WAN DL

Getting Started Guide for NPAT and IP/MPLSView
# Table of Contents

**About the Documentation** ................................................................. ix

- Documentation and Release Notes .................................................. ix
- Documentation Feedback ................................................................. ix
- Requesting Technical Support ........................................................... ix
  - Self-Help Online Tools and Resources ........................................... x
  - Opening a Case with JTAC ............................................................. x

**Chapter 1** System Requirements for IP/MPLSView ................................ 1

- Outline ............................................................................................. 1
- Recommended System Configuration .................................................. 1
  - Server ............................................................................................ 1
  - Client ............................................................................................. 1
  - Traffic Data Collector (for Online Traffic Collection Module) .......... 2
- Required Ports to Open in Firewalls .................................................. 2
  - Port Map ....................................................................................... 3
  - Key .................................................................................................. 3
  - Basic Configuration ....................................................................... 4
  - Advanced Configuration ............................................................... 4
  - Port Table ....................................................................................... 5

**Chapter 2** Installing IP/MPLSView .................................................... 7

- Overview .......................................................................................... 7
- IP/MPLSView Installation ................................................................. 7
  - IP/MPLSView Server, Client, Data Collection, and Distributed Database Installation on Solaris ................................................................. 7
  - Installation from CD vs. FTP ............................................................ 7
  - Preparing for Installation ............................................................... 8
  - Server Installation ......................................................................... 9
  - Main Menu ..................................................................................... 10
  - NAT ............................................................................................... 16
  - Client ............................................................................................. 17
  - SNMP Data Collector .................................................................... 17
  - Replication and Rsync Package ..................................................... 17
  - Preserving Files From Previous Installation ................................. 18
  - Java Applet Permission ............................................................... 18
  - License File ................................................................................... 18
  - User Administration ...................................................................... 18
- Distributed Database Installation ....................................................... 18
- Distributed Traffic Collector Installation ............................................ 19
  - Installation settings and components ............................................ 19
  - Installing as Non-root User ........................................................... 20
  - Installing From Scratch ............................................................... 20
- IP/MPLSView Client Installation ....................................................... 21
  - PC Client Installation ................................................................. 21
  - Java Web Start Client Installation ................................................ 21
### Chapter 3 Installing Remote Collection Server

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outline</td>
<td>23</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>23</td>
</tr>
<tr>
<td>Installation for Collection Server</td>
<td>23</td>
</tr>
<tr>
<td>Sample Installation</td>
<td>24</td>
</tr>
<tr>
<td>Installation of Central Parsing Server</td>
<td>27</td>
</tr>
</tbody>
</table>

### Chapter 4 Installing Jump Server

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>When To Use the Jump Server</td>
<td>29</td>
</tr>
<tr>
<td>Outline</td>
<td>29</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>30</td>
</tr>
<tr>
<td>Installation for Jump Server</td>
<td>30</td>
</tr>
<tr>
<td>Sample Installation</td>
<td>31</td>
</tr>
<tr>
<td>Sample Environment Using Jump Server</td>
<td>34</td>
</tr>
<tr>
<td>Distributed Database Server Setup</td>
<td>35</td>
</tr>
<tr>
<td>Application Server Setup</td>
<td>35</td>
</tr>
<tr>
<td>Jumper Server Setup</td>
<td>36</td>
</tr>
<tr>
<td>Data Collector Server Setup</td>
<td>37</td>
</tr>
<tr>
<td>Firewall Setup</td>
<td>38</td>
</tr>
<tr>
<td>LAN Rules</td>
<td>38</td>
</tr>
<tr>
<td>Wan Rules</td>
<td>38</td>
</tr>
<tr>
<td>WAN Inbound NAT</td>
<td>38</td>
</tr>
<tr>
<td>Verification</td>
<td>39</td>
</tr>
</tbody>
</table>

### Chapter 5 Installing Viewserver

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>When To Use Viewserver</td>
<td>41</td>
</tr>
<tr>
<td>Viewserver Client</td>
<td>41</td>
</tr>
<tr>
<td>Application Client</td>
<td>42</td>
</tr>
<tr>
<td>Outline</td>
<td>42</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>43</td>
</tr>
<tr>
<td>Requirements</td>
<td>43</td>
</tr>
<tr>
<td>Installation</td>
<td>43</td>
</tr>
<tr>
<td>Configuration</td>
<td>45</td>
</tr>
<tr>
<td>User Account Setup</td>
<td>46</td>
</tr>
<tr>
<td>Startup Viewserver</td>
<td>46</td>
</tr>
<tr>
<td>Stop Viewserver</td>
<td>47</td>
</tr>
<tr>
<td>Launch Viewserver Client</td>
<td>47</td>
</tr>
<tr>
<td>Launching the Client Using Webstart</td>
<td>47</td>
</tr>
<tr>
<td>Launch the Client Using MS Windows</td>
<td>47</td>
</tr>
<tr>
<td>Commands and Paths</td>
<td>48</td>
</tr>
<tr>
<td>Viewserver</td>
<td>48</td>
</tr>
<tr>
<td>Application Server</td>
<td>48</td>
</tr>
<tr>
<td>Environmental Variables</td>
<td>48</td>
</tr>
</tbody>
</table>

### Chapter 6 Installing Report Server

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>When To Use Viewserver</td>
<td>49</td>
</tr>
<tr>
<td>Outline</td>
<td>50</td>
</tr>
</tbody>
</table>
Chapter 7 Installing Replication and Rsync

Outline

Prerequisites for Rsync

Rsync Package

Automatic Login

SSH Key Exchange Setup for IP/MPLSView Administrative Account (Rsync Only)

Installing Rsync (Backup of Online Data Collection only)

SSH Key Exchange

Installation of Rsync on Primary Application Server

Installation of Rsync on Backup Application Server

Rsync Administration

Failover Process

Switching to the Backup Server

Switching Back to the Primary Server

Installing Rsync and Replication (Four Machine Setup)

Initial Setup (Four Machine Setup)

Replication

Rsync

Installing Rsync and Replication (Two Machine Setup)

Initial Setup (Two Machine Setup)

Replication

Rsync

Failover Process

Primary server is recovered

Out-of-Sync Database Replication

Determine Sync Status

Re-Sync Procedure

Chapter 8 Installing High Availability

When to Use

Outline

Prerequisites

Software Configuration

San Storage Disk Partition

Sun Cluster Installation

Mount external SAN storage disk

IPMP Configuration

Cluster Setup

Pre Installation Steps

Configure Shared IP Addresses and Nodenames

Create Resource Groups and Assign Nodes

Create Application and Database Data Directories on External Storage Disk

Automate SSH Login from Database Servers to Application Servers

Pre Installation Checklist

IP/MPLSView Installation
About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes. Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page at the Juniper Networks Technical Documentation site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at https://www.juniper.net/cgi-bin/docbugreport/.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.


- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.

- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.
Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/
- To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico). For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.
Chapter 1

System Requirements for IP/MPLSView

Welcome to IP/MPLSView, offering solutions for both network planning and network management. IP/MPLSView is a network planning solution that provides concise and in-depth views of a router network in an intuitive graphical format. It helps managers optimize time, network bandwidth, and network resources; and can also be used to anticipate the impact of network growth or realignment. IP/MPLSView is also a network management solution that provides you with quasi real-time views of your network configurations including LSP tunnel setup, tunnel state, and traffic flows. This guide will explain the installation procedures and how to get the IP/MPLSView system up and running.

Outline

- Recommended System Configuration
- Required Ports to Open in Firewalls

Recommended System Configuration

IP/MPLSView is a client-server application and allows the user to access the program on a Solaris or Linux server via a JAVA client on a Windows, Solaris, or Linux platform. Before installing IP/MPLSView, check your hardware specifications. The following system configuration is recommended.

Server

- Sun Workstation running Solaris 10 English version; or
- Linux Red Hat/CentOS 5.5 or higher
- Minimum 2 GB RAM (4 GB RAM or more recommended)
- Minimum 40 GB disk space (100 GB or more recommended for online features)
- The swap space can be configured as approximately 2 times the physical RAM. For Solaris 10, it is recommended to enable the ZFS file system.
- CD-ROM drive*

Client

- PC running Windows XP/Vista/7; or
- Sun SPARCstation running Solaris 10; or
- Linux supporting Sun VM
- XVGA monitor and graphics card
- Minimum 512 MB RAM (1 GB RAM or more is recommended)
• 100 MB disk space
• Optical drive (CD-ROM, DVD-ROM or similar)

Traffic Data Collector (for Online Traffic Collection Module)
• PC running Windows XP/Vista/7; or
• Sun SPARCstation running Solaris 10; or
• Linux supporting Sun Microsystems (R) Java Runtime
• 1 collector per 100 to 150 devices
• Minimum 1 GB RAM (2 GB RAM or more recommended)
• Minimum 75 GB disk space
• Optical drive (CD-ROM, DVD-ROM or similar)

Informational Note: An optical drive is not required if using FTP to transfer installation files to your system.

Required Ports to Open in Firewalls

The following ports need to be opened between the client and the server so that they are able to communicate with each other. Most of the port numbers can be configured to user-defined port numbers if needed during the installation process.

<table>
<thead>
<tr>
<th>Default Port Number</th>
<th>Used For</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 7000</td>
<td>Connection to IP/MPLSView server</td>
</tr>
<tr>
<td>TCP 3389</td>
<td>LDAP (user login/administration)</td>
</tr>
<tr>
<td>TCP 8091</td>
<td>Webserver (http)</td>
</tr>
<tr>
<td>TCP 8443</td>
<td>Webserver, SSL (https)</td>
</tr>
<tr>
<td>TCP 2099</td>
<td>Task Manager (RMI registry)</td>
</tr>
<tr>
<td>TCP 1856</td>
<td>JMS JNDI / RMI, JMS Bi-Socket (Traffic collection)</td>
</tr>
<tr>
<td>TCP 8093, 8094</td>
<td>Telnet Proxy (Connect to Device)</td>
</tr>
<tr>
<td>TCP 1098, 1099, 3873, 7911</td>
<td>JNDI, RMI, EJB (Used for SNMP, CLI, processes and client-server file access).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default Port Number</th>
<th>Used For</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 22</td>
<td>SSH</td>
</tr>
<tr>
<td>TCP 23</td>
<td>Telnet</td>
</tr>
<tr>
<td>UDP 161</td>
<td>SNMP GET</td>
</tr>
<tr>
<td>UDP 162</td>
<td>SNMP Trap</td>
</tr>
</tbody>
</table>

For HTTP tunneling, if there is a firewall between the client and server, the external IP address should also be configured in the Advanced Configuration Settings. For more information, refer to NAT on page 16.

For SSH tunneling, see Setting Up Port Forwarding for Secure Communications on page 113.
Port Map

The following diagram illustrates the required ports and direction in a completely distributed environment using all server packages.

**Informational Note:** A distributed environment is not required to run IP/MPLSView. The distributed environment may be used in the Manage & Monitor package to alleviate the processing load on the server when the network is large. Not all server packages are required.

![Port Map Diagram](image)

**Key**

- **Base Ports** are a group of ports used for Offline and Online networks.
- **Clients** are a group of ports used for Performance Management and Fault Management features using a client connection to the Application server or Viewserver. The features marked with * are only available for clients connected to the Application server.
- **Online Networks** are a group of ports used for Online networks.
Basic Configuration

- The **Application Server** is the main data processing and simulation server. The default installation setting installs the Database, LDAP, and Data Collector Program packages on the Application server. If those packages are not specified as distributed, then the port and direction along those paths can be ignored. For more details on this or any other installation topic, see Chapter 2, Installing IP/MPLSView.

- The **Client** is the client machine running either Windows, Solaris, or Java Web Start.

- The **Data Collector Program** can be used to distribute the data collectors for traffic collection.

Advanced Configuration

- The **Viewserver** compliments the Application server by featuring a streamlined client connected to the Viewserver designed for network operators and planners. Only network administrators would need the full capabilities of the client connected to the Application server. This offloads users and system resources from the Application server. For more details see Chapter 5, Installing Viewserver.

- The **Distributed Database** server can be used for data storage apart from the Application server. For more details see Chapter 2, Installing IP/MPLSView.

- The **Collection Server** can be used for the remote VLAN auto-discovery module and remote data collection. For more details see Chapter 3, Installing Remote Collection Server.

- The **External LDAP** server can be used for user administration and authentication apart from the Application server. For more details see the Security Management chapter in the Management and Monitoring Guide.

- The **Backup Application** server can be used with Rsync packages for redundancy. For more details see Chapter 7, Installing Replication and Rsync.

- The **Backup Database** server can be used with Rsync and Replication packages for redundancy. For more details see Chapter 7, Installing Replication and Rsync.
### Port Table

The following table lists the required ports and direction by Suite, Module, or Package.

<table>
<thead>
<tr>
<th>Source &gt; Destination</th>
<th>Usage</th>
<th>Destination Port</th>
<th>Product</th>
<th>Modules</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Clients</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client &gt; App &amp; View</td>
<td>Simulation Engine</td>
<td>7000</td>
<td>IP/MPLSView, NPAT</td>
<td>Management, Provision, Design Essentials</td>
</tr>
<tr>
<td>Client &gt; App &amp; View</td>
<td>Task Manager</td>
<td>2099</td>
<td>IP/MPLSView, NPAT</td>
<td>Management, Provision, Design Essentials</td>
</tr>
<tr>
<td>Client &gt; App &amp; View</td>
<td>Web Server</td>
<td>8091</td>
<td>IP/MPLSView, NPAT</td>
<td>Management Essentials, Web</td>
</tr>
<tr>
<td>Client &gt; App &amp; View</td>
<td>Web Server SSL</td>
<td>8443</td>
<td>IP/MPLSView, NPAT</td>
<td>Optional secure Web</td>
</tr>
<tr>
<td>Client &gt; App &amp; View</td>
<td>Live Network</td>
<td>2099, 1098, 1099</td>
<td>IP/MPLSView</td>
<td>Management, Provision Essentials</td>
</tr>
<tr>
<td>Client &gt; App &amp; View</td>
<td>Telnet Proxy</td>
<td>8093, 8084</td>
<td>IP/MPLSView</td>
<td>Management, Provision Essentials</td>
</tr>
<tr>
<td>Client &gt; App &amp; View</td>
<td>View Live</td>
<td>3673, 7911</td>
<td>IP/MPLSView</td>
<td>Performance Management</td>
</tr>
<tr>
<td>Client &gt; App &amp; View</td>
<td>MiB Browser</td>
<td>3873</td>
<td>IP/MPLSView</td>
<td>MiB Browser</td>
</tr>
<tr>
<td>Client &gt; App &amp; View</td>
<td>Event Browser</td>
<td>1856</td>
<td>IP/MPLSView</td>
<td>Fault Management</td>
</tr>
<tr>
<td>Client &gt; App &amp; View</td>
<td>Web Event Browser</td>
<td>1856</td>
<td>IP/MPLSView</td>
<td>Fault Management</td>
</tr>
<tr>
<td>Client &gt; App &amp; View</td>
<td>User Admin</td>
<td>3389</td>
<td>IP/MPLSView</td>
<td>Security Management</td>
</tr>
<tr>
<td>Client &gt; External LDAP</td>
<td>User Admin</td>
<td>3389</td>
<td>IP/MPLSView</td>
<td>Security Management</td>
</tr>
<tr>
<td><strong>Application Client only</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client &gt; App</td>
<td>Traffic Manager</td>
<td>1856</td>
<td>IP/MPLSView</td>
<td>Performance Management</td>
</tr>
<tr>
<td>Client &gt; App</td>
<td>Event Subscription</td>
<td>1856</td>
<td>IP/MPLSView</td>
<td>Fault Management</td>
</tr>
<tr>
<td>Client &gt; App</td>
<td>Threshold Editor</td>
<td>1856</td>
<td>IP/MPLSView</td>
<td>Threshold Crossing Alerts</td>
</tr>
<tr>
<td><strong>Application &amp; Viewserver</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>App &amp; View &gt; Network</td>
<td>SNMP GET</td>
<td>161</td>
<td>IP/MPLSView</td>
<td>Performance Management</td>
</tr>
<tr>
<td>App &amp; View &gt; Network</td>
<td>SSH</td>
<td>22</td>
<td>IP/MPLSView</td>
<td>Management, Provision Essentials</td>
</tr>
<tr>
<td>App &amp; View &gt; Network</td>
<td>Telnet</td>
<td>23</td>
<td>IP/MPLSView</td>
<td>Management, Provision Essentials</td>
</tr>
<tr>
<td>Network &gt; App &amp; View</td>
<td>SNMP Trap</td>
<td>162</td>
<td>IP/MPLSView</td>
<td>Fault Management</td>
</tr>
<tr>
<td>App &amp; View &gt; DB</td>
<td>Rsync</td>
<td>22</td>
<td>IP/MPLSView</td>
<td>Rsync &amp; Replication</td>
</tr>
<tr>
<td>App &amp; View &gt; DB</td>
<td>MySQL</td>
<td>3333</td>
<td>IP/MPLSView</td>
<td>Distributed Database</td>
</tr>
<tr>
<td>DC &gt; App &amp; View</td>
<td>Traffic Collection</td>
<td>1856</td>
<td>IP/MPLSView</td>
<td>Performance Management</td>
</tr>
<tr>
<td><strong>Data Collector Program</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DC &gt; Network</td>
<td>SNMP GET</td>
<td>161</td>
<td>IP/MPLSView</td>
<td>Performance Management</td>
</tr>
<tr>
<td>DC &gt; Network</td>
<td>SSH</td>
<td>22</td>
<td>IP/MPLSView</td>
<td>Performance Management</td>
</tr>
<tr>
<td>DC &gt; Network</td>
<td>Telnet</td>
<td>23</td>
<td>IP/MPLSView</td>
<td>Performance Management</td>
</tr>
<tr>
<td>Network &gt; DC</td>
<td>FTP, STP, Bulkstats</td>
<td>21, 22</td>
<td>IP/MPLSView</td>
<td>Performance Management</td>
</tr>
<tr>
<td><strong>Primary and Backup</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary App &gt; Backup App</td>
<td>Rsync</td>
<td>22</td>
<td>IP/MPLSView</td>
<td>Rsync &amp; Replication</td>
</tr>
<tr>
<td>Primary DB &gt; Primary DB</td>
<td>Rsync</td>
<td>22</td>
<td>IP/MPLSView</td>
<td>Rsync &amp; Replication</td>
</tr>
<tr>
<td>Backup DB &gt; Primary DB</td>
<td>MySQL</td>
<td>3333</td>
<td>IP/MPLSView</td>
<td>Rsync &amp; Replication</td>
</tr>
<tr>
<td><strong>Collection Server</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collection &gt; App</td>
<td>Data Collection</td>
<td>1856</td>
<td>IP/MPLSView</td>
<td>Management Essentials</td>
</tr>
<tr>
<td>Collection &gt; App</td>
<td>SNMP Trap</td>
<td>162</td>
<td>IP/MPLSView</td>
<td>Management Essentials</td>
</tr>
<tr>
<td>App &gt; Collection</td>
<td>Tank Manager</td>
<td>2099</td>
<td>IP/MPLSView</td>
<td>Management Essentials</td>
</tr>
<tr>
<td>App &gt; Collection</td>
<td>Proxy Relay</td>
<td>7911</td>
<td>IP/MPLSView</td>
<td>Management Essentials</td>
</tr>
</tbody>
</table>

Figure 2: Port Table
Chapter 2

Installing IP/MPLSView

IP/MPLSView software is a client-server application. The IP/MPLSView server is installed on a Sun or Linux platform and can be accessed from an IP/MPLSView client installed on a Windows™, Solaris™, or Linux™ platform. This chapter explains the installation procedure for both the server and client software.

Overview

- IP/MPLSView Installation on 7
  - Installing IP/MPLSView server, client, data collector, and distributed database for Solaris 10
  - Installing IP/MPLSView client and data collector for Windows XP/Vista/7, Solaris 10
  - Installing Web Start client for Windows XP/Vista/7, Solaris 10
- Updating the IP/MPLSView Server on 22

Informational Note: If you have difficulties installing IP/MPLSView, please contact Juniper support.

IP/MPLSView Installation

The following instructions describe how to install the IP/MPLSView software after logging in as root user. A non-root user should not be used for a new installation except for special circumstances.

IP/MPLSView Server, Client, Data Collection, and Distributed Database Installation on Solaris

This procedure will set up the IP/MPLSView server, JAVA client, Data Collection, and Distributed Database on your Solaris machine.

Installation from CD vs. FTP

For an installation from a CD, insert the IP/MPLSView CD-ROM into the CD-ROM drive on the Sun machine which you will be using as your server. Your installation directory will be /cdrom/cdrom0.
For an installation from the ftp site, create an install directory on your server and download all the installation files to that directory. Make sure that you have downloaded the version for the appropriate processor, Solaris Sparc, Solaris x86 (AMD), or Linux. To check which processor your server uses, run the command “uname -a” on the IP/MPLSView server. After downloading the installation files, extract the server, client, dcollect, and optionally the replication package for the following directories: server, client, dcollect, and replication. Exact file names may vary.

If the files end in .tar, extract them using “tar xvf”:

```
tar xvf MPLSserver.tar
.tar xvf MPLSdcollect.tar
.tar xvf MPLSclient.tar
.tar xvf MPLSreplication.tar
```

If the files instead end in .tar.gz, extract them using “gunzip < file.tar.gz | tar xvf -”:

```
gunzip < MPLSserver.tar.gz | tar xvf -
gunzip < MPLSdcollect.tar.gz | tar xvf -
gunzip < MPLSclient.tar.gz | tar xvf -
gunzip < MPLSreplication.tar.gz | tar xvf -
```

Preparing for Installation

If there is a previous IP/MPLSView installation on the machine, switch to the IP/MPLSView admin user (usually this user is wandl) and shut down the existing services before starting a new installation.

```
$ /u/wandl/dcollect/dc.sh stop all
$ /u/wandl/bin/stop_mplsview
```

If the previous IP/MPLSView installation includes traffic collection, it is recommended to backup the data. Check for sufficient disk space using command “df -k”. Compress and zip the files using command “cd /u/wandl; tar chvf - data | gzip -c > data.tar.gz”. The tar ‘h’ flag is necessary to archive the data pointing to the logical link /u/wandl/data.

Server Hostname and IP Address

On the Sun machine, log in as root user. If you do not have direct access to the Sun machine, you can telnet or ssh from a different machine using a non-root user login and then switch to root user using the “su” command.

If you intend to change the IP address or hostname of the server, it is recommended to do this before running the server installation.

- In some cases, the server has more than one interface, one with an IP address configured for the internal network and another with IP address configured for the external network. For the server’s IP address, choose the IP address that can be reached by the client machine(s) from which you plan to access the server, which is usually the external IP address.
- In other cases, the server’s IP address is a private NAT IP address, and the client will need to reach it over the public NAT IP address. For more details on setting up the installation to support NAT environments, see NAT on 16.
Make sure the hostname points to the IP address that you want to use for the installation, so that the installation picks up the correct default IP address. To check this, try running on the server a traceroute to the hostname via “/usr/sbin/traceroute <hostname>” and see if the result includes the desired IP address.

**Create a Group and User ID**

Before the installation, you should create a user ID and group ID to use for the IP/MPLSView admin.

To create a new group id for the IP/MPLSView admin, use the command “groupadd groupname” as root user and substitute the groupname with a name of your choosing.

To create a new user id for the IP/MPLSView admin, use the command “useradd” as root user. Sample command, “useradd -g staff -s /bin/ksh -d /export/home/wandl -m wandl” will add the user “wandl” in group “staff” with the administrative home directory, or $HOME, set to /export/home/wandl.

The user's administrative home directory should be created with the right ownership and privileges for the administrative user. If the administrative home directory is going to be /export/home/wandl, use “chown -R wandl:staff /export/home/wandl” to give wandl ownership of the directory and “chmod -R 755 /export/home/wandl” to give wandl full privileges and other users read and executable privileges.

After adding a new user, a password should be created for the new user using the “passwd” command. Command “passwd wandl” will prompt for a new password for user wandl.

**Informational Note:** If your UNIX machine is under your company's NIS or NIS+ system, the local root access may not be able to create a new group, or the creation may cause conflicts with the NIS/NIS+ system. In this case, ask the system administrator to create the proper group and add all the users to the group before the installation.

**Server Installation**

1. If installing from CD, go to the server directory in /cdrom/cdrom0: If installing from FTP, go to the server directory where you extracted the files.
2. As the root user, run the ./install.sh script.
   
   You will be asked to shut down existing IP/MPLSView processes to prevent conflicts with the new installation. The program will also check to see which Solaris Java patches you may need to install.
3. At any time during the installation, if you press <Enter> without entering any text, the default settings will be used. At any time during the installation, you can press <Ctrl>-c to abort the installation.
4. The first general setting is the Admin User, which defaults to “wandl”. Users should input a valid UNIX user id besides “root”. For instructions adding a user ID, refer back to Create a Group and User ID on 9.
5. The second general setting is the Admin Group, which defaults to the group id of the user id. If you want to use a different group id, then enter the new group id here. If this group does not exist, the installation program will create one and ask you to add its members. Please be aware that if a user is currently logged on to the system, the installation program cannot add the user to the group. You will need to contact your system administrator to add all the users into the group.
6. The third general setting is the **Installation Directory**. Please make sure there is sufficient disk space to install the program (approximately 1 GB). The directory will be created by the installation program if it is not there. At the end of the installation, `/u/wandl/` is automatically linked to this directory.

**Informational Note:** Do not use the operating system partition “/” for the installation directory as this may lead to errors if the partition becomes full.

If you are upgrading from an existing installation and are planning to use online features such as traffic data collection, it is recommended to install IP/MPLSView in a new installation directory.

7. The last general setting is the **Data Directory**, which is where most of the user data, including the MySQL database, will be stored. Please make sure there is sufficient disk space, especially if you plan to run data collection on your network. At the end of the installation, `/u/wandl/data` is automatically linked to this directory.

**Informational Note:** If you are upgrading from a previous installation and have previously collected data that you wish to still load from IP/MPLSView, you should enter in that data directory’s complete path. To determine that path, run `"ls -l /u/wandl/data"`. Due to database structural changes, it is recommended to backup the previous data directory.

If you do not have any previously collected data, it is recommended to perform a fresh install with a new data directory.

**Main Menu**

The following server configuration settings allow for more advanced options of IP/MPLSView. For example, you may wish to use these settings in the following situations:

- If you have a NAT environment, see **IP Address Settings** on 12 and **NAT** on 16.
- If you wish to install the database on a different Sun workstation from the main application server for a distributed environment, see **IP Address Settings** on 12
- If you are using the online traffic collection features, which require increasing some default memory settings, see **Memory Settings** on 12
- If you would like e-mail capability or notification if server processes fail, see **Overall Settings** on 11
- If you have a firewall and need to modify port numbers, see **Port Settings (Server to Client)** on 13
- If you are using the online fault management settings and would like to enable background ping to check for device reachability, or to enable trap forwarding, see **Online Fault Management Settings** on 14.

**Main Menu**

**Server Configuration Settings:**
(A) **Overall Settings**
(B) **IP Address**
(C) **Memory Settings**
(D) **Port Settings (Server to Client)**
(E) **Port Settings (Advanced)**
(F) **Online Performance Management Settings**
(G) **Online Fault Management Settings**
(H) **Advanced Configuration**
Some of these options can be changed after installation using the command /u/wandl/bin/changeconfig.sh. Changing these settings requires first stopping IP/MPLSView using command /u/wandl/bin/stop_mplsview. After the settings have been changed, IP/MPLSView can be restarted using command /u/wandl/bin/startup_mplsview.

**Overall Settings**

8. The overall settings are the general administrative settings.

(A) Overall Settings

General Administrative Settings:

1.) Installation Directory.....: Application server installation directory.
2.) Data Directory...............: User data and MySQL database directory.
3.) Admin User..................: Super-user name.
4.) Admin Group................: Super-user group.
5.) Email Server IP.............: Email server IP.

The Email server IP is used by certain online functions to send e-mail, such as the Aggregated Traffic Report task, Event Subscription, and the Application Monitor, which provides status notifications regarding IP/MPLSView processes. This IP can be the IP address of your company’s e-mail server. Your application server should be able to reach this IP address, and your company's e-mail server may need to be configured accordingly.

To set up your Solaris server to send email, you can edit /etc/hosts:

```
mail_server_ip  servername   servername.customer.com   mailhost
```

Next, as root, run "svcadm restart sendmail" (Solaris 10) or "/etc/init.d/sendmail stop; /etc/init.d/sendmail start" (Solaris 9)

6.) Email Server User...............: Email server login name.
7.) Email Server Password...........: Email server login password.
8.) Application Monitor Email Recipient....;

If you wish to have the application monitor notify you via e-mail of IP/MPLSView application process status information such as when processes go down.

9.) Enable Server Monitoring............;

This setting allows you to view the application’s processes monitored by Application Monitor from the Web under Admin > View System Monitor.

10.) Mapping for non-Unicode characters....;

Method to translate the non-Unicode characters. This setting allows you to change the character encoding used by IP/MPLSView in both the Java and web interface. This feature may be needed if your data files, for example, configuration files, contain special characters. By default the character encoding is ASCII. To see a list of supported code set names use the command "/usr/bin/iconv -l". When prompted to enter a new coding, type in the code set name. Note that the code set name is case sensitive.
IP Address Settings
If the server has more than one interface with different IP addresses, double-check that
the server IP address used is accessible by the client (see Server Hostname and IP Address
on 8). If the server will be accessed via a public NAT address, see NAT on 16.

(B) IP Address
IP/MPLSView Server IP Address Settings:
1.) Webserver IP

The Web Server IP is used to access the Web Interface. It is usually the same as the
Server IP.

2.) LDAP Server IP

The LDAP Server IP is required for IP/MPLSView user administration and should be the
same as the Server IP.

3.) External Webserver IP (for NAT)

The External Webserver IP is used for special NAT and port forwarding situations. If you
have a firewall forwarding internalIP:port to externalIP:port, set the external Webserver IP
to the public NAT IP and enable the option for NAT. See NAT on page 16 for more details
on how to configure this option.

4.) Use Remote Database

If you wish to set up the server environment as a distributed database, you should set this
option to YES. This will install the MySQL database on a different server than the
IP/MPLSView application server. Further instructions can be found in Server Hostname
and IP Address on page 8

Remote Database IP

The IP address of the remote database.

Remote Database Port

The port of the remote database.

Memory Settings
Check how much physical memory (RAM) is available on your server using the command
"/usr/sbin/prtconf | grep 'Memory'". Some servers may not support more than 2048 MB per
process even if the total RAM resources are larger than 2 GB. If the process is using the 32
bit address space, the maximum memory it can allocate is 4 GB.

Memory usage during operation can be checked using command
/u/wandl/bin/status_mplsview

(C) Memory Settings
1.) Task Manager Memory
2.) Webserver Memory
3.) Thrift Server Memory
4.) HornetQ Memory
5.) DGS Memory
6.) Application Monitor Memory
7.) Threshold Server Memory
8.) SNMP Trap Daemon Memory
9.) MongoDB Memory
10.) Event Server Memory
11.) Aggregation Memory
12.) Selective Interface Manager Memory.....: 256
13.) Database Memory......................: 256

Total system physical memory:  3933 Megabytes

**Port Settings (Server to Client)**

These are the required ports to open between the server and client. Generally, these ports do not need to be modified, unless they are in conflict with other applications which need to use these ports, or due to special firewall requirements. If the Server, LDAP, or Webserver port settings are modified on the server, they also need to be modified on the client as well.

**(D) Port Settings**

1.) Server Port........: 7000
2.) LDAP Server Port.....: 3389
3.) Webserver Port.......: 8091
4.) SSL Port........: 8443
   - SSL Domain......: Unknown
   - SSL Department..: Unknown
   - SSL Organization: Unknown
   - SSL Loc./City....: Unknown
   - SSL State/Prov.: Unknown
   - SSL Country.....: United States,us
5.) Task Manager Primary Port...: 2099
6.) HornetQ Port................: 1856
7.) Thrift Server Port........: 7911

**Port Settings (Advanced)**

These are the required ports to open when advanced settings are used. Generally, these ports do not need to be modified.

**(E) Port Settings (Advanced)**

1.) SNMP Trap Daemon Port.............: 162
2.) Event Post Port...................: 7077
3.) JBoss Web JNDI Port...............: 1099
4.) JBoss Web JNDI-RMI Port..........: 1098
5.) JBoss Web JRMP Port...............: 5444
6.) JBoss Web JRMP Invoker Port.......: 5446
7.) JBoss Web AJP Port...............: 8009
8.) JBoss Web Classloader Port.......: 8083
9.) MariaDB Database Port............: 3333

**Online Performance Management Settings**

These settings are used in traffic collection and aggregation processing.

**(F) Online Performance Management Settings**

**Aggregation Settings:**

1.) Maximum Traffic Capacity in Days......:

The number of days of raw data to store for traffic processing. Corresponds to the key ‘archiveCapacity’ in /u/wandl/db/config/agg.xml and in
/u/wandl/web/wandl/WEB-INF/web.xml. After this point, the raw data will be aggregated and overwritten in the database.

2.) Aggregation Memory...................:

Memory usage for aggregation processing.
3.) Maximum Historical Traffic Capacity...:

The number of days to store the aggregated traffic files. After this point, the traffic files will be deleted from the server.

4.) Archive Traffic in MariaDB Export Format:

If this option is set to YES, traffic archive will run daily and be stored in /u/wandl/data/traffic.archive. A cronjob is used to run the agg.sh script at a set time each day.

Online Fault Management Settings

These settings are used in trap collection and event processing. The SNMP Trap Daemon IP could potentially be different from the Application Server IP if the server has a different interface to reach the router lab and the client machine.

(G) Online Fault Management Settings
SNMP Trap Settings:
1.) SNMP Trap Daemon IP.................:

The SNMP Trap Daemon IP is the IP address on the IP/MPLSView server, which will receive traps from network devices. Make sure it is reachable by network devices, and is configured on the network devices as the SNMP target address.

2.) SNMP Trap Store Capacity...........:

The number of days the SNMP traps will be saved. Trap data beyond this number of days will be discarded.

3.) Enable Trap Forwarder...............:

Use this option to enable or disable trap forwarding to a third-party NMS supporting JMS.

4.) Trap Forwarding Upstream Address...:

The Trap Forwarding Upstream Address can be used to forward traps from IP/MPLSView to a third-party NMS supporting JMS. Make sure that this IP address is reachable by the IP/MPLSView application server, and that the third party is listening on port 162 (default). Additional configuration is also required from Application > Event Subscription Editor. See the Management & Monitoring Guide for more info.

5.) Trap Forwarding Upstream Port......:

Traps sent to the destination IP goes through this port

Event Settings:
6.) Network Event Storage Capacity.....:

The number of days the network events processed from traps will be saved. Event data beyond this number of days will be discarded. By default 30 days of events are stored in directory /u/wandl/data/event. Events older than the specified value are removed.

7.) Event Post Port....................:

Events go through this port.

8.) Event Server Memory................:

Memory usage of event server for processing events.
9.) Event AIM User...........:
10.) Event AIM Password......:
11.) Event Gtalk User........:
12.) Event Gtalk Password....:
13.) Event Msn User.........:
14.) Event Msn Password......:
15.) Event Yahoo User.......:
16.) Event Yahoo Password...:
17.) Threshold Initial Notification...:

Background Ping Settings:
18.) Background Ping.....................:

Allows you to ping all devices in the Live network and will send an event to the Event Browser if a device becomes unreachable.

Background Ping Interval.....................:
Background Ping Number of Retry.............:
Background Ping Retry Interval...............:
Background SNMP connectivity test............:
Background connectivity test via telnet/SSH...:
Use FPING.....................................:
FPING PATH....................................:

The Enhanced Background Ping
This setting allows you to multi-thread the ping process for faster performance and add additional device profiles not collected in the network. The additional devices will appear as an event in the Event Browser when it becomes unreachable. Edit the file /u/wandl/db/config/diag.xml. Within the <DevicePing> tag, you can add <threadcount>integer</threadcount> for multi-thread, and <addprofile>filename</addprofile> for additional device profiles. You can add multiple <addprofile> tags using one tag per profile. The addprofile file format is the same as the Router Profile and must be in the same directory under /u/wandl/data/.TaskManager/profile/. Changes to the diag.xml take effect when the network is loaded. See the Management and Monitoring Guide for more details.

Advanced Configuration
This setting is for advanced configuration to allow NAT access, enable the jump server environment, or enable the remote data collectors.

(H) Advanced Configuration
Advanced Configuration Settings:
1.) Enable NAT access for JMS....:

This setting allows you to use the Public NAT IP address (External Webserver IP) instead of the private NAT IP address when there is a NAT or firewall in the server environment. You need to specify the IP address in the External Webserver IP option and set Enable NAT access option to ON for this feature to work. See NAT on page 16 for more details.

2.) External Webserver IP (for NAT)........:

IP address of external webserver, or the Public NAT IP. For more details, see NAT on page 16.

3.) Enable Jump Server..........:
This setting allows you to setup a jump server into the server environment. The jump server will relay requests for CLI, SNMP polling, and forward traps to the application server for processing. See Chapter 4, Installing Jump Server for more details.

4.) Distributed Collection Servers........:

List of IP_address:port of remote polling servers, where the port is usually 2099. For more information, see Chapter 3, Installing Remote Collection Server.

5.) Database Temp Directory..............:

A temporary directory used by the MariaDB server for daily traffic aggregation.

6.) Email Sender Address..................:

The email address for task server notifications.

NAT

Note that for NAT environments, 2 additional ports should be opened in the firewall between the server machine and client machine (1101 and 21101) using the Port Settings option.

The following settings should be used for the NAT option when installing and launching the client, setting Event Browser, Traffic Collection Manager, and Threshold Editor options. Assuming the IP for server installation is the private NAT address and the IP for the client installation is the public NAT address.

Server Installation

- Use the public NAT IP for the “External Webserver IP (for NAT)” setting.
- Use the private NAT IP for the “Webserver, LDAP, and Remote Database IP” settings.

IP/MPLSView Server IP Address Settings:

1.) Webserver IP..........................: Private NAT IP
2.) LDAP Server IP.........................: Private NAT IP
3.) External Webserver IP (for NAT)....: Public NAT IP
4.) Use Remote Database.................: YES
   Remote Database IP....................: Private NAT IP
   Remote Database Port...............: 3333

Client Installation

- Use the public NAT IP for IP address entries
- Install with “Use HTTP Tunneling for Firewall” option checked or
- Add the keyword "FIREWALL" to the end of the resulting ipmplsview.bat file's java command after the installation is done. The ipmplsview.bat file can typically be found on the PC's desktop, or in C:\Program Files\wandl\IP-MPLSViewX.X where X.X is the version number:

%JRE% -Xms%MEMORY% -Xmx%MEMORY% -XX:NewRatio=2 -Dsun.java2d.nodraw=true -classpath %CLASSPATH% bbdsgn %SERVER% %SERVERPORT% %WEBSERVER% %WEBSEVERPORT% %LDAPSERVER% %LDAPPORT% mplsvie FIREWALL

Launching Web Start Client

- Use public NAT IP for the IP address entries
- Check “Use HTTP Tunneling for Firewall”
Installing IP/MPLSView

Client Options
- Select Application > Options > JMS Access pane, “Use HTTP Tunneling” option

Traffic Collection Manager, Event Browser, and Threshold Editor parameter window
- When opening the Traffic Collection Manager, Event Browser, or Threshold Editor window for the first time, a dialog box will appear with configuration options. Select “Use HTTP Tunneling.”
- If this option does not appear, you may need to delete any IP/MPLSView cached xml files from previous instances of these windows. On Windows, the xml files may be in C:\Users\<username>\AppData\Roaming\wandl

Client
After installing the server, you will be asked if you want to install the client on the Sun machine. Press <Enter> or ‘y’ to continue.

You can install the client at a later time by running the following script as a non-root user:
/cdrom/cdrom0/client/solaris/install.client

You may also install the Windows client on a Windows XP/Vista/7 machine from the CD’s executable, \client\MSWindows\installIPMPLSView.exe. Further instructions can be found in IP/MPLSView Client Installation on 21.

The required information includes the server name or IP address, port number for communication, and the name or IP address of the application server and its port number.

SNMP Data Collector
After installing the client, you will be asked if you want to install the data collector.

Distributed Traffic Collectors

Informational Note: If you want to install the data collector on a different Solaris system, you can answer “N” and then run the installation script from the CD on the other system: /cdrom/cdrom0/dcollect/unix/install.dcollect. It is recommended to set up one data collector per 100 to 150 devices. When installing the data collector on another system, enter in the IP address of the main IP/MPLSView server when prompted for the JMS server. See Distributed Traffic Collector Installation on 19 for a sample installation.

Replication and Rsync Package
After installing the data collector, you may be asked if you want to install the replication and rsync package. The replication and rsync package is used for the IP/MPLSView online functions (data and traffic collection) to keep in sync the files and database on the primary server and a secondary server. The purpose of the package is to have a backup copy in case the primary server fails. The rsync package will backup files from the primary application server to the backup application server, and the replication package will update the secondary database to be in sync with the primary database.

Informational Note: This package requires that the backup IP/MPLSView server have a separate license. Additionally, the actual rsync program should be separately installed, if not already available on the server, using /cdrom/cdrom0/replication/inst_rsync.sh
Preserving Files From Previous Installation
If you have previously installed IP/MPLSView and it is linked by /u/wandl, the program will provide the option to copy over files from the previous installation which may have customized user settings. For example, the default is to preserve previous LDAP user account data, and previous commands and command templates. Original and new files from /u/wandl/db/command will be backed up regardless of your selection.
If you want to do a completely fresh installation ignoring the old settings, toggle options to "N".
You may want to answer “Y” to User Admin settings to avoid having to recreate the user groups and privilege mappings, and assignment of Unix IDs to user groups.

Java Applet Permission
Before the end of the installation, you will be prompted whether or not to “Give JAVA Applets write-permission (default=no)? [y/n]”. Choose “yes” if you would like the capability of saving images or reports to the client from the chart and trending applets accessed via the Web Interface.

License File
After the installation is complete, you will be asked to update the /u/wandl link. Select Yes or press enter.
If the license file was found from the previous installation, you will be prompted to start up the IP/MPLSView server.
Otherwise, copy the license file (npatpw) into directory /u/wandl/db/sys as the IP/MPLSView admin user. If you do not have a license file, contact Juniper support.
After the license file is in place, the server can be started using command /u/wandl/bin/startup_mplsview”. See Starting Up the IP/MPLSView Server on page 103 for more information.

User Administration
For more information on creating user groups and adding additional users into groups, see Launching the User Administration Tool on page 117 and Performing User Administration from Text Mode on page 119.

Distributed Database Installation
If you wish to install the MySQL database on a different machine from the IP/MPLSView server, first check that rsync is installed on the database server “pkginfo | grep rsync”. If rsync is not installed, run the replication/inst_rsync.sh script as root user.
Secondly, the `wandl` user on the database server needs to be able to auto-login to the `wandl` user on the IP/MPLSView application server. For this to happen, the database server’s public key (id_rsa.pub) must be present in the IP/MPLSView application server’s authorized keys (~wandl/.ssh/authorized_keys). See Automatic Login on page 62 for detailed procedures of creating a private and public key for the database server, but do it for the `wandl` user (not root user). Copy over the public key to the remote server’s .ssh/authorized_keys file to enable automatic login. Only one-way SSH from the traffic collector to the IP/MPLSView server is needed in this case.

Switch to the root user using “su”, change directory to the installation’s server directory, and run “./instdatabase.sh” on the machine where you want the database to be installed. Follow the installation instructions as they appear on the screen.

**Informational Note:** Make sure that during the installation of the main IP/MPLSView application server that you configure the settings for “Distributed Database” under “IP/MPLSView Server IP Address Settings”. After installation of the database and the IP/MPLSView application server, the database server should be started before starting the IP/MPLSView application server.

### Distributed Traffic Collector Installation

Switch to the admin user (wandl), change directory to the installation’s server directory, and run “./install.dcollect” on the machine where you want the data collector to be installed. Follow the installation instructions as they appear on the screen.

### Installation settings and components

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Contains settings for the NPAT Server, the Task Server, and the SNMP Trap Daemon</td>
</tr>
<tr>
<td>JBoss</td>
<td>Contains settings for JBoss, which powers the Web Server and provides JMS for communication between different applications within IP/MPLSView</td>
</tr>
<tr>
<td>Email</td>
<td>Contains Email settings for the Event Server, enabling the automatic notification of certain events via Email</td>
</tr>
<tr>
<td>Event</td>
<td>Contains settings for the Event Server</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPAT Server</td>
<td>The core design and simulation engine that powers NPAT</td>
</tr>
<tr>
<td>Task Server</td>
<td>The server process that powers the Task Manager (Application&gt;Task Manager). It is used to schedule tasks such as Discovery, Network Data Collection, and Network Monitoring for online users and Configuration Management tasks for both online and offline users</td>
</tr>
<tr>
<td>MySQL</td>
<td>The database used to store traffic collection data</td>
</tr>
<tr>
<td>Web Server</td>
<td>The server process that powers the IP/MPLSView Web interface (File &gt; Launch Web) as well as the online help (accessed via Help buttons). The IP/MPLSView Web interface is a convenient interface for web viewers to access Network Reports. For online users, it also offers near-real-time access to network, event, and diagnostics data and charts for the live network.</td>
</tr>
<tr>
<td>Event Server</td>
<td>The server process that powers the Event Map (Application&gt;Maps&gt;Event Map) and Event Browser (Application&gt;Event Browser). In the live network, the event server manages and monitors events and SNMP traps on network devices</td>
</tr>
</tbody>
</table>
Installing as Non-root User

Installing as a user id other than root will ensure that no processes generated by the IP/MPLSView software will have root ownership. When installing as a non-root user id for the first time, you should install from scratch, that is, install in an entirely new directory.

There are several things that the user must be aware of when installing as a user id other than root. Please read the following guidelines carefully to understand the effects of using a user id other than root. We will refer to the user id that installs and starts up the server as the “owner of the application”.

- The application should be brought up by the owner of the application.
- All processes will be owned by the application owner.
- Any files generated by IP/MPLSView will be owned by the application owner.
- If there are multiple users, all users of the application must have the same group id as the application owner.
- All the users' directories must be "read/writable" by the application owner to ensure that all application output can be saved.
- Any future updates of the software must be performed by the application owner.

Installing From Scratch

If you have a version of IP/MPLSView already installed, first stop it:

```bash
$ cd /u/wandl/bin
$ ./stop_mplsview
```

If you previously installed as root and linked /u/wandl, you must first remove this link. You may need root privileges (log in as root) in order to remove the link. Before you do anything, check to make sure /u is a link by running "ls -l /u". If so, you will see "wandl ->" followed by the location that /u/wandl is linked to.

```
# rm /u/wandl
```

Log into the server as the desired user id and perform the steps described earlier in this chapter. That is, once the CD is inserted, run the install script:

```bash
cd /cdrom/cdrom0/server
$ ./install.sh
```

After the application owner starts up the application, other users can still log into the application as long as they belong to the same group id as the owner of the application.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Gateway Server</td>
<td>The server process that takes traffic collection data from the data collectors and stores it in the MySQL database</td>
</tr>
<tr>
<td>Aggregation</td>
<td>A scheduled task that aggregates the traffic collection data stored in the MySQL database</td>
</tr>
<tr>
<td>LDAP Server</td>
<td>Lightweight Directory Access Protocol needed for User Administration</td>
</tr>
</tbody>
</table>
However, all IP/MPLSView files or output generated by other users will be saved with the ownership set to that of the application owner.

**IP/MPLSView Client Installation**

Make sure that your client machine can connect to the application server. Before the client installation, you should have the server's IP address ready.

**PC Client Installation**

1. If installing from a CD, insert the IP/MPLSView CD-ROM into the CD-ROM drive of your PC workstation. Double-click the **Computer** icon. Double-click the CD-ROM drive icon. In the CD-ROM folder, navigate to the \client\MSWindows\ folder. If installing from the FTP site, download the installIPMPLSView.exe file to the PC client.

2. Double-click the **installIPMPLSView.exe** icon to begin running the IP/MPLSView PC client installation program. Follow the on-screen instructions to install the client. The installer will ask you to enter the name or IP address of the server in which you have IP/MPLSView installed. Enter the IP address here. Note that you may also enter the hostname if your hostname is listed in the hosts file of your PC.

3. Choose the default port number for the server, unless those ports were specially configured.

4. For the memory allocation option, generally a higher setting allows for better application performance for large networks. However, reserve some RAM for other applications that you may be running at the same time.

5. Select the directory in which to install the client. The default directory will be C:\Program Files\wandl\IP-MPLSViewx.x (x.x being the release number). Alternatively, use the **Browse** button to select the directory of your choice.

You may click on the **Back** or **Cancel** button at any time to go back to the previous steps for correction or to exit out of the installation program and install at a later time.

After the client installation is finished, it will create the file ipmplsview.bat in the installation directory. To modify the IP address, port information, and memory options afterwards, this file may be manually edited using a text editor such as Notepad.

**Launching the PC client is explained in Launch the Client Using MS Windows on page 47.**

**Java Web Start Client Installation**

Java Web Start provides an alternate method for launching the IP/MPLSView client. One of the major benefits of Web Start is the ability to locally cache the application. It may take a few minutes to download all the necessary files the first time the client is launched. Afterwards all subsequent launches will be instantaneous. Web Start also performs version control, so if there is a new version of the application installed on the server, it will upgrade the client automatically at run-time. In this way, the server and client will always be in sync. Web Start may be installed on both the Solaris and Windows environment.

Informational Note: For Vista users, the installation directory and ipmplsview.bat file is Read-Only by default. To change the permission, navigate to the C:\Program Files\wandl directory, right-click on the installation directory, and select **Properties**. In the **Security** tab, click **Edit**, select the row for **Users** and check that modify are allowed.

Launching the PC client is explained in Launch the Client Using MS Windows on page 47.
Updating the IP/MPLSView Server

When updating IP/MPLSView, it is recommended to install into a new application directory. You may choose an existing data directory to preserve the existing data. Otherwise enter a new data directory to start from scratch.

Updating the IP/MPLSView Client

Please check to make sure that all existing IP/MPLSView client windows are closed before you update the IP/MPLSView client.

For the IP/MPLSView client, the instructions are the same as the first time you installed the IP/MPLSView client. Refer back to IP/MPLSView Client Installation on 21.

Updating the Distributed Database and Traffic Collectors

Update the distributed database using `instdatabase.sh` and the traffic collectors using `install.dcollect` installation scripts.
Chapter 3

Installing Remote Collection Server

The remote collection server is a distributed CLI/SNMP poller which can be used for VLAN auto-discovery and CLI collection. When a task is run from the Task Manager on the central parsing server, the task can be dispatched to the distributed polling server. The final results will be transferred back to the central parsing server.

Informational Note: This feature requires a license. Contact Juniper Support or your sales representative for more information.

Outline

- Prerequisites on page 23
- Installation for Collection Server on page 23
- Installation of Central Parsing Server on page 27

Prerequisites

You should extract the collection server installation files from the CD or FTP onto the machine hosting the remote polling server.

The port 2099 should be open between the application server and the polling server, if there is a firewall in between.

See Chapter 2, Installing IP/MPLSView for more information about the installation process for the application packages.

Installation for Collection Server

The collection server package should be installed on each remote polling server. During the installation of the polling server, the IP address of the central parsing server should be entered. The central parsing server will also be installed, and during the installation of the central parsing server, the IP addresses of the remote polling servers should be entered.

This section discusses how to install the polling server.

1. Login as root user, browse to the jump directory, and install the collection package.
   
   # ./installcollection.sh

2. Enter the user ID. The default is wandl.

3. Enter the group ID. The default is staff.
4. Enter the directory where the jump server files will be installed, for example, /export/home/wandl/collection.

5. Follow the on screen prompts until the configuration setting menu appears.

6. Configuration settings should be set at the prompt to modify entries for the central parsing server.
   - Enter 15 and 17 to add the IP address of the central parsing server.

7. Use default values for the remaining settings.

8. Accept these values and enter ‘y’ to continue installation.

9. Enter ‘y’ to install the Data Collector package.

10. Switch out of root user to the user ID given in step 2. Start the collection server.

   > /u/wandl/bin/startup_collection

Sample Installation

The following sample is the jump server installation run for a first time installation as the root user id. For this sample, 10.0.0.5 is the polling server being installed, and 192.168.1.3 is the application server.

   # ./installcollection.sh

Please read the Getting Started document before installing this software.
Note that you can stop the installation at any time using <Ctrl>-c.

Preparing to install IP/MPLSView ...

We have determined that the Solaris Server Management Facility is running on this machine. If you have configured IP/MPLSView to be managed by this, then please quit the installation and disable the IP/MPLSView entry in the Solaris Server Management Facility before restarting the IP/MPLSView installation. If IP/MPLSView is not configured (or is already disabled) in the Solaris Server Management Facility, then please ignore this message and continue with the installation.

Continue with installation (default=yes)? [y/n]

Checking Sun Solaris patches ...

This software requires a UNIX ID as the owner.
A UNIX ID is the login name when you login to this UNIX server
Please input the IP/MPLSView user ID (wandl):
Owner is set to: wandl

You should have a group created for all the users who will use this program (a group may have only one member, if only one person uses this program)
The installation script will assign the right permissions for the users of this group to use, update and maintain the programs.
Please input group ID (staff):
Group is set to: staff

It is required that you shut down all IP/MPLSView servers before installation
I will try to detect existing running servers and shut them down.
Installing Remote Collection Server

Proceed (default=yes)? [y/n]
Shutdown Task Manager(pid=21939) ...
Shutdown JBoss Collection Server(pid=21921) ...

Please enter the directory where this software will be installed. 
(default=/export/home/wandl/ipmplsview): /export/home/wandl/collection1010

Are you sure you want to install into/export/home/wandl/collection1010 
(default=yes)? [y/n]

Checking available disk space ...

Copying Java native library files...

Switching user to "wandl" ...

Reading configuration settings from /u/wandl/bin/mplsenvsetup.sh ... Done!

General Settings:
1.) Installation Directory.....: /export/home/wandl/collection1010
2.) Admin User..................: wandl
3.) Admin Group................: staff

JBoss Web Settings:
4.) Webserver IP.............: 10.0.0.5
5.) Webserver Port..........: 8091
6.) External Webserver IP:
7.) SSL Port.............: 8443
   SSL Domain........: Unknown
   SSL Department....: Unknown
   SSL Organization.: Unknown
   SSL Loc./City....: Unknown
   SSL State/Prov.: Unknown
   SSL Country.....: United States
8.) JNDI Port.............: 1099
9.) JNDI-RMI Port.........: 1098
10.) JRMP Port...............: 5444
11.) JRMP Invoker Port....: 5446
12.) AJP Port.............: 8009
13.) Classloader Port.....: 8083
14.) JBoss Web Memory.....: 512

JBoss JMS Settings:
15.) JMS IP...................: 192.168.1.3
16.) JMS Port.................: 1856

MySQL Settings:
17.) Database IP.........: 192.168.1.3
18.) Database Port.......: 3333

ask Server Settings:
19.) Task Server Memory....: 512
20.) Task Server Port......: 2099

mail Server Settings:
21.) Email Server IP........:
22.) Email Server Port......: 25
23.) Email Server User.......: wandl
24.) Email Server Password...:

Optional Settings:
25.) Enable Server Monitoring............: ON

Please select a number to modify.
[<CR>=accept, q=quit]:

Accept these values (default=no)? [y/n] y

Install Data Collector (default=yes)? [y/n]

Copying over existing license file.
Extracting server files (this may take some time) ............... Done!

Installing collection server... Done!

Creating symbolic links ... Done!

Installing data collector ...

Configure Data Collectors for Selective Interface (default=no)?[y/n]:

Data collector crontab entries added successfully.

Done!

You may start the Data Collector by running the following commands:
   cd /export/home/wandl/collection1010/dcollect
   ./dc.sh start 0

Successfully created a symbolic link from /u/wandl to
/export/home/wandl/collection1010.

Configuration file: '/export/home/wandl/collection1010/bin/mplsenvsetup.sh' was
created on Mon Oct 10 10:24:13 EDT 2011

Creating JBoss collection server configuration files ... Done!

Creating Diagnostics configuration files ... Done!

Creating Task Manager configuration files ... Done!

Creating Application Monitor configuration files ... Done!

Creating Data Collector configuration files ... Done!

You may start up the IP/MPLSView server by running the following command:
   /export/home/wandl/collection1010/bin/startup_collection

# exit
   > /export/home/wandl/collection1010/bin/startup_collection

Purging temporary files... done!

Detecting existing servers
JBoss Collection Server started
Starting Task Server
Task Server started

If you are running data collection, please start data collectors manually

Note: The various servers have been started but may take a few
minutes (depending on processor, memory and disk speed) to finish
Installing Remote Collection Server

Installation of Central Parsing Server

During the installation of the central parsing server, or central application server, use option (H) Advanced Configuration:

Main Menu
Server Configuration Settings:
(A) Overall Settings
(B) IP Address
(C) Memory Settings
(D) Port Settings (Server to Client)
(E) Port Settings (Advanced)
(F) Online Performance Management Settings
(G) Online Fault Management Settings
(H) Advanced Configuration

Next, select option 4.) Distributed Collection Servers to enter in the remote polling servers via a comma separated list of IP_address:port, using 2099 as the port.

(H) Advanced Configuration
Advanced Configuration Settings:
1.) Enable NAT access for JMS.............: OFF
2.) External Webserver IP (for NAT)........:
3.) Enable Jump Server....................: OFF
4.) Distributed Collection Servers........: 10.0.0.5:2099,10.0.0.6:2099

After installation, this list of polling servers can be changed by option (H) Advanced Configuration of the /u/wandl/bin/changeconfig.sh script.

After running this script to change the polling server list, it is necessary to stop and restart the central parsing server. This can be done running /u/wandl/bin/stop_mplsview followed by /u/wandl/bin/startup_mplsview.

their deployment. Please wait a few minutes and then run
/export/home/wandl/collection1010/bin/status_jump
to determine the deployment status.
Chapter 4

Installing Jump Server

The jump server is an agent that will relay requests for CLI, SNMP polling, and forward traps to the application server for processing by IP/MPLSView. This chapter will cover installation of the jump server package and walk-through a sample environment where the jump server may be used.

When To Use the Jump Server

The jump server package can be used to reach the network you are monitoring with IP/MPLSView when it cannot be accessed directly by the application server or data collector server. This situation may arise when the application server on your internal network is separated by a firewall from the network being monitored. The figure below illustrates this scenario.

![Figure 3: Sample Environment using Jump Server](image)

Outline

- Prerequisites on page 30
- Installation for Jump Server on page 30
- Sample Environment Using Jump Server on page 34
Prerequisites

See Chapter 2, Installing IP/MPLSView for more information about the installation process for the application, database, and data collector packages.

Before installing the jump server package, gateway routes should be added on the machines hosting the application server and jump server. The application server should add a route to the jump server external network and data collector if you use traffic collection. The jump server, and data collector server if applicable, should add a route to the application server network.

If there is a firewall separating the jump server and application server, verify that both servers can reach each other on the required ports specified in Firewall Setup on page 38. You can use “telnet x.x.x.x port_number” to check if the NAT is working fine on the firewall for every port.

You should extract the jump package installation files from the CD or FTP onto the machine hosting the jump server.

Installation for Jump Server

1. Log in as root user, browse to the jump directory, and install the jump package.
   
   # ./installjump.sh

2. Enter the user ID. The default is wandl.

3. Enter the group ID. The default is staff.

4. Enter the directory where the jump server files will be installed. The default is /export/home/wandl/ipmplsview.

5. Follow the on screen prompts until the configuration setting menu appears.

6. Configuration settings should be set at the prompt to modify entries for the application server and data collector server.
   
   - Enter 21 to modify the JBoss JMS Settings for the JMS IP. Then enter the IP address of your application server. By default the JMS IP is set to the local machine IP, so it is important to set this to the application IP.
   
   - Enter 25 to modify the SNMP Trap Forwarder Settings and set Enable Trap Forwarder to ON.
   
   - Enter 26 to modify the SNMP Trap Forwarder Settings for the Upstream Address. Then enter the IP address of the application server.
   
   - Enter 27 to modify the SNMP Trap Forwarder Settings for the Upstream Port. Then enter 162 for the port.

7. Use default values for the remaining settings.

8. Accept these values and enter ‘y’ to continue installation.

9. Enter ‘y’ to install the Data Collector package.

10. Start the jump server.

   > /u/wandl/bin/startup_jump
Sample Installation

The following sample is the jump server installation run for a first time installation as the root user id. For this sample:

- Application server IP is 1.1.1.1
- Jump server IP is 2.2.2.2

Please read the Getting Started document before installing this software. Note that you can stop the installation at any time using <Ctrl>-c.

Preparing to install IP/MPLSView ...

We have determined that the Solaris Server Management Facility is running on this machine. If you have configured IP/MPLSView to be managed by this, then please quit the installation and disable the IP/MPLSView entry in the Solaris Server Management Facility before restarting the IP/MPLSView installation. If IP/MPLSView is not configured (or is already disabled) in the Solaris Server Management Facility, then please ignore this message and continue with the installation.

Continue with installation (default=yes)? [y/n]

Checking Sun Solaris patches ...

This software requires a UNIX ID as the owner. A UNIX ID is the login name when you login to this UNIX server to input the IP/MPLSView user ID (wandl):

Owner is set to: wandl

You should have a group created for all the users who will use this program (a group may have only one member, if only one person uses this program). The installation script will assign the right permissions for the users of this group to use, update and maintain the programs. Please input group ID (staff):

Group is set to: staff

It is required that you shut down all IP/MPLSView servers before installation. I will try to detect existing running servers and shut them down.

Proceed (default=yes)? [y/n]

Please enter the directory where this software will be installed.

(default=/export/home/wandl/ipmplsview):

Are you sure you want to install into /export/home/wandl/ipmplsview (default=yes)? [y/n]

Checking available disk space ...

Copying Java native library files...
Switching user to "wandl" ...

Reading configuration settings from
/export/home/wandl/ipmplsview/bin/mplsenvsetup.sh ... Done!
General Settings:
1.) Installation Directory.....: /export/home/wandl/ipmplsview
2.) Admin User................: wandl
3.) Admin Group...............: staff
4.) Server IP...............: 2.2.2.2
5.) Server Port...........: 7000
6.) SNMP Trap Daemon IP.......: 2.2.2.2
7.) SNMP Trap Daemon Port.....: 162
8.) SNMP Trap Daemon Memory...: 128
9.) SNMP Trap Store Capacity...: 30

JBoss Web Settings:
10.) Webserver IP.........: 2.2.2.2
11.) Webserver Port.......: 8091
12.) External Webserver IP:
13.) SSL Port........: 8443
    SSL Domain.......: Unknown
    SSL Department..: Unknown
    SSL Organization: Unknown
    SSL Loc./City...: Unknown
    SSL State/Prov.: Unknown
    SSL Country.....: United States,us
14.) JNDI Port............: 1099
15.) JNDI-RMI Port.........: 1098
16.) JRMP Port............: 5444
17.) JRMP Invoker Port....: 5446
18.) AJP Port.............: 8009
19.) Classloader Port.....: 8083
20.) JBoss Web Memory.....: 256

JBoss JMS Settings:
21.) JMS IP..................: 1.1.1.1
22.) JMS Port................: 1856

MySQL Settings:
23.) Database IP.........: 2.2.2.2
24.) Database Port.......: 3333

SNMP Trap Forwarder Settings:
25.) Enable Trap Forwarder...............: ON
26.) Upstream Address....................: 1.1.1.1
27.) Upstream Port.......................: 162

Please select a number to modify.
[<CR>=accept, q=quit]: 21
21 selected!

Current JMS IP IP Address: 2.2.2.2

Please enter a new JMS IP IP Address: 1.1.1.1

Please select a number to modify.
[<CR>=accept, q=quit]: 25

Please select a number to modify.
[<CR>=accept, q=quit]: 26
26 selected!

Current IP Address: SNMP Upstream
Please enter a new IP Address: 1.1.1.1

Please select a number to modify.
[<CR>=accept, q=quit]: 27
27 selected!

Current Port: SNMP Upstream

Please enter a new Port: 162

Please select a number to modify.
[<CR>=accept, q=quit]:

Accept these values (default=no)? [y/n] y

Install Data Collector (default=yes)? [y/n] y
crontab added successfully.

Done!

You may start the Data Collector by running the following commands:
cd /export/home/wandl/ipmplsview/dcollect
./dc.sh start 0

Successfully created a symbolic link from /u/wandl to
/export/home/wandl/ipmplsview.

Configuration file: '/export/home/wandl/ipmplsview/bin/mplsenvsetup.sh' was created on Fri Jun 25 18:19:12 EDT 2010

Creating Jumpserver configuration files ... Done!

Creating Snmptrap configuration files ... Done!

Creating Data Collector configuration files ... Done!

You may start the SNMP Trap Listener by running the following command:
/export/home/wandl/ipmplsview/bin/.snmptrap start

You may start up the IP/MPLSView server by running the following command:
/export/home/wandl/ipmplsview/bin/startup_jump

Start up the IP/MPLSView server (default=yes)? [y/n] y

Purging temporary files... done!

Detecting existing servers
Removing Aggregation crontask...
Aggregation crontask removed
Removing Bulk stat interface traffic generation crontask...
Bulk stat interface traffic generation crontask removed
WANDL_HOME=/export/home/wandl/ipmplsview
NPAT Server started on port 7000
Jboss Jump started
If you are running data collection, please start data collectors manually
Would you like to start the SNMP Trap Server (default=yes)? [y/n] y
Starting SNMP Trap Server
SNMP Trap Server started

Note: The various servers have been started but may take a few
minutes (depending on processor, memory and disk speed) to finish
their deployment. Please wait a few minutes and then run
/export/home/wandl/ipmplsview/bin/status_jump
to determine the deployment status.

#

**Sample Environment Using Jump Server**

The following section describes a sample environment where the jump server package
may be used and the setup instructions to start IP/MPLSView. The sample environment
has two network areas. One area is the internal network where the application and
distributed database servers are located. The second area is the external network behind a
firewall NAT where the routers being monitored are located. To use IP/MPLSView and
collect data traffic on the external network from the internal network, the jump server and
data collector package are installed on machines in the external network. See Figure 4 for
the IP addresses used in this walk-through.

To use the jump server package, configuration settings will need to be modified on the
application server, database server, data collector server, jump server, and firewall.

- Distributed Database Server Setup on page 35
- Application Server Setup on page 35
- Jumper Server Setup on page 36
- Data Collector Server Setup on page 37
- Firewall Setup on page 38
Distributed Database Server Setup

1. To use the distributed database, it is required to setup the database server prior to setup of the application server. Otherwise, if the database package is installed on the same server together with the application package, then you may skip this section and move onto the Application Server Setup.

2. Login as wandl user, and stop IP/MPLSView on the database server.
   
   ```
   > /u/wandl/bin/stop_mplsview
   ```

3. Switch to root user, browse to the server directory, and install the database package.
   
   ```
   # ./instdatabase.sh
   ```

4. Use the default values during the database installation process.

5. Start IP/MPLSView on the database server.
   
   ```
   > /u/wandl/bin/startup_mplsview
   ```

Application Server Setup

1. Login as root user and add a gateway route to the external network through the internal network firewall using the "route add" command.

   ```
   # route add 2.0.0.0/8 1.1.1.9
   ```

2. Switch to wandl user, and stop IP/MPLSView on the application server.

   ```
   > /u/wandl/bin/stop_mplsview
   ```
3. Switch to root user, browse to the server directory, and install the application package.

   # ./install.sh

4. Follow the on screen prompts until the configuration setting menu appears.

5. Configuration settings should be set at the prompt to modify entries for the database server and jumper server.
   - Enter 38 to modify the MySQL Settings for the Distributed Database. Then enter the IP address of your database server. If the database is installed on the same server as the application, then you may skip this step.
   - Enter 70 to modify the Advance Options and set Enable Jump Server to ON.

6. Use default values for the remaining settings.

7. Accept these values and enter ‘y’ to continue installation.

8. Enter ‘y’ to install the Client and Data Collector packages.

9. Installation of the Rsync & Database Replication package is optional.

10. Start IP/MPLSView on the application server.

   > /u/wandl/bin/startup_mplsview

11. Start an IP/MPLSView client.

12. Open the Router Profile by selecting **Application > Task Manager** and clicking **Router Profile**.

13. Every router being monitored will need its Router Profile Entry updated for the Agent field. Select the router, click Modify, and enter the jump server IP address in the Agent(s) field. Note you may select multiple routers to modify at once by pressing Ctrl-a, shift-click, or Ctrl-click in the router profile list.

![Figure 5: Router Profile Entry](image)

**Jumper Server Setup**

1. Login as root user and add a gateway route to the internal network through the external network firewall using the “route add” command.
Installing Jump Server

2. As root user, browse to the jump directory, and install the jump package.
   \# ./installjump.sh

3. Enter the user ID. The default is wandl.

4. Enter the group ID. The default is staff.

5. Enter the directory where the jump server files will be installed. The default is /export/home/wandl/ipmplsview.

6. Follow the on screen prompts until the configuration setting menu appears.

7. Configuration settings should be set at the prompt to modify entries for the application server and data collector server.
   - Enter 21 to modify the JBoss JMS Settings for the JMS IP. Then enter the IP address of your application server. By default the JMS IP is set to the local machine IP, so it is important to set this to the application IP.
   - Enter 25 to modify the SNMP Trap Forwarder Settings and set Enable Trap Forwarder to ON.
   - Enter 26 to modify the SNMP Trap Forwarder Settings for the Upstream Address. Then enter the IP address of the application server.
   - Enter 27 to modify the SNMP Trap Forwarder Settings for the Upstream Port. Then enter 162 for the port.

8. Use default values for the remaining settings.

9. Accept these values and enter ‘y’ to continue installation.

10. Enter ‘y’ to install the Data Collector package.

11. Start the jump server.
    \> /u/wandl/bin/startup_jump

Data Collector Server Setup

1. Login as root user and add a gateway route to the internal network through the external network firewall using the “route add” command.
   \# route add 1.0.0.0/8 2.2.2.9

2. Switch to wandl user, and stop any existing data collectors on the data collector server.
    \> /u/wandl/dcollect/dc.sh stop all

3. As the wandl user, browse to the dcollect directory, and install the data collector package.
    \> ./install.dcollect

4. At the prompt enter the IP address of the application server.
    Please supply the name or IP address of the JMS server

5. Use default values for the remaining settings.

6. Start a data collector instance on the data collector server.
    \> ./dc.sh start 1
Firewall Setup

In the sample environment, a firewall separates the jump server and data collector server located in the external network from the application server located in the internal network. Based on the NAT configuration, the firewall will translate requested destinations on the external interface IP and external interface ports to the internal server IP and internal server ports. The following rules, protocols, and ports need to be set, enabled, and opened on the firewall:

LAN Rules

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Application IP</td>
<td>*</td>
<td>Jump/DcollectIP</td>
<td>*</td>
</tr>
</tbody>
</table>

Wan Rules

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP</td>
<td>Jump IP</td>
<td>*</td>
<td>Application IP</td>
<td>162</td>
</tr>
<tr>
<td>TCP</td>
<td>Jump/Dcollect IP</td>
<td>*</td>
<td>Application IP</td>
<td>1856</td>
</tr>
<tr>
<td>TCP</td>
<td>Jump/Dcollect IP</td>
<td>*</td>
<td>Application IP</td>
<td>4457-4459</td>
</tr>
<tr>
<td>TCP</td>
<td>Jump/Dcollect IP</td>
<td>*</td>
<td>Application IP</td>
<td>4444</td>
</tr>
<tr>
<td>TCP</td>
<td>Jump/Dcollect IP</td>
<td>*</td>
<td>Application IP</td>
<td>1098</td>
</tr>
<tr>
<td>TCP</td>
<td>Jump/Dcollect IP</td>
<td>*</td>
<td>Application IP</td>
<td>1099</td>
</tr>
<tr>
<td>TCP</td>
<td>Jump/Dcollect IP</td>
<td>*</td>
<td>Application IP</td>
<td>21101</td>
</tr>
<tr>
<td>TCP</td>
<td>Jump/Dcollect IP</td>
<td>*</td>
<td>Application IP</td>
<td>3873</td>
</tr>
<tr>
<td>TCP</td>
<td>Jump/Dcollect IP</td>
<td>*</td>
<td>Application IP</td>
<td>1101</td>
</tr>
</tbody>
</table>

WAN Inbound NAT

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Usage</th>
<th>External Port</th>
<th>NAT IP</th>
<th>Internal Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP</td>
<td>Traffic</td>
<td>162</td>
<td>Application IP</td>
<td>162</td>
</tr>
<tr>
<td>TCP</td>
<td>JMS</td>
<td>1856</td>
<td>Application IP</td>
<td>1856</td>
</tr>
<tr>
<td>TCP</td>
<td>JMS</td>
<td>4457</td>
<td>Application IP</td>
<td>4457</td>
</tr>
<tr>
<td>TCP</td>
<td>JMS</td>
<td>4458</td>
<td>Application IP</td>
<td>4458</td>
</tr>
<tr>
<td>TCP</td>
<td>JMS admin</td>
<td>4444</td>
<td>Application IP</td>
<td>4444</td>
</tr>
<tr>
<td>TCP</td>
<td>Jump server</td>
<td>1098</td>
<td>Application IP</td>
<td>1098</td>
</tr>
<tr>
<td>TCP</td>
<td>Jump server</td>
<td>1099</td>
<td>Application IP</td>
<td>1099</td>
</tr>
<tr>
<td>TCP</td>
<td>HTTP invoker</td>
<td>21101</td>
<td>Application IP</td>
<td>21101</td>
</tr>
<tr>
<td>TCP</td>
<td>Jump server</td>
<td>3873</td>
<td>Application IP</td>
<td>3873</td>
</tr>
<tr>
<td>TCP</td>
<td>HTTP invoker</td>
<td>1101</td>
<td>Application IP</td>
<td>1101</td>
</tr>
</tbody>
</table>
Verification

IP/MPLSView is ready to monitor the external network and collect data in this sample environment after the four packages and firewall have been setup. Verify this by opening the live network and run traffic collection.
Chapter 5

Installing Viewserver

Viewserver compliments the Application server by featuring a streamlined client designed for network operators and planners. Only network administrators would need to use the full capabilities of the client from the application server. This enhances overall system performance by off loading users and system resources from the application server in a distributed server environment. Thus, Viewserver supports scalability for a large number of users.

When to Use

It's recommended to use Viewserver if you plan to have more than three concurrent client sessions open or if you have more than ten users. If there are too many concurrent Application Client users, this may effect user performance because the Application Client includes administrative and collection tools which requires more system resources than the Viewserver Client. The Viewserver Client uses less system resources and has all the capabilities needed for network operators and planners. The Application Client has additional capabilities needed only for network administrators.

Viewserver Client

Viewserver client has the following features. Modules available are dependent on your user license.

- Topology Map
- Report Manager
- Configuration Management
  - Network Health
  - Device Inventory
  - MIB Browser
  - Configuration Conformance
- Fault Management
  - Event Browser
  - Historical Event Browser
  - Event Map
- Performance Management
  - Network Dashboard
  - View live traffic, CPU, memory, temperature
  - Network Performance Report
• Design & Plan
   Backbone Design
   MPLS-TE
   T-Solve
   Simulation

Application Client

Application client has the same features as Viewserver client and additional features below. Modules available are dependent on your user license.

• Task Manager collection tasks
• Traffic Collection Manager
• Modify mode
• Run CLI Update Live
• Threshold Crossing Alert
• Subscription Editor
• Trap editing
• Hardware Inventory collection
• Provisioning
• OS/Config Manager
• Hardware Vendor Type Manager
• Device Change Tracking
• Save to .network directory
• Save to Web
• User Administration

Outline

• Prerequisites on page 43
• Requirements on page 43
• Installation on page 43
• Configuration on page 45
• User Account Setup on page 46
• Startup Viewserver on page 46
• Stop Viewserver on page 47
• Launch Viewserver Client on page 47
• Commands and Paths on page 48
• Environmental Variables on page 48
Prerequisites

See Chapter 2, Installing IP/MPLSView for more information about the installation process for the application and database packages.

Before installing the Viewserver package, you should verify that existing servers for application, database, and data collectors are running properly.

You should extract the Viewserver package installation files from the CD or FTP onto the machine hosting the Viewserver.

The Viewserver installation package requires a license. Please contact your Juniper representative for more information.

Requirements

The following are requirements for Viewserver installation and usage:

- The Application server and Viewserver must use the same system platform. Example, AMD64-AMD64 or SPARC-SPARC are compatible. AMD32-AMD64 or AMD-SPARC are not compatible.
- npatpw password file in directory /u/wandl/db/sys/ is required for each Viewserver machine.
- Create the Remote Data Directory before installation as wandl user. Remote Data Directory must use the same name as Application Data Directory.
- Configuration Settings:
  - IP Address
  - LDAP Server IP = Application server IP
  - Distributed Database = Yes
  - Local Database IP = Viewserver IP
  - Distributed Database IP = Application or Database server IP
  - Viewserver user accounts must be created on both Application server and Viewserver.

Installation

This section will guide you through installation of Viewserver. It's recommended to write down the IP address and directories of your distributed server environment. The table below will be used as an example in this guide.

<table>
<thead>
<tr>
<th>Server</th>
<th>IP Address</th>
<th>Description</th>
<th>Directory</th>
<th>Environmental Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Server</td>
<td>1.1.1.1</td>
<td>application install directory</td>
<td>/export/home/wandl/ipmplsview</td>
<td>-</td>
</tr>
<tr>
<td>Application Server</td>
<td>1.1.1.1</td>
<td>application data directory</td>
<td>/export/home/wandl/wandldata</td>
<td>-</td>
</tr>
<tr>
<td>Viewserver</td>
<td>2.2.2.2</td>
<td>viewserver install directory</td>
<td>/export/home/wandl/viewserver</td>
<td>-</td>
</tr>
<tr>
<td>Viewserver</td>
<td>2.2.2.2</td>
<td>viewserver data directory</td>
<td>/export/home/wandl/viewdata</td>
<td>LOCAL_DATA_DIR</td>
</tr>
<tr>
<td>Viewserver</td>
<td>2.2.2.2</td>
<td>remote data directory</td>
<td>/export/home/wandl/wandldata</td>
<td>REMOTE_DATA_DIR</td>
</tr>
</tbody>
</table>
Informational Note: The remote data directory requires the same name as the application data directory.

Note: The remote data directory requires the same name as the application data directory.

1. Copy and extract the Viewserver installation packages to a temporary installation directory on the Viewserver.

2. As wandl user create the remote data directory. It must be the same name as the application data directory.
   
   ```
   mkdir /export/home/wandl/wandldata
   ```

3. As root user run the installation script from the temporary installation directory.
   
   ```
   ./inst_viewerserver.sh
   ```

4. At prompt input the View Server user ID, recommend using default wandl

5. At prompt input group ID, recommended using default staff

6. At prompt enter the directory where this software will be installed, recommend using /export/home/wandl/viewserver

7. At prompt enter the directory where the data will be stored, recommend using /export/home/wandl/viewdata

8. At Main Menu, select IP Address.
   - Set LDAP Server IP to the Application server IP.
   - Set Distributed Database to YES
   - Set Distributed Database IP to the Application server IP. If the Application and Database are on distributed servers, then set this to the Database server IP.

(B) IP Address

IP/MPLSView Server IP Address Settings:

1.) View Server IP.....................: 2.2.2.2
2.) Webserver IP......................: 2.2.2.2
3.) LDAP Server IP.....................: 1.1.1.1
4.) External Webserver IP (for NAT)....:
5.) Local Database IP..................: 2.2.2.2
6.) Distributed Database...............: YES
   Distributed Database IP..............: 1.1.1.1
   Database Port.......................: 3333
7.) Email Server IP....................:

99.) Change All IP Addresses for 1, 2, 3, 5

9. Only the IP Address settings need to be changed for Viewserver setup. You may review the other options in the Main Menu. Accept these values when ready.

10. The following are OPTIONAL prompts if the installation packages are detected:
Installing Viewserver

- At prompt to Install Client, if you want to use the Solaris Client enter y to install, otherwise enter n
- At prompt to Install Data Collector, if you want to use the Data Collector on the Viewserver enter y to install, otherwise enter n
- At prompt to Install Rsync & Replication, if you want to use Rsync and Replication features enter y to install, otherwise enter n

11. At prompt copy files from the old installation to the new installation, select the options you want to copy over.
12. At prompt enter the mount point of the remote data directory, use the remote data directory /export/home/wandl/wandldata

**Informational Note:** The remote data directory must be created before running the installation script.

13. At prompt enter the IP address of application server, use the application server IP.
14. At prompt give JAVA Applets write permission, enter y to allow saving Java charts and trending reports from the Web or enter n to skip.
15. At prompt to startup View server, enter y to start or enter n to skip and start at a later time.

Before launching a client session, see the sections on Configuration on page 45 and User Account Setup on page 46 to configure Viewserver for file sharing.

**Configuration**

The shared user data directory on the application server should be shared as read-only to Viewserver. Also, symbolic links should be created for the Task Manager profile directory and .diag file. This configuration is required view the Live Network and be in sync with shared user data.

1. Log in to the application server.
2. Locate the absolute data directory path.

   ```bash
   ls -l /u/wandl/data
   lrwxrwxrwx 1 wandl staff 31 Jun 23 10:46 /u/wandl/data -> /export/home/wandl/wandldata
   ```

3. As root user share the application data directory as read-only to Viewserver (client machine).

   ```bash
   share -F nfs -o ro=2.2.2.2 /export/home/wandl/wandldata
   ```

4. Log in to Viewserver.
5. As root user mount the remote data directory using the shared path. In the Requirements section, the remote data directory was created as wandl user and uses the same name as the application data directory.

   ```bash
   mount 1.1.1.1:/export/home/wandl/wandldata /export/home/wandl/wandldata
   ```
6. As wandl user create symbolic links from the local data directory to the remote data directory for the Task Manager profile directory and .diag file to support proper SNMP, Diagnostics, Run CLI, and RCA functionality.

```bash
cd /export/home/wandl/viewdata/.TaskManager
ln -s /export/home/wandl/wandldata/.TaskManager/profile profile
ln -s /export/home/wandl/wandldata/.TaskManager/tmp/.diag tmp/.diag
```

### User Account Setup

Viewserver users need accounts created on both Application server and Viewserver. Then the administrator on the application server can set user permissions from the User Admin module. The user account on the application server is used to manage permissions and regional views. The user account on the Viewserver is for Web and Client access and user data storage.

1. As root user add user accounts on both the Application server and Viewserver. Then set the password. The user password does not have to be the same on both servers. When logging in to the Viewserver Web or Viewserver Client, the password prompt uses the password set on Viewserver. Command below creates new user called viewuser in group staff, creates and sets her home directory to /export/home/viewuser, and sets her profile to use bash shell.

```bash
useradd -g staff -d /export/home/viewuser -m -s /bin/bash viewuser
passwd viewuser
```

2. Repeat step 1 for each additional user.

3. As wandl user login to the Application Client.

4. Use Admin > User Administration to manage the permissions and regions of the Viewserver users.

### Startup Viewserver

The following list briefly summarizes the process to start using Viewserver:

- **Requirements**
  1. Create the Remote Data Directory before installation as wandl user. Remote Data Directory must use the same name as Application Data Directory.

- **Installation**
  2. As root user run the installation script from the temporary installation directory.
  3. During installation at the Main Menu prompt, enter the IP Address settings and change LDAP IP, set Distributed Database YES, and enter Distributed Database IP.

- **Configuration**
  4. Share the Application server application data directory.
  5. Mount the Viewserver remote data directory.
  6. Create symbolic links from the Viewserver local data directory to remote data directory in the .TaskManager path.

- **User Account Setup**
7. Create Viewserver user accounts on both Application server and Viewserver.
8. Manage Viewserver user permissions through the Application Client.

As wandl user, start up Viewserver using the command

```
/u/wandl/bin/startup_viewerserver
```

**Stop Viewserver**

Stopping Viewserver will send a warning message to all clients stating the server will shut down in 1 minute. As wandl user stop Viewserver using the command

```
/u/wandl/bin/stop_viewerserver
```

**Launch Viewserver Client**

Once Viewserver is running, you can launch the Viewserver client using Webstart or a desktop client.

**Launching the Client Using Webstart**

1. Open a web browser and enter the Viewserver's IP address on port 8091.
   `viewserver_ip:8091`
2. Log in to the Web using the user credentials setup on the Viewserver
3. Click Webclient
4. Click IP/MPLSView
5. Log in to the Client using the user credentials setup on the Viewserver

**Launch the Client Using MS Windows**

1. Install the client using the following IP settings:
   - IP/MPLSView IP Address is the Viewserver IP. SERVER
   - Web Server Address is the Viewserver IP. WEBSERVER
   - LDAP IP Address is the Application IP. LDAPSERVER
2. If the client is already installed, right-click edit the IP/MPLSView Client icon or `ipmplsview.bat` file to edit the IP settings:

   ```
   SET SERVER=2.2.2.2
   SET SERVERPORT=7000
   SET WEBSERVER=2.2.2.2
   SET WEBSERVERPORT=8091
   SET LDAPSERVER=1.1.1.1
   SET LDAPPORT=3389
   SET MEMORY=256MB
   ```
3. Double-click the IP/MPLSView Client icon or `ipmplsview.bat` file.
4. Login to the Client using the user credentials setup on the Viewserver.
Commands and Paths

Viewserver

- directory: /u/wandl/bin
- start server command: /u/wandl/bin/startup_viewerserver
- stop server command: /u/wandl/bin/stop_viewerserver
- status server command: /u/wandl/bin/status_viewerserver
- install directory: /export/home/wandl/viewserver
- local data directory: /export/home/wandl/viewdata
- remote data directory: /export/home/wandl/wandldata
- mount command: mount application_server_IP:/app_data_dir /remote_data_dir
- link profile command: ln -s remote_data_dir/.TaskManager/profile local_data_dir/.TaskManager/profile
- link .diag command: ln -s remote_data_dir/.TaskManager/tmp/.diag local_data_dir/.TaskManager/tmp/.diag

Application Server

- directory: /u/wandl/bin
- application data directory: /export/home/wandl/wandldata
- share command: share -F nfs -o ro=viewserver_IP /app_data_dir

Environmental Variables

The following variables were introduced for Viewserver implementation. These values are set in /u/wandl/bin/mqlsenvsetup.sh during installation or by running /u/wandl/bin/changeconfig.sh command. Do not manually edit these values. The information provided is for reference.

VIEW_ONLY=0; export VIEW_ONLY
LOCAL_DATA_DIR=/export/home/wandl/viewdata ; export LOCAL_DATA_DIR
VIEW_SERVER_APPIP=1.1.1.1; export VIEW_SERVER_APPIP
REMOTE_DATA_DIR=/export/home/wandl/wandldata ; export REMOTE_DATA_DIR
Chapter 6

Installing Report Server

The report server is a standalone Task Manager and Web server for network data report generation and viewing. These functions are identical to those on the application server used by IP/MPLSView. The report server is used specifically to run those report tasks to alleviate the application server’s resources. This chapter will cover installation of the report server package and walk through a sample environment where the report server may be used.

When To Use

The report server package can be used to improve performance of the application server by off loading Task Manager and reporting processes from the application server to the report server. This situation may arise when the network being monitored is very large and processing for IP/MPLSView needs to be distributed. The figure below illustrates a typical distributed setup for a primary and backup site.

![Figure 6: Distributed Set-up with Report Server](image-url)
Outline

- Prerequisites on page 50
- Installation for Report Server on page 50
- User Administration for Report Server on page 58

Prerequisites

See Chapter 2, Installing IP/MPLSView for more information about the installation process for the application and database packages.

Before installing the report server package, you should verify that existing servers for application, database, and backups are running properly.

You should extract both report package and application package installation files from the CD or FTP onto the machine hosting the report server.

The report server installation package requires a license. Please contact your Juniper representative for more information.

Installation for Report Server

1. Login as root user, browse to the report directory, and install the report package.
   
   # ./inst_reportserver.sh

2. The installation script will display a message for recommended settings that should be configured on the report server. Parameters should be set for the Task Manager, distributed database, email notification, and LDAP server at the configuration setting menu.

3. The installation script calls upon the application package install.sh script and installs only the functions needed by the report server. Enter the directory where the install.sh file is located.

4. Follow the same steps as you would when installing the primary application package until you reach the configuration setting menu.

5. Configuration settings should be set at the prompt to modify these entries.
   - Enter 7 to modify the General Settings for the Task Manager Memory. Enter the memory size in MB. A recommended guide line would be to set the value at 60%-80% of the physical memory which can be viewed using the "prtconf" command. By default 256 MB of memory is set so it is important to allocate sufficient memory.
   - Enter 52 to modify the LDAP Server settings. Enter the application server IP. By default the LDAP server IP is the local machine so it is important to set this to the application server.

6. The following configuration settings are optional and should be modified if the distributed database and/or email notification is used in your setup.
   - Enter 38 to modify the MySQL Settings and set Distributed Database to YES. Enter the distributed database IP. Enter ‘3333’ for the database port.
   - Enter 39 to modify the Email Settings for the Email Server IP. Enter the email IP.
   - Enter 40 to modify the Email Settings for the User. Enter the email username.
Installing Report Server

- Enter 41 to modify the Email Settings for the Password. Enter the email password.
7. Use default values for the remaining settings.
8. Accept these values and enter ‘y’ to continue installation.
9. Enter ‘n’ when prompted to install the Client.
10. Enter ‘n’ when prompted to install the Data Collector.
11. Enter ‘n’ when prompted to install the Rsync & Database Replication Package.
12. At the Copy files menu prompt, enter ‘1’ and ‘y’ to toggle all fields to YES. Then accept the values and continue.
13. Enter ‘y’ when prompted to give JAVA Applets write-permission.
14. Enter ‘n’ when prompted to start IP/MPLSView server.
15. At the post-installation procedures, press enter to use the default directory /u/wandl. A symbolic link is created from /u/wandl to the report server directory you specified at the beginning of installation.
16. The installation will detect the processor of the system. For systems using 64-bit processors, more than 2GB of memory can be allocated. For CPU's with multiple cores, parallel garbage collection can be used. Both options are to enhance performance. Enter ‘y’ or ‘n’ to enable these options.
17. Once the installation is successful, enter ‘n’ when prompted to start the standalone server.
18. Before starting the report server, the following directory and file should be copied from the application server to the report server.
   - /u/wandl/data/.TaskManager/tmp
   - /u/wandl/data/.TaskManager/task.store
19. Verify that the npatpw license file provided by your Juniper representative has been copied to /u/wandl/db/sys/ on the report server.
20. Switch to wandl user and start report server.
   > /u/wandl/bin/startup_reportserver
21. Check the status of the report server and verify there are no warnings or errors.
   /u/wandl/bin/status_reportserver
22. Verify WebStart client to the report server by opening a web browser to the report server IP. Click on Web Client to open the WebStart pop-up screen. Enter the application server IP in the LDAP Server IP Address field. Press Run IP/MPLSView to start the client.

Sample Installation

The following sample is the report server installation run for a first time installation as the root user id. For this sample:
- Application server IP is 1.1.1.1
- Distributed database server IP is 3.3.3.3
- Report server IP is 4.4.4.4

This script will install standalone Task Manager and web server for network data report generation and viewing, do you wish to continue? (default=no)? [y/n] y
Please set the following parameters for the standalone server:

1. Task Manager Memory setting (option 7)
2. YES for Distributed Database (option 38)
3. SMTP server for E-mail notification (options 39-41)
4. LDAP server for web login (option 52-53)

Press ENTER to continue installation:
Please enter the directory where IP-MPLSView install.sh is located.
: /installation_directory/server
Please read the Getting Started document before installing this software.
Note that you can stop the installation at any time using <Ctrl>-c.

Which version would you like to install?
  1) 32-bit
  2) 64-bit
(1:32-bit(default) 2:64-bit): 1

Preparing to install IP/MPLSView ...

We have determined that the Solaris Server Management Facility is running on this machine. If you have configured IP/MPLSView to be managed by this, then please quit the installation and disable the IP/MPLSView entry in the Solaris Server Management Facility before restarting the IP/MPLSView installation. If IP/MPLSView is not configured (or is already disabled) in the Solaris Server Management Facility, then please ignore this message and continue with the installation.

Continue with installation (default=yes)? [y/n] y

Checking Sun Solaris patches ...

This software requires a UNIX ID as the owner.
A UNIX ID is the login name when you login to this UNIX server
Please input the IP/MPLSView user ID (wandl):
Owner is set to: wandl

You should have a group created for all the users who will use this program (a group may have only one member, if only one person uses this program)
The installation script will assign the right permissions for the users of this group to use, update and maintain the programs.
Please input group ID (staff):
Group is set to: staff

It is required that you shut down all IP/MPLSView servers before installation.
I will try to detect existing running servers and shut them down.

Proceed (default=yes)? [y/n] y
Please enter the directory where this software will be installed.
(default=/export/home/wandl/ipmplsview): /export/home/wandl/report

Are you sure you want to install into /export/home/wandl/report (default=yes)? [y/n] y

Checking available disk space ...
Please enter the directory where the data will be stored.
(default=/export/home/wandl/wandldata): /export/home/wandl/reportdata

Warning: You have selected a data directory other than the existing /export/home/wandl/wandldata.
Are you sure you want to install into /export/home/wandl/reportdata
(default=yes)? [y/n] y

Would you like to copy the contents of /u/wandl/data to the new data directory?
(default=no) [y/n]  n

Copying Java native library files...
An identical file has been detected, do you wish to overwrite it? [no] n

Skipped copying Java native library files...

Switching user to "wandl"

Reading configuration settings from /u/wandl/bin/mplsenvsetup.sh ... Done!

General Settings:
1.) Installation Directory.....: /export/home/wandl/report
2.) Data Directory.............: /export/home/wandl/reportdata
3.) Admin User.................: wandl
4.) Admin Group...............: staff
5.) Task Manager Primary Port.: 2099
6.) Task Manager Secondary Port: 2100
7.) Task Manager Memory.......: 2048
8.) Server IP..................: 4.4.4.4
9.) Server Port................: 7000
10.) SNMP Trap Daemon IP.......: 4.4.4.4
11.) SNMP Trap Daemon Port.....: 162
12.) SNMP Trap Daemon Memory...: 128
13.) SNMP Trap Store Capacity..: 30
14.) DGS Memory...............: 256

JBoss Web Settings:
15.) Webserver IP.........: 4.4.4.4
16.) Webserver Port.......: 8091
17.) External Webserver IP:
18.) SSL Port...........: 8443
   SSL Domain......: Unknown
   SSL Department..: Unknown
   SSL Organization: Unknown
   SSL Loc./City...: Unknown
   SSL State/Prov.: Unknown
   SSL Country....: United States,us
19.) JNDI Port.............: 1099
20.) JNDI-RMI Port.........: 1098
21.) JRMP Port.............: 5444
22.) JRMP Invoker Port......: 5446
23.) AJP Port.............: 8009
24.) Classloader Port......: 8083
25.) JBoss Web Memory.....: 256

JBoss JMS Settings:
26.) JNDI Port...............: 1856
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>27.) JNDI-RMI Port...............: 4458</td>
<td></td>
</tr>
<tr>
<td>28.) JRMP Port....................: 4444</td>
<td></td>
</tr>
<tr>
<td>29.) JRMP Invoker Port............: 4446</td>
<td></td>
</tr>
<tr>
<td>30.) Bi-Socket Primary Port......: 4457</td>
<td></td>
</tr>
<tr>
<td>31.) Bi-Socket Secondary Port....: 4459</td>
<td></td>
</tr>
<tr>
<td>32.) Web Port.....................: 21101</td>
<td></td>
</tr>
<tr>
<td>33.) HTTP Invoker Port............: 1101</td>
<td></td>
</tr>
<tr>
<td>34.) JBoss JMS Memory.............: 256</td>
<td></td>
</tr>
</tbody>
</table>

MySQL Settings:
- 35.) Database IP.........: 4.4.4.4
- 36.) Database Port.......: 3333
- 37.) Database Memory.....: 256
- 38.) Distributed Database: YES
  - Database IP.........: 3.3.3.3
  - Database Port.......: 3333

Email Settings:
- 39.) Email Server IP......: 1.1.1.1
- 40.) Email Server User....: wandl
- 41.) Email Server Password:

Event Settings:
- 42.) Event Post Port....: 7077
- 43.) Event Server Memory: 256
- 44.) Event AIM User:
- 45.) Event AIM Password:
- 46.) Event Gtalk User:
- 47.) Event Gtalk Password:
- 48.) Event Msn User:
- 49.) Event Msn Password:
- 50.) Event Yahoo User:
- 51.) Event Yahoo Password:

LDAP Server Settings:
- 52.) LDAP Server IP.......: 1.1.1.1
- 53.) LDAP Server Port.....: 3389

Aggregation Settings:
- 54.) Maximum Traffic Capacity in Days......: 35
- 55.) Aggregation Week Interval Divisor.....: 6
- 56.) Aggregation Number Days per Week......: 7
- 57.) Aggregation Month Interval Divisor....: 24
- 58.) Aggregation Number Days per Month.....: 35
- 59.) Aggregation Memory....................: 256
- 60.) Archive Traffic in MySQL Export Format: OFF
- 61.) Compute Traffic Reference.............: OFF

Application Monitor Settings:
- 62.) Application Monitor Email Recipient...:
- 63.) Application Monitor Memory............: 128

Threshold Server Settings:
- 64.) Threshold Server Memory..............: 256

SNMP Trap Forwarder Settings:
- 65.) Enable Trap Forwarder...............: ON
- 66.) Upstream Address....................:
- 67.) Upstream Port.......................: 162
Advanced Options:
68.) Enable NAT access for JMS...............: OFF
69.) Network Event Storage Capacity.........: 30
70.) Enable Jump Server.....................: OFF

Please select a number to modify.
[<CR>=accept, q=quit]: 7
7 selected!

Current Task Manager Memory Setting: 256

Please enter a new Task Manager Memory Setting: 2048
Changing Task Manager Memory Setting from '256' to '2048'

Please select a number to modify.
[<CR>=accept, q=quit]: 52
52 selected!

Current LDAP Server IP Address: 4.4.4.4

Please enter a new LDAP Server IP Address: 1.1.1.1
Changing LDAP Server IP Address from '4.4.4.4' to '1.1.1.1'

Please select a number to modify.
[<CR>=accept, q=quit]: 38
38 selected!

Use Distributed Database (default=no)? [y/n]: y

Current Distributed Database IP Address: 4.4.4.4

Please enter a new Distributed Database IP Address: 3.3.3.3
Changing Distributed Database IP Address from '4.4.4.4' to '3.3.3.3'

Current Distributed Database Port: 3333

Please enter a new Distributed Database Port: 3333

No changes were made...

Please select a number to modify.
[<CR>=accept, q=quit]: 39
39 selected!

Current Email IP Address: 4.4.4.4

Please enter a new Email IP Address: 1.1.1.1

Please select a number to modify.
[<CR>=accept, q=quit]: 40
40 selected!

Current Email User: wandl

Please enter a new Email User: wandl

Please select a number to modify.
[<CR>=accept, q=quit]: 41
41 selected!

Please enter a new Email Password:
Please select a number to modify.
[<CR>=accept, q=quit]:

Accept these values (default=no)? [y/n] y

Install Client (default=yes)? [y/n] n
You may install the Client on Solaris86 systems by running /u2/NPAT5.5.1/current.mpls/client/solaris_86/install.client.

Install Data Collector (default=yes)? [y/n] n
You may install the Data Collector on Solaris86 systems by running /u2/NPAT5.5.1/current.mpls/dcollect/solaris86/install.dcollect.

Install Rsync & Database Replication Package (default=no)? [y/n] n
You may install the Rsync & Database Replication Package by running /u2/NPAT5.5.1/current.mpls/replication/instrepl.sh

Copying over existing license file.
Extracting server files (this may take some time) .................... Done!

Installing webserver ... Done!

Note: Files from the previous installation will be backed up to
/export/home/wandl/report/db/command.bak,
/export/home/wandl/report/db/cmdtemplate.bak, and
/export/home/wandl/report/db/config.bak
Note: Original files from the new package will be backed up to
/export/home/wandl/report/db/command.orig,
/export/home/wandl/report/db/cmdtemplate.orig, and
/export/home/wandl/report/db/config.orig

Copy files from the old installation to the new installation?:

1.) [YES] all commands in /export/home/wandl/ipmplsview/db/command
2.) [YES] all command templates in /export/home/wandl/ipmplsview/db/cmdtemplate
3.) [YES] all LDAP user account data
4.) [YES] /export/home/wandl/ipmplsview/db/config/collectioncmds.xml
5.) [YES] /export/home/wandl/ipmplsview/db/config/eventserver.xml
6.) [YES] /export/home/wandl/ipmplsview/db/config/eventtypes.store
7.) [YES] /export/home/wandl/ipmplsview/db/config/snmptrap.store
8.) [YES] /export/home/wandl/ipmplsview/db/config/subscriptions.store
9.) [YES] /export/home/wandl/ipmplsview/db/config/thresholdrules.store
10.) [YES] /export/home/wandl/ipmplsview/db/config/hardwaretypeitmapting.csv
11.) [YES] /export/home/wandl/ipmplsview/db/config/vendortemplatefile.csv
12.) [YES] /export/home/wandl/ipmplsview/db/config/autoclearpairing.csv
13.) [YES] /export/home/wandl/ipmplsview/db/config/diagnosticcmds
14.) [YES] /export/home/wandl/ipmplsview/db/config/shownodecmds
15.) [YES] /export/home/wandl/ipmplsview/db/config/showwpcmds
16.) [YES] /export/home/wandl/ipmplsview/db/config/proverrmap.txt
17.) [YES] /export/home/wandl/ipmplsview/db/config/rca-rules

Y.) Toggle all files listed in 4-17 as [YES]
N.) Toggle all files listed in 4-17 as [NO]

Please select a number to modify.
[<CR>=accept]:
Accept these values (default=no)? [y/n] y

Copying old command directory ... Done!
Copying old command template directory ... Done!
Copying LDAP user account data ... Done!
Copying old configuration files ... Done!

Creating database files for installation...Done.
Creating database tables ... Done!
Creating symbolic links ... Done!
Creating event repository ... Done!

Configuration file: '/export/home/wandl/report/bin/mplsenvsetup.sh' was created on Thu Jul  1 16:32:34 EDT 2010
Creating Webserver configuration files ... Done!
Creating Diagnostics configuration files ... Done!
Creating Event Model configuration files ... Done!
Creating Traffic Summary configuration files ... Done!
Creating DGS configuration files ... Done!
Creating Event Server configuration files ... Done!
Creating Monitor configuration files ... Done!
Creating IP/MPLSView Application Monitor configuration files ... Done!
Creating Task Manager configuration files ... Done!
Creating database files ... Done!
Creating LDAP files ... Done!

Initializing LDAP directory ... Done!

Give JAVA Applets write-permission (default=no)? [y/n] y
Signing files ...............
Successfully created a symbolic link from /u/wandl to /export/home/wandl/report.

You may start the SNMP Trap Listener by running the following command:
/export/home/wandl/report/bin/.snmptrap start

You may start up the IP/MPLSView server by running the following command:
/export/home/wandl/report/bin/startup_mplsview

Start up the IP/MPLSView server (default=yes)? [y/n]n
Executing post-installation procedures for standalone server
Please enter the directory where IP-MPLSView has been installed.
(default=/u/wandl):

Detecting processor information...

64-bit processor detected, do you want to use 64-bit Java to allocate more than 2GB memory (default=yes)? [y/n] y

2 CPUs (or cores) detected, do you want to use parallel garbage collection (default=yes)? [y/n]

Saving configurations to /u/wandl/bin/tmngenvsetup.sh

Modifying startup.sh... Done.

Creating symbolic link for 64-bit native library ... Done!

Installation was successful, do you want to start the standalone server [y/n]: n

---

**User Administration for Report Server**

It is recommended to setup the user accounts to the report server for the sole purpose of running Network Performance Data Reports and to prevent report server users from running duplicate collection tasks performed by the application server.

Login as an administrator to the application server where LDAP is running, in order to specify the settings for the account that will have access to the report server. This is accessed under Admin > User Administration. The report server should not run Fault Management, Provisioning, Network collection tasks, and any items related to Event Browser should be disabled or unchecked in the User Administration window.

The following report server user functions should be disabled with certain exceptions under Task Manager:

- Provisioning
- Event Browser
- Task Manager
Figure 7: Report User Disabled Functions

The following Task Manager functions can be enabled for reporting purposes:

- Configuration Check Report
- Hardware Inventory Report
- Integrity Check
- Network Data Report
- Server Performance Data Collection
- Traffic Summary Report
- Web Report
Figure 8: Report User Enabled Functions
Chapter 7

Installing Replication and Rsync

The replication and rsync package can be used for maintaining backup server(s) with up to date version of the files and database of the primary server(s) they are backing up. These utilities are designed for backing up information from IP/MPLSView’s data and traffic collection.

The third-party rsync package will backup files from the primary application server to the backup application server, and the MySQL replication package will keep the backup database in sync with the primary database. Both of these packages are designed to synchronize data in a way by sending deltas in a way that reduces data transfer.

For the backup of data collection files only and not traffic collection, only rsync is needed, since the MySQL database is not involved. See Installing Rsync (Backup of Online Data Collection only) on page 64 for more details.

For the backup of data and traffic collection data, two different setups are possible with respect to the application server and database:

- **Four Machine Setup**: The primary IP/MPLSView server has a distributed primary database on another machine. In this case, the backup IP/MPLSView server will be on a separate machine with a distributed database on yet another machine. See Installing Rsync and Replication (Four Machine Setup) on page 69 for more details.

- **Two Machine Setup**: The primary application server and primary database are on the same machine, in which case they can be backed up by a second machine with both the application server and database installed. See Installing Rsync and Replication (Two Machine Setup) on page 72 for more details.

In both cases, there can also be multiple data collectors running on separate machines.

---

**Informational Note:** This package requires that the backup IP/MPLSView server have a separate license.

---

**Informational Note:** Replication and rsync options are provided from the following scripts if installing via CD-ROM: `/cdrom/cdrom0/server/install.sh` and `/cdrom/cdrom0/dcobject/solaris86/instdatabase.sh` or `/cdrom/cdrom0/dcobject/unix/instdatabase.sh`.

If skipping that option, you can install this package later using the following installation script `/cdrom/cdrom0/replication/instrepl.sh`. 
Prerequisites for Rsync

Prerequisite steps are required before installing the rsync package. If you have already reached the replication and rsync option from the installation script, these steps can be run from a separate telnet/ssh window prior to continuing the installation.

Rsync Package

Rsync package should be installed on the primary and backup application servers. This can be done before or after the replication and rsync option from the installation script. Check if your server already has rsync by checking for the file /usr/local/bin/rsync or using the command "pkginfo | grep rsync". If rsync is not installed, the root user can install rsync via replication/inst_rsync.sh from the rsync installation package. If your server is Linux, to check rsync use command “rpm -qa | grep rsync”.

Automatic Login

1. To allow for automatic rsync via a cron job, the primary and backup application servers’ users should be able to automatically log in using SSH to each other without the need for a password. For this to happen, the primary servers’ public key (id_rsa.pub) must be present in the backup server’s authorized keys (authorized_keys) and vice versa. The following procedure, that automates the login process, must be done on both the primary and backup application servers before running the install script for rsync.

2. Log in as 'wandl' user and switch the current directory to the home directory. (For the example below, the home directory will be /export/home/wandl. For Linux the home directory usually is /home/wandl). Generate a pair of authentication keys. Do not enter a passphrase:

```bash
/export/home/wandl> ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/export/home/wandl/.ssh/id_rsa):
Created directory '/export/home/wandl/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /export/home/wandl/.ssh/id_rsa.
Your public key has been saved in /export/home/wandl/.ssh/id_rsa.pub.
The key fingerprint is:
wandl@lexus
```
3. For the transfer of data collection information only between primary and backup application server, setting up rsync using the IP/MPLSView administrative user account (for example, wandl) is usually sufficient. However, if traffic collection data needs to be transferred, automatic login needs to be set up for the root account because some of the files that need to be transferred may be owned by the root account.

Ssh Key Exchange Setup for Root (Required for Traffic Collection Backup)

```
/root# ssh root@<remotehostip> mkdir -p .ssh
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '<remotehostip>' (RSA) to the list of known hosts.
```

```
Password:
```

4. Append the local host's new public key to the remote host's authorized keys and enter the remote host's root password one last time.

```
/root# cat .ssh/id_rsa.pub | ssh root@<remotehostip> 'cat >> .ssh/authorized_keys'
```

```
Password:
```

5. Repeat the above steps for the backup IP/MPLSView server.

6. Note that you need to set PermitRootLogin to yes in the sshd_config file (for example, /etc/ssh/sshd_config or /usr/local/etc/sshd_config). If it is not set, edit the file and then restart the 'sshd' process using “svcadm refresh ssh” for Solaris 10. For Solaris 8 or 9, run "ps -ef | grep sshd" to find the main sshd process, the parent of the other sshd processes, which has a low PPID. To refresh the service, run "kill -1 <PID>", substituting in the PID of the main sshd process.

**Caution:** This might terminate currently open SSH sessions.

7. Check to make sure the permission of the .ssh directory is restricted as follows:

```
/export/home/wandl> chmod 700 .ssh
```

8. For Linux RedHat, additional permissions on the authorized_keys file is required as follows:

```
/export/home/wandl/.ssh> chmod 600 authorized_keys
```

9. Finally, test the automatic login from both machines to each other using "ssh root@<remotehostip>" to see if you can login without entering in a password.

**SSH Key Exchange Setup for IP/MPLSView Administrative Account (Rsync Only)**

1. Login to the IP/MPLSView Administrative account from which you will transfer data and SSH to create the directory .ssh on the remote host. Substitute <remotehostip> below with the IP address of the remote host. Enter 'yes' when prompted to continue connecting. Enter the remote host's password when prompted.

```
/export/home/wandl> ssh wandl@<remotehostip> mkdir -p .ssh
Are you sure you want to continue connecting (yes/no)? yes
```
Warning: Permanently added '<remotehostip>' (RSA) to the list of known hosts. 
Password:

2. Append the local host’s new public key to the remote host’s authorized keys and enter the remote host’s root password one last time.

/export/home/wandl> cat .ssh/id_rsa.pub | ssh wandl@<remotehostip> 'cat >> .ssh/authorized_keys'
Password:

3. Repeat the above steps for the backup IP/MPLSView server.

4. Check to make sure the permission of the .ssh directory is restricted as follows:

/export/home/wandl> chmod 700 .ssh

5. For Linux RedHat, additional permissions on the authorized_keys file is required as follows:

/export/home/wandl/.ssh> chmod 600 authorized_keys

6. Finally, test the automatic login from both machines to each other using “ssh wandl@<remotehostip>” to see if you can login without entering in a password.

Installing Rsync (Backup of Online Data Collection only)

For transfer of data from the primary application server to the backup application server for online data collection only, and not traffic collection, only the rsync package is required, and not replication. Furthermore, the SSH key exchange can be performed using the IP/MPLSView administrative account (for example, wandl) rather than root. The following steps will guide you through the process of setting up rsync.

SSH Key Exchange

Set up the SSH key exchange so that the wandl account on the primary server can access the wandl account on the backup server and vice versa.

Installation of Rsync on Primary Application Server

1. Install the Rsync package via ./instrepl.sh using the wandl user.

   -bash-3.00$ cd replication/
   -bash-3.00$ ./instrepl.sh

   Installation of Rsync/Replication

   In a normal setup for traffic collection (Application and Database are on the same server): (1) Rsync should be configured and (2) The Database Replication Package should be installed.

   In a Distributed setup for traffic collection:
   - For the Application server, only (1) Rsync should be configured.
   - For the Database server, only (2) Database Replication Package should be installed.

   If traffic collection is *not* used and only file backup is needed, e.g., for online data collection, then only (1) Rsync should be configured

   Don't forget to set the server as Primary or Backup via menu (3)

   If you wish to later change the settings, you may run /export/home/wandl/replication/instrepl.sh
Rsnc & Replication Settings
1.) Setup Rsnc for Application Server.....YES
2.) Install Database Replication Package...YES
3.) Setup as Primary or Backup Server......PRIMARY
4.) Preserve files on target server........YES (Recommended)

Please select a number to modify.
<CR>=accept, q=quit]: 2

2. For the primary machine installation, turn off the Replication function via menu #2 below, since only Rsnc will be used. Replication is a feature related to MySQL database that is used for the online traffic module.

Rsnc & Replication Settings
1.) Setup Rsnc for Application Server.....YES
2.) Install Database Replication Package...NO
3.) Setup as Primary or Backup Server......PRIMARY
4.) Preserve files on target server........YES (Recommended)

Please select a number to modify.
<CR>=accept, q=quit]:
Accept these values (default=no)? [y/n] y

Rsnc may be run using a non-root user for data collected via configuration management module. However, the root user should be used for performance and fault management modules for which some of the transferred files may be owned by root.

3. For the rsnc user ID, choose wandl instead of root for the Rsnc-only usage. Root is only required if the files to be transferred or MySQL-related files to be replicated are owned by a user other than wandl, such as root, which would occur in the case of the online traffic module.

Please input the rsnc user ID (root): wandl ?Changed to wandl
Indicate the IP address of the alternate server.
Please enter the IP address of the alternate MPLSView server: n.n.n.n ?Enter backup server IP
Please enter the wandl user ssh host key (/export/home/wandl/.ssh/id_rsa):

4. Next, indicate which files are to be synchronized:

Synchronize the following files/directories?:
You can later manually modify the entries in /u/wandl/bin/rsync.sh
1.) [YES] /u/wandl/data/
2.) [YES] /u/wandl/db/config/snmptrap.store (Fault Management)
3.) [YES] /u/wandl/db/config/subscriptions.store (Fault Management)
4.) [YES] /u/wandl/db/config/eventtypes.store (Fault Management)
5.) [YES] /u/wandl/db/config/productionscopes.store (Fault Management)
6.) [YES] /u/wandl/db/config/collectioncmds.xml
7.) [YES] /u/wandl/db/config/diagnosticcmds
8.) [YES] /u/wandl/db/config/shownodecmds
9.) [YES] /u/wandl/db/config/showvpncmds
10.) [YES] /u/wandl/db/command/
12.) [YES] /u/wandl/data/.TaskManager/profile/
13.) [YES] /u/wandl/data/.TaskManager/tmp/.diag
14.) [YES] /u/wandl/data/device/
15.) [YES] /u/wandl/data/ping/
16.) [YES] /u/wandl/data/sla/
17.) [YES] /u/wandl/data/summary/ (Fault Management)
18.) [YES] /u/wandl/data/latency/
19.) [YES] /u/wandl/data/event/ (Fault Management)
20.) [YES] /u/wandl/data/LDPTraffic/ (Performance Management)

Please select a number to modify.
[<CR>=accept]:

5. After making desired selections, accept the changes.

Accept these values (default=no)? [y/n] y
Directories can be modified by editing the file /u/wandl/bin/rsync.sh
Would you like to add additional directories? (default=no)? [y/n]

6. Here you can add additional directories to be sync'ed between primary and backup server. If there are any additional files or directories outside of /u/wandl that need to be backed up, they should be added manually to the list. For example, LDAP can also be added to the backup (unless the backup server will maintain a separate set of logins):

/u/wandl/thirdparty/openldap/var/openldap-data

For example:

Would you like to add additional directories? (default=no)? [y/n] y/
Enter directory/file on application server to include in rsync transfer (or c to cancel) /u/wandl/thirdparty/openldap/var/openldap-data
Enter directory/file on backup server to transfer to:
(default/u/wandl/thirdparty/openldap/var/openldap-data) /u/wandl/thirdparty/openldap/var/openldap-data2 ?
You can choose a different destination directory to avoid interfering with backup server, if it should maintain a different set of logins than the application server
Added entry. Please verify the entry at the end of /u/wandl/bin/rsync.sh.

At the end, select the interval in which to run rsync. The default is 1 hour.

Please select the crontab interval in minutes (60): [0-60] 60
Crontab updated:
0 * * * * /u/wandl/bin/rsync.sh exec > /u/wandl/log/rsync.log

Rsync will synchronize /u/wandl and /u/wandl/data every 60 minutes

This will generate a file /u/wandl/bin/rsync.sh where the files/directories can be modified, in case there is additional information to transfer from primary to backup server.
To make modifications to the frequency of rsync, you can rerun the install script or directly edit the crontab entry.
$ EDITOR=vi
$ export EDITOR
$ crontab -e
0 * * * * /u/wandl/bin/rsync.sh exec > /u/wandl/log/rsync.log

Installation of Rsync on Backup Application Server

The next step is to install rsync on the backup server. Run replication/inst_rsync.sh on the backup server to install rsync if it does not exist.
Run replication/instrepl.sh on the backup server, again disabling option (2) but this time also toggling option (3) to specify that it is the backup server.

Rsync & Replication Settings
1.) Setup Rsync for Application Server...: YES
2.) Install Database Replication Package.: NO
3.) Setup as Primary or Backup Server....: BACKUP
4.) Preserve files on target server........YES (Recommended)

The other options are similar to before, although this time the cron job is not set up, because the backup server will only need to transfer the data back to the primary server once (manually) when the primary server comes back up. When specifying additional directories/files, make sure to include the same as those which were chosen for the primary server.

Rsync Administration

Once rsync is installed, it is enabled based on the selected interval. To later disable rsync, use the following command:

$ /u/wandl/bin/rsync.sh stop

In this case, rsync.sh will terminate before executing any file transfers.

To enable rsync, use the following command:

$ /u/wandl/bin/rsync.sh start

To check the status of rsync, use the following command:

$ /u/wandl/bin/rsync.sh status

As a safety feature, the rsync.sh command run from the cron job on the primary server will terminate before performing any transfers under the following conditions:

- If Rsync is disabled via /u/wandl/bin/rsync.sh stop on this server
- If Rsync is disabled via /u/wandl/bin/rsync.sh stop on the alternate server (this is required because the primary server may not be accessible anymore, but we need a way to prevent rsync from restarting when the primary server automatically comes online and becomes accessible.)
- If IP/MPLSView is not running -or-
- If a pre-existing Rsync process is already detected

Rsync.sh run from the backup server will terminate before performing any transfers under the following conditions (note that the primary server should be disabled in this case):

- If Rsync is disabled via /u/wandl/bin/rsync.sh stop on this server
- If IP/MPLSView is not running -or-
- If A pre-existing Rsync process is already detected

To manually run rsync apart from the cron job, for testing purposes, or for on-demand file backup, use the following command:

$ /u/wandl/bin/rsync.sh exec

The console output will indicate the log of the transfer. Note that when the cron job runs rsync, the log of the last execution will be stored in /u/wandl/log/rsync.log
Failover Process

Switching to the Backup Server

The following process can be performed when the primary server is down to activate up the backup server.

1. Disable rsync on the backup server to prevent further rsync transfers by cron job from the primary server, which could result in loss of data if the primary server becomes accessible and active after already activating the backup server.
   
   ```bash
   $ /u/wandl/bin/rsync.sh stop
   ```

2. The primary server will check the backup server's status prior to transfer. If rsync is disabled on the backup server, the primary server will not continue with the transfer.

3. Once the primary server is down, the IP/MPLSView task server must be restarted on the backup server in order to refresh the Task Manager with the tasks that were transferred from the primary server:
   
   ```bash
   $ /u/wandl/bin/stop_mplsview
   $ /u/wandl/bin/startup_mplsview
   ```

   This will overwrite any tasks on the backup server that were previously loaded in the Task Manager, based on the newly transferred files. Alternatively, if IP/MPLSView is running, a shortcut is to stop and restart the Task server only:

   ```bash
   $ /u/wandl/bin/.tmng stop
   $ /u/wandl/bin/.tmng
   ```

4. Launch the IP/MPLSView client, changing the server IP to the backup server in the standalone Java client’s ipmplsview.bat file or in the WebStart settings.

5. Open the Task Manager via Admin > Task Manager.

   The tasks should all be grayed out, to prevent them from being run twice should the primary server be up simultaneously.

6. Once you have verified that the primary server is down, select the task(s) to be reactivated. Then select Actions > Reactivate. The Reactivate option is also in the right-click menu for each task. The tasks will then be reactivated, and will no longer be gray.

7. The Modification Log tab will indicate the change in the IP address tag from the primary server IP address to the backup server IP address, for example:

   ```
   John modified from wind (192.168.1.22)
   Client Userid= wandl, OS=Windows 7 6.1 (6.0.2 Build: 2012024)
   IP tag updates: 192.168.1.55 to 192.168.1.88 11/03/2012 22:53:30
   ```

   Now you can continue using these tasks from the backup server.

Informational Note: If the primary server is powered up by itself, IP/MPLSView is not automatically started, and rsync.sh will terminate before executing any file transfers as a protection. However, this step is still necessary to prevent the scenario where the primary server is up, but is merely inaccessible, in which case there is a danger that when it becomes accessible, that it will continue to transfer data by the cron job to the backup server, after it is up.
Switching Back to the Primary Server
1. When the primary server is restored, disable rsync on the primary server using
   
   /u/wandl/bin/rsync.sh stop

2. Next, transfer the updated data from the backup server to the primary server by
   running "/u/wandl/bin/rsync.sh exec" on the backup server

3. When the transfer is complete, re-enable rsync on the primary server, so that
   subsequent changes will be backed up again to the backup server.

4. Restart the task server on the primary server and login via the client but now to the
   primary server IP address. Open the Task Manager, select all tasks, and reactivate.
   The Modification log will indicate that the IP address tag has again been updated.

Installing Rsync and Replication (Four Machine Setup)

Figure 9: Setup A, Primary IP/MPLSView Server with Distributed Database

1. The rsync and replication package installation can be run as part of the general
   installation, using the command ./install.sh on the application servers and
   ./instdatabase.sh on the database servers. If answering no to installing rsync and
   replication during the installation, the following steps can also be taken afterwards
   using the replication/instrepl.sh script. Note that the package should be installed by
   wandl.

2. Press "y" to install the replication package when prompted during the installation script.
   
   Install Rsync & Database Replication Package (default=no)? [y/n] y

3. Configure the respective servers with the following settings.
   
   On Primary Application Server:
   Rsync & Replication Settings
   1.) Setup Rsync for Application Server.....YES
   2.) Install Database Replication Package...NO
   3.) Setup as Primary or Backup Server......PRIMARY
4.) Preserve files on target server........YES (Recommended)

On the primary database server:

Rsync & Replication Settings
1.) Setup Rsync for Application Server.....NO
2.) Install Database Replication Package...YES
3.) Setup as Primary or Backup Server......PRIMARY
4.) Preserve files on target server........YES (Recommended)

On the backup application server:

Rsync & Replication Settings
1.) Setup Rsync for Application Server.....YES
2.) Install Database Replication Package...NO
3.) Setup as Primary or Backup Server......BACKUP
4.) Preserve files on target server........YES (Recommended)

On the backup database server:

Rsync & Replication Settings
1.) Setup Rsync for Application Server.....NO
2.) Install Database Replication Package...YES
3.) Setup as Primary or Backup Server......BACKUP
4.) Preserve files on target server........YES (Recommended)

4. Enter the IP address of the corresponding backup server for the primary servers and the corresponding primary server for the backup servers.

Please enter the IP address of the alternate MPLSView server: <ipaddress>

5. Enter the ssh directories of the alternate MPLSView server if the actual paths do not conform to the default paths.

Please enter the wandl user ssh host key /export/home/wandl/.ssh/id_rsa):

6. For the primary application server, you will be asked which directories and files to synchronize. Check that the backup server has enough disk space in the IP/MPLSView home directory.

Synchronize the following files/directories?:
You can later manually modify the entries in /u/wandl/bin/rsync.sh
1.) [YES] /u/wandl/data/
2.) [YES] /u/wandl/db/config/snmptrap.store
3.) [YES] /u/wandl/db/config/subscriptions.store
4.) [YES] /u/wandl/db/config/eventtypes.store
5.) [YES] /u/wandl/db/config/productionscopes.store
6.) [YES] /u/wandl/db/config/collectioncmds.xml
7.) [YES] /u/wandl/db/config/diagnosticcmds
8.) [YES] /u/wandl/db/config/shownodecmds
9.) [YES] /u/wandl/db/config/showvpncmds
10.) [YES] /u/wandl/db/command/
11.) [YES] /u/wandl/data/..network/
12.) [YES] /u/wandl/data/..TaskManager/profile/
13.) [YES] /u/wandl/data/..TaskManager/tmp/..diag
14.) [YES] /u/wandl/data/device/
15.) [YES] /u/wandl/data/ping/
16.) [YES] /u/wandl/data/sla/
17.) [YES] /u/wandl/data/summary/
18.) [YES] /u/wandl/data/latency/
19.) [YES] /u/wandl/data/event/
20.) [YES] /u/wandl/data/LDPTraffic/
Please select a number to modify.
[*CR*=accept]:
Accept these values {default=no}? [y/n] y

7. In the next step, additional directories can be synchronized by specifying source and destination directories and/or files. Which directories/files are synchronized can also be modified after the installation by editing the `/u/wandl/bin/rsync.sh` script. Note that the rsync.sh, ssh, and MySQL database files are automatically excluded from the default options. If you manually edit rsync.sh, make sure that the new entries also exclude these files.

8. Enter the time interval you want the backup Application server to synchronize with the primary Application server.

   Please select the crontab interval in minutes (60): [0-60] <#>

   This time interval can be modified later by rerunning /cdrom/cdrom0/replication/instrepl.sh. (Alternatively, you can directly modify the crontab settings as wandl user. For example, you can set the EDITOR to vi using “EDITOR=vi”, export the variable using “export EDITOR”, and then run “crontab -e”. Check the man page for more information.)

Initial Setup (Four Machine Setup)

Replication

1. After installing replication package on the application and database servers, follow these steps that configure them to run in their respective modes.

2. Startup IP/MPLSView on the primary MySQL server (master) only, if it is not started up during installation.

   > /u/wandl/bin/stop_mplsview
   > /u/wandl/bin/startup_mplsview

3. Startup IP/MPLSView on the primary App server, if it is not started up during installation. NO data collectors in the entire system should be started up yet.

   > /u/wandl/bin/stop_mplsview
   > /u/wandl/bin/startup_mplsview

4. Stop IP/MPLSView on the backup App server.

   > /u/wandl/bin/stop_mplsview

5. Startup the backup MySQL server (slave)

   > . /u/wandl/bin/mplsenvsetup.sh
   > /u/wandl/bin/mysql.server start slave
   ...
   Slave Mysql server connected to Master: <primary server ip>
   ...

6. Start up all data collectors -- depending on your configuration, start them up on the primary App server or on the separate data collector server(s)

   > /u/wandl/dcollect/dc.sh start <data collector #>

7. Check the MySQL master/slave status on both primary (master) and backup (slave) MySQL servers.
8. On the Slave server you should see the following output:

Slave Mysql server connected to Master: <primary server ip/hostname>

9. On the Master server you should see the following output:

Master Mysql server is running
Slave server: <backup server ip/hostname> #Once the slave server is running

Rsync

10. On the Primary server, the rsync.sh script will run according to the interval specified. Depending on synchronization requirements, 30 or 60 minute intervals should be frequent enough. Each time the script runs, it synchronizes /u/wandl/data (excluding the mysql traffic database directory) directories between the Primary and the Backup servers – push synchronization. After the designated interval, check the /u/wandl/data directory on the backup application server to make sure that the file system data has been copied.

Installing Rsync and Replication (Two Machine Setup)

Figure 10: Setup B, Primary IP/MPLSView Server with Database on Same Machine

The rsync and replication package installation, which is part of the installation script, can be done by running ./install.sh. If answering no to installing rsync and replication during the installation, the following steps can also be taken afterwards using the replication/instrepl.sh script as wandl.

1. Press "y" to install the replication package.

Install Rsync & Database Replication Package (default=no)? [y/n] y

2. Configure the respective servers with the following settings.

On the primary server:

Rsync & Replication Settings
1.) Setup Rsync for Application Server.....YES
2.) Install Database Replication Package...YES
3.) Setup as Primary or Backup Server......PRIMARY
4.) Preserve files on target server........YES (Recommended)

On the backup server:

Rsync & Replication Settings
1.) Setup Rsync for Application Server.....YES
2.) Install Database Replication Package...YES
3.) Setup as Primary or Backup Server......BACKUP
4.) Preserve files on target server........YES (Recommended)

3. Enter the backup server’s IP on the primary server and viceversa.

Please enter the IP address of the alternate MPLSView server: <ipaddress>

4. Enter the ssh directory of the alternate MPLSView server if the actual paths do not conform to the default paths.

Please enter the wandl user ssh host key /export/home/wandl/.ssh/id_rsa):

5. Then you will be asked which directories and files to synchronize. Check that the backup server has enough disk space in the IP/MPLSView home directory.

Synchronize the following files/directories?:
You can later manually modify the entries in /u/wandl/bin/rsync.sh
1.) [YES] /u/wandl/data/
2.) [YES] /u/wandl/db/config/snmptrap.store
3.) [YES] /u/wandl/db/config/subscriptions.store
4.) [YES] /u/wandl/db/config/eventtypes.store
5.) [YES] /u/wandl/db/config/productionscopes.store
6.) [YES] /u/wandl/db/config/collectioncmds.xml
7.) [YES] /u/wandl/db/config/diagnosticcmds
8.) [YES] /u/wandl/db/config/shownodecmds
9.) [YES] /u/wandl/db/config/showvpncmds
10.) [YES] /u/wandl/db/command/
12.) [YES] /u/wandl/data/.TaskManager/profile/
13.) [YES] /u/wandl/data/.TaskManager/tmp/.diag
14.) [YES] /u/wandl/data/device/
15.) [YES] /u/wandl/data/ping/
16.) [YES] /u/wandl/data/sla/
17.) [YES] /u/wandl/data/summary/
18.) [YES] /u/wandl/data/latency/
19.) [YES] /u/wandl/data/event/
20.) [YES] /u/wandl/data/LDPTraffic/

Please select a number to modify.
[<CR>=accept]

Accept these values (default=no)? [y/n] y

By default, the administrative home directory will not be synchronized. If you do wish to synchronize this directory, first check the size of the directory, to make sure it is reasonable and that you want to copy all of its contents over to the backup server. For example, if the directory is /export/home/wandl/, check the size in KB with “du -ks /export/home/wandl”.

Which directories/files are synchronized can also be modified after the installation is over by editing the /u/wandl/bin/rsync.sh script. Note that the database files must be excluded from the rsync.
6. Finally, enter the time interval you want the backup App server to synchronize with the primary App server.

   Please select the crontab interval in minutes (60): [0-60] <#>

   This time interval can be modified later by rerunning /cdrom/cdrom0/replication/instrepl.sh. (Alternatively, you can directly modify the crontab settings as wandl user. For example, you can set the EDITOR to vi using “EDITOR=vi” and then run “crontab -e”. Check the man page for more information.)

Initial Setup (Two Machine Setup)

Replication

After installing replication package on both the servers, follow these steps that configure them to run in their respective modes.

1. Startup IP/MPLSView on the primary server (master) only, if it is not started up during installation.

   > /u/wandl/bin/stop_mplsview
   > /u/wandl/bin/startup_mplsview

2. Stop IP/MPLSView on the backup server.

   > /u/wandl/bin/stop_mplsview

3. Startup the backup MySQL server (slave)

   > . /u/wandl/bin/mplsenvsetup.sh
   > /u/wandl/bin/mysql.server start slave

   ... Slave Mysql server connected to Master: <primary server ip>

   ...

4. Start up all data collectors -- depending on your configuration, start them up on the primary App server or on the separate data collector server(s)

   > /u/wandl/dcollect/dc.sh start <data collector #>

5. Check the MySQL master/slave status on both primary (master) and backup (slave) servers.

   > /u/wandl/bin/mysql_repl.sh status

   On the Slave server you should see the following output:

   Slave Mysql server connected to Master: <primary server ip/host>

   ... On the Master server you should see the following output:

   Master Mysql server is running
   Slave server: <backup server ip/host> #Once the slave server is running

Rsync

On the Primary server, the /u/wandl/bin/rsync.sh script will run according to the interval specified. Depending on synchronization requirements, 30 or 60 minute intervals should be frequent enough. Each time the script runs, it synchronizes /u/wandl/data (excluding the mysql traffic database directory) directories between the Primary and the Backup servers – push synchronization.
After the designated interval, check the /u/wandl/data directory on the backup application server to make sure that the file system data has been copied.

### Failover Process

Assuming that the primary App or MySQL server fails, the following steps walk you through the procedure to switchover to the backup server and bring it up for operation until the primary server is recovered.

1. Stop all data collectors – on the App and data collector servers, depending where they are running.
   
   ```bash
   > /u/wandl/dcollect/dc.sh stop all
   ```

2. If either the primary App or primary MySQL server failed, stop the remaining services on the primary server.
   
   ```bash
   > /u/wandl/bin/stop_mplsview
   ```

3. Stop the cronjob for the /u/wandl/bin/rsync.sh script on the primary server. The cronjob is under the admin user id that installed IP/MPLSView. By default this user id is wandl. Comment out of the following line in crontab.
   
   ```bash
   > crontab -e
   #0,30 * * * * /u/wandl/bin/rsync.sh exec > /u/wandl/log/rsync.log
   ```

4. Stop the backup MySQL (slave) server.
   
   ```bash
   > . /u/wandl/bin/mplsenvsetup.sh
   > /u/wandl/bin/mysql.server stop
   ```

5. Start IP/MPLSView on both the backup MySQL server and backup App server. This backup MySQL server now becomes the master.
   
   ```bash
   > /u/wandl/bin/startup_mplsview
   ```

6. Check the MySQL server status on the backup MySQL server.
   
   ```bash
   > /u/wandl/bin/mysql_repl.sh status
   ```

7. Verify that ALL IP/MPLSView applications are running on both the backup App and MySQL servers.
   
   ```bash
   > /u/wandl/bin/status_mplsview
   ```

8. Restart all data collectors on the backup App server and data collector server(s), depending where they are configured. For data collector server(s), you need to make sure that they are pointing to the backup App (JBoss/JMS) server.

9. If you are using a separate set of backup data collector servers, in the event of primary data collector server failure you will need to startup the data collectors on the backup servers. The user will need to manually re-assign the collection groups to the backup data collectors since the backup servers will have a different set of collector/queue names since they will be registered using a different server name/IP from the backup data collector.

10. Start up the data collectors on the Backup App or Data collector server(s)
    
    ```bash
    > /u/wandl/dcollect/dc.sh start <data collector #>
    ```
11. Configure data collection to use the Backup server data collectors through the IP/MPLSView client

12. That completes the backup process. Open the Traffic Collection manager on the backup App server and make sure the traffic is collecting. Open a traffic chart and see if all historical traffic data is present. If it is, that is a sign that the MySQL replication was successful.

**Primary server is recovered**

1. Assume the primary App and MySQL server resumes functionality. The next step is reverse data synchronization.

2. Start the primary MySQL server in slave mode.
   
   ```
   > . /u/wandl/bin/mplsenvsetup.sh
   > /u/wandl/bin/mysql.server start slave
   ...
   Slave Mysql server connected to Master: <backup server ip>
   ...
   ```

3. Check the last data received on both primary and backup MySQL servers.
   
   ```
   > u/wandl/bin/mysql_repl.sh lastdata
   ```

   This command outputs an 11-digit number that corresponds to the time when the last data was collected. Wait until both the MySQL servers display same output as that confirms synchronization between them.

4. Stop all data collectors that may be running on backup App server or data collector servers.
   
   ```
   > /u/wandl/dcollect/dc.sh stop all
   ```

5. Synchronize the primary App server with the backup App server if any changes to the network have been made, when the primary was down. On the backup App server run command.
   
   ```
   > /u/wandl/bin/rsync.sh exec
   ```

6. Stop IP/MPLSView on both the backup App server and backup MySQL server.
   
   ```
   > /u/wandl/bin/stop_mplsview
   ```

7. Stop the primary MySQL server from running in slave mode.
   
   ```
   > . /u/wandl/bin/mplsenvsetup.sh
   > /u/wandl/bin/mysql.server stop
   ```

8. Start up IP/MPLSView on both the primary MySQL server and primary App server.
   
   ```
   > /u/wandl/bin/startup_mplsview
   ```

9. Confirm primary App and MySQL server’s IP/MPLSView status.
   
   ```
   > /u/wandl/bin/status_mplsview
   ```

10. Check master MySQL server status on primary MySQL server.
    
    ```
    > /u/wandl/bin/mysql_repl.sh status
    Master Mysql server is running
    ```
11. Re-enable the cronjob for the `/u/wandl/bin/rsync.sh` script on the primary server. The cronjob is under the admin user id that installed IP/MPLSView. By default this user id is wandl. Enable the following line in crontab.

```
> crontab -e
0,30 * * * * /u/wandl/bin/rsync.sh exec > /u/wandl/log/rsync.log
```

12. Startup backup server MySQL database in slave mode.

```
> . /u/wandl/bin/mplsenvsetup.sh
> /u/wandl/bin/mysql.server start slave
...
Slave Mysql server connected to Master: <primary server ip>
...
```

13. Startup data collectors on primary App server and/or data collector server(s).

14. Open the Traffic Collection manager on the primary App server and make sure the traffic is collecting. Open a traffic chart and see if all historical traffic data is present. If it is, that is a sign that the MySQL replication and recovery was successful.

15. Old traffic data should be preserved (as confirmed by viewing MySQL database traffic charts) when switching to and from backup servers.

---

### Out-of-Sync Database Replication

The following section describes the procedure to re-sync the database tables between the primary application and backup database servers during the MySQL replication process. The MySQL replication process may become out-of-sync when either server is improperly shut down or interrupted such as during a power outage.

#### Determine Sync Status

To determine if the primary application and backup database servers are out-of-sync, run the command `/u/wandl/bin/mysql_repl.sh lastdata` on both servers. The value returned is the timestamp of the last data written to the database tables. If the two values are not equal, then the servers are potentially out-of-sync. Run the command `/u/wandl/bin/mysql_repl.sh lastdata` again after at least 5 minutes to allow the replication process to complete a cycle to confirm if the databases are out-of-sync.

---

**Informational Note:** The format of the value returned is YearMonthInterval (YYYYMMIII). The Month of January starts at 0 through December at 11. The Interval is a multiple of 5 minutes after 12:00am with 288 5-minute intervals in a 24-hour period or day. For example, the timestamp of lastdata value 20101023133 is November 23, 2010 11:05am.

---

### Re-Sync Procedure

Assuming the primary application server and backup database servers are running, the following steps detail the repair procedure to re-sync the databases. The terms “primary or master” and “backup or slave” are used interchangeably. The commands executed will be through the server console or the MySQL CLI as specified in each step. (In the following procedure, the terms slave and master are emphasized to help avoid confusion.)

1. **On the slave** database, run these two commands in the console to enter the MySQL CLI:

   ```
   . /u/wandl/bin/mplsenvsetup.sh
   ```
2. Stop the **slave** database replication thread by entering this command in the MySQL CLI:

   `stop slave;`

3. Clean the **slave** replication data on the slave database:

   `reset slave;`

4. Exit the **slave** MySQL CLI:

   `exit`

5. Stop the **slave** database:

   `/u/wandl/bin/..mysql stop slave`

6. Enter the **master** database MySQL CLI using the same commands as step 1:

   `. /u/wandl/bin/mplsenvsetup.sh
   /u/wandl/thirdparty/mysql/bin/mysql -uroot -pwandlroot -A wandltraffic`

7. Reset the **master** database replication record by entering:

   `reset master;`

8. Exit the **master** MySQL CLI:

   `exit`

9. Stop the **primary** application server:

   `/u/wandl/bin/stop_mplsview`

10. Copy the directory and all files under `/u/wandl/data/mysql/data/wandltraffic` from the master to slave server. **Note:** You may optionally want to backup the `wandltraffic` directory on the destination server prior to the copy over.

11. After the copy is complete, run this command on the out-of-sync machine to repair the database tables.

    `/u/wandl/bin/fixmysql.sh`

12. After the repair is complete, startup the **primary** application server:

    `/u/wandl/bin/startup_mplsview`

13. Startup the **slave** database:

    `/u/wandl/bin/..mysql start slave`

14. Login to the **slave** MySQL CLI using the same commands as step 1:

    `. /u/wandl/bin/mplsenvsetup.sh
    /u/wandl/thirdparty/mysql/bin/mysql -uroot -pwandlroot -A wandltraffic`

15. Start the **slave** replication thread in the MySQL CLI:

    `start slave;`

16. Check for error messages in the **slave** database:

    `show slave status \G;`
17. Exit the **slave** MySQL CLI:

```bash
exit
```

Once the steps above are complete, wait at least 5 minutes for the replication cycle and then check the databases' last data using command `/u/wandl/bin/mysql_repl.sh lastdata` on both primary and backup servers. If the lastdata values are equal, then the re-sync process was successful.
Chapter 8

Installing High Availability

The high availability feature uses computer clusters for providing fail over and high availability services of IP/MPLSView. High availability can be setup for the application and database servers. This chapter covers installation of the high availability package and walk through a sample environment where the high availability feature may be used.

When to Use

The high availability installation package can be used when IP/MPLSView services such as monitoring, data, and traffic collection are critical requirements in a Live network model. The figure below illustrates a sample high availability cluster environment for the application and database servers. AS1, AS2 are application servers; DB1, DB2 are database servers; DC is a data collector server; and Nge<n>, fi<n> are Ethernet and fiber optic ports respectively. This sample environment will be referenced for high availability setup and installation in this chapter.

Figure 11: High Availability Cluster Environment
Outline

- Prerequisites on page 82
- Software Configuration on page 82
- Cluster Setup on page 84
- Pre Installation Steps on page 85
- Pre Installation Checklist on page 87
- IP/MPLSView Installation on page 87
- Rsync Installation on page 97
- High Availability Installation on page 97
- Post Installation Checklist on page 97
- Starting IP/MPLSView on page 98
- Administration on page 100

Prerequisites

See Chapter 2, Installing IP/MPLSView for more information about the installation process for the application and database packages.

Solaris OS version 10 is recommended for installation on all the servers.

Each server in the cluster environment will need a separate license. Please contact your Juniper representative for information to obtain the license.

Software Configuration

San Storage Disk Partition

Active application and database servers save the data collected from the router network as well the processed data in the SAN disk. The data saved by application and database servers requires segregation on the storage disk. Hence the storage disk should be partitioned into two such that each will be accessible to a cluster group. Note that the partition that can be accessible to the application cluster group should not be accessible to the database cluster group and vice versa.

Sun Cluster Installation

Sun Cluster 3.2 standard package is recommended for installation on all application and database servers.

The servers should be configured with cluster groups such that both the application servers belong to one group and the database servers to another group. Standard (typical) configuration is recommended. All the servers that belong to a cluster group are supposed to have dedicated private interconnects connected either directly or through an Ethernet switch. Typically, if a cluster group involves only two nodes, then direct connections will be used.

The Data collector server does not need cluster installation because IP/MPLSView processes can detect failure on the active data collector and switch over the data collection process to a standby instance.
Note that Sun does not recommend to enable routing and NAT functionalities on the servers configured with clusters. Refer to Sun Documents for more details.

Mount external SAN storage disk

Mounts should be created from each cluster server to that partition on the external storage disk that can be accessed by the cluster group and reserved for saving the data.

Creating the mount point from one server in the cluster group automates the creation of mount point on all other servers in the group. Make sure that the mount entry is created in the directory /etc/vfstab of each cluster server such that the mount is not lost when a server in the group is rebooted.

Note that the mount point will be lost when all the servers in the cluster group are shut down at the same time. Hence as a precautionary step, it is advised not to shut down both the servers simultaneously. If the servers were shut down simultaneously by accident, make sure that the mount point is created manually after the servers reboot.

IPMP Configuration

IP Multipath configuration should be done on all the public interfaces of application and database servers that connect to the router network. Public interfaces of the application server cluster should belong to one group and public interfaces on the database server cluster in another group.

IP Multipathing does failure monitoring and recovery on the interfaces that are configured with ipmp groups. As the public interfaces on the servers will be configured with IP addresses, probe-based monitoring mechanism will be used. In this method, IPMP sends continuous ICMP probes to the gateway IPs present in the server’s routing table (netstat –rn) for failure detection. When adding any static routes on the ipmp configured servers, verify “ping” from the server to the gateway IP succeeds.

When ipmp reports all the interfaces on the active server as failed, the cluster switches over to the standby server since the cluster interprets the server that is currently active cannot be remotely accessible due to interface failures reported by ipmp. Thus ipmp configuration is required even if a server has one public interface.

In the illustrated sample environment see Figure 11, each server consists of two public interfaces for resiliency purposes connected to the Ethernet switch that in turn connects to the router network. On each cluster server, one interface, usually the loghost interface in the /etc/hosts file, is configured as the primary ipmp interface and another one as standby interface as shown below:

Primary interface configuration:

```
ifconfig <interfacename> group <ipmp_group_name> up addif <ipmp_testIP_nge0> deprecated -failover netmask + broadcast + up
```

Edit /etc/hostname.<interfacename> file to retain the ipmp configuration upon server reboot:

```
<nodename> group <ipmp_group_name> up addif <ipmp_testIP_nge0> deprecated -failover netmask + broadcast + up
```

Standby interface configuration:

```
ifconfig <interfacename> group <ipmp_group_name> up addif <ipmp_testIP_ngel> deprecated -failover netmask + broadcast + standby up
```
Edit /etc/hostname.<interfacename> file to retain the ipmp configuration upon server reboot:

```
<ipmp_testIP_nge1> netmask + broadcast + deprecated group <ipmp_group_name>
-failover standby up
```

When the primary ipmp interface fails on a server, then ipmp routes the traffic of all applications that use primary interface’s IP through the standby interface. Although IP/MPLSView uses the primary loghost interface’s IP for running most of the processes, the processes should run seamlessly even if the primary interface fails through ipmp configuration.

## Cluster Setup

The following diagram shows how the cluster is setup in the sample environment. The installation script messages in this chapter uses this high availability cluster configuration.

**Figure 12: Sample Cluster Setup**

- Application Cluster IP is 7.7.7.7
- Application Primary Server IP is 7.7.7.1
- Application Backup Server IP is 7.7.7.2
- Database Cluster IP is 8.8.8.8
- Database Primary Server IP is 8.8.8.1
- Database Backup Server IP is 8.8.8.2
Pre Installation Steps

Configure Shared IP Addresses and Nodenames

Sun cluster introduces the concept of a shared IP address and shared node name that correspond to the resource group. These shared IP and node names are different than each node’s IP and node name values. Every node in a resource group should be assigned with this shared IP address and nodename. The definition of a resource group will be explained in the next section.

In the context of IP/MPLSView-HA, primary and backup application servers belong to a resource group and thus share a common shared IP and nodenames. The same applies for primary and backup database servers. IP/MPLSView accesses the server using this shared IP address on application server and the Sun cluster has internal mapping mechanism that directs the packets to the active member in the resource group. Hence shared IP and nodenames keeps the client or end user unaware of server switchover and eliminates the hassle of changing server IP addresses every time there is a server switchover.

Configure the shared IP and nodenames on each server by creating an entry in the /etc/hosts file. It is recommended to add both application and database servers shared IP and nodenames on all the servers.

Create Resource Groups and Assign Nodes

Resource group is a selected group of nodes in a cluster. In the context of high availability, these groups are created to define the scope of failover. Sun cluster picks up one of the nodes in the resource group as the owner of the group and continuously monitors several resources on it for its failure detection. When the cluster detects a failure on the owner, then the ownership will be switched over to other node in the group and so forth.

The following command is used to create a resource group and assign nodes to it:

```
#/usr/cluster/bin/clrg create -p nodelist=<clusternodename1>,<clusternodename2> <resourcegroupname>
```

Sun cluster treats the first node defined in the nodelist as the owner of the group by default. The node names defined are Sun cluster node names. Use the command, ‘clnode list’ to get a list of all nodes that are defined in a cluster.

In IP/MPLSView-HA setup, two resource groups have to be created, one for application servers, with a fixed IP/MPLSView reserved name MPLSView-harg and another for the database servers, with a fixed IP/MPLSView reserved name, MPLSDB-harg. Note that the resource group names are fixed as IP/MPLSView-HA software functions correctly only with these fixed names.

Note that any cluster related command can be run as root user only. While logging in as root, login as "su -" so that you don’t have to type the absolute path of the command.

Run the following command as root user on any application server to create resource group for application servers and assign nodes to the group.

```
#/usr/cluster/bin/clrg create -p nodelist=<AppServClustNodeName1>,<AppServClustNodeName2> MPLSView-harg
```

Run the following command as root user on any database server to create resource group for database servers and assign nodes to the group.

```
#/usr/cluster/bin/clrg create -p nodelist=<DBServClustNodeName1>,<DBServClustNodeName2> MPLSDB-harg
```
The cluster treats the first node in the nodelist as the owner of the resource group. The owner can be changed with the following command:

```
#/usr/cluster/bin/clrg switch -n <NewActiveNode> <ResourceGroupName>
```

### Create Application and Database Data Directories on External Storage Disk

Two directories should be created on the external storage disk that represent the physical locations of the data directories on application and database servers. During IP/MPLSView installation on application and database servers, you should enter the respective data directories (absolute path) created on the external storage so that the installation script creates a symbolic link `/u/wandl/data` on the local server that will point to the directories on the common storage disk.

### Automate SSH Login from Database Servers to Application Servers

Follow the steps below on the primary and backup database servers to automatically log in using SSH to the application servers. Automatic login is required for the database servers to rsync the aggregated traffic data to the application servers.

Note that this is a one time procedure and does not need to be run every time the software is upgraded unless any changes to the server’s passwords or IP addresses take place.

1. Login as ‘wandl’ user on the primary data base server and switch the current directory to the IP/MPLSView home directory. For the example below, the home directory will be `/export/home/wandl`. Generate a pair of authentication keys. Do not enter a passphrase:

   ```
   /export/home/wandl> ssh-keygen -t rsa
   Generating public/private rsa key pair.
   Enter file in which to save the key (/export/home/wandl/.ssh/id_rsa):
   Created directory '/export/home/wandl/.ssh'.
   Enter passphrase (empty for no passphrase):  
   Enter same passphrase again:
   Your identification has been saved in /export/home/wandl/.ssh/id_rsa.
   Your public key has been saved in /export/home/wandl/.ssh/id_rsa.pub.
   The key fingerprint is:
   ```

2. Now use SSH to create the directory `.ssh` on the primary application server. Substitute `<remotehostip>` below with the primary application server’s IP. Enter ‘yes’ when prompted to continue connecting. Enter the remote host’s IP/MPLSView password when prompted.

   ```
   /export/home/wandl> ssh wandl@<remotehostip> mkdir -p .ssh
   The authenticity of host '<remotehostip>' (192.168.1.2) can't be established.
   RSA key fingerprint is 8a:da:9a:9c:59:1e:fa:73:3c:9f:00:8f:fa:ef:80:0b.
   Are you sure you want to continue connecting (yes/no)? yes
   Warning: Permanently added '<remotehostip>' (RSA) to the list of known hosts.
   Password:
   ```

3. Append the local host’s new public key to the primary application server’s authorized keys and enter the primary application server’s IP/MPLSView password one last time.

   ```
   /export/home/wandl> cat .ssh/id_rsa.pub | ssh wandl@<remotehostip> 'cat >> .ssh/authorized_keys'
   ```

```
```
Password:

4. Repeat steps 2 and 3 on the primary database server replacing <remotehostip> with the backup application server’s IP

5. Repeat steps 2, 3, and 4 on the backup database server

Test the automatic login setup by logging in to application servers from database servers and check if that allows direct login without a password.

Pre Installation Checklist

Before installation verify the following items in the checklist. Make sure the items are verified on all the servers.

- Check the cluster status of the servers by running /usr/cluster/bin/scstat. Verify the servers in the same cluster group are listed under “Cluster Nodes” and “Device Group Servers” and “Device Group” status displays online; resource groups and the nodes assigned to them are listed under “Resource Groups” section; and IPMP configured interfaces in a cluster group are listed under “IPMP Groups” section

- Check the resource group status of the servers by running clrg status. Verify the application servers are listed under “MPLSView-harg” and the database servers under “MPLSDB-harg”. Verify the nodes are not in a suspended state. Below is an example of the application server cluster.

```
# /usr/cluster/bin/clrg status
=== Cluster Resource Groups ===
Group Name         Node Name      Suspended     Status
----------         ---------      ---------     -----
MPLSView-harg      walnut         No            Unmanaged
             peanut         No            Unmanaged
```

- Primary and backup application and database servers should have the same login/password for both root and IP/MPLView users.
- SSH services should be enabled on the application and database servers
- Each database server should log in using SSH to both the application servers without having to enter the password

IP/MPLSView Installation

IP/MPLSView Installation on Application Server

IP/MPLSView Installation steps are the same on primary and backup application servers. Perform the following installation steps on the primary application server and repeat the same steps on the backup application server.

On each application server go to the server directory in the installation package and run the install.sh script. Do the installation as you would do for standard IP/MPLSView installation. Reasons to change the default values are explained as a note below each section.

```
root@walnut # cd /cdrom/cdrom0/server
root@walnut # ./install.sh
```
Please read the Getting Started document before installing this software.

Note that you can stop the installation at any time using <Ctrl>-c.

Which version would you like to install?
1) 32-bit
2) 64-bit
(1:32-bit (default) 2:64-bit): 1
Note: Select the version that applies to your environment.

Preparing to install IP/MPLSView ...

We have determined that the Solaris Server Management Facility is running on this machine. If you have configured IP/MPLSView to be managed by this, then please quit the installation and disable the IP/MPLSView entry in the Solaris Server Management Facility before restarting the IP/MPLSView installation. If IP/MPLSView is not configured (or is already disabled) in the Solaris Server Management Facility, then please ignore this message and continue with the installation.

Continue with installation (default=yes)? [y/n]

Checking Sun Solaris patches ...

This software requires a UNIX ID as the owner.

A UNIX ID is the login name when you login to this UNIX server. Please input the IP/MPLSView user ID (wandl):

Owner is set to: wandl

You should have a group created for all the users who will use this program (a group may have only one member, if only one person uses this program)

The installation script will assign the right permissions for the Users of this group to use, update and maintain the programs.

Please input group ID (staff):

Group is set to: staff

Please enter the directory where this software will be installed.
(default=/export/home/wandl/ipmplsview):
/export/home/wandl/ipmplsview

Checking available disk space ...
Please enter the directory where the data will be stored.
(default=/export/home/wandl/wandldata): /global/Storage/AppData

**Informational Note:** Data inside /u/wandl/data/ should be stored in an external storage device that is accessible to both the primary and backup application servers. By specifying the mounted external storage directory here /u/wandl/data will be linked to the specified directory.
Copying Java native library files...
Found an existing libjli.so in /usr/lib directory, owned by root, created on Jan 23 2009

Do you want to overwrite it [y]?

Switching user to "wandl" ...
Done!

General Settings:
1.) Installation Directory.......: export/home/wandl/ipmplsview
2.) Data Directory...............: /global/Storage/AppData
3.) Admin User..................: wandl
4.) Admin Group..................: staff
5.) Task Manager Primary Port..: 2099
6.) Task Manager Secondary Port: 2100
7.) Task Manager Memory........: 1G
8.) Server IP..................: 7.7.7.7
9.) Server Port..................: 7000
10.) SNMP Trap Daemon IP.........: 7.7.7.7
11.) SNMP Trap Daemon Port......: 162
12.) SNMP Trap Daemon Memory....: 256
13.) SNMP Trap Store Capacity...: 30
14.) DGS Memory................: 1G

JBoss Web Settings:
15.) Webserver IP.............: 7.7.7.7
16.) Webserver Port..........: 8091
17.) External Webserver IP:
18.) SSL Port...............: 8443
SSL Domain.......: Unknown
SSL Department..: Unknown
SSL Organization: Unknown
SSL Loc./City....: Unknown
SSL State/Prov..: Unknown
SSL Country.....: United States, us
19.) JNDI Port................: 1099
20.) JNDI-RMI Port...........: 1098
21.) JRMP Port...............: 5444
22.) JRMP Invoker Port.......: 5446
23.) AJP Port...............: 8009
24.) Classloader Port......: 8083
25.) JBoss Web Memory......: 1G

JBoss JMS Settings:
26.) JNDI Port..............: 1856
27.) JNDI-RMI Port..........: 4458
28.) JRMP Port..............: 4444
29.) JRMP Invoker Port.....: 4446
30.) Bi-Socket Primary Port.: 4457
31.) Bi-Socket Secondary Port.: 4459
32.) SSL Bi-Socket Primary Port.: 1100
33.) SSL Bi-Socket Secondary Port.: 21100
34.) JBoss JMS Memory.......: 1G

MySQL Settings:
35.) Database IP..........: 7.7.7.1
36.) Database Port......: 3333
37.) Database Memory.....: 512
38.) Distributed Database: YES  
Database IP........: 8.8.8.8  
Database Port.....: 3333  

Email Settings:  
39.) Email Server IP......: 7.7.7.1  
40.) Email Server User....: wandl  
41.) Email Server Password:  

Event Settings:  
42.) Event Post Port.....: 7077  
43.) Event Server Memory: 1G  
44.) Event AIM User:  
45.) Event AIM Password:  
46.) Event Gtalk User:  
47.) Event Gtalk Password:  
48.) Event Msn User:  
49.) Event Msn Password:  
50.) Event Yahoo User:  
51.) Event Yahoo Password:  

LDAP Server Settings:  
52.) LDAP Server IP.......: 7.7.7.1  
53.) LDAP Server Port.....: 3389  

Aggregation Settings:  
54.) Maximum Traffic Capacity in Days.......: 35  
55.) Aggregation Week Interval Divisor......: 6  
56.) Aggregation Number Days per Week......: 7  
57.) Aggregation Month Interval Divisor.....: 24  
58.) Aggregation Number Days per Month.....: 35  
59.) Aggregation Memory....................: 1G  
60.) Archive Traffic in MySQL Export Format: OFF  
61.) Compute Traffic Reference.............: OFF  

Application Monitor Settings:  
62.) Application Monitor Email Recipient...:  
63.) Application Monitor Memory............: 128  

Threshold Server Settings:  
64.) Threshold Server Memory..............: 512  

SNMP Trap Forwarder Settings:  
65.) Enable Trap Forwarder.................: OFF  
66.) Upstream Address....................:  
67.) Upstream Port.......................:  

Advanced Options:  
68.) Enable NAT access for JMS..............: OFF  
69.) Network Event Storage Capacity........: 30  

Please select a number to modify.  
[<CR>=accept, q=quit]: 8  
8 selected!  
Current Server IP Address: 7.7.7.1  
Please enter a new Server IP Address: 7.7.7.7  
Changing Server IP Address from '7.7.7.1' to '7.7.7.7'
Informational Note: The IP addresses that will be involved in client-server interaction have to be changed to the shared IP address of the application servers. This way the client will be ignorant of server switchovers. Thus change setting ‘8’ Server IP to shared IP address.

Please select a number to modify.
[<CR>=accept, q=quit]: 10
10 selected!
Current SNMP Trap Daemon IP Address: 7.7.7.1
Please enter a new SNMP Trap Daemon IP Address: 7.7.7.7
Changing SNMP Trap Daemon IP Address from '7.7.7.1' to '7.7.7.7'

Informational Note: The SNMP Trap Daemon IP address has to be changed to the shared IP address of the application servers.

Please select a number to modify.
[<CR>=accept, q=quit]: 15
15 selected!
Current Webserver IP Address: 7.7.7.1
Please enter a new Webserver IP Address: 7.7.7.7
Changing Webserver IP Address from '7.7.7.1' to '7.7.7.7'

Informational Note: Change setting ‘15’ Webserver IP Address to Application servers’ shared IP address.

Please select a number to modify.
[<CR>=accept, q=quit]: 38
38 selected!
Use Distributed Database (default=no)? [y/n]: y
Current Distributed Database IP Address: 7.7.7.1
Please enter a new Distributed Database IP Address: 8.8.8.8
Changing Distributed Database IP Address from '7.7.7.1' to '8.8.8.8'
Current Distributed Database Port: 3333
Please enter a new Distributed Database Port:
No changes were made...

Informational Note: In a distributed database setup where the database will run on a different server from application server, change setting ‘38’ to set the distributed database IP address to the databases’ shared IP. If database server will run on the same machine as application server, then change setting ‘35’ to the application servers’ shared IP.

Please select a number to modify.
[<CR>=accept, q=quit]:

Accept these values (default=no)? [y/n] y
Install Client (default=yes)? [y/n] n

You may install the Client on Solaris86 systems by running /cdrom/cdrom0/client/solaris_86/install.client.

Install Data Collector (default=yes)? [y/n]

**Informational Note:** Choose ‘n’ on the primary application server and ‘y’ on the backup application server because the backup application server will acts as the backup data collector server.

Install Rsync & Database Replication Package (default=no)? [y/n]

You may install the Rsync & Database Replication Package by running /cdrom/cdrom0/replication/instrepl.sh

Extracting server files (This may take some time) .................. Done!

Installing webserver ... Done!

Creating database files for installation...Done.

Creating database tables ... Done!

Creating symbolic links ... Done!

Creating event repository ... Done!

Installing data collector ...

crontab added successfully.

Done!

Configuration file:
'/export/home/wandl/ipmplsview/bin/mplsenvsetup.sh' was created on Wed Nov 11 11:49:04 EST 2009

Creating Webserver configuration files ... Done!

Creating Diagnostics configuration files ... Done!

Creating Event Model configuration files ... Done!

Creating Traffic Summary configuration files ... Done!

Creating DGS configuration files ... Done!

Creating Event Server configuration files ... Done!

Creating Monitor configuration files ... Done!

Creating IP/MPLSView Application Monitor configuration files ...

Done!
Creating Task Manager configuration files ... Done!

Creating database files ... Done!

Creating LDAP files ... Done!

Initializing LDAP directory ... Done!

Creating Data Collector configuration files ... Done!

Give JAVA Applets write-permission (default=no)? [y/n] y

You may start the Data Collector by running the following commands:
cd /export/home/wandl/ipmplsview/dcollect
./dc.sh start 0

Successfully created a symbolic link from /u/wandl to
/export/home/wandl/ipmplsview.

Please copy your license file to /u/wandl/db/sys/npatpw.
If you do not have a license file, please contact Juniper support.
After activating the software, you may start the IP/MPLSView server
by running the following command:
/u/wandl/bin/startup_mplsview

Informational Note: If IP/MPLSView is installed on the server for the first time, then the
license file has to be copied to /u/wandl/db/sys/ directory after installation. The above
installation block displays when IP/MPLSView is installed for the first time. If
IP/MPLSView installation is performed on a server that has a previous installation, then
the install script automatically copies the license file to the new installation directory, and
there would be a slight change in the installation messages.

You may start up the IP/MPLSView server by running the following command:
/export/home/wandl/ipmplsview/bin/startup_mplsview
Start up the IP/MPLSView server (default=yes)? [y/n] n

Informational Note: It is important to choose ‘n’ and not start the application server. By
default ‘y’ the script starts the application after installation. For the primary application
server, IP/MPLSView has to be started only after the primary database is started. Also the
startup command for high availability installation is different from the standard
/u/wandl/bin/startup_mplsview because the application has to be started inside the
cluster. For the backup application server, IP/MPLSView should not be started.

IP/MPLSView Installation on Database Server

The installation procedure is the same for primary and backup database servers. Perform
the following installation steps on the primary database server and repeat the same steps
on the backup database server.

Installations on both the primary and backup servers for database and application should
be done one after another and not simultaneously because the installation process
accesses and writes the same files in the external storage disk. Running simultaneous
installations may corrupt the files.
In the installation package directory, open the server directory and run instdatabase.sh. Run the installation as you would run standard installation. Reasons to change the default values are explained as a note below each section.

```
root@walnut # cd /cdrom/cdrom0/server
```

```
bash-3.00# ./instdatabase.sh
```

Please read the Getting Started document before installing this software.

Note that you can stop the installation at any time using <Ctrl>-c.

Which version would you like to install?
1) 32-bit
2) 64-bit
(1:32-bit(default) 2:64-bit):
Preparing to install IP/MPLSView Database ...

We have determined that the Solaris Server Management Facility is running on this machine. If you have configured IP/MPLSView Database to be managed by this, then please quit the installation and disable the IP/MPLSView Database entry in the Solaris Server Management Facility before restarting the IP/MPLSView Database installation. If IP/MPLSView Database is not configured (or is already disabled) in the Solaris Server Management Facility, then please ignore this message and continue with the installation.

```
Continue with installation (default=yes)? [y/n]
```

This software requires a UNIX ID as the owner.

A UNIX ID is the login name when you login to this UNIX server
Please input the IP/MPLSView Database user ID (wandl):

```
Owner is set to: wandl
```

You should have a group created for all the users who will use this program (a group may have only one member, if only one person uses this program)
The installation script will assign the right permissions for the users of this group to use, update and maintain the programs.
Please input group ID (staff):

```
Group is set to: staff
```

Please enter the directory where this software will be installed.
(default=/export/home/wandl/ipmplsview): /export/home/wandl/ipmplsview

Please enter the directory where the data will be stored.
(default=/global/Storage/DBData): /global/Storage/DBData

```
Switching user to "wandl" ...
```

```
Done!
```

General Settings:

**Informational Note:** Data inside /u/wandl/data/ should be stored in an external storage device that is accessible to both the primary and backup database servers. By specifying the mounted external storage directory here /u/wandl/data will be linked to the specified directory.
Installing High Availability

1.) Installation Directory.....: /export/home/wandl/ipmplsview
2.) Data Directory.............: /global/Storage/DBData
3.) Admin User..................: wandl
4.) Admin Group................: staff

MySQL Settings:
5.) Database Port..: 3333
6.) Database Memory: 256

Aggregation Settings:
7.) Maximum Traffic Capacity in Days......: 35
8.) Aggregation Week Interval Divisor.....: 6
9.) Aggregation Number Days per Week......: 7
10.) Aggregation Month Interval Divisor....: 24
11.) Aggregation Number Days per Month.....: 35
12.) Aggregation Memory....................: 256
13.) Archive Traffic in MySQL Export Format: OFF
14.) Compute Traffic Reference.............: OFF

Please select a number to modify.
[<CR>=accept, q=quit]:
Accept these values (default=no)? [y/n] y

Checking available disk space ...

Install Rsync & Database Replication Package (default=no)? [y/n]

You may install the Rsync & Database Replication Package by running
/export/home/wandl/ipmplsview/instrepl.sh

Extracting database files (this may take some time)............. Done!

Creating database files for installation...Done.

Creating database tables ... Done!

Configuration file:
'/export/home/wandl/ipmplsview/bin/mplsenvsetup.sh' was created on Wed Nov 11
12:00:51 EST 2009

Creating database files ... Done!

Do you want to set up aggregation replication? [n]:

The symbolic link /u/wandl does not exist.

Do you want to create this link as the root user? (Yes) [Y/N]

You may start up the database server by running the following command:
/export/home/wandl/ipmplsview/bin/startup_mplsview
Start up the database server (default=yes)? [y/n]n

Informational Note: It is important to choose ‘n’ and not start the database server. By default ‘y’ the script starts the database after installation. The command to start IP/MPLSView with high availability cluster is different from the standard
/u/wandl/bin/startup_mplsview.
IP/MPLSView Installation on Data Collector

This installation is required when the data collectors are run on a different machine from the application server. Go to dcollect directory and then the relevant OS directory in the installation package and run install.dcollect.

```
root@walnut # cd /cdrom/cdrom0/dcollect/unix/

wandl@poweredge1 /dcollect/solaris86> ./install.dcollect
```

Please enter the root directory where this software will be installed
(default=/u/wandl)

Extracting files, This may take a few seconds
PLEASE WAIT..............

******************************************************************************
A directory for storage of incoming router data is required and this directory should be outside the Data Collector installation location. The directory specified will then be soft-linked to the Data Collector install directory under dcollect/bulkstats.
******************************************************************************

Please enter the directory for incoming BulkStats traffic data
(default=/export/home/wandl/wandldata/bulkstats): 

Is /export/home/wandl/wandldata/bulkstats correct [Y/N] (Y)?

Creating BulkStats directory under /export/home/wandl/wandldata/bulkstats ....

Creating soft-link ... to /u/wandl/dcollect/bulkstats

Copying Files ...

For this part of the installation, you need to supply the name of the server to which you are connecting (default is the local machine) and the port number for communication (default is 7000). If you don't know this information, ask the person who installed the server portion of the software, or just take the defaults. You will always have the chance to change them by editing the appropriate /u/wandl/dcollect/dcconfig_wandl_<N>.xml file.

```
The "-h <appl server IP addr>" option may also be used to override the settings in the dcconfig_wandl_<N>.xml file.
```

Please supply the name or IP address of the JMS server [ 7.7.7.1 ] 7.7.7.7

Note: The IP address must be pointing to the shared IP address of the application server.

Please supply the JNDI Port [ 1856 ]

crontab added successfully.

**Informational Note:** Once the data collector is started subsequent changes to the dcconfig xml file will have no effect until that data collector is stopped and restarted.
********** INSTALLATION COMPLETE **********

You may start the Data Collector by running the following command:
/u/wandl/dcollect/dc.sh start 0

Rsync Installation

Rsync installation should be done on the application and database servers only. Installation of rsync is only a one time setup and does not need to be installed every time IP/MPLSView is upgraded unless explicitly mentioned.

root@walnut # cd /cdrom/cdrom0/replication
bash-3.00# ./inst_rsync.sh

Installation of <SMClgcc346> was successful.

Installation of <SMCliconv> was successful.

Installation of <SMClintl> was successful.

Installation of <SMCpopt> was successful.

Installation of <SMCrsync> was successful.

High Availability Installation

High availability cluster installation has to be done after standard IP/MPLSView installation on the application and database servers only. The cluster installation script creates a cluster directory under /u/wandl and creates log files under /var/cluster/logs/.

The installation steps for the cluster are the same on all the servers. In the installation package go to the cluster directory and run the inst_ha_cluster.sh script.

root@walnut # cd /cdrom/cdrom0/cluster
bash-3.00# ./inst_ha_cluster.sh

This script will install Sun Cluster support file for IP/MPLSView, do you wish to continue? [y/n]: y

The installation directory was detected as '/export/home/wandl/ipmplsview', is this correct? (default=yes)? [y/n]

Installation of <MPLSView> was successful.

Installation for Sun Cluster support files finished successfully.

Post Installation Checklist

Verify the following items in the checklist after installation and proceed to the next steps only if all the items are verified.

1. On database servers verify the data directory is pointing to the correct physical location on the external storage device by running /u/wandl/bin/changeconfig.sh. If the directory is pointing to incorrect location, change it here.

# /u/wandl/bin/changeconfig.sh

Reading configuration settings from /u/wandl/bin/mplsenvsetup.sh ... Done!

General Settings:
1.) Installation Directory......: /u/wandl
2.) Data Directory.............: /global/Storage/DBData
3.) Admin User..................: wandl
4.) Admin Group................: staff

2. On application servers verify the data directory is pointing to the correct physical location on the external storage device and the IP addresses of the highlighted server processes are set to the right shared IP addresses by running 
   /u/wandl/bin/changeconfig.sh. If any values are incorrect, they can be changed here.

   # /u/wandl/bin/changeconfig.sh
   Reading configuration settings from /u/wandl/bin/mplsenvsetup.sh ... Done!

   General Settings:
   1.) Installation Directory.....: /u/wandl
   2.) Data Directory.............: /global/Storage/AppData
   3.) Admin User...............: wandl
   4.) Admin Group..............: staff
   5.) Task Manager Primary Port.: 2099
   6.) Task Manager Secondary Port: 2100
   7.) Task Manager Memory.......: 256
   8.) Server IP................: 7.7.7.7
   9.) Server Port...............: 7000
   10.) SNMP Trap Daemon IP.......: 7.7.7.7
   11.) SNMP Trap Daemon Port.....: 162
   12.) SNMP Trap Daemon Memory...: 128
   13.) SNMP Trap Store Capacity..: 30
   14.) DGS Memory...............: 256

   JBoss Web Settings:
   15.) Webserver IP.........: 7.7.7.7
   16.) - 25.)

   JBoss JMS Settings:
   26.) - 34.)

   MySQL Settings:
   35.) Database IP.........: 7.7.7.1
   36.) Database Port.......: 3333
   37.) Database Memory.....: 256
   38.) Distributed Database: YES

   Database IP.........: 8.8.8.8
   Database Port.......: 3333

   Please select a number to modify.
   [<CR>=accept, q=quit]:

Starting IP/MPLSView

The commands in this section starts IP/MPLSView as a cluster service.

Starting Database Server

Run the following command on any database server. The command starts the database process in the cluster service. Database process starts on the owner in the resource group.

   #/u/wandl/cluster/WANDLMPLSView/util/startMPLSView –h <DBServClusterNodeName>

   No nafo groups or network adapters specified ... will try to auto-discover the network adapters and configure them into nafo groups.
   Creating a failover instance ...
   Resource type <SUNW.gds:6> has been registered already
   Resource group <MPLSDB-harg> already exists
   Creating logical host resource <DBServClusterNodeName>...done.
   Creating resource <MPLSDB-harg> for the resource type <SUNW.gds:6>...done.
   Bringing resource group <MPLSDB-harg> online...done.
Installing High Availability

Starting Application Server

Before starting the application server, verify the license file `npatpw` is copied to `/u/wandl/db/sys/` directory on both the application servers. Run the following command on any application server. The command starts the application process on the owner in the resource group.

```
#/u/wandl/cluster/WANDLMPLSView/util/startMPLSView -h <AppServClusterNodeName>
```

Creating a failover instance ...

No nafo groups or network adapters specified ... will try to auto-discover the network adapters and configure them into nafo groups.

Creating logical host resource `<AppServClusterNodeName>`...done.

Creating resource `<MPLSView-hars>` for the resource type `<SUNW.gds:6>`...done.

Bringing resource group `<MPLSView-harg>` online...done.

This completes the high availability installation process and IP/MPLSView processes should be up and running. Run the clrg status command to check the status of the active application and database servers. Run `/u/wandl/bin/status_mplsview` on the active servers to check the status of IP/MPLSView processes.

Starting Rsync Cronjob on Database Servers

The database server aggregates the traffic collected for the day at the end of each day and saves it in IP/MPLSView object format files. Rsync needs to be installed and configured to replicate these files from database server to application server as cronjob. The following script configures the cronjob.

Run the script `inst_agg_rsync.sh` on each database server as shown below. Note that running this script is a one time step and is not needed every time IP/MPLSView is upgraded unless explicitly instructed.

```
wandl@lexus /u/wandl/bin> ./inst_agg_rsync.sh
```

Please enter the complete path of rsync `/usr/local/bin/rsync`

This script will generate replication scripts and schedule a task in the crontab, do you wish to continue? [n]:y

The installation directory was detected as `/export/home/wandl/ipmplsview, is this correct? (default=yes)? [y/n]`

```
[1] Add a target server
[2] Remove a target server
[3] Show current targets
[4] Regenerate script files
[5] Quit
```

Please enter your selection: 1

[Add server selected]

Please enter
IP address of the target server: 7.7.7.7
Remote IP/MPLSView product home directory [/u/wandl]:

Informational Note: It is important to start the database server before the application server, otherwise the DGS process on the application server tries to establish a TCP connection to the database server and it fails.
Remote login ID associated with the SSH authorized key [wandl]:
Remote rsync installation path [/usr/local/bin/rsync]:
aggregation rsync script generated...

Settings for 7.7.7.7 saved successfully, press any key to continue...

[1] Add a target server
[2] Remove a target server
[3] Show current targets
[4] Regenerate script files
[5] Quit

Please enter your selection: 5

Administration

This section covers administrative commands for the servers in the high availability environment.

Check IP/MPLSView process status.
> /u/wandl/bin/status_mplsview

Check cluster resource status. In this example the active node name is "peanut".
# clresourcegroup status MPLSView-harg

=== Cluster Resource Groups ===

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Node Name</th>
<th>Suspended</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLSView-harg</td>
<td>peanut</td>
<td>No</td>
<td>Online</td>
</tr>
<tr>
<td>walnut</td>
<td>No</td>
<td>No</td>
<td>Offline</td>
</tr>
</tbody>
</table>

Switch over the active node in the cluster. In this example the new active node is "walnut".

# clresourcegroup switch -n walnut MPLSView-harg

Sun Cluster system logs can be found under /var/cluster/logs, IP/MPLSView cluster service specified nodes can be found under /var/cluster/logs/DS/MPLSView-harg/MPLSView-hars and /var/cluster/logs/DS/MPLSDB-harg/MPLSDB-hars. Note you need root user level to access those directories.

- **probe_log.txt**: Contains information about the IP/MPLSView service probe results.
- **start_stop_log.txt**: Contains information about startup and shutdown on cluster nodes.

The clsetup utility may be used to administer cluster functions as well.

# /usr/cluster/bin/clsetup

*** Main Menu ***

Please select from one of the following options:

1) Quorum
2) Resource groups
3) Data Services
4) Cluster interconnect
5) Device groups and volumes
6) Private hostnames
7) New nodes
8) Other cluster tasks
?) Help with menu options
q) Quit

Application Server Administration

Start and register IP/MPLSView application server as cluster service with root user assuming logical hostname resource is “mplsh”.

# /u/wandl/cluster/WANDLMPLSView/util/startMPLSView -h mplslh

Stop IP/MPLSView on the application server
#/u/wandl/cluster/WANDLMPLSView/util/stopMPLSView –h <AppServClusterNodeName>

Stop Resource group on application server.

Informational Note: For the logical host names it has to exist in the /etc/hostsfile on all cluster nodes before you start and register the cluster resource using that logical host name as a dependency.

Database Server Administration

Start and register IP/MPLSView database server as cluster service with root user assuming logical hostname resource is “mplsdblh”.

#/u/wandl/cluster/WANDLMPLSView/util/startMPLSView -h mplsdblh

Stop IP/MPLSView on the database server
#/u/wandl/cluster/WANDLMPLSView/util/stopMPLSView –h <DBServClusterNodeName>

Stop Resource group on database server.

Informational Note: The service is still registered in Sun cluster.

Informational Note: The service is still registered in Sun cluster.

Delete the resource group on the application server:
# /usr/cluster/bin/clresourcegroup offline MPLSView-harg
# /usr/cluster/bin/clresource disable MPLSView-hars
# /usr/cluster/bin/clresource disable <SharedAppServNodeName>
# /usr/cluster/bin/clresource delete MPLSView-hars
# /usr/cluster/bin/clresource delete <SharedAppServNodeName>
# /usr/cluster/bin/clresourcegroup delete MPLSView-harg

Delete the resource group on the database server
# clresourcegroup offline MPLSDB-harg

Delete the resource group on the database server
#/usr/cluster/bin/clresourcegroup offline MPLSDB-harg
#/usr/cluster/bin/clresource disable MPLSDB-hars
#/usr/cluster/bin/clresource disable <SharedDBServNodeName>
#/usr/cluster/bin/clresource delete MPLSDB-hars
#/usr/cluster/bin/clresource delete <SharedDBServNodeName>
#/usr/cluster/bin/clresourcegroup delete MPLSDB-harg
Before using IP/MPLSView, you need to start up the IP/MPLSView server and connect to it from an IP/MPLSView client. The IP/MPLSView server software runs on a UNIX machine; the client software can run either on a UNIX machine or PC with Microsoft Windows. This chapter explains how to start up the server and connect to it with the client.

**Prerequisites**: Before starting the IP/MPLSView server or client, you should have installed them as described in Chapter 2, Installing IP/MPLSView.

### Overview

- Starting Up the IP/MPLSView Server on page 103
  - Launching IP/MPLSView Data Collector from UNIX on page 105
  - Launching IP/MPLSView Trap Daemon from UNIX on page 106
  - Launching the Event Server on page 106
  - Launching the Distributed Database from UNIX on page 106
- Launching the IP/MPLSView Client on page 107
  - Launching IP/MPLSView Client on Solaris on page 107
  - Launching IP/MPLSView Client on Microsoft Windows on page 108
  - Launching IP/MPLSView Client using Web Start (Solaris & Windows) on page 108
- Logging In on page 110
- Related Documentation on page 111

### Starting Up the IP/MPLSView Server

#### License File

Before starting IP/MPLSView, contact Juniper support for the activation license file. To determine your hostid, type `hostid` and <Enter> at the prompt. The license file name should be changed to `npatpw` and moved to the `/u/wandl/db/sys` folder, or the `$WANDL_HOME/db/sys` folder. The license file can also be uploaded from the Web Interface to the application server and viewed from the Web Interface. This feature is available from the Web menu Admin > Administration > Upload License and Show License.

#### Server Commands

1. Log into the UNIX server as the IP/MPLSView admin user; the wandi user id is recommended when applicable. Once you have logged in, type:
2. Check if the IP/MPLSView-related servers are running using the `./status_mplsview` command. If they are not, then use the `./startup_mplsview` command to start the servers. The following table provides a summary of the commands to start up, stop, and determine the status of IP/MPLSView servers. Do not use root to startup the IP/MPLSView servers because this may lead to ownership and process conflicts.

Among the servers started should be the IP/MPLSView server and JBoss server (a Java web application server). The default port number for the IP/MPLSView server is 7000 and is used for communication between the server and client. When you startup IP/MPLSView, the IP/MPLSView data collection driver (wDriver) will also take port 7001.

3. If the default port is in use, you can start the server with another port number by using the command:

   ```bash
   $ ./startup_mplsview port_number
   ```

   where `port_number` is substituted with a valid unused port number. The IP/MPLSView data collection driver's port number will then be set to `port_number+1`.

<table>
<thead>
<tr>
<th>Command</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>status_mplsview</td>
<td>Type this command to check the status of the IP/MPLSView servers. This command displays IP/MPLSView process information for CPU/Memory usage, as well as any warnings or errors regarding the status of IP/MPLSView-related processes. The process information at the beginning of the status output can be used to fine-tune the server memory usage settings, which can be configured using <code>/u/wandl/bin/changeconfig.sh</code>. All errors here are fatal. They indicate that the server or the IP/MPLSView data collection driver is not running. Any warnings that are displayed at the end should warrant attention.</td>
</tr>
<tr>
<td>startup_mplsview [portnumber]</td>
<td>Type this command to start all the servers. The startup script will either confirm the startup process if the IP/MPLSView servers started successfully or provide error message(s) if the start server process has failed. Do not use root to startup the IP/MPLSView servers.</td>
</tr>
<tr>
<td>stop_mplsview</td>
<td>Type this command to stop all the servers. <strong>Note</strong>: This command will give the IP/MPLSView clients a minute's notice in which to save unfinished work.</td>
</tr>
</tbody>
</table>

**Setting Up the PATH Variable**

The user can optionally set up the PATH variable as a shortcut to access the commands located in `/u/wandl/bin` and `/u/wandl/client` folders from other directories without specifying the full path. The following commands can be placed in “$HOME/.profile”:

```bash
PATH=/u/wandl/bin:/u/wandl/client:$PATH
export PATH
```

To use the settings in the `.profile`, it can be executed as follows:

```bash
# . ~/.profile
```
Launching IP/MPLSView Data Collector from UNIX

The Data Collector should be started on the server if you wish to collect traffic data using the IP/MPLSView client.

To launch the data collector application, first switch to the directory where the data collector is installed (for example, /u/wandl/dcollect) and then execute the dc.sh command. Enter:

```
$ cd /u/wandl/dcollect
$ ./dc.sh start instance#
```

where `instance#` can be any positive integer representing the instance number of the collector that is being started. There can be more than one instance of the data collector running at once on the same server or on other servers. You should see some messages like the following:

```
Trying to start using pid=8608
Data Collector (pid=8608) Started.
```

If a data collector is on a different machine than the main IP/MPLSView application server, specify the IP address of the application server using the `-h` option:

```
$ ./dc.sh start instance# -h host_ip_address
```

Multiple `instance#` can also be started in sequence using a comma or a number range.

The following example starts instance 2, 3, 5, and 7.

```
$ ./dc.sh start 2,3,5,7
```

The following example starts instance 0, 1, 2, 3, 4, and 5 inclusive.

```
$ ./dc.sh start 0-5
```

Run the following command to see the status of the collector:

```
$ ./dc.sh status
Found collector instance wandl_0 with pid=8608 (running)
Found collector instance wandl_1 with pid=8628 (running)
```

where “wandl_#” represents the instance identifier of that data collector. (Here, “wandl” represents the user id that started the data collector.) Afterward, you can specify what to collect using the Traffic Collection Manager in an IP/MPLSView client. The client can be on a different machine.

To stop a specific data collector instance, enter the following:

```
./dc.sh stop instance#
```

To stop all data collector instances, enter the following:

```
./dc.sh stop all
```
If an instance is having difficulty stopping, you may force a shut down using -f flag.

```
./dc.sh -f stop instance#
```

Launching IP/MPLSView Trap Daemon from UNIX

When running startup_mplsview or stop_mplsview, you may be asked to stop or start the SNMP trap server. The SNMP trap server is used for the online Fault Management module. Refer to the Management and Monitoring Guide chapter, “Fault Management,” for more details.

The SNMP Trap Daemon can also be manually started on the server if you wish to view traps using the IP/MPLSView client, such as through the event browser.

To launch the trap daemon, first switch to the bin directory of where IP/MPLSView is installed (for example, /u/wandl/bin) and then execute the .snmptrap command. E.g.,

```
$ cd /u/wandl/bin
$ ./.snmptrap start
```

You should see the following message:

```
SNMP trap daemon started on port 162
```

To stop the trap daemon, first stop the application monitor if it is enabled. Otherwise the application monitor may detect that the SNMP trap server is down, and automatically restart it.

```
$ ./appmonitor stop
```

Then enter the following:

```
./.snmptrap stop
```

Launching the Event Server

Note that the event server will automatically be started up using the startup_mplsview command in /u/wandl/bin. However, if you need to manually stop and restart it, the following commands can be used:

```
$ cd /u/wandl/bin
$ ./appmonitor stop
$ ./eventserver stop
$ ./eventserver start /u/wandl/db/config/eventserver.xml
$ ./appmonitor start
```

By default, the event server will only display application events. In order to also display SNMP trap events, the trap daemon should also be started as explained in Launching IP/MPLSView Trap Daemon from UNIX on page 106.

Launching the Distributed Database from UNIX

In most cases, the database will be installed with the IP/MPLSView server. If so, starting up the IP/MPLSView server will also start up the database. However, if the database is installed on a different machine from IP/MPLSView, switch to the bin directory of where the distributed database is installed. (for example, /u/wandl/bin).

To startup up the database, enter:

```
$ startup_mplsview
```
To shut down the database, enter:

$ stop_mplsview

**Restarting Task Server**

Under special circumstances, it may be desirable to stop and restart the Task Server only, without taking down other processes. Again, the application monitor should be stopped beforehand, so that it does not automatically restart the Task Manager when it sees that it is down.

To stop the Task Server process, use the following commands:

$ cd /u/wandl/bin
$ ./appmonitor stop
$ ./tmng stop

To restart the Task Server process, use the following commands:

$ cd /u/wandl/bin
$ ./tmng
$ ./appmonitor start

**Launching the IP/MPLSView Client**

**Launching IP/MPLSView Client on Solaris**

1. To start the JAVA client in Solaris, enter the following commands:

   $ cd /u/wandl/client
   $ ./ipmplsview

   The IP/MPLSView login screen should appear.

2. To connect to a different server or to connect using a different port number, enter the following command from /u/wandl/client:

   $ ./ipmplsview [server_host port_number]

   with the proper substitution for server_host and port_number. Note that if you specify a hostname for server_host, you will need to edit the /etc/hosts file. If you specify an IP address for server_host, this extra step will not be necessary.

   Alternatively, you may edit the ipmplsview file.
Launching IP/MPLSView Client on Microsoft Windows

1. If you want to run the JAVA client on a Windows PC, double-click the desktop icon that says “IP-MPLSView Client”. The IP/MPLSView login screen should appear.

![IP/MPLSView Login Window](image)

Figure 13: IP/MPLSView Login Window

2. Select “Login as a view only mode user” only if you wish to use a viewer license instead of a full user license, to reserve the full user license for another session. Clicking the “i” button will indicate how many licenses are currently in use. (Note that a license is not in use until after opening a network project.)

3. If you lose your shortcut icon, you can also double-click the ipmplsview.bat file in the directory where you installed IP/MPLSView (by default, C:\Program Files\wandl\IP-MPLSView). You can also open a DOS window (click on Start Menu>Run and type “cmd” or “command” next to where it says, “Open”). If you switch (using the cd command) to the directory where you installed IP/MPLSView, you can type “ipmplsview” at the prompt to start the program.

4. To change the server, edit the SERVER variable in the ipmplsview.bat file. You can do this directly from the desktop icon by right-clicking the desktop icon and using the Edit with Notepad or other similar menu option provided by your Windows operating system. If this option is not available, you may need to navigate to the installation directory to change the file. For Windows Vista or later, you may need to right-click on the directory to add edit permissions for your user from the Security tab, Edit button and remove the Read-only attribute from the General tab.

Launching IP/MPLSView Client using Web Start (Solaris & Windows)

Before launching the web start client, please make sure that Web Start has been set up. If it is not, you can follow the instructions described in Java Web Start Client Installation on page 21. Additionally, make sure that your client machine supports the same version of Java. Currently, the 6.1 release uses jre1.7.0_02.

Figure 14: IP/MPLSView Web Interface with Web Client Access
In the following window, you can configure several run-time parameters. An important option is how much memory is to be used by the client.

Figure 15: Server and WebServer selection and Client Memory Allocation
2. Click the Run button and the application files will be downloaded.

Figure 16: Application Files Downloading Window
3. If you see the warning as shown in Figure 17, you may ignore it. Just click the Start button and the IP/MPLSView application should be launched. In case of problems, please see the Troubleshooting section of this Getting Started Guide.
Changing the Client Language

The default language of the client software is English. To change languages, create a file called locale.txt in the local user's directory, that is, C:\Users\username\.java\com\wandl. Then edit the locale.txt file and add the corresponding code for the desired language. Changes take effect when the client software is launched.

<table>
<thead>
<tr>
<th>Code</th>
<th>Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>en_EN</td>
<td>English</td>
</tr>
<tr>
<td>zh_CN</td>
<td>Simplified Chinese</td>
</tr>
<tr>
<td>ch_TW</td>
<td>Traditional Chinese</td>
</tr>
<tr>
<td>ru_RU</td>
<td>Russian</td>
</tr>
</tbody>
</table>

Logging In

If there are still problems connecting, “ping” the server to make sure you have connectivity. If you do not have connectivity, please check that your client machine is on the same subnet as your server machine.

If you have connectivity, but still cannot log in, check to make sure that you have started up IP/MPLSView properly using the status_mplsview command on the server. If not, try running startup_mplsview again.

For logins other than the administrative user, check that appropriate privileges are given through the User Admin window, or via the /u/wandl/bin/addWandlUser.sh script. For more information, refer to Launching the User Administration Tool on page 117 and Performing User Administration from Text Mode on page 119.

1. When you launch the IP/MPLSView JAVA client, the login window will be displayed. You may enter your login and password (the same login and password as the account on the server from which IP/MPLSView was installed). Then press <Enter> or click Login.
2. Select one of the two access privileges (that is, Full-control, View Only). Users with “View Only” can view the reports and monitor the network (for online module), but have restricted ability for modification, simulation, and design.

3. The IP/MPLSView GUI starts up with the Start Page.

4. To close the client, select File > Exit. Then select “Yes”.

**Client Notice Message**

A Client Notice pop-up window can be enabled when launching the client to display a custom message to the software end user. This can be used to display Terms of Use or Legal Notices. To enable this feature, add the text file notice.txt in the directory /u/wandl/data/custom. An optional title message can be given to this pop-up window by adding an entry “title=title of notice” in the notice.txt file.

**Related Documentation**

The following are guides that you can refer to for further information on using IP/MPLSView. These documents are also available from IP/MPLSView’s Help menu.

<table>
<thead>
<tr>
<th>Book</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Guide</td>
<td>For instructions on performing IP/MPLSView user tasks with the JAVA™ Graphical User Interface, refer to the remainder of this guide.</td>
</tr>
<tr>
<td>Reference Guide</td>
<td>Contains detailed reference information about Graphical User Interface windows</td>
</tr>
<tr>
<td>Router Guide</td>
<td>Contains guides for features specific to router technologies</td>
</tr>
<tr>
<td>File Format Guide</td>
<td>Contains input file formats and explanations of output files.</td>
</tr>
<tr>
<td>Getting Started Guide</td>
<td>Provides instructions for the installation of IP/MPLSView as well as how to start up and log on to the server</td>
</tr>
</tbody>
</table>

For more specific documents, see the other documents in your /u/wandl/doc (or $WANDL_HOME/doc) directory.
Chapter 10

System Administration

The System Administration tool allows the IP/MPLSView administrator to control access and security settings for the Graphical Interface and Web Interface. With this tool, the administrator can change user privileges, update the message of the day, and modify login policy settings. Please refer to the "User Administration Tool" chapter of the Reference Guide for information on the more advanced tasks.

Outline

- Setting Up Port Forwarding for Secure Communications on page 113
- Launching the Web Interface on page 117
- Launching the User Administration Tool on page 117
- Setting up a Connection to the Router Network on page 120
- Tuning Solaris Systems on page 122

Setting Up Port Forwarding for Secure Communications

Port forwarding can be used to set up SSH Tunneling for communications (a) between the client and the server or (b) between the client and the firewall/gateway over the internet, in which case the firewall and server need to be able to connect to each other on the same LAN.

Port forwarding can also be used when one of the required client ports has been reserved for another purpose, and the client needs to choose a different port. For example, suppose the client already uses port 3389 for a different application. In this case, you can use port forwarding to map an alternative port on the client (for example, port 33389) to the server’s port 3389.

Enable Port Forwarding on the Server

1. Login via telnet or SSH to the IP/MPLSView server machine or firewall/gateway.
2. As root user, edit /etc/ssh/sshd_config (for Solaris10) and set “AllowTcpForwarding” to yes. Note that the port used for port forwarding can be changed by editing the Listen port value "Port 22" to another port value that is not required for other purposes. Run “svcadm refresh ssh” (for Solaris 10) to refresh the service with the new configuration information.
3. If you are connecting to the IP/MPLSView server via a gateway, make sure that the server and gateway can ping each other. If not, set up a route between them (for example, using “route add”). For help on using “route add”, see Setting up a Connection to the Router Network on page 120.
Windows Client Setup

The setup of port forwarding requires the use of an SSH client with the ability to create SSH tunnels. Additionally, port forwarding capability should be turned on for the SSH server. PuTTY is a free SSH client, with this capability, which can be downloaded from the Internet, and will be used in the example below.

Informational Note: The Traffic Collection Manager and Event Browser are special cases which will only work with port forwarding if the IP/MPLSView server is installed using the IP address 127.0.0.1. For regular offline/Task Manager functionality, this is not required.

Set Up the SSH Tunneling Session

1. Open an SSH client that supports port forwarding, such as PuTTY.
2. In the left pane, select Connections > SSH > Tunnels.
3. For use of the software in offline mode, add the following “Source” ports and map them to the corresponding Remote IP and Remote Port on the IP/MPLSView server. Even if you are connecting to a gateway or firewall, the SSH tunnel destination should be the IP/MPLSView server.
   - 8091 - Web port
   - 7000 - Client communications port
   - 3389 - LDAP
   - 22 - add this port if the remote side is not 22
4. The following ports can also be added for additional functionality:
   - 2099 and 2100 - Task Manager port
   - 1856, 4457, 4458, 4459 - Additional ports for traffic collection / MySQL database
   - 22, 23, 8443 - Standard ports for SSH, telnet, and https. Change the remote side’s port as necessary, for example, if the server is using a different port.
   - 8093-8094 - Ports for telnet proxy (for example, Connect to Device capability)
   - 1101, 21101 - Only required for special NAT situations
System Administration

Figure 18: SSH Tunneling Options for IP/MPLSView server 10.1.1.15

5. Scroll up in the left pane and select “Session”. Enter the hostname or IP of the public address with which you want to establish the tunnel (the IP/MPLSView server or the gateway). Select SSH as your protocol. Enter in the SSH port, either the default value of 22, or the customized value specified in step 2 on page 113). If the port value is not 22, the appropriate mapping for the SSH port should also be indicated in the SSH > Tunnel options as discussed earlier.

6. Enter in a name for the session and click the Save button.

7. Click Open to start the putty session, enter in the login credentials, and keep the putty session open when using the client.

Figure 19: Saving Session Information
8. In case of setting up the SSH tunnel to a gateway instead of to the IP/MPLSView server, there may be cases where there is also a firewall between the gateway and the server. If the required ports are not all open, but the SSH port is provided, a second SSH tunnel can be set up between the gateway and the IP/MPLSView server. For example, the following is an example setup (add more ports as required).

```
```

Substitute the serverIP and username with the IP address of the IP/MPLSView server and the login user.

**Login to the Web Client or Java Application**

Now you can login to the IP/MPLSView server securely via the web using http://localhost:8091 or http://127.0.0.1:8091

To login via the Java client directly, first edit the ipmplsview.bat file to change the server IP address to 127.0.0.1.

**Troubleshooting**

- If you see that the login session has begun but it seems to have hung, it is possible that the LDAP port is also being used locally for a third party application such as Remote Desktop. In that case, you may want to choose a different local port, for example, 33389.
  
  In this case, make changes to the SSH Tunneling options, for example, set up the appropriate mapping using local port 33389 to remote port 3389. Then change the LDAP port value to 3389 in the ipmplsview.bat file by specifying LDAP<port number> in the MISC field. For example, use LDAP3389 to indicate the alternate use of port 3389 on the client side. Then launch the application.

- Make sure that the server machine is enabled for port forwarding as described in the beginning of this section.

- In some cases, the PC’s firewall may also be causing a problem. Try login to the server and run “netstat -na | grep 8091” from one telnet/ssh session. Then telnet to the server using the same port, for example, “telnet <server> 8091” and quickly rerun “netstat -na | grep 8091” from the previous window to see if any new connection is listed as “ESTABLISHED”. If not, you may want to check your PC’s firewall settings (Control Panel > Security Center, Windows Firewall).

- If the Traffic Collection Manager or Event Browser do not work, note that these are special cases for port forwarding, which require the IP/MPLSView server to be installed with IP address 127.0.0.1.

**Unix Client Setup**

To run the client on a separate Unix box (Linux, Solaris, or MAC), the SSH tunnels can be set up at the command prompt (add more ports as required):

```
```

Additional ports to forward (see the list in the Windows Client Setup section) can be added similarly by using the -L flag.
Launching the Web Interface

1. Launch the IP/MPLSView web interface via the URL: http://<ip-addr>:8091/ where <ip-addr> is the IP address of the server in which you have IP/MPLSView installed.

2. Alternatively, to access the web interface using a secure HTTP connection, use instead the URL https://<ip-addr>:8443. If navigation is blocked due to security certificate warning, you can click “Continue to this website” to continue.

3. The login credentials use the same user id and passwords setup on the Unix server. Administrators will have access to administrative functions in the Admin menu.
   - To change passwords, use command passwd on the Unix server.
   - To add, remove, or update web users, manage these user through IP/MPLSView User Administration tool.
   - To help troubleshoot server applications related issues, various log files are created under /u/wandl/log and are accessible from the web from Admin > View > Logs. Select to view collection log files or task log files by clicking on the tabs on the left pane and clicking the desired log file to view.
     Refer to the Reference Guide chapter “IP/MPLSView Web Interface” for more details.

Launching the User Administration Tool

The User Administration tool allows for the creation of user groups that share the same view and modify privileges. To access this tool, login to the IP/MPLSView client using the admin user used to install IP/MPLSView (usually “wandl”). Select Admin > User Administration to open the User Administration Tool.

The command line interface can also be used to add users into already created user groups. For more information, refer to Performing User Administration from Text Mode on page 119.
Creating a User Group

Three types of user groups can be added: Full Access (for IP/MPLSView client and optionally web access), Web Portal (for web-only users without Unix login), or Web VPN (for web-only users who can only view particular VPN customer(s)). Full access users who are given web access will be able to login to the web portal using their Unix ID and password.

![User Groups](image)

Figure 20: User Groups

Click the Green button (left) to add a new group and the Red button (right) to delete a group. Select a group in the left pane to display the privileges for the group in the right pane. To change these privileges, check off the privileges that you want to give the group. Note that selecting a row colored gray will toggle the selection of all the check boxes for that category. Scroll down to see the access privileges for the web functions.

Regional Access (Live Network only)

Regional permissions can be set up to limit direct access to live routers through IP/MPLSView. For devices outside of the permitted regions, view-only access will be provided, and features such as ping, traceroute, show config, and hardware inventory will be disabled.

First create the regions in the top Regions tab. Next, select the User Groups tab, and in the right pane, select the bottom Regions tab. De-select “All Regions” and then select the region(s) that can be accessed.

VPN Access (Live Network only)

For Web Portal and Web VPN groups, select the VPN Customers tab to select which VPN Customers to enable for the group. To populate the VPN Customers from the live network, you should have first scheduled and run a live network task.
Creating a User

After creating a user group, add users to that group by clicking the "Users" tab. In the Users tab, click the Green button (left) to add a new user and the Red button (right) to delete a user. To modify a user, double-click the user or select the user and click the Gear button (middle).

![User Administration Tool](Image)

**Figure 21: Users**

When specifying the user details, you must either map the user to a pre-existing Unix User ID (for Full Access users), which can be created as described in Create a Group and User ID on page 9, or enter a web password (for Web Portal and Web VPN users). Make sure a password is also created for the Unix User ID for Full Access users. If it has not been set, the root user can change the password using the command "passwd userid" substituting `userid` with the Unix User ID. This user’s login to the web will then be the "Name" and the password will be the password set for the Unix User ID.

Performing User Administration from Text Mode

In addition to using the GUI interface to perform user administration, users can also be added from text mode using `/u/wandl/bin/addWandlUser.sh`.

**Usage:** `addWandlUser.sh: "name" "group" <-u "uid"|w "webpassword"> [-a <Full|Browsing|Restricted|Blocked>] [-e "email"] [-p "phone"] [-i "im"] [-d "description"]`

- `name` => mandatory username
- `group` => mandatory user admin group
- `-u unixloginname` => unix user id (mandatory if group is a full access group)
- `-w webpassword` => password for web user (mandatory if group is a web or vpn group)
- `-a <Full|Browsing|Restricted|Blocked>` => sets access level to one of the 4 choices (defaults to Full if not specified for non web/vpn group)
- `-e email` => optional email
-p phone => optional phone
-i im => optional im
-d description => optional description

Example:

$ cd /u/wandl/bin
$ ./addWandlUser.sh lab Administrators -u lab -a Full -d "for test"

To configure the maximum number of logins per user, edit the file
/u/wandl/data/.usr/.usercount with one line per user to control. The last line is the default
maximum number of logins. For example, to configure at most three wandl users, and at
most one user for all other users, the format is as follows:

wandl 3
1

For more details refer to the Tools chapter in the Reference Guide or the Security
Management chapter in the Management and Monitoring Guide.

### Setting up a Connection to the Router Network

To set up a connection to a router for the network management features of IP/MPLSView,
you can manually add a static route into the routing table as explained below. The server
should be connected to the routers for telnet collection.

### Sun Solaris

First try to ping a router in your network by typing “ping `router-IP-address`”, substituting
`router-IP-address` with the IP address of a router in your network. If it is successful, you are
already connected. Otherwise proceed with the following steps:

Open a console window and switch to super user if you are not already user id “root” by
using the “su” command.

### Viewing, Adding, and Removing Routes

1. To check what routes are listed in the current routing table, use the following
   command:

   ```
   # /usr/bin/netstat -rn
   ```

2. To add a route to a network through a gateway IP address, enter the following
   command, substituting `router-network-IP-address` and `gateway-IP-address` with their
   proper values:

   ```
   # /usr/sbin/route add -net router-network-IP-address gateway-IP-address
   ```

   For example, if 12.0.0.0 is the router network IP address and 136.20.34.22 is the
   gateway to the router network, type the following command:

   ```
   # /usr/sbin/route add -net 12.0.0.0 136.20.34.22
   ```

3. To add a route to a specific router as opposed to a network, use the same command
   but omit the “-net” keyword.

   Note that if a preexisting route to the same destination is listed before the one you add,
your new route will not be used. To remove a preexisting route, type:

   ```
   # /usr/sbin/route delete router-network-IP-address gateway-to-router-ntwk-IP
   ```
4. To remove all the current routes before installing new ones, type:

```
#/usr/sbin/route flush
```

### Persistent Routes

To make the routes persistent so that they are still available after rebooting the system, the “route -p” command can be used for Solaris 10 (if the -p option is available), which will add routes to the /etc/inet/static_routes file. For example,

```
#/usr/sbin/route -p add -net x.x.x.x -netmask 255.255.0.0 x.x.x.x
```

Note that the “-p” option is not available for all Solaris 10 installations. In that case, another option is to create a script file listing all the route commands, one route command per line, including the “route flush” command as the first line. The script should be executable (use `chmod +x filename` if not) and try executing the script as the root user to test it. Then as the root user, call the script at the end of the /etc/rc2 file.

### Default Route

To set up a default route, enter the following command:

```
#/usr/sbin/route add default gateway-to-router-network-IP
```

substituting `gateway-to-router-network-IP` with the gateway to the router network and ensure that it also is not overridden by an incorrect route.

To avoid losing the default route when rebooting the machine, create or edit the file defaultrouter in /etc with the IP address of the gateway.

For further help, check the reference manual pages for defaultrouter and route.

### Troubleshooting

- If the server has an interface card, check that the interface card is full duplex rather than half duplex. To do so, find the names of the interfaces first using “ifconfig -a”. Suppose one of the interface is named nge0. Then run the ndd command as follows:

```
ndd /dev/nge0 link_duplex
```

  The command will return 0 if the link is down, 1 if it is half duplex, and 2 if it is full duplex. If the command returns 1, check with your hardware manual for instructions on configuring the interface to be full duplex.

- If the server has more than one interface cards, the server may be acting as a router, which may cause connectivity problems. In this case, create the file /etc/notrouter as the root user with the following command:

```
#/usr/bin/touch /etc/notrouter
```

- If ping and traceroute still do not work, check that there is no firewall between the IP/MPLSView server and the router network.

  If the routers cannot be reached directly due to a firewall but can be reached by first logging into an intermediate router, then create the file /u/wandl/db/config/wtalk.agent with a list of the IP address(es) of the intermediate routers that should be logged into in the right order, one per line.
Tuning Solaris Systems

The following tuning parameters are specific to the Solaris operating system. Because the Solaris operating system is not a JBoss Application product, be aware that it can change and results may vary.

About this task

On the Solaris operating system, JBoss Application Server runs on the Sun Hotspot Java virtual machine (JVM). It is important to use the correct tuning parameters with the Sun JVM to utilize its performance optimizing features.


Also, consider the following parameters that are specific to the Solaris operating system to ensure that JBoss Application Server has enough resources.

Procedures

The tuning procedures improve the performance of JBoss Application Server on the Solaris operating system. Configure the following settings or variables according to your tuning needs:

File descriptors (ulimit)

Description: Specifies the maximum number of open files supported. If the value of this parameter is too low, a "Too many files open" error is displayed in the JBoss Application Server stderr.log file.

How to view or set: Check the Unix reference pages on the ulimit command for the syntax of different shells. For the KornShell (ksh) shell use ulimit -a command to display the current settings. Use the ulimit -n 2000 command to set the values. The change may not take effect until you log out and then log back in. Confirm the change with ulimit -a.

Alternatively, if this does not work, the following command can be used on the Solaris application server to increase the maximum number of open files supported from the default of 256 to 65536:

ulimit -Hn 65536
ulimit -Sn 65536

For a linux server, for example, used as a polling or traffic collection server, try the following command to increase the maximum number of open files from the default of 1024 to 65536, for the user "wandl":

vi /etc/security/limits.conf file
wandl soft nofile 65536
wandl hard nofile 65536

Alternatively, to set the permissions on a per-group basis, indicate the group with @group. For example, if the group name is staff, we have:

@staff soft nofile 65536
@staff hard nofile 65536

Default value: None

Recommended value: 10000

Recommended setting: ulimit -Hn 65536
Solaris TCP_TIME_WAIT_INTERVAL

Description: Notifies TCP/IP on how long to keep the connection control blocks closed. After the applications complete the TCP/IP connection, the control blocks are kept for the specified time. When high connection rates occur, a large backlog of the TCP/IP connections accumulates and can slow server performance. The server can stall during certain peak periods. If the server stalls, the `netstat` command shows that many of the sockets that are opened to the HTTP server are in the CLOSE_WAIT or FIN_WAIT_2 state. Visible delays can occur for up to four minutes, during which time the server does not send any responses, but CPU utilization stays high, with all of the activities in system processes.

How to view or set: Use the `get` command to determine the current interval and the `set` command to specify an interval of 30 seconds. For example:

```
ndd -get /dev/tcp tcp_time_wait_interval
ndd -set /dev/tcp tcp_time_wait_interval 30000
```

Default value: The default time wait interval for a Solaris operating system is 240000 milliseconds, which is equal to 4 minutes.

Recommended value: 60000 milliseconds

Recommended setting: `ndd -set /dev/tcp tcp_time_wait_interval 60000`

Solaris TCP_FIN_WAIT_2_FLUSH_INTERVAL

Description: Specifies the timer interval prohibiting a connection in the FIN_WAIT_2 state to remain in that state. When high connection rates occur, a large backlog of TCP/IP connections accumulates and can slow server performance. The server can stall during peak periods. If the server stalls, using the `netstat` command shows that many of the sockets opened to the HTTP server are in the CLOSE_WAIT or FIN_WAIT_2 state. Visible delays can occur for up to four minutes, during which time the server does not send any responses, but CPU utilization stays high, with all of the activity in system processes.

How to view and set: Use the `get` command to determine the current interval and the `set` command to specify an interval of 67.5 seconds. For example:

```
ndd -get /dev/tcp tcp_fin_wait_2_flush_interval
ndd -set /dev/tcp tcp_fin_wait_2_flush_interval 67500
```

Default value: 675000 milliseconds

Recommended value: 67500 milliseconds

Recommended setting: `ndd -set /dev/tcp tcp_fin_wait_2_flush_interval 67500`

Solaris TCP_KEEPALIVE_INTERVAL

Description: The keepalive packet ensures that a connection stays in an active and established state.

How to view or set: Use the `ndd` command to determine the current value or to set the value. For example:

```
ndd -set /dev/tcp tcp_keepalive_interval 300000
```

Default value: 7200000 milliseconds

Recommended value: 15000 milliseconds

Recommended setting: `ndd -set /dev/tcp tcp_keepalive_interval 15000`
For more information on Solaris 10 parameters and resource controls, search for "tunable parameters" and "resource control" on the Sun Microsystems Web site at http://docs.sun.com.

Connection backlog

**Description:** Change the following parameter when a high rate of incoming connection requests result in connection failures:

```
ndd -get /dev/tcp tcp_conn_req_max_q
ndd -set /dev/tcp tcp_conn_req_max_q 8000
```

**Default value:** For Solaris 9 and Solaris 10, the default value is 128.

**Recommended value:** 8000

**Recommended setting:** `ndd -set /dev/tcp tcp_conn_req_max_q 8000`

**Large page support**

Using large pages can reduce the CPU overhead of managing a large JVM heap.

With Solaris 9 and Solaris 10, large page support is provided by default. No operating system or JVM parameters are necessary to make use of large pages for the JVM heap.
Chapter 11

Troubleshooting

This troubleshooting chapter addresses problems related to installation, system administration, and the user interface. If your question is not in here, please check the Troubleshooting sections of the Management and Monitoring Guide or Juniper support explaining what the problem is.

When you contact Juniper support, please provide the build date of the server. The server build date can be found on the server by executing the command "/u/wandl/bin/bbdsgn -v".

General Procedures

This section outlines general procedures for troubleshooting issues with IP/MPLSView such as unexpected behavior, hanging, Java exceptions, or error messages. First step is to check the status of the application server. Second step is to identify any conflicting, missing, or lingering processes. Third step is to gracefully shut down and restart those problematic processes. Specific troubleshooting questions are answered in further sections of this Troubleshooting chapter.

Check Status of Application Server

Login to the application server as wandl user, or as the administrative user that installed IP/MPLSView, and change directory to /u/wandl/bin. Execute the command ./status_mplsview to see the status of the application server.

```
# ./status_mplsview
NPAT Server (pid=21896) detected on port 7000
MySQL detected on port 3333, pid=21933
JBoss JMS (pid=21956) detected, Memory usage: 122M/256M, CPU usage: 0.1%
Web server (pid=21975) detected, Memory usage: 249M/256M, CPU usage: 0.5%
Web server started up successfully!
Task Server (pid=21992) detected, Memory usage: 72M/512M, CPU usage: 0.7%
Event Server (pid=22007) detected, Memory usage: 90M/256M, CPU usage: 0.1%
Warning! : Threshold Server not detected
DGS (pid=22032) detected, Memory usage: 108M/256M, CPU usage: 0.1%
Aggregation crontask scheduled at 0:30
Bulk stat interface traffic generation crontask scheduled
LDAP detected on port 3389, pid=22067
IP/MPLSView Application Monitor (pid=12529) detected
SNMP Trap Server Process detected, pid=22083
Errors : 0
Warnings : 1
Active Process for ROUTER-module: Process id=13175, User name=wandl.
Wed Sep 08 12:24:06 2010 IP: 7.7.7.7 Process ID: 13157 User wandl
```
This command will display various processes used by the IP/MPLSView. Note some of your processes may be different than the above example depending on your license.

- The Error message occurs when processes required to run IP/MPLSView are not detected.
- The Warning message occurs when expected processes are not detected, however these processes are not required to run IP/MPLSView.
- The Active Process for ROUTER-module shows open clients. It displays the timestamp when the client started, the IP that started the client, the process ID, and user ID.

### Identify Processes to Fix

Use the `./status_mplsview` command in combination with the Unix command “ps” can help identify the processes to fix.

Execute the command “ps -ef | grep java” to report all the java processes used by IP/MPLSView. The java processes reported should be the same as the pid’s detected using `./status_mplsview`. If there are duplicate or missing java processes reported by “ps”, then this could lead to conflicts.

Execute the command “ps -ef | grep wandl” to report all the wandl processes used by IP/MPLSView, or replace wandl with the administrative user that installed IP/MPLSview. The wandl processes reported should be the same as the pid’s detected using `./status_mplsview`. If there are duplicate or missing wandl processes reported by “ps”, then this could lead to conflicts.

Execute the command “ps -ef | grep <user>” to report <user> processes used by IP/MPLSView, where <user> is the user detected by `./status_mplsview`. Verify the user is not running lingering or outdated processes.

The LDAP pid can be verified using “ps -ef | grep ldap”.

**Sample “ps -ef | grep java” report when the application server is running properly:**

```bash
# ps -ef | grep java
root 25995 25991 0 00:43:01 ? 0:09 /usr/jdk/latest/bin/java
-noaccess 641 1 0 Aug 12 ? 18:21 /usr/java/bin/java -server
-Xmx128M -XX:+UseParallelGC -XX:ParallelGCThreads=4
wandl 12529 1 0 12:19:18 pts/3 0:46
/export/home/wandl/ipmplsview/java/bin/java -Dprogram.name=appmonitor -Xmx128M
-Dwandl 22032 1 0 16:44:59 ? 0:36
/export/home/wandl/ipmplsview/java/bin/java -Dprogram.name=DGS -Xmx256M -cp
/u/wa
wandl 22007 1 0 16:44:46 ? 1:00
/export/home/wandl/ipmplsview/java/bin/java -Dprogram.name=eventserver -Xmx256M
-wandl 21956 1 0 16:44:20 ? 2:03
/export/home/wandl/ipmplsview/java/bin/java -Dprogram.name=taskserver -server
-X wandl 21992 1 1 16:44:41 ? 16:21 /u/wandl/java/bin/java
-Xmx512M -server -Djava.security.policy=taskserver.policy
wandl 13686 1 0 12:25:42 pts/3 0:09
/export/home/wandl/ipmplsview/java/bin/java -Dprogram.name=threshold -Xmx256M
-Dj
root 26035 26026 49 00:43:02 ? 1637:00 /usr/jdk/latest/bin/java
-version:1.5+ -Djava.library.path=/usr/lib/cc-ccr/lib
```
Troubleshooting

Shut Down and Start Procedure

Application Server Restart

Once the problematic processes are identified, some processes can be stopped and started individually although it is recommended to stop and start the entire application server. Close all clients running IP/MPLSView by exiting or closing the window. Be sure to Save your work. If you do not have direct access to close a client, these will be closed automatically when the stop_mplsview command is executed.

Change directory to /u/wandl/bin and execute command ./stop_mplsview. This command will attempt a graceful shutdown of npatserver, rtserver, filemanager, and processes used by IP/MPLSView. Open clients will receive a pop-up message warning the user that the server will be shut down in 1 minute. Users should Save their work and close the client. After stop_mplsview completes the shutdown messages, wait at least 2 minutes to allow the processes to shut down.

# ./stop_mplsview
Shutdown IP/MPLSView Application Monitor(pid=12529) ...
Would you like to stop the SNMP Trap Server (default=no)? [y/n] y
Shutdown SNMP Trap Server(pid=22083) ...
Shutdown LDAP Server(pid=22067) ...
Removing Aggregation crontask...
Aggregation crontask removed
Removing Bulk stat interface traffic generation crontask...
Bulk stat interface traffic generation crontask removed
Shutdown DGS(pid=22032) ...
Shutdown Event Server(pid=22007) ...
Shutdown Threshold Server(pid=13686) ...
Shutdown Task Manager(pid=21992) ...
Shutdown JBoss(pid=21956) ...
Shutdown Web server(pid=21975) ...
Shutdown MySQL(pid=21933) ...
Shutdown NPAT Server(pid=21896) on port 7000 ...

Execute the command "ps -ef | grep java" and "ps -ef | grep wandl" to verify there are no lingering java and wandl processes related to IP/MPLSView. If there are processes still running, use the Unix kill command to force a shutdown. If lingering processes cannot be shut down, then the Sun server should be rebooted as the last option.

Sample “ps -ef | grep java” report when application server is shut down properly with no lingering processes:

# ps -ef | grep java
root 25995 25991 0 Sep 08 ? 20:20 /usr/jdk/latest/bin/java
   -version:1.5+ -jar /usr/lib/patch/swupa.jar -autoAnaly
noaccess 641 1 0 Aug 12 ? 18:42 /usr/java/bin/java -server
   -Xmx128m -XX:+UseParallelGC -XX:ParallelGCThreads=4
wandl 25845 28108 0 09:29:37 pts/3 0:00 grep java
root 26035 26026 50 Sep 08 ? 3874:45 /usr/jdk/latest/bin/java
   -version:1.5+ -Djava.library.path=/usr/lib/cc-ccr/lib
After verifying the processes were properly shut down, run "./startup_mplsview" as wandl user to restart the application server. After startup_mplsview completes the startup messages, wait at least 3 minutes to allow processes to start. Execute "./status_mplsview" to check the status of the application server and verify there are no warning or error messages.

Launch the client to confirm the issues are resolved.

**Individual Process Restart**

The following table are the commands to stop and start individual processes. This should be done as the wandl user or the user that installed IP/MPLSView, in directory "/u/wandl/bin.

Do not run these commands as root because this may lead to ownership and process conflicts. Some commands are hidden in the directory and can be viewed with command "ls -a". Note that if Application Monitor is running, it will automatically restart processes when it no longer detects a heartbeat from that process. To prevent a process from automatically restarting and keeping it stopped, Application Monitor should be stopped first.

<table>
<thead>
<tr>
<th>Process</th>
<th>Effected Function</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Monitor</td>
<td>System Monitor</td>
<td>&quot;./appmonitor start or stop&quot;</td>
</tr>
<tr>
<td>Event Server</td>
<td>Event Browser</td>
<td>&quot;./eventserver start or stop&quot;</td>
</tr>
<tr>
<td>Threshold Server</td>
<td>Threshold Editor</td>
<td>&quot;./threshold start or stop&quot;</td>
</tr>
<tr>
<td>LDAP Server</td>
<td>User Authentication</td>
<td>&quot;./ldap start or stop&quot;</td>
</tr>
<tr>
<td>SNMP Trap Server</td>
<td>Event Browser</td>
<td>&quot;./snmptrap start or stop&quot;</td>
</tr>
<tr>
<td>Task Server</td>
<td>Task Manager</td>
<td>&quot;./tmng start or stop&quot;</td>
</tr>
<tr>
<td>DGS</td>
<td>Traffic Collection</td>
<td>&quot;./dgs start or stop&quot;</td>
</tr>
<tr>
<td>MySQL</td>
<td>MySQL Database</td>
<td>&quot;./mysql start or stop&quot;</td>
</tr>
<tr>
<td>Webserver</td>
<td>Web</td>
<td>&quot;/webserver.sh&quot;</td>
</tr>
<tr>
<td>Application Server</td>
<td>All</td>
<td>&quot;./startup_mplsview or &quot;/stop_mplsview&quot;</td>
</tr>
</tbody>
</table>

**System Diagnostics**

For advance troubleshooting with the Juniper support team, the following diagnostic scripts in "/u/wandl/bin" can be executed:

- **system-diagnostic.sh** will gather information, messages, hardware and software configurations, java heap and thread dumps, and system information related to IP/MPLSView. Then it zips the text output into the local user’s home directory as support-ymmd.zip. This script should be executed before restarting any services or processes so the current state of the server can be captured.

- **hornetq-debug.sh** generates console output similar to system-diagnostic.sh and will show information about the active event browser, data collector, and JMS server. This script gathers counts from the server management and should not be executed too frequently because this may cause conflicts with the JMS server. If this script will be executed repeatedly as part of custom monitoring, the recommended collection interval is every 30 minutes.
## Troubleshooting

### Server Installation

I am getting errors during installation related to the SSL Certificate.

The error message may look like the following:

```
Generating SSL Certificate (this may take some time)...
Unexpected Signal : 11 occurred at PC=0x ...
Function name=JVM_MonitorWait
Library=/export/home/test0513-32/java/jre/lib/sparc/client/libjvm.so
```

Current Java thread:

```
[error occurred during error reporting]
./install.sh[802]: 28082 Segmentation Fault
As a result, JBoss may not startup properly:
Error! : JBoss not detected
```

To fix this problem, you should install Java patches from the following website:

http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access. Select the appropriate OS version and hardware type.

I am getting errors such as “/usr/ucb/whoami: not found” and “test: argument expected.”

Certain basic UNIX commands are necessary for the installation program to work. These error messages may appear if only the core Solaris operating system is installed and default Unix commands are not installed.

**After installing the activation key, I get the following error message: “Password for IP/MPLSView is either missing or expired!”**

Please do the following to double-check whether you have the correct installation of the IP/MPLSView password file:

1. Switch to the /u/wandl/db/sys directory: cd /u/wandl/db/sys
2. View the contents of the npatpw file and make sure there is no extra character or typing error: cat npatpw

**The NPAT server does not start up properly because the default NPAT port is in use.**

If you have an IP/MPLSView client window open, closing it may free up the port. Then you can try “startup_mplsview” again. Otherwise, try using the following command:

```
$ /u/wandl/bin/startup_mplsview [port_number]
```

To find which ports are in use, you can use the command “/usr/bin/netstat -a” on the server.

**I see an error similar to this: “Error: please check whether the server is running on xxx.xxx.xxx.xxx and, if so, please CHECK whether the port number is 7000.”**

To check if the server is running, log into that server and try the “/u/wandl/bin/status_mplsview” command. This should also give you a port number. Use “/u/wandl/bin/startup_mplsview port_number” to change the port number, substituting `port_number` with an unused unreserved port number. To see a list of used port numbers, you can execute “/usr/bin/netstat -a” on the server side.

I chose the wrong port value 334 by accident and that caused some problems. I got the message: Error! : mySQL not detected. How can I change the port?

To change the port, cd /u/wandl/bin and run ./changeconfig.sh
After I completed installation on the server, I ran the startup script for IP/MPLSview. However, the DGS server still says it is not running. How do I fix this?

First, check the log file in /u/wandl/log/dgs.log.0 and dgs.msg. If the dgs.msg file says: “Got error 134 from table handler appears in the dgs.log”, then the problem is most likely in the database tables.

To repair the database, run the following: (Note: mysql must be running)

$ cd /u/wandl/thirdparty/mysql
$ bin/mysqlcheck -r -uroot -pwandlroot -S /u/wandl/data/mysql/data/mysql.sock
mplsview

Check the output to see if the database tables are repaired. Next, restart the DGS server by running the following:

$ cd u/wandl/bin
$ .dgs start ../db/config/dgs.xml

When I run startup_mplsview, I get the message “Only root may start NPAT server”. The permissions of some of the files in the bin folder may have been corrupted. To fix this problem please run the following commands as the root user in the IP/MPLSView bin directory:

# chmod 4750 .npat .stopnpat
# chown root .npat .stopnpat

When I run status_mplsview, I get the warning message “Task Server detected, but not fully initialized”. What’s wrong?

The Task Manager may take a while to fully deploy. Wait a few minutes and check again.

I cannot view the online help or web interface.
Check /u/wandl/bin/status_mplsview. If you just started up the server, wait another 5 minutes, as the web server takes time to initialize. Then rerun /u/wandl/bin/status_mplsview. If you see the error message “Web server ERROR: Unable to connect to web server!”, go to the /u/wandl/bin directory and run the following commands:

$ . ./mplsenvsetup.sh
$ ./webserver.sh stop
$ ./webserver.sh start

Although I installed a new version of IP/MPLSView, it seems like I am still using the old version.
In some cases, the existing server is not properly shut down, or there is a conflict with a previous installation of IP/MPLSView. In such a case, you can try “ps -ef | grep mysql”, “ps -ef | grep security”, “ps -ef | grep java”, and “ps -ef | grep server”. To ensure the listed processes, if any, are from IP/MPLSView, check the path listed and see if that includes a directory in which IP/MPLSView was installed. If so, then you can try “kill -9 pid1 pid2...” substituting pid1 pid2... by the process ids found in the previous two commands. You may also want to close any currently running clients from previous installations. Afterward, try restarting IP/MPLSView using the above command.
To avoid running into this problem, please be sure to have stopped any old IP/MPLSView programs that may be running on the same system using the command “/u/wandl/bin/stop_mplsview”.


I changed my Solaris machine’s IP address and can no longer access the web.
Run /u/wandl/bin/changeconfig.sh and change the IP address wherever it is listed. Check the /u/wandl/bin/mplsenvsetup.sh file to make sure the IP addresses have properly been updated. Then shut down and restart the IP/MPLSView server using stop_mplsview and startup_mplsview.

I am getting a MySQL Installation Error “Creating database tables …Error: installation of mysql failed. Please check the log for details: $WANDL_HOME/log/instmysql.log”
Please try the following steps:
1. Stop MPLSView via /u/wandl/bin/stop_mplsview
2. Run “ps -ef|grep mysql” and then kill any stray mysql processes via “kill -TERM <pid>” or “kill -9 <pid>”, substituting “<pid>” with the process id’s returned by the above command.
3. cd /u/wandl/bin
4. “. ./mplsenvsetup.sh” (Note the space after the dot: .<space>/mplsenvsetup.sh)
5. Type in the exact command as follows in a single line:
```bash
./mysql_install_db --defaults-file=$WANDL_HOME/db/config/my.cnf --basedir=$WANDL_HOME/thirdparty/mysql --1data=$WANDL_HOME/data/mysql/data >> $WANDL_HOME/log/instmysql.log 2>&1
```
5. Run “ps -ef|grep mysql” Again, kill any processes which persist.
6. Startup MPLSView again via /u/wandl/bin/startup_mplsview

Informational Note: There is a /u/wandl/bin/fixmysql.sh to repair tables in the case of a shutdown without using stop_mplsview command, for example due to a power failure.

Client Installation

I get an error message when I install the client on my PC. A certain file could not be written.
This can be caused by previous IP/MPLSView client sessions on your PC that are still open. Try closing them and then re-install the client.

I am unable to start the PC client and get the following message: “Out of environment space”.
This issue will arise when you do not have enough memory in your MS-DOS environment to set an environment variable. For more information about this issue and alternative solutions, see Microsoft’s Knowledge Base Article # 230205:
http://support.microsoft.com:80/support/kb/articles/Q230/2/05.ASP&NoWebContent=1

I can’t connect from the client to the Solaris server.
This could be due to a firewall. To check if there is a firewall, try the following:
1. Log into the server machine and check to see if the chosen port is open and listening by using: netstat -a |grep 7000 (7000 is the default IP/MPLSView server port). If the port is listening, then go to step two.
2. Execute “telnet IP_address 7000” with the appropriate substitution for IP_address. Wait to see the response. If you have access to the port you may see a message like “Escape character is ‘^[’ “. The cursor will stay and the session won’t get time out. In this case, it may not be a firewall problem. On the other hand, if the port is open, but you do not have access to it, it is a firewall problem.

Check that the required ports are open between the client and server in Required Ports to Open in Firewalls on page 2.

If there is a firewall, and you do not require online modules, you may want to try SSH tunneling as described in Setting Up Port Forwarding for Secure Communications on page 113. For NAT situations, refer to NAT on page 16.

I can't connect from the client to the Linux server.
This could be due to a firewall. To check if there is a firewall, try the following:
Log into the server machine and check to see if the chosen port is open and listening by using: netstat -a |grep 7000 (7000 is the default IP/MPLSView server port).
To disable the firewall on Centos 6.x try the following:
1. service iptables stop
2. service ip6tables stop
3. chkconfig iptables off
4. chkconfig ip6tables off
5. vi /etc/sysconfig/selinux
6. Change the entry selinux=enforcing to selinux=disabled
7. Reboot the machine after making the changes

I get a login error although I entered the correct login and password.
If the /u/wandl/db/sys/npatpw license file contains the license for “useradmin”, the access to the graphical interface will be controlled by the Advanced User Admin tool, and each unix account other than “wandl” must be authorized separately. Refer to Launching the User Administration Tool on page 117 for more details.

I can't open the Task Manager.
If the Task Manager is not displayed, close the client window and wait a couple of minutes before restarting the client and attempting to open the Task Manager. To check the status of the processes, run /u/wandl/bin/status_mplsview or check /u/wandl/log/tmng.log.0.
If this does not help, you may want to try stopping and restarting the Task Manager using /u/wandl/bin/.tmng stop. After that is done, try /u/wandl/bin/.tmng to restart the Task Manager. Check that the process ID for the TMNG process in /u/wandl/tmp/.pids is correct by using the command “ps -fp <pid>” substituting <pid> with the process ID.
Check that the port 2099 and 2100 are opened between the client and server as indicated in Required Ports to Open in Firewalls on page 2.

After a couple minutes of use, the client always becomes unresponsive or hangs.
This may be due to a firewall closing idle connections. You can specify a shorter keep-alive message interval (for example, 60 seconds) by going to Application > Keep-Alive Message.
Troubleshooting

How do I increase the memory that Java can use on my PC client?
Edit the batch file ipmplsview.bat used to start the client. To change the memory setting from 128M to 192M, change “SET MEMORY=128M” to “SET MEMORY=192M”. This number should not exceed the PC’s RAM. Additionally, if you are also using your PC for other tasks while you run IP/MPLSView, make sure to reserve some memory for other applications on your PC. Otherwise, they may be slowed down significantly.

I could not invoke the browser for the Help manual on the Solaris operating system.
On the Solaris operating system, you may need to set the path to access Netscape to avoid the following error message: “Could not invoke browser, command=netscape -remote openURL(...)”. To do so, append the path for Netscape to the PATH environment variable. For example, if netscape is located in /usr/dt/bin, type in the following command:

```
PATH=/usr/dt/bin:$PATH; export PATH
```

To permanently set the PATH variable, please create or edit the .profile in your Unix user’s administrative home directory.

Web Start

I am trying to launch the client via Java Web Start, but when I click the “Run IP/MPLSView” button, nothing happens.
Popup blockers can interfere with this operation. Either try holding down the CTRL button while clicking Run button or else disable your popup blocker.

When launching the client via Java Web Start, I got an error message that said: “Unable to find file: c:\.....\<client-ip-addr>.jnlp”.
Sometimes the browser’s cache is out of synch. This often happens if the browser’s cache is set too large. To fix this problem, clear your browser’s cache and set it to a more reasonable size (100MB should be more than enough).

How do I launch Java Web Start’s Application Manager in order to change Java Web Start’s settings?
For Windows, run Start > Programs > Java Web Start > Java Web Start. For Solaris, run javaws in the /javaws subdirectory of where the client was installed for Solaris (for example, /u/wandl/client/javaws). Then select File > Preferences.

I am experiencing odd problems when launching the client via Java Web Start?
Sometimes Web Start’s cache gets corrupted. First make sure that the client is not running. Launch Java Web Start’s Applications Manager. Select File > Preferences and click on the Advanced tab. Click on the Clear Folder button to clear the applications folder. If the Current Size (in KBytes) is not reset to 0, you may have to manually delete the files. In order to do this, browse to the directory displayed in Applications Folder and delete everything in there. If you are unable to delete everything, it may mean that a copy of the client is still running.

How do I enable my Java output console when using Java Web Start?
You may open a Java output console window by launching Java Web Start’s Application Manager. Select File > Preferences and click on the Advanced tab. Check the box for Show Java Console.
Java Web Start has trouble using my JRE.
If you have installed a new JRE or uninstalled an existing JRE, the old settings may be kept, which causes problems. You can reconfigure the JRE settings by launching Java Web Start's Application Manager. Select File > Preferences and click on the Java tab. An alternative solution would be to uninstall Webstart and all JRE's, then reinstall Java and Webstart.

System Administration

How can I determine the build date of the version of IP/MPLSView I installed?
To determine the build date of the server, try the following command:

```
$ bin/bbdsgn -v
```

Or, after you have opened a spec file on the JAVA client, select Help> About for this information.

How do I create another user account?
IP/MPLSView will not create the user account for you. You have to do this manually using the useradd command. See Create a Group and User ID on page 9.

When I log in as wandl to a server on another machine, I get the error message, “Unable to access home directory of wandl.”
The reason for this error message could be that you have moved user wandl's administration home directory (as opposed to user wandl's installation home directory). For example, suppose user id wandl has home directory /export/home/wandl, but is installed under /space/wandl and /u/wandl is linked to /space/wandl. Then WANDL_HOME=/u/wandl, but IP/MPLSView's Administrative home directory is /export/home/wandl.

I cannot use the /u drive on my server to create the symbolic link to my program.
In order to use IP/MPLSView without the /u/wandl link, you should set the variable WANDL_HOME before running the program as follows:

```
$ WANDL_HOME=installation_directory
$ export WANDL_HOME
```

What kind of printer driver/software do I need to have to use the Print feature?
You can use any printer driver/software on your computer with IP/MPLSView. For UNIX, IP/MPLSView will give you a window where you can specify the print command (lp). For Windows, IP/MPLSView will give you a window in which you can choose your printer.

User Interface

I have an input file specified in the spec file, but the program cannot find it.
Any misspelling may cause the problem. Also note that the keywords and filenames are case-sensitive.

What is the difference between a router name and a router id?
This just provides you with two ways to label your routers. You can keep your id fixed (to make bookkeeping easier) while changing the router name to something meaningful.
How do I find a router with a particular name or id?
To locate a network element, right-click on the topology view and select Find Nodes/Groups from the pull-down menu of the left pane of the topology window.

How do I change my map background color?
To change global color settings for your client, select Application > Options > Map Preferences. Click on the box to the right of "Background." In the Choose A Color window, click the desired color and then click OK. Check to make sure the Foreground text and Mouse Drag Lines are a different color and visible against the background color.

How do I turn off the multiple curve lines between two nodes?
To turn off the multiple curve lines between two nodes, select Application > Options > Map Preferences. Unclick the Draw Mult Links as Curves checkbox to straighten out the curved links in the network model.

How do I turn on the geographical map?
Right-click on the map portion of the topology window. Choose "Country Maps." Then select "All" and "OK" to turn on all of the available maps. If you don't see the map, select Application > Options > Map Preferences and change the "Country Borders" color.

My nodes are not where I specified that they should be.
Right-click on the map portion of the topology window and select Layout > Recalculate Layout from the right-click menu. This will rearrange your nodes according to the location settings given to the nodes.

How do I get my router name on the screen?
To label the devices, right-click on the map and select Labels > Node Labels from the right-click menu. Select All and click OK to label all nodes. Select to label the nodes by Name and click OK.

I keep losing my node rearrangements. How do I save them?
The node geographical coordinates are stored in the graphcoord input file and do not get saved until you save the design environment through the File menu.

I opened the Live Network, but I don't see anything on the Topology Map
You need to schedule a live collection in the Task Manager at least once in order to have a complete network data.

I cannot launch the Task Manager using a Windows machine.
Check the network settings of Internet Explorer from Tools > Internet Options > Connections. If the machine is configured to use a proxy, this may cause problems because it is trying to search the proxy for the application server's private address. The proxy may eventually be able to determine the local address but this could still cause issues. Disable the proxy and allow for a direct connection.