manager software.
3. Unzip the *.tar.gz file.

   ```
   gunzip <filename>.tar.gz
   ```
4. Extract the files using one of the following command:

   ```
   tar -xvf <filename>.tar
   ```
5. Change directory to NNC73/bin. For example:

   ```
   cd /opt/AcmePacket/NNC73/bin
   ```
6. Run the setup.sh script.

   ```
   ./setup.sh
   ```

   The migration tool detects any previous versions of Session Delivery Manager and prompts you based on whether the existing instalation is a standalone or clustered system.

   You can apply the Session Delivery Manager license and complete the Session Delivery Manager installation in standalone or cluster mode.

   If you try to migrate data without running setup first, the following message appears.

   ```
   Starting Migration Application 2011-05-25 14:11:27,086
           Please run Session Delivery Manager setup first. 2011-05-25
   14:11:52,377
   ```

Migrating from Net-Net Route Manager Central 1.x

To migrate data from Net-Net Route Manager Central:

Ensure you have run setup.sh first and have shutdown Route Manager Central before you migrate data. The Route Manager Central data files need to be located on the same system as Session Delivery Manager.

1. Login as root.

2. Change directory to NNC73/bin. For example:

```
cd /opt/AcmePacket/NNC73/bin
```

3. Run the dataMigration.sh script to start the migration.

```
./dataMigration.sh
```

The migration options appear.

```
Migration Options:
1 EMS 6.x     :   Migrating data from EMS 6.x to NNC 7.x
2 RMC 1.x     :   Migrating data from RMC 1.x to NNC 7.x
3 Quit.
Select [2]
```

4. Enter 2 and press Enter to migrate data from RMC 1.x. You are prompted for the path to the dbxml files.

```
Path to RMC dbxml files (required):
```

5. Enter the path to the files and press Enter.

```
/opt/ACMEPacket/rmc/db
```

The database migration starts and progress information displays on the screen.

```
Migrating ems details data ... 2011-05-26 14:49:11,155
Migrating device details data ... 2011-05-26 14:49:11,467
Migrating user security data ... 2011-05-26 14:49:12,264
Migrating audit trail logging data ... 2011-05-26 14:49:12,295
Start to load data into database 2011-05-26 14:49:13,052
Loading: AuditTrail.xml into database ... 2011-05-26 14:49:13,177
Loaded:  AuditTrail.xml into database successfully. 2011-05-26 14:49:16,863
Loading: EMSDetails.xml into database ... 2011-05-26 14:49:17,332
Loaded:  EMSDetails.xml into database successfully. 2011-05-26 14:49:18,316
Loading: DeviceDetails.xml into database ... 2011-05-26 14:49:18,316
Loaded:  DeviceDetails.xml into database successfully. 2011-05-26
14:49:18,621
Loading: UserSecurity.xml into database ... 2011-05-26 14:49:18,621
Loaded:  UserSecurity.xml into database successfully. 2011-05-26
14:49:18,941
Loading: rms.xml into database ... 2011-05-26 14:49:18,949
Loaded:  rms.xml into database successfully. 2011-05-26 14:49:19,245
Loaded data into database successfully 2011-05-26 14:49:19,245
Completed data migration successfully! 2011-05-26 14:49:19,245
```

Upgrading to Net-Net Central 7.3

You can migrate data from older versions of Session Delivery Manager to Session Delivery Manager 7.3+ using the instructions below. The data migration tool will automatically detect older versions of Session Delivery Manager during setup and prompt you with the option of migrating data.

Requirements

The requirements for migrating data from an older version of Session Delivery Manager include:

- Session Delivery Manager 7.0+ installed prior to migration

Before You Migrate Data

Before you migrate data to a newer version of Session Delivery Manager, you must delete or rename certain duplicate objects. Repeat steps until there are no longer duplicated objects in the listed areas.

Deleting Duplicate Devices

To delete duplicate devices from the Device column:

1. Expand the Device Manager > Devices.
2. Select the duplicate device and click Delete.

Renaming Duplicate Device Groups

To rename duplicate device groups:

1. Expand the Device Manager > Device group.
2. Select the duplicate device group and click Rename.

Deleting Duplicate Users

To delete duplicate users:

1. Expand the Security Manager > User management > Users.
2. Select the duplicate user and click Delete.

Deleting Duplicate User Groups

To delete duplicate user groups:

1. Expand the Security Manager > User management > Groups.
2. Select the duplicate user group and click Delete.

Deleting Duplicate Work Orders

To delete duplicate work orders:

1. Expand the Device Manager > Software upgrade > Work order administration.
2. Select the duplicate work order and click Delete.

Deleting Duplicate Global Work Orders

To delete duplicate global work orders:

1. Expand the Configuration Manager > Global parameters.
2. Click the Admin tab.
3. Select the duplicate work order and click Delete.

Shutting Down NNC

Before you migrate data, you must make sure that Session Delivery Manager is not running and execute the setup.sh script to configure the Session Delivery Manager database and environment.

See Shutting down the Session Delivery Manager Server for more information.

Running setup.sh

To run setup:

1. Obtain the appropriate tar.gz file from the Oracle customer portal. The tar.gz files include the following:
   - NNC73Linux64bit.tar.gz for Linux RHEL v5.5 64 bit installation
   - NNC73FC1364bit.tar.gz for Linux Fedora Core 13 64 bit installation
2. FTP the tar.gz file to your system. Place the file in the opt/AcmePacket directory where you have previously installed Session Delivery Manager software.
3. Unzip the *.tar.gz file.

   ```
   gunzip <filename>.tar.gz
   ```
4. Extract the files using one of the following command:

   ```
   tar -xvf <filename>.tar
   ```
5. Change directory to NNC73/bin. For example:

```
cd /opt/AcmePacket/NNC73/bin
```

6. Run the setup.sh script.

```
./setup.sh
```

The migration tool detects any previous versions of Net-Net Central and prompts you based on whether the existing instalation is a standalone or clustered system.

You can apply the Session Delivery Manager license and complete the Session Delivery Manager installation in standalone or cluster mode.

If you try to migrate data without running setup first, the following message appears.

```
Starting Migration Application 2011-05-25 14:11:27,086
```

Please run Session Delivery Manager setup first. 2011-05-25 14:11:52,377

Migrate Data from Older Versions of Net-Net Central

Ensure you have run setup.sh first and have shutdown Route Manager Central before you migrate data. The Route Manager Central data files need to be located on the same system as Session Delivery Manager.

Standalone System

To migrate data on a standalone system:

1. Enter 1 to proceed with database migration.

```
Setup has detected that database migration needs to be performed.
The migration process involves backing up the existing database and then
performing various operations to migrate the database to the current
version.
Depending on size of the existing database and the operations to be
performed,
this process may take up to an hour to complete, however you can cancel and
rollback the process at any time by pressing the <a> key followed by
<enter>.
Note that database migration MUST be performed before setup can continue.
[X]  1 - Proceed with database migration   [Default]
[ ]  2 - Cancel and exit setup
Please select an option [1] 1
```

2. Enter Yes to migrate data from the previous Session Delivery Manager installation.

```
[X]  1 - Proceed with database migration   [Default]
[ ]  2 - Cancel and exit setup
Do you want to continue Yes/No?  Yes
```

Pressing the a key anytime during the process will abort the current migration. You will not be able to launch the target version of Session Delivery Manager until setup is re-run and database migration is performed.

```
Database migration beginning.
To abort and rollback database migration, press <a> then <enter> at any time
```

The database migration starts and progress information displays on the screen.

```
backing up existing database....done
migrating database...done
creating migrated master database archive...done
Database migration is now complete.
Press <enter> to continue with setup
```

3. Press enter to continue with Session Delivery Manager Setup.

Clustered Systems Master Node

To migrate data on a master node:

1. Enter 1 to migrate data from the previous Session Delivery Manager installation.

```
Setup has detected that database migration needs to be performed.
The migration process involves backing up the existing database and then
performing various operations to migrate the database to the current
version.
Depending on size of the existing database and the operations to be
performed,
this process may take up to an hour to complete, however you can cancel and
rollback the process at any time by pressing the <a> key followed by
<enter>.
Note that database migration MUST be performed before setup can continue.
[X]  1 - Proceed with database migration   [Default]
[ ]  2 - Cancel and exit setup
Please select an option [1] 1
```

2. Yes to migrate data from the previous Session Delivery Manager installation.

```
[X]  1 - Proceed with database migration   [Default]
[ ]  2 - Cancel and exit setup
Do you want to continue Yes/No?  Yes
Database migration beginning.
To abort and rollback database migration, press <a> then <enter> at any time
backing up existing database....done
migrating database...done
creating migrated master database archive...done
```

3. Enter 1 to copy the migrated database to other cluster nodes.

```
Your existing setup is configured for a clustered environment.  Setup on all
other nodes in your cluster will require the migrated database archive just
created.  Setup can now attempt to copy this archive via SFTP to other
cluster
nodes.
Note that if you skip this step, you must manually copy the migrated
database
archive to all other nodes in the cluster, as this archive will be required
during setup on the other cluster nodesz
[X]  1 - Copy the migrated database archive to other cluster nodes
[Default]
[ ]  2 - Do not copy the migrated database archive
Please select an option [1] 1
```

4. Enter Yes to continue.

```
[X]  1 - Copy the migrated database archive to other cluster nodes
[Default]
[ ]  2 - Do not copy the migrated database archive
Do you want to continue Yes/No? Yes
```

5. Enter the username, password, and folder path for the SFTP credentials for each cluster node when prompted.

```
Provide SFTP credentials for cluster node 2.2.2.2:
username:  [] myuser
password:  [] xxxxx
remote folder path:  [        ] /home/myuser
remote folder path:  [/home/myuser]
```

For example, upon successful migration you will see:

```
cluster node: 2.2.2.2
destination file: /home/myuser/ColdBackup_2012_02_13_112911_db.tar.gz
result:  SUCCEEDED
cluster node: 3.3.3.3
destination file: /home/otheruser/ColdBackup_2012_02_13_112911_db.tar.gz
result:  SUCCEEDED
Press <enter> to continue
Database migration is now complete.
Press <enter> to continue with setup
```

Clustered Systems Replicated Node

To migrate data on a replicated node:

Note: Setup must be performed on each replica member of the cluster.

1. Enter 1 to continue importing the database backup.

```
Setup has detected that database migration needs to be performed.
The migration process involves backing up the existing database and then
performing various operations to migrate the database to the current
version.
Depending on size of the existing database and the operations to be
performed,
this process may take up to an hour to complete, however you can cancel and
rollback the process at any time by pressing the <a> key followed by
<enter>.
Note that database migration MUST be performed before setup can continue.
[X]  1 - Proceed with database migration   [Default]
[ ]  2 - Cancel and exit setup
Please select an option [1] 1
```

2. Enter Yes to continue.

```
[X]  1 - Proceed with database migration   [Default]
[ ]  2 - Cancel and exit setup
Do you want to continue Yes/No? Yes
```

3. Enter 1 to continue.

```
Your existing setup is configured for a clustered environment.  For your
existing environment, setup must be run on cluster node 1.1.1.1 prior
to running setup on any other cluster node (including this one).  When setup
is run on cluster node 1.1.1.1, a migrated master database archive
file will be produced.
If you have already run setup on 1.1.1.1 and either allowed setup to
automatically copy the database archive file to this node, or have copied
this
file manually, please select option [1] below.  Otherwise, please select
option [2] below to cancel setup.  Then run setup on 1.1.1.1 before
running setup again on this node.
[X]  1 - Specify location of migrated master database archive file
[Default]
[ ]  2 - Cancel and exit setup
Please select an option [1] 1
```

4. Enter Yes to continue.

```
[X]  1 - Proceed with database migration   [Default]
[ ]  2 - Cancel and exit setup
Do you want to continue Yes/No? Yes
```

5. Enter the full path to the database backup and enter yes to continue the import process.

```
Enter migrated master database archive file path:
[        ] /home/myuser/ColdBackup_2012_02_13_112911_db.tar.gz
[/home/myuser/ColdBackup_2012_02_13_112911_db.tar.gz]
backing up existing database....done
restoring the migrated master database...done
Restore migrated master database archive succeeded
Press <enter> to continue with setup
```

Setup will proceed to the standard installation procedure.

You can now run startnnc.sh on cluster nodes.

Net-Net EMS 6.X to Net-Net Central 7.3 Database Migration Information

Running Database Migration Again

You cannot run database migration a second time without re-initializing the Session Delivery Manager database first. Reinitializing the database permanently clears all the data it contains.

To reinitialize a database:

Note: This section only applies to migration from EMS 6.x to NNC7.x. Following these steps for Session Delivery Manager 7.x to NNC7.3 migrations may result in data loss.

1. Login to the Session Delivery Manager server as root user.
2. Change directory to NNC73/bin. For example:

```
cd /opt/AcmePacket/NNC73/bin
```

3. Enter the following command to reinitialize the database:

```
./reinitialize.sh
```

Reinitialize Database with Data

```
./reinitialize.sh
Reinitialize options
[ ] 1 - Reintialize: This will clear all databases
[X] 2-Quit : Exit Reinitialize
Select an option [2] 1
Warning : This will delete all the content in database. Do you want to
continue Yes/No ?yes
Deleting file ../../db/local/data/alarms.dbxml ...
Deleting file ../../db/local/data/AuditTrail.dbxml ...
Deleting file ../../db/local/data/__db.001 ...
Deleting file ../../db/local/data/__db.002 ...
Deleting file ../../db/local/data/__db.003 ...
Deleting file ../../db/local/data/__db.004 ...
Deleting file ../../db/local/data/__db.005 ...
Deleting file ../../db/local/data/__db.006 ...
Deleting file ../../db/local/data/events.dbxml ...
Deleting file ../../db/local/data/log.0000000001 ...
Deleting file ../../db/replicated/data/__db.001 ...
Deleting file ../../db/replicated/data/__db.002 ...
Deleting file ../../db/replicated/data/__db.003 ...
Deleting file ../../db/replicated/data/__db.004 ...
Deleting file ../../db/replicated/data/__db.005 ...
Deleting file ../../db/replicated/data/__db.006 ...
Deleting file ../../db/replicated/data/DeviceDetails.dbxml ...
Deleting file ../../db/replicated/data/DeviceGroup.dbxml ...
Deleting file ../../db/replicated/data/EMSDetails.dbxml ...
Deleting file ../../db/replicated/data/Fault.dbxml ...
Deleting file ../../db/replicated/data/log.0000000001 ...
Deleting file ../../db/replicated/data/UserSecurity.dbxml ...
Deleting file ../../db/local/migrationdb/alarms.xml ...
Deleting file ../../db/local/migrationdb/AuditTrail.xml ...
Deleting file ../../db/local/migrationdb/events.xml ...
Deleting file ../../db/replicated/migrationdb/DeviceDetails.xml ...
Deleting file ../../db/replicated/migrationdb/DeviceGroup.xml ...
Deleting file ../../db/replicated/migrationdb/EMSDetails.xml ...
Deleting file ../../db/replicated/migrationdb/Fault.xml ...
Deleting file ../../db/replicated/migrationdb/UserSecurity.xml ...
```

Reinitialize Database without Data

```
./reinitialize.sh
Reinitialize options
[ ] 1 - Reintialize: This will clear all databases
[X] 2-Quit : Exit Reinitialize
Select an option [2] 1
Warning : This will delete all the content in database. Do you want to
continue Yes/No ?yes
```

Data Migration Logging

Information about the data migration flow is captured in the Migration.log file located in the /AcmePacket/NNC73/logs directory.

The information includes:

- Net-Net EMS 6.x

  MySQL database open/close connection

  User management and security

  Alerts

  Events

  Device Details

  Device Groups

  Audit trails

  Fault

  Banner
- Net-Net Route Manager Central 1.x

  Berkeley database XML open/close containers

  Database connection

  User management and security

  Device Details

  Device Groups

  Audit trails

  Route sets

  Route Management System (RMS)

Error Logging

Errors are logged as well as the data migration flow information. If errors in data migration occur, you need to reinitialize the database before you can retry the migration.

Mapping Device Groups to User Groups

After the data migration occurs, the devices exist in the Session Delivery Manager database but they might not be immediately visible in the Session Delivery Manager GUI. You need to map device groups to user groups for security purposes. Until that mapping is created, users in the user groups will not be able to see any of the devices in the device group.

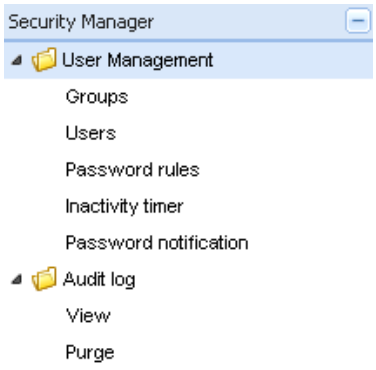
The Session Delivery Manager administrator must decide which of the device groups can be seen and managed by which the default user groups that are created by default when Session Delivery Manager is installed:

- administrators: Super user group privileged to perform all operations
- LIAdministrators: Privileged to perform most operations including Lawful Intercept (LI) configuration changes
- provisioners: Privileged to configure Net-Net SBCs (if licensed for Element Manager) and save and apply the configuration with the exception of a LI configuration.
- monitors: Privileged to only view data, both configuration and other kinds of data.

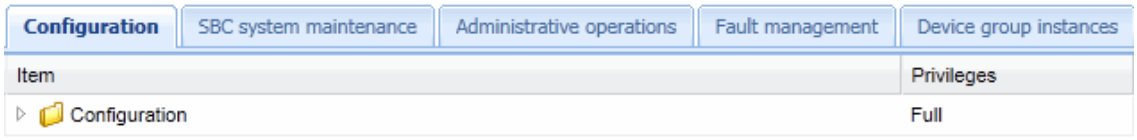
Oracle recommends that all four of the default user groups have full visibility into all migrated device groups.

To map device groups to user groups:

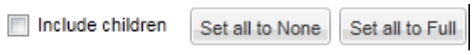
1. Login to Session Delivery Manager as admin.
2. Expand the Security slider in the Navigation bar.
3. Expand the User Management directory.



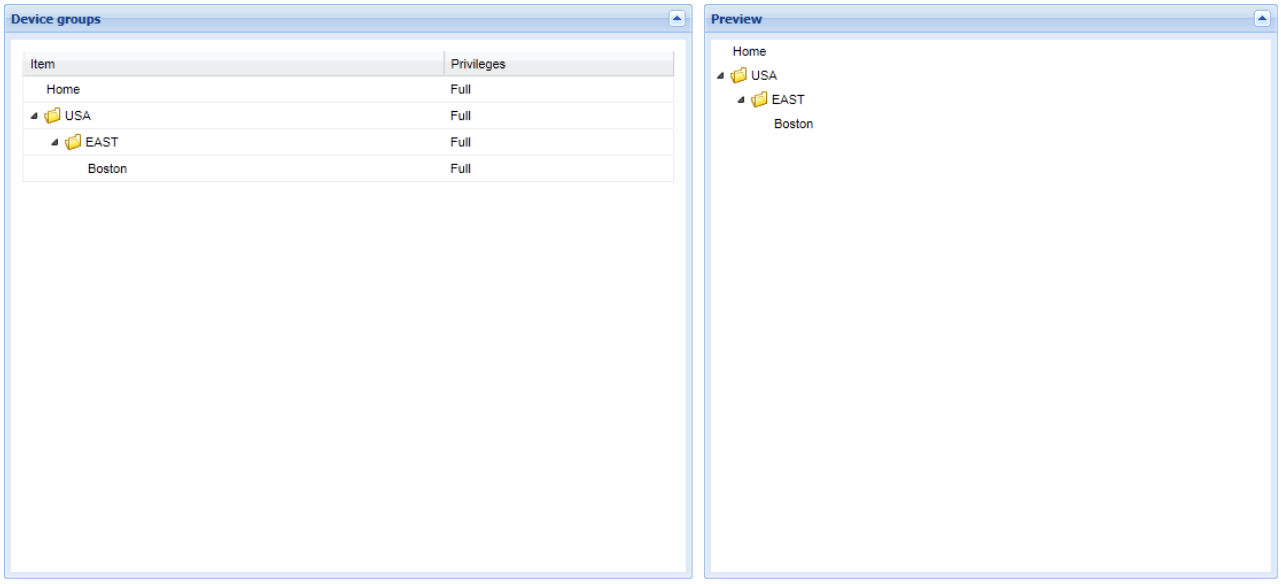
4. Click Groups in the Navigation bar. A table of user groups appears in the content body. The table displays all of the operations categories with the current privilege levels for each user group.
5. Click a user group name in the table and click Edit. For example, click LIAdministrators. The operations tabs appear.



6. Click Device group instances. The Device group instances tab lets you assign privileges and preview the device group hierarchy based on the privileges selected. That hierarchy will be reflected on the Device Manager slider.
7. Click Set all to Full.



The permissions on all device groups is set to Full. The device groups appear in the Preview column.



8. Click Apply.
9. Repeat steps 4 through 7 to assign privileges to each user group.

Backup and Restore Database Servers

If you have administrator privileges, you can back up your servers either while they are shutdown or while still running. If you want to backup a server while it is running, tell any user working on that server to minimize their usage during backup.

You can enter command line flags when issuing the back up script to specify the database and destination of the back up. By default, --all is assumed if no flag is entered.

-d — Specifies the directory to store the backed up file.

--all — Backs up core database and postgres database.

--core — Backs up core database only.

--postgres — Backs up postgres database only.

For Example:

```
./backuphot.sh --postgres
```

Backing Up with Server Shutdown

Backing up while the server is shutdown is a cold backup. After all backups are complete, you can restart the servers.

To back up the server while shutdown:

1. Shutdown all servers you want to backup.
2. Log in as root.
3. Change directory to NNC73/bin. For example:

   ```
   cd /opt/AcmePacket/NNC73/bin
   ```
4. Run the coldbackup script.

   ```
   ./backupcold.sh
   ```

   The backup process runs.

Backing Up with Server Running

Backing up while the server is running is a hot backup.

Note: Remember to tell any user on the server to minimize their system usage during backup.

To back up the server while running:

1. Ensure the server is running.
2. Log in as root.
3. Change directory to NNC73/bin. For example:

   ```
   cd /opt/AcmePacket/NNC73/bin
   ```

4. Start the hot backup script.

   ```
   ./backuphot.sh
   ```

   The backup process runs.

Restoring Database Backups

You need to shutdown all servers on which you are restoring database backups. If restoring database backups on servers in a cluster, you need to restore databases on each one.

1. Shutdown all servers you plan to restore backups on.
2. Log in as root.
3. Change directory to NNC73/bin. For example:

   ```
   cd /opt/AcmePacket/NNC73/bin
   ```

4. Start the database restore script.

   ```
   ./restoredb.sh
   ```

   The database restoration process runs.

3

Installing NNC Patches

This section explains how to install Session Delivery Manager software patches using the Session Delivery Manager patch management tool. This process is applied for patches subsequent to Session Delivery Manager software version 7.1.

To install patches beyond Session Delivery Manager 7.1, you need to obtain the appropriate patch tar.gz file for your environment from your Oracle representative. You also must have Session Delivery Manager already installed and have run setup before. The patch management tool is distributed with the Session Delivery Manager GA software release.

The patch management tool allows you to perform the following operations:

- List imported patches
- Import patches
- Apply a patch
- Remove patches

You FTP the patch tar.gz to a directory on your system. The location is not specified. Note the path for your own reference when the patch management tool prompts you for the file location. When directed, the patch management tool unzips and extracts the necessary files, and places them in the original Session Delivery Manager installation directory, appending a /patches directory where the patch files will be located.

You can run the patch management tool while the Session Delivery Manager server is running, but you will be restricted to the following options:

- List available patches on the system.
- Import the patches.

In order to apply or remove patches, the Session Delivery Manager server must be shut down.

Patches are cumulative in that patch 5 contains patches 1-4 as well.

Once you have successfully applied a new patch with the patch management tool, you can verify the new Session Delivery Manager software version by performing one of the following actions:

- Use the tool to list imported patches. The current version is marked with an asterisk.
- Once the server is started, Click Help > About in the Session Delivery Manager GUI.

Shutting Down NNC Servers

You must shutdown the Session Delivery Manager server in order to apply or remove patches. See Shutting down the Session Delivery Manager Server for more information.

Running the Patch Management Tool in a Cluster

In order to run the patch tool in a cluster, you must shutdown all nodes in a cluster, and apply the patch manually for each cluster. The recommended steps for this process are to:

1. Shutdown Session Delivery Manager servers in the cluster.
2. Apply the patch to each Session Delivery Manager host in the cluster.
3. Startup the Session Delivery Manager servers in the cluster.

Identifying the Master Node NNC Patch Version in a Cluster

During the startup sequence, if a node in a cluster is not at the same patch version as the master node, the startup terminates and an error message is displayed.

```
System is at NNC73P1, Master is at NNC73P2. All hosts must be at same patch
level. Terminating startup.
```

Installing Net-Net Central Patches

To run the patch management tool:

1. Login to the Session Delivery Manager server as root.
2. Navigate to the bin directory. For example:

   ```
   cd /opt/AcmePacket/NNC73/bin
   ```

3. Run the patchManagement.sh script.

   ```
   ./patchManagement.sh
   ```

   A Welcome message appears and initialization processes occur. Patch management checks that minimal system requirements are met and whether the system is running.

   ```
   cd /opt/AcmePacket/NNC73/bin
   [root@nncentral bin]# ./patchManagement.sh
   ========================================================
   Welcome to Session Delivery Manager Patch Management application
   Current Session Delivery Manager Version: NNC73P1
   OS : Linux : amd64 : 2.6.18-194.el5
   ========================================================
   Please wait while application loads
   Checking environment for patch management application.
   Please wait ....
   100%[==================================================]
   Patch Management Menu
   Please select from the following options:
   [X] 1 - List Imported patches
   [ ] 2 - Import patch
   [ ] 3 - Apply patch
   [ ] 4 - Remove all applied patches
   [ ] 5 - Quit
   Please select an option [1]
   ```

   You must select an option to perform one of the following options:

4. List imported patches

5. Import patches
6. Apply a patch
7. Remove patches
8. Quit

The options are described below.

Listing Imported Patches

To list the patches available on the system, select option 1 in the prompt.

The patch management tool checks the system for available patches. If the current-running software version is a patch, that version will have an asterisk [*]beside it.

```
=========================================================
LIST_IMPORTED_PATCH
This option will list all imported patches
(*) Current Patch Level
NNC73P1*
=========================================================
```

Importing Patches

To import patches, select option 2 in the prompt.

1. Patch file name [ ]—When prompted, enter the patch file name and its full directory path. For example:

   ```
   /opt/NNC71P1Linux64bit.tar.gz
   ```

2. Hit Enter.

The patch management tool performs the following actions sequentially:

- Checks that the import directory and patch file specified by the user exists.
- Checks that the parent destination directory exists. If not, the parent directory, /patches, is created.
- Checks whether a patch directory with the same name already exists. If so, the tool displays a message indicating that this patch has already been imported. The tool backs out from this option, and the user can select another option.
- Extracts the patch version information from the tar.gz file.
- Checks that the patch version matches the current Session Delivery Manager GA version. If a mismatch is detected, an error message is displayed indicating that the patch version is not applicable to the current GA version. The extracted file is removed and the import process is halted.
- If the version check is successful, the tool extracts the remaining contents of the patch.
- Checks each file's MD5 hash to ensure the files are valid. If a discrepancy is detected during this process, the patch is considered corrupted and is removed from the patches directory. An error message is displayed.

Below is the output for a successful patch import:

```
=========================================================
IMPORT_PATCH
This option will import a user specified patch
Please specify the patch file to import with full path
Patch file name  [        ] /opt/NNC71P1Linux64bit.tar.gz
Patch file name  [/opt/NNC71P1Linux64bit.tar.gz]
100%[==================================================]
```

Applying Patches

To apply patches, select option 3 in the prompt.

If you select option 3 to apply the patch, the patch tool checks to see if the Session Delivery Manager server is running. You cannot apply the patch if the server is running.

```
============================================================
APPLY_PATCH
This option allows the end user to apply an imported patch
 to the destination directory
Checking the server status....
Session Delivery Manager server is running
The option can not be performed when server is running
```

If the server is shut down, the patch tool displays a list of available patches on the system, and prompts you to select a patch.

The system will ask if you wish to continue. If you select Yes, the patch management tool performs the following actions sequentially:

- If the selected patch version is the same as the current-running patch version, the tool stops. The tool will prompt you to select one of two options: go back to the main menu, or select another patch to apply.
- If the current-running software version is a patch, the system is rolled back to the GA software version first, and then proceed to the next step. If the current-running version is not a patch, it will proceed to the last step.
- Backs up the GA software version and files that the target patch will replace.
- Applies the targeted patch.

A success message is displayed once a patch is successfully applied.

```
(*) Current Patch Level
[  ] 1. NNC73P1 (*)
[  ] 2. NNC73P2
[  ] 3. NNC73P5
[X] 4. Quit
Please select an option [4] 2
[  ] 1.  NNC73P1 (*)
[X] 2.  NNC73P2
[  ] 3.  NNC73P5
[  ] 4.  Quit
Do you want to continue Yes/No?
Patch applied successfully!
```

Removing All Applied Patches

To remove patches, select option 4 in the prompt.

If you select option 4 to uninstall all patches, the patch tool checks to see if the Session Delivery Manager server is running. You cannot remove patches if the server is running. If the server is running, the system sends a warning message:

```
============================================================
ROLLBACK_TO_GA
This option allows the end user to remove the current installed patch
Session Delivery Manager Server is running
The option can not be performed when server is running
```

If the server is not running, the patch management tool performs the following actions sequentially:

- If the current-running software version is a patch, the system is rolled back to the GA software version first. If the current-running version is not a patch, the tool completes the process.

The patch tool displays the following confirmation:

```
============================================================
ROLLBACK_TO_GA
This option allows the end user to remove the current installed patch
Do you want to rollback from the current version NNC73P1 to the GA release
[ ]  1 - Yes
[X]  2 - No   [Default]
Please select an option [2] 1
[X]  1 - Yes
```

```
[ ]  2 - No   [Default]
Do you want to continue Yes/No?y
Starts to rollback from NNC73P1 to GA release
Applied patch removed successfully
```

Re-establishing User-Configured Setup Configurations

It is possible that applying a new patch modifies user-configured setup options. In the event that setup files are modified, the setup process attempts to reapply the last setup configurations. This process is comprised of three components:

Pre-condition-Checks to see if there is a version change for this session. If so, it checks to see if the current version modified any of the setup configuration files.

User-required Inputs-It is possible you will be asked to input information for external dependencies such as license file location.

Post-process-If required, performs internal processes for reapplying the original setup configuration. The screen output for this process is shown below:

If you decide not to run the auto-setup, it is possible that setup will not run properly. If you select No, you will receive a warning message.

```
Auto Setup pre-checking starts...
Current installed version: NNC737P1  Initial installed version: NNC73
Detect setup configuration file change!
Done pre-checking for Auto Setup
Auto Setup is needed
Do you want to continue Yes/No?
============================================================
Welcome to Auto Setup Application
Version : NNC73
OS : Linux : amd64 : 2.6.18-194.26.1.el5
============================================================
Please wait while application loads
WARNING!!!! This process will automatically apply the previous setup
Do you want to continue Yes/No?
Checking environment and setting permissions.
Please wait ....
100%[==================================================]
============================================================
System Physical Memory Diagnostics
Total System Physical Memory = 24098 MB
Total System Free Physical Memory = 1637 MB
============================================================
System Disk Space Diagnostics
Total System Disk Space = 144 GB
Free System Disk Space = 93 GB
WARNING: Disk space is insufficient for running this application.
The recommended total disk space that should be available is = 300 GB
============================================================
System Port Availability Diagnostics : Session Delivery Manager Required Ports
The following port is available [ 5000 ]
The following port is available [ 8080 ]
The following port is available [ 61616 ]
The following port is available [ 9000 ]
The following port is available [ 8443 ]
The following port is available [ 1099 ]
The following port is available [ 8009 ]
The following port is available [ 1098 ]
The following port is available [ 8005 ]
============================================================
Check and Apply License
```

```
License Details
License number                  : 102356-1-43
ClientName                      : Acme Packet
LicenseType                     : permanent
IssuedDate                      : Fri Apr 22 16:34:20 EDT 201
Key                             : 2.0.1
StartDate                       : 2011-04-22
ExpirationDate                  :
Cluster                         : Enabled
Applications
Application                     Number of licensed devices
RouteManager                    : 500
ElementManager                  : 500
Accepting this license will replace an existing license
[X]  1 - Accept license   [Default]
[ ]  2 - Do not accept license
Please select an option [1]
[X]  1 - Accept license   [Default]
[ ]  2 - Do not accept license
Do you want to continue Yes/No?
Valid Oracle Session Delivery Manager license exists
License Details
License number                  : 102356-1-43
ClientName                      : Acme Packet
LicenseType                     : permanent
IssuedDate                      : Fri Apr 22 16:34:20 EDT 201
Key                             : 2.0.1
StartDate                       : 2011-04-22
ExpirationDate                  :
Cluster                         : Enabled
Applications
Application                     Number of licensed devices
RouteManager                    : 500
ElementManager                  : 500
[X]  1 - Accept license   [Default]
[ ]  2 - Apply new license
Please select an option [1]
[X]  1 - Accept license   [Default]
[ ]  2 - Apply new license
Do you want to continue Yes/No?
Auto setup completed for CHECK_APPLY_LICENSE
============================================================
HTTP/HTTPS configuration
No previous setup information found for HTTP
Auto setup completed for HTTPS
============================================================
Fault Management configuration
Auto setup completed for TRANSITION_HIDE
============================================================
Session Delivery Manager cluster management.
No previous setup information found for CLUSTER_MEMBERSHIP
No previous setup information found for ROUTE_MGMT_SFTP
============================================================
Route Manager Central configuration
No previous setup information found for ROUTE_MGMT
============================================================
SAML Single sign on configuration
SANE does not support AutoSetup! Manual setup is required for this
configuration
============================================================
Mail Server configuration
No previous setup information found for CONFIG_MAIL_SERVER
                      Exit Auto Setup Application
```