



---

# Getting Started Guide for IP/MPLSView



---

Modified: 2018-06-29

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

*Getting Started Guide for IP/MPLSView*

Copyright © 2018 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

#### YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

#### END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://www.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Table of Contents

	About the Documentation . . . . .	xi
	Documentation and Release Notes . . . . .	xi
	Documentation Conventions . . . . .	xi
	Documentation Feedback . . . . .	xiii
	Requesting Technical Support . . . . .	xiv
	Self-Help Online Tools and Resources . . . . .	xiv
	Opening a Case with JTAC . . . . .	xiv
<b>Chapter 1</b>	<b>System Requirements for IP/MPLSView . . . . .</b>	<b>17</b>
	Introduction . . . . .	17
	Recommended System Configuration . . . . .	17
	Server Configuration . . . . .	17
	Client Configuration . . . . .	18
	Traffic Data Collector Configuration . . . . .	18
	Browser Support . . . . .	19
	VM Support . . . . .	19
	Hardware Support . . . . .	19
	Required Ports to Open in Firewalls . . . . .	21
	Port Map . . . . .	22
	Key . . . . .	23
	Basic Configuration . . . . .	24
	Advanced Configuration . . . . .	24
	Port Table . . . . .	24
<b>Chapter 2</b>	<b>Installing IP/MPLSView . . . . .</b>	<b>29</b>
	IP/MPLSView Installation Overview . . . . .	29
	Installing the IP/MPLSView Server, Client, Traffic Data Collector, and Rsync Package . . . . .	32
	Downloading and Extracting the IP/MPLSView Software . . . . .	32
	Preparing for Installation . . . . .	33
	Starting the Server Installation . . . . .	35
	Installation Main Menu Advanced Options . . . . .	37
	Installing the IP/MPLSView Client on the Local Server . . . . .	42
	Installing the Traffic Data Collector on the Local Server . . . . .	43
	Installing the Replication and Rsync Package on the Local Server . . . . .	43
	Additional Steps for Installing IP/MPLSView in a NAT Environment . . . . .	44
	Installing IP/MPLSView as a Non-Root User . . . . .	45
	Installing IP/MPLSView Without Reusing Existing Settings and Data . . . . .	46
	Updating the IP/MPLSView Server . . . . .	47
	Installing the IP/MPLSView Distributed Database and Traffic Data Collector . . . . .	47
	Installing the IP/MPLSView Client on a PC . . . . .	49

<b>Chapter 3</b>	<b>Installing the Remote Collection Server</b>	<b>51</b>
	Remote Collection Server Overview	51
	Installing the Remote Collection Server	52
<b>Chapter 4</b>	<b>Installing the Viewserver</b>	<b>57</b>
	Viewserver Overview	57
	When to Use the Viewserver	57
	Viewserver Client	57
	Application Client	58
	Installing the Viewserver	59
<b>Chapter 5</b>	<b>Configuring Traffic Updates from IP/MPLSView to NorthStar Controller</b>	<b>67</b>
	Traffic Updates from IP/MPLSView to NorthStar Controller Overview	67
	Traffic Updates from IP/MPLSView to NorthStar Controller	67
	System Requirements	69
	NorthStar AMQP Agent	69
	Configuring NorthStar AMQP Agent	70
	Configuring Additional Attributes	71
	Starting or Stopping the NorthStar AMQP Agent	72
<b>Chapter 6</b>	<b>Configuring and Administering IP/MPLSView in a Distributed Environment</b>	<b>73</b>
	Replication and Rsync in Distributed Environments Overview	73
	Installing the Rsync Package and Automating SSH Login	74
	Installing and Administering IP/MPLSView Replication and Rsync in a Two-Server Environment	77
	Installing IP/MPLSView with Replication and Rsync in a Two-Server Environment	78
	Starting IP/MPLSView in a Two-Server Environment	80
	Failing Over to the Backup Server	81
	Synchronizing the Data from the Backup Server to the Original Primary Server	82
	Switching Back to the Original Primary Server	84
	Installing and Administering IP/MPLSView Replication and Rsync in a Four-Server Environment	85
	Installing and Administering IP/MPLS View in a Four-Server Distributed Environment	87
	Starting IP/MPLSView in a Four-Server Environment	89
	Starting IP/MPLSView on the Database Servers in a Four-Server Environment	91
	Configuring an Rsync Cronjob to Replicate Traffic Collection Data	92
	Failing Over to the Backup Servers in a Four-Server Environment	92
	Synchronizing the Database from the Backup Server to the Original Primary Server	94
	Switching Back to the Original Primary Server	96
	Administering Failovers in a Distributed Environment	97
	Administering Failovers Using the Setup-failover Script	97
	Example Failovers In a Distributed Environment	98
	Troubleshooting Database Synchronization in a Distributed Environment	100

<b>Chapter 7</b>	<b>Installing IP/MPLSView High Availability for Linux OS . . . . .</b>	<b>103</b>
	IP/MPLSView Linux OS High Availability Overview . . . . .	103
	Installing the Linux Operating System for IP/MPLSView High Availability . . . . .	105
	Installing Linux OS on Your Servers . . . . .	105
	Installing Linux OS on the Management Nodes . . . . .	106
	Guidelines for Partitioning the SAN Storage Disk . . . . .	106
	Installing the Red Hat Enterprise Linux High Availability Add-On . . . . .	108
	Creating the Quorum Disk . . . . .	108
	Setting Up the Global File System 2 Partition . . . . .	109
	Configuring the Linux Operating System for IP/MPLSView High Availability . . . . .	110
	Assigning a Password to the Ricci Daemon . . . . .	110
	Starting Conga Services . . . . .	111
	Accessing the Luci Console . . . . .	111
	Creating the High Availability Cluster . . . . .	112
	Configuring the Quorum Disk . . . . .	114
	Configuring Fence Devices . . . . .	114
	Configuring Nodes to Use Fence Devices . . . . .	116
	Configuring the Failover Domain . . . . .	117
	Creating Service Groups . . . . .	119
	Automating SSH Login from All Servers . . . . .	121
	Installing IP/MPLSView in a Distributed Environment . . . . .	122
	Installing IP/MPLSView on Distributed Application and Database Servers . . . . .	123
	Starting, Relocating, and Stopping IP/MPLSView from the GUI or CLI . . . . .	131
	Starting the Application Server Using the GUI . . . . .	131
	Starting the Application Server Using the CLI . . . . .	132
	Relocating the Application Server Using the GUI . . . . .	132
	Relocating the Application Server Using the CLI . . . . .	133
	Stopping the IP/MPLSView High Availability Cluster Using the GUI . . . . .	133
	Stopping the IP/MPLSView High Availability Cluster Using the CLI . . . . .	134
	Recording Cluster Setup Information . . . . .	134
	Frequently Asked Questions: Cluster Administration . . . . .	135
<b>Chapter 8</b>	<b>Getting Started with IP/MPLSView . . . . .</b>	<b>137</b>
	Starting IP/MPLSView Servers . . . . .	137
	Starting Up the IP/MPLSView Server . . . . .	138
	Starting the IP/MPLSView Traffic Data Collector . . . . .	140
	Starting the IP/MPLSView Trap Daemon from Linux . . . . .	141
	Manually Starting the Event Server . . . . .	142
	Manually Starting the Distributed Database in Linux . . . . .	142
	Restarting the Task Server . . . . .	142
	Launching the IP/MPLSView Client . . . . .	143
	Launching the IP/MPLSView Client on Linux . . . . .	143
	Launching the IP/MPLSView Client on Microsoft Windows . . . . .	144
	Launching IP/MPLSView Client Using Web Start (Linux and Windows) . . . . .	146

<b>Chapter 9</b>	<b>System Administration . . . . .</b>	<b>149</b>
	IP/MPLSView System Administration Overview . . . . .	149
	Backing Up the Data Directories . . . . .	149
	Setting Up Port Forwarding for Secure Communications . . . . .	150
	Launching the IP/MPLSView Web Interface . . . . .	154
	Creating Users and Groups Using the User Administration Tool . . . . .	154
	Setting Up an IP/MPLSView Connection to the Router Network . . . . .	157
<b>Chapter 10</b>	<b>Troubleshooting the IP/MPLSView Installation . . . . .</b>	<b>161</b>
	Troubleshooting IP/MPLSView Overview . . . . .	161
	General Procedures for Troubleshooting the IP/MPLSView Installation . . . . .	161
	Running Advanced IP/MPLSView System Diagnostics Scripts . . . . .	165
	IP/MPLSView Server Installation Frequently Asked Questions . . . . .	166
	IP/MPLSView Client Installation Frequently Asked Questions . . . . .	169
	IP/MPLSView Java Web Start Frequently Asked Questions . . . . .	172
	IP/MPLSView System Administration Frequently Asked Questions . . . . .	173
	IP/MPLSView User Interface Frequently Asked Questions . . . . .	173
	Troubleshooting IP/MPLSView Database Synchronization . . . . .	175

# List of Figures

<b>Chapter 1</b>	<b>System Requirements for IP/MPLSView .....</b>	<b>17</b>
	Figure 1: Port Map .....	23
<b>Chapter 3</b>	<b>Installing the Remote Collection Server .....</b>	<b>51</b>
	Figure 2: Sample Environment Using a Remote Collection Server .....	51
<b>Chapter 5</b>	<b>Configuring Traffic Updates from IP/MPLSView to NorthStar Controller .....</b>	<b>67</b>
	Figure 3: Traffic Update Architecture for IP/MPLSView to NorthStar .....	68
<b>Chapter 6</b>	<b>Configuring and Administering IP/MPLSView in a Distributed Environment .....</b>	<b>73</b>
	Figure 4: Example IP/MPLSView Setup for a Two-Server Distributed Environment .....	77
	Figure 5: Example IP/MPLSView Setup for a Four-Server Distributed Environment .....	86
<b>Chapter 7</b>	<b>Installing IP/MPLSView High Availability for Linux OS .....</b>	<b>103</b>
	Figure 6: Linux OS High Availability Hardware Setup .....	104
	Figure 7: High Availability Luci Console .....	112
	Figure 8: High Availability Manage Clusters Luci Console .....	112
	Figure 9: High Availability Manage Clusters Actions .....	112
	Figure 10: Create New Cluster Window .....	113
	Figure 11: Create New Cluster Add Nodes Window .....	113
	Figure 12: Quarum Disk Configuration Window .....	114
	Figure 13: Add Node1 and Node2 Fence Device (Instance) Windows .....	115
	Figure 14: Add Fence Device Window Fence Method .....	117
	Figure 15: Add Fence Device Window Nodes List .....	117
	Figure 16: Add Failover Domain to Cluster Dialog Box .....	118
	Figure 17: Add Service Group to Cluster Window .....	119
	Figure 18: Add Resource to Service Window .....	120
	Figure 19: Service Groups Edit Service .....	121
	Figure 20: Join and Leave Cluster Selections .....	123
	Figure 21: High Availability Service Groups Window .....	132
	Figure 22: High Availability Service Groups Stop Action .....	133
<b>Chapter 8</b>	<b>Getting Started with IP/MPLSView .....</b>	<b>137</b>
	Figure 23: IP/MPLSView Login Window .....	144
	Figure 24: IP/MPLSView Web Interface with Web Client Access .....	146
	Figure 25: Server and WebServer Selection and Client Memory Allocation .....	146
	Figure 26: Application Files Downloading Window .....	147
	Figure 27: Web Start Warning Message .....	147

<b>Chapter 9</b>	<b>System Administration . . . . .</b>	<b>149</b>
	Figure 28: SSH Tunneling Options for the IP/MPLSView Server . . . . .	151
	Figure 29: Saving Session Information . . . . .	152
	Figure 30: User Administration User Groups Tab . . . . .	155
	Figure 31: User Administration Users Tab . . . . .	156



# List of Tables

	<b>About the Documentation</b> . . . . .	<b>xi</b>
	Table 1: Notice Icons . . . . .	xii
	Table 2: Text and Syntax Conventions . . . . .	xii
<b>Chapter 1</b>	<b>System Requirements for IP/MPLSView</b> . . . . .	<b>17</b>
	Table 3: Recommended Server Configuration . . . . .	18
	Table 4: Recommended Client Configuration . . . . .	18
	Table 5: Recommended Traffic Data Collector Configuration . . . . .	18
	Table 6: Browser Support . . . . .	19
	Table 7: VM Support . . . . .	19
	Table 8: Hardware Support . . . . .	20
	Table 9: Required Ports to Open in Firewalls for Servers . . . . .	21
	Table 10: Required Ports to Open in Firewalls for Protocols . . . . .	21
	Table 11: IP/MPLSView Port Table For Clients . . . . .	24
	Table 12: IP/MPLSView Port Table for the Application Client . . . . .	25
	Table 13: IP/MPLSView Port Table for the Application and Viewserver . . . . .	25
	Table 14: IP/MPLSView Port Table for the Traffic Data Collector . . . . .	26
	Table 15: IP/MPLSView Port Table for the Primary and Backup Servers . . . . .	26
	Table 16: IP/MPLSView Port Table for the Remote Collection Server . . . . .	27
<b>Chapter 2</b>	<b>Installing IP/MPLSView</b> . . . . .	<b>29</b>
	Table 17: Installation Settings . . . . .	30
	Table 18: Installation Components . . . . .	31
<b>Chapter 4</b>	<b>Installing the Viewserver</b> . . . . .	<b>57</b>
	Table 19: Distributed Server Address Example . . . . .	59
<b>Chapter 5</b>	<b>Configuring Traffic Updates from IP/MPLSView to NorthStar Controller</b> . . . . .	<b>67</b>
	Table 20: Variables for NorthStar AMQP Agent . . . . .	71
<b>Chapter 7</b>	<b>Installing IP/MPLSView High Availability for Linux OS</b> . . . . .	<b>103</b>
	Table 21: Server Network Record . . . . .	134
	Table 22: Server Data Record . . . . .	134
<b>Chapter 8</b>	<b>Getting Started with IP/MPLSView</b> . . . . .	<b>137</b>
	Table 23: Starting, Stopping, and Verifying Status Commands . . . . .	138
	Table 24: Language Codes . . . . .	147



# About the Documentation

- Documentation and Release Notes on page xi
- Documentation Conventions on page xi
- Documentation Feedback on page xiii
- Requesting Technical Support on page xiv

## 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 <https://www.juniper.net/documentation/>.

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 <https://www.juniper.net/books>.

## Documentation Conventions

---

Table 1 on page xii defines notice icons used in this guide.

Table 1: Notice Icons







Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  user@host> <b>configure</b>
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> <b>show chassis alarms</b>  No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Introduces or emphasizes important new terms.</li> <li>Identifies guide names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul>	<ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS CLI User Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name:  [edit] root@# <b>set system domain-name</b> <i>domain-name</i>

Table 2: Text and Syntax Conventions (continued)

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"><li>To configure a stub area, include the <b>stub</b> statement at the <b>[edit protocols ospf area area-id]</b> hierarchy level.</li><li>The console port is labeled <b>CONSOLE</b>.</li></ul>
< > (angle brackets)	Encloses optional keywords or variables.	<b>stub &lt;default-metric <i>metric</i>&gt;;</b>
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	<b>broadcast   multicast</b>  <b>(<i>string1</i>   <i>string2</i>   <i>string3</i>)</b>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	<b>community name members [ <i>community-ids</i> ]</b>
Indentation and braces ( { } )	Identifies a level in the configuration hierarchy.	<pre>[edit] routing-options {   static {     route default {       nexthop <i>address</i>;       retain;     }   } }</pre>
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"><li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li><li>To cancel the configuration, click <b>Cancel</b>.</li></ul>
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## 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 of the Juniper Networks TechLibrary site at <https://www.juniper.net/documentation/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/documentation/feedback/>.

- E-mail—Send your comments to [techpubs-comments@juniper.net](mailto: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 Partner Support Service 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.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://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: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <https://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

## 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 <https://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 <https://www.juniper.net/support/requesting-support.html>.





## CHAPTER 1

# System Requirements for IP/MPLSView

- [Introduction on page 17](#)
- [Recommended System Configuration on page 17](#)
- [Required Ports to Open in Firewalls on page 21](#)

## Introduction

---

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, as well as 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, and tunnel state. This guide explains the installation procedures and how to get the IP/MPLSView system up and running.

### Related Documentation

- [Recommended System Configuration on page 17](#)
- [IP/MPLSView Installation Overview on page 29](#)
- [Installing the IP/MPLSView Server, Client, Traffic Data Collector, and Rsync Package on page 32](#)

## Recommended System Configuration

---

IP/MPLSView software is a client-server application. The IP/MPLSView server is installed on a Linux platform and can be accessed from an IP/MPLSView client installed on a Windows or Linux platform. Before installing IP/MPLSView, check your hardware specifications. We recommend the following system configuration.



NOTE: IP/MPLSView Release 6.2.0 and later are not distributed on CD.

## Server Configuration

[Table 3 on page 18](#) lists the recommended server configuration with IP/MPLSView.

**Table 3: Recommended Server Configuration**

Server Configuration
64-bit Linux OS can be:
<ul style="list-style-type: none"> <li>CentOS 6.7 - CentOS 7.2</li> <li>Red Hat 6.7 - Red Hat 7.2</li> </ul>
Minimum 8 GB RAM
Minimum 100 GB disk space
Swap space can be configured as approximately two times the physical RAM

For more information about Linux versions, including CentOS source-code monthstamps, see your operating system vendor. For more information about IP/MPLSView compatibility, contact the Juniper Networks Technical Assistance Center (JTAC).

## Client Configuration

Table 4 on page 18 lists the recommended client configuration with IP/MPLSView.

**Table 4: Recommended Client Configuration**

Client Configuration
PC running:
<ul style="list-style-type: none"> <li>Windows 10</li> <li>Windows 8</li> <li>Windows 7</li> </ul>
Linux
XVGA monitor and graphics card
Minimum 4 GB RAM
100 MB disk space

## Traffic Data Collector Configuration

Table 5 on page 18 lists the recommended Traffic Data Collector configuration for the Online Traffic Collection Module.

**Table 5: Recommended Traffic Data Collector Configuration**

Traffic Data Collector Configuration
Linux
1 collector per 100 to 150 devices

*Table 5: Recommended Traffic Data Collector Configuration (continued)*

Traffic Data Collector Configuration
Minimum 4 GB RAM
Minimum 75 GB disk space



**NOTE:** One collector server can run many instances (10-20 or more) to distribute load but the total number of devices is limited.

## Browser Support

Table 6 on page 19 lists the operating systems and browsers supported with IP/MPLSView.

*Table 6: Browser Support*

OS	Browser
Windows 10	<ul style="list-style-type: none"> <li>Google Chrome 56 and Chrome 55</li> <li>Firefox 51 (32 bit), Firefox 50</li> <li>Internet Explorer 11</li> </ul>
Windows 7	<ul style="list-style-type: none"> <li>Google Chrome 56</li> <li>Firefox 51 (32 bit)</li> <li>Internet Explorer 11</li> </ul>
CentOS 7, CentOS 6.8	<ul style="list-style-type: none"> <li>Google Chrome 56 (64 bit)</li> <li>Firefox 51 (64 bit)</li> </ul>

## VM Support

Table 7 on page 19 lists VM support with IP/MPLSView.

*Table 7: VM Support*

VM Support
CentOS 6.7 - CentOS 7.2
Red Hat 6.7 - Red Hat 7.2
OpenStack Kilo, OpenStack Liberty

## Hardware Support

Table 8 on page 20 lists the hardware supported with IP/MPLSView.

**Table 8: Hardware Support**

Vendor	Devices
Juniper Networks	<ul style="list-style-type: none"> <li>IP routers: Junos-based M, T, MX, PTX</li> <li>Switches: Junos-based QFX</li> <li>Other: Junos E and ERX</li> <li>NetScreen Firewall</li> </ul>
Nokia (Alcatel)	<ul style="list-style-type: none"> <li>IP routers: SR OS devices such as 7750, 7950, 7505</li> <li>ATM devices: 7670, 7470, 5620, or PNNI-based routing</li> </ul>
Cisco Systems	<ul style="list-style-type: none"> <li>Routers: IOS-based devices such as 7500, 7600, GSR 12000, ASR 900</li> <li>Routers: IOS-XR-based devices such as GSR 12000, CRS-1/3/X, ASR 9000</li> <li>ATM devices: IGX 8400, BPX 8600, MGX 8800, and Lightstream 1010</li> <li>Optical: ONS 15454, 15327, 15000</li> <li>PIX firewall</li> </ul>
Huawei	<ul style="list-style-type: none"> <li>NetEngine Series and AR Series Enterprise</li> </ul>
Ericsson (Redback)	<ul style="list-style-type: none"> <li>SmartEdge Services Router</li> </ul>
Brocade (Foundry)	<ul style="list-style-type: none"> <li>NetIron IMR and XMR Series</li> </ul>
ECI Telecom LTD	<ul style="list-style-type: none"> <li>T: :D A X</li> </ul>
Dell (Force10)	<ul style="list-style-type: none"> <li>Force10 E Router</li> </ul>
Lucent Technologies (Ascend Communications)	<ul style="list-style-type: none"> <li>B-STDx</li> <li>CBX 500, GX 550</li> </ul>
Marconi	<ul style="list-style-type: none"> <li>ForeRunner ASX, TNX</li> </ul>
net.com	<ul style="list-style-type: none"> <li>Micro20, IDNX20/70/90</li> <li>Promina 100/200/400/800</li> <li>FrameXpress, CellXpress, SCLX</li> <li>SCREAM 50/100</li> <li>STM</li> </ul>
Nortel	<ul style="list-style-type: none"> <li>Multiservice Switch: 6400/7400/15000/20000</li> <li>MPE 9000 Series</li> </ul>
Sycamore	<ul style="list-style-type: none"> <li>SN3000, SN16000, SN16000SC</li> </ul>
Coriant (Tellabs)	<ul style="list-style-type: none"> <li>8800 Multi-Service Router Series</li> </ul>
RAD	<ul style="list-style-type: none"> <li>Megaplex Series, IPmux Series</li> </ul>

**Related Documentation** • [IP/MPLSView Installation Overview on page 29](#)

- [Installing the IP/MPLSView Server, Client, Traffic Data Collector, and Rsync Package on page 32](#)

## Required Ports to Open in Firewalls

[Table 9 on page 21](#) lists the ports that need to be opened between the client and the server so that the client and server 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 9: Required Ports to Open in Firewalls for Servers**

Default Port Number	Used For
TCP 7000	Connection to IP/MPLSView server
TCP 5672	Connection for IP/MPLSView to NorthStar Controller traffic
TCP 3389	LDAP (user login and administration)
TCP 8091	Webserver (HTTP)
TCP 8443	Webserver, SSL (HTTPS)
TCP 2099	Task Manager (RMI registry)
TCP 1856	JMS JNDI / RMI, JMS Bi-Socket (traffic collection)
TCP 8093, 8094	Telnet Proxy (connect to device)
TCP 1098, 1099, 3873, 7911	JNDI, RMI, EJB (used for SNMP, CLI, processes, and client-server file access).
7077	Event post Pport
27017	MongoDB application server

**Table 10: Required Ports to Open in Firewalls for Protocols**

Default Port Number	Used For
TCP 22	SSH
TCP 23	Telnet
UDP 161	SNMP GET
UDP 162	SNMP trap

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, see [“Additional Steps for Installing IP/MPLSView in a NAT Environment” on page 44](#).

For more information about SSH tunneling, see [“Setting Up Port Forwarding for Secure Communications” on page 150](#).

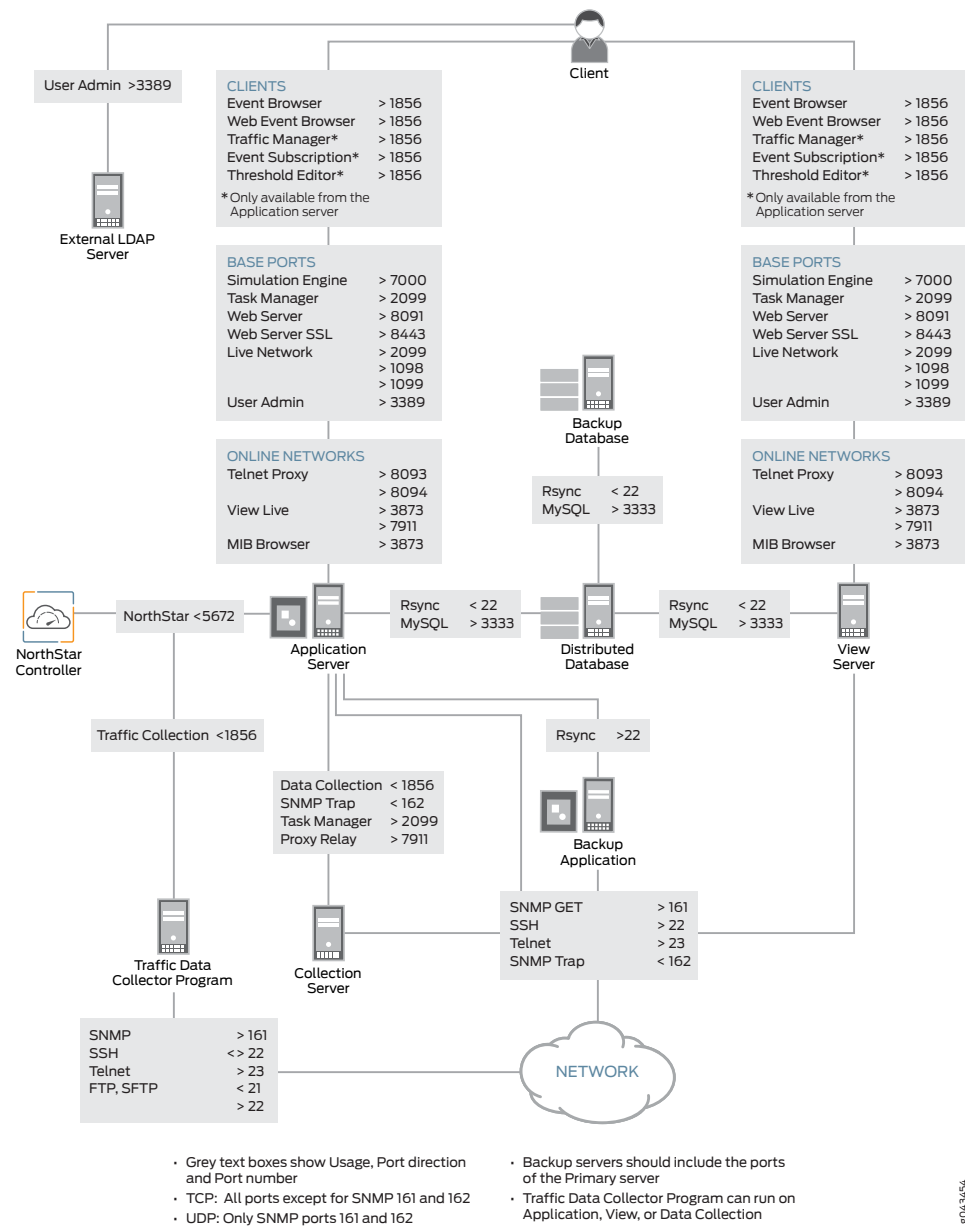
## Port Map

[Figure 1 on page 23](#) illustrates the required ports and direction in a completely distributed environment using all server packages.



NOTE: The illustrations shows data flows, not physical connections.

*Figure 1: Port Map*



## Key

In the illustration:

- **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 an asterisk (\*) 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 Traffic Data Collector program packages on the application server. If these packages are not specified as distributed, then the port and direction along those paths can be ignored.
- The **Client** is the client machine running either Windows or Java Web Start.
- The **Traffic Data Collector** can be used to distribute the traffic collection.

### Advanced Configuration

- The **Viewserver** complements the application server by offering a streamlined client for network operators and planners who don't require the full capabilities of the application server. Only network administrators need the full capabilities of the client connected to the application server. Using the Viewserver offloads users and system resources from the application server.
- The **Distributed Database** server can be used for data storage on a server other than the application server.
- The **Collection Server** can be used for the remote VLAN autodiscovery module and remote data collection.
- The **External LDAP** server can be used for user administration and authentication on a server other than the application server. For more information, see the *Security Management* chapter in the *IP/MPLSView Java-based Management and Monitoring Guide*.
- The **Backup Application** server can be used with Rsync packages for redundancy.
- The **Backup Database** server can be used with Rsync and Replication packages for redundancy.

## Port Table

Table 11 on page 24 lists the required ports and direction by suite, module, or package for clients.

Table 11: IP/MPLSView Port Table For Clients

Source > Destination	Usage	Destination Port	Modules
Client > Application and Viewserver	Simulation Engine	7000	Management, Provision, Design Essentials
Client > Application and Viewserver	Task Manager	2099	Management, Provision, Design Essentials
Client > Application and Viewserver	Web Server	8091	Management Essentials, Web



**Table 11: IP/MPLSView Port Table For Clients (continued)**

Source > Destination	Usage	Destination Port	Modules
Client > Application and Viewserver	Web Server SSL	8443	Optional Secure Web
Client > Application and Viewserver	Live Network	2099, 1098, 1099	Management, Provision Essentials
Client > Application and Viewserver	Telnet Proxv	8093, 8094	Management, Provision Essentials
Client > Application and Viewserver	View Live	3873, 7911	Performance Management
Client > Application and Viewserver	MIB Browser	3873	MIB Browser
Client > Application and Viewserver	Event Browser	1856	Fault Management
Client > Application and Viewserver	Web Event Browser	1856	Fault Management
Client > Application and Viewserver	User Admin	3389	Security Management
Client > External LDAP	User Admin	3389	Security Management

[Table 12 on page 25](#) lists the required ports and direction by suite, module, or package for the application client only.

**Table 12: IP/MPLSView Port Table for the Application Client**

Source > Destination	Usage	Destination Port	Modules
Client > Application	Traffic Manager	1856	Performance Management
Client > Application	Event Subscription	1856	Fault Management
Client > Application	Threshold Editor	1856	Threshold Crossing Alerts

[Table 13 on page 25](#) lists the required ports and direction by suite, module, or package for the application and Viewserver.

**Table 13: IP/MPLSView Port Table for the Application and Viewserver**

Source > Destination	Usage	Destination Port	Modules
Application and Viewserver > Network	SNMP Get	161	Performance Management

**Table 13: IP/MPLSView Port Table for the Application and Viewserver (continued)**

Source > Destination	Usage	Destination Port	Modules
Application and Viewserver > Network	SSH	22	Management, Provision Essentials
Application and Viewserver > Network	Telnet	23	Management, Provision Essentials
Network > Application and Viewserver	SNMP Trap	162	Fault Management
Application and Viewserver > Database	Rsync	22	Rsync and Replication
Application and Viewserver > Database	MySQL	3333	Distributed Database
Traffic Data Collector > Application and Viewserver	Traffic Data Collection	1856	Performance Management

[Table 14 on page 26](#) lists the required ports and direction by suite, module, or package for the Traffic Data Collector.

**Table 14: IP/MPLSView Port Table for the Traffic Data Collector**

Source > Destination	Usage	Destination Port	Modules
Traffic Data Collector > Network	SNMP Get	161	Performance Management
Traffic Data Collector > Network	SSH	22	Performance Management
Traffic Data Collector > Network	Telnet	23	Performance Management
Network > Traffic Data Collector	FTP, SFTP	21, 22	Performance Management

[Table 15 on page 26](#) lists the required ports and direction by suite, module, or package for the primary and backup application servers.

**Table 15: IP/MPLSView Port Table for the Primary and Backup Servers**

Source > Destination	Usage	Destination Port	Modules
Primary Application > Backup Application	Rsync	22	Rsync and Replication
Primary Database > Backup Database	Rsync	22	Rsync and Replication

*Table 15: IP/MPLSView Port Table for the Primary and Backup Servers (continued)*

Source > Destination	Usage	Destination Port	Modules
Backup Database > Primary Database	MySQL	3333	Rsync and Replication

[Table 16 on page 27](#) lists the required ports and direction by suite, module, or package for the Remote Collection Server.

*Table 16: IP/MPLSView Port Table for the Remote Collection Server*

Source > Destination	Usage	Destination Port	Modules
Remote Collection Server > Application	Data Collection	1856	Management Essentials
Remote Collection Server > Application	SNMP Trap	162	Management Essentials
Application > Remote Collection Server	Task Manager	2099	Management Essentials
Application > Remote Collection Server	Proxy Relay	7911	Management Essentials

**Related Documentation**

- [Recommended System Configuration on page 17](#)
- [IP/MPLSView Installation Overview on page 29](#)
- [Installing the IP/MPLSView Server, Client, Traffic Data Collector, and Rsync Package on page 32](#)
- [Traffic Updates from IP/MPLSView to NorthStar Controller Overview on page 67](#)



## CHAPTER 2

# Installing IP/MPLSView

- [IP/MPLSView Installation Overview on page 29](#)
- [Installing the IP/MPLSView Server, Client, Traffic Data Collector, and Rsync Package on page 32](#)
- [Additional Steps for Installing IP/MPLSView in a NAT Environment on page 44](#)
- [Installing IP/MPLSView as a Non-Root User on page 45](#)
- [Installing IP/MPLSView Without Reusing Existing Settings and Data on page 46](#)
- [Updating the IP/MPLSView Server on page 47](#)
- [Installing the IP/MPLSView Distributed Database and Traffic Data Collector on page 47](#)
- [Installing the IP/MPLSView Client on a PC on page 49](#)

## IP/MPLSView Installation Overview

---

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



**NOTE:** Starting with Release 6.3.0, IP/MPLSView uses MariaDB. For simplicity, some of the directories might still be named `mysql` and some of the installation scripts might still display `MySQL`.

### Installing Linux OS on Your Servers

Before you install any of the compatible 64-bit Linux distributions on your servers, make sure your systems have static IP addresses configured for all of the interfaces that will be used.

- When installing, use the minimal desktop installation option according to your local policies.
- As a best practice, we recommend that after installing Linux, you update the 64-bit OS installation packages on each server by using the following command:

```
yum -y update
```

If you want to update only specific packages, use the following command and specify the packages you want to update:

```
yum -y update package-name
```

- Update the **/lib64/libaio.so.n** library using the following command:

```
yum install libaio
```

- Install the nonstandard telnet and ksh packages.
- If installing for high availability (HA), assign private IP addresses (such as 10.10.10.0/24) between the **eth1** interfaces.

For more information regarding HA installation, see [“Installing the Linux Operating System for IP/MPLSView High Availability” on page 105](#).

- As the root user, use the following commands to disable the iptables, ip6tables, and NetworkManager services.

For CentOS 6.6:

```
chkconfig iptables off
chkconfig ip6tables off
chkconfig NetworkManager off
```

For CentOS 7.0:

```
sysctl disable firewallld
```

- As the root user, edit the file **/etc/sysconfig/selinux** and disable SELinux by changing the entry in the file from **enforcing** to **disabled**.

Disabling SELinux prevents it from blocking or interfering with some of the ports that must be opened for high availability and the application.

- As the root user, edit the file **/etc/sysctl.conf** and add the following two lines to disable IPv6 networking:

```
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
```

- Reboot the device.

[Table 17 on page 30](#) describes the settings used during the installation.

**Table 17: Installation Settings**

Settings	Description
General	Contains settings for the NPAT Server, the Task Server, and the SNMP Trap Daemon.

*Table 17: Installation Settings (continued)*

Settings	Description
Email	Contains e-mail settings for the Event Server, enabling the automatic notification of certain events using e-mail.
Event	Contains settings for the Event Server.

[Table 18 on page 31](#) describes the components used during the installation.

*Table 18: Installation Components*

Components	Description
NPAT Server	The core design and simulation engine.
Task Server	The server process that powers the Task Manager ( <b>Application &gt; Task Manager</b> ). 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.
MariaDB	The database used to store traffic collection data.
Web Server	The server process that powers the IP/MPLSView Web interface as well as the online help (accessed through 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.
Event Server	The server process that powers the Event Map ( <b>Application &gt; Maps &gt; Event Map</b> ) and Event Browser ( <b>Application &gt; Event Browser</b> ). In the live network, the event server manages and monitors events and SNMP traps on network devices.
Data Gateway Server	The server process that takes traffic collection data from the data collectors and stores it in the MariaDB database.
Aggregation Crontask	A scheduled task that aggregates the traffic collection data stored in the MariaDB database.
LDAP Server	Lightweight Directory Access Protocol needed for user administration.

#### Related Documentation

- [Installing the IP/MPLSView Server, Client, Traffic Data Collector, and Rsync Package on page 32](#)
- [Additional Steps for Installing IP/MPLSView in a NAT Environment on page 44](#)
- [Installing the IP/MPLSView Distributed Database and Traffic Data Collector on page 47](#)
- [Installing IP/MPLSView as a Non-Root User on page 45](#)
- [Installing IP/MPLSView Without Reusing Existing Settings and Data on page 46](#)

## Installing the IP/MPLSView Server, Client, Traffic Data Collector, and Rsync Package

This procedure describes how to install the default IP/MPLSView servers and clients. The procedure installs the following:

- The Application Server is the main data processing and simulation server. The default installation settings install the Database, LDAP, and Traffic Data Collector packages on the application server.
- The Client is the client running on the local server.
- The Traffic Data Collector is used to distribute the traffic collection.
- The replication and rsync package is used to keep the files and database on the primary server and a secondary server in sync.

To install the IP/MPLSView servers and clients, follow the steps in the following procedures:

- [Downloading and Extracting the IP/MPLSView Software on page 32](#)
- [Preparing for Installation on page 33](#)
- [Starting the Server Installation on page 35](#)
- [Installation Main Menu Advanced Options on page 37](#)
- [Installing the IP/MPLSView Client on the Local Server on page 42](#)
- [Installing the Traffic Data Collector on the Local Server on page 43](#)
- [Installing the Replication and Rsync Package on the Local Server on page 43](#)

### Downloading and Extracting the IP/MPLSView Software

To download and extract the IP/MPLSView software:

1. Access the Juniper WANDL IP/MPLSView - Download Software page at <https://www.juniper.net/support/downloads/?p=wandl#sw>. Select the install package. The package name is similar to **WANDL IP/MPLS View, version X.X.X, Linux!**.
2. Download the software bundle. The filename is similar to **MPLSView\_621\_Linux\_0128\_17.tar.gz**.
3. Copy the file to a directory on the server where you want to install IP/MPLSView.
4. Extract all the files using the following command:

```
gunzip < MPLSView_621_Linux_0128_17.tar.gz | tar xvf -
```



The extracted files are used by the install script. You are now ready to install the application server using the instructions in this topic.

5. Some compressed files are also extracted. The compressed files are used to install individual packages such as the client, dcollect, and optionally the replication package on separate servers.

To extract the compressed files that end in .tar.gz on the target server:

```
gunzip < dcserver.tar.gz | tar xvf -
gunzip < dserver_linux.tar.gz | tar xvf -
gunzip < ljavafiles.tar.gz | tar xvf -
```

To extract the compressed files that end in .tar on the target server:

```
tar xvf dcserverFiles.tar
tar xvf replication.tar
```

Exact filenames might vary.

## Preparing for Installation

IP/MPLSView Release 6.2.1 and later releases are only supported on 64-bit processors. To verify that your server has a 64-bit processor, use the following command:

```
uname -a
```

Before upgrading IP/MPLSView from a previous installation, ensure that your customer maintenance license has not expired. To verify your license:

```
$cat /u/wanddb/sys/npatpw
expire_date=0
hostid= 1234567(hex)
node_limit=500
usercount=5
viewercount=5
webviewer=20
customer=TMP CUSTOMER
maintenance=12/31/2016
# General Passwords
~
~
~
```

The contents of the **npatpw** license file varies depending on the type of server you are using. Verify that the date in the *maintenance* line has not passed, as shown in the sample output.

If you upgrade IP/MPLSView after the customer maintenance license has expired, the upgrade succeeds but you are not be able to access the GUI interface.

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. For example:

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

If the previous IP/MPLSView installation includes traffic collection, we recommend that you back up the data. Check for sufficient disk space using the following command:

```
$ df -k
```

Compress and zip the files using the following 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**.

Log in as the root user. If you do not have direct access, 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, you should 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 an IP address configured for the external network. For the server 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 IP address is a private NAT IP address, and the client needs to reach it over the public NAT IP address. For more information about setting up the installation to support NAT environments, see [“Additional Steps for Installing IP/MPLSView in a NAT Environment” on page 44](#).

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, run a traceroute to the hostname on the server using the following command and verify that the results include the desired IP address:

```
/usr/sbin/traceroute hostname
```

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 following command as the root user and substitute the *groupname* with a name of your choosing:

```
groupadd groupname
```

To create a new user ID named *wandl*, in the group named *staff*, with the administrative home directory, or *\$HOME*, set to */home/wandl*, for the IP/MPLSView admin, use the following command as the root user:

```
useradd -g staff -s /bin/ksh -d /home/wandl -m wandl
```

Create your administrative home directory with the correct ownership and privileges for the administrative user. For example, if the administrative home directory is */home/wandl*, use the following two commands to give *wandl* ownership of the directory, give *wandl* full privileges, and give other users read and execute privileges:

```
chown -R wandl:staff /home/wandl
```

```
chmod -R 755 /home/wandl
```

After adding a new user, create a password (for example, *wandl*) for the new user using the following command:

```
passwd wandl
```



**NOTE:** If your machine is under your company NIS or NIS+ system, the local root access might not be able to create a new group, or the creation might cause conflicts with the NIS/NIS+ system. In this case, ask the NIS system administrator to create the proper group and add all the users to the group before installing IP/MPLSView.

## Starting the Server Installation

The following are general instructions for the installation:

- File paths are assumed to be under the server directory where you extracted the files.
- During the installation, press Enter without entering any text to select the default settings.
- At any time during the installation, you can press Ctrl-c to abort the installation.

To install IP/MPLSView:

1. Run the installation script as root.

```
# ./install.sh
```

The system prompts you to continue.

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

2. The first required general setting is the Admin User, which defaults to the **wandl** user. Enter a valid system user ID other than **root**.

This software requires a Linux ID as the owner.  
A Linux ID is the login name when you login to this Linux server

```
Please input the IP/MPLSView user ID (wandl):
Owner is set to: wandl
```

3. The second required 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. If this group does not exist, the installation program creates one and asks 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. In this case, you need to contact your system administrator to add all the users into the group.

```
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
```

4. The third required general setting is the installation directory. Make sure there is sufficient disk space to install the program (approximately 1 GB). The directory is created by the installation program if it does not already exist. At the end of the installation, the `/u/wandl/` directory is automatically linked to this directory.



**NOTE:** Do not use the operating system partition “/” for the installation directory as this might 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, we recommend installing IP/MPLSView in a new installation directory.

```
Please enter the directory where this software will be installed.
(default=/home/wandl/ipmplsview): /home/wandl/collection1010
Are you sure you want to install into /home/wandl/ipmplsview (default=yes)?
[y/n ] y
```

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



**NOTE:** If you are upgrading from a previous installation and have previously collected data that you still want to load from IP/MPLSView, enter the complete path for that data directory. To determine that path, use the `ls -l /u/wandl/data` command. Due to database structural changes, we recommend that you back up the previous data directory. If you do not have any previously collected data, we recommend that you perform a fresh install with a new data directory.

```
Please enter the directory where the data will be stored.
(default=/home/wandl/wandldata):
```

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

## Installation Main Menu Advanced Options

This procedure describes setting advanced installation options. Some of these options can be changed after installation using the `/u/wandl/bin/changeconfig.sh` script. Changing these settings requires first stopping IP/MPLSView using the `/u/wandl/bin/stop_mplsview` command. After the settings have been changed, restart IP/MPLSView using the `/u/wandl/bin/startup_mplsview` command.

1. After the installation script finishes prompting for required settings, the Main Menu is displayed.

```
Main Menu
Server Configuration Settings:
(A) Overall Settings
(B) IP Address
(C) Memory Settings
(D) Port Settings
(E) Data Storage Capacity Settings
(F) Online Fault Management Settings
(G) Advanced Configuration
(H) NorthStar AMQP Settings
```

2. Select **(A) Overall Settings** to display the following General Administrative Settings:

```
(A) Overall Settings
General Administrative Settings:
1.) Installation Directory.....: Application server installation directory.
2.) Data Directory.....: User data and MariaDB database directory.
3.) Admin User.....: Super-user name.
4.) Admin Group.....: Super-user group.
5.) Email Server IP.....: Email server IP.
6.) Email Server User.....: wandl
7.) Email Server Password.....:
8.) Application Monitor Email Recipient...:
9.) Enable Server Monitoring.....: OFF
10.) Mapping for non-Unicode characters....:
Please select a number to modify.
[<CR>=return to main menu]:
```

3. Select **5.) Email Server IP**. The e-mail server IP address 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 address 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 might need to be configured accordingly.
4. To set up your server to send e-mail, edit the `/etc/hosts` file as follows, and then run the `svcadm restart sendmail` command or the `/etc/init.d/sendmail stop;`  
`/etc/init.d/sendmail start` command, depending on your environment.

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

In this example, it is assumed that the e-mail server is on the same subnet or that there is a route to reach it.

5. To have the application monitor notify you via e-mail of IP/MPLSView application process status information, such as when processes go down, select **9.) Enable Server Monitoring**. This setting allows you to view the application processes monitored by Application Monitor from the Web by selecting **Admin > View > System Monitor**.
6. To change the character encoding used by IP/MPLSView in both the Java and Web interface, select **10.) Mapping for non-Unicode characters**. This feature might 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 `/usr/bin/iconv -l` command. When prompted for a new coding, enter the code set name. Note that the code set name is case sensitive.
7. From the Main Menu, select **(B) IP Address**. The IP Address menu is displayed.

```
(B) IP Address
IP/MPLSView Server IP Address Settings:
1.) Webserver IP.....:
2.) LDAP Server IP.....:
3.) External Webserver IP (for NAT)....:
4.) Mongo DB IP.....:
5.) Use Remote Maria Database.....: NO
```
8. Select **1.) Webserver IP**. Enter the webserver IP address. The webserver IP address is used to access the Web interface. It is usually the same as the server IP address. If the server has more than one interface with different IP addresses, verify that the server IP address used is accessible by the client. For more information, see [“Preparing for Installation” on page 33](#).
9. Select **2.) LDAP Server IP**. The LDAP server IP address is required for IP/MPLSView user administration. Set it to the same address as the server IP address.
10. Select **3.) External Webserver IP (for NAT)**. The external webserver IP address 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 address to the public NAT IP address and enable the option for NAT. For more information, see [“Additional Steps for Installing IP/MPLSView in a NAT Environment” on page 44](#).
11. Select **4.) Mongo DB IP**. Set the address to be the MongoDB local host or remote server IP address.
12. Select **5.) Use Remote Maria Database**. If you want to set up the server environment as a distributed database, set this option to YES. Setting the option to YES installs the MariaDB database on a server other than the IP/MPLSView application server. (see [“Preparing for Installation” on page 33](#).) A menu is displayed with options to set the remote Maria database IP address and port.

13. Select **Remote Maria Database IP**. Set this to the IP address of the remote database server.
14. Select **Remote Maria Database Port**. Set this to the protocol port of the remote database server.
15. From the Main Menu, select **(C) Memory Settings**. The Memory Settings menu is displayed.

```
(C) Memory Settings
1.) Task Manager Memory.....: 512
2.) Webserver Memory.....: 256
3.) Thrift Server Memory.....: 256
4.) HornetQ Memory.....: 256
5.) DGS Memory.....: 512
6.) Application Monitor Memory.....: 128
7.) Threshold Server Memory.....: 256
8.) SNMP Trap Daemon Memory.....: 128
9.) MongoDB Memory.....: 512
10.) Event Server Memory.....: 256
11.) PM Aggregation Memory.....: 256
12.) Selective Interface Manager Memory.....: 256
13.) Maria Database Memory.....: 256
Total system physical memory: 3933 Megabytes
```

16. Set the memory settings for your server environment.

You can display how much physical memory (RAM) is available on your server using the **more /proc/meminfo** command. Some servers might not support more than 2048 MB per process even if the total RAM resources are larger than 2 GB.

You can display memory usage during operation using the **/u/wandl/bin/status\_mplsview** command.

17. From the Main Menu, select **(D) Port Settings**. The Port Settings Server to Client Settings and Port Settings (Advanced) menus are displayed.

```
(D) Port Settings
Server to Client 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)
11.) SNMP Trap Daemon Port.....: 162
12.) Event Post Port.....: 7077
```

- 13.) MariaDB Database Port.....: 3333
- 14.) MongoDB Application Server Port...: 27017

The Port Settings Server to Client Settings menu items 1 through 7 are the required ports to open between the server and client. Generally, you do not need to modify these ports unless they are in conflict with other applications which need to use them 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. See [“Required Ports to Open in Firewalls” on page 21](#).

The Port Settings (Advanced) menu items 11 through 14 are the required ports to open when advanced settings are used. Generally, these ports do not need to be modified.

18. From the Main Menu, select **(E) Data Storage Capacity Settings**. The Data Storage Capacity Settings menu is displayed.

- (E) Data Storage Capacity Settings
- Performance Management Data Max Storage Days:
- 1.) Traffic - Live.....: 60
- 2.) Traffic - Aggregated.....: 180
- 3.) Traffic - Archived.....: 100
- 4.) LDP Traffic.....: 180
- 5.) LSP Traffic.....: 180
- 6.) Device and Network - Live.....: 180
- 7.) Device and Network - Archived.....: 180
- Fault Management Data Max Storage Days:
- 8.) SNMP Trap.....: 60
- 9.) Network Event.....: 180
- Configuration Management Data Max Storage Days:
- 10.) Hardware Inventory.....: 60
- Administration Data Max Storage Days:
- 11.) User Activity.....: 60

The following list describes the data storage capacity settings. Make the appropriate changes for your environment:

**Traffic – Live**—Set this to the number of days you want the 5-minute traffic data stored in the MariaDB.

**Traffic – Aggregated**—Set this to the number of days you want the hourly traffic data, aggregated on a daily basis, stored in the `/u/wandl/data/traffic_history` directory.

**Traffic – Archived**—Set this to the number of days you want the aggregated traffic stored in the database for daily, weekly, monthly, and yearly reports.

**LDP Traffic**—Set this to the number of days you want the LDP traffic collected using TaskManager to be stored in the file system.

**LSP Traffic**—Set this to the number of days you want the LSP traffic collected using TaskManager to be stored in the file system.

**Device and Network – Live**—Set this to the number of days you want the device and network performance data to be stored in the file system.



**Device and Network – Archived**—Set this to the number of days you want the device and network performance data aggregated and stored in the database for daily, weekly, monthly, and yearly reports.

The following list describes the Fault Management Data Max Storage Days settings. Make the appropriate changes for your environment:

**SNMP Trap**—Set this to the number of days you want the raw SNMP trap to be stored in the `/u/wandl/data/trap` file.

**Network Event**—Set this to the number of days you want the network event data to be stored in the database.

19. From the Data Storage Capacity Settings menu, select **10.) Hardware Inventory**. Set this to the number of days you want network event data to be stored in the database.
20. From the Data Storage Capacity Settings menu, select **11.) User Activity**. Set this to the number of days you want the user activity logs to be stored in the database.
21. From the Main Menu, select **(F) Online Fault Management Settings**. The Online Fault Management Settings menu is displayed.

```
(F) Online Fault Management Settings
SNMP Trap Settings:
1.) SNMP Trap Daemon IP.....: xxx.xxx.xxx.xxx
2.) Enable Trap Forwarder.....: OFF
3.) Trap Forwarding Upstream Address...:
4.) Trap Forwarding Upstream Port.....:

Event Settings:
5.) Threshold Initial Notification...: OFF

Background Ping Settings:
6.) Background Ping.....:Yes
Background Ping Interval.....:Yes
Background Ping Number of Retry.....:Yes
Background Ping Retry.....:Yes
Background Ping Interval.....:Yes
Background SNMP connectivity test.....:Yes
Background connectivity test via telnet/SSH...:Yes
Use FPING.....:Yes
```

22. Select **1.) SNMP Trap Daemon IP**. Set this to the IP address of the IP/MPLSView server which receives traps from network devices. Make sure it is reachable by network devices, and is configured on the network devices as the SNMP target address.
23. Select **2.) Enable Trap Forwarder**. As necessary, enable or disable trap forwarding to a third-party server.
24. Select **3.) Trap Forwarding Upstream Address**. If necessary, set this to the IP address of a third-party NMS supporting JMS to forward traps from IP/MPLSView. Make sure that the IP address is reachable from the IP/MPLSView application server, and that

the third party device is listening on port 162 (the default). Additional configuration is also required by selecting **Application > Event Subscription Editor**. For more information, see the *IP/MPLSView Java-Based Management and Monitoring Guide*.

25. Select **4.) Trap Forwarding Upstream Port**. If necessary, set this to the protocol port of a third-party server.
26. Select **5.) Threshold Initial Notification**. Enable or disable initial threshold notification.
27. Select **6.) Background Ping**. The background ping allows you to ping all devices in the live network and sends an event to the Event Browser if a device becomes unreachable.

There is a setting (not part of this installation procedure) that allows you to multi-thread the ping process for faster performance and add additional device profiles not collected in the network. The additional devices appear as an event in the Event Browser when it becomes unreachable. Edit the `/u/wandl/db/config/diag.xml` file. 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 the `/u/wandl/data/TaskManager/profile/` directory. Changes to the `diag.xml` file take effect when the network is loaded. For more information, see the *IP/MPLSView Java-Based Management and Monitoring Guide*.

28. To enable the distributed remote collection servers, select **(G) Advanced Configuration** from the Main Menu. The Advanced Configuration menu is displayed.

```
(G) Advanced Configuration
Advanced Configuration Settings:
1.) Distributed Collection Servers.....:
2.) Database Temp Directory.....:
3.) Email Sender Address.....:
```

29. From the Advanced Configuration menu, select **1.) Distributed Collection Servers**. You must also create a file containing a list of IP addresses and ports (IP\_address:port) of the remote collection servers. The port is normally 2099.
30. From the Advanced Configuration menu, select **2.) Database Temp Directory** and enter a temporary directory used by the MariaDB server for daily traffic aggregation.
31. From the Advanced Configuration menu, select **3.) Email Sender Address** and enter the e-mail address for task server notifications.

## Installing the IP/MPLSView Client on the Local Server

After installing the server, the script prompts you to install the client on the machine.

You can install the client at a later time by running the following script as a non-root user:

```
/install_dir/client/linux/install.client
```

To install the client on the local server:

1. Press Enter or **y** to continue.
2. When prompted by the installation script, enter the server name or IP address, port number for communication, the name or IP address of the application server, and the server protocol port number.

## Installing the Traffic Data Collector on the Local Server

After installing the client, the script prompts you to install the Traffic Data Collector on the machine.

To install the Traffic Data Collector on the local server:

1. Press Enter or type **y** to continue.
2. When prompted by the installation script, enter the appropriate information.

If you want to install the Traffic Data Collector on a different system, you can enter **N**, and then run the `/install_dir/dcollect/unix/install.dcollect` installation script from the other system. We recommend that you set up one Traffic Data Collector per 100 to 150 devices. When installing the Traffic Data Collector on another system, enter the IP address of the main IP/MPLSView server when prompted for the JMS server.

## Installing the Replication and Rsync Package on the Local Server

After installing the Traffic Data Collector, you might 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 the files and database on the primary server and a secondary server in sync. The purpose of the package is to have a backup copy in case the primary server fails. The rsync package backs up files from the primary application server to the backup application server, and the replication package updates the secondary database to be in sync with the primary database.



**NOTE:** The Replication and Rsync package requires the backup IP/MPLSView server to have a separate license. Additionally, the actual rsync program should be separately installed using the `/install_dir/replication/inst_rsync.sh` script if it is not already available on the server,



**NOTE:** If you want to install the Replication and Rsync package later, then enter **N** at the prompt. The installation script is also available from the `/install_dir/replication/instrepl.sh` script. Some prerequisites are required before running the script. The prerequisite steps can be performed from another open telnet or SSH session.

- Related Documentation**
- [IP/MPLSView Installation Overview on page 29](#)
  - [Installing IP/MPLSView as a Non-Root User on page 45](#)
  - [Installing IP/MPLSView Without Reusing Existing Settings and Data on page 46](#)
  - [Installing the IP/MPLSView Distributed Database and Traffic Data Collector on page 47](#)
  - [General Procedures for Troubleshooting the IP/MPLSView Installation on page 161](#)
  - [IP/MPLSView Server Installation Frequently Asked Questions on page 166](#)

---

## Additional Steps for Installing IP/MPLSView in a NAT Environment

For IP/MPLSView running in a NAT environment, two additional ports (1101 and 21101) should be opened in the firewall between the server machine and client machine. See [“Required Ports to Open in Firewalls” on page 21](#).

In addition, use the following IP address options during the server installation. In this example, the IP address for server installation is the private NAT address and the IP address for the client installation is the public NAT address.

1. To install IP/MPLSView in a NAT environment: from the Main Menu, select **(B) IP Address**. The IP Address menu is displayed.

```
(B) IP Address
IP/MPLSView Server IP Address Settings:
1.) Webserver IP.....:
2.) LDAP Server IP.....:
3.) External Webserver IP (for NAT)....:
4.) Mongo DB IP.....:
5.) Use Remote Database.....: YES
Remote Database IP.....: Private NAT IP
Remote Database Port.....: 3333
```

2. Select **1.) Webserver IP**. Enter the private NAT IP address.
3. Select **2.) LDAP Server IP**. Enter the private NAT IP address.
4. Select **3.) External Webserver IP (for NAT)**. Enter the public NAT IP address.

For more information, see “Required Ports to Open in Firewalls” in [“Installing the IP/MPLSView Server, Client, Traffic Data Collector, and Rsync Package” on page 32](#).

5. Select **5.) Use Remote Database**. Set this option to Yes. Enter the private NAT IP address and the protocol port.

Also, do the following during the remote client installation on a Windows-based PC:

1. Select the **Use HTTP Tunneling for Firewall** option during the installation, or after the client installation is complete, edit the `ipmplsview.bat` file. Add the **FIREWALL** keyword to the end of the Java command. For example:

```
%JRE% -Xms%MEMORY% -Xmx%MEMORY% -XX:NewRatio=2 -Dsun.java2d.noddraw=true
-classpath %CLASSPATH% bbdsgn %SERVER% %SERVERPORT% %WEBSERVER%
%WEBSERVERPORT%
%LDAPSERVER% %LDAPPORT% mp1sview FIREWALL
```

The `ipmplsview.bat` file can typically be found on the PC's desktop, or in the `C:\Program Files\wand\IP-MPLSViewX.X` folder, where X.X is the version number.

The following are additional things to note for using IP/MPLSView in a NAT environment:

- During the client installation, use the public NAT IP address for IP address entries.
- When launching the Web Start Client, use the public NAT IP address for the IP address.
- In the Java-based GUI, select the **Application > Options > JMS Access pane > Use HTTP Tunneling** client option.
- When opening the Traffic Collection Manager, Event Browser, or Threshold Editor window for the first time, a dialog box is displayed with configuration options. Select **Use HTTP Tunneling**. If this option is not displayed, you might need to delete any IP/MPLSView cached XML files from previous instances of these windows. On Windows-based PCs, the XML files might be in the `C:\Users\<username>\AppData\Roaming\wandl` folder.

#### Related Documentation

- [IP/MPLSView Installation Overview on page 29](#)
- [Installing the IP/MPLSView Server, Client, Traffic Data Collector, and Rsync Package on page 32](#)

## Installing IP/MPLSView as a Non-Root User

Installing IP/MPLSView using a user ID other than root ensures that no processes generated by the IP/MPLSView software 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 you must be aware of when installing as a user ID other than root. This topic refers to the user ID that installs and starts up the server as the *owner of the application*.

Read the following guidelines carefully to understand the effects of using a user ID other than root:

- The application should be brought up by the owner of the application.
- All processes are owned by the owner of the application.
- Any files generated by IP/MPLSView are owned by the owner of the application.
- If there are multiple users, all users of the application must have the same group ID as the owner of the application.

- All of the users' directories must be readable and writable by the owner of the application to ensure that all application output can be saved.
- Any future updates of the software must be performed by the owner of the application.

#### Related Documentation

- [IP/MPLSView Installation Overview on page 29](#)
- [Installing the IP/MPLSView Server, Client, Traffic Data Collector, and Rsync Package on page 32](#)

## Installing IP/MPLSView Without Reusing Existing Settings and Data

If you are installing IP/MPLSView on a server where it is already installed, there are two possible scenarios:

**Software upgrade on top of a previous installation**—In this case, the previous configuration settings and network data, including the database, are reused.

**Software installation from *scratch***—In this case, you do not want to reuse previous settings and network data. Therefore, you need a new data directory and software configuration.

To install from scratch:

1. Stop the processes of the previous installation using the following commands:

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

2. Verify that the **/u/wandl** directory is linked .

```
ls -l /u
lrwxrwxrwx 1 wandl wandl 27 Feb 16 17:55 wandl -> /home/wandl/mp1s621-0216-S1
```

If the directory is linked, the output displays **wandl ->** followed by the location to which the **/u/wandl** directory is linked.



**NOTE:** Only remove the **/u/wandl** directory if it is a link. If it is not a link, you will delete your directory.

3. If you previously installed as root and linked to the **/u/wandl** directory, remove the link using the following command:

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

4. Log in to the server as the desired user ID.
5. Run the install script as described in ["Installing the IP/MPLSView Server, Client, Traffic Data Collector, and Rsync Package" on page 32.](#)

```
cd /install_dir/server
$ ./install.sh
```

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

All IP/MPLSView files or output generated by other users are saved with the ownership of the owner of the application.

**Related Documentation**

- [IP/MPLSView Installation Overview on page 29](#)
- [Installing the IP/MPLSView Server, Client, Traffic Data Collector, and Rsync Package on page 32](#)
- [Installing IP/MPLSView as a Non-Root User on page 45](#)

---

## Updating the IP/MPLSView Server

When updating IP/MPLSView, we recommend that you install the software into a new application directory. You do not need to use the existing data directory to preserve existing data. The update automatically updates the necessary settings.

**Updating the IP/MPLSView Client**

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. See [“Installing the IP/MPLSView Client on a PC” on page 49](#).

**Updating the Distributed Database and Traffic Collectors**

Update the distributed database using the `instdatabase.sh` script. Update the traffic collectors using the `install.dcollect` script.

**Related Documentation**

- [Installing the IP/MPLSView Distributed Database and Traffic Data Collector on page 47](#)
- [Installing the IP/MPLSView Client on a PC on page 49](#)

---

## Installing the IP/MPLSView Distributed Database and Traffic Data Collector

This topic describes how to install the MariaDB database on a different machine from the IP/MPLSView server.

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 public key (`id_rsa.pub`) must be present in the IP/MPLSView application server authorized keys (`~wandl/.ssh/authorized_keys`). Do this for the `wandl` user (not root user). Copy over the public key to the remote server `.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.

For more information about public keys, see [“Installing the Rsync Package and Automating SSH Login” on page 74](#).

During the installation of the IP/MPLSView application server, configure the settings for the Distributed Database under IP/MPLSView Server IP Address Settings. After the database and the IP/MPLSView application server are installed, the database server should be started before starting the IP/MPLSView application server.

To install the MariaDB distributed database:

1. Verify that Rsync is installed on the database server using the following command:

```
pkginfo | grep rsync
```

2. If Rsync is not installed, install it by using the following script as the root user:

```
replication/inst_rsync.sh
```

3. Switch to the root user.

```
su
```

4. Change directory to the installation server directory, and use the install script.

```
cd /install_dir/  
./instdatabase.sh
```

The install script prompts you to shut down all servers.

5. Accept the default to shut down the servers.

The install script prompts you to enter the directory where the software should be installed.

6. Enter the directory path. For example:

```
/home/wand1/mp1s621-01210-d
```

The install script prompts you to confirm that you want to install in that directory.

7. Accept the default.

The install script prompts you to enter the directory where the data is stored.

8. Enter the directory where you want the data to be stored or accept the default. The default is:

```
/home/wand1/wand1data6
```

The install script displays General Settings, MariaDB Settings, and Aggregation Settings.

9. Change the settings if necessary, then accept the settings to continue.

The install script prompts you to install Rsync.

10. Accept the default.



11. After a few minutes, the install script prompts you to update the link to the `/u/wandl` directory.
12. Accept the default.
13. The install script completes and prompts you to start the database server.

To install the distributed Traffic Collector:

1. Switch to the admin user (wandl).

```
su wandl
```

2. Change directory to the installation server directory, and use the install script.

```
cd /install_dir/dcollect/linux/  
./install.dcollect
```

Follow the installation instructions as they appear on the screen.

**Related  
Documentation**

- [Installing the IP/MPLSView Server, Client, Traffic Data Collector, and Rsync Package on page 32](#)
- [Updating the IP/MPLSView Server on page 47](#)

---

## Installing the IP/MPLSView Client on a PC

This topic describes how to install the IP/MPLSView client on a Windows-based PC.

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

To install the client:

1. Download the **installIPMPLSView.exe** file to the client PC.
2. Double-click the **installIPMPLSView.exe** icon.  
  
The installer program prompts you to enter the name or IP address of the server on which you have IP/MPLSView installed.
3. Enter the IP address or hostname if your hostname is listed in the hosts file of your PC.
4. Select the default port number for the server, unless those ports were configured for a non-default port.

The installer program prompts you to set the RAM allocation for the application.

5. Set the RAM allocation. Generally a higher setting allows for better application performance for large networks. However, reserve some RAM for other applications that you might be running at the same time.
6. Select the directory in which to install the client. The default directory is **C:\Program Files\wand\IP-MPLSViewx.x**, where **x.x** is the release number. Alternately, use the **Browse** button to select the directory of your choice.

During the installation, you can click **Back** at any time to go back to a previous step to make corrections. You can click **Cancel** at any time to exit the installation program and install at a later time.

After the client installation is complete, the system creates the **ipmplsview.bat** file in the installation directory. To modify the IP address, port information, and memory options after the installation, edit the **ipmplsview.bat** file using a text editor such as Notepad.



**NOTE:** For Windows Vista users, the installation directory and **ipmplsview.bat** file are read-only by default. To change the permission, navigate to the **C:\Program Files\wand\** 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** is allowed.

For information about launching the PC client, see “Launching the Viewserver Client” in [“Installing the Viewserver” on page 59](#).

#### Installing The Java Web Start Client

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 might take a few minutes to download all the necessary files the first time the client is launched. Afterwards, all subsequent launches are instantaneous. Web Start also performs version control, so if there is a new version of the application installed on the server, it upgrades the client automatically at runtime. In this way, the server and client are always in sync.

#### Related Documentation

- [IP/MPLSView Installation Overview on page 29](#)
- [Installing the IP/MPLSView Server, Client, Traffic Data Collector, and Rsync Package on page 32](#)
- [Launching the IP/MPLSView Client on page 143](#)
- [IP/MPLSView Client Installation Frequently Asked Questions on page 169](#)

## CHAPTER 3

# Installing the Remote Collection Server

- [Remote Collection Server Overview on page 51](#)
- [Installing the Remote Collection Server on page 52](#)

## Remote Collection Server Overview

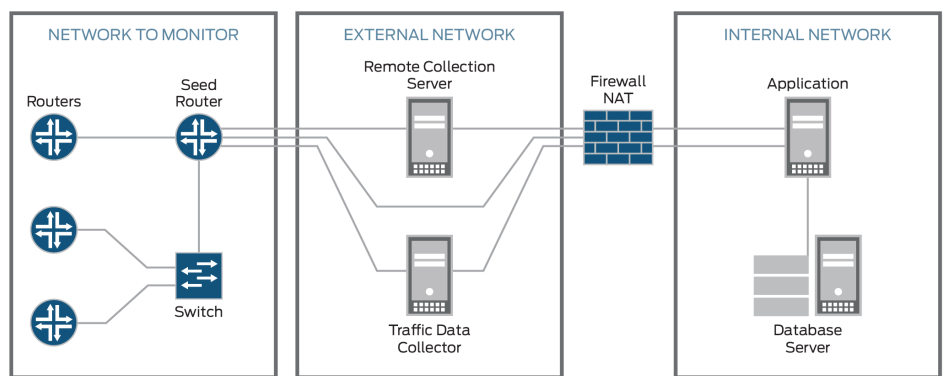
The remote collection server is a distributed CLI/SNMP poller that can be used for VLAN autodiscovery, CLI collection, and device and network performance data collection. When a task is run from the Task Manager on the central parsing server, the task can be dispatched to the remote collection server. The final results are transferred back to the central application server.



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

The remote collection server can be used to reach the network you are monitoring with IP/MPLSView when it cannot be accessed directly by the application server. This situation might arise when the application server on your internal network is separated by a firewall from the network being monitored. [Figure 2 on page 51](#) illustrates this scenario.

*Figure 2: Sample Environment Using a Remote Collection Server*





**NOTE:** There are certain discovery tasks that cannot be run on the remote collection server. Therefore, one router (shown in [Figure 2 on page 51](#) as the seed router) on the network to be monitored, must be reachable from the application server over the following ports: TCP port 22 (ssh), UDP port 161 (SNMP Get), UDP port 162 (SNMP Trap), and ICMP type 0 and 8 (ping).



**NOTE:** The remote collection server is not the same as the agent configured in the device profile window. The Agent(s) field in the device profile is used to identify an intermediate host that the application server can log in to, and from there log in to the network device to perform CLI operations.

**Related  
Documentation**

- [Installing the Remote Collection Server on page 52](#)

## Installing the Remote Collection Server

The collection server package should be installed on each remote collection server. During the installation of the remote collection server, the IP address of the central parsing server should be entered. The central parsing server is also installed. During the installation of the central parsing server, the IP addresses of the remote collection servers should be entered. This section discusses how to install the remote collection server.

To install the remote collection server package:

1. Log in as the root user, browse to the jump directory, and install the remote collection server 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 you want to install the server. For example, **/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 the menu items 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 the installation.
  9. Enter **y** to install the Traffic Data Collector package.
  10. Switch out of root user to the user ID given in Step 2. Start the remote collection server.
- ```
> /u/wandl/bin/startup_collection
```

### Example Installation

The following example is a remote collection server installation run by the root user ID for a first-time installation. In this example, 10.0.0.5 is the IP address of the remote collection server being installed, and 192.168.1.3 is the IP address of 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 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 Server Management Facility before restarting the
IP/MPLSView installation. If IP/MPLSView
is not configured (or is already disabled) in the
Server Management Facility, then please ignore
this message and continue with the installation.
```

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

```
Checking patches ...
```

```
This software requires a Linux ID as the owner.
A Linux ID is the login name when you login to this Linux 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]
Shutdown Task Manager(pid=21939) ...
Shutdown HornetQ Collection Server(pid=21921) ...
```

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

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

Checking available disk space ...

Copying Java native library files...

Copying Java native library files...

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

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

SNMP Settings:
4.) SNMP Trap Daemon IP.....: 172.25.153.122
5.) SNMP Trap Daemon Port.....: 162
6.) SNMP Trap Daemon Memory....: 128
7.) SNMP Trap Store Capacity...: 30

SNMP Settings:
4.) SNMP Trap Daemon IP.....: 172.25.153.122
5.) SNMP Trap Daemon Port.....: 162
6.) SNMP Trap Daemon Memory....: 128
7.) SNMP Trap Store Capacity...: 30

Thrift Server Settings:
11.) Thrift Server Port.....: 7911
12.) Thrift Server Memory.....: 256
13.) Thrift Server Memory.....: 120

Tomcat JMS Settings:
14.) JMS IP.....: 172.25.152.76
15.) JMS Port.....: 1856

MySQL Settings:
16.) Database IP.....: 172.25.152.77
17.) Database Port.....: 3333

Task Server Settings:
11.) Task Server Memory.....: 512
12.) Thrift Server Port.....: 2099

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 /home/wandl/collection1010/dcollect
./dc.sh start 0
```

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

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

Creating HornetQ 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:

```
/home/wandl/collection1010/bin/startup_collection
```

```
# exit
```

```
> /home/wandl/collection1010/bin/startup_collection
```

Purging temporary files... done!

Detecting existing servers

HornetQ 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 their deployment. Please wait a few minutes and then run /home/wandl/collection1010/bin/status\_jump to determine the deployment status.

**Related Documentation**

- [Remote Collection Server Overview on page 51](#)





## CHAPTER 4

# Installing the Viewserver

- [Viewserver Overview on page 57](#)
- [Installing the Viewserver on page 59](#)

### Viewserver Overview

---

For more information about the installation process for the application and database packages, see the [“Installing the IP/MPLSView Server, Client, Traffic Data Collector, and Rsync Package” on page 32](#).

The Viewserver compliments the application server by featuring a streamlined client designed for network operators and planners. Only network administrators need to use the full capabilities of the client from the application server. Using the Viewserver enhances overall system performance by offloading 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 the Viewserver

Use the Viewserver if you plan to have many concurrent client sessions. If there are too many concurrent application client users, this might affect user performance because the application client includes administrative and collection tools which require more system resources than the Viewserver client. The Viewserver client uses fewer 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

---

The 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

- Fault Management
  - Event Browser
  - Historical Event Browser
  - Event Map
- Performance Management
  - Network Dashboard
  - View live traffic, CPU, memory, temperature
  - Network Performance Report
- Design and Plan
  - MPLS-TE
  - T-Solve
  - Simulation

---

### Application Client

The application client has the same features as the Viewserver client plus the following additional features. The selection of available modules depends 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
- Hardware Vendor Type Manager
- Save to .network directory
- Save to Web
- User Administration

### Related Documentation

- [IP/MPLSView Installation Overview on page 29](#)
- [Installing the Viewserver on page 59](#)

## Installing the Viewserver

- [Requirements on page 59](#)
- [Overview on page 59](#)
- [Viewserver Installation on page 60](#)

### Requirements

The following are requirements for the Viewserver installation and usage:

- The application server and Viewserver must use the same system platform.
- The `npatpw` password file in the `/u/wandl/db/sys/` directory is required for each Viewserver machine.
- Create the remote data directory as the `wandl` user before installing. The remote data directory must use the same name as the application data directory.
- Configuration settings:
  - IP address
  - LDAP Server IP address = Application server IP address
  - Distributed Database = Yes
  - Local Database IP address = Viewserver IP address
  - Distributed Database IP address = Application or database server IP address
- The Viewserver user accounts must be created on both the application server and the Viewserver.

Before installing the Viewserver package:

- Verify that existing servers for application, database, and traffic data collectors are running properly.
- Copy the Viewserver package installation files to the machine hosting the Viewserver.
- Contact your Juniper representative to obtain the Viewserver installation package license.

### Overview

This section guides you through installation of the Viewserver. We recommend that you write down the IP address and directories of your distributed server environment.

[Table 19 on page 59](#) is used as the example in this guide.

**Table 19: Distributed Server Address Example**

| Server             | IP Address | Description                   | Directory              | Environmental Variable |
|--------------------|------------|-------------------------------|------------------------|------------------------|
| Application server | 172.16.1.1 | Application install directory | /home/wandl/ipmplsview | -                      |

Table 19: Distributed Server Address Example (continued)

| Server             | IP Address | Description                  | Directory              | Environmental Variable |
|--------------------|------------|------------------------------|------------------------|------------------------|
| Application server | 172.16.1.1 | Application data directory   | /home/wandl/wandldata  | -                      |
| Viewserver         | 172.26.2.2 | Viewserver install directory | /home/wandl/viewserver | -                      |
| Viewserver         | 172.26.2.2 | Viewserver data directory    | /home/wandl/viewdata   | LOCAL_DATA_DIR         |
| Viewserver         | 172.26.2.2 | Remote data directory        | /home/wandl/wandldata  | REMOTE_DATA_DIR        |



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

## Viewserver Installation

This procedure describes the following tasks:

- [Installing the Viewserver on page 60](#)
- [Configuring the Viewserver on page 62](#)
- [Viewserver User Account Setup on page 63](#)
- [Starting and Stopping the Viewserver on page 63](#)
- [Launching the Viewserver Client on page 64](#)
- [Viewserver and Application Server Commands, Paths, and Variables on page 66](#)

### Installing the Viewserver

#### Step-by-Step Procedure

To install the Viewserver:

1. Copy and extract the Viewserver installation packages to a temporary installation directory on the Viewserver.
2. As the wandl user, create the remote data directory. It must have the same name as the application data directory.  
  

```
mkdir /home/wandl/wandldata
```
3. As the root user, run the installation script from the temporary installation directory.  
  

```
./inst_viewserver.sh
```
4. At the prompt, input the View Server user ID. We recommend using the default wandl ID.
5. At the prompt, input the group ID. We recommend using the default **staff** ID.

6. The install script prompts you to shut down the servers. Enter **Yes**.
7. At the prompt, enter the directory where you want this software installed. We recommend using the **/home/wandl/viewserver** directory.
8. At the prompt, enter the directory where you want the data stored. We recommend using the **/home/wandl/viewdata** directory.
9. At the main menu, select **IP Address**.
  - Set the LDAP Server IP address to be the same as the Application server IP address.
  - Set the Distributed Database to **YES**.
  - Set the Distributed Database IP address to be the same as the Application server IP address. If the application and database are on distributed servers, then set these to the database server IP address.

```

(B) IP Address
IP/MPLSView Server IP Address Settings:
1.) View Server IP.....: 172.26.2.2
2.) Webserver IP.....: 172.26.2.2
3.) LDAP Server IP.....: 172.16.1.1
4.) External Webserver IP (for NAT)....:
5.) Local Database IP.....: 172.26.2.2
6.) Distributed Database.....: YES
....Distributed Database IP.....: 172.16.1.1
....Database Port.....: 3333
9.) MongoDB IP.....:
99.) Change All IP Addresses for 1, 2, 3, 5
      
```
10. Only the IP Address settings need to be changed for the Viewserver setup. You can review the other options in the main menu. Accept these values when you are ready.
11. The following are optional prompts if the installation packages are detected:
  - At the Install Client prompt, if you want to use the Linux Client, enter **y** to install it; otherwise, enter **n**.
  - At the prompt to install the Traffic Data Collector, if you want to use the Traffic Data Collector on the Viewserver, enter **y** to install it; otherwise, enter **n**.
  - At the prompt to Install Rsync & Replication, if you want to use the Rsync and Replication features, enter **y** to install these; otherwise, enter **n**.
12. At the prompt to copy files from the old installation to the new installation, select the options you want to copy over.
13. At the prompt to enter the mount point of the remote data directory, use the **/home/wandl/wandldata** remote data directory.



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

14. At the prompt to enter the IP address of the application server, use the application server IP address.
15. At the prompt to give the Java applets write permission, enter **y** to allow saving Java charts and trending reports from the Web, or enter **n** to skip this.
16. At the prompt to start up the Viewserver, enter **y** to start, or enter **n** to skip and start at a later time.

Before launching a client session, read the *Configuring the Viewserver* and *Viewserver User Account Setup* sections on this topic.

### Configuring the Viewserver

#### Step-by-Step Procedure

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

```
ls -l /u/wandl/data
lrwxrwxrwx 1 wandl staff 31 Jun 23 10:46 /u/wandl/data ->
/home/wandl/wandldata
```
3. As the root user, share the application data directory as read-only to the Viewserver (client machine).
 

```
[root@nfsserver ~]# vi /etc/exports

/home/wandl/wandldata 192.168.0.101 (ro,sync,no_root_squash)
#service nfs restart
```
4. Log in to the Viewserver.
5. As the root user, mount the remote data directory using the shared path. In the Requirements section, the remote data directory is created as the wandl user and uses the same name as the application data directory.

```
mount 172.16.1.1:/home/wandl/wandldata /home/wandl/wandldata
```

6. As the 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.

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

### Viewserver User Account Setup

**Step-by-Step Procedure** Viewserver users need accounts created on both the Application server and Viewserver. The administrator on the application server can then 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.

To set up a Viewserver user account:

1. As the 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 the Viewserver. The following command creates a new user named *viewuser* in the staff group, creates and sets the user's home directory to **/home/viewuser**, and sets the profile to use a bash shell.

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

2. Repeat Step 1 for each additional user.
3. As the wandl user, log in to the Application Client.
4. Select **Admin > User Administration** to manage the permissions and regions of the Viewserver users.

### Starting and Stopping the Viewserver

**Step-by-Step Procedure** To start, use, and stop the Viewserver:

1. Create the remote data directory, as the wandl user, before starting the installation. The remote data directory must have the same name as the application data directory.
2. As the 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 the LDAP IP address, set the distributed database to YES, and enter the distributed database IP address.
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 the remote data directory in the TaskManager path.
7. Create the Viewserver user accounts on both the application server and Viewserver.
8. Manage the Viewserver user permissions through the application client.
9. As the wandl user, start up the Viewserver using the following command:  
  
`/u/wandl/bin/startup_viewerserver`
10. To stop the Viewserver and send a warning message to all clients stating the server is shutting down in 1 minute, log in as the wandl user and stop the Viewserver using the following command:  
  
`/u/wandl/bin/stop_viewerserver`

---

### Launching the Viewserver Client

#### Step-by-Step Procedure

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

1. To start the client using Webclient:
  - a. Open a Web browser and enter the Viewserver IP address on port 8091.  
  
`viewserver_ip:8091`
  - b. Log in to the Web using the user credentials set up on the Viewserver.
  - c. Click Webclient.
  - d. Click IP/MPLSView.
  - e. Log in to the client using the user credentials set up on the Viewserver.



2. To start the client using a desktop client:
  - a. Install the client using the appropriate settings for each of the following:
    - **SERVER**—Set the IP/MPLSView application server IP address to be the same as the Viewserver IP address.
    - **WEBSERVER**—Set the Web server IP address to be the same as the Viewserver IP address.
    - **LDAPSERVER**—Set the LDAP server IP address to be the same as the application server IP address.
  - b. If the client is already installed, right-click the IP/MPLSView Client icon and select edit, or edit the **ipmplsview.bat** file to change the following settings:

```
SET SERVER=172.26.2.2
SET SERVERPORT=7000
SET WEBSERVER=172.26.2.2
SET WEBSERVERPORT=8091
SET LDAPSERVER=172.16.1.1
SET LDAPPOR=3389
SET MEMORY=256MB
```
  - c. Double-click the IP/MPLSView Client icon or the **ipmplsview.bat** file.
  - d. Log in to the client using the user credentials set up on the Viewserver.

## Viewserver and Application Server Commands, Paths, and Variables

### Step-by-Step Procedure

The following are the Viewserver commands and paths:

- Directory: `/u/wandl/bin`
- Start server command: `/u/wandl/bin/startup_viewerserver`
- Stop server command: `/u/wandl/bin/stop_viewerserver`
- Server status command: `/u/wandl/bin/status_viewerserver`
- Install directory: `/home/wandl/viewserver`
- Local data directory: `/home/wandl/viewdata`
- Remote data directory: `/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`

The following are the application server commands and paths:

- Directory: `/u/wandl/bin`
- Application data directory: `/home/wandl/wandldata`

The following variables are used for Viewserver implementation. These values are set in the `/u/wandl/bin/mplsenvsetup.sh` script during installation or by running the `/u/wandl/bin/changeconfig.sh` command. Do not manually edit these values. The following information is provided for reference only.

```
VIEW_ONLY=0; export VIEW_ONLY
LOCAL_DATA_DIR=/home/wandl/viewdata ; export LOCAL_DATA_DIR
VIEW_SERVER_APPIP=172.16.1.1; export VIEW_SERVER_APPIP
REMOTE_DATA_DIR=/home/wandl/wandldata ; export REMOTE_DATA_DIR
```

### Related Documentation

- [IP/MPLSView Installation Overview on page 29](#)
- [Viewserver Overview on page 57](#)

## CHAPTER 5

# Configuring Traffic Updates from IP/MPLSView to NorthStar Controller

- [Traffic Updates from IP/MPLSView to NorthStar Controller Overview on page 67](#)

## Traffic Updates from IP/MPLSView to NorthStar Controller Overview

---

This section describes the following:

- [Traffic Updates from IP/MPLSView to NorthStar Controller on page 67](#)
- [System Requirements on page 69](#)
- [NorthStar AMQP Agent on page 69](#)
- [Configuring NorthStar AMQP Agent on page 70](#)
- [Configuring Additional Attributes on page 71](#)
- [Starting or Stopping the NorthStar AMQP Agent on page 72](#)

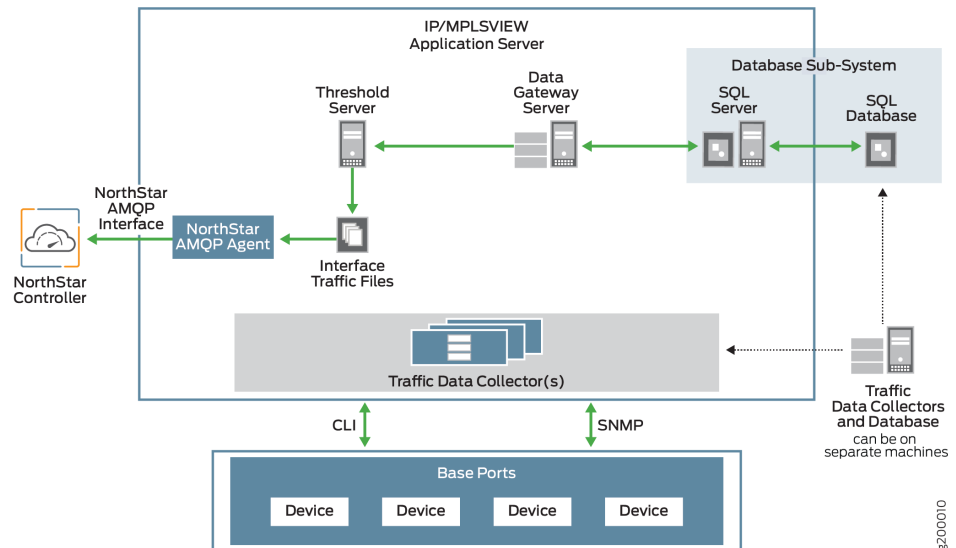
## Traffic Updates from IP/MPLSView to NorthStar Controller

Juniper Networks IP/MPLSView and Juniper Networks NorthStar Controller are similar in modeling network topology and monitoring network updates. IP/MPLSView has a static topology view and receives network events passively. NorthStar Controller is an SDN controller that enables granular visibility and control of IP/MPLS tunnels in large service provider and enterprise networks. NorthStar can receive traffic statistic updates from IP/MPLSView.

You must have an IP/MPLSView Performance Management license to receive these updates. The Performance Management license allows the router interface data and LSP traffic statistics to be collected, and then sent over the interface to NorthStar Controller. These updates include node and link changes, as well as node and link status.

[Figure 3 on page 68](#) shows how the router interface data and LSP traffic statistics are exchanged between the IP/MPLSView system to the NorthStar Controller. Advanced Message Queuing Protocol (AMQP) is used for the system-to-system communication.

Figure 3: Traffic Update Architecture for IP/MPLSView to NorthStar



The following list describes interactions among the components in [Figure 3 on page 68](#):

**Base Ports**—A group of ports used for offline and online networks.

**Traffic Data Collection**—A performance management subsystem that collects traffic statistics on a periodic basis. The Data Gateway Server (DGS) and the Traffic Data Collectors (TDCs) are the primary application processes involved in collecting and storing the traffic statistics from all routers defined in a traffic collection set of devices. These routers are queried on a regular interval, typically a 5-minute interval. The results of these queries are stored in the traffic collection database by the DGS process. In addition, these traffic results are stored in readable text files in `/u/wandl/data/.network`.

**Traffic Data Files**—A data collection accessed and stored in `/u/wandl/data/.network/interface.traffic` and `/u/wandl/data/.network/tunnel.traffic`.

**NorthStar AMQP Agent**—An agent that reads the traffic data files on a periodic basis, creates a data structure populated by this data, and sends these structures to the configured NorthStar Controller.

**Frequency of Data Transmission to NorthStar Controller**—A data transmission that does not require any special configuration of the agent to schedule the publishing of data. You can configure the IP/MPLSView system to collect traffic statistics at different intervals, such as every 5 minutes, 10 minutes, 15 minutes, or longer. The NorthStar AMQP Agent uses this same interval for publishing data to the remote NorthStar Controller.

**Threshold Server**—A server that creates and updates the interface and tunnel traffic files in `/u/wandl/data/.network` as part of the overall performance management subsystem.

**Application Monitor Server**—A server that is responsible for monitoring the various application processes in the IP/MPLSView system. The monitoring functions include a periodic check (once a minute) to ensure that a configured process is running. If the monitored process does not exist (assuming it was previously started), it will automatically restart that process.

## System Requirements

For traffic updates from IP/MPLSView to NorthStar Controller, the following system requirements apply:

- Both IP/MPLSView and NorthStar Controller must be installed.
- An IP/MPLSView Performance Management license must be installed to receive updates.

## NorthStar AMQP Agent

NorthStar AMQP Agent reads the traffic data files on a periodic basis, creates a data structure populated by this data, and sends these structures to the configured NorthStar system. The data is sent at a time interval defined in the Traffic Data Collector subsystem.

You start the NorthStar AMQP Agent by invoking the `/u/wandl/bin/nsamqpagent` script when you run the `/u/wandl/bin/startup_mplsview` script. After the process starts, the following steps are performed:

1. The agent reads the configuration information in the `/u/wandl/db/config/nsamqpagent.config` file. This file contains all the necessary access information including the login and password values used to access the remote NorthStar Controller.
2. The agent connects to the NorthStar Controller using the access credentials described in Step 1.
3. After successfully connecting, the agent monitors the update to the `/u/wandl/data/network/interface.traffic` and `/u/wandl/data/network/tunnel.traffic` files.
4. When the threshold server posts an update to the interface or tunnel traffic files, the agent reads the contents of these files and formats a data structure that defines the contents.
5. After constructing the message, the agent sends (publishes) the data to the remote NorthStar Controller.
6. Step 3 through Step 5 are repeated indefinitely while the agent process is running.

## Configuring NorthStar AMQP Agent

The NorthStar AMQP Agent is configured using the `/u/wandl/bin/changeconfig.sh` script. Changing the settings for the agent requires first stopping IP/MPLSView using the `/u/wandl/bin/stop_mplsview` command. After the settings have been changed, restart IP/MPLSView using the `/u/wandl/bin/startup_mplsview` command.

The variables used for configuring the NorthStar AMQP Agent are the values that the agent process uses to access the remote NorthStar Controller. In addition to setting the variables, the `changeconfig.sh` script also creates and updates the `/u/wandl/db/config/nsamqpagent.config` file.



**NOTE:** If needed, you can run the `/u/wandl/bin/changeconfig.sh` script to increase the allocated memory size used by the agent process.

Log files are created in the `/u/wandl/log` directory and the specific log file names are all prefixed with `nsamqpagent`. Log files can also be accessed from the user interface by selecting **Admin > View > Logs**.

To configure the NorthStar AMQP Agent:

1. After the installation script finishes prompting for required settings, the Main Menu is displayed.

```
Main Menu
Server Configuration Settings:
(A) Overall Settings
(B) IP Address
(C) Memory Settings
(D) Port Settings
(E) Data Storage Capacity Settings
(F) Online Fault Management Settings
(G) Advanced Configuration
(H) NorthStar AMQP Settings
Please select a number to modify.
[<CR>=accept, q=quit]: H
```

2. Select **(H) NorthStar AMQP Settings** to display the following settings:

```
(H) NorthStar AMQP Configuration
NorthStar AMQP Configuration Settings:
```

If you want to change "NorthStar System Password" then enter the unencrypted value.

```
1.) IP Address of NorthStar System.....: 172.16.10.1
2.) NorthStar System Port.....: 5672
3.) NorthStar System Username.....: northstar2
4.) NorthStar System Password .....: <password>
5.) NorthStar System Exchange Name.....:
controller.wan.stats1.
Please select a number to modify.
[<CR>=return to main menu]:
```

3. Select **1.) IP Address of NorthStar System**. Enter the IP address of the remote NorthStar Controller.
4. Select **2.) NorthStar System Port**. Enter the port number to access the remote NorthStar Controller. The default is **5672**.
5. Select **3.) NorthStar System Username**. Enter the user account of the remote NorthStar Controller. The default is **northstar**.
6. Select **4.) NorthStar System Password**. Enter the encrypted user password of the remote NorthStar Controller.
7. Select **5.) NorthStar System Exchange Name**. Enter the exchange name of the remote NorthStar Controller. The default is **controller.wan.stats**.

## Configuring Additional Attributes

The changes made by using the `/u/wandl/bin/changeconfig.sh` script provide the ability to change the settings necessary to configure different access credentials to a Northstar Controller. There are some additional attributes available that can only be manually changed in the `/u/wandl/db/config/nsamqpagent.config` file.

The following output shows an example of a `nsamqpagent.config` file, and [Table 20 on page 71](#) describes these attributes that can only be manually changed.

```
mq_host = 172.25.152.246
mq_username = root
mq_password = nM0EkDeGmDbDpGfKmCfP1AnAbM00
mq_port = 5672
mq_exchangename = controller.wan.stats
mq_noconnect = false
mq_trafficfileset = interface.traffic,tunnel.traffic
mq_useipaddr = true
```

*Table 20: Variables for NorthStar AMQP Agent*

| Config EntryName         | Description                                                                                                                                                              | Default Value                                                                      |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| <b>mq_noconnect</b>      | When set to <b>true</b> , the agent process does not connect to the remote NorthStar Controller.                                                                         | false<br><br>Allowed values: true, false                                           |
| <b>mq_trafficfileset</b> | You can define the type of traffic statistics to send—interface, tunnel, or both.                                                                                        | interface.traffic,tunnel.traffic<br><br>Allowed values: One or both of the values. |
| <b>mq_useipaddr</b>      | The agent can send either the name or IP address of the device.<br><br>Setting the value to <b>false</b> sends the device name rather than the IP address of the device. | true<br><br>Allowed values: true, false                                            |



**NOTE:** If needed, you can run the `/u/wandl/bin/changeconfig.sh` script to increase the allocated memory size used by the agent process.

Log files are created in the `/u/wandl/log` directory and the specific log file names are all prefixed with `nsamqpagent`. Log files can also be accessed from the user interface by selecting **Admin > View > Logs**.

---

## Starting or Stopping the NorthStar AMQP Agent

The NorthStar AMQP Agent process is started by using the `/u/wandl/bin/startup_mplsview` command, which is used to start all of the IP/MPLSView application processes.

To start the NorthStar AMQP Agent:

1. Run the `/u/wandl/bin/startup_mplsview` command. (By default, the NorthStar AMQP Agent is not running.)

The system displays:

**Would you like to start the Northstar AMQP Agent (default=no)? [y/n]**

2. Press Enter or y to continue.

The `startup_mplsview` command invokes the `/u/wandl/bin/nsamqpagent start` script to start the agent process.

To stop NorthStar AMQP Agent:

1. Stop NorthStar AMQP Agent using the `/u/wandl/bin/nsamqpagent stop` command.



**NOTE:** The `/u/wandl/bin/stop_mplsview` command stops all application processes, including the NorthStar AMQP Agent.

### Related Documentation

- [Starting IP/MPLSView Servers on page 137](#)
- [Required Ports to Open in Firewalls on page 21](#)



## CHAPTER 6

# Configuring and Administering IP/MPLSView in a Distributed Environment

- [Replication and Rsync in Distributed Environments Overview on page 73](#)
- [Installing the Rsync Package and Automating SSH Login on page 74](#)
- [Installing and Administering IP/MPLSView Replication and Resync in a Two-Server Environment on page 77](#)
- [Installing and Administering IP/MPLSView Replication and Rsync in a Four-Server Environment on page 85](#)
- [Administering Failovers in a Distributed Environment on page 97](#)
- [Troubleshooting Database Synchronization in a Distributed Environment on page 100](#)

### Replication and Rsync in Distributed Environments Overview

---

IP/MPLSView includes third-party replication and remote synchronization (rsync) software packages that you can use to back up information for IP/MPLSView data and traffic collection. The replication and rsync utilities are designed to maintain backup servers with up-to-date versions of the files and the database of the primary servers they are backing up, and to replicate data in the event of a failure so the backup server can resume operation.

The third-party rsync package backs up files from the primary application server to the backup application server and the Mongo database (MongoDB) and MariaDB replication packages keep the backup databases synchronized with the primary database. To synchronize the data, the replication and rsync software compares the data in the backup and primary databases and sends deltas in order to reduce overall data transfer.

You can use the replication and rsync utilities to back up data in either of the following ways:

- To only back up data collection files without traffic collection data, only use the rsync package because then the MariaDB database is not involved. For more information, see [“Installing the Rsync Package and Automating SSH Login” on page 74](#).
- To back up network data, data stored in the MongoDB, and traffic collection data stored in the Maria database (MariaDB), set up your distributed environment in one of the following ways:

- Two-server setup—The primary IP/MPLSView application server and primary database are on the same server. You can back up this server by using a second server that has both the application server and database installed. For more information, see *Installing and Administering IP/MPLSView Replication and Rsync in a Two-Server Environment*.
- Four-server setup—The primary IP/MPLSView application server has a distributed primary database on a different server. In this case, the backup application server is on a separate server, with a distributed database on another server. For more information, see *Installing and Administering IP/MPLSView Replication and Rsync in a Four-Server Environment*.

You must install a separate license on the backup IP/MPLSView application server.

Use the following utilities to administer the distributed servers:

- **set-ip-all.sh**—Sets up all IP addresses for all distributed servers.
- **stop-all.sh**—Stops all distributed servers.
- **status-all.sh**—Checks the running status for all distributed servers.

**Related  
Documentation**

- [Installing the Rsync Package and Automating SSH Login on page 74](#)
- [Installing and Administering IP/MPLSView Replication and Rsync in a Two-Server Environment on page 77](#)
- [Installing and Administering IP/MPLSView Replication and Rsync in a Four-Server Environment on page 85](#)
- [Troubleshooting Database Synchronization in a Distributed Environment on page 100](#)

---

## Installing the Rsync Package and Automating SSH Login

Before you can use the replication and rsync packages to back up the IP/MPLSView servers and databases in a distributed environment, make sure you have completed all of the following prerequisites:

- Set up the **/etc/hosts** file.
- Install the rsync software package.
- Automate SSH login on the primary and backup application servers.

Make sure each application server and database server in your network has entries in its **/etc/hosts** file to every other application server and database server. These entries enable you to use either IP addresses or hostnames to ping each server in the network.

### Installing the Rsync Package

You can install the rsync package before, during, or after installing the IP/MPLSView application.

To install the rsync package on the primary application server and backup application servers:

1. Determine whether your server already has rsync installed by doing one of the following:
  - Checking your server for the presence of the `/usr/local/bin/rsync` file.
  - On Linux servers, issuing the `rpm -qa | grep rsync` command as the root user.
2. If rsync is not installed, install it from the rsync installation package as the root user.
  - On non-Linux servers, use the `replication/inst_rsync.sh` command.
  - On Linux servers, issue the `yum -y rsync` command.

### Automating SSH Login

Cron is a time-based job scheduler for Linux-based operating systems. You can use cron to schedule jobs (commands or shell scripts) to run periodically at fixed times, dates, or intervals.

To ensure that you can perform an automatic rsync with a cron job, you must automate the SSH login process on the primary and backup application servers so you can use SSH to log in remotely without needing to specify a password. Automating SSH login also facilitates the processes for performing status checks, and for starting and stopping the application and databases.

If you need to only transfer data collection information between the primary and backup application servers, you can automate the SSH login for only the wandl user account. However, if you also need to transfer traffic collection data, you must automate the SSH login for both the wandl user and the root user accounts because the root user account might own some of the traffic collection files that you need to transfer.

After you perform this procedure, the wandl user should be able to log in as the root user on all servers in your distributed environment. This is accomplished by making sure that the primary server's public key (`id_rsa.pub`) is present in the backup server's authorized keys (`authorized_keys`), and the backup server's authorized keys (`authorized_keys`) are in the primary server's public key (`id_rsa.pub`).

To automate SSH login on all database servers:

1. On the primary database server, log in as the wandl user and change directory to the wandl home directory (`/home/wandl`).
2. Generate a pair of authentication keys without specifying a passphrase.

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

```
Your public key has been saved in /home/wandl/.ssh/id_rsa.pub.
The key fingerprint is:
94:7c:a6:d2:b6:80:19:a4:b9:f4:7d:7f:09:d4:f2:52 wandl@server
```

3. Use SSH to create the **.ssh** directory on the primary application server.

Substitute *remosthostip* with the IP address of the primary application server. When prompted, enter the wandl password of the remote host.

```
/home/wandl> ssh wandl@remosthostip mkdir -p .ssh
The authenticity of host '<remosthostip> (<remosthostip>)' can't be established.
RSA key fingerprint is 8a:d9:a9:c5:91:6a:e6:23:8c:2f:ad:4f:ea:48:78:0b.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '<remosthostip>' (RSA) to the list of known
hosts.
Password:
```

4. Append the local host's new public key to the primary application server's authorized keys, and enter the wandl password for the primary application server.

```
/home/wandl> cat .ssh/id_rsa.pub | ssh wandl@remosthostip 'cat >>
.ssh/authorized_keys'
Password:
```

5. Set **PermitRootLogin** to **yes** in the **sshd\_config** file. For example, **/etc/ssh/sshd\_config** or **/usr/local/etc/sshd\_config**.

If **PermitRootLogin** is not set to yes, edit the **sshd\_config** file and use the **service sshd restart** command to restart the **sshd** process.

6. (Optional) Refresh the **sshd** process by stopping it, if needed.

Kill the SSH process. Use the process ID (PID) of the main **sshd** process. Note that issuing the following command might terminate currently open SSH sessions.

```
> kill -1 PID
```

7. Repeat Steps 1 through 6 for each backup application server.

8. Confirm that the **.ssh** directory has restricted permissions.

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

9. From the database servers, log in to the application servers to confirm that automatic SSH login is enabled.

If automatic SSH login is working properly, you should be able to directly log in to the application servers from the database servers and to the database servers from the application servers without specifying a password.

#### Related Documentation

- [Replication and Rsync in Distributed Environments Overview on page 73](#)
- [Installing and Administering IP/MPLSView Replication and Resync in a Two-Server Environment on page 77](#)

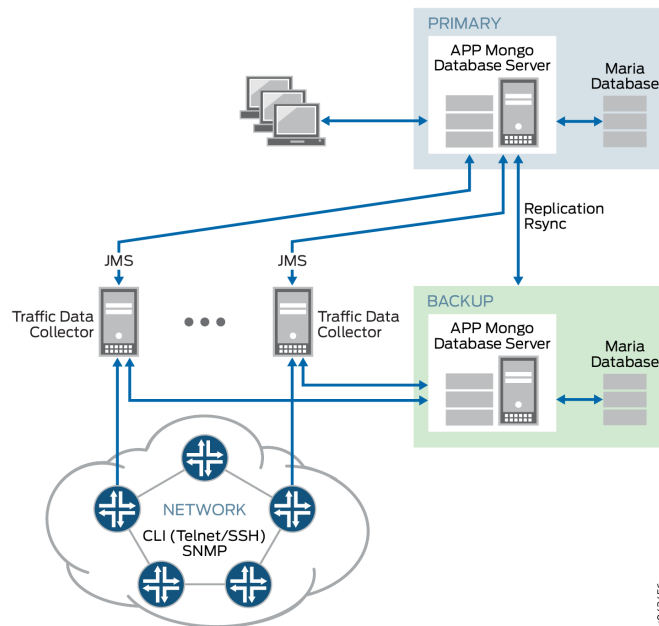
- [Installing and Administering IP/MPLSView Replication and Rsync in a Four-Server Environment on page 85](#)
- [Troubleshooting Database Synchronization in a Distributed Environment on page 100](#)

## Installing and Administering IP/MPLSView Replication and Resync in a Two-Server Environment

This section describes how to set up, install, start, and administer IP/MPLSView in a two-server distributed environment. It includes step-by-step procedures for failing over to the backup server when the primary server goes down, synchronizing the data, and switching back to the primary server when it resumes operation.

[Figure 4 on page 77](#) shows a typical setup for using IP/MPLSView in a distributed environment that consists of two servers—a primary application server and a backup application server—each of which runs both the IP/MPLSView application and the IP/MPLSView database.

*Figure 4: Example IP/MPLSView Setup for a Two-Server Distributed Environment*



You can install the replication and rsync package as part of the IP/MPLSView installation script. If you choose not to install the replication and rsync package during the standard installation procedure, you can install it later by running the **replication/instrepl.sh** script as the **wandl** user.

The sample setup consists of the following hardware and software components:

- One primary application server (labeled Primary AP)
- One backup application server (labeled Backup AP)

- Two Traffic Data Collectors (each labeled DC)
- Replication and rsync software running between the primary and backup application servers
- MongoDB fault management database
- MariaDB performance management database on the primary and backup application servers
- Java Message Service (JMS), which sends messages between the application servers and the Traffic Data Collectors
- [Installing IP/MPLSView with Replication and Rsync in a Two-Server Environment on page 78](#)
- [Starting IP/MPLSView in a Two-Server Environment on page 80](#)
- [Failing Over to the Backup Server on page 81](#)
- [Synchronizing the Data from the Backup Server to the Original Primary Server on page 82](#)
- [Switching Back to the Original Primary Server on page 84](#)

## Installing IP/MPLSView with Replication and Rsync in a Two-Server Environment

To install IP/MPLSView with replication and rsync software in a two-server distributed environment:

1. Use the **server/install.sh** script in the installation directory and follow the standard installation procedure.

```
%install_directory% /server/install.sh
```

2. Install the rsync and replication package when prompted.

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

3. Configure the primary application server with the appropriate replication and rsync settings.

```
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)
```

4. Configure the backup application server with the appropriate replication and rsync settings.

```
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)
```

5. Enter the IP address of the backup server on the primary servers and, conversely, enter the IP address of the primary server on the backup server.

Please enter the IP address of the alternate MPLSView server: *ip-address*

6. Enter the **ssh** directory of the alternate IP/MPLSView server if the actual paths do not conform to the default paths.
7. Enter the SSH host key of the **wandl** user, for example, **/home/wandl/.ssh/id\_rsa**.
8. Check the size of the IP/MPLSView home (**/home/wandl**) directory to make sure the backup server has sufficient disk space in the home directory.

```
du -ks /home/wandl
```

By default, the administrative home directory is not synchronized. To synchronize this directory, check the size of the home directory to make sure it is not too large to copy its entire contents to the backup server.

After the installation, you can modify which directories and files are synchronized by editing the **/u/wandl/bin/rsync.sh** script. You must exclude the database files from the rsync.

9. Synchronize directories and files when prompted.

```
Synchronize the following files/directories?:
You can later manually modify the entries in
/u/wandl/bin/rsync.sh [YES]y
1.) /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
```

10. Schedule the time interval to use for synchronizing the backup application server with the primary application server.

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

11. (Optional) To modify the time interval after the installation, run the following script:

```
/install_dir/replication/instrepl.sh
```

Alternatively, you can directly modify the crontab settings as the wandl user and export the **EDITOR** variable by using the **export** EDITOR command. For example, you can enter **EDITOR=vi** to set the editor to vi, and then run the **crontab -e** command.

## Starting IP/MPLSView in a Two-Server Environment

To start IP/MPLSView on the primary and backup application servers:

1. Start IP/MPLSView on the primary application server (master).

If it does not start during installation, use the following command:

```
/u/wandl/bin/startup_mplsview
```

2. Make sure the following entry is in the `/u/wandl/db/config/mongodb.conf` file:

```
repSet = rs0
```

3. Start MongoDB on the backup application server.

```
/u/wandl/bin/mongodb.sh start
```

4. Start MongoDB in slave mode on the primary application server.

```
/u/wandl/bin/mongodb_rep1.sh addslave
```

5. Check the status of MongoDB on both the primary and the backup application servers.

```
/u/wandl/bin/mongodb_rep1.sh status
```

```
Primary MongoDB is running
Primary replication position: 1
Secondary: <ip-address>:27017 is up and running
Secondary: <ip-address>:27017 replication position 1
```

6. (Optional) To start IP/MPLSView if the **addslave** command does not cause the MongoDB to run in slave mode:
  - a. Configure the primary and backup application servers with the replication settings in the `/u/wandl/db/config/mongodb.conf` file.
  - b. Make sure the following entry appears in the `/u/wandl/db/config/mongodb.conf` file:

```
repSet = rs0
```
  - c. Access the MongoDB CLI (`/u/wandl/thirdparty/mongodb/bin/mongo`) on the primary application server, and issue the following commands to initiate MongoDB and run it in slave mode:

```
run rs.initiate();
rs.add({_id: 1, host: "<slave-ip>:27017", priority: 0.5});
```



7. Start the backup MariaDB server in slave mode.

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

8. On the backup application server, register the MariaDB server with the master MariaDB server.

```
/u/wandl/bin/mysql_rep1.sh registermaster
```

9. Check the status of the MariaDB slave server.

```
/u/wandl/bin/mysql_rep1.sh status
Slave Mysql server connected to Master: primary-server ip-address/hostname
```

10. Check the status of the MariaDB master server.

```
/u/wandl/bin/mysql_rep1.sh status
Master Mysql server is running
Slave server: backup-server ip-address/hostname
```

11. Verify that rsync is enabled.

```
crontab -l
```

On the primary application server, the **/u/wandl/bin/rsync.sh** script runs according to the interval you specify during the installation. Depending on your synchronization requirements, specifying an interval of 30 minutes or 60 minutes should be sufficiently frequent.

Each time the **rsync.sh** script runs, it synchronizes the directories in the **/u/wandl/data** directory, excluding the MariaDB traffic database and MongoDB directories, between the primary application server and the backup application server. This is referred to as *push synchronization*. This process also replicates the MariaDB and MongoDB databases.

12. After the interval you specified for rsync, check the **/u/wandl/data** directory on the backup application server to make sure the file system data has been copied.

## Failing Over to the Backup Server

In the event that the IP/MPLSView primary application server fails, you can fail over to the backup application server and initiate operation on the backup server until the primary server recovers.

To fail over to the backup application server if the primary application server fails:

1. Stop the remaining services on the primary application server.

```
/u/wandl/bin/stop_mplsview
```

2. On the primary application server, stop the cronjob for the **/u/wandl/bin/rsync.sh** script as both the **root** user and the **wandl** user.

```
crontab -e
```

The cronjob is owned by the administrative user ID who installed IP/MPLSView. By default, this is the **wandl** user.

3. Comment out (disable) the following line in crontab:

```
#0,30 * * * * /u/wandl/bin/rsync.sh exec > /u/wandl/log/rsync.log
```

4. Stop the backup application server.

```
/u/wandl/bin/stop_mplsview
```

5. Make sure the cronjob is disabled (commented out).

```
crontab -e
```

6. Start IP/MPLSView on the backup application server.

This action causes the backup application server to become the primary (master) application server.

```
/u/wandl/bin/startup_mplsview
```

7. Comment out the following entry in the `/u/wandl/db/config/mongodb.conf` file:

```
replicaSet = rs0
```

8. Restart the MongoDB process.

```
/u/wandl/bin/mongodb.sh stop  
/u/wandl/bin/mongodb.sh start
```

9. Access the MongoDB CLI and issue the following commands:

```
/u/wandl/thirdparty/mongodb/bin/mongo  
use local;  
db.dropDatabase();
```

## Synchronizing the Data from the Backup Server to the Original Primary Server

When the original primary application server resumes operation, you must synchronize the data from the backup application server to the primary application server.

To synchronize data from the backup server to the original primary server:

1. Start the original primary MariaDB server in slave mode.

```
/u/wandl/bin/.mysql start slave  
Slave MySQL server connected to master: backup-server ip-address
```

2. Register the master MariaDB server on the backup application server.

```
/u/wandl/bin/.mysql registermaster
```

3. Check the last data received on both the primary application server and the backup application server to make sure the data is synchronized.

```
/u/wandl/bin/mysql_rep1.sh lastdata
```

When you issue this command, the software displays an 11-digit timestamp that corresponds to the time of the last data collection. When both the primary MariaDB server and the master MariaDB server display the same 11-digit timestamp, the data is synchronized.

For more information about the format of the timestamp, see [“Troubleshooting Database Synchronization in a Distributed Environment” on page 100](#).

4. Start the MongoDB.

```
/u/wandl/bin/mongodb.sh start
```

5. Leave (stop) the MongoDB cluster on the original primary application server.

```
/u/wandl/bin/mongodb_rep1.sh leavecluster
```

6. On the backup application server, restart the MongoDB in cluster mode, and uncomment the following entry in the `/u/wandl/db/config/mongodb.conf` file:

```
rep1Set = rs0
```

7. Stop and restart the MongoDB process.

```
/u/wandl/bin/mongodb.sh stop  
/u/wandl/bin/mongodb.sh start
```

8. Start the MongoDB in slave mode on the backup application server.

```
/u/wandl/bin/mongodb_rep1.sh addslave
```

9. Stop IP/MPLSView on the backup application server.

```
/u/wandl/bin/stop_mplsview
```

10. If changes occurred in the network while the primary application server was out of service, issue the following command only once on the backup application server to synchronize the original primary application server with the backup application server:

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

11. Verify that the data has been synchronized.

```
/u/wandl/bin/mongodb_rep1.sh status  
/u/wandl/bin/mongodb_rep1.sh lastdata
```

## Switching Back to the Original Primary Server

To switch back to the original primary application server after it resumes operation:

1. Stop IP/MPLSView on the backup application server and then on the primary application server, in that order.
2. Check the status of IP/MPLSView on both application servers to confirm that it has been stopped.

```
/u/wandl/bin/status_mplsview
```

3. On the backup application server, start MongoDB and leave the cluster.

```
/u/wandl/bin/mongodb.sh start  
/u/wandl/bin/mongodb_rep1.sh leavecluster
```

4. On the primary application server, start MongoDB and leave the cluster.

```
/u/wandl/bin/mongodb.sh start  
/u/wandl/bin/mongodb_rep1.sh leavecluster  
/u/wandl/bin/mongodb.sh stop
```

5. Start IP/MPLSView on the primary application server.

```
/u/wandl/bin/startup_mplsview
```

6. Start MongoDB in slave mode on the primary application server.

```
/u/wandl/bin/mongodb_rep1.sh addslave
```

7. Check the status of MongoDB on the primary application server and then on the backup application server, in that order.

```
/u/wandl/bin/mongodb_rep1.sh status
```

8. Start the MariaDB server in slave mode on the backup application server.

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

9. On the backup application server, register the MariaDB server with the master MariaDB server.

```
/u/wandl/bin/mysql_rep1.sh registermaster
```

10. Check the status on the primary and backup MariaDB servers.

```
/u/wandl/bin/mysql_rep1.sh status
```

11. Check the data consistency on the primary MariaDB server.

```
/u/wandl/bin/mysql_rep1.sh lastdata
```

12. On the primary application server, check crontab for the root and wandl user accounts to verify if **rsync.sh** is commented out.

```
crontab -l
```

13. If cronjob is commented out in the **/u/wandl/bin/rsync.sh** script on the primary application server, reenable it.

```
crontab -e
```

The cronjob is owned by the administrative user ID who installed IP/MPLSView. By default, this is the wandl user.

14. Uncomment (enable) the following line in crontab:

```
#0,30 * * * * /u/wandl/bin/rsync.sh exec > /u/wandl/log/rsync.log
```

15. Stop IP/MPLSView on the backup application server.

```
/u/wandl/bin/stop_mplsview
```

16. Make sure the cronjob is commented out (disabled).

```
crontab -e
```

17. If the cronjob is not disabled on the backup application server, comment out (disable) the following line in crontab:

```
#0,30 * * * * /u/wandl/bin/rsync.sh exec > /u/wandl/log/rsync.log
```

#### Related Documentation

- [Replication and Rsync in Distributed Environments Overview on page 73](#)
- [Installing the Rsync Package and Automating SSH Login on page 74](#)
- [Troubleshooting Database Synchronization in a Distributed Environment on page 100](#)

## Installing and Administering IP/MPLSView Replication and Rsync in a Four-Server Environment

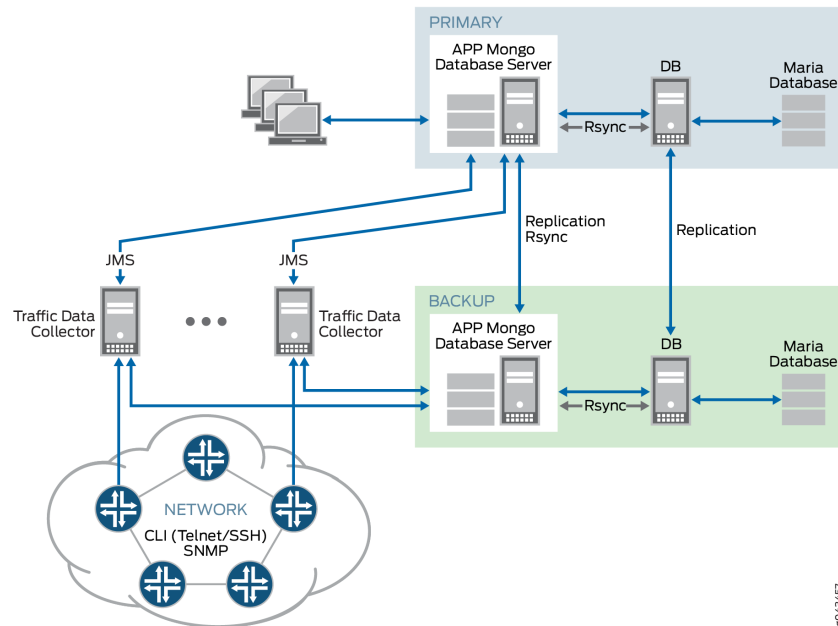
This section describes how to set up, install, start, and administer IP/MPLSView in a four-server distributed environment. It includes step-by-step procedures for failing over to the backup server when the primary server goes down, synchronizing the data, and switching back to the primary server when it resumes operation.

[Figure 5 on page 86](#) shows a typical setup for using IP/MPLSView in a distributed environment that consists of two application servers and two database servers. In this configuration, the primary and backup application servers run the IP/MPLSView application, and the primary and backup database servers run the IP/MPLSView database.

For optimal performance and to simplify setup and administration, we recommend that you pair the primary application server with the primary database server, and the backup

application server with the backup database server. After you complete the installation, verify that the remote database is working properly and that the servers are configured with the correct IP address pairings.

*Figure 5: Example IP/MPLSView Setup for a Four-Server Distributed Environment*



The example setup consists of the following hardware and software components:

- One primary application server (labeled Primary AP) paired with one primary database server (labeled Primary DB)
- One backup application server (labeled Backup AP) paired with one backup database server (labeled Backup DB)
- Two traffic data collectors (each labeled DC)
- Replication and rsync software running between the primary and backup application servers
- Replication software running between the primary and backup database servers
- MongoDB fault management database
- MariaDB performance management database on the primary and backup database servers
- Java Message Service (JMS), which sends messages between the primary and backup application servers and the traffic data collectors
- [Installing and Administering IP/MPLS View in a Four-Server Distributed Environment on page 87](#)
- [Starting IP/MPLSView in a Four-Server Environment on page 89](#)
- [Starting IP/MPLSView on the Database Servers in a Four-Server Environment on page 91](#)

- [Configuring an Rsync Cronjob to Replicate Traffic Collection Data on page 92](#)
- [Failing Over to the Backup Servers in a Four-Server Environment on page 92](#)
- [Synchronizing the Database from the Backup Server to the Original Primary Server on page 94](#)
- [Switching Back to the Original Primary Server on page 96](#)

## Installing and Administering IP/MPLS View in a Four-Server Distributed Environment

To install IP/MPLSView with replication and rsync software in a four-server distributed environment:

1. Follow the standard installation procedure in the installation directory.

```
install_dir/server/install.sh
```

You can install the replication and rsync software package as part of the IP/MPLSView installation. If you choose not to install the replication and rsync package during the standard installation procedure, you can install it later by running the **replication/instrepl.sh** script as the **wandl** user.

2. Install the rsync and replication package when prompted.

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

3. Configure the primary application server with the appropriate replication and rsync settings.

```
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
```

4. Configure the primary database server with the appropriate replication and rsync settings.

```
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
```

5. Configure the backup application server with the appropriate replication and rsync settings.

```
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
```

6. Configure the backup database server with the appropriate replication and rsync settings.

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

7. Enter the IP address of the corresponding backup server for the primary servers and, conversely, enter the IP address of the primary server on the corresponding backup servers.

Please enter the IP address of the alternate MPLSView server: *ip-address*

8. Enter the **ssh** directory of the alternate IP/MPLSView server if the actual paths do not conform to the default paths.
9. Enter the SSH host key of the **wandl** user, for example, **/home/wandl/.ssh/id\_rsa**.
10. Check the size of the IP/MPLSView home directory (for example, **/home/wandl**) to make sure the backup server has sufficient disk space in the home directory.

```
du -ks /home/wandl
```

By default, the administrative home directory is not synchronized. To synchronize this directory, check the size of the home directory to make sure it is not too large to copy its entire contents to the backup server.

After the installation, you can modify which directories and files are synchronized by editing the **/u/wandl/bin/rsync.sh** script. You must exclude the database files from the rsync.

11. Synchronize directories and files when prompted.

```
Synchronize the following files/directories?:
You can later manually modify the entries in
/u/wandl/bin/rsync.sh [YES]y
1.) /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

```

12. Schedule the time interval to use for synchronizing the backup application server with the primary application server.

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

13. (Optional) To modify the time interval after the installation, run the following script:

```
/install_dir/replication/instrepl.sh
```

Alternatively, you can directly modify the crontab settings as the wandl user. For example, you can enter **EDITOR=vi** to set the editor to vi, export the **EDITOR** variable by using the **export** EDITOR command, and then run the **crontab -e** command.

## Starting IP/MPLSView in a Four-Server Environment

To ensure that the data is synchronized when you use IP/MPLSView in a four-server distributed environment, you must start the paired primary application server and primary database server in active mode, and start the paired backup application server and backup database server in slave mode.

To start IP/MPLSView on the primary and backup application servers:

1. Make sure the MariaDB is started on the primary database server.
2. Make sure the following entry appears in the **/u/wandl/db/config/mongodb.conf** file on both the primary application server and the backup application server:

```
repSet = rs0
```

3. Start IP/MPLSView.

```
/u/wandl/bin/startup_mplsview
```

4. Start MongoDB on the backup application server.

```
mongodb.sh start
```

5. Start MongoDB in slave mode on the primary application server.

```
/u/wandl/bin/mongodb_rep1.sh addslave
```

6. Check the status of MongoDB on both application servers.

```
/u/wandl/bin/mongodb_rep1.sh status
```

```
Primary MongoDB is running
Primary replication position: 1
Secondary: <ip-address>:27017 is up and running
Secondary: <ip-address>:27017 replication position 1
```

7. (Optional) To start IP/MPLSView if the **addslave** command does not cause the MongoDB to run in slave mode:
  - a. Configure the primary and backup application servers with the replication settings in the `/u/wandl/db/config/mongodb.conf` file.
  - b. Make sure the following entry appears in the `/u/wandl/db/config/mongodb.conf` file:

```
repSet = rs0
```

- c. Access the MongoDB CLI (`/u/wandl/thirdparty/mongodb/bin/mongo`) on the primary application server, and issue the following commands to initiate MongoDB and run it in slave mode:

```
run rs.initiate();
rs.add({_id: 1, host: "<slave-ip>:27017", priority: 0.5});
```

8. Verify that rsync is enabled.

```
crontab -l
```

On the primary application server, the `/u/wandl/bin/rsync.sh` script runs according to the interval you specify during the installation. Depending on your synchronization requirements, specifying an interval of 30 minutes or 60 minutes should be sufficiently frequent.

Each time the **rsync.sh** script runs, it synchronizes the directories in `/u/wandl/data`, excluding the MongoDB data directory, between the primary application server and the backup application servers. This is referred to as *push synchronization*.

9. After the interval you specified for rsync, check the `/u/wandl/data` directory on the backup application server to make sure the file system data has been copied.

You can exclude both the MongoDB databases and the MariaDB traffic collection databases. MongoDB is replicated by means of the replication process, and MariaDB is handled on the database server.

## Starting IP/MPLSView on the Database Servers in a Four-Server Environment

To start IP/MPLSView on the primary and backup database servers:

1. Start the MariaDB database on the primary (master) database server.

```
/u/wandl/bin/startup_mplsview
```

You must start MariaDB on the primary database server before you start IP/MPLSView on the primary application server.

2. Start MariaDB on the backup database server in slave mode.

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

3. Register the master MariaDB server on the backup application server.

```
/u/wandl/bin/.mysql registermaster
```

4. Check the status of the MariaDB slave server.

```
/u/wandl/bin/mysql_repl.sh status  
Slave Mysql server connected to Master: primary-server ip-address/hostname
```

5. Check the status of the MariaDB master server.

```
/u/wandl/bin/mysql_repl.sh status  
Master Mysql server is running  
Slave server:backup-server ip-address/hostname
```

## Configuring an Rsync Cronjob to Replicate Traffic Collection Data

When you use IP/MPLSView, the database servers aggregate the day's traffic collection at the end of each day and save the data in object format files. To replicate the traffic collection files from the database servers to the application servers as a cronjob, you must run the **inst\_agg\_rsync.sh** script once on each database server.

You do not need to run the **inst\_agg\_rsync.sh** script every time you upgrade IP/MPLSView unless you are explicitly told to do so by the Juniper Networks Technical Assistance Center (JTAC).

To configure the rsync cronjob on the database servers, run the **inst\_agg\_rsync.sh** script once on the primary database server and once on the backup database server:

```
wandl@server /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 '/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: 172.17.7.7
Remote IP/MPLSView product home directory [/u/wandl]:
Remote login ID associated with the SSH authorized key [wandl]:
Remote rsync installation path [/usr/local/bin/rsync]:
Aggregation rsync script generated...

Settings for 172.17.7.7 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
```

## Failing Over to the Backup Servers in a Four-Server Environment

In the event that the IP/MPLSView primary application server or primary database server fails, you can fail over to the corresponding backup application server or backup database server and initiate operation on the backup servers until the primary servers recover.

When you use IP/MPLSView in a four-server distributed environment, we recommend that you pair the primary application server with the primary database server, and the backup application server with the backup database server. As a result, when either the primary application server or primary database server fails, the server pair must fail over from primary to backup together.

If either the primary database server or the primary application server fails, stop the remaining services on the primary server. In this situation, you must fail over the primary database server first to prevent the data gateway server that is running on the primary application server from losing connectivity with the database.

To fail over to the backup database server if the primary database server fails:

1. Stop the backup database server.

```
/u/wandl/bin/stop_mplsview
```

2. Start IP/MPLSView on the backup database server.

```
/u/wandl/bin/startup_mplsview
```

This action causes the backup database server to become the master (primary) database server.

3. Make sure the aggregated traffic cronjob is disabled on the original primary database server and enabled on the backup database server.

4. To fail over to the backup application server if the primary application server fails, stop the remaining services on the primary application server.

```
/u/wandl/bin/stop_mplsview
```

5. On the primary application server, stop the rsync cronjob for the `/u/wandl/bin/rsync.sh` script as both the root user and the wandl user.

```
crontab -e
```

The cronjob is owned by the administrative user ID who installed IP/MPLSView. By default, this is the **wandl** user.

6. Comment out (disable) the following line in crontab:

```
#0,30 * * * * /u/wandl/bin/rsync.sh exec > /u/wandl/log/rsync.log
```

7. Stop the backup application server.

```
/u/wandl/bin/stop_mplsview
```

8. Make sure the rsync cronjob is disabled (commented out).

```
crontab -e
```

9. Start IP/MPLSView on the backup application server.

```
/u/wandl/bin/startup_mplsview
```

This action causes the backup application server to become the primary (master) application server.

10. Comment out the following entry in the `/u/wandl/db/config/mongodb.conf` file:

```
replicaSet = rs0
```

11. Restart the MongoDB process.

```
/u/wandl/bin/mongodb.sh stop
/u/wandl/bin/mongodb.sh start
```

12. Access the MongoDB CLI and issue the following commands:

```
/u/wandl/thirdparty/mongodb/bin/mongo
use local;
db.dropDatabase();
```

## Synchronizing the Database from the Backup Server to the Original Primary Server

When the original primary application server or the original primary database server resumes operating, you must synchronize the data from the backup server to the original primary server.

To synchronize data from the backup database server to the original primary database server:

1. Start the original primary MariaDB server in slave mode.

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

```
Slave MySQL server connected to master: backup-server ip-address
```

2. Register the master MariaDB server on the backup application server.

```
/u/wandl/bin/.mysql registermaster
```

3. Check the last data received on both the primary application server and the backup application server to make sure the data is synchronized.

```
/u/wandl/bin/mysql_rep1.sh lastdata
```

When you issue this command, the software displays an 11-digit timestamp that corresponds to the time of the last data collection. When both the primary MariaDB

server and the master MariaDB server display the same 11-digit timestamp, the data is synchronized.

For more information about the format of the timestamp, see [“Troubleshooting Database Synchronization in a Distributed Environment” on page 100](#).

4. To synchronize data from the backup application server to the original primary application server, start MongoDB.

```
/u/wand1/bin/mongodb.sh start
```

5. Leave (stop) the MongoDB cluster on the original primary application server.

```
/u/wand1/bin/mongodb_rep1.sh leavecluster
```

6. On the backup application server, restart the MongoDB in cluster mode, and uncomment the following entry in the `/u/wand1/db/config/mongodb.conf` file:

```
rep1Set = rs0
```

7. Stop and restart the MongoDB process.

```
/u/wand1/bin/mongodb.sh stop  
/u/wand1/bin/mongodb.sh start
```

8. Start MongoDB in slave mode on the backup application server.

```
/u/wand1/bin/mongodb_rep1.sh addslave
```

9. Stop IP/MPLSView on the backup application server.

```
/u/wand1/bin/stop_mplsview
```

10. If changes occurred in the network while the primary application server is out of service, use the following command only once on the backup application server to synchronize the original primary application server with the backup application server:

```
/u/wand1/bin/rsync.sh exec
```

11. Verify that the data has been synchronized.

```
/u/wand1/bin/mongodb_rep1.sh status  
/u/wand1/bin/mongodb_rep1.sh lastdata
```

## Switching Back to the Original Primary Server

After you synchronize the data from the backup application or database server to the original primary application or database server, you can switch back to the original primary server and resume operation.

To switch back to the original primary database server:

1. Stop IP/MPLSView on the backup database server and then on the primary database server, in that order.

```
/u/wandl/bin/stop_mplsview
```

2. Start the MariaDB server in slave mode on the backup database server.

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

3. Start MariaDB on the primary database server.

```
/u/wandl/bin/startup_mplsview
```

4. On the backup application server, register the MariaDB server with the master MariaDB server.

```
/u/wandl/bin/mysql_rep1.sh registermaster
```

5. Check the status on the primary and backup MariaDB servers.

```
/u/wandl/bin/mysql_rep1.sh status
```

6. Check the data consistency on the primary MariaDB server.

```
/u/wandl/bin/mysql_rep1.sh lastdata
```

7. To switch back to the original primary application server, on the backup application server, start the MongoDB and then leave the cluster.

```
/u/wandl/bin/mongodb.sh start  
/u/wandl/bin/mongodb_rep1.sh leavecluster
```

8. On the primary application server, start MongoDB and leave the cluster.

```
/u/wandl/bin/mongodb.sh start  
/u/wandl/bin/mongodb_rep1.sh leavecluster  
/u/wandl/bin/mongodb.sh stop
```

9. Restart the MongoDB in cluster node, and uncomment the following entry in the **/u/wandl/db/config/mongodb.conf** file:

```
rep1Set = rs0
```

10. Start IP/MPLSView on the primary application server.

```
/u/wandl/bin/startup_mplsview
```



11. Start MongoDB in slave mode on the primary application server.

```
/u/wandl/bin/mongodb_rep1.sh adds1ave
```

12. Check the status of MongoDB on the primary application server and then on the backup application server, in that order.

```
/u/wandl/bin/mongodb_rep1.sh status
```

13. If cronjob is commented out in the `/u/wandl/bin/rsync.sh` script on the primary application server, reenale it.

```
crontab -e
```

The cronjob is owned by the administrative user ID who installed IP/MPLSView. By default, this is the wandl user.

14. Uncomment (enable) the following line in crontab:

```
#0,30 * * * * /u/wandl/bin/rsync.sh exec > /u/wandl/log/rsync.log
```

#### Related Documentation

- [Replication and Rsync in Distributed Environments Overview on page 73](#)
- [Installing the Rsync Package and Automating SSH Login on page 74](#)
- [Troubleshooting Database Synchronization in a Distributed Environment on page 100](#)

---

## Administering Failovers in a Distributed Environment

This topic describes how to administer application and database server failovers in a distributed environment.

- [Administering Failovers Using the Setup-failover Script on page 97](#)
- [Example Failovers In a Distributed Environment on page 98](#)

### Administering Failovers Using the Setup-failover Script

Use the **setup-failover.sh** script to administer failovers.

When the primary and secondary application and database servers are running correctly, use the **setup-failover.sh** script and specify the **switchover** option on the secondary server to switch it to be the primary:

```
# /u/wandl/util/adminTools/setup-failover.sh switchover
```

If the primary servers has failed, use the **setup-failover.sh** script and specify the **survivor** option on the secondary server to make it run as a standalone server:

```
# /u/wandl/util/adminTools/setup-failover.sh survivor
```

After you make the survivor server run as a standalone, when the server that was previously failed comes back online, use the **setup-failover.sh** script and specify the **recover** option on the surviving primary server to synchronize data with the recovered server, and configure the recovered server to run as the secondary.

```
# /u/wandl/util/adminTools/setup-failover.sh recover
```



**NOTE:** Servers must be shut down using the **stop-all.sh** script before using the **setup-failover.sh** script.

## Example Failovers In a Distributed Environment

Use the following example procedure to understand how to administer failovers in a distributed environment.

In this example, the initial states of the servers are:

- ServerA—The primary application server. The IP address is represented as aaa.aaa.aaa.aaa.
- ServerB—The backup application server. The IP address is represented as bbb.bbb.bbb.bbb.
- ServerC—The primary database server. The IP address is represented as ccc.ccc.ccc.ccc.
- ServerD—The backup database server. The IP address is represented as ddd.ddd.ddd.ddd.

To administer failovers in a distributed environment:

1. To display the current state, run the following script on the primary application server:

```
ServerA# /u/wandl/util/adminTools/set-ip-all.sh
Current IP settings:
1.) Local (Primary Application Server) IP: aaa.aaa.aaa.aaa
2.) Backup Application Server IP: bbb.bbb.bbb.bbb
3.) Primary Distributed Database IP: ccc.ccc.ccc.ccc
4.) Backup Distributed Database IP: ddd.ddd.ddd.ddd
5.) Viewer Server IP: < if applicable >
6.) Remote Collection Servers: < if applicable >
7.) Data Collector Servers: < if applicable >
Numbers of Data Collector: < if applicable >
```

2. To verify the current state, run the following script on the secondary application server:

```
ServerB# /u/wandl/util/adminTools/set-ip-all.sh
Current IP settings:
Current IP settings:
1.) Local (Primary Application Server) IP: bbb.bbb.bbb.bbb
2.) Backup Application Server IP: aaa.aaa.aaa.aaa
3.) Primary Distributed Database IP: ddd.ddd.ddd.ddd
4.) Backup Distributed Database IP: ccc.ccc.ccc.ccc
5.) Viewer Server IP: < if applicable >
6.) Remote Collection Servers: < if applicable >
```

7.) Data Collector Servers: < if applicable >  
Numbers of Data Collector: < if applicable >

3. If ServerA fails, use the following three scripts on ServerB to shut down the server, configure it to run as a standalone server, and then start the server:

```
ServerB# /u/wandl/util/adminTools/stop-all.sh
ServerB# /u/wandl/util/adminTools/setup-failover.sh survivor
ServerB# /u/wandl/util/adminTools/start-all.sh
```

At this point:

- ServerA is failed.
  - ServerB is the standalone application server.
  - ServerC is the current backup database server.
  - ServerD is the current primary database server.
4. If after ServerB is configured to run as a standalone server, ServerA comes back online, use the following three scripts on ServerB to shut down the service, configure the recovered server to run as the secondary, and synchronize data from the survivor ServerB to recovered ServerA:

```
ServerB# /u/wandl/util/adminTools/stop-all.sh
ServerB# /u/wandl/util/adminTools/setup-failover.sh recover
ServerB# /u/wandl/util/adminTools/start-all.sh
```

At this point:

- ServerA is the current backup application server.
  - ServerB is the current primary application server.
  - ServerC is the current backup database server.
  - ServerD is the current primary database server.
5. If after ServerA, ServerB, ServerC, and ServerD are stable for a period of time and you want to restore the original state, use the following three scripts on the appropriate server to shut down the service, and configure ServerA to run as the primary:

```
ServerB# /u/wandl/util/adminTools/stop-all.sh
ServerA# /u/wandl/util/adminTools/setup-failover.sh switchover
ServerA# /u/wandl/util/adminTools/start-all.sh
```

At this point:

- ServerA is the current primary application server.
- ServerB is the current backup application server.
- ServerC is the current primary database server.
- ServerD is the current backup database server.

- Related Documentation**
- [Replication and Rsync in Distributed Environments Overview on page 73](#)
  - [Troubleshooting Database Synchronization in a Distributed Environment on page 100](#)

---

## Troubleshooting Database Synchronization in a Distributed Environment

---

During the MariaDB replication process, the IP/MPLSView database tables can become unsynchronized between the primary application server and the backup database server. An out-of-sync condition can occur for one or more of the following reasons:

- Either server is improperly shut down.
- Either server is interrupted by an event such as a power outage.

To troubleshoot synchronization problems that can occur during the MariaDB replication process, you must determine whether the databases are unsynchronized, and if so, use the following the procedure to resynchronize the databases.

To determine whether the database tables between the primary application server and the backup database server are synchronized:

1. Check the last data received on both the primary application server and the backup database server.

```
/u/wand1/bin/mysql_repl.sh lastdata
```

When you issue the **mysql\_repl.sh lastdata** command, the software displays the timestamp of the last data written to the database tables. If the command output for the primary application server and the backup database server displays the same timestamp, the database tables are synchronized. Conversely, if the output for the primary application server and the backup database server displays different timestamps, the database tables on the servers are potentially unsynchronized.

The timestamp is an 11-digit number in the format *YYYYMMDDIII*, where *YYYY* is the 4-digit year, *MM* is the 2-digit month, *DD* is the 2-digit day, and *III* is the 3-digit interval. The month is represented as a 2-digit integer starting with 00 for January through 11 for December. The interval is represented as a multiple of 5 minutes after 12:00 A.M., with a total of 288 five-minute intervals in a 24-hour period (one day).

For example, the timestamp 20101023133 (year 2010, month 10, day 23, interval 133) is November 23, 2010 at 11:05 A.M.

2. Run the **mysql\_repl.sh lastdata** command again after at least 5 minutes to confirm that the database tables are unsynchronized.

Wait at least 5 minutes before running the command again to allow sufficient time for one MariaDB replication cycle to complete.

If the output for the primary application server and the backup database server still displays different timestamps, the database tables are unsynchronized.

The following procedure uses the MariaDB CLI to resynchronize the IP/MPLSView databases between the primary application server and the backup database server. In this procedure, the terms *backup* and *slave* are equivalent, as are the terms *primary* and *master*.

To resynchronize the IP/MPLSView databases when they become unsynchronized:

1. On the backup (slave) database, access the MariaDB CLI.

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

2. Stop the backup database replication thread.

```
stop slave;
```

3. Reset (clean) the backup replication data on the backup database, and exit the MariaDB CLI.

```
reset slave;  
exit
```

4. Stop the backup (slave) database.

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

5. On the primary (master) database, access the MariaDB CLI.

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

6. Reset the master database replication record, and exit the MariaDB CLI.

```
reset master;  
exit
```

7. Stop IP/MPLSView on the primary application server.

```
/u/wandl/bin/stop_mplsview
```

8. (Optional) Back up the contents of the `/u/wandl/data/mysql/data/wandltraffic` directory on the backup database server.

9. Copy the directory and all files in the `/u/wandl/data/mysql/data/wandltraffic` directory from the primary application server to the backup database server.

10. Repair the MariaDB database tables on the unsynchronized server.

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

11. When the repair completes, start IP/MPLSView on the primary application server.

```
/u/wandl/bin/startup_mplsview
```

12. Start the backup (slave) database.

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

13. Register the backup (slave) to master, and start replication thread.

```
/u/wandl/bin/mysql_repl.sh registermaster
```

14. On the backup database, access the MariaDB CLI.

```
/u/wandl/bin/mp1senvsetup.sh  
/u/wandl/thirdparty/mysql/bin/mysql -uroot -pwandlroot -A wandltraffic
```

15. Check the backup database for error messages, where *database-drive* is the letter of the drive on which the backup database resides (for example, \G).

```
show slave status \database-drive;
```

16. Exit the MariaDB CLI.

```
exit
```

17. After waiting at least 5 minutes, check the last data received on both the primary application server and the backup database server to make sure the database tables are resynchronized.

```
/u/wandl/bin/mysql_repl.sh lastdata
```

Waiting at least 5 minutes before running the **mysql\_repl.sh lastdata** command allows sufficient time for one MariaDB replication cycle to complete.

If the command output for the primary application server and the backup database server displays the same timestamp, the database tables are resynchronized.

**Related  
Documentation**

- [Replication and Rsync in Distributed Environments Overview on page 73](#)
- [Installing the Rsync Package and Automating SSH Login on page 74](#)

## CHAPTER 7

# Installing IP/MPLSView High Availability for Linux OS

- [IP/MPLSView Linux OS High Availability Overview on page 103](#)
- [Installing the Linux Operating System for IP/MPLSView High Availability on page 105](#)
- [Configuring the Linux Operating System for IP/MPLSView High Availability on page 110](#)
- [Installing IP/MPLSView in a Distributed Environment on page 122](#)
- [Starting, Relocating, and Stopping IP/MPLSView from the GUI or CLI on page 131](#)
- [Recording Cluster Setup Information on page 134](#)
- [Frequently Asked Questions: Cluster Administration on page 135](#)

### IP/MPLSView Linux OS High Availability Overview

---

The high availability feature uses computer clusters for providing failover and high availability services for IP/MPLSView. You can configure high availability for the application and database servers.

This chapter provides detailed instructions for installing and configuring high availability support for the Community Enterprise Operating System (CentOS) 6.6 and later 64-bit Linux operating systems with IP/MPLSView Release 6.3.0. CentOS is a free Linux distribution built from the open source code of Red Hat Enterprise Linux (RHEL).

High availability provides redundancy, reliability, and resiliency for packet-based communications to ensure service continuity in the event of a network outage or device failure. High availability provides both hardware-specific and software-specific methods to ensure minimal downtime and ultimately improve the performance of your network.

The following software components, which are part of the RHEL High Availability Add-On, are installed for high availability:

- Resilient storage—Global File System 2 (GFS2) supports concurrent access.
- High availability—The CentOS high availability add-on reduces application downtime, ensures that a cluster has no single point of failure, and isolates unresponsive applications and devices to prevent corruption of critical enterprise data.

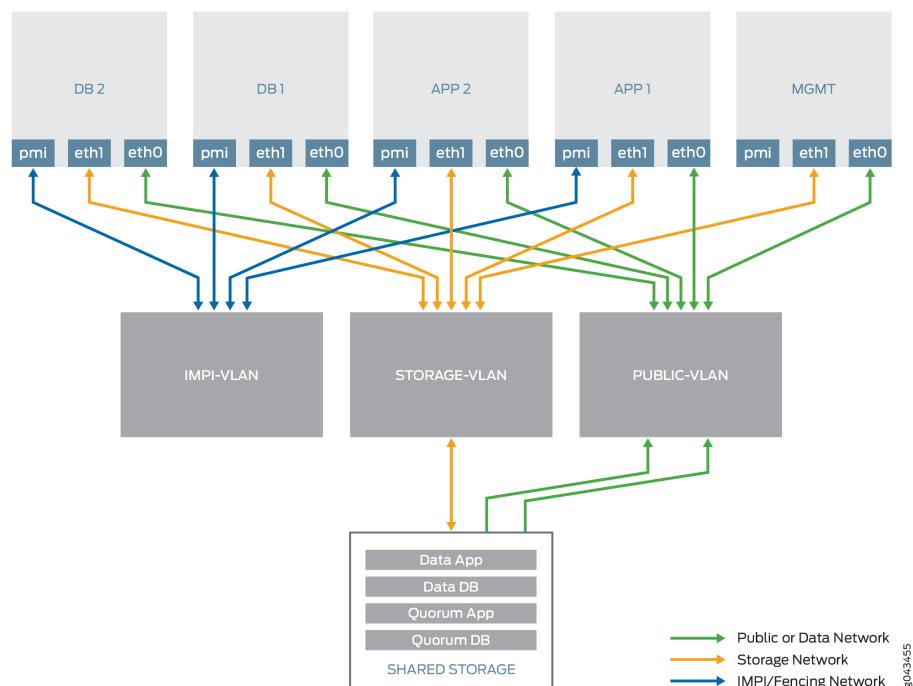
- High availability management—High availability service management, which is installed only on the management node, enables you to create and manage high-availability cluster services in a CentOS cluster.

Figure 6 on page 104 shows a typical server setup for installing Linux high availability support for CentOS 6.6. Your setup can vary depending on the server and storage area network (SAN) vendor you are using.

The sample hardware setup consists of the following components:

- Two 64-bit application servers (labeled APP1 and APP2)
- Two database servers (labeled DB1 and DB2)
- One management node (labeled MGMT)
- One SAN (labeled Shared Storage)
- One network (fiber) switch

**Figure 6: Linux OS High Availability Hardware Setup**



#### Related Documentation

- [Installing the Linux Operating System for IP/MPLSView High Availability on page 105](#)
- [Configuring the Linux Operating System for IP/MPLSView High Availability on page 110](#)
- [Installing IP/MPLSView in a Distributed Environment on page 122](#)
- [Starting, Relocating, and Stopping IP/MPLSView from the GUI or CLI on page 131](#)
- [Frequently Asked Questions: Cluster Administration on page 135](#)



## Installing the Linux Operating System for IP/MPLSView High Availability

This topic describes how to install and configure the CentOS 6.6 64-bit operating system on the application servers, database servers, and management nodes in your network. In addition, it provides guidelines for partitioning the SAN storage disk so that each partition is accessible to a CentOS cluster group.

- [Installing Linux OS on Your Servers on page 105](#)
- [Installing Linux OS on the Management Nodes on page 106](#)
- [Guidelines for Partitioning the SAN Storage Disk on page 106](#)
- [Installing the Red Hat Enterprise Linux High Availability Add-On on page 108](#)
- [Creating the Quorum Disk on page 108](#)
- [Setting Up the Global File System 2 Partition on page 109](#)

### Installing Linux OS on Your Servers

Before you install CentOS 6.6 64-bit OS on your network servers:

- Make sure your system has static IP addresses configured for both public and private interfaces.
- In the `/etc/hosts` file, include an entry for each node participating in the CentOS cluster.

To install the CentOS 6.6 64-bit OS package on all servers in your network:

1. Use the minimal desktop installation option according to your local policies.
2. Update each server with the CentOS 6.6 64-bit OS installation package using the following command:

```
yum -y update package-name
```

3. Install the nonstandard telnet and ksh packages.
4. Assign private IP addresses (such as 10.10.10.0/24) between the `eth1` interfaces.

For example, using the sample high availability hardware setup, you might assign these addresses as follows:

```
Node1:eth0:172.25.152.19 (public network)
Node1:eth1:10.10.10.1/24 (storage network)
Node1:IPMI:172.25.152.116 (fencing network)
Node2:eth0:172.25.152.20 (public network)
Node2:eth1:10.10.10.2/24 (storage network)
Node2:IPMI:172.25.152.117(fencing network)
```

5. Use the following commands to configure the CentOS cluster as the root user to disable the IPTables, IP6Tables, and NetworkManager services.

```
chkconfig iptables off
chkconfig ip6tables off
chkconfig NetworkManager off
```

6. Disable SELinux by changing the entry in the `/etc/sysconfig/selinux` file from **enforcing** to **disabled**.

```
vi file: /etc/sysconfig/selinux
```

Disabling SELinux prevents it from blocking or interfering with some of the ports that must be opened for high availability and the application.

7. Reboot the device.

## Installing Linux OS on the Management Nodes

Before you install the CentOS 6.6 64-bit OS on the management nodes:

- Make sure each management node in your network meets the following minimum requirements:
  - 2.0 GHz CPU
  - 4 GB memory
  - 20 GB hard disk drive
  - 1 Ethernet interface
- Make sure your system has static IP addresses configured for both public and private interfaces.
- In the `/etc/hosts` file, include an entry for each node in your network.

To install the CentOS 6.6 64-bit OS package on all management nodes in your network:

1. Use the minimal desktop installation option according to your local policies.
2. Update each management node with the CentOS 6.6 64-bit OS installation package.

```
yum -y update package-name
```

## Guidelines for Partitioning the SAN Storage Disk



**BEST PRACTICE:** Active application and database servers save both the data collected from the router network and the processed data in the shared disk. The data saved by application and database servers requires segregation on the storage disk. As a result, you should create two partitions on the storage disk to ensure that each partition is accessible to a cluster group.

The partition accessible to the application cluster group should not be accessible to the database cluster group. Conversely, the partition accessible

to the database cluster group should not be accessible to the application cluster group.

You can create these shared storage devices by using the Internet Small Computer System Interface (iSCSI) standard, or by directly attaching Fibre Channel Arbitrated Loop (FC-AL) host bus adapters (HBAs).

For information about installing required drivers, creating logical unit numbers (LUNs), and identifying the LUNs to the CentOS servers, see the documentation provided by your SAN vendor.

When the CentOS software can detect and identify the LUNs, install the Linux OS high availability software. If you are running the database and application on the same server, you can allow access to both servers in tandem regardless of the server's role in the cluster.

---

## Installing the Red Hat Enterprise Linux High Availability Add-On

To install the RHEL High Availability Add-On:

- Install the required processes (daemons) and services for high availability clustering by issuing the following commands as the root user on each node:

```
[root@node1 ~]# yum groupinstall "High Availability" "Resilient Storage"
[root@node2 ~]# yum groupinstall "High Availability" "Resilient Storage"
[root@node3 ~]# yum groupinstall "High Availability Management" "High
Availability"
```

In this example, node3 is the management node.

## Creating the Quorum Disk

Configuring a quorum disk, also known as a QDisk, in combination with fencing for a CentOS high availability cluster, detects and sends notifications about available nodes in the cluster and shuts off any nodes in the cluster that are unavailable. Fencing is the process of separating an unavailable or malfunctioning cluster node from the resources it manages, without the support of the node being fenced. When used in combination with a quorum disk, fencing can prevent resources from being improperly used in a high availability cluster.

This section describes a typical procedure for configuring the quorum disk. Depending on your SAN setup, your procedure might vary. Consult the documentation provided by your SAN vendor for the instructions you should follow.

For more information about configuring and using a quorum disk in a CentOS high availability cluster, including options for sizing the quorum disk, see [“Frequently Asked Questions: Cluster Administration” on page 135](#).

To create the quorum disk:

1. Confirm that the partition in which you are configuring the quorum disk is not in use by other users.
2. Create the quorum disk on each node (node1 and node2 in this example) by issuing the following command as the root user:



**NOTE:** Using the following `mkqdisk` command to configure the quorum disk destroys all data in the specified partition.

```
[root@node1 ~]# mkqdisk -c /dev/sdd -l quorum
```

```
mkq disk v3.0.12.1
```

```
Writing new quorum disk label 'quorum' to /dev/sdd.
```

```
WARNING: About to destroy all data on /dev/sdd; proceed [N/y] ? y
```

Warning: Initializing previously initialized partition

Initializing status block for node 1...

Initializing status block for node 2...

When you set up the QDisk, use the label quorum, as specified in the **mkqdisk** command.

## Setting Up the Global File System 2 Partition

Global File System 2 (GFS2) is a clustered file system in which data is shared among GFS2 nodes with a single, consistent, and coherent view of the file system name space. Processes on different nodes work with GFS2 files in the same way that processes on one node can share files in a local file system.

To set up GFS2 services on the cluster:

1. Format the SAN target on which the cluster nodes are mapped (**/dev/sdc** in this example) to use the following description:

- Formatting file system: **GFS2**
- Locking protocol: **lock\_dlm**
- Cluster name: **cluster1**
- File system name: **GFS**
- Journal: **2**
- Partition: **/dev/sdc**

2. Configure the GFS2 file system on any of the nodes in the partition by issuing the following command as the root user.

This command takes effect on all other nodes participating in the same partition (**/dev/sdc** in this example) and creates a lock table based on the specified cluster name.

```
[root@node1 ~]# mkfs.gfs2 -p lock_dlm -t application:GFS -j 2 /dev/sdc
```

This will destroy any data on **/dev/sdc**.

It appears to contain: Linux GFS2 Filesystem (blocksize 4096, lockproto lock\_dlm)

Are you sure you want to proceed? [y/n] y

```
Device:                /dev/sdc
Blocksize:             4096
Device Size            49.34 GB (2711552 blocks)
Filesystem Size:       49.34 GB (2711552 blocks)
Journals:              2
Resource Groups:       42
Locking Protocol:      "lock_dlm"
Lock Table:            "application:GFS"
UUID:                  2ff81375-31f9-c57d-59d1-7573cdfaff42
```

- Related Documentation**
- [IP/MPLSView Linux OS High Availability Overview on page 103](#)
  - [Configuring the Linux Operating System for IP/MPLSView High Availability on page 110](#)
  - [Installing IP/MPLSView in a Distributed Environment on page 122](#)
  - [Recording Cluster Setup Information on page 134](#)
  - [Frequently Asked Questions: Cluster Administration on page 135](#)

## Configuring the Linux Operating System for IP/MPLSView High Availability

---

- [Assigning a Password to the Ricci Daemon on page 110](#)
- [Starting Conga Services on page 111](#)
- [Accessing the Luci Console on page 111](#)
- [Creating the High Availability Cluster on page 112](#)
- [Configuring the Quorum Disk on page 114](#)
- [Configuring Fence Devices on page 114](#)
- [Configuring Nodes to Use Fence Devices on page 116](#)
- [Configuring the Failover Domain on page 117](#)
- [Creating Service Groups on page 119](#)
- [Automating SSH Login from All Servers on page 121](#)

### Assigning a Password to the Ricci Daemon

The *ricci* daemon is a cluster management and configuration process that dispatches incoming messages to underlying management modules. When *ricci* is run with no options, it runs as a daemon and listens to the default port (11111). You must run *ricci* as the root user.

To assign a password to the *ricci* daemon:

1. Use the following command as the root user on both cluster servers:

```
[root@node1 ~]# passwd examplepw
```

```
Changing password for user ricci.
```

```
New password:
```

```
BAD PASSWORD: it is based on a dictionary word
```

```
BAD PASSWORD: is too simple
```

```
Retype new password:
```

```
passwd: all authentication tokens updated successfully.
```

```
Restart the ricci services to take the changes affect
```

```
[root@node1 ~]# /etc/init.d/ricci start
```

```
Starting oddjobd:
```

```
[ OK ]
```

```
generating SSL certificates... done
```

```
Generating NSS database... done
```

```
Starting ricci:
```

```
[ OK ]
```

2. Confirm that the ricci services start after the reboot.

```
[root@node1 ~]# chkconfig ricci on
```

## Starting Conga Services

The ricci daemon works in conjunction with *luci*, which is the cluster management process that oversees and manages all of the ricci nodes. The ricci and luci daemons are collectively referred to as Conga, which is the GUI application you use to configure the services and cluster nodes. The Conga application provides centralized configuration and management for the RHEL High Availability Add-On.

You must start Conga services on the management server, which is node3 in this example.

To start Conga services (luci) on the management server:

1. As the root user, start the luci services.

```
[root@node3 ~]# /etc/init.d/luci start
```

```
Adding following auto-detected host IDs (IP addresses/domain names),
corresponding to 'node3.example' address, to the configuration of
self-managed certificate '/var/lib/luci/etc/cacert.config' (you can change
them by editing '/var/lib/luci/etc/cacert.config', removing the generated
certificate '/var/lib/luci/certs/host.pem' and restarting luci): (none
suitable found, you can still do it manually as mentioned above)
```

```
Generating a 2048 bit RSA private key
writing new private key to '/var/lib/luci/certs/host.pem'
Starting saslauthd: [ OK ]
Start luci... [ OK ]
```

2. Confirm that the luci services start.

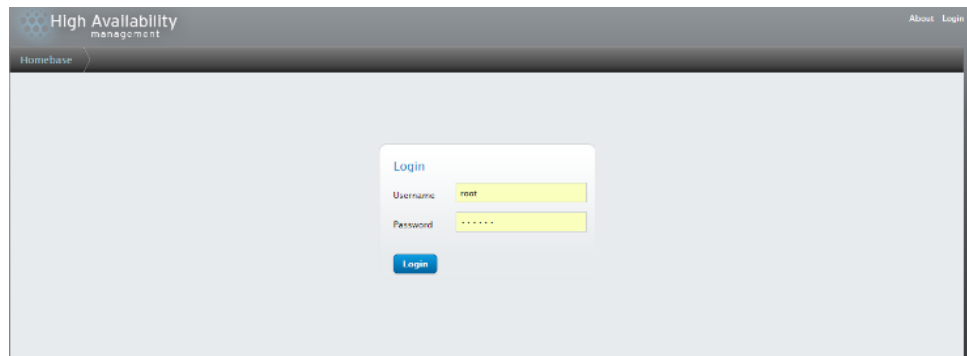
```
[root@node1 ~]# chkconfig luci on
```

## Accessing the Luci Console

To access the luci console:

1. In your Web browser, enter **https://ip-address:8084**, where *ip-address* is the IP address of your management server.

Figure 7: High Availability Luci Console



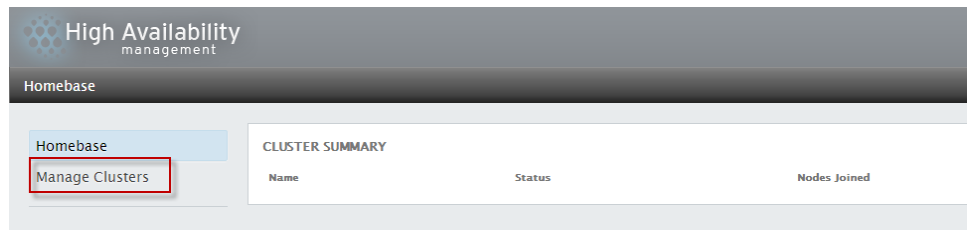
2. In the Username field, enter **root**.
3. In the Password field, enter the root password.

## Creating the High Availability Cluster

To create a new high availability cluster:

1. In the Homebase window, select **Manage Clusters**.

Figure 8: High Availability Manage Clusters Luci Console



2. Click **Create** to display the Create New Cluster window.

Figure 9: High Availability Manage Clusters Actions



3. In the Create New Cluster window, provide the properties for the new cluster.



Figure 10: Create New Cluster Window

Cluster Name: application

☒ Use the Same Password for All Nodes

| Node Name | Password | Ricci Hostname | Ricci Port |
|-----------|----------|----------------|------------|
| node1     | .....    | node1          | 11111      |
| node2     | .....    | node2          | 11111      |

Add Another Node

☐ Download Packages  
☒ Use Locally Installed Packages  
☐ Reboot Nodes Before Joining Cluster

☒ Enable Shared Storage Support

Create Cluster Cancel

- In the Cluster Name field, enter the name of the new cluster (**application** in this example).
- In the Node Name fields, enter the name, password, ricci hostname, and default ricci port for each node participating in the cluster.

In this example, the node names and ricci hostnames are **node1** and **node2**, the password is the value specified in *Assigning a Password to the Ricci Daemon*, and the default ricci port is **11111**. Make sure each node you specify is reachable.

- Select **Use Locally Installed Packages**.
- Select **Enable Shared Storage Support** to specify that GFS2 is being used to share data among the nodes in the cluster.
- Click **Create Cluster**.

The nodes are added to the high availability cluster.

Figure 11: Create New Cluster Add Nodes Window

| Node Name | Node ID | Votes | Status         | Uptime      | Hostname |
|-----------|---------|-------|----------------|-------------|----------|
| node1     | 1       | 1     | Cluster Member | 56:21:33:36 | node1    |
| node2     | 2       | 1     | Cluster Member | 51:22:30:58 | node2    |

## Configuring the Quorum Disk

To configure the quorum disk:

1. Select the **Configure** tab.
2. Select the **QDisk** tab. The Quorum Disk Configuration window is displayed.

*Figure 12: Quorum Disk Configuration Window*

3. In the **By Device Label** field, enter the label name of the quorum disk specified in *Creating the Quorum Disk*.
4. In the **Heuristics** fields, enter the command you want the software to use to check the quorum status among all nodes in the cluster, and the interval at which you want to run the command.  
  
The Heuristics fields specify where your heartbeat connection is configured (for example, the **eth1** interface).
5. Click **Apply**.

## Configuring Fence Devices

To configure the fence devices:

1. Select the **Fence Devices** tab.
2. Select the **Fence Daemon** tab and click **Add**.
3. In the **Add Fence Device (Instance)** window, specify information for each fence device you want to add.
4. Click **Submit** to add the specified fence device to the cluster.

Figure 13: Add Node1 and Node2 Fence Device (Instance) Windows

### Add Fence Device (Instance)

IPMI Lan

▼

|                            |                                             |
|----------------------------|---------------------------------------------|
| Fence Type                 | IPMI Lan                                    |
| Name                       | <input type="text" value="node1-ipmi"/>     |
| IP Address or Hostname     | <input type="text" value="172.25.152.116"/> |
| Login                      | <input type="text" value="ADMIN"/>          |
| Password                   | <input type="password" value="....."/>      |
| Password Script (optional) | <input type="text"/>                        |
| Authentication Type        | <div>Password▼</div>                        |
| Use Lanplus                | <input type="checkbox"/>                    |
| Ciphersuite to use         | <input type="text"/>                        |
| Privilege Level            | <div>Default▼</div>                         |
| IPMI Operation Timeout     | <input type="text"/>                        |
| Power Wait (seconds)       | <input type="text"/>                        |
| Delay (seconds)            | <input type="text"/>                        |

Submit

Cancel

### Add Fence Device (Instance)

|                                                                                          |                                             |
|------------------------------------------------------------------------------------------|---------------------------------------------|
| <div>IPMI Lan ▼</div>                                                                    |                                             |
| Fence Type                                                                               | IPMI Lan                                    |
| Name                                                                                     | <input type="text" value="node2-ipmi"/>     |
| IP Address or Hostname                                                                   | <input type="text" value="172.25.152.117"/> |
| Login                                                                                    | <input type="text" value="ADMIN"/>          |
| Password                                                                                 | <input type="password" value="....."/>      |
| Password Script (optional)                                                               | <input type="text"/>                        |
| Authentication Type                                                                      | <div>Password ▼</div>                       |
| Use Lanplus                                                                              | <input type="checkbox"/>                    |
| Ciphersuite to use                                                                       | <input type="text"/>                        |
| Privilege Level                                                                          | <div>Default ▼</div>                        |
| IPMI Operation Timeout                                                                   | <input type="text"/>                        |
| Power Wait (seconds)                                                                     | <input type="text"/>                        |
| Delay (seconds)                                                                          | <input type="text"/>                        |
| <div> <input type="button" value="Submit"/> <input type="button" value="Cancel"/> </div> |                                             |



### Configuring Nodes to Use Fence Devices

To configure nodes to use fence devices:

1. Select **Homebase** and click on the cluster name.
2. Select one of the hosts.
3. In the Fence Device pane, select **Add Fence Method** and enter **IPMI Lan**.

Figure 14: Add Fence Device Window Fence Method

| node1 | 1 | 1 | Cluster Member | 09:17:51:08 | node1 |
|-------|---|---|----------------|-------------|-------|
| node2 | 2 | 1 | Cluster Member | 30:01:23:06 | node2 |

node1  
Status Cluster Member

Properties

Number of votes:

ricci host:

ricci port:

Services

Failover Domains

application-fd

Priority

Fence Devices

Method

IPMI

Name:  Type/Values: IPMI Lan

4. Click **Add Fence Instance** and select an appropriate IPMI device.

5. Repeat Steps 1 to 4 for the other nodes in the cluster.

Figure 15: Add Fence Device Window Nodes List

| Add Delete |            |             |                |
|------------|------------|-------------|----------------|
| Name       | Fence Type | Nodes Using | Hostname       |
| node1-ipmi | IPMI Lan   | 1           | 172.25.152.116 |
| node2-ipmi | IPMI Lan   | 1           | 172.25.152.117 |

Select an item to view details

## Configuring the Failover Domain

To configure the failover domain:

1. Select the **Failover Domains** tab.
2. Click **Add**.
3. Enter a name for the failover domain and provide other required information.
4. Click **Create** to create the new failover domain.

Figure 16: Add Failover Domain to Cluster Dialog Box

### Add Failover Domain to Cluster

Name

☐ Prioritized Order the nodes to which services failover.

☐ Restricted Service can run only on nodes specified.

☐ No Failback Do not send service back to 1st priority node when it becomes available again.

| Member |                                     | Priority                       |
|--------|-------------------------------------|--------------------------------|
| node1  | <input checked="" type="checkbox"/> | <input type="text" value="1"/> |
| node2  | <input checked="" type="checkbox"/> | <input type="text" value="1"/> |

## Creating Service Groups

After you configure the GFS2, IP address, and script services for the high availability cluster, you must configure a service group and add these same services to the service group. With IP/MPLSView, you can use multiple failover domains and multiple service groups instead of multiple clusters.

To create a service group and add resources to it:

1. Select the **Service Groups** tab and click **Add**.

The Add Service Group to Cluster window is displayed.

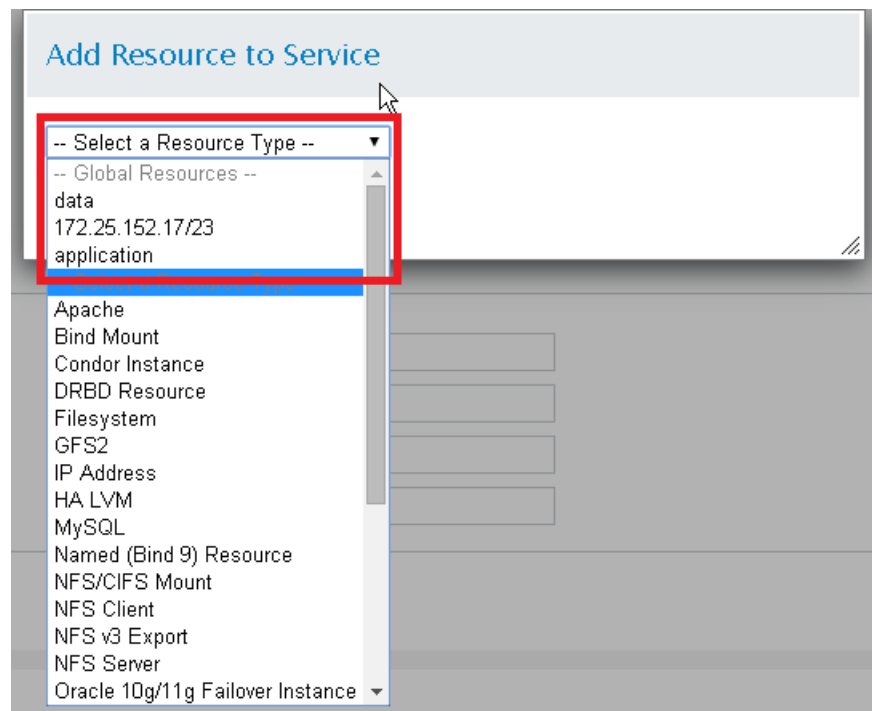
*Figure 17: Add Service Group to Cluster Window*

The screenshot shows the 'Add Service Group to Cluster' window. The 'Service Name' field contains 'application-SG'. The 'Automatically Start This Service' checkbox is checked. The 'Run Exclusive' checkbox is unchecked. The 'Failover Domain' dropdown menu is set to 'application-FD'. The 'Recovery Policy' dropdown menu is set to 'Relocate'. Below these fields is a section titled 'Restart Options' with two input fields: 'Maximum Number of Restart Failures Before Relocating' and 'Length of Time in Seconds After Which to Forget a Restart'. At the bottom of the window are three buttons: 'Add Resource', 'Submit', and 'Cancel'. The 'Submit' button is highlighted with a red box.

2. Provide the following information for the new service group:
  - a. In the Service Name field, enter the name of the new service group (**application-SG** in this example).
  - b. Select **Automatically Start This Service**.
  - c. In the Failover Domain field, select the name of the failure domain configured in *Configuring Nodes to Use Fence Devices* (**application-FD** in this example).
  - d. In the Recovery Policy field, select **Relocate**.
3. Click **Add Resource**.

The Add Resource to Service window is displayed.

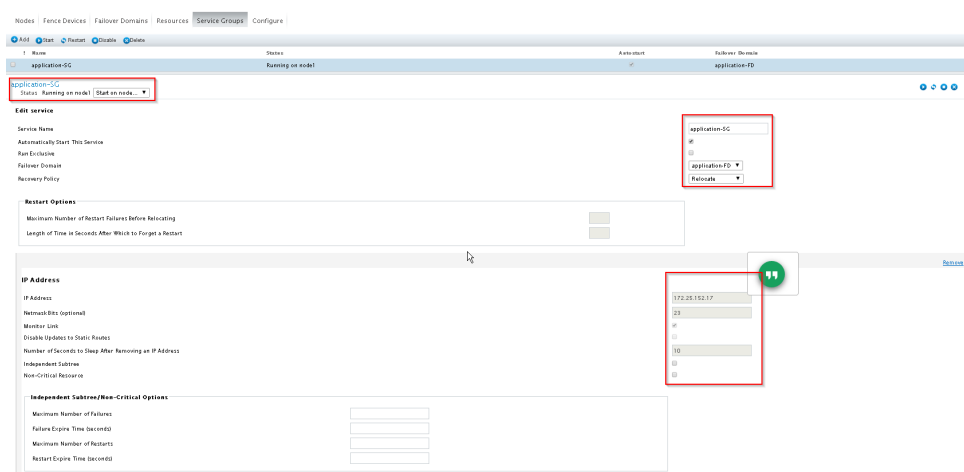
Figure 18: Add Resource to Service Window



4. Add the GFS2 resource to the service group.
  - a. Select **Select a Resource Type > GFS2**.  
 The Add Resource to Cluster window for GFS2 is displayed, as shown in *Creating Resources*.
  - b. Click **Submit** to add the GFS2 resource to the service group.
5. Add the IP Address resource to the service group.
  - a. Select **Select a Resource Type > IP Address**.  
 The Add Resource to Cluster window for IP Address is displayed, as shown in *Creating Resources*.
  - b. Click **Submit** to add the IP Address resource to the service group.
6. Add the Script resource to the service group.
  - a. Select **Select a Resource Type > Script**.  
 The Add Resource to Cluster window for Script is displayed, as shown in *Creating Resources*.
  - b. Click **Submit** to add the Script resource to the service group.
7. Refresh the Web console to verify that the GFS2, IP Address, and Script resources are running on any of the nodes in your cluster.



Figure 19: Service Groups Edit Service



## Automating SSH Login from All Servers

To ensure that you can perform an automatic SSH login from the database servers to the application servers, you must automate the SSH login process on both database servers.

You perform this procedure only once. You do not need to repeat the procedure when you upgrade the software unless you change the password or IP address of the server as part of the upgrade.

To automate SSH login on all database servers:

1. On the primary database server, log in as the wandl user and change the current directory to the wandl home directory (`/home/wandl` in this example.)
2. Generate a pair of authentication keys without specifying a passphrase.

```
/home/wandl> ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/wandl/.ssh/id_rsa):
Created directory '/home/wandl/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/wandl/.ssh/id_rsa.
Your public key has been saved in /home/wandl/.ssh/id_rsa.pub.
The key fingerprint is:
94:7c:a6:d2:b6:80:19:a4:b9:f4:7d:7f:09:d4:f2:52 wandl@lexu
```

3. Use SSH to create the `.ssh` directory on the primary application server.

Substitute *remosthostip* with the IP address of the primary application server. When prompted, enter the wandl password of the remote host.

```
/home/wandl> ssh wandl@remosthostip mkdir -p .ssh
```

The authenticity of host '*<remosthostip>* (*<remosthostip>*)' can't be

established.

RSA key fingerprint is 8a:d9:a9:c5:91:6a:e6:23:8c:2f:ad:4f:ea:48:78:0b.

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 primary application server's authorized keys, and enter the wandl password for the primary application server.

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

5. From the database servers, log in to the application servers to confirm that automatic SSH login is enabled.

If automatic SSH login is working properly, you should be able to directly log in to the application servers from the database servers without specifying a password.

#### Related Documentation

- [IP/MPLSView Linux OS High Availability Overview on page 103](#)
- [Installing the Linux Operating System for IP/MPLSView High Availability on page 105](#)

---

## Installing IP/MPLSView in a Distributed Environment

---

This section describes how to install IP/MPLSView on your application servers and database servers.

Before you install IP/MPLSView, make sure your configuration meets all of the following prerequisites:

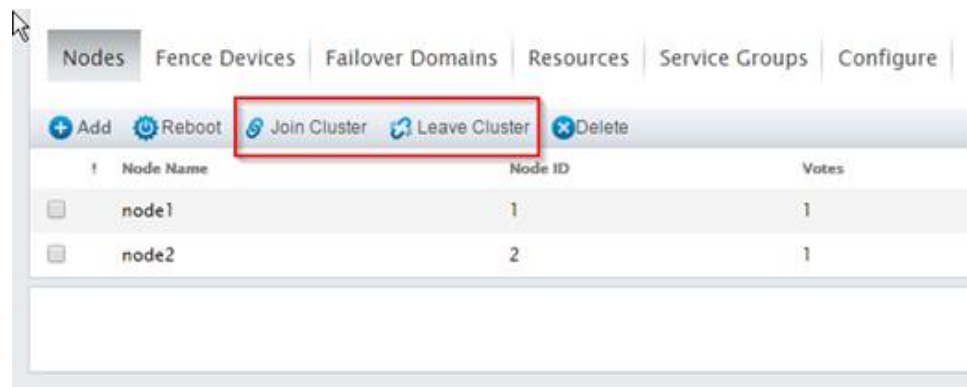
- In a distributed environment where the database server and the application server are running on separate servers, follow the steps in “[Installing the Linux Operating System for IP/MPLSView High Availability](#)” on page 105 and “[Configuring the Linux Operating System for IP/MPLSView High Availability](#)” on page 110 for both the database server and the application server.
- Apply all required patches for the network hardware (servers, HBAs, and storage) to the operating system.
- Assign the same login ID and password for both the root user and the wandl user on all primary and backup servers.
- Enable SSH login services on the servers.
- Ensure that you can use SSH to log in to the application servers from the database servers without having to specify a password.
- Use the **yum -y update** command to ensure that all servers have the same patch level installed.

## Installing IP/MPLSView on Distributed Application and Database Servers

To install IP/MPLSView on the primary application and primary database servers:

1. Make sure the cluster works with IP/GFS2 share. Do this by first failing back and forth to test the Linux high availability performance and reliability.
2. Always install the application into a new application directory such as `/home/wandl/ipmplsview_02_05_15/` and place the data into the shared storage GFS2 disk. For example: `/data/wandldata/`.
3. Select **Node 2** and click **Leave Cluster**.

Figure 20: Join and Leave Cluster Selections



4. On Node1, start Application-SG with disk and VIP resources enabled only.
5. Install the application on the first node from the server directory in the installation package. Run the install script as you do for a standard IP/MPLSView installation without high availability support. Do not start IP/MPLSView.
6. Select Node1 and click **Leave Cluster**.
7. Select Node 2 and click **Join Cluster**.
8. On Node2, start the Application-SG with the disk and VIP resources enabled only.
9. Install the application on the second node from the server directory in the installation package. Run the install script as you do for a standard IP/MPLSView installation without high availability support. Do not start IP/MPLSView.
10. Enable a script resource in the Application-SG Service Group.

11. Start on either node (this can take a while once the application is added).
12. To test the installation, use the following command on both servers to verify how long the processes take to bring down and then restore and compare the results:

```
#while true; do /u/wandl/bin/status_mplsview; sleep 5; done
```

13. Repeat the installation on the backup application server and backup database server.  
Keep the following guidelines in mind when installing IP/MPLSView on your application and database servers:

- Store the data in the **/u/wandl/data** directory in an external storage device that is accessible to both the primary and backup application and database servers.
- When you configure the IP address settings, change the following parameters to the shared IP address, also known as the virtual IP address (VIP), of the application server to ensure that switchovers on the server do not affect the client application.
  - Server IP—Change to the shared IP address.
  - Webserver IP—Change to the shared IP address if you are in a distributed environment and using separate application and database servers.
  - Mongo DB—Used for the application server only.
  - Remote Database—Change to the shared IP address if you are using a remote database not hosted by the application server.

The following is an example of the installation script for a typical IP/MPLSView installation.

```
[root@db1-1ha server]# ./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.
Preparing to install IP/MPLSView ...
Setting soft limit of open files to 65535 for wandl user
Setting hard limit of open files to 65535 for wandl user
Setting soft limit of open processes to 10240 for wandl user
Setting hard limit of open processes to 10240 for wandl user
RHEL6 detected, disable huge page
saving settings to /etc/rc.local...
```

```
Changing ipv4/tcp_fin_timeout from 60 to recommended value 30
Changing ipv4/tcp_keepalive_intvl from 75 to recommended value 30
Changing ipv4/tcp_keepalive_probes from 9 to recommended value 5
Changing core/netdev_max_backlog from 1000 to recommended value 3000
Changing core/somaxconn from 128 to recommended value 3000
```

```
This software requires a Linux ID as the owner.
A Linux ID is the login name when you login to this Linux 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 (wandl):
Group is set to: wandl
Please enter the directory where this software will be installed.
(default=/home/wandl/ipmplsview):
Are you sure you want to install into /home/wandl/ipmplsview (default=yes)? [y/n]
] y

```

```

Checking available disk space ...
Please enter the directory where the data will be stored.
(default=/home/wandl/wandldata):
Are you sure you want to install into /home/wandl/wandldata (default=yes)? [y/n]
y

```

```

Copying Java native library files...
Switching user to "wandl" ...
Main Menu
Server Configuration Settings:
(A) Overall Settings
(B) IP Address
(C) Memory Settings
(D) Port Settings
(E) Data Storage Capacity Settings
(F) Online Fault Management Settings
(G) Advanced Configuration
(H) NorthStar AMQP Settings

```

```

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

```

```

(A) Overall Settings
General Administrative Settings for server db1-lha :
1.) Installation Directory.....: /home/wandl/ipmplsview
2.) Data Directory.....: /home/wandl/wandldata
3.) Admin User.....: wandl
4.) Admin Group.....: wandl
5.) Email Server IP.....: 172.25.152.112
6.) Email Server User.....: wandl
7.) Email Server Password.....:
8.) Application Monitor Email Recipient...:
9.) Enable Server Monitoring.....: OFF
10.) Mapping for non-Unicode characters....:

```

```

Please select a number to modify.
[<CR>=return to main menu]:

```

```

Main Menu
Server Configuration Settings:
(A) Overall Settings
(B) IP Address
(C) Memory Settings
(D) Port Settings
(E) Data Storage Capacity Settings
(F) Online Fault Management Settings
(G) Advanced Configuration
(H) NorthStar AMQP Settings

```

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

(B) IP Address  
IP/MPLSView Server IP Address Settings:  
1.) Webserver IP.....: 172.25.152.9  
2.) LDAP Server IP.....: 172.25.152.112  
3.) External Webserver IP (for NAT)....:  
4.) Mongo DB IP.....: 127.0.0.1  
5.) Use Remote Database.....: NO

Please select a number to modify.  
[<CR>=return to main menu]:

Main Menu  
Server Configuration Settings:  
(A) Overall Settings  
(B) IP Address  
(C) Memory Settings  
  
(D) Port Settings  
(E) Data Storage Capacity Settings  
(F) Online Fault Management Settings  
(G) Advanced Configuration  
(H) NorthStar AMQP Settings

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

(C) Memory Settings  
1.) Task Manager Memory.....: 256  
2.) Webserver Memory.....: 1024  
3.) Thrift Server Memory.....: 256  
4.) HornetQ Memory.....: 256  
5.) DGS Memory.....: 512  
6.) Application Monitor Memory.....: 128  
7.) Threshold Server Memory.....: 256  
8.) SNMP Trap Daemon Memory.....: 128  
9.) MongoDB Memory.....: 512  
10.) Event Server Memory.....: 256  
11.) Aggregation Memory.....: 1024  
12.) Selective Interface Manager Memory.....: 256  
13.) Maria Database Memory.....: 256  
Total system physical memory: 32081 MB

After starting IP/MPLSView, check "/u/wandl/bin/status\_mplsview" to see the actual memory usage, which can be used to tune the memory settings.

Please select a number to modify.  
[<CR>=return to main menu]:

Main Menu  
Server Configuration Settings:  
(A) Overall Settings  
(B) IP Address  
(C) Memory Settings  
(D) Port Settings  
(E) Data Storage Capacity Settings  
(F) Online Fault Management Settings  
(G) Advanced Configuration

## (H) NorthStar AMQP Settings

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

## (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

Please select a number to modify.  
[<CR>=return to main menu]:

## Main Menu

## Server Configuration Settings:

(A) Overall Settings  
(B) IP Address  
(C) Memory Settings  
(D) Port Settings  
(E) Data Storage Capacity Settings  
(F) Online Fault Management Settings  
(G) Advanced Configuration  
(H) NorthStar AMQP Settings

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

## (D) Port Settings (Advanced)

11.) SNMP Trap Daemon Port.....: 162  
12.) Event Post Port.....: 7077  
13.) MariaDB Database Port.....: 3333  
10.) MongoDB Application Server Port...: 27017

Please select a number to modify.  
[<CR>=return to main menu]:

## Main Menu

## Server Configuration Settings:

(A) Overall Settings  
(B) IP Address  
(C) Memory Settings  
(D) Port Settings  
(E) Data Storage Capacity Settings  
(F) Online Fault Management Settings  
(G) Advanced Configuration  
(H) NorthStar AMQP Settings

Please select a number to modify.

[<CR>=accept, q=quit]: f

(F) Online Fault Management Settings

SNMP Trap Settings:

- 1.) SNMP Trap Daemon IP.....: 172.25.152.112
- 2.) Enable Trap Forwarder.....: OFF
- 3.) Trap Forwarding Upstream Address....:
- 4.) Trap Forwarding Upstream Port.....:

Event Settings:

- 5.) Threshold Initial Notification....: OFF

Main Menu

Server Configuration Settings:

- (A) Overall Settings
- (B) IP Address
- (C) Memory Settings
- (D) Port Settings
- (E) Data Storage Capacity Settings
- (F) Online Fault Management Settings
- (G) Advanced Configuration
- (H) NorthStar AMQP Settings

Please select a number to modify.

[<CR>=accept, q=quit]:

(A) Overall Settings

General Administrative Settings for server db1-lha :

- 1.) Installation Directory.....: /home/wandl/ipmplsview
- 2.) Data Directory.....: /home/wandl/wandldata
- 3.) Admin User.....: wandl
- 4.) Admin Group.....: wandl
- 5.) Email Server IP.....: 172.25.152.17
- 6.) Email Server User.....: wandl
- 7.) Email Server Password.....:
- 8.) Application Monitor Email Recipient....:
- 9.) Enable Server Monitoring.....: OFF
- 10.) Mapping for non-Unicode characters....:

(B) IP Address

IP/MPLSView Server IP Address Settings:

- 1.) Webserver IP.....: 172.25.152.17
- 2.) LDAP Server IP.....: 172.25.152.17
- 3.) External Webserver IP (for NAT)....:
- 4.) Mongo DB IP.....: 127.0.0.1
- 5.) Use Remote Database.....: NO

Note the web server should be changed to the shared VIP address.

(C) Memory Settings

- 1.) Task Manager Memory.....: 256
- 2.) Webserver Memory.....: 1024
- 3.) Thrift Server Memory.....: 256
- 4.) HornetQ Memory.....: 256
- 5.) DGS Memory.....: 512
- 6.) Application Monitor Memory.....: 128
- 7.) Threshold Server Memory.....: 256



```

8.) SNMP Trap Daemon Memory.....: 128
9.) MongoDB Memory.....: 512
10.) Event Server Memory.....: 256
11.) Aggregation Memory.....: 1024
12.) Selective Interface Manager Memory.....: 256
13.) Maria Database Memory.....: 256

```

Total system physical memory: 32081 MB

After starting IP/MPLSView, check "/u/wandl/bin/status\_mplsview" to see the actual memory usage, which can be used to tune the memory settings.

((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

```

(D) Port Settings (Advanced)

```

11.) SNMP Trap Daemon Port.....: 162
12.) Event Post Port.....: 7077
13.) MariaDB Database Port.....: 3333
10.) MongoDB Application Server Port...: 27017

```

(F) Online Fault Management Settings

SNMP Trap Settings:

```

1.) SNMP Trap Daemon IP.....: 172.25.152.112
2.) Enable Trap Forwarder.....: OFF
3.) Trap Forwarding Upstream Address...:
4.) Trap Forwarding Upstream Port.....:

```

Event Settings:

```

6.) Threshold Initial Notification...: OFF

```

(G) Advanced Configuration

Advanced Configuration Settings:

```

1.) Distributed Collection Servers.....:
2.) Database Temp Directory.....: /home/wandl/wandldata/mysql/tmp
3.) Email Sender Address.....:

```

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

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

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

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

You may install the Rsync & Database Replication Package by running

```
/u2/NPAT6.2.0/current.mpls/replication/instrepl.sh

no crontab for wandl

no crontab for wandl

Extracting server files (this may take some time) ..... Done!
Installing webserver ... Done!
Creating database files for installation...Done.
Analyzing database tables for upgrade...Done.
Creating database tables ... Done.
Upgrading database tables...Done.
Creating symbolic links ... Done!
Creating event repository ... Done!
Relinking files ... Done!
Installing client ... Done!
Installing data collector...

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

Data collector crontab entries added successfully.

Done!

Configuration file:'/home/wandl/ipmplsview/bin/mplsenvsetup.sh' was created on
Thu Jun 4 06:23:31 EDT 2015

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!
Configuring Task Manager native library files... Done!
Creating Selective Interface Manager configuration files ... Done!
Creating database files ... Done!
Creating MongoDB files ... Done!
Creating LDAP files ... Done!
Initializing LDAP directory ... Done!
Creating Data Collector configuration files ... Done!

You may start the client by running the following command:
/home/wandl/ipmplsview/client/ipmplsview
Remember to start the server before starting the client

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

Successfully created a symbolic link from /u/wandl to /home/wandl/ipmplsview.
Please copy your license file to /home/wandl/ipmplsview/db/sys/npatpw.

If you do not have a license file, please contact Juniper Technical Assistance
```

Center (JTAC).

After activating the software, you may start the IP/MPLSView server by running the following command:  
`/home/wandl/ipmplsview/bin/startup_mplsview`

- Related Documentation**
- [IP/MPLSView Linux OS High Availability Overview on page 103](#)
  - [Installing the Linux Operating System for IP/MPLSView High Availability on page 105](#)

## Starting, Relocating, and Stopping IP/MPLSView from the GUI or CLI

You can use either the Web browser GUI or the CLI to start IP/MPLSView as a high availability cluster service. Use the IP/MPLS View high availability GUI if you are accessing IP/MPLSView in a Web browser; use CLI commands if you are accessing IP/MPLSView by means of SSH.



**NOTE:** Before you start the application server, make sure you copy the `npapw` license file to the `/u/wandl/db/sys/` directory on both application servers.

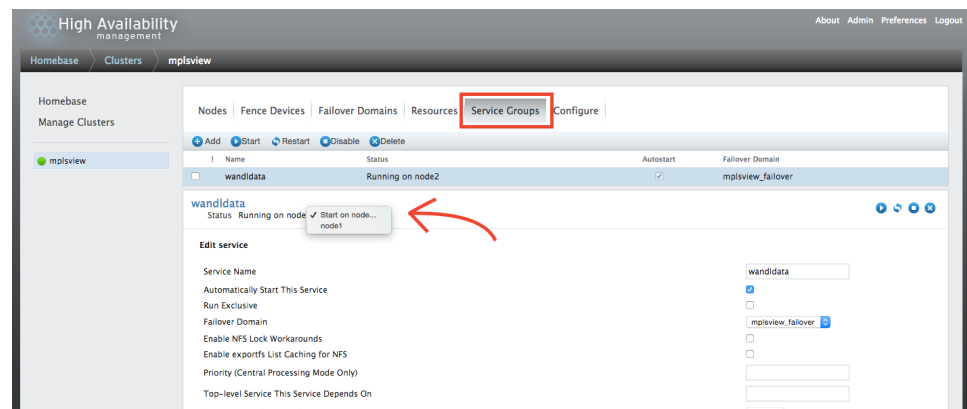
- [Starting the Application Server Using the GUI on page 131](#)
- [Starting the Application Server Using the CLI on page 132](#)
- [Relocating the Application Server Using the GUI on page 132](#)
- [Relocating the Application Server Using the CLI on page 133](#)
- [Stopping the IP/MPLSView High Availability Cluster Using the GUI on page 133](#)
- [Stopping the IP/MPLSView High Availability Cluster Using the CLI on page 134](#)

## Starting the Application Server Using the GUI

To start the IP/MPLSView application server by using the GUI:

1. Select the **Service Groups** tab.
2. Select the name of the service group to display expanded details for that group.

Figure 21: High Availability Service Groups Window



3. From the **Start on node** drop-down menu in the Status field, select the target node on which to start the application server.

If you are running the database independently from the application, you must start the database server first.

4. Click the play icon (right arrow) below the name of the selected service group to start the IP/MPLSView application server as a cluster service on the specified node.

## Starting the Application Server Using the CLI

To start the IP/MPLSView application server by using the CLI:

1. Issue the following command as the root user, where *service-group* is the name of the configured service group, and *target-node* is the name of the node on which you want to start the IP/MPLSView application server.

```
# clusvcadm -e service-group -m target-node
```

2. Verify the cluster status.

```
# /usr/sbin/clustat
# /u/wandl/bin/status_mplsview
```

## Relocating the Application Server Using the GUI

The steps for switching the IP/MPLSView application server to run on a different node are identical to the steps for starting the application server.

To relocate the IP/MPLSView application server to run on a different node by using the GUI:

1. Select the **Service Groups** tab.
2. Select the name of the service group to display expanded details for that group.

3. From the **Start on node** drop-down menu in the Status field, select the target node to which you want to relocate the application server.
4. Click the play icon (right arrow) below the name of the selected service group to relocate the IP/MPLSView application server to the specified node.

## Relocating the Application Server Using the CLI

To relocate the IP/MPLSView application server to run on a different node by using the CLI:

1. Issue the following command as the root user, where **service-group** is the name of the configured service group, and **target-node** is the name of the node on which you want to start the IP/MPLSView application server.

```
# clusvcadm -e service-group -m target-node
```

2. Verify the cluster status.

```
# /usr/sbin/clustat
# /u/wandl/bin/status_mplsview
```

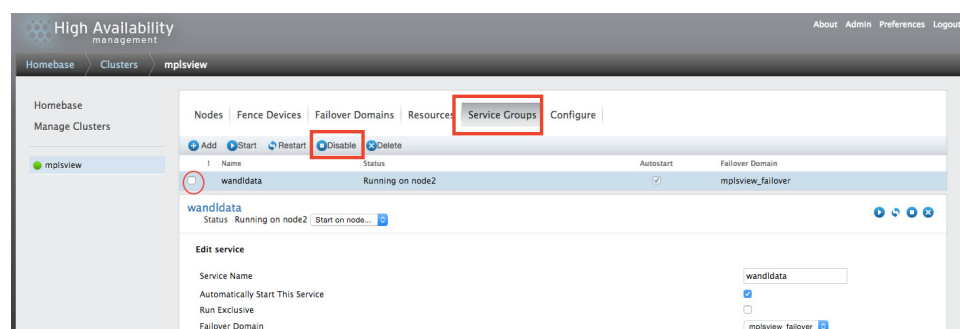
## Stopping the IP/MPLSView High Availability Cluster Using the GUI

You can use either the Web browser GUI or the CLI to stop (disable) the IP/MPLSView high availability cluster.

To stop the IP/MPLSView high availability cluster by using the GUI:

1. Select the **Service Groups** tab.

*Figure 22: High Availability Service Groups Stop Action*



2. Select the name of the service group to disable.
3. Click **Disable**.

## Stopping the IP/MPLSView High Availability Cluster Using the CLI

To stop the IP/MPLSView high availability cluster by using the CLI:

1. Issue the following command as the **root** user, where *service-group* is the name of the configured service group:

```
# clusvcadm -s service-group
```

2. Verify the cluster status.

```
# /u/wandl/bin/status_mplsview
```

The main **linux\_cluster\_mplsview.sh** script controls starting and stopping for failover and leaving cluster mode.

### Related Documentation

- [IP/MPLSView Linux OS High Availability Overview on page 103](#)
- [IP/MPLSView User Interface Frequently Asked Questions on page 173](#)

## Recording Cluster Setup Information

When you configure Linux OS high availability support for IP/MPLSView, we recommend that you use the following tables to record important details about the hardware and software components in your high availability cluster.

Having this information readily available can help you identify and troubleshoot problems, and can provide useful information if you need to contact the Juniper Networks Technical Assistance Center (JTAC) for support.

**Table 21: Server Network Record**

| Server                     | Hostname | IP Address | Cluster Node Name | Shared Node Name | Shared IP Address | NIC Name |
|----------------------------|----------|------------|-------------------|------------------|-------------------|----------|
| Primary Application Server |          |            |                   |                  |                   |          |
| Backup Application Server  |          |            |                   |                  |                   |          |
| Primary Database Server    |          |            |                   |                  |                   |          |
| Backup Database Server     |          |            |                   |                  |                   |          |

**Table 22: Server Data Record**

| Server Directory                             | Path Name | Device Name | Cluster Node Name | Size | RAID Type | Comment |
|----------------------------------------------|-----------|-------------|-------------------|------|-----------|---------|
| Primary Application Server Program Directory |           |             |                   |      |           |         |
| Backup Application Server Program Directory  |           |             |                   |      |           |         |

Table 22: Server Data Record (continued)

| Server Directory                          | Path Name | Device Name | Cluster Node Name | Size | RAID Type | Comment |
|-------------------------------------------|-----------|-------------|-------------------|------|-----------|---------|
| Primary Database Server Program Directory |           |             |                   |      |           |         |
| Backup Database Server Program Directory  |           |             |                   |      |           |         |
| Database Server Data Directory            |           |             |                   |      |           |         |

- Related Documentation**
- [IP/MPLSView Linux OS High Availability Overview on page 103](#)
  - [Installing IP/MPLSView in a Distributed Environment on page 122](#)

## Frequently Asked Questions: Cluster Administration

This section answers frequently asked questions about administering high availability clusters.

### What does quorum mean and why is it necessary?

*Quorum* is a voting algorithm used by the cluster manager.

A cluster can function correctly only if there is general agreement among the cluster members about quorum rules. A cluster has quorum if a majority of the nodes are operational, communicating, and agree on the active cluster members. For example, in a 13-node cluster, quorum is reached only if seven or more nodes are communicating. If the seventh node is no longer operational, the cluster loses quorum and can no longer function.

A cluster must maintain quorum to prevent split-brain problems. For example, if quorum rules are not enforced in the 13-node cluster and a communication error occurs, a situation might result in which six nodes are operating on the shared disk, and the other six nodes are operating independently on the shared disk. The communication error causes the two partial clusters to overwrite areas of the disk and corrupt the file system. By contrast, if quorum rules are enforced, only one of the partial clusters can use the shared storage, thus protecting data integrity.

Although quorum rules do not prevent split-brain problems, they do determine which member is dominant and allowed to function in the cluster. If split-brain problems occur, quorum prevents more than one cluster group from taking action.

### What is the minimum size of a quorum disk or partition?

The official minimum size for a quorum disk is 10 MB. The actual size is approximately 100 KB; however, we recommend reserving at least 10 MB for possible future expansion and features.

### How can I rename my cluster?

To rename your cluster:

1. Unmount all GFS partitions and stop all clustering software on all nodes in the cluster.
2. In the `/etc/cluster.conf` file, change the old cluster name to the new cluster name.
3. If you have GFS partitions in your cluster, issue the following command to change their superblock to use the new cluster name:  
  

```
# gfs_tool sb /dev/vg_name/gfs1 table new_cluster_name:gfs1
```
4. Restart the clustering software on all nodes in the cluster.
5. Remount your GFS partitions.

**If both nodes in a two-node cluster lose contact with each other, don't they try to fence each other?**

Yes. When each node recognizes that the other node has stopped responding, it tries to fence the other node. Fencing is the process of separating an unavailable or malfunctioning cluster node from the resources it manages, without the support of the node being fenced. When used in combination with a quorum disk, fencing can prevent resources from being improperly used in a high availability cluster.

The node that is the first to fence the other node “wins” and becomes dominant. However, if both nodes go down simultaneously, the entire cluster is lost.

To avoid cluster loss in a two-node cluster, you can use an Intelligent Platform Management Interface (IPMI) LAN that serializes the two fencing operations, ensuring that one node reboots and the other node never fences the first.

**Where can I get more information?**

For more information about cluster administration, see the following Red Hat Enterprise Linux 6 documentation:

- *Red Hat Enterprise Linux 6 Cluster Administration: Configuring and Managing the High Availability Add-On*  
([https://access.redhat.com/documentation/en-US/Red\\_Hat\\_Enterprise\\_Linux/6/html/Cluster\\_Administration/index.html](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Cluster_Administration/index.html))
- *Red Hat Enterprise Linux 6 6.5 Technical Notes*  
([https://access.redhat.com/documentation/en-US/Red\\_Hat\\_Enterprise\\_Linux/6/html/6.5\\_Technical\\_Notes/index.html](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/6.5_Technical_Notes/index.html))

**Related  
Documentation**

- [IP/MPLSView Linux OS High Availability Overview on page 103](#)
- [Troubleshooting IP/MPLSView Overview on page 161](#)
- [General Procedures for Troubleshooting the IP/MPLSView Installation on page 161](#)



## CHAPTER 8

# Getting Started with IP/MPLSView

- [Starting IP/MPLSView Servers on page 137](#)
- [Launching the IP/MPLSView Client on page 143](#)

### Starting IP/MPLSView Servers

---

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 Linux machine; the client software can run either on a Linux machine or PC with Microsoft Windows. This chapter explains how to start up the server and connect to it with the client.

- [Starting Up the IP/MPLSView Server on page 138](#)
- [Starting the IP/MPLSView Traffic Data Collector on page 140](#)
- [Starting the IP/MPLSView Trap Daemon from Linux on page 141](#)
- [Manually Starting the Event Server on page 142](#)
- [Manually Starting the Distributed Database in Linux on page 142](#)
- [Restarting the Task Server on page 142](#)

## Starting Up the IP/MPLSView Server

Before starting the IP/MPLSView server or client, install them. For more information, see [“Installing the IP/MPLSView Server, Client, Traffic Data Collector, and Rsync Package”](#) on page 32.

[Table 23 on page 138](#) provides a summary of the commands used to start, stop, and determine the status of IP/MPLSView servers. Do not use root to startup the IP/MPLSView servers because this might lead to ownership and process conflicts.

**Table 23: Starting, Stopping, and Verifying Status Commands**

| Command                                 | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>status_mplsview</b>                  | <p>Use 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.</p> <p>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> script.</p> <p>All errors displayed 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.</p> |
| <b>startup_mplsview<br/>port-number</b> | Use this command to start all the servers. The startup script either confirms the startup process if the IP/MPLSView servers started successfully or provides error message(s) if the start server process fails. Do not use root to startup the IP/MPLSView servers.                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>stop_mplsview</b>                    | <p>Use this command to stop all the servers.</p> <p><b>NOTE:</b> This command gives the IP/MPLSView clients a one minute notice in which to save unfinished work.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>nodejs_server.sh start</b>           | Use this command to start the IP/MPLSView servers if you are using the RESTful API through the Web-based UI. The <b>Node.js</b> process must be up for the Web UI to be accessible.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>nodejs_server.sh stop</b>            | Use this command to stop the IP/MPLSView servers if you are using the RESTful API through the Web-based UI. The <b>Node.js</b> process must be up for the Web UI to be accessible.                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

The `./nodejs_server.sh start` and `./nodejs_server.sh stop` commands start and stop the IP/MPLSView servers if you are using the Representation State Transfer (RESTful) API included in IP/MPLSView. The RESTful API enables northbound systems to receive various sets of data by means of standard HTTP requests.

The “Node” product (Node.js) receives and processes RESTful API HTTP requests on the IP/MPLSView application server. It uses a port other than the standard 8091 port used by the application. The default port for this interface is 3000.

1. Before starting IP/MPLSView, contact Juniper support to obtain an activation license file. You need the host ID of your server. To determine your host ID:

```
hostid
```

Change the license filename to **npatpw** and move it to the **/u/wandl/db/sys** folder, or the **\$WANDL\_HOME/db/sys** folder.

You can also upload the license file from the Web Interface to the application server and view it from the Web Interface. This feature is available from the Web menu by selecting **Admin > Administration > Upload License** and **Show License**.

2. Log into the server as the IP/MPLSView admin user; the wandl user ID is recommended when applicable. After you log in, change directory using the following command:

```
$ cd /u/wandl/bin
```

3. Verify that the IP/MPLSView-related servers are running using the following command.

```
./status_mplsview
```

4. If the servers are not running, start them using the following command:

```
./startup_mplsview
```

The IP/MPLSView server and Tomcat server (a web application server) should be listed in the servers that are running. 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) also takes port 7001.

5. If the default port is in use, you can start the server with another port number by using the command:

```
$ ./startup_mplsview port_number
```

In this example, substitute *port\_number* with a valid unused port number. The IP/MPLSView data collection driver port number is then set to *port\_number+1*.

6. You can optionally set up the PATH variable to access the commands located in **/u/wandl/bin** and **/u/wandl/client** folders from other directories without specifying the full path. The following variable can be placed in the **\$HOME/.profile** file.

```
PATH=/u/wandl/bin:/u/wandl/client:$PATH
export PATH
```

7. After setting the PATH variables, you can use the settings in the **.profile** file, using the following:

```
# . ./profile
```



**CAUTION:** If you choose to setup the PATH in the .profile file, remember to change the PATH when reinstalling IP/MPLSView in a different folder. Otherwise, an older version might be executed from the directory in the path instead of the version from your current directory. You can check which version you are running by using the **which** command.

---

## Starting the IP/MPLSView Traffic Data Collector

The Traffic Data Collector should be started on the server if you want to collect traffic data using the IP/MPLSView client.

To launch the Traffic Data Collector application:

1. Switch to the directory where the Traffic Data Collector is installed. For example, **/u/wandl/dcollect**, and then execute the **dc.sh** script.

```
$ cd /u/wandl/dcollect
$ ./dc.sh start instance#
```

In this example, *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 Traffic Data Collector running at once on the same server or on other servers. You should see some messages similar to the following:

```
Trying to start using pid=8608
Data Collector (pid=8608) Started.
```

2. If a Traffic 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
```

3. 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)
```

In this example, **wandl\_#** represents the instance identifier of that Traffic Data Collector and **wandl** represents the user ID that started the Traffic Data Collector.

After verifying the status of the collector, you can specify what to collect using the Traffic Collection Manager in an IP/MPLSView client. The client can be on a different machine.

4. To stop a specific Traffic Data Collector instance, use the following:

```
./dc.sh stop instance#
```

5. To stop all Traffic Data Collector instances, use the following:

```
./dc.sh stop all
```

6. If an instance is having difficulty stopping, you might force a shut down using the **-f** flag.

```
./dc.sh -f stop instance#
```

## Starting the IP/MPLSView Trap Daemon from Linux

When running the **startup\_mplsview** or **stop\_mplsview** scripts, you might be asked to stop or start the SNMP trap server. The SNMP trap server is used for the online Fault Management module.

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 start the SNMP trap daemon:

1. To launch the trap daemon, first change directory to the bin directory where IP/MPLSView is installed (for example, **/u/wandl/bin**) and then use the **.snmptrap start** command.

```
$ cd /u/wandl/bin  
$ ./snmptrap start  
SNMP trap daemon started on port 162
```

2. Before you can stop the SNMP trap daemon, first stop the application monitor if it is enabled.

```
$ ./appmonitor stop
```

If the application monitor is not stopped first, it might detect that the SNMP trap server is down, and automatically restart it.

3. Stop the SNMP trap daemon.

```
./snmptrap stop
```

## Manually Starting the Event Server

Note that the event server is automatically started up when you use the `/u/wandl/bin/startup_mplsview` command. There might be circumstances when you need to manually stop and restart the event server.

1. To manually stop and restart event server:

```
$ cd /u/wandl/bin
$ ./appmonitor stop
$ ./eventserver stop
$ ./eventserver start /u/wandl/db/config/eventserver.xml
$ ./appmonitor start
```

By default, the event server only displays application events. In order to also display SNMP trap events, start the trap daemon as explained in *Starting the IP/MPLSView Trap Daemon from Linux*.

## Manually Starting the Distributed Database in Linux

In most cases, the database is installed with the IP/MPLSView server. If so, starting up the IP/MPLSView server also starts up the database. However, if the database is installed on a different machine from IP/MPLSView, change directory to the bin directory of where the distributed database is installed. For example, `/u/wandl/bin`.

1. To start up the database:

```
$ startup_mplsview
```

2. To shut down the database:

```
$ stop_mplsview
```

## Restarting the Task Server

Under special circumstances, you might want to stop and restart the Task Server only, without taking down other processes. The application monitor should be stopped beforehand, so that it does not automatically restart the Task Manager when it detects that it is down.

1. To stop the Task Server process, use the following commands:

```
$ cd /u/wandl/bin
$ ./appmonitor stop
$ ./tmng stop
```

2. To restart the Task Server process, use the following commands:

```
$ cd /u/wandl/bin
$ ./tmng
$ ./appmonitor start
```

- Related Documentation**
- [IP/MPLSView Installation Overview on page 29](#)
  - [IP/MPLSView Server Installation Frequently Asked Questions on page 166](#)
  - [General Procedures for Troubleshooting the IP/MPLSView Installation on page 161](#)

## Launching the IP/MPLSView Client

---

This topic describes how to launch the IP/MPLSView client on Linux and on Windows.

- [Launching the IP/MPLSView Client on Linux on page 143](#)
- [Launching the IP/MPLSView Client on Microsoft Windows on page 144](#)
- [Launching IP/MPLSView Client Using Web Start \(Linux and Windows\) on page 146](#)

### Launching the IP/MPLSView Client on Linux

1. To start the Java client in Linux, enter the following commands:

```
$ cd /u/wandl/client
$ ./ipmplsview
```

The IP/MPLSView login screen is displayed.

2. To connect to a different server or to connect using a different port number, enter the following command from the **/u/wandl/client** directory:

```
$ ./ipmplsview [server_host port_number]
```

Substitute the correct **server\_host** and **port\_number**. Note that if you specify a hostname for **server\_host**, you need to edit the **/etc/hosts** file. If you specify an IP address for **server\_host**, this extra step is not necessary.

Alternatively, you can edit the **ipmplsview** file.

## Launching the IP/MPLSView Client on Microsoft Windows

1. If you want to run the Java client on a Windows PC, double-click the **IP-MPLSView Client** desktop icon. The IP/MPLSView login window is displayed. [Figure 23 on page 144](#) shows the IP/MPLSView Login window.

Figure 23: 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. Click the information *i* button to 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\wand\IP-MPLSView**). You can also open a DOS window (select **Start Menu > Run** and enter **cmd** or **command** in the Open field.). If you change directory to the directory where you installed IP/MPLSView, you can enter **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 selecting **Edit with Notepad** or other similar menu option provided by your Windows operating system. If this option is not available, you might need to navigate to the installation directory to change the file. For Windows Vista or later, you might need to right-click



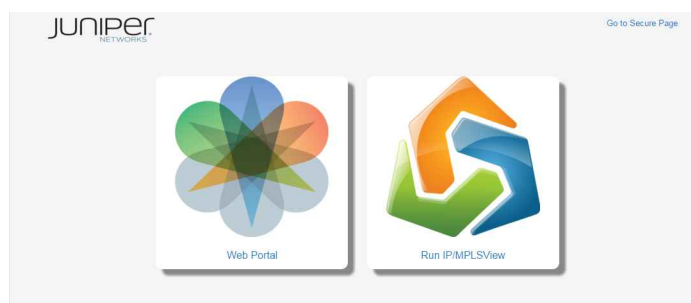
on the directory to add edit permissions for your user from the **Security** tab, **Edit** button and remove the Read-only attribute from the General tab.

## Launching IP/MPLSView Client Using Web Start (Linux and Windows)

Before launching the Web Start client, verify that Web Start has been set up. If it is not, follow the instructions described in *Installing the IP/MPLSView Client on the Local Server*. Additionally, verify that your client machine supports the same version of Java. The 6.3.0 release uses jre1.8.0\_45.

1. Launch your Web browser and log in to the IP/MPLSView website (<http://serveripaddress:8091> or <https://serveripaddress:8443>). Click **Run IP/MPLSView**. Figure 24 on page 146 shows the client access.

Figure 24: IP/MPLSView Web Interface with Web Client Access



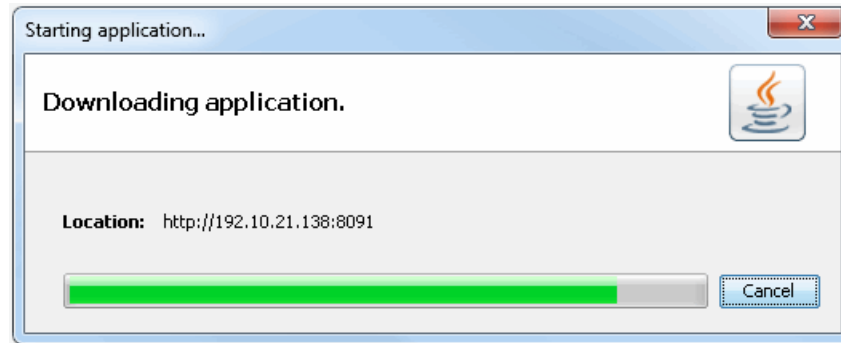
In the Figure 25 on page 146 window, you can configure several run-time parameters. An important option is how much memory the client uses.

Figure 25: Server and WebServer Selection and Client Memory Allocation



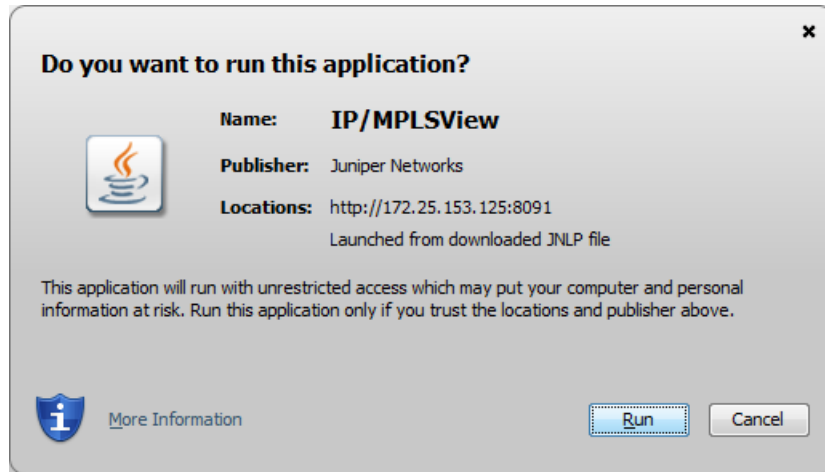
- Click **Run IP/MPLSView** and the application files are downloaded. [Figure 26 on page 147](#) shows the download window.

*Figure 26: Application Files Downloading Window*



- If you see the warning shown in [Figure 27 on page 147](#), you can ignore it. Click **Run** and the IP/MPLSView application launches. In case of problems, see [“General Procedures for Troubleshooting the IP/MPLSView Installation” on page 161](#).

*Figure 27: Web Start Warning Message*



- The default language of the client software is English. To change languages, create a file named **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 24: Language Codes*

| Code  | Language           |
|-------|--------------------|
| en_EN | English            |
| zh_CN | Simplified Chinese |

Table 24: Language Codes (continued)

| Code  | Language            |
|-------|---------------------|
| ch_TW | Traditional Chinese |
| ru_RU | Russian             |

- If there are still problems connecting, use the **ping** command to test the server to make sure you have connectivity. If you do not have connectivity, verify if 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 the **startup\_mplsview** command again.

For logins other than the administrative user, check that appropriate privileges are given through the User Admin window, or using the `/u/wandl/bin/addWandlUser.sh` script. For more information, see [“Creating Users and Groups Using the User Administration Tool” on page 154](#) and [Performing User Administration from Text Mode](#).

- When you launch the IP/MPLSView Java client, the login window is displayed. You can 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**.
- Select one of the two access privileges (that is, Full-control, View Only). Users with View Only privilege can view the reports and monitor the network (for online module), but have restricted ability for modification, simulation, and design.

The IP/MPLSView GUI starts up with the Start Page.

- To close the client, select **File > Exit**. Then select **Yes**.
- 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 **notice.txt** file to the `/u/wandl/data/custom` directory. An optional title message can be given to this pop-up window by adding a **title=title of notice** entry in the **notice.txt** file.

#### Related Documentation

- [Installing the IP/MPLSView Server, Client, Traffic Data Collector, and Rsync Package on page 32](#)
- [Additional Steps for Installing IP/MPLSView in a NAT Environment on page 44](#)
- [Installing the IP/MPLSView Client on a PC on page 49](#)

## CHAPTER 9

# System Administration

- [IP/MPLSView System Administration Overview on page 149](#)
- [Setting Up Port Forwarding for Secure Communications on page 150](#)
- [Launching the IP/MPLSView Web Interface on page 154](#)
- [Creating Users and Groups Using the User Administration Tool on page 154](#)
- [Setting Up an IP/MPLSView Connection to the Router Network on page 157](#)

### IP/MPLSView System Administration Overview

---

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 *IP/MPLSView Java-based Graphical User Interface Reference* for information on the more advanced tasks.

### Backing Up the Data Directories

Use the `/u/wandl/util/backup_data.sh` script to create a mapping file that lists the directories you want to back up.

```
/u/wandl/util/backup_data.sh mapping-file output-directory
```

In the command example:

- The mapping-file is the name of the file containing the list of directories, such as `/u/wandl/data/device` and `/u/wandl/data/lsping`.
- The output-directory is the directory where the TAR file is saved. By default, this is the current directory.

The backup filename created has the format **wandl.yyyymmdd.tar.gz**.

#### Related Documentation

- [Creating Users and Groups Using the User Administration Tool on page 154](#)
- [Troubleshooting IP/MPLSView Overview on page 161](#)
- [General Procedures for Troubleshooting the IP/MPLSView Installation on page 161](#)
- [IP/MPLSView System Administration Frequently Asked Questions on page 173](#)

## Setting Up Port Forwarding for Secure Communications

---

Port forwarding can be used to set up SSH tunneling for communications between the client and the server or 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

To enable port forwarding on the server:

1. Log in using telnet or SSH to the IP/MPLSView server machine or firewall/gateway.
2. As the root user, edit the `/etc/ssh/sshd_config` file 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. Use the **service sshd restart** command to refresh the service with the new configuration information.
3. If you are connecting to the IP/MPLSView server using a gateway, make sure that the server and gateway can ping each other. If not, set up a route between them (for example, using the **route add** command). For help on using the **route add** command, see ["Setting Up an IP/MPLSView Connection to the Router Network" on page 157](#).

## Setting Up a Windows Client to Work With Port Forwarding

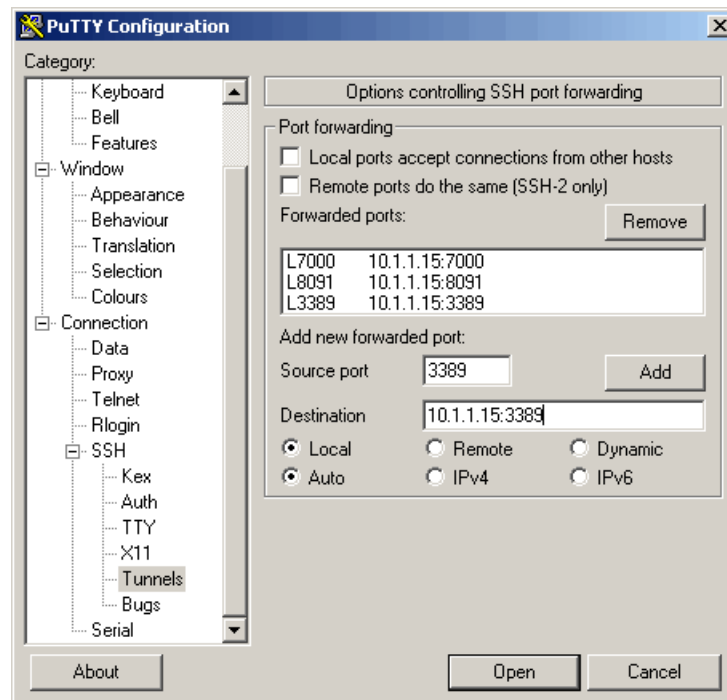
Setting up port forwarding, requires the use of an SSH client with the ability to create SSH tunnels. Additionally, port forwarding capability should be turned on for the SSH server. PuTTY is a free SSH client, which can be downloaded from the Internet, with this capability, and is used in the example below.



**NOTE:** The Traffic Collection Manager and Event Browser are special cases that 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.

1. Open an SSH client that supports port forwarding. This example uses PuTTY.
2. In the left pane, select **Connections > SSH > Tunnels**.

*Figure 28: SSH Tunneling Options for the IP/MPLSView Server*

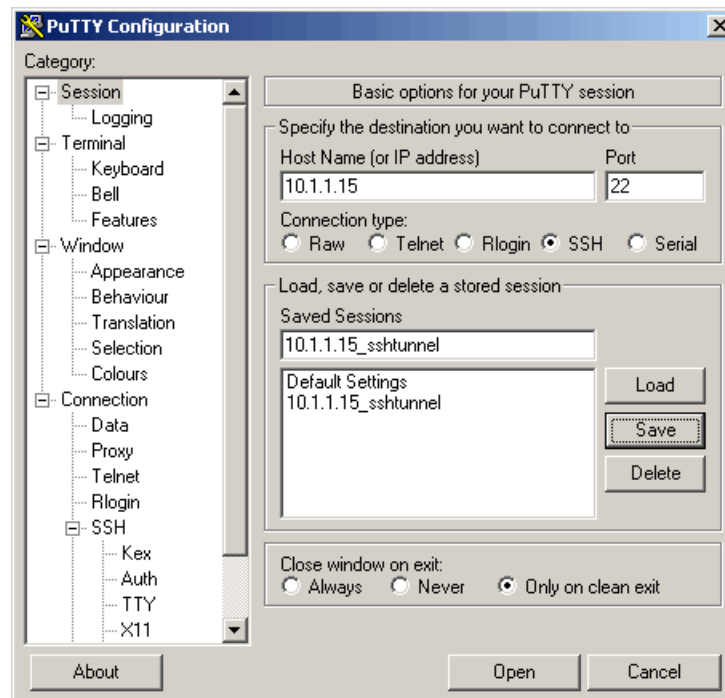


3. For use of the software in offline mode, add the following *Source* ports and map them to the corresponding remote IP address and remote port on the IP/MPLSView server. Even if you are connecting to a gateway or firewall, the SSH tunnel destination should be the IP/MPLSView server.

- 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 and MariaDB 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
5. Scroll up in the left pane and select **Session**. Enter the hostname or public IP 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 [“Setting Up Port Forwarding for Secure Communications” on page 150](#)). If the port value is not 22, the appropriate mapping for the SSH port should also be indicated in the SSH Tunnel options.

*Figure 29: Saving Session Information*



6. Enter in a name for the session and click **Save**.



7. Click **Open** to start the PuTTY session, enter the login credentials, and keep the PuTTY session open when using the client.
8. If you are setting up the SSH tunnel to a gateway instead of to the IP/MPLSView server, there might 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):

```
ssh -f -N -L 8091:serverIP:8091 -L 7000:serverIP:7000 -L 3389:serverIP:3389
-L 2099:serverIP:2099 -L 2 100:serverIP -L 1856:serverIP:1856 -L
4457:serverIP:4457 -L 4458:serverIP:4458 -L 4459:serverIP:4459 username@serverIP
```

Substitute the **serverIP** and **username** variables with the IP address of the IP/MPLSView server and the login user.

Now you can log in to the IP/MPLSView server Web interface securely using:  
**http://localhost:8091** or **http://127.0.0.1:8091**

To login using the Java client directly, first edit the **ipmplsview.bat** file to change the server IP address to 127.0.0.1.

### Troubleshooting Port Forwarding

- 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 might 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 33389 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 might also be causing a problem. Try logging in to the server and running **netstat -na | grep 8091** from one telnet or ssh session. Then telnet to the server using the same port, for example, **telnet <server> 8091** and quickly rerun the **netstat -na | grep 8091** command from the previous window to see if any new connection is listed as ESTABLISHED. If not, you might want to check your PC firewall settings by selecting **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.

### Setting Up a Linux Client to Work With Port Forwarding

To run the client on a separate Linux or MAC system, the SSH tunnels can be set up at the command prompt (add more ports as required):

```
ssh -f -N -L 8091:localhost:8091 -L 7000:localhost:7000 -L 3389:localhost:3389  
-L 2099:localhost:2099 -L 2100:localhost -L 1856:localhost:1856 -L  
4457:localhost:4457 -L 4458:localhost:4458 -L 4459:localhost:4459  
<user>@<server_ip> ...
```

Additional ports to forward can be added similarly by using the `-L` flag. For more information, see *Setting Up a Windows Client to Work With Port Forwarding*.

**Related  
Documentation**

- [Required Ports to Open in Firewalls on page 21](#)
- [Installing the Rsync Package and Automating SSH Login on page 74](#)

---

## Launching the IP/MPLSView Web Interface

To launch the Web interface:

1. Launch the IP/MPLSView Web interface using 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 the URL `https://<ip-addr>:8443` instead. If navigation is blocked due to a 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 Linux server. Administrators have access to administrative functions in the Admin menu.
  - To change passwords, use the **passwd** command on the server.
  - To add, remove, or update Web users, manage these user through the IP/MPLSView User Administration tool.
  - To help troubleshoot server application-related issues, various log files are created under the `/u/wandl/log` directory and are accessible from the Web by selecting **Admin > View > Logs**. Select 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 *IP/MPLSView Web-based Graphical User Interface Reference* for more information.

**Related  
Documentation**

- [IP/MPLSView System Administration Overview on page 149](#)

---

## Creating Users and Groups Using the User Administration Tool

The User Administration tool allows you to create 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**. The **User Administration Tool** is displayed.

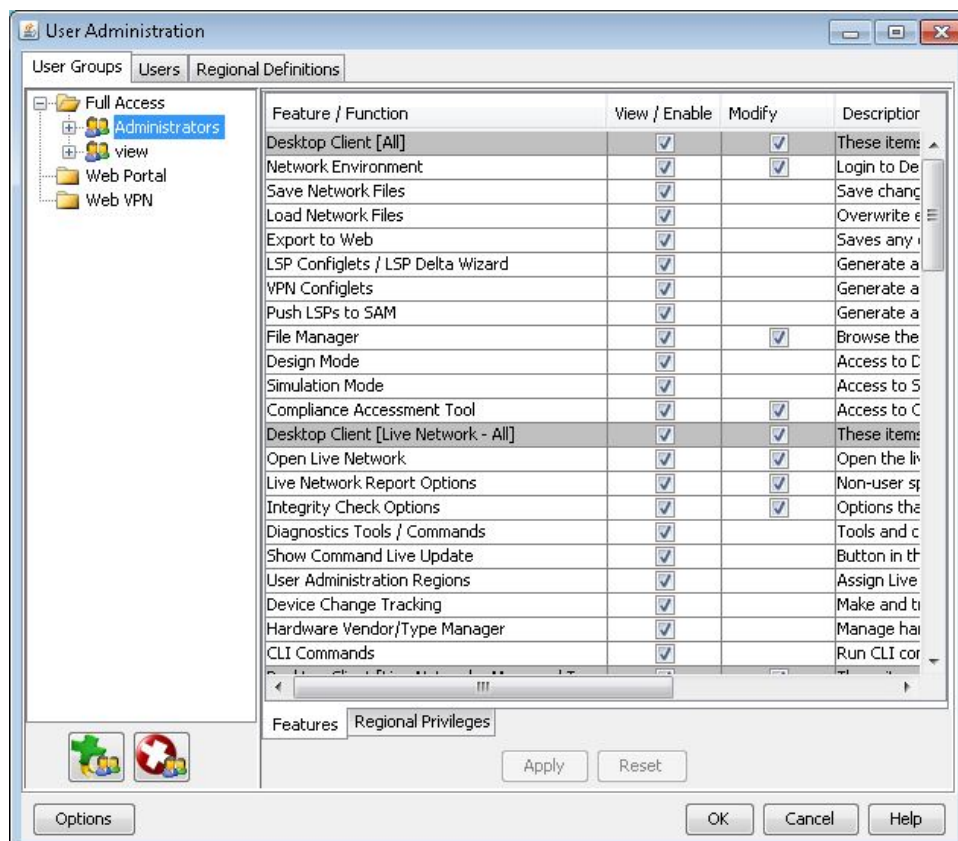
The command line interface can also be used to add users into existing user groups.

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 a Linux login).
- Web VPN (for Web-only users who can only view particular VPN customer(s)).

Full access users who are given Web access are able to log in to the Web portal using their Linux ID and password.

*Figure 30: User Administration User Groups Tab*



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, select the privileges that you want to give the group. Note that selecting a row colored gray toggles 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 is provided, and features such as ping, traceroute, show config, and hardware inventory are disabled.

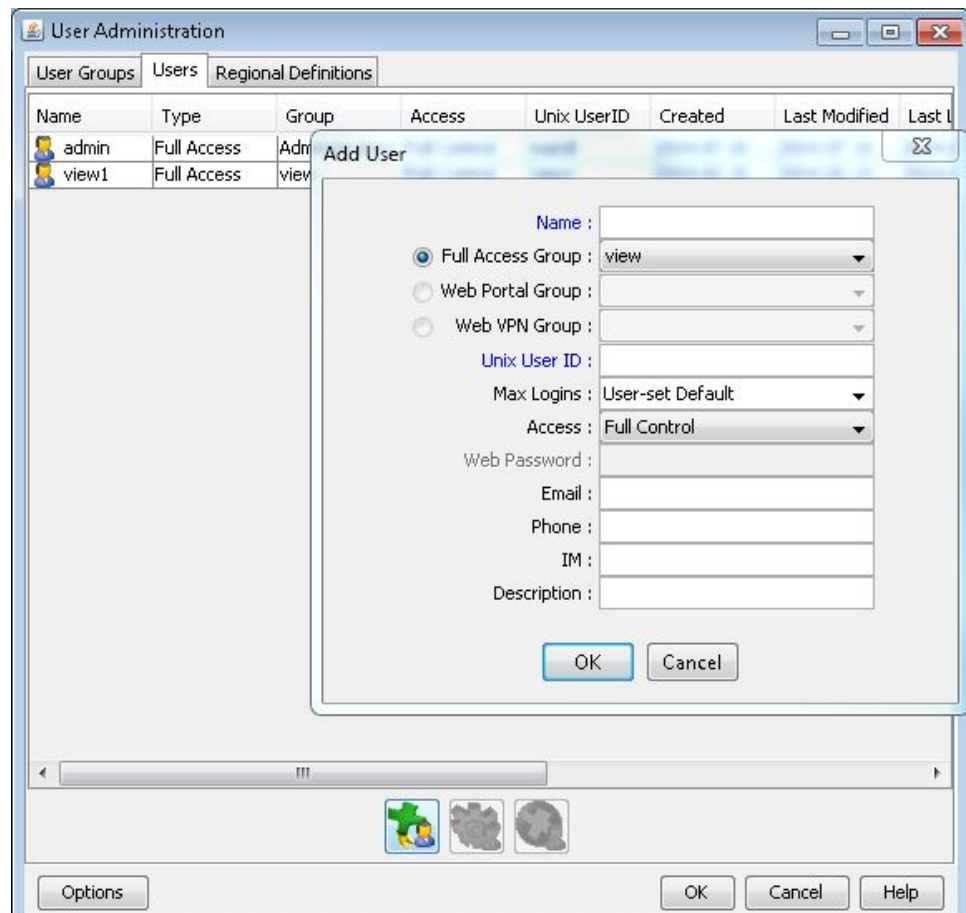
First create the regions in the top Regions tab. Next, select the **User Groups** tab, and in the right pane, select the bottom Regions tab. De-select **All Regions**, and then select the region(s) that can be accessed.

### 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 must first schedule and run a live network task.

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).

Figure 31: User Administration Users Tab



When specifying the user details, you must either map the user to a pre-existing system User ID (for Full Access users), which can be created as described in ["Installing the](#)

IP/MPLSView Server, Client, Traffic Data Collector, and Rsync Package” on page 32, or enter a Web password (for Web Portal and Web VPN users). Make sure a password is also created for the system User ID for Full Access users. If it has not been set, the root user can change the password using the **passwd userid** command and substituting *userid* with the system User ID. The login to the Web is then the name and the password is the password set for the system user ID.

In addition to using the GUI interface to perform user administration, you can also add users from text mode using the following:

```
/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 linuxloginname => linux 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 **/u/wandl/data/usr.usercount** file, with one line per user to control. The last line is the default maximum number of logins. For example, to configure a maximum of three wandl users, and a maximum of one other user, enter the following:

```
wandl 3
1
```

For more details, refer to the *IP/MPLSView Java-Based Management and Monitoring Guide*.

#### Related Documentation

- [Setting Up Port Forwarding for Secure Communications on page 150](#)
- [Launching the IP/MPLSView Web Interface on page 154](#)

## Setting Up an IP/MPLSView 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.

This procedure can be used to verify, add, and remove routes to the router network. 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 the ping is successful, you are already connected. Otherwise proceed with the following steps:

Open a console window and switch to super user by using the **su** command if you are not already user ID *root*.

1. To check what routes are listed in the current routing table, use the following command:

```
# /bin/netstat -rn
```

2. To add a route to a network through a gateway, use the **route add** command.

For example:

```
ip route add router-network-address via gateway-address dev interface
```

Substitute the router-network-address and the gateway-address with the proper values:

```
# /usr/sbin/ip route add X.X.X.X/X via X.X.X.X dev interface
```

In this example, **X.X.X.X/X** is the network number and netmask for the static route and **X.X.X.X** and **interface** are the IP address and interface for the default gateway.

The **X.X.X.X** address does not have to be the default gateway IP address. In most cases, **X.X.X.X** is an IP address in a different subnet, and **interface** is the interface that is connected to, or can reach, that subnet.

For example, if 172.16.0.0 is the router network subnet and 192.168.34.22 is the gateway to the router network, enter the following command:

```
# /usr/sbin/ip route add 172.16.0.0 via 192.168.34.22 dev eth0
```

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 is not used. To remove a preexisting route:

```
# /usr/sbin/route delete router-network-IP-address gateway-to-router-ntwk-IP
```

4. To remove all the current routes before installing new ones:

```
# /usr/sbin/route flush
```

5. To make the routes persistent so that they are still available after rebooting the system, use the **route -p** command (if the **-p** option is available). This adds routes to the **/etc/inet/static\_routes** file. For example:

```
# 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 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. If it is not, use the **chmod +x filename** command and execute 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.

6. To set up a default route, enter the following command:

```
# /usr/sbin/route add default gateway-to-router-network-IP
```

In this example, substitute *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 **/etc/defaultrouter** file with the IP address of the gateway.

For additional information, read the reference manual pages for the **defaultrouter** and **route** commands.

This procedure can be used to troubleshoot the connection to the router network. If the server has an interface card, verify that the interface card is full duplex rather than half duplex. To verify the duplex:

1. Find the names of the interfaces.

```
ifconfig -a
```

The command returns the name of the interfaces. For example, **nge0**.

2. Use the **nnd** command to verify the duplex setting.

```
nnd /dev/nge0 link_duplex
```

The command returns 0 if the link is down, 1 if it is half duplex, and 2 if it is full duplex. If the command returns 1, read your hardware manual for instructions on how to configure the interface to be full duplex.

3. If the server has more than one interface card, the server might be acting as a router, which might cause connectivity problems. In this case, create the **/etc/notrouter** file as the root user using the following command:

```
# /usr/bin/touch /etc/notrouter
```

4. If ping and traceroute still do not work, verify that there is no firewall between the IP/MPLSView server and the router network.
5. If the routers cannot be reached directly due to a firewall, use a Remote Collection Server.

- Related Documentation**
- [IP/MPLSView System Administration Overview on page 149](#)



## CHAPTER 10

# Troubleshooting the IP/MPLSView Installation

- [Troubleshooting IP/MPLSView Overview on page 161](#)
- [General Procedures for Troubleshooting the IP/MPLSView Installation on page 161](#)
- [Running Advanced IP/MPLSView System Diagnostics Scripts on page 165](#)
- [IP/MPLSView Server Installation Frequently Asked Questions on page 166](#)
- [IP/MPLSView Client Installation Frequently Asked Questions on page 169](#)
- [IP/MPLSView Java Web Start Frequently Asked Questions on page 172](#)
- [IP/MPLSView System Administration Frequently Asked Questions on page 173](#)
- [IP/MPLSView User Interface Frequently Asked Questions on page 173](#)
- [Troubleshooting IP/MPLSView Database Synchronization on page 175](#)

### Troubleshooting IP/MPLSView Overview

---

The *Troubleshooting the IP/MPLSView Installation* chapter addresses problems related to installation, system administration, and the user interface. If your question is not answered here, read the troubleshooting sections of the *IP/MPLSView Java-Based Management and Monitoring Guide* or contact Juniper support.

When you contact Juniper support, please provide the build date of the server. The server build date can be found on the server by issuing the `/u/wandl/bin/bbdsgrn -v` command.

### General Procedures for Troubleshooting the IP/MPLSView Installation

---

This topic outlines general procedures for troubleshooting issues with IP/MPLSView, such as unexpected behavior, hanging, Java exceptions, or error messages. The first step is to check the status of the application server. The second step is to identify any conflicting, missing, or lingering processes. The third step is to gracefully shut down and restart those problematic processes. Specific troubleshooting questions are answered in other topics in the *Troubleshooting the IP/MPLSView Installation* chapter.

## Checking the Status of the Application Server

- Log in to the application server as the wandl user, or as the administrative user that installed IP/MPLSView, and change directory to `/u/wandl/bin`. Use the `./status_mplsview` command 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
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: 172.17.7.7 Process ID: 13157 User wandl
Wed Sep 08 14:22:20 2010 IP: 172.18.8.8 Process ID: 21996 User tester
```

This command displays various processes used by the IP/MPLSView. Note some of your processes might be different from the 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.

## Identifying Processes to Fix

- Using the `./status_mplsview` command in combination with the Linux `ps` command can help identify the processes to fix.
- Use the `ps -ef | grep java` command to report all the Java processes used by IP/MPLSView. The Java processes reported should be the same as the pid's detected using the `./status_mplsview` command. If there are duplicate or missing Java processes reported by the `ps` command, then this could lead to conflicts.

3. Use the **ps -ef | grep wandl** command 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 the **./status\_mplsview** command. If there are duplicate or missing wandl processes reported by the **ps** command, then this could lead to conflicts.
4. Use the **ps -ef | grep <user>** command, where **<user>** is the user detected by the **./status\_mplsview** command, to report user processes used by IP/MPLSView. Verify the user is not running lingering or outdated processes.

The LDAP pid can be verified using the **ps -ef | grep ldap** command.

5. The following is an example **ps -ef | grep java** command output of when the application server is running properly:

```
# ps -ef | grep java
```

```
root 25995 25991 0 00:43:01 ? 0:09 /usr/jdk/latest/bin/java
-version:1.5+ -jar /usr/lib/patch/swupa.jar -autoAnaly
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
/home/wandl/ipmplsview/java/bin/java -Dprogram.name=appmonitor -Xmx128M -D
wandl 22032 1 0 16:44:59 ? 0:36
/home/wandl/ipmplsview/java/bin/java -Dprogram.name=DGS -Xmx256M -cp /u/wa
wandl 22007 1 0 16:44:46 ? 1:00
/home/wandl/ipmplsview/java/bin/java -Dprogram.name=eventserver -Xmx256M -
wandl 21956 1 0 16:44:20 ? 2:03
/home/wandl/ipmplsview/java/bin/java -Dprogram.name=HornetQjms.sh -server -X
wandl 21992 1 1 16:44:41 ? 16:21 /u/wandl/java/bin/java -Xmx5
12M -server -Djava.security.policy=taskserver.polic
wandl 13686 1 0 12:25:42 pts/3 0:09
/home/wandl/ipmplsview/java/bin/java -Dprogram.name=threshold -Xmx256M -Dj
root 26035 26026 49 00:43:02 ? 16:37:00 /usr/jdk/latest/bin/java
-version:1.5+ -Djava.library.path=/usr/lib/cc-ccr/lib
root 22083 1 0 16:45:11 pts/3 0:53
/home/wandl/ipmplsview/java/bin/java -Djava.util.logging.config.file=/u/wa
wandl 21975 1 0 16:44:31 ? 6:27
/home/wandl/ipmplsview/java/bin/java -Dprogram.name=webserver.sh -server -
```

## Restarting the Application Server

1. Once the problematic processes are identified, some processes can be stopped and started individually although we recommend that you 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 are closed automatically when the **stop\_mplsview** command is used.

Change directory to the **/u/wandl/bin** directory and execute the **./stop\_mplsview** command. This command attempts a graceful shutdown of the **npatservice**, **rtserver**, and **filemanager** processes and processes used by IP/MPLSView. Open clients 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 the **stop\_mplsview** command

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 Web server(pid=21975) ...
Shutdown MySQL(pid=21933) ...
Shutdown NPAT Server(pid=21896) on port 7000 ...
```

2. Execute the **ps -ef | grep java** command and **ps -ef | grep wandl** command to verify there are no lingering Java and wandl processes related to IP/MPLSView. If there are processes still running, use the Linux **kill** command to force a shutdown. If lingering processes cannot be shut down, then the server should be rebooted as the last option.

The following is an example **ps -ef | grep java** command of when the application server is shut down properly with no lingering processes:

#### # ps -ef | grep java

```
root 25995 25991 0 Sep 08 ? 0:20 /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, use the **./startup\_mplsview** command as the wandl user to restart the application server. After the **startup\_mplsview** command completes the startup messages, wait at least 3 minutes to allow processes to start. Use the **./status\_mplsview** command 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.

## Restarting Individual Processes

The following table lists the commands to stop and start individual processes. This should be done as the `wandl` user or the user that installed IP/MPLSView, in the `/u/wandl/bin` directory. Do not run these commands as root because this might lead to ownership and process conflicts. Some commands are hidden in the directory and can be viewed with `ls -a` command. Note that if Application Monitor is running, it automatically restarts 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.

| Process             | Effectuated Function | Command                                            |
|---------------------|----------------------|----------------------------------------------------|
| Application Monitor | System Monitor       | <code>./appmonitor start or stop</code>            |
| Event Server        | Event Browser        | <code>./eventserver start or stop</code>           |
| Threshold Server    | Threshold Editor     | <code>./threshold start or stop</code>             |
| LDAP Server         | User Authentication  | <code>./ldap start or stop</code>                  |
| SNMP Trap Server    | Event Browser        | <code>./snmptrap start or stop</code>              |
| Task Server         | Task Manager         | <code>./tmng start or stop</code>                  |
| DGS                 | Traffic Collection   | <code>./dgs start or stop</code>                   |
| MariaDB             | MariaDB Database     | <code>./mysql start or stop</code>                 |
| Webserver           | Web                  | <code>./webserver.sh</code>                        |
| Application Server  | All                  | <code>./startup_mplsview or ./stop_mplsview</code> |

- Related Documentation**
- [Troubleshooting IP/MPLSView Overview on page 161](#)
  - [IP/MPLSView Installation Overview on page 29](#)

## Running Advanced IP/MPLSView System Diagnostics Scripts

For advance troubleshooting with the Juniper support team, the following diagnostic scripts in the `/u/wandl/bin` directory can be executed:

- The **system-diagnostic.sh** script gathers information, messages, hardware and software configurations, Java heap and thread dumps, and system information related to IP/MPLSView. Then it zip-compresses the text output into the local user's home directory as **support-yyymmdd.zip**. This script should be executed before restarting any services or processes so the current state of the server can be captured.

- The **hornetq-debug.sh** script generates console output similar to the **system-diagnostic.sh** script and shows information about the active event browser, Traffic Data Collector, and JMS server. This script gathers counts from the server management and should not be executed too frequently because this might cause conflicts with the JMS server. If this script is executed repeatedly as part of custom monitoring, the recommended collection interval is every 30 minutes.

**Related  
Documentation**

- [Troubleshooting IP/MPLSView Overview on page 161](#)
- [General Procedures for Troubleshooting the IP/MPLSView Installation on page 161](#)

---

## IP/MPLSView Server Installation Frequently Asked Questions

---

### I am getting errors during installation related to the SSL Certificate.

The error message might look like the following

```
# ./status_mplsview
NPAT Server (pid=21896) detected on port 7000
MySQL detected on port 3333, pid=21933
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: 172.17.7.7 Process ID: 13157 User wandl
Wed Sep 08 14:22:20 2010 IP: 172.18.8.8 Process ID: 21996 User tester
```

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 commands are necessary for the installation program to work. These error messages might appear if only the core operating system is installed and default 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 verify whether you have the correct installation of the IP/MPLSView password file:

1. Change directory to the `/u/wandl/db/sys` directory:

```
cd /u/wandl/db/sys
```

2. View the contents of the `npatpw` file and verify 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 might free up the port. Then you can use the `startup_mplsview` command. Otherwise, try using the following command:

```
$ /u/wandl/bin/startup_mplsview [port_number]
```

To find which ports are in use, you can use the `/usr/bin/netstat -a` command 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 use the `/u/wandl/bin/status_mplsview` command. This gives you a port number. Use the `/u/wandl/bin/startup_mplsview port_number` command to change the port number, substituting `port_number` with an unused unreserved port number. To see a list of used port numbers, use the `/usr/bin/netstat -a` command 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
./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 the `/u/wandl/log/dgs.log.0` directory and the `dgs.msg` file. If the `dgs.msg` file displays: **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, use the following commands (note that 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 using 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 might have been corrupted. To fix this problem use 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 might take a while to fully deploy. Wait a few minutes and check again.

**I cannot view the online help or wWeb interface.**

Verify status using the `/u/wandl/bin/status_mplsview` command. If you just started up the server, wait another 5 minutes, as the Web server takes time to initialize. Then rerun the `/u/wandl/bin/status_mplsview` command. If you see the **Web server ERROR: Unable to connect to web server!** error message, change directory to the `/u/wandl/bin` directory and use 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 this case, you can try the using the `ps -ef | grep mysql`, `ps -ef | grep securit`, `ps -ef | grep java`, and `ps -ef | grep server` commands. To ensure the listed processes, if any, are from IP/MPLSView, check the path listed and see if it includes a directory in which IP/MPLSView is installed. If so, then use the `kill -9 pid1 pid2...` command, substituting `pid1 pid2...` with the process IDs found in the previous two commands. You might 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, be sure to stop any old IP/MPLSView programs that might be running on the same system using the `/u/wandl/bin/stop_mplsview` command.

**I changed my machine’s IP address and can no longer access the Web.**

Use the `/u/wandl/bin/changeconfig.sh` script 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 the **stop\_mplsview** and **startup\_mplsview** commands.

I am getting the MySQL Installation Error “Creating database tables ...Error: installation of mysql failed. Please check the log for details: \$WANDL\_HOME/log/instmysql.log”.

Perform the following steps:

1. Stop IP/MPLSView using the **/u/wandl/bin/stop\_mplsview** command.
2. Use the **ps -ef|grep mysql** command and then kill any stray mysql processes using the **kill -TERM <pid>** or **kill -9 <pid>** command, substituting **<pid>** with the process IDs returned by the **ps** command.

3. Change directories.

```
cd /u/wandl/bin
```

4. Use the setup script. (Note the space after the dot: **.<space>./mplsenvsetup.sh**.)

```
./mplsenvsetup.sh
```

5. Enter the exact command as follows in a single line:

```
./mysql_install_db --defaults-file=$WANDL_HOME/db/config/my.cnf
--basedir=$WANDL_HOME/thirdparty/mysql --ldata=$WANDL_HOME/data/mysql/data >>
$WANDL_HOME/log/instmysql.log 2>&1
```

6. Kill any processes that persist.

```
ps -ef|grep mysql
kill -TERM <pid>
```

7. Start MPLSView again.

```
/u/wandl/bin/startup_mplsview
```



**NOTE:** Use the **/u/wandl/bin/fixmysql.sh** script to repair tables in the case of a shutdown that happened without using the **stop\_mplsview** command, for example due to a power failure.

#### Related Documentation

- [Troubleshooting IP/MPLSView Overview on page 161](#)
- [General Procedures for Troubleshooting the IP/MPLSView Installation on page 161](#)

## IP/MPLSView Client Installation Frequently Asked Questions

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 reinstall the client.

**I am unable to start the PC client and get the following message: “Out of environment space”.**

This issue arises 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 server.**

This could be due to a firewall. To check if there is a firewall, do the following:

1. Log into the server machine and check to see if the chosen port is open and listening by using the **netstat -a |grep 7000** command. (7000 is the default IP/MPLSView server port). If the port is listening, go to Step 2.
2. Use the **telnet IP\_address 7000** command with the appropriate substitution for *IP\_address*. Wait to see the response. If you have access to the port, you might see a message like **Escape character is '^['**. The cursor stays and the session does not time out. In this case, it might not be a firewall problem. However, 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. See “[Required Ports to Open in Firewalls](#)” on page 21.

If there is a firewall, and you do not require online modules, you might want to try SSH tunneling, as described in “[Installing the Rsync Package and Automating SSH Login](#)” on page 74. For NAT situations, see “[Additional Steps for Installing IP/MPLSView in a NAT Environment](#)” on page 44.

**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:

1. Log in to the server machine and check to see if the chosen port is open and listening. (7000 is the default IP/MPLSView server port).

```
netstat -a |grep 7000
```

2. To disable the firewall on Centos 6.x use the following commands:

```
service iptables stop
service ip6tables stop
chkconfig iptables off
chkconfig ip6tables off
vi /etc/sysconfig/selinux
```

3. Change the **selinux=enforcing** entry to **selinux=disabled**.
4. 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 is controlled by the Advanced User Admin tool, and each Linux account other than *wandl* must be authorized separately. For more information, see [“Creating Users and Groups Using the User Administration Tool” on page 154](#).

**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, use the `/u/wandl/bin/status_mplsview` command or read the `/u/wandl/log/tmng.log.0` file.

If this does not help, you might want to try stopping and restarting the Task Manager using the `/u/wandl/bin/tmng stop` command. After that is done, use the `/u/wandl/bin/tmng` command to restart the Task Manager. Verify that the process ID for the TMNG process in the `/u/wandl/tmp/pids` file is correct by using the `ps -fp <pid>` command, substituting `<pid>` with the process ID.

Verify that the 2099 and 2100 ports are opened between the client and server, as indicated in [“Required Ports to Open in Firewalls” on page 21](#).

**After a couple of minutes of use, the client always becomes unresponsive or hangs.**

This might be due to a firewall closing idle connections. You can specify a shorter keepalive message interval (for example, 60 seconds) by selecting **Application > Keep-Alive Message**.

**How do I increase the memory that Java can use on my PC client?**

Edit the `ipmplsview.bat` batch file 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 might be slowed down significantly.

**I could not invoke the browser for the Help manual on the operating system.**

On the operating system, you might 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`, use the following command:

```
PATH=/usr/dt/bin:$PATH; export PATH
```

To permanently set the PATH variable, create or edit the **.profile** file in your Linux user's administrative home directory.

- Related Documentation**
- [General Procedures for Troubleshooting the IP/MPLSView Installation on page 161](#)
  - [Installing the IP/MPLSView Client on a PC on page 49](#)

---

## IP/MPLSView Java Web Start Frequently Asked Questions

---

**I am trying to launch the client via Java Web Start, but when I click the “Run IP/MPLSView” button, nothing happens.**

Pop-up blockers can interfere with this operation. Either hold down the CTRL button while clicking the **Run** button or disable your pop-up 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 (100 MB 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, select **Start > Programs > Java Web Start > Java Web Start**. Use the **javaws** command in the **/javaws** subdirectory of where the client was installed (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 **Clear Folder** to clear the applications folder. If the Current Size (in KBytes) is not reset to 0, you might 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 might mean that a copy of the client is still running.

**How do I enable my Java output console when using Java Web Start?**

You can open a Java output console window by launching Java Web Start's Application Manager. Select **File > Preferences** and click the **Advanced** tab. Select 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 might be kept, which causes problems. You can reconfigure the JRE settings by launching Java Web Start's Application Manager. Select **File > Preferences** and click the **Java** tab. An alternative solution is to uninstall Webstart and all JRE's, then reinstall Java and Webstart.

**Related Documentation** • [Troubleshooting IP/MPLSView Overview on page 161](#)

## IP/MPLSView System Administration Frequently Asked Questions

### How can I determine the build date of the version of IP/MPLSView I installed?

To determine the build date of the server, use the following command:

```
$ bin/bbdsgrn -v
```

Alternately, after you open a spec file on the Java client, select **Help > About** for this information.

### How do I create another user account?

IP/MPLSView does not create the user account for you. You have to do this manually using the **useradd** command. See [“Creating Users and Groups Using the User Administration Tool” on page 154](#).

### 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 wandl user’s administration home directory (as opposed to wandl user’s installation home directory). For example, suppose user ID wandl has the **/home/wandl** home directory, but is installed under **/space/wandl**, and **/u/wandl** is linked to **/space/wandl**. Then **WANDL\_HOME=/u/wandl**, but the IP/MPLSView Administrative home directory is **/home/wandl**.

### I cannot use the /u drive on my server to create the symbolic link to my program.

To use IP/MPLSView without the **/u/wandl** link, set the **WANDL\_HOME** variable 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. IP/MPLSView gives you a window where you can specify the print command (lp). For Windows, IP/MPLSView gives you a window in which you can choose your printer.

**Related Documentation** • [IP/MPLSView System Administration Overview on page 149](#)

## IP/MPLSView User Interface Frequently Asked Questions

### I have an input file specified in the spec file, but the program cannot find it.

Any misspelling might 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**. Verify that 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**. Unselect the Draw Mult Links as Curves check box 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 do not 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 rearranges 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 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.**

Verify the network settings of Internet Explorer by selecting **Tools > Internet Options > Connections**. If the machine is configured to use a proxy, this might cause problems because it is trying to search the proxy for the application server private address. The proxy might eventually be able to determine the local address, but this could still cause issues. Disable the proxy and allow for a direct connection.

- Related Documentation**
- [Troubleshooting IP/MPLSView Overview on page 161](#)
  - [Launching the IP/MPLSView Web Interface on page 154](#)

---

## Troubleshooting IP/MPLSView Database Synchronization

---

During the MariaDB replication process in a two-server or four-server distributed environment, the IP/MPLSView database tables can become unsynchronized between the primary application server and the backup database server. An out-of-sync condition can occur when either server is improperly shut down, or when either server is interrupted by an event such as a power outage.

- Related Documentation**
- [Replication and Rsync in Distributed Environments Overview on page 73](#)
  - [Troubleshooting Database Synchronization in a Distributed Environment on page 100](#)

