Copyright Notice

Copyright IBM Corporation 2001. All rights reserved. May only be used pursuant to a Tivoli Systems Software License Agreement, an IBM Software License Agreement, or Addendum for Tivoli Products to IBM Customer or License Agreement. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, without prior written permission of IBM Corporation. IBM Corporation grants you limited permission to make hardcopy or other reproductions of any machine-readable documentation for your own use, provided that each such reproduction shall carry the IBM Corporation copyright notice. No other rights under copyright are granted without prior written permission of IBM Corporation. The document is not intended for production and is furnished “as is” without warranty of any kind. All warranties on this document are hereby disclaimed, including the warranties of merchantability and fitness for a particular purpose.

U.S. Government Users Restricted Rights-Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corporation.

Copyright © Hewlett-Packard Company 1991, 1993. All rights reserved. Reproduced by permission. This product is based, in part, on Hewlett-Packard Company’s OpenView product.

Copyright © Dartmouth College 1992. All rights reserved. Reproduced by permission.

Trademarks

IBM, the IBM logo, Tivoli, the Tivoli logo, AIX, DB2, NetView, Nways, Tivoli Certified, Tivoli Enterprise, Tivoli Enterprise Console, Tivoli Ready, and TME are trademarks or registered trademarks of International Business Machines Corporation or Tivoli Systems Inc. in the United States, other countries, or both.

Cisco is a registered trademark of Cisco Systems, Inc. CiscoWorks software is based in part on HP OpenView under license from the Hewlett-Packard Company.

InstallShield is a registered trademark of InstallShield Corporation.

Java, JAR, and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Microsoft, Windows, Windows NT, Windows98, SQL Server, Microsoft Internet Explorer and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the United States and other countries.

Optivity is a registered trademark of Nortel Networks Limited.

UNIX is a registered trademark of The Open Group in the United States and other countries.

WinZip is a registered trademark of Nico Mak Computing, Inc.

Other company, product, and service names mentioned in this document may be trademarks or service marks of others.
Notices

References in this publication to Tivoli Systems or IBM products, programs, or services do not imply that they will be available in all countries in which Tivoli Systems or IBM operates. Any reference to these products, programs, or services is not intended to imply that only Tivoli Systems or IBM products, programs, or services can be used. Subject to valid intellectual property or other legally protectable right of Tivoli Systems or IBM, any functionally equivalent product, program, or service can be used instead of the referenced product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by Tivoli Systems or IBM, are the responsibility of the user. Tivoli Systems or IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, New York 10504-1785, U.S.A.
## Contents

**New Features and Enhancements** ................................................................. 13

- Revised NetView Tivoli Management Framework Configuration Menus (UNIX) 13
- New Server Setup Options for NetView Web Console ................................. 13
  - Server Setup Options on Windows .......................................................... 14
    - Registering Web Daemons ................................................................. 14
    - Stopping and Starting Web Daemons ................................................. 14
    - Launching Web Console Security ...................................................... 14
  - Server Setup Options on UNIX .............................................................. 14
    - Stopping and Starting Web Daemons ................................................. 14
    - Launching Web Console Security ...................................................... 15
- New and Modified Daemons ...................................................................... 15
  - webserver and snmpserver Daemons ................................................... 15
  - netviewd Daemon ................................................................................ 15
  - Interaction with Native NetView Console on Windows ...................... 16
  - Interaction with the Native NetView Console on UNIX ...................... 16
- Location Sensitive Topology ..................................................................... 17
  - Auto-placement of Routers .................................................................. 17
  - Gateway/Router Entries ..................................................................... 17
  - Syntax Extended .................................................................................. 18
- Hot Backup .............................................................................................. 18
  - Hot Backup on Windows ..................................................................... 19
  - Hot Backup on UNIX ......................................................................... 19
  - Restoring from a backed-up Database ................................................. 19
- Environment Variables ............................................................................ 20
  - NVPAUSECHECKINTERVAL ............................................................ 20
  - NVPAUSEWAITINTERVAL ............................................................. 20
  - NVPAUSEBAILINTERVAL ............................................................... 21
  - NVPAUSERESUMEINTERVAL ......................................................... 21
- Web Console MIB Loader (SNMP V1/V2) .................................................... 22
  - Unload MIB ..................................................................................... 22
  - Load MIB ....................................................................................... 22
  - Using the MIB Loader from the Command Line .................................. 23

---

*Tivoli NetView Release Notes* 5
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scopes</td>
<td>35</td>
</tr>
<tr>
<td>Creating a New Scope</td>
<td>36</td>
</tr>
<tr>
<td>Roles</td>
<td>37</td>
</tr>
<tr>
<td>Default Roles</td>
<td>38</td>
</tr>
<tr>
<td>Creating a New Role</td>
<td>38</td>
</tr>
<tr>
<td>Users</td>
<td>39</td>
</tr>
<tr>
<td>Creating a New User</td>
<td>39</td>
</tr>
<tr>
<td>Manually Restarting the Web Server</td>
<td>40</td>
</tr>
<tr>
<td>Reverting to a Previous Security Configuration</td>
<td>40</td>
</tr>
<tr>
<td>Additional Web Console Security Information</td>
<td>41</td>
</tr>
<tr>
<td>Changing a Web Server's Port</td>
<td>41</td>
</tr>
<tr>
<td>About Realms</td>
<td>41</td>
</tr>
<tr>
<td>Logging</td>
<td>42</td>
</tr>
<tr>
<td>NetView Web Application Configuration</td>
<td>44</td>
</tr>
<tr>
<td>Web Console</td>
<td>44</td>
</tr>
<tr>
<td>Starting the Web Console</td>
<td>45</td>
</tr>
<tr>
<td>Logging on to the Web Console</td>
<td>46</td>
</tr>
<tr>
<td>New Icons</td>
<td>46</td>
</tr>
<tr>
<td>Table View Filtering and Sorting</td>
<td>46</td>
</tr>
<tr>
<td>Main Menu Changes</td>
<td>47</td>
</tr>
<tr>
<td>Using the Help Menu</td>
<td>48</td>
</tr>
<tr>
<td>Right-clicking on Network Objects</td>
<td>48</td>
</tr>
<tr>
<td>Web Server Communication Status Light</td>
<td>49</td>
</tr>
<tr>
<td>Context Sensitivity in Diagnostics and Object Properties</td>
<td>50</td>
</tr>
<tr>
<td>Submap Explorer</td>
<td>50</td>
</tr>
<tr>
<td>New Object Holding Area</td>
<td>50</td>
</tr>
<tr>
<td>Time and Date</td>
<td>50</td>
</tr>
<tr>
<td>ISDN Dormant Status Display</td>
<td>51</td>
</tr>
<tr>
<td>Manage/Unmanage — Acknowledge/Unacknowledge</td>
<td>51</td>
</tr>
<tr>
<td>New View Columns</td>
<td>51</td>
</tr>
<tr>
<td>Show in</td>
<td>51</td>
</tr>
<tr>
<td>Find</td>
<td>51</td>
</tr>
<tr>
<td>Find</td>
<td>52</td>
</tr>
</tbody>
</table>
Other nvsniffer for Windows Changes ................................................................. 61
nvsniffer for UNIX ................................................................................................ 62
New Varbind on Some NetView Enterprise Traps ................................................. 64
New OVw Field Network Address for Network Object ........................................ 64
Additional netviewd Information for UNIX .......................................................... 64
  SmartSet Behavior ........................................................................................... 64
  Application Startup Behavior .......................................................................... 64
  Multiple Maps with netviewd ......................................................................... 65
  Example: ....................................................................................................... 65
Additional NetView Information .............................................................................. 65
Deprecated Components ........................................................................................... 68
  On UNIX ....................................................................................................... 68
  On Windows ................................................................................................. 68
  On UNIX and Windows .................................................................................... 68
CiscoWorks 2000 Integration .................................................................................... 68
Tivoli Business System Manager Adapter V1.1 ...................................................... 69
Installing the NetView Program on Windows ..................................................... 70
  Installation and System Requirements .............................................................. 71
    Hardware Requirements .................................................................................. 71
    Software Requirements .................................................................................. 72
    Browser Requirements .................................................................................... 72
  Before Installing the Tivoli NetView Program .................................................... 72
  Installing the NetView Program ........................................................................ 73
    Installing the NetView Server or Standalone .................................................. 73
    Installing the NetView Client .......................................................................... 75
    IBM License Agreement .................................................................................. 76
  Migrating from a Previous Version of the NetView Program ............................... 76
  The Installation Process ..................................................................................... 77
Creating NetView Accounts on the Server ............................................................ 78
  Manually Creating the NetView Account on the Server .................................... 79
SQL Databases ...................................................................................................... 79
  Updating ODBC Components and Access Drivers .......................................... 79
Microsoft SQL Server ............................................................................................. 79
SQL Server Licenses .............................................................................................80
SQL Server Configuration ...................................................................................80
Installation Problems ........................................................................................80
Installing the NetView Program on UNIX ...........................................................82
Installation and System Requirements ...............................................................83
Hardware Requirements ....................................................................................83
Software Requirements .....................................................................................84
Disk Space Requirements in /usr/OV .................................................................85
Additional Requirements ...................................................................................86
Browser Requirements ......................................................................................88
TCP/IP Connection Requirements .....................................................................88
About the Tivoli NetView Software Components .............................................90
Tivoli NetView Server .......................................................................................90
Tivoli NetView Books .......................................................................................91
Tivoli NetView Database ..................................................................................91
Tivoli NetView Client ........................................................................................91
Installation and Configuration Considerations ...............................................91
Tivoli NetView Server Considerations ...............................................................91
Tivoli NetView Client Considerations ...............................................................92
Fresh Installation vs. Update Installation .........................................................93
Tasks to Complete Prior to Upgrade Installation .............................................94
Backing up the Tivoli NetView Database ...........................................................94
In a non-Tivoli Management Framework Environment ...................................94
In a Tivoli Management Framework Environment .........................................94
Migrating RDBMS from 6.x to 7.1 .................................................................95
Files Migrated during Upgrade Installation .....................................................95
To Ensure A Smooth Migration .......................................................................96
Setting the LANG and LC_MESSAGES Variables ...........................................97
Installing the NetView Program in a non-Tivoli Management Framework Environment ...........................................98
Installing the NetView Server, Clients, and Books ..........................................98
Installing the NetView Program in a Tivoli Management Framework Environment .........................................................99
Managing Tivoli NetView Installation from the Tivoli Desktop .......................100
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli Management Framework Installation</td>
<td>100</td>
</tr>
<tr>
<td>Starting the Tivoli Desktop</td>
<td>101</td>
</tr>
<tr>
<td>Tivoli NetView Framework Patch</td>
<td>101</td>
</tr>
<tr>
<td>Installing a Tivoli NetView Server or Client</td>
<td>103</td>
</tr>
<tr>
<td>Installation Problems</td>
<td>105</td>
</tr>
<tr>
<td>NVenvironment script</td>
<td>106</td>
</tr>
<tr>
<td><strong>Installing the NetView Web Console</strong></td>
<td>106</td>
</tr>
<tr>
<td>Installing the Web Console from the Server</td>
<td>106</td>
</tr>
<tr>
<td>Installing the Windows Web Console from the CD</td>
<td>108</td>
</tr>
<tr>
<td>Using the Self-extracting Windows Web Console Script from the Server Download Area</td>
<td>108</td>
</tr>
<tr>
<td>Starting the Web Console on Windows</td>
<td>109</td>
</tr>
<tr>
<td>Starting the Web Console on UNIX</td>
<td>109</td>
</tr>
<tr>
<td>Installing the Tivoli NetView Mid-Level Manager</td>
<td>110</td>
</tr>
<tr>
<td>Installing the Tivoli Integration Pack for Tivoli NetView (TIPN)</td>
<td>110</td>
</tr>
<tr>
<td>Additional AIX Information</td>
<td>111</td>
</tr>
<tr>
<td>Mounting a CD-ROM on AIX</td>
<td>111</td>
</tr>
<tr>
<td>Tuning Suggestions for AIX Systems</td>
<td>111</td>
</tr>
<tr>
<td>Recommended AIX Machine Types</td>
<td>112</td>
</tr>
<tr>
<td>Tuning AIX for Tivoli NetView</td>
<td>112</td>
</tr>
<tr>
<td>AIX 4.3.3 Support</td>
<td>113</td>
</tr>
<tr>
<td>Additional Solaris Information</td>
<td>113</td>
</tr>
<tr>
<td>Solstice Enterprise Agent (SEA) Issues</td>
<td>113</td>
</tr>
<tr>
<td>MLM Issues</td>
<td>113</td>
</tr>
</tbody>
</table>
Release Notes

This Release Notes document provides important information about Version 7.1 of the Tivoli® NetView® program. These notes are the most current information for the product and take precedence over all other documentation.

Please review these notes thoroughly before installing or using this product.

The Tivoli NetView Version 7.1 program is available for use on AIX®, Solaris®, Windows NT®, and Windows 2000®. In addition, the Web Console client is available for Windows 98®.

These release notes include the following topics:

- New Features and Enhancements
- Windows® Installation and System Requirements
- UNIX® Installation and System Requirements

Tivoli frequently updates the Tivoli Customer Support home page with new information about configuring and using Tivoli products. This information includes the following:

- Updated versions of these release notes
- Updated versions of Tivoli documentation
- Searchable support databases
- Additional product patches
- Access to training schedules

For support inside the United States, for this or any other Tivoli product, contact Tivoli Customer Support in one of the following ways:

- Submit a PMR electronically through the IBMLink™ system. For information about IBMLink registration and access, refer to the IBM Web page at http://www.ibmlink.ibm.com.
- Send e-mail to support@tivoli.com.
Customers in the U.S. can call 1-800-TIVOLI8 (1-800-848-6548).


When you contact Tivoli Customer Support, be prepared to provide identification information for your company so that support personnel can assist you more readily.

New Features and Enhancements

Revised NetView Tivoli Management Framework Configuration Menus (UNIX only)

The Tivoli Management Framework icon menus for the NetView program have been redesigned for ease of use. The NetView Configuration, Control and Diagnose menus have been removed from the Tivoli Management Framework window. A new menu option, Administer NetView, allows the user to perform these and other functions. The Administer NetView menu option starts the Server Setup application when on a NetView server, or the Client Setup when on a NetView client. Also, the menu option for starting the NetView user interface has been relocated in the icon menu to the top level for easier access.

NOTE: You must install the NetView Framework Update Patch to update the menus.

New Server Setup Options for NetView Web Console

New menu items have been added to the Server Setup application for Web Server administration functions.
Server Setup Options on Windows

Registering Web Daemons
From the Server Setup window, in the Daemons tab, select the Web Server option from the drop-down list. From here you can register or unregister the three web server daemons: webserver (the web server daemon), snmpserver (the SNMP server daemon), and netviewd (the console daemon). The webserver and snmpserver daemons are registered and started by default. The netviewd daemon is not. See “New and Modified Daemons” on page 15 for more information about the new daemons.

Stopping and Starting Web Daemons
You can start and stop the new daemons in the Server Setup's Daemons tab. Select the registered daemon from the list and select Start. The Web daemons are also started and stopped from operations that stop or start all daemons.

Launching Web Console Security
You can launch the Web Console Security application from the Server Setup window by selecting the Daemons tab. Select the Web Server option from the drop-down list, and press the Configure Web Console Security button. You must use this application to create user accounts and passwords and to restart the webserver before using the Web Console. See “Web Console Security” on page 34 for more information.

Server Setup Options on UNIX

Registering Web Daemons
From the Server Setup window, select Configure, then select Configure Web Server → Enable Web Daemons to register or unregister the three web server daemons: webserver (web server daemon), snmpserver (the SNMP server daemon) and netviewd (the console daemon). The webserver and snmpserver daemons are registered and started by default. The netviewd daemon is not. See “New and Modified Daemons” on page 15 for more information about these daemons.

Stopping and Starting Web Daemons
From the Server Setup window, select Control, then select Select daemons to stop or restart → Select Web Server daemon(s) to stop or restart to
stop and restart the Web daemons. The Web daemons are also started and stopped from operations that stop or start all daemons.

**Launching Web Console Security**

From the Server Setup window, select **Configure**, then select **Configure Web Server -> Configure Web Console Security** to create user accounts and passwords and to restart the webserver before using the Web Console. See “Web Console Security” on page 34 for more information.

**New and Modified Daemons**

**webserver and snmpserver Daemons**

The **webserver** and **snmpserver** daemons are under the control of the ovspmd program. They are dependent on other daemons, and are started and stopped automatically with the other NetView daemons (using **ovstart** and **ovstop** or Server Setup).

The **webserver** daemon starts the NetView Web Server and must be running for the Web Console to connect to the Web Server.

The **snmpserver** daemon starts the NetView SNMP Server (previously called the mibserver). The snmpserver daemon must be running to use the MIB Browser, MIB Loader, and MPLS functions in Diagnostics. The snmpserver daemon is not dependent on the webserver daemon running.

On Windows, the polld daemon monitors the state of the registered daemons and restarts them as needed.

**netviewd Daemon**

The native console can now run in **unattended** mode as the **netviewd** daemon, without a user being logged on. This provides the ability to run the NetView program as the native console or as the netviewd daemon, with no loss of functionality.

Previous versions of the NetView program required that a native console be running in order for the Web Console to access map data. This posed problems in environments where the NetView server ran with no operator in attendance, because it required that a user always be logged onto the system and be running the native console.
The netviewd daemon is not registered or started by default. Use the Server Setup application to enable the netviewd daemon. See “Registering Web Daemons” on page 14 for more information. When the netviewd daemon is registered, it is automatically started and stopped by operations that stop and start all other daemons.

**Interaction with Native NetView Console on Windows**

The Windows native console cannot run when the netviewd daemon is running, and vice-versa. An error is displayed if the user tries to start both at the same time. One must be stopped and the other started in order to switch modes. If the netviewd daemon is running, the user must `ovstop netviewd` and then start the console to switch to the native console. If the native console is displayed, the user must exit the console and `ovstart netviewd` to switch to the daemon.

**Interaction with the Native NetView Console on UNIX**

On UNIX, the native console and the netviewd daemon can be run simultaneously. When netview starts up, it tries to open the default map in read-write mode. While netviewd has the read-write map open, all other users running NetView consoles are limited to read-only versions of the default map and all pertinent read-only map restrictions will apply. If a user wants to use the read-write map, they must either stop and unregister the netviewd daemon and start the native console or use the `-dconsole` option to the `netview` script by typing:

```bash
netview -dconsole
```

This option temporarily suspends the netviewd daemon and allows the NetView program to be opened with the default map in read-write mode. The netviewd daemon is restarted automatically when the native console exits. Because the current map is closed and a new read-write map is opened, any open connections to the Web Console’s Submap Explorer will be lost and a new Submap Explorer must be opened at the Web Console.

See “Additional netviewd Information for UNIX” on page 64 for additional information about the netviewd daemon.

**NOTE:** The log file for the UNIX netviewd daemon is `/usr/OV/log/netview_daemon.log`. 
Location Sensitive Topology

The functionality of `location.conf` has been extended to automatically place routers in the appropriate locations. In the hierarchy of locations, routers are placed in the first location submap that includes all the networks to which the router is connected, which might be the top-level IP Internet submap.

Router placement can also be specified in the `location.conf` file using the new Gateway entries. This function is for users with exact placement requirements for routers (for whom the new auto-placement of routers is not enough).

The syntax of `location.conf` has also been extended to allow spaces in the location name and symbol name. This enables the `N. America` and `S. America` location symbols to be used. Also, the 1000 entry limitation has been removed. Error checking has been enhanced.

Auto-placement of Routers

A router will be placed in the lowest nested location that includes all of the networks to which the router is connected:

- If all of the router's networks are inside one location, the router appears in this location connected to all the networks.
- If the router's networks are in more than one location, the router appears in the first location (up the parent chain), which includes all the locations for these networks. The router appears in the parent location connected to one or more child locations.
- If the router's networks have no common location in the parent chain, or if one of the networks appears in the IP Internet submap, the router is placed in the top level IP Internet submap.
- If the router is discovered as unmanaged, it is placed in the top level IP Internet submap (its interfaces have not been discovered in this case).

Gateway/Router Entries

Gateway entries include:

```
locationName address
```

where `locationName` is the name of the location under which the gateway should be placed; and `address` is the IP address of one of the gateway's interfaces (for example, `westford-gate.ma.dev.tivoli.com` or `146.84.242.221`). A parent location entry must occur in the `location.conf` file prior to any child gateway entries (similar to
the restriction on nested child location entries). Gateway entries will take precedence over the auto-placement of routers. If conflicting gateway entries exist in `location.conf`, the first address that matches one of the gateway’s interfaces is used.

**Syntax Extended**

The syntax has been extended to optionally allow double quotation marks ("") to be placed around each field. If a field contains a space, the use of the quotation marks is mandatory. Refer to the sample `location.conf` file in the `conf` directory for exact syntax changes.

**Hot Backup**

The NetView Version 7.1 program includes the ability to back up the NetView database without stopping and re-starting the NetView server or user interface. Hot Backup pauses the critical NetView daemons, makes the databases inactive for long enough to copy them with integrity, then resumes normal daemon activity. This allows customers to implement custom, script-based, failover facilities more efficiently.

Hot Backup provides a high-performance backup mechanism that creates a completely consistent set of NetView databases for backup or copying purposes. This eliminates the need to shut down a NetView server to get a consistent backup. Hot Backup also allows a new set of databases to be put in place on a NetView server with minimum consistency checking on startup, an enhancement that can reduce startup time from nearly an hour to a matter of minutes.

Backup time for a NetView database should be minimal, especially on UNIX where disk I/O is very fast.

**NOTE:** The NetView database actually refers to three separate databases: the map database, the topology database, and the ovwdb object database.

Hot Backup comprises three parts: a pause command (**nvpause**) which pauses netmon, ovtopmd and ovwdb (the paused state can be seen in `ovstatus`); a backup command (**tar** on UNIX, **xcopy** on Windows); and a resume command (**nvresume**) which resumes the daemons.
When the `nvhotbackup` command is issued, a dialog is displayed at the native NetView console and user activity is suspended for the duration of the Hot Backup.

**Hot Backup on Windows**

You can run Hot Backup from the Windows **Start** command by selecting **Run**, then typing `nvhotbackup` in the Open field. You can run Hot Backup from the DOS command line, or from Windows Explorer. The syntax is as follows:

```
nvhotbackup [directory] [filename]
```

where

- `[directory]` specifies the directory where the backed-up tar file resides.
- The default directory is `/usr/ov`.
- `[filename]` specifies the name of the backed-up tar file.
- The default file name is `hotdata.bak`.

**Hot Backup on UNIX**

From a command line, type:

```
nvhotbackup [-d directory] [-f filename]
```

where

- `-d` specifies the directory where the backed-up tar file resides.
- The default directory is `/usr/OV`.
- `-f` specifies the name of the backed-up tar file.
- The default file name is `NVdatabases.tar`.

**Restoring from a backed-up Database**

Follow these directions to restore from a backed-up database:

1. Go to the system where the backed-up database will be restored.
2. Exit the NetView Console if it is running.
3. Type `ovstop` on a command line to stop the NetView daemons.
4. Follow the directions for On UNIX or for On Windows.

```plaintext
On UNIX

cd /usr/OV/databases
remove the contents under /usr/OV/databases/openview
tar xvf /usr/OV/NVdatabases.tar

On Windows

go to \usr\ov\databases
remove the contents under \usr\ov\databases\openview
copy \usr\ov\hotdata.bak to \usr\ov\databases
```

5. Ensure that the directory structure is the same as before.

6. Type `ovstart` on a command line and restart the NetView application.

### Environment Variables

Hot Backup has a set of optional environment variables that can be tuned to reset timing intervals. The default values should make changing these variables unnecessary for most customers.

**NVPAUSECHECKINTERVAL**

Used by NetView consoles and the netviewd daemon to determine how often to check for the existence (or non-existence) of a pause signal file.

Default is 4000 milliseconds (4 to 5 seconds).

You can set a lower value if there is a need for the NetView consoles to respond faster to pause and resume requests.

If the value is set lower than 400 milliseconds, NetView console performance might degrade.

If the value is set too high, Hot Backup might not work properly. If this occurs, the NetView console might post a message that it cannot connect to the netmon daemon.

**NVPAUSEWAITINTERVAL**

The interval between sending a pause signal to NetView consoles and the netviewd daemon and sending a pause signal to the key NetView daemons.
This value is necessary to ensure that the NetView consoles pause before the daemons pause.

Default is 30 seconds.

You can set the value lower to decrease the time it takes for Hot Backup to complete.

If the value is set too low, the daemons might pause before the NetView consoles pause.

**NVPAUSEBAI LI NTERVAL**

The time period in which the pause and resume commands abort.

This value is necessary so that ovspmd can go back to servicing other requests like ovstart, ovstop, and ovstatus.

Default is 300 seconds (5 minutes).

If the value is set too low, NetView console performance gradually degrades.

**NVPAUSERESUMEI NTERVAL**

The time period in which the daemons and the NetView consoles automatically stop being in the pause state and resume normal NetView operations.

This value is necessary so the NetView program can function normally again.

Default is 180 seconds (3 minutes).

Hot Backup fails if the daemons resume before the database is backed up.

You can lower the value to ensure that the NetView program continues to function.

If the value is set too low, Hot Backup always fails.

You can raise the value to ensure that Hot Backup always succeeds.

If the value is set too high, the NetView program might lose track of network events and might not function properly.

**NOTE:** On large UNIX systems, we recommend increasing the number of objects to hold in cache. This is accomplished as follows:

From the Server Setup window, select **Configure -> Set options for daemons.** Then select **Set options for topology, discovery, and database daemons -> Set options for ovwdb daemon.**
Then change the **Number of objects to hold in cache** to a number approximately equal to the number of objects in your database.

**Additional Information:**

- Hot Backup should be put on a cron job and run on a regular basis.
- Hot Backup should be run at times of low system activity to avoid interruption of normal operations.
- Ovstop, ovstart and ovstatus use is suspended during a Hot Backup.
- The NetView console might not repaint during Hot Backup activity. It resumes when Hot Backup is complete.
- Any Web Consoles using a Web Server during Hot Backup temporarily lose their connections until the Hot Backup has completed.

**Web Console MIB Loader (SNMP V1/ V2)**

The new SNMP V1/V2 Web Console MIB Loader is located in the native console under **Tools → Web Console MIB Loader**. This replaces the old native V2 MIB Loader.

The initial MIB Loader window displays a list of the loaded MIBs. Use this tool to load MIBs for the Web Console MIB Browser.

**Unload MIB**

To unload a MIB, select it from the list of loaded MIBs and select **Unload**. An **Unloading MIBs** window is displayed. A progress bar shows the file processing status. The **Messages** pane displays informational messages and prompts you to select **OK** to commit the changes if parsing encountered no errors.

**Load MIB**

To load a new MIB, select **Load**. Find the files to load in the **Look In** drop-down list, or enter the path/filenames directly into the **File Name** field. With the preferred MIBs selected, select **Load**. A **Loading MIBs** window is displayed, a progress bar shows file processing status, and the **Messages** pane provides information messages. Parsing errors are displayed in this pane, as are success messages prompting you to select **OK** to commit the changes.
Additional Information:

The MIB Loader shows progress bars during startup and while loading and unloading MIBs.

Using the MIB Loader from the Command Line

You can also run the MIB Loader from the command line.

<table>
<thead>
<tr>
<th>Platform</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>\usr\ov\bin\mibloader.bat</td>
</tr>
<tr>
<td>UNIX</td>
<td>/usr/OV/bin/mibloader.sh</td>
</tr>
</tbody>
</table>

Usage:

```
mibloader.[sh|bat] [ <options> ...]
mibloader.[sh|bat] --showLoadedMibs [ --trace | --logconfig log4j.properties]
mibloader.[sh|bat] --load MIBfile.mib [ --commit ] [ --skipDuplicates ] [ --trace | --logconfig log4j.properties]
mibloader.[sh|bat] --unload MIBfile.mib [ --unload ] [ --trace | --logconfig log4j.properties]
mibloader.[sh|bat] --mib2Trap MIBfile.mib --mib2TrapOut Outputfile.[bat|sh] [ --trace | --logconfig log4j.properties]
```

Options:

- `-h` `--help` - show this list
- `-showLoadedMibs` - display the loaded MIB list
- `-load <MIB file>` - load the mib files specified
- `-unload <MIB file>` - unload the mib files specified
- `-commit` - commit the changes
  Without this option the changes aren’t permanent
- `-mib2Trap <MIB file>` - creates addTrap scripts from specified MIBs
- `-mib2TrapOut <script file>` - file name to write addTrap scripts to. Defaults to loadTraps
- `-skipDuplicates` - skip duplicate MIBs when committing a load
--trace - turns on detailed debugging
--logconfig <logconfigfile> - use specified logconfigfile for logging options

NOTE: When run on Windows, all file paths must be absolute paths.

NOTE: The mib2Trap option of mibloader.sh does not create the optional baroc file for use with the Tivoli Event Console.

Web Console MIB Browser (SNMP V1/ V2)

The Web Console MIB Browser window has been redesigned for consistency and ease of use. It has been enhanced by the addition of Read and Write Community Name fields, SNMP Version options, SNMP Walk ability, and real-time Graphing. This replaces the old native V2 MIB Browser.

The new MIB Browser window design shows a tree view in the left-hand pane with information about the selected node in the right-hand pane. A branch node is the color white until it is selected. It changes to a darker color when selected, indicating that it is expanding or retrieving data. When expansion or data retrieval is complete, it changes to a very dark color, indicating that it has completed its task. The color of the node depends on the color preferences you have set on your computer.

Additional Information:

The MIB Browser shows progress bars during startup and during data retrieval.

Read and Write Community Names

By default, the MIB Browser uses the Community Names configured in SNMP Options (Windows) or SNMP Configuration (UNIX) located in the native console Options menu. To use a Community Name other than the default, deselect the Use Default option and enter the Read or Write Community Name you want to use.

SNMP Version

The MIB Browser now has an SNMP Version button with two options: Version 1 and Version 2. This is a manual override button that was added so Walk can retrieve SNMPv2 objects correctly.
In all features except Walk, if a table or object contains any SNMPv2-only objects (for example, counter64), it automatically switches to try to use SNMPv2. But because SNMPv2 is not automatically selected for Walks, you must select Version 2 for Walks on SNMPv2 tables or objects.

Walk

When a valid Name or IP Address is entered, you can select a MIB value to activate the Walk button. Select Walk to begin a Walk of the MIB tree. When the Walk is in process, you can select Stop at any time to terminate the Walk.

Graph

When a valid Name or IP Address is entered and a relevant MIB object is selected, the Graph button becomes enabled. Select Graph to begin real-time graphing of the MIB results. Select Stop to end the graphing.

MIB Loader (SNMP V1)

The SNMP V1 MIB Loader is unchanged from previous releases.

<table>
<thead>
<tr>
<th>On UNIX</th>
<th>The SNMP V1 MIB Loader is located under the Options main menu option. Select Load/Unload SNMP V1 MIBs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>On Windows</td>
<td>The SNMP V1 MIB Loader is located under the Tools main menu option. Select MIB -&gt; Loader SNMP V1.</td>
</tr>
</tbody>
</table>

NOTE: Use this tool in conjunction with the MIB Application Builder and the MIB and SNMP Data Collection tools. See “Web Console MIB Loader (SNMP V1/V2)” on page 22 for more information about the new MIB Loader.
Mi B Browser (SNMP V1)

The SNMP V1 MIB Browser is unchanged from previous releases.

<table>
<thead>
<tr>
<th>On UNIX</th>
</tr>
</thead>
<tbody>
<tr>
<td>The SNMP V1 MIB Browser is located under the <strong>Tools</strong> main menu option. Select <strong>MIB Browser SNMP V1</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>On Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>The SNMP V1 MIB Browser is located under the <strong>Tools</strong> main menu option. Select <strong>MIB -&gt; Browser SNMP V1</strong>.</td>
</tr>
</tbody>
</table>

**NOTE:** The new, enhanced SNMP V1/V2 MIB Browser is now accessed only from the Web Console for both UNIX and Windows. See “Web Console MIB Browser (SNMP V1/V2)” on page 24 for more information about the new MIB Browser.

**Discovery, netmon.seed, Netmon Seed File Editor**

The netmon daemon has been enhanced in a number of areas:

- Backbone discovery option.
- Netmon Seed File Editor user interface enhancements.
- Support for Dormant ifOperStatus.
- SNMP Status Support enhancement.
- Support for redundant router addressing (extension of HSRP support).
- Netmon ignores unresolved host names in the seed file, producing an error message as appropriate.
- The Windows netmon seed file has been enhanced to support all the UNIX netmon seed file options.
Backbone Discovery Option

In addition to the Local Subnet Only and All Networks discovery options available through Server Setup, netmon now offers a Backbone discovery option. This option performs a maximum performance discovery of only connectors (primarily routers and switches) and subnetworks.

<table>
<thead>
<tr>
<th>On UNIX</th>
</tr>
</thead>
<tbody>
<tr>
<td>The discovery options are available from the Server Setup window. Select Configure –&gt; Set options for daemons. Then select Set options for topology, discovery, and database daemons –&gt; Set options for netmon daemon. Select a pull-down choice from Range of automatic discovery.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>On Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>The discovery options are available from the Server Setup window. Select the Discovery tab, then select Range of Automatic Discovery. These options are also offered during a fresh installation of the NetView program.</td>
</tr>
</tbody>
</table>

Unresolved Hostnames

All seed file errors are logged in the /usr/OV/log/nv.log file. Invalid entries are ignored.

Netmon Seed File Editor

The new Netmon Seed File Editor allows users to easily add, modify, and remove entries from the netmon.seed file to specify discovery options. The available options are Set Initial Discovery Seeds, Limit Discovery, and Monitor Special Devices.

The Set Initial Discovery Seeds option identifies specific nodes for proactive discovery. You can choose to limit discover to the specified nodes, or extend discovery beyond the specified nodes.

The Limit Discovery option specifies ranges and wildcards. Support has been added for OIDs (nodes to include and exclude) on Windows.

The Monitor Special Devices option allows you to set specialized options for status monitoring. Use these options for special devices that require
specialized management behaviors. Support has been added for DHCP Clients, HSRP Interfaces, ISDN Backup Interfaces and inclusion and exclusion of nodes for SNMP Status Checking.

**Opening the Seed File Editor**

You can access the Netmon Seed File Editor in four different ways on Windows and two different ways on UNIX.

<table>
<thead>
<tr>
<th>On UNIX</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. From the Server Setup window, select <strong>Configure –&gt; Set options for daemons</strong>. Then select <strong>Set options for topology, discovery, and database daemons –&gt; Set options for netmon daemon</strong>. From the Setup Options window, select <strong>Full name of seed file –&gt; Edit</strong>.</td>
</tr>
<tr>
<td>2. From the native NetView console main menu, select <strong>Options –&gt; Netmon Seed Editor</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>On Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. From the Windows <strong>Start</strong> menu, select <strong>Programs –&gt; Tivoli NetView</strong>. Then select <strong>Administration –&gt; Server Setup</strong>. In the Server Setup window, select the <strong>Discovery</strong> tab. Then select <strong>Use Seed File –&gt; Edit</strong>.</td>
</tr>
<tr>
<td>2. From the native NetView console, select <strong>Options</strong> from the main menu. Then select <strong>Server Setup –&gt; Discovery</strong> tab. In the Discovery tab, select <strong>Use Seed File –&gt; Edit</strong>.</td>
</tr>
<tr>
<td>3. From the native NetView console, select <strong>Options</strong> from the main menu. Then select <strong>Discovery</strong>. In the Discovery tab, select <strong>Use Seed File –&gt; Edit</strong>.</td>
</tr>
<tr>
<td>4. From the native NetView console, select <strong>Options</strong> from the main menu. Then select <strong>Netmon Seed Editor</strong>.</td>
</tr>
</tbody>
</table>

The following options are available in the Network Monitor Seed File Editor window:

**Set Initial Discovery Seeds**

Seed entries are single entries (no wildcards or ranges). IP addresses or hostnames can be specified for the netmon daemon to use as starting points for discovery when netmon is started. Netmon always attempts to discover these nodes. Seed nodes must be reachable and should support SNMP.
Routers make good candidates. Single hostnames and IP addresses are accepted, ranges and wildcards are not.

For example:
16.21.144.20
router1.eng.com

If the node’s name cannot be resolved by the name server, then the seed node is considered invalid and is ignored. If an IP address cannot be resolved by the name server, a seed hint is still added and a warning is logged in the /usr/OV/log/nv.log file.

The **Set Initial Discovery Seeds** option identifies specific nodes for proactive discovery. Assuming they are reachable, these nodes *and all their interfaces* will always be discovered, regardless of any specified limit to exclude them. You can choose to extend discovery beyond these specified seeds, or to limit discovery to these seeds (plus any entries in the Limit Discovery section).

You can limit discovery to *only* these seeds by selecting **Options > Limit Discovery to this Seed File**. If this option is checked, it means that discovery is restricted to the listed seeds (as well as anything specified elsewhere in the seed file). If this option is not checked, discovery will extend beyond the listed seeds.

**Limit Discovery**

Filtering discovery with entries in this seed file works in conjunction with the modes of discovery: Discover Local Subnets, Discover Backbone (routers and other connectors), and Discover All.

**Limit by IP Address**

**Include**

Use this option to restrict discovery to the specified seed entries. Ranges and wildcards are accepted, for example:

| 10.2.*.1-100 | Range of addresses using * and - |
| router_boston* | Wildcards using * and ? (single character) |
Exclude

Use this option to exclude certain nodes from seed entry discovery. Single hostnames, single IP addresses, ranges and wildcards are accepted, as is a hostname with a wildcard, for example:

10.1.1.2 Specific entry
10.*.1.1-100 Ranges using * or -
router_boston* Wildcards using * and ? (single character)

Limit by OID

Include

Use this option to restrict discovery to the specified seed entries. Single OIDs and OID wildcards (as the last octet only) are accepted, for example:

1.3.6.1.4.1.36.* Wildcards as final char using *

Limit by OID

Exclude

Use this option to exclude certain nodes from seed entry discovery. Single OIDs and OID wildcards are accepted, for example:

1.3.6.1.4.1.9.* Wildcards as final char using *
0 Zero filters out all non-SNMP supported devices.

NOTE: Excluded entries have priority for filtering. If there is any overlap with an included entry, the excluded has priority and is not discovered.

Monitor Special Devices

Monitor DHCP Clients (Windows only)

Enter the same IP address ranges that are configured on your DHCP servers. Use the same syntax for ranges and wildcards as the included entries above. For example, suppose the address range 1.1.1.1 to 1.1.1.255 is reserved for DHCP clients, except for 1.1.1.10 to 1.1.1.15 which are dedicated to print servers, and so on. Also, everything in the range 1.2.252-255.* This would be represented as:
Monitor HSRP Interfaces

HSRP interfaces can be specified here for the netmon daemon to acknowledge them. Only the public IP address need be entered.

Ranges and wildcards as described above for included seed entries can be used. For example, if 1.1.1.1 is the IP address of the HSRP interface that switches between two routers, enter: 1.1.1.1

Monitor ISDN Backup Interfaces

By default, interfaces with an SNMP ifOperStatus of DORMANT are handled as if the status is NORMAL and the icon status color will be NORMAL. However, in the special case of ISDN backup lines, when the status is NORMAL, it usually means the primary line has a problem, and when DORMANT, the primary line is usually okay. In this case the status transitions to UP, and DORMANT might indicate the need for operator intervention.

The following features are intended to help operators handle ISDN backup lines:

- The status of a backup line in DORMANT state is USER1, otherwise the status is as usual (NORMAL, DOWN). Note that the backup line with a status of AdminDown will also be USER1.
- When the status changes to UP (from any state) the event Backup Line is ACTIVE is sent.
- When the status transitions to DORMANT (from any state, including AdminDown) the event Backup Line is DORMANT is sent.

To tell the NetView program to handle specific interfaces as ISDN Backup lines, use the same syntax for ranges and wildcards described above for excluded seed entries.

For example: 10.1.2-10.221-230

This automatically enables SNMP status polling for these entries.
Enable SNMP Status Checking

Include

Nodes that have serial interface cards will automatically use SNMP to query for ifAdminStatus and ifOperStatus for all interfaces on that node. Specify other nodes on which you would like to use SNMP to query for status instead of ICMP pings.

Use the same syntax for ranges and wildcards described above for included seed entries. For example: 1.1.2-10.221-230

Exclude

Use this option to indicate exceptions in the ranges or wildcards, including routers on which netmon would normally enable SNMP status polling, such as those with unnumbered serial interfaces. For example: 1.1.9-10.230

Update Network Monitor

This option is available from the File menu, and rereads the seed file without stopping and restarting netmon. This option is active only for discovery node changes and when netmon has previously been configured to use netmon.seed for discovery. Changes to HSRP, DHCP, ISDN Backup, or SNMP Status require the netmon daemon to be stopped and restarted. In this event you are prompted to stop and restart netmon.

You can also invoke a reread of the seed file from the command line by typing netmonaction.bat seed on Windows and netmonaction.sh seed on UNIX.

Additional Information:

⊙ Occasionally, when you open the seed editor on the AIX platform, it might look like the menu bar is missing. Resize the screen slightly to see the menu bar.

⊙ You can open the seed file in a text editor if you want more information about the tokens that are entered in the seed file by the netmon seed file editor.

⊙ You can use a seed file other than the default (netmon.seed).

On Windows, use the Browse button in the Discovery tab of Server Setup to specify the seed file that you want the netmon daemon to use. Note that the seed file must reside on the same drive as the NetView program. After specifying the seed file, you can use the Edit button to make changes to it.
On UNIX, in the Server Setup window, enter the name of the desired seed file in the **Full name of seed file** field.

**Ping Enhancement (AIX only)**

After a fresh AIX install, the default ping count is one. On AIX, a user can change the default Ping count by selecting a node and selecting **Test -> Ping** from the main menu. One ping is sent to the node.

To change the ping number, select **Options** from the main menu, then select **Change Ping Count**. Enter a new ping value, then select **Restart**. The specified number of pings is sent.

**ATM/ Frame Relay MAC addresses**

ATM (and Frame Relay) MAC addresses have been increased from 12 to 20 characters (topology database).

**MPLS**

Devices with MPLS capability are identified and further queried for MPLS-specific data. The NetView program manages LSRs (Label Switch Routers). LSRs act as connectors between segments and make forwarding decisions based on labels. See “MPLS” on page 53 for more information.

**Polling Configuration File Changes**

The polling configuration file has been moved from the `/usr/OV/databases/openview/topo` directory to the `/usr/OV/conf` directory. The polling configuration settings are now preserved when databases are regenerated.
Web Console Security

The NetView program is now configured to provide authorization through local configuration files. User, Role and Scope profiles are created using the new Web Console Security window, and these profiles are used to validate Web Console access to the Web Server.

Actions and areas of visibility are regulated by Roles and Scoping, which are assigned to a user's profile. Using a combination of Roles and Scoping, you can fine-tune the actions a user can perform and limit the view that the user has of the network.

In the Web Console, security is used to validate access to the Submap Explorer, Object Properties, Diagnostics, Event Browser and the MIB Browser.

For example, a user's Role can be customized to not enable use of Diagnostics, or to enable its use, but only for a particular action, like Ping, of the many possible actions within it. The user's Scope can be customized to limit visibility to only particular Networks and Locations. When the user attempts to perform actions for objects outside of this scope (for example, from Object Properties, Diagnostics, Event Browser, MIB Browser or Submap Explorer) scoping checks are performed to deny the action if the target object is out-of-scope.

This roles- and scoping-based security mechanism applies only to users accessing the NetView program through the Web Console. Users with direct access to the NetView server and the conventional NetView client will continue to have their access controlled by the existing NetView security mechanisms. Users with root access to the NetView server machine will continue to have essentially unlimited access to NetView capabilities and data. We expect customers to control physical access to the NetView server machine (and a firewall if necessary) in order to protect their network. Some administrative tasks will require physical and root access to the NetView server, as this is the appropriate way to control access to those functions.
The Web Console Security window can be accessed in two different ways on UNIX and in three different ways on Windows.

### On UNIX

1. From the native NetView console, select **Administer** from the main menu. Select **Security Administration -> Web Console Security**.
2. From the **Server Setup** window, select **Configure -> Configure Web Server**. Select **Web Client User Accounts**.

### On Windows

1. From the native console, select **Options** from the main menu, then select **Web Console Security**.
2. From the native console, select **Options** from the main menu, then select **Server Setup -> Daemons** tab. In the Daemons tab, from the pull-down list, select **Web Server** then press the **Configure Web Console Security** button.
3. From the Windows **Start** menu, select **Programs -> Tivoli NetView**. Select **Administration -> Server Setup**. Select the **Daemons** tab. In the Daemons tab, from the pull-down list, select **Web Server** then press the **Configure Web Console Security** button.

**NOTE:** You must use Web Console security to add new users before you can log on to the Web Console.

### Scopes

Scopes are used to limit the network topology that users can view. Scopes are also used to limit the target objects that users can perform actions against.

A scope is defined by the set of top level Locations and Networks that are to be considered in scope. All logical objects (Networks and Segments) and physical devices (Routers, Nodes, Interfaces) beneath a particular scope's set of root Locations and Networks are treated as in scope and available for viewing in the Submap Explorer as well as for performing actions against in Diagnostics, Object Properties, MIB Browser and Event Browser.

The predefined No scoping restrictions scope allows full access, effectively turning off scoping for those users that are assigned this scope.
For scoping to be available, the default map must be open, either as the netviewd daemon or as the native console.

The following differences exist when using a scoped account:

### Submap Explorer Differences:

- The only map enabled for viewing is the Default map.
- The Root submap contains only those networks and locations that are within scope. This submap uses a row and column layout style. Scoped accounts cannot view the SmartSet submaps.
- Node submaps do not display any out-of-scope interfaces.
- The **Find** feature does not show any symbol matches that are out-of-scope.
- When you right-click on an object, the **Show in** menu displayed on the pop-up menu does not contain any out-of-scope symbols.

### Diagnostics, Object Properties, MIB Browser Differences:

- If you type in an object name, hostname or IP address that is out-of-scope, you are informed of this and the operation does not complete.

### Event Browser [if Role is configured to filter this]:

- Events for out-of-scope nodes will not be displayed. See “Creating a New Role” on page 38 for more information about scoping in the Event Browser.

## Creating a New Scope

Follow these steps to create a new scope:

1. Select **Scopes** and select the **Add** icon or select **Selected → Add** from the main menu.
2. When the **Add Scope** window opens, enter a scope name and select **OK**. The new scope name is displayed in the Web Console Security window.
3. From the **Type** option, select **Network** or **Location**.
4. Enter the Network Address or Location and select the **Add** button to the right. The network or location displays in the **Allowed Networks and Locations** list.

5. Continue to add Networks and Locations to the scope until you attain the desired coverage.

To add another scope, repeat Steps 1 through 5.

6. When you have completed creating your scopes, select the **Save** icon or select **File -> Save**. You are prompted to restart the Web Server for the changes to take effect. You can restart the Web Server at any time by selecting **File -> Restart Web Server**.

7. If you have no more Security Console modifications to make, select **Yes**. Otherwise, select **No** and start creating Users or Roles.

**NOTE:** You can select **Remove** and **Copy** from the **Selected** menu option to remove users, roles and scopes or to copy existing ones. You can also select the **Copy** and **Remove** icons on the window.

**Additional Information:**

- You can enter Networks and Locations that have not yet been discovered — just be sure to discover them in the near future.
- If you enter a Network as an address, then later associate a name with that address, you must update the scope to use that name instead of the address. Scoping works on an object’s selection name.
- The Scope routines correctly handle networks that have names in the `/etc/networks` file, but you can not have a scope with a network address (10.1.1) in the `ScopeInfo.xml` file if the network name (`West`) is set in the `/etc/networks` file for this network.
- A scoped Location must contain a network in order for Scoping to work properly. A Location that contains no networks, only devices, will report that those devices are out of scope.

**Roles**

A user’s role constrains the actions that they are allowed to perform in two ways:

- By the actions that are visible at the NetView Web Console
By a filtering mechanism at the Web Server that rejects unauthorized actions, if they are initiated by an unauthorized role.

Default Roles

The default Roles are User, Operator, Administrator and SuperUser. By default, Administrator and SuperUser roles are allowed all actions. The Operator role is not permitted to Manage or Unmanage Objects. The User role can access only the Submap Explorer, Object Properties, the Event Browser, and the device’s Web home page.

Creating a New Role

Follow these steps to create a new role:

1. Select Roles and select the Add icon or select Selected –> Add from the main menu.
2. When the Add Role window opens, enter a role name and a description of the role, then select OK. The new role name is displayed in the Web Console Security window.
3. If you want this role to use scoping in the Event Browser, select the Enable Scoping in Event Browser checkbox.
4. From the Actions list, select the actions you want assigned to this role.

To add another role, repeat Steps 1 through 4.

5. When you have completed creating your roles, select the Save icon or select File –> Save. You are prompted to restart the Web Server for the changes to take effect. You can restart the Web Server at any time by selecting File –> Restart Web Server.

6. If you have no more Security Console modifications to make, select Yes. Otherwise, select No and start creating Users.

NOTE: You can select Remove and Copy from the Selected menu option to remove users, roles and scopes or to copy existing ones. You can also select the Copy and Remove icons on the window.
Users

A user is a profile that contains a name, password, role, and a scope. No default users are shipped with the NetView Version 7.1 program. You must create users before you can access the NetView Web Console.

Creating a New User

Follow these steps to create a new user:

1. Select **Users** and select the **Add** icon or select **Selected –> Add** from the main menu.

2. When the **Add User** window opens, enter a user **Name** and a user **Password**. Retype the password to confirm it. You must assign a password to a user.

3. From the **Role** drop-down list, select a default role or a role that you created in “Creating a New Role” on page 38.

4. From the **Scope** drop-down list, select the default scope (**No scoping restrictions**) or a scope that you created in “Creating a New Scope” on page 36.

5. When the new user has the appropriate role and scope assignments, press **OK**.

To add another user, repeat Steps 1 through 5.

6. When you have completed creating your users, select the **Save** icon or select **File –> Save**. You are prompted to restart the Web Server for the changes to take effect. You can restart the Web Server at any time by selecting **File –> Restart Web Server**.

7. If you have no more Security Console modifications to make, select **Yes**. Otherwise, select **No** and continue making modifications.

**NOTE:** You can select **Remove** and **Copy** from the **Selected** menu option to remove users, roles and scopes or to copy existing ones. You can also select the **Copy** and **Remove** icons on the window.

**Additional Information:**

- Use of the following characters in the Web Console Security is not allowed.
- In User Name, User Password, Role Name and Scope Name: tab, <enter>, space, equals (=), colon (:)

---

*Tivoli NetView Release Notes* 39
Manually Restarting the Web Server

You can manually restart the webserver daemon at any time to force the Web Console to recognize changes you've made in the Web Console Security windows. From the main menu in the Web Console Security window, choose File -> Restart Web Server.

Reverting to a Previous Security Configuration

Every time you press Save in the Web Console Security window, a zip file is created in the /usr/OV/www/webapps/netview/warf directory. If you ever need to revert to a previous web console security configuration, you can do so by following the steps below. The instructions are valid for both UNIX and Windows (using the appropriate slash direction and capitalization).

1. Go to /usr/OV/www/webapps/netview/warf. You will see some directories, some zip files, an xml file, two xsl files and a dtd file.

2. Select all directories except the Template directory. Select only the directories (Administrator, Operator, etc.) Do not select the zip files or other files – just the directories.

3. Delete the directories selected in step 2.

4. Look at the .zip files — a new one is created each time you Save the Web Console Security settings. Select the .zip file with a timestamp that corresponds to the Web Console Security settings that you want to return to. If you're unsure of which file is the correct one, you can use the oldest file to return to the original default settings.

5. Extract the appropriate zip file. On Windows, you can use the JAR tool (jar xvf filename.zip) or any file extraction tool (like WinZip). On UNIX, you can use the jar, unzip, gzip, or gunzip commands. The JAR tool is available from the Solaris or IBM web sites. The gzip executable is available from the GNU website.
Additional Web Console Security Information

The Web Console Security window only defines users in the NetView realm. To view NetView or Jetty log files over HTTP, one or more users must be defined in the NetView Admin and Jetty Admin realms by editing the corresponding .properties file.

The Web Console Security window provides an easy way to configure a small number of user accounts, but if you plan to configure a large number of accounts you might find it easier to write a script to modify the NetViewRealm.properties file. The following sections explain more about the Web security-related files.

Refer to “About Realms” on page 41 for more information on realms.

In the following sections, the paths are shown in UNIX format. For Windows, simply change the forward slashes to backward slashes.

Changing a Web Server’s Port


2. Find <Set name="Port">8080</Set>.

3. Change 8080 to another port number.

4. Save the file.

5. Restart the web server:
   ostop webserver
   ovstart webserver

More information about configuring Jetty can be found at http://jetty.mortbay.com/jetty/doc/JettyConfiguration.html

About Realms

A realm is a web server security policy domain. Three realms are configured (in /usr/OV/www/conf/jetty.xml) for NetView’s embedded web server. The realms are named NetView, NetView Admin, and Jetty Admin. Each realm has a corresponding properties file for defining user accounts in that realm.
Each time you enter a URL for a different realm, you must enter a username and password for an account in that realm.

The format of both administrative realms is the same. Each account is defined by a line containing a user name, password, and role, in the following format:

```
username : password,role
```

For example,

```
jsmith : qaz321,Administrator
```

In addition to username, password, and role, the NetView realm file specifies each user’s scope:

```
username : password,role;scope
```

For example,

```
janedoe : m89ko,Operator;Westford_LAN
```

Accounts in each administrative realm must be configured by editing the properties file.

Accounts in the NetView realm may be configured with the Web Console Security window.

### Logging

Web server log files are located in `/usr/OV/www/logs`.

The daily web server log files are named `yyyy_mm_dd.request.log`. Log files are retained for 90 days. This can be configured in `jetty.xml`.

<table>
<thead>
<tr>
<th>Realm</th>
<th>Properties File</th>
<th>URL Prefix</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetView</td>
<td>NetViewRealm.properties</td>
<td>/netview/*</td>
<td>NetView Web Application</td>
</tr>
<tr>
<td>NetView Admin</td>
<td>NetViewAdminRealm.properties</td>
<td>/netview/logs/*</td>
<td>NetView log files under /usr/OV/log</td>
</tr>
<tr>
<td>Jetty Admin</td>
<td>JettyAdminRealm.properties</td>
<td>/jetty/logs/*</td>
<td>Jetty log files under /usr/OV/www/log</td>
</tr>
</tbody>
</table>
The web server log uses the *Extended Common Log Format*. Each line consists of the following nine fields, separated by a space. If a field value is not known, a minus sign (-) is placed in the field.

1. remote hostname or IP address
2. remote login name of the user
3. authenticated username (available when using password protected WWW resources)
4. date and time of the request
5. HTTP request
6. HTTP response code
7. number of bytes transferred
8. URL the client was using before requesting this URL
9. *User agent* is defined as the software the client claims to be using.

In addition to the web server logs, there are two other log files, *filechecker.log* and *netview servlets.log*. Each time the web server is started, its security configuration files are checked for consistency and the results are logged in *filechecker.log*. The web server will not start if any errors are found in its security configuration files.

Diagnostic output from NetView servlets is logged in *netview servlets.log*. The level of diagnostic output can be configured by editing */usr/OV/www/classes/log4j.properties*.

More information about configuring the log4j logging package can be found at:

http://jakarta.apache.org/log4j/docs/index.html

*The security configuration files are:

/usr/OV/www/conf/NetViewRealm.properties
/usr/OV/www/conf/ScopeInfo.xml
/usr/OV/www/webapps/netview/WEB-INF/web.xml
/usr/OV/www/webapps/netview/warf/*.*.xml
NetView Web Application Configuration

The NetView Web Console is packaged as a web application according to the Java™ Servlet Specification, v2.2. It is configured by its deployment descriptor, /usr/OV/www/webapps/netview/WEB-INF/web.xml.

Web Console

Substantial enhancements have been made to the Tivoli NetView Web Console.

- Enhanced look and feel for all components and new icons.
- Menu restructuring for consistency and ease of use.
- Manage/Unmanage, Acknowledge/Unacknowledge.
- Respect manual layout from server and display new object holding area in topology view.
- Submap Explorer now supports Star topology layouts.
- Submap Explorer caches table views and displays date and time when the table was obtained.
- Dormant Status is displayed (ISDN Backup) in Submap Explorer.
- Web Server communication status light.
- New information in View Columns: MPLS, MAC Address, HSRP, Alias, ISDN Backup.
- Context sensitivity in Diagnostics and Object Properties.
- Submap Explorer features a symbol pop-up menu Show in ability.
- Submap Explorer contains a Find feature (by object name, hostname, or IP address).
- New Diagnostic tests including Test –> QuickTest and Test –> QuickTest Critical, a new MPLS category (Node and Interface view) and Switch Management category (Port View, Switch Status, MAC View, Inactive Ports)
- Object Properties can now be used for object types other than nodes (including IP Internet, Networks, Segments and Interfaces).
- Improved Event Browser with enhanced filtering capability including filtering by trap, description, and category. The node filter was extended
to allow filtering on a list of nodes. On Windows only, a date and time filter was added, allowing the display of events before or after a specified date and time. On UNIX only, filtering by Ruleset has been added, including support for the Resolve function. Event Details, Severity Graph and all event columns from Windows are now available on UNIX.

- Redesign of MIB Browser, with Read/Write Community Names, SNMPv1/v2, full or partial walks, real-time graphing.
- Enhanced Server Status window.
- Security, addressed in “Web Console Security” on page 34.
- Web Console now works through firewalls, because the Web Console needs access to only the single port that the Web Server is bound to. The default value for this port is 8080.

Starting the Web Console

You can run the Tivoli NetView Web Console in two ways: as an applet that runs in your web browser window, or as an application which does not require a web browser window.

The Web Console applet can be started in a browser by entering http://<hostname>:8080/netview/NetViewApplet in the browser’s Location field.

The Web Console application can be launched in a number of ways:

<table>
<thead>
<tr>
<th>On a Windows NetView Server or Client</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>From the Windows Start menu, select Programs -&gt; Tivoli NetView, then select NetView Web Console</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>On a Windows NetView Web Console Only</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>From the Windows Start menu, select Programs -&gt; Tivoli NetView Web Console, then select NetView Web Console</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>From a DOS command line on a Windows NetView Server or Client</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Type \usr\ov\bin\nvwc.bat</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>From a DOS command line on a Windows NetView Web Console Only</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Type \Program Files\Tivoli Systems\Tivoli NetView Web Console\nvwc.bat</td>
<td></td>
</tr>
</tbody>
</table>
**On a UNIX NetView Server**

On the Web Server, type `./OV/bin/nvwc.sh` on the command line.

**On a UNIX NetView Client**

To go directly to the designated NetView web server from the NetView client, type `/usr/OV/bin/nvwebclient` on the command line. This command will not work unless a server is configured.

To be able to enter the name of any NetView web server from the NetView client, type `/usr/OV/bin/nvwc.sh` on the command line.

---

**Logging on to the Web Console**

When the Tivoli NetView sign-on window is displayed, enter a User ID and Password created in “Creating a New User” on page 39. Enter the Web Server you want to connect to in the Hostname field. The default port is 8080. Enter a different port if you use a port other than the default. When these fields are complete, the **OK** button becomes available. If the User ID and Password are correct, a Welcome window is displayed. You can select the **Do not show this again** choice to suppress its appearance when logging on with that User ID in the future. You can select **Books On-line** to launch the Tivoli NetView Product Library.

**New Icons**

Many menu icons have been updated. If you are unsure of the function of any icon, hover over it with your cursor to see a tool tip about its use.

**Table View Filtering and Sorting**

In all non-topology views, each table displays a filtering arrow and each column displays sorting arrows for column headers. This is true in the Submap Explorer, Event Browser, and many Object, Monitor, Test and Tools windows.

To use the filtering feature, follow these steps:

1. Select the right-pointing triangle to the right of the column headings.
2. Select **Show Filter Row** from the available options.
3. Select `<no filter>` in the column to be filtered.
4. Enter the text to filter on.
5. Select either **Contains** or **Starts with** from the drop-down list.
6. Select **Match Case** if you want the filter to be case-sensitive.
7. Press OK.

Repeat steps 1 through 7 to filter on another column.

To use the sorting feature, select the up or down arrows in each column header to change the sorting order.

### Main Menu Changes

Tools (Diagnostics, Object Properties, Event Browser, MIB Browser, and Server Status) can be opened and used without opening a map, provided the user enters an object ID that is within the Scope of that User.

The menu options have been rearranged for increased ease of use. The options in the main menu are now grouped as follows:

<table>
<thead>
<tr>
<th>Object</th>
<th>Monitor</th>
<th>Test</th>
<th>Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage</td>
<td>Network</td>
<td>Connectivity</td>
<td></td>
</tr>
<tr>
<td>Unmanage</td>
<td>System</td>
<td>Ping</td>
<td></td>
</tr>
<tr>
<td>Acknowledge</td>
<td>LAN Manager</td>
<td>Demand Poll</td>
<td></td>
</tr>
<tr>
<td>Unacknowledge</td>
<td>Other</td>
<td>Locate Route</td>
<td></td>
</tr>
<tr>
<td>Object Properties</td>
<td>MPLS</td>
<td>QuickTest</td>
<td></td>
</tr>
<tr>
<td>MIB Browser</td>
<td>Switch Management</td>
<td>QuickTest Critical</td>
<td></td>
</tr>
<tr>
<td>Home Page</td>
<td>Management Page</td>
<td>Diagnostics</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Object Properties</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event Browser</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MIB Browser</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Server Status</td>
<td></td>
</tr>
</tbody>
</table>

All the menu options shown above are available for the SuperUser and Administrator roles.

A user assigned the User role can access only the Object Properties, Home Page, and Event Browser options, as well as options from the Help menu.

A user assigned the Operator role can access everything except Manage and Unmanage.
Using the Help Menu

The Help menu options are Books On-line and About Tivoli NetView Web Console.

Selecting the Books On-line option opens a browser window with a list of NetView documentation available in both PDF and HTML formats. The selection is determined by the operating system of the Web Server.

Selecting the About Tivoli NetView Web Console option opens a browser window that displays all the Open Source Software, the Commercial Software, and the Open APIs used in the Tivoli NetView Web Console.

Right-clicking on Network Objects

Right-clicking on a symbol in the Submap Explorer displays the menu options shown below.

<table>
<thead>
<tr>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
</tr>
<tr>
<td>Manage</td>
</tr>
<tr>
<td>Unmanage</td>
</tr>
<tr>
<td>Acknowledge</td>
</tr>
<tr>
<td>Unacknowledge</td>
</tr>
<tr>
<td>Object Properties</td>
</tr>
<tr>
<td>Home Page</td>
</tr>
<tr>
<td>Management Page</td>
</tr>
<tr>
<td>Ping</td>
</tr>
<tr>
<td>Show In</td>
</tr>
</tbody>
</table>

The Object Properties, Monitor and Test menu options are context-sensitive, indicated by the diamonds displayed next to the options. (Select an option from the Monitor menu arrow to see the diamond.) Only those options that are valid for a selected object within Submap Explorer are active. See “Context Sensitivity in Diagnostics and Object Properties” on page 50 for a more detailed explanation of context sensitivity.
Web Server Communication Status Light

The Web Console’s Submap Explorer now contains status lights in the bottom right to report the Web Server’s communication status. The light on the left is the green light. The light on the right is the red light.

<table>
<thead>
<tr>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steady green</td>
<td>functioning correctly, no current communication</td>
</tr>
<tr>
<td>Blinking green</td>
<td>communicating</td>
</tr>
<tr>
<td>Red</td>
<td>disconnected</td>
</tr>
<tr>
<td>Blinking red</td>
<td>trying to reconnect</td>
</tr>
</tbody>
</table>

The right status light turns dark red whenever the Web Console notices (either through user activity or background polls) that a request has failed to reach the Web Server. This red light pulses every few seconds (default is 5 seconds) as the Web Console automatically sends out requests to check on the connection.

When the Web Server becomes available again, the Web Console attempts to determine if the Web Server has been stopped and restarted and, if so, indicates that you must restart the Web Console (closing the dialog results in closing the applet or application). If, on the other hand, the Web Server has not been stopped and restarted, you can continue working with your current Web Console and the blinking resumes with the normal green color on the left. This situation might occur if, for example, someone removed the network drop from the Web Server and later reconnected it.

There is one exception to continuing a session with a Web Server that has not been stopped and restarted. If the loss in communication was due to networking problems, the Web Console might become invalidated as the Web Server is, by default, configured to invalidate any client that has been inactive for 1 hour or more. If this situation occurs, the Web Console will behave exactly as it would when it detects a recycled Web Server — it will inform you that you must restart the Web Console.
**Context Sensitivity in Diagnostics and Object Properties**

If you compare the **Tools** menu with the **Test** menu, for example, you will notice that the options in the **Test** menu have diamond symbols in front of them, while the items in the **Tools** menu do not.

The diamonds signify that the selected object name will be entered automatically in the Name or IP address field of the option selected. The diamonds also appear in the submenus under **Monitor**.

In the **Tools** menu, where there are no diamonds, the selected object name will not be automatically inserted in the name field.

The availability of menu options also depends on the object selected. Only the tasks that an object is capable of performing are made available. For example, if an object is not running SNMP, the Diagnostics window would allow you to access **Test** options, but not the Network, System, LAN Manager, Other, MPLS or Switch Management options.

The **Object**, **Test**, and right-click options are available when an object is selected.

**Submap Explorer**

**New Object Holding Area**

A New Object Holding Area in the Submap Explorer is displayed when the native NetView server is in manual layout mode.

When in manual layout mode on the native console, moving symbols in the native console (using mouse button 2 on UNIX) now results in corresponding symbol move updates in the Submap Explorer. Toggling the auto layout in the main menu of the native NetView program also toggles the New Object Holding Area in the Submap Explorer.

**Time and Date**

The Submap Explorer now caches all table views. If you drill into the same submap table or switch back to a previously queried table, the prior results are displayed and the original query time and date are displayed in the status bar area. Click the **Refresh** toolbar button to get new results.
ISDN Dormant Status Display

Dormant status is displayed in the Submap Explorer. See “Monitor ISDN Backup Interfaces” on page 31 for a detailed description of Dormant Status Display.

Manage/Unmanage — Acknowledge/Unacknowledge

With appropriate privileges assigned from the Web Console Security window, users can Manage/Unmanage and Acknowledge/Unacknowledge an object by right-clicking on the object or by selecting the action from the Object menu.

New View Columns

- System Configuration View: MPLS status (True, False)
- IP Address View: MAC Address (extended from 12 to 20 characters)
- Interface View: HSRP (True, False), Alias, ISDN Backup (True, False)

Show in

When you right-click on an object in the submap explorer, the pop-up menu now contains a Show in option that is similar to the feature found on the native Windows console. The Show in option lists all the other submaps for which other symbols are attached to the same object. Selecting an item from the Show in option results in switching the context to that submap and selecting the appropriate sibling symbol within that submap.

Find

The Find feature enables finding objects by selection name, IP address, or hostname. The resulting matches can be found in either the main topology/table area or the New Object Holding Area.

Select the Find icon or select Edit -> Find from the main menu. You can search by Hostname, Object Name or IP Address by selecting it from the associated pull-down list. (HINT: you can locate objects other than nodes by using the Object Name category.) You can search by selecting Using Wildcards, Exactly, or Using a Regular Expression by selecting it from the associated pull-down list.

NOTE: Use the asterisk (*) as the wildcard character.
**Find** is executed by selecting the flashlight icon or by selecting the `<Enter>` key after the search data.

The **Find** toolbar is displayed and hidden using either the **Edit** menu or the desktop icon. The list of found objects is displayed or hidden by selecting the **Find Results** icon.

Total number found, total number displayed, and total selected are shown in the bottom left of the **Find** pane.

**Find**

The Find option presents a list of submaps in which the object is found. Click on the column headings to sort the list. Double-click on an entry in the list to bring the submap and selection to that object. **Find** always presents a list and allows the user to choose the submap to open.

**QuickFind**

The QuickFind option, however, opens a submap immediately (without presenting a list) if the search finds just one submap in which the object exists. If the object exists in more than one submap, a list of submaps is displayed.

**Diagnostics**

The new Diagnostics window design shows a tree view in the left-hand pane, with information about the selected branch or leaf in the right-hand pane. The branches are Test, Network, System, Other, MPLS, and Switch Management. Only those branches that are relevant to the selected object are displayed.

A branch node is the color white until it is selected. It changes to a darker color when selected, indicating that it is expanding or retrieving data. When expansion and data retrieval is complete, it changes to a very dark color, indicating that it has completed its task. The color of the node depends on the color preferences you have set on your computer.

The functionality of the **Network**, **System** and **Other** options has not changed from previous releases. The **Test** option has two new tests: **QuickTest** and **QuickTest Critical**. **MPLS** and **Switch Management** are new to Version 7.1.
Test

QuickTest
All interfaces on a device are polled. The status is checked for all managed interfaces, and updated if changed. Ping or SNMP is used, depending on the regular status method.

QuickTest Critical
Only interfaces that are down are polled.

MPLS

MPLS Node View
Available Information: InSeg ifIndex, InSeg Label, Oper Status, Admin Status, OutSeg ifIndex, OutSeg Label, Next Hop.
Note that Oper and Admin status show the cross-connect status.

MPLS Interface View
Available Information: Oper Status, Admin Status, OutSeg ifIndex, OutSeg Label, NextHop.
Note that this view shows only those segments that enter the LSR on the selected interface.

Switch Management

Port View
Available Information: Port Number, Port MAC Address, Spanning Tree Status, IP Status, Forward to MAC(s), IP Address(es), Host Name(s).

Switch Status
Available Information: Port Number, IP Status, Spanning Tree Status.

MAC View
Available Information: MAC Address, IP Address, HostName, Port Number, IP Status.
Inactive Ports

Available Information: Port Number, IP Status, Spanning Tree Status.

NOTE: If a required device is not supported by the MPLS or Switch Management views, please file an enhancement request with Tivoli Support. In general, devices that support the dot1dBridge MIB are supported by the Switch Management views. Similarly, the MPLS views are supported on devices that support the MPLS LSR MIB.

Get Object From Map

This button inserts the object name of an object selected in the map into the name field.

If you have an object selected and use the context-sensitive options (the ones with diamonds) the object name is entered directly into the name field. However, if you use the non-context-sensitive options (such as from the Tools menu) you can easily insert the object name of an object selected in the map into the name field by selecting Get Object From Map.

Object Properties

The new Object Properties window design shows a tree view in the left-hand pane with information about the selected branch in the right-hand pane. The branches are General, Events, and Other. Only those branches that are relevant to the selected object are displayed.

In addition to using Object Properties for node objects, you can also ask for the Object Properties of interfaces, segments, networks and IP Internet.

The branch node is the color white until it is selected. It changes to a darker color when selected, indicating that it is expanding or retrieving data. When expansion and data retrieval is complete, it changes to a very dark color, indicating that it has completed its task. The color of the node depends on the color preferences you have set on your computer.

General

Covers such information as Object Name, Vendor, SNMP Agent, SNMP Supported, SNMP Proxyed, Hostname, IP Status, MPLS, SNMP Address, Location, Object ID, and Contact.

Note that only properties (table rows) relevant for the object are displayed (the top 5 are always displayed).
Events
Shows the time, severity and description of object-specific events.

Other
Displays information such as Description, Interface, Status, IP Address, Network Mask, Link Address, and Interface Type.

Get Object From Map
This button inserts the object name of an object selected in the map into the name field.

If you have an object selected and use the context-sensitive options (the ones with diamonds) the object name is entered directly into the name field.
However, if you use the non-context-sensitive options (such as from the Tools menu) you can easily insert the object name of an object selected in the map into the name field by selecting Get Object From Map.

Event Browser
The Event Browser window was redesigned for consistency and ease of use. The Event Filter dialog was enhanced to include general event filtering for nodes and for events with descriptions. The Trap filter options allow filtering on all trap events, selected trap events, and the exclusion of selected trap events. In addition to filtering on events by Severity, you can now also filter on events by Category. On Windows only, a date and time filter was added, allowing the display of events before or after a specified date and time.

Use the View option on the Event Browser menu to Pause and restart dynamic event refresh. Use View → Columns... to configure the columns you want to see in the Event Browser. Double-click on an event, or select Event → Details from the Event Browser menu to see more detailed information about an event.

To begin filtering in the Event Browser, select the Filter icon, or select Filter → Set from the Event Browser menu bar. The Event Browser filtering window is displayed. The three filtering categories are General, Traps, and Other.
General

In the General window, you can select **Events for Nodes**. Add the name of a node and select **Add**. The node name is added to the list. You can also select **Events with Description** and enter a description of the particular event you want to filter.

On Windows, you can further filter on the date and time of the event by choosing to view all events that happened before, after, or before and after a certain date and time.

Traps

In the Traps window, if the checkbox is not selected, all traps are activated. To select traps to be included, select the checkbox, select the **Include Events for Selected Traps** option, then select the traps to be included. To select traps to be excluded, select the checkbox, select **Exclude Events for Selected Traps** from the drop-down list, and select the traps to be excluded.

Other

In the Other window, select **Events with Categories** to filter on specific Categories. Select the categories you want to filter. You can also select **Events with Severities**, and choose the severities to filter.

Event Browser Rulesets (UNIX Server only)

A list of ruleset names appears in the Event Browser's drop-down list (All Events is the default) when connected to a UNIX Web Server. Selecting a ruleset will filter events using that ruleset. This includes support for **Resolved** events which will be removed from the event display. A limit of five rulesets can be active per server (selected in any Web Console connected to the same server) at one time. One copy of the rectrap process is started to communicate with nvcorrd, for each ruleset that is active in a Web Console attached to that server (one per active ruleset, not per active ruleset per console). The **All Events** option displays all events with no ruleset filtering.

Additional filtering occurs for criteria selected in the Filter dialog and for scoped accounts.

**Additional Information:**

© In the Web Console Event Browser, user-defined categories will be displayed in the event display as integers, not text names. Also, it is not
Currently possible to filter on user-defined categories in the Web Console Event Browser.

Server Status

From the Tools option in the Web Console main menu, the Server Status window now allows column sorting, repositioning and resizing.

View Logs

The View Logs option has been removed from the Web Console's Tools menu. Log viewing is done through a browser. To view NetView Logs and Jetty Logs, go to the following Web addresses:

http://<hostname>:8080/netview/logs
http://<hostname>:8080/jetty/logs

Log on with a user name and password that has the correct permissions to view these log files.

For more information about log files, see See “New Log Files” on page 60 and “Logging” on page 42. For more information on log file security, see “About Realms” on page 41.

mibExpr.conf file for UNIX

The mibExpr.conf file has been enhanced to contain the same expressions as are available on Windows.

Move and Rename nv6000.log (UNIX only)

The Tivoli NetView console log file has been renamed and relocated. Traditionally, the log files generated by the NetView console were placed in a user's home directory and called nv6000.log. A user had the option to give the log file a different name via the Tivoli Management Framework NetView startup dialog. These log files have been renamed and relocated for easier maintenance. The files for all users are now stored in the /usr/OV/log directory and given the name netview_$LOGNAME.log, where $LOGNAME is the user's UNIX login account name. The user still has the option of renaming the log file at startup.
**Xcolormap Exhaustion (UNIX only)**

When attempting to run the NetView program on a system that has limited available color cells in the X colormap, a problem can occur where the colors needed by the NetView program cannot be allocated. In past releases, such colormap exhaustion would result in either an inoperable network map or in icons resorting to either black or white. In the Tivoli NetView Version 7.1 program, color approximation now occurs when the colormap becomes exhausted. When colors have to be approximated, the NetView program displays a warning dialog to the user indicating this, and enters a warning message in the user’s NetView log file, `/usr/OV/log/netview_$LOGNAME.log`.

**Tivoli Event Console Adapter**

The Tivoli Event Console configuration files and rules have been modified to include the Router Fault Isolation (RFI) events.

One additional step is required on the Tivoli Event Console itself for the Tivoli Event Console Adapter to work correctly with the RFI events. The file `rfi.rls` located in `/usr/OV/conf` must be moved over to the Tivoli Event Console machine and added as a ruleset to the active Tivoli Event Console rule base (wimprbrules).

Mapping between NetView RFI events and Tivoli Event Console classes is:

<table>
<thead>
<tr>
<th>Event</th>
<th>Tivoli Event Console Class</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>NETREACH_EV</td>
<td>NV_Subnet_Reachability</td>
<td>severity=HARMLESS</td>
</tr>
<tr>
<td>NETUNREACH_EV</td>
<td>NV_Subnet_Reachability</td>
<td>severity=CRITICAL</td>
</tr>
<tr>
<td>ROUTERUP_EV</td>
<td>NV_Router_Status</td>
<td>severity=HARMLESS</td>
</tr>
<tr>
<td>ROUTDOWN_EV</td>
<td>NV_Router_Status</td>
<td>severity=FATAL</td>
</tr>
<tr>
<td>ROUTMARG_EV</td>
<td>NV_Router_Marginal</td>
<td>severity=FATAL</td>
</tr>
<tr>
<td>ROUTUNREACH_EV</td>
<td>NV_Router_UnReachable</td>
<td>severity=CRITICAL</td>
</tr>
</tbody>
</table>

The third varbind of each event that contains the trap description maps to the standard Tivoli Event Console slot named `msg`. The rules have been written so that the following is true:

- One and only one copy of the following events is displayed:
  ROUTDOWN_EV, ROUTUNREACH_EV, ROUTMARG_EV, and NETUNREACH_EV.
- A ROUTDOWN_EV event will cancel out a ROUTMARG_EV event and vice-versa.
A ROUTERUP_EV event will cancel out ROUTDOWN_EV, ROUTMARG_EV, and ROUTUNREACH_EV events. The ROUTERUP_EV event itself is not displayed on the Tivoli Event Console.

A NETREACH_EV event will cancel out a NETUNREACH_EV event. The NETREACH_EV event itself is not displayed on the Tivoli Event Console.

The following commands can be used to trigger RFI events in substitution for actually triggering such events by bringing down routers, networks, etc.

```
event -b openview -e ROUTERUP_EV -a "0 269" -h "<none>" -d "Network 146.84.242.0 UP, mask(255.255.255.0)"
```

```
event -b openview -e NETREACH_EV -a "0 269" -h "<none>" -d "Network 146.84.242.0 Unreachable, mask(255.255.255.0)"
```

```
event -b openview -e ROUTDOWN_EV -a "0 269" -h "<none>" -d "Network 146.84.242.0 Down, mask(255.255.255.0)"
```

```
event -b openview -e ROUTMARG_EV -a "0 269" -h "<none>" -d "Network 146.84.242.0 Marginal, mask(255.255.255.0)"
```

```
event -b openview -e NETUNREACH_EV -a "0 269" -h "<none>" -d "Network 146.84.242.0 Unreachable, mask(255.255.255.0)"
```
New Log Files

<table>
<thead>
<tr>
<th>File Path</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>/usr/OV/file</td>
<td></td>
</tr>
<tr>
<td>log/securityconsole.log</td>
<td>Web Console Security window activity</td>
</tr>
<tr>
<td>log/seededitor.log</td>
<td>Seed Editor activity</td>
</tr>
<tr>
<td>log/snmpserver.log</td>
<td>snmpserver activity</td>
</tr>
<tr>
<td>log/virtualdesktop.log</td>
<td>Virtual Desktop activity*</td>
</tr>
<tr>
<td>www/logs/&lt;date&gt;.request.log</td>
<td>Web Console activity</td>
</tr>
<tr>
<td>www/logs/netviewservlets.log</td>
<td>Web Console Servlet activity</td>
</tr>
<tr>
<td>www/logs/filechecker.log</td>
<td>Reports on validity of security files**</td>
</tr>
</tbody>
</table>

* Virtual Desktop: The Virtual Desktop is used to launch Java applications such as MIB Loader, Web Console Security window, and Seed Editor from the native console. It is not visible to the user in any way.

** Filechecker: The Filechecker is used to verify the contents of files used or generated by the Web Console Security window. It is not visible to the user in any way, other than by generating error dialogs if something is incorrect in their files.

nvsniffer Changes

nvsniffer for Windows

Two new flags have been added to the nvsniffer application:

- **-m**
  Optionally, force the nvsniffer command to execute even if another instance of nvsniffer is already running. Use this option sparingly since each instance of nvsniffer can consume significant system resources.

- **-p phymem**
  Optionally specify the maximum amount of virtual memory (in megabytes) that the Java Virtual Machine (JVM) running the nvsniffer application should occupy. The value specified for this option is not validated by nvsniffer; it is passed directly to the JVM.
that will execute the nvsniffer application. Tivoli recommends avoiding values higher than 64, especially if the \texttt{-m} option is used.

For further information about these flags, refer to “Additional NetView Information” on page 65 and read the bullet item that refers to Java-based applications.

\textbullet\ The nvsniffer application no longer supports the use of extension DLLs containing the NvServiceTest() API as custom plug-in modules. The following changes have been made:

\textbullet\ A deprecated version of nvsniffer named \texttt{nvsniffer-DEPRECATED.exe} is included in this release but is not supported by Tivoli Systems, and will not be included in future releases. It includes the ability to use extension DLLs containing the NvServiceTest() API, and is included for migration purposes only.

\textbullet\ The two associated program samples, \texttt{\usr\ov\prg\samples\nvsniffext} and \texttt{\usr\ov\prg\samples\nvsniffext2}, are no longer installed.

\textbullet\ A deprecated version of the example extension DLL is included as \texttt{\usr\ov\bin\snmpsni f fext-DEPRECATED.dll} but is not supported by Tivoli Systems, and will not be included in future releases. It is included for migration purposes only.

Please ignore all references to the use of extension DLLs as custom plug-in modules and all references to the NvServiceTest() API in section \textit{Managing the nvsniffer.conf File} and in section \textit{Using Custom Plug-In Modules for Discovery and Status Checking} in Chapter 8 of the \textit{NetView for Windows User’s Guide}, and also on the nvsniffer reference page in Chapter 2 of the \textit{NetView for Windows Programmer’s Reference}.

\textbf{NOTE:} Launchable tasks are still supported as custom plug-in modules for nvsniffer.

\textbf{Other nvsniffer for Windows Changes}

Quotation marks are no longer required for the \texttt{(Service SmartSet)} or \texttt{(Service Label Name)} fields in the nvsniffer configuration files. Extra white space and quotation marks are ignored.

A few new entries are included in the default nvsniffer configuration file located at \texttt{\usr\ov\conf\nvsniffer.conf}. If you are upgrading from a previous version of the NetView program, the existing \texttt{nvsniffer.conf} file is not automatically migrated to the new format – it is archived to the
The new default configuration file is located in the \usr\ov\conf\nvsniffer.conf directory. The new default configuration file is located at \usr\ov\conf\nvsniffer.conf, and it contains the equivalent entries provided in the default file installed by previous releases of the NetView program. Customizations made to your existing file will need to be migrated by hand to the new file format.

The file \usr\ov\doc\nvsniffer.readme is no longer installed; references to this file in the online help and in the NetView for Windows Programmer’s Reference should be ignored. Please reference Chapter 8 of the NetView for Windows User’s Guide instead.

The default timeout for tests to complete has been reduced from 120 seconds to 10 seconds. The -T <timeout_value> switch is also now applied to raw TCP port tests as well as to launchable tasks. Some platforms do not allow raw TCP port tests to be preempted. For these platforms, if the timeout value is exceeded while performing the raw TCP port tests to a single node than any remaining port tests to that node are skipped and a warning is issued. The NetView for Windows Programmer’s Reference incorrectly states that the -T switch is applied to launched tasks only.

The online help incorrectly states that the maximum value for the -t <numThreads> switch is 300. The actual maximum value is 50.

The NetView for Windows Programmer’s Reference incorrectly states that the maximum value for the -T <timeout> switch is 300. The actual maximum value is 120.

The -c <configFile> switch can also be specified using -f <configFile>.

Chapter 8 of the NetView for Windows User’s Guide incorrectly states that some messages are logged to the \usr\ov\log\nv.log file. All nvsniffer errors and warnings are logged to stdout and, if specified, to the file designated by the -l switch.

nvsniffer for UNIX

The nvsniffer application has been enhanced to have equivalent functionality to the NetView Windows version. The format of the configuration file has changed and is documented in the nvsniffer manpage. If you are upgrading the NetView program, the existing nvsniffer.conf is not automatically migrated to the new format due to the complexities involved. The new default configuration file is located at /usr/OV/conf/nvsniffer.conf, and it contains the equivalent entries provided in the default file installed by previous releases of the NetView program.
Customizations made to your existing file will need to be migrated by hand to the new file format (note the location of the nvsniffer.conf file in previous NetView releases was /usr/OV/conf/nvdbtools/nvsniffer.conf).

Please review the nvsniffer manpage for details on how to use the new capabilities, or enter nvsniffer -h at a command prompt for brief usage information.

The enhanced nvsniffer can reschedule itself for automatic restarts using the -r switch; this capability uses the at command. To remove a scheduled nvsniffer job, use the at -l command to view all scheduled jobs, then use the at -r command to remove the specific jobs that you no longer want scheduled. The NetView program uninstall process does not automatically remove any scheduled nvsniffer jobs.

A new program sample has been included to demonstrate nvsniffer’s ability to launch custom plug-in modules for discovering and monitoring the status of services. The program sample includes a README file and Makefiles. It is located at /usr/OV/prg_samples/launchport. This program sample performs the same standard raw TCP port test as is performed internally by nvsniffer.

When using custom plug-in modules, if you cannot guarantee that your module is thread-safe, type the -t switch with a value of 1 to limit nvsniffer to using one worker thread.

Two new flags have been added to the nvsniffer application:

- **-m** Optionally, force the nvsniffer command to execute even if another instance of nvsniffer is already running. Use this option sparingly since each instance of nvsniffer can consume significant system resources.

- **-p physmem** Optionally specify the maximum amount of virtual memory (in megabytes) that the Java Virtual Machine (JVM) running the nvsniffer application should occupy. The value specified for this option is not validated by nvsniffer; it is passed directly to the JVM that will execute the nvsniffer application. Tivoli recommends avoiding values higher than 64, especially if the -m option is used.

For further information about these flags, refer to “Additional NetView Information” on page 65 and read the bullet item that refers to Java-based applications.
New Varbind on Some NetView Enterprise Traps

In order to facilitate integration with other event-handling products, a sixth Varbind is added to traps that netmon generates for topology objects. This varbind contains the OVw selection name of the object the trap refers to, which the NetView program uses to uniquely identify the object.

New OVw Field Network Address for Network Object

The network object uses the field IP Address for the IP network address. This causes a conflict with the IP Address field in the Interface object when 32 bit addressing is used so that the network address is the same as the host address. A new field has been added to the network object called Network Address that holds the full IP network address, such as 10.1.20.0.

Additional netviewd Information for UNIX

SmartSet Behavior

When the netviewd daemon is in use, it automatically populates the SmartSet submaps.

This behavior is controlled by an environment variable, NVUNATTENTENTED, which is set by the netviewd daemon and is invisible to the user. If the collmap application detects the existence of this environment variable, it populates the SmartSet submaps automatically on startup.

Application Startup Behavior

When the NetView console is running as netviewd, it starts only those applications that have the flags -Initial and -Restart set in the Command construct of the registration file.

If one of these applications exits prematurely, the netviewd daemon attempts to restart it. The netviewd daemon first checks if the application is restartable prior to restarting it. If the application is dependent upon one or more daemons being running, netviewd checks the daemons’ run states before starting the application. If the daemons are not running, netviewd checks if they are registered in the /usr/OV/conf/ovsuf file. If they are not registered, netviewd discontinues attempts to restart the application. An
environment variable called NVRESTARTINTERVAL can be set to adjust the interval used between restart attempts. The default restart interval is 5 minutes.

Multiple Maps with netviewd

It is possible to have multiple netviewd daemons running on a single server, each with a different map. You can accomplish this by creating a new lrf file for each netviewd that you want to run, each with a different map specified.

Example:

1. On a command line, change directory by typing: `cd /usr/OV/lrf`
2. Copy the original lrf file by typing: `cp netviewd.lrf netviewd_<map name>.lrf`
3. Edit the file `netviewd_<map name>.lrf`
4. Replace the first `netviewd` on the first line to be `netviewd_<map name>`
5. Add `-map <map name>` to the command line options just before the `-spmd` option.
6. Save the file.
7. Enable the daemon: `/usr/OV/bin/ovaddobj /usr/OV/lrf/netviewd_<map name>.lrf`
8. Start the daemon: `/usr/OV/bin/ovstart netviewd_<map name>`
9. From now on, you can type `netview-dconsole -map <mapname>` to open a specific map.

Additional NetView Information

- On Solaris and AIX, no visual indication is given when a service is no longer supported for a node. It is marked in the object database and will be removed from the collection after seven days.
- UNIX: In order to use native UNIX security in conjunction with the Web Console, a UNIX root user must be logged in to NetView security (nvauth).
- In the native NT NetView application, regardless of how many nodes you select to ping, only five Ping windows are displayed. The Web Console
does not have this limit of five nodes. If you request to ping more than five nodes in the Web Console, you might get out-of-memory errors, depending on your system resources.

If you notice that Demand Polls and QuickTests are not completing because the network monitor (netmon daemon) on the server is not responding, or if you notice that certain expected traps are not arriving in the events display in a timely fashion, stop and restart the NetView daemons. Be aware that this may leave rogue ndemandpoll and quicktest processes that will exit only if you reboot or if you kill the processes.

Several Java-based applications are included in the NetView 7.1 kit. Each of these applications executes within its own Java Virtual Machine (JVM). Under normal operations, these applications are designed to run harmoniously with all other NetView applications.

Each JVM is allowed to consume virtual memory (primarily heap space) up to a system-specific default or up to a limit specified in the command syntax used to launch the JVM in which the Java application runs. Several of the NetView Java applications specify an explicit maximum in their Java launch syntax using the `-Xmx###m` command switch, where `###` is the maximum size (in megabytes) of virtual memory that the JVM is allowed to consume.

Because it is possible to simultaneously run multiple instances of many of the Java-based applications, there is a risk of using all available virtual memory on a system. Great care must be taken to avoid this condition, as the behavior of the NetView applications can become unpredictable, especially the Java-based applications. Symptoms of this issue include occurrences of Dr. Watson errors, exceptions on NetView/NT and Windows 2000 systems, and the creation of Javacore stack dumps. Overall system performance degrades as the amount of available memory resources decreases.

Since the nvsniffer application has the capability of rescheduling itself (via the `-r` option), it has a built-in feature to prevent more than one instance of itself from running at a given time. This restriction can be overridden using the `-m` switch, but this option should be used sparingly. In addition, the nvsniffer `-p` option allows you to override the default virtual memory maximum used by the JVM. The default value is system-specific, but it generally ranges from 64 to 128 megabytes. Using a smaller value such as 32 or 16 on systems with less physical memory reduces the risk of the system running out of available memory resources. Be aware
that specifying a value that is too small for the number of managed IP nodes in the NetView database increases the risk that the nvsniffer application will run out of memory.

Tivoli recommends that the `-Xmx###m` command switch in the launch syntax for all Web Console-related processes not be modified from their original settings, as these values have been tuned to fit the needs of most working environments.

© A fix has been made to ovactiond, nvcorrd and actionsvr to close up a potential security hole where any non-authorized user, with some knowledge of NetView trap customization, could gain root access to the NetView system by sending a trap to the NetView system from anywhere in the network.

This did not happen in the product as it is shipped, but could occur after trap customization was done by the NetView administrator or anyone with root authority on the NetView system. The security hole was opened when a trap was customized to include a variable in the Command for Automatic Action field. A trap could then be sent from any system using command substitution, rather than the intended variable, to execute unauthorized operating system commands on the NetView system.

The UNIX daemons impacted by this fix are ovactiond, nvcorrd and actionsvr. The Windows daemons impacted by this fix are nvcord and trapd. These daemons now filter out all non-alphanumeric characters except for the minus sign (-) and the decimal point (.). All characters not falling into this set are replaced with an underscore. If a minus sign or decimal point is encountered, it is escaped (preceded by a backslash) as a precaution.

If any non-alphanumeric character is encountered (and filtering is not disabled), a message is logged to the appropriate log file (if logging is enabled). On UNIX, the log files are `/usr/OV/log/nvcorrd.alog`, `/usr/OV/log/ovactiond.log`, and `/usr/OV/log/nvaction.alog`. On Windows, the log files are `\usr\ov\log\nvcorrd.alog` and `trapd.log`.

A list of the modified characters follows:

$ ' ; & | @ # % ^ < > / \ = { } - " !

When these characters are encountered, a message is entered into the appropriate daemon log file.

This list of filtered characters can be configured by creating a variable (UNIX) or a registry variable (Windows) called
AdditionalLegalTrapCharacters. If you set this variable to disable, then no filtering is done. If you set the variable to a string containing non-alphanumeric characters, then the filtering allows those characters to pass through the filter, but they will be escaped.

Stop and restart the NetView daemons after setting the variable.

NOTE: On UNIX, the best way to set an environment variable for an ovspmd-controlled daemon is to put the definition of the environment variable into the /usr/OV/bin/netnmrc.pre file.

Deprecated Components

The following list of components no longer seem useful and will be deprecated in a future release:

On UNIX

- Backup
- Openmon
- OVORS/CMOT support (XMP)
- noniptopod

On Windows

- topo2sql

On UNIX and Windows

- netmon: HP and AIX SNMPSets (trap destination, for example)

CiscoWorks 2000 Integration

Tivoli NetView supports the CiscoWorks 2000 integration model. This release ships with the necessary adapters in the Adapters/Cisco directory of the NetView installation CD-ROM. The README files in each of those directories provides directions for performing the integration. More information about these procedures and the overall integration model can be found on the Cisco Web site at http://cisco.com/warp/customer/cc/cisco/mkt/enm/cw2000/tech/cwnms_tb.html (CCO login is required).
NOTE: Currently, there is a problem with proper launching of Cisco applications with Netscape Version 4.76 on UNIX. Check the Cisco and Tivoli support websites periodically for updates on this problem.

A temporary workaround, until changes are made to the Cisco launch script, is as follows.

Open the /opt/CSCOpx/bin/invokebrowser.sh file.

Find the following lines:

```
$BROWSER -remote "openUrl($1, new-window)"  2> /dev/null
if [ $? != 0 ]; then
  $BROWSER $1
fi
```

and change them to this:

```
$BROWSER -remote "openUrl($1, new-window)"  2>$$
if [ $? != 0 -o -s $$ ]; then
  $BROWSER $1
fi
rm $$
```

Tivoli Business System Manager Adapter V1.1

The Tivoli Business System Manager (TBSM) Adapter Version 1.1 for Tivoli NetView is installed after installing the NetView program. It is included on the NetView distribution media and is supported on the following platforms:

- Windows NT 4.0
- Windows 2000
- AIX 4.3.3.10

TBSM provides a consolidated view of network and system information from a variety of IBM products to present a single management interface. The NetView program uploads network management data via the adapter to the TBSM server and is dynamically maintained. This is offered as a service. For more information please contact your local IBM/Tivoli representative.
Installing the NetView Program on Windows

This section describes how to install the Tivoli NetView program. It also describes the hardware, software, and system configuration requirements for the Tivoli NetView program. In addition, this section describes some additional information that might be needed, depending on your configuration.

After verifying that your system meets the installation and system requirements listed in “Installation and System Requirements” on page 71, you can go directly to one of the following sections:

- “Installing the NetView Server or Standalone” on page 73
- “Installing the NetView Client” on page 75
- “Installing the NetView Web Console” on page 110

Refer to the following sections for supplemental information as required:

- “Migrating from a Previous Version of the NetView Program” on page 76
- “The Installation Process” on page 77
- “Creating NetView Accounts on the Server” on page 78
- “SQL Databases” on page 79
- “Microsoft SQL Server” on page 79
- “Installation Problems” on page 80

If you already have the NetView program on your system, please ensure that it is not running during your installation.

If you have a previous version of the NetView program installed, you will be asked if you want to perform an upgrade installation or a fresh installation. Use the upgrade installation to preserve your existing databases and configuration files. The fresh installation will replace your existing NetView program.
Installation and System Requirements

Before installing the NetView program, ensure that your system meets the following specifications.

Hardware Requirements

<table>
<thead>
<tr>
<th>Product</th>
<th>Minimum Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC</td>
<td>Intel Pentium II class machine</td>
</tr>
<tr>
<td>RAM*</td>
<td>256 MB (512 MB recommended)</td>
</tr>
<tr>
<td>Paging File Space*</td>
<td>Double the RAM figure set above.</td>
</tr>
<tr>
<td>Disk Space: Install Drive*</td>
<td>170 MB</td>
</tr>
<tr>
<td>Drives</td>
<td>NTFS or FAT drive or partition that supports long file names</td>
</tr>
<tr>
<td>Cards</td>
<td>Network adaptor card and network connection</td>
</tr>
<tr>
<td>Graphics Card</td>
<td>SVGA</td>
</tr>
<tr>
<td>Monitor</td>
<td>1024 x 768 pixels x 256 colors (1280x1024 recommended)</td>
</tr>
<tr>
<td>For NetView Microsoft Access Database Space</td>
<td>partition with at least 250 MB of available disk space</td>
</tr>
<tr>
<td>For NetView Microsoft SQL Server Database</td>
<td>partition with at least 250 MB of available disk space.</td>
</tr>
</tbody>
</table>

**NOTE:** On Windows platforms, configurations of up to 13,000 nodes and 10 simultaneous Web Console displays have been tested. Please contact Tivoli Support for the latest capacity recommendations before deploying configurations larger than this.

*Additional memory for large networks will improve NetView performance. Tivoli recommends 1 gigabyte of memory for a network configuration similar to that described in the above Note.
Software Requirements

<table>
<thead>
<tr>
<th>Product</th>
<th>Minimum Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>NT</td>
<td>Version 4 with Service Pack 5 (Workstation or Server)</td>
</tr>
<tr>
<td>Windows 2000</td>
<td>Service Pack 1 (Professional or Server)</td>
</tr>
<tr>
<td>TCP/IP Protocol</td>
<td>Installed and configured</td>
</tr>
<tr>
<td>SNMP Service</td>
<td>Installed and configured</td>
</tr>
<tr>
<td>SNMP Trap Service</td>
<td>Installed and configured</td>
</tr>
<tr>
<td>ODBC</td>
<td>V3.51 or later</td>
</tr>
<tr>
<td>Optional: SQL Server®</td>
<td>Version 6.5, 7.0 or 2000</td>
</tr>
</tbody>
</table>

NOTE: Windows XP is not supported in this release.

Browser Requirements

Ú Netscape® Version 4.5 or Microsoft Internet Explorer® Version 5.0.

Before Installing the Tivoli NetView Program

Ú Back up the NetView databases by stopping all NetView daemons and making a copy of everything in the \usr\ov\databases directory.

Ú Ensure that the following applications are stopped:

· Web Console
· Web Console Security
· MIB Loader
· MIB Browser
· Netmon Seed Editor
· Tivoli Event Console Adaptor Configurator
Installing the NetView Program

After verifying that your system meets all the hardware and software requirements listed in “Installation and System Requirements” on page 71, log on as a member of the Windows Administrators group.

Before installing the NetView program, close all Windows Explorers, command prompts, and any other applications that might be holding a NetView installation directory open.

Insert the NetView installation media in the CD-ROM drive.

NOTE: If the autorun dialog does not display, select Run from the Start menu. In the Command Line box, type:

```
e:\NetView\i386\setup.exe
```

Replace “e” with the drive letter of your CD-ROM drive.

The Tivoli NetView Installation window is displayed. The following options are available:

- Install Tivoli NetView
- Install Web Console Only
- Install Attended MLM
- Read Release Notes
- Exit

Proceed to “Installing the NetView Server or Standalone” on page 73 or “Installing the NetView Client” on page 75.

Installing the NetView Server or Standalone

To install the NetView Server, follow these steps:

1. Select Install Tivoli NetView. A Setup window is briefly displayed, followed by a Welcome window.

2. When you have read the Welcome window, select Next.

3. If this is the first time that the NetView Version 7.1 program has been installed, you must read and accept the software license agreement to proceed. Select Accept to accept the agreement.

4. Enter your Name and the name of your Company and select Next.
5. If the setup program detects that a copy of the NetView program exists on your system, you have the option of performing either an upgrade installation or a fresh installation. Select **Upgrade Existing Installation** or **Perform Fresh Installation**. If the setup program does not detect a copy of the NetView program on your system, a fresh installation is automatically performed. Select **Next** to continue.

**NOTE:** If the installation has been previously upgraded, or if a previous upgrade installation failed, you will be asked which directory you want to upgrade from (`\usr\ov` or `\usr\ov_00`). If the previous upgrade was successful, select `\usr\ov`. If the previous upgrade was not successful, select `\usr\ov_00`.

6. In the Choose Destination Drive window, select the drive on which to install the program. Note the **Space Required** and **Space Available** information at the bottom of the window. An upgrade installation does not display this window because the upgraded NetView remains on the original installation drive. Select **Next** to continue.

7. If you chose **Upgrade Existing Installation** in Step 5, the available options for a server will be Standalone and Server. Select **Server** or **Standalone**, then select **Next** to continue.

   The **Server** selection creates a fileshare for the root directory of the drive where the NetView program is installed. By default, access is restricted to the **NetView** account. The Server selection allows access by both native clients and Web Console clients.

   The **Standalone** selection does not support native clients, but does support Web Console clients.

8. Enter a password for the NetView account. Retype the password to confirm it. Select **Next** to continue.

9. In the Enter Community Names window you have the option of entering a few read-only SNMP community names. Do not enter the default community name. Select **Next** to continue.

10. The NetView installation program proceeds. A progress bar shows the completion percentage and text messages show the progress of the installation.

11. The Setup Complete window offers you the choice of restarting your computer now or later. You must restart your computer before running the NetView program, but you do not have to do it immediately. Select **Finish** when you have chosen to restart the computer now or later.
12. After you have restarted the computer, double-click the Tivoli NetView icon on the desktop to start the native NetView application.

Installing the NetView Client

To install the NetView Client, follow these steps:

1. Select **Install Tivoli NetView**. A Setup window is briefly displayed, followed by a **Welcome** window.

2. When you have read the Welcome window, select **Next**.

3. If this is the first time that the NetView Version 7.1 program has been installed, you must read and accept the software license agreement to proceed. See “Installing the NetView Client” on page 75 for more information. Select **Accept** to accept the agreement.

4. Enter your Name and the name of your Company and select **Next**.

5. If the setup program detects that a copy of the NetView program exists on your system, you have the option of performing either an upgrade installation or a fresh installation. Select **Upgrade Existing Installation** or **Perform Fresh Installation**. If the setup program does not detect a copy of the NetView program on your system, a fresh installation is automatically performed. Select **Next** to continue.

   **NOTE:** If the installation has been previously upgraded, or if a previous upgrade installation failed, you will be asked which directory you want to upgrade from (\usr\ov or \usr\ov_00). If the previous upgrade was successful, select \usr\ov. If the previous upgrade was not successful, select \usr\ov_00.

6. In the Choose Destination Drive window, select the drive on which to install the program. Note the **Space Required** and **Space Available** information at the bottom of the window. An upgrade installation does not display this window because the upgraded NetView remains on the original installation drive. Select **Next** to continue.

7. In the NetView Setup window, enter the IP address of the server that this client will use. Select **Next** to continue.

8. In the Password window, enter the password for the NetView account on the Server. Select **Next** to continue.
9. The NetView installation program proceeds. A progress bar shows the completion percentage and text messages show the progress of the installation.

10. The Setup Complete window offers you the choice of restarting your computer now or later. You must restart your computer before running the NetView program, but you do not have to do it immediately. Select **Finish** when you have chosen to restart the computer now or later.

11. After you have restarted the computer, double-click the Tivoli NetView icon on the desktop to start the native NetView application.

**IBM License Agreement**

The Software License Agreement is displayed at the beginning of the installation. The user is prompted to Accept or Decline the license agreement. The Agreement must be accepted before proceeding with the installation. The text of the license is available in the file `\usr\ov\license\V7.1\English.txt`.

The user is prompted only once to accept the license agreement for the same version of the NetView program. However, if the program is uninstalled and reinstalled, the user is again prompted to accept the license agreement.

**Migrating from a Previous Version of the NetView Program**

The Tivoli NetView program supports migration from Version 5.1 and later. If you are migrating from a previous version, the upgrade installation will save a copy of your customized files from the NetView directory in the `\usr\ov_00` directory.

Tivoli recommends backing up your system before any migration or installation is performed.

During migration, some files are replaced, some are archived, and some are migrated.

The archived files are user-customizable files that are copied to the V51_archive, V6_archive or V601_archive directory, depending on what version you are upgrading from. These files are replaced with updated versions of the files, and desired customizations must be merged back in.
The migrated files are user-customizable files in which the customizations are preserved. The following files are migrated from your old version to Version 7.1 when you perform an upgrade installation:

- /usr/ov/conf/location.conf
- /usr/ov/conf/netmon.seed
- /usr/ov/conf/trapd.conf
- /usr/ov/conf/snmpcol.conf

As a general rule, the following files are migrated:

- Third-party files
- Most files in the following directories:
  - /usr/ov/conf
  - /usr/ov/databases
  - /usr/ov/filters
  - /usr/ov/lrf
  - /usr/ov/reg
  - /usr/ov/registration

The exceptions are non-user-customizable files and files that are archived. All of your database files (all files in the /usr/ov/databases directory) are preserved.

**The Installation Process**

The installation updates the registry with the following NetView environment variables:

APPMON_TIMER_SEC, MIBDB, MIBFILES, NLSPATH, NVSNMP_CONF, NV_DRIVE, NV_TCL, OVwHelpDir, SNMPCOLLECTDIR, SNMPCOL_CONF, TCL_LIBRARY, TRAPD_CONF, TRALERTD_CONF.

The PATH environment variable is modified to include /usr/ov/bin.

The Tivoli NetView program menu (available from the Windows Start menu), with icons for the most common NetView programs, is created by the installation.

The port numbers used by the NetView program are added to the \<winnt>\system32\drivers\etc\services file. If any of these port numbers are used by other applications, a message box will ask you to manually update the file. Examine the nvinstan.log file for details on how to edit the file manually if problems are encountered during installation.
The `/usr/tivolog/nvinstall.log` file tracks the progress and records the details of the installation. From the Windows **Start** menu, go to **Programs** → **Tivoli NetView**. Then select **Installation** → **Installation Log** to display this log file.

## Creating NetView Accounts on the Server

When installing the NetView program, the installation procedure will create a local account on the machine to run the NetView Service. The user performing the installation must have sufficient local administrator privileges to create the account. The NetView account has local administrator privileges and the *log on as a Service* right.

If your account administration policy requires that a domain account be used for the NetView Service account, be sure that this account is created with sufficient local privileges to act as an Administrator and to log on as a Service. Incorrect local authority can cause the NetView Service to fail on startup.

For performance reasons, it is not advisable to install the NetView program on a domain or backup domain controller. However, if you do, the installation tries to create a NetView account on the local machine. This is acceptable on a primary domain controller, but you cannot create an account, local or domain, on a Windows backup domain controller. To install the NetView program on a backup domain controller, first create a NetView domain account.

The installation process can be told to use the existing account by setting the environment variable `nvoptions` to the string `SaveUserAccount` in the process where the installation will be performed. This environment variable value provides the same functionality as the `-nu` parameter available in the TME 10 NetView for NT V5 installation.

Then, install the NetView program from a command prompt window in the NetView kit directory by entering the following command:

```bash
setup.exe
```

This command installs the NetView program using an existing NetView account.
Manually Creating the NetView Account on the Server

If you are manually creating the NetView account, ensure you do the following:

1. Place the NetView account in the Administrator group.
2. In the User Manager, select:
   Policies -> User Rights. Then select Advanced User Rights -> Log on as a Service.

SQL Databases

If the Structured Query Language (SQL) Server is not installed, the NetView program uses Access databases (Jet engine) and installs the drivers, if necessary. If SQL Server is installed, but you want to use Access instead, set the environment variable DATABASE_TYPE to ACCESS using the System icon on the Control Panel before installing the NetView program.

If the NetView server is running SQL Server, clients can connect remotely to the SQL Server. The SQL Server does not need to be installed on the NetView client.

Updating ODBC Components and Access Drivers

The NetView program requires ODBC V3.51 or higher. These drivers can be installed using MDAC 2.0 or higher. For more information about Microsoft Data Access Components 2.0, see http://www.microsoft.com/data.

Additional Information:

© If you have difficulty running the nvdbexport utility – specifically, if you receive abnormal program termination or Couldn’t create database Exception, install Microsoft DAO version 3.5, which is shipped on the NetView CD, and is known to be compatible with nvdbexport.

Microsoft SQL Server

This section contains information pertinent to the Microsoft SQL Server.
**SQL Server Licenses**

When using the SQL Server in a client/server NetView environment, be sure that the SQL Server has sufficient licenses; one for each attached client and one for the server.

**SQL Server Configuration**

You may need to perform the following additional configuration tasks:

- For SQL Server Version 6.5 only, if you anticipate many events (20,000 or more), increase the size of the `tempdb` database. A reasonable size is 50 MB for this situation.

- The file `\usr\ov\databases\odbc\create_sqldb.bat` (or `create_sqldb7.bat` for SQL Server Version 7.0) is used by the installation process to create the SQL Server devices, databases, and database schemas used by the NetView program.

- The SQL Server value for Maximum User Connections is set to 30. If you are using a large number of clients, increase this value. Each NetView console or Event Browser you expect to run will consume two connections.

**Installation Problems**

If you encounter any problems with the installation, refer to the *Tivoli NetView for Windows User’s Guide*.

**Additional Information:**

- If you install the NetView CNAT Extensions (nvCNAT) V1.* onto a NetView Windows system, the uninstall procedure for the NetView program gets overwritten by the nvCNAT uninstall procedure, which results in the inability to successfully uninstall the NetView software. The NetView/CNAT Extension Version 2.1.0 and higher corrects this problem. But if you rename `WINNT4\system32\NetView\uninstall\Uninst.isu` to something else before installing nvCNAT, you can later use the newly-named .isu file if you need to uninstall the NetView program.

- Fresh installation erases third-party files. To work around this issue, after uninstalling the NetView program, save all directories that remain before performing the installation and copy back the third-party files after the installation is complete.
For migration of the web console from V6.0 to V7.1 we archive the web console configuration files and delete and replace the rest of the web console. User accounts and passwords must be recreated using the new Web Console Security application. For migration of the web console from V7.1 to V7.1.* we migrate the web console configuration files and delete and replace the rest of the web console.

When running the NetView Tivoli Event Console Adapter on a Windows 2000 system, you must first ensure that there is a C:\temp directory. Windows 2000 does not always create this directory by default and the tecd_nv6k executable is dependent upon it.

You must reboot Windows 98 after installing the Web Console in order to see the Web Console folder in the Start menu.
Installing the NetView Program on UNIX

This section describes how to install the Tivoli NetView program. It also describes the hardware, software, and system configuration requirements for the Tivoli NetView program as well as explaining the Tivoli NetView software components. In addition, this section describes some planning questions you need to answer and the tasks you need to perform before you can install the Tivoli NetView program.

All references in this document to server or client refer to the Tivoli NetView server or client unless otherwise specified.

Verify that your system meets the installation and system requirements listed in the following sections:

- “Installation and System Requirements” on page 83

To review your installation strategy, can consult the following sections:

- “About the Tivoli NetView Software Components” on page 90
- “Installation and Configuration Considerations” on page 91

Before you begin your installation, refer to the following sections:

- “Tasks to Complete Prior to Upgrade Installation” on page 94
- “Setting the LANG and LC_MESSAGES Variables” on page 97

You can go directly to the following sections to begin installing the NetView program without using the Tivoli Management Framework:

- “Installing the NetView Program in a non-Tivoli Management Framework Environment” on page 98
- “Installing the NetView Web Console” on page 110

Or you can go to the following sections to install the NetView program using the Tivoli Management Framework:

- “Installing the NetView Program in a Tivoli Management Framework Environment” on page 99

Refer to the following sections for supplemental information as required:

- “Installation Problems” on page 105
- “Installing the Tivoli NetView Mid-Level Manager” on page 113
- “Installing the Tivoli Integration Pack for Tivoli NetView (TIPN)” on page 113

NOTE: The Tivoli NetView program includes the NetView server application, the Tivoli NetView client application, and the NetView
Mid-Level Manager (MLM) application. You are entitled to use an unlimited number of Tivoli NetView clients and Tivoli NetView MLMs with each copy of the Tivoli NetView server purchased.

Installation and System Requirements

Hardware Requirements

The following hardware is required to run the Tivoli NetView program:

<table>
<thead>
<tr>
<th>Product</th>
<th>Minimum Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli NetView Web Console only*</td>
<td>128 MB memory</td>
</tr>
<tr>
<td></td>
<td>(256 MB recommended)</td>
</tr>
<tr>
<td>Server only (native console)*</td>
<td>128 MB memory</td>
</tr>
<tr>
<td></td>
<td>(256 MB recommended)</td>
</tr>
<tr>
<td>Web Console and Server*</td>
<td>256 MB memory</td>
</tr>
</tbody>
</table>

Determine how much memory your current system has as follows:

<table>
<thead>
<tr>
<th>For...</th>
<th>Enter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>`lsattr -E -l sys0</td>
</tr>
<tr>
<td>Solaris</td>
<td>`prtconf</td>
</tr>
</tbody>
</table>
Software Requirements

The following software is required to run the Tivoli NetView program:

<table>
<thead>
<tr>
<th>Product</th>
<th>Minimum Requirements</th>
</tr>
</thead>
</table>
| AIX 4.3.3                      | Maintenance Level 4330-08  
The netviewd daemon requires X11.vfb 4.3.3.0  
Virtual Frame Buffer Software (CD 3 of 4 on the AIX V4.3.3 cd set) |
| Solaris 2.7                     | All Sun-recommended patches                                                           |
| Solaris 2.8                     | All Sun-recommended patches  
Install the en_US.ISO8859-1 locale  
Install the SUNWbtool (Solaris CD 2 of 2) |
| Tivoli Management Framework®   | Version 3.6.3 or higher - required only if installing through the Tivoli Management Framework |

Additional Information:

- If you want to use RIM with NetView 7.1 on Solaris you must use Tivoli Management Framework 3.6.3 and not the 3.7 version of Tivoli Management Framework.

- If you want to install the TIPN Tivoli Event Console Integration adapter on a NetView Server you must use Tivoli Management Framework 3.6.3 and not the 3.7 version of Tivoli Management Framework.

- AIX 5.1 is not supported in this release.

- On Solaris 2.8, a system directory is missing that is required by the Tivoli NetView installation process. You must create the directory `/usr/lib/locate/en_US/LC_MESSAGES` manually if it does not exist in order for the installation to complete successfully.

- The SUNWbtool is required by the installation’s NVprereq check on Solaris machines. Although the Solaris 2.7 development environment installs this tool by default, it is not installed by default with Solaris 2.8.
Disk Space Requirements in /usr/OV

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Product</th>
<th>Installation Type</th>
<th>Minimum Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>NetView Server</td>
<td>Fresh Installation</td>
<td>470 MB</td>
</tr>
<tr>
<td>AIX</td>
<td>NetView Server</td>
<td>Upgrade from V6.0</td>
<td>215 MB</td>
</tr>
<tr>
<td>AIX</td>
<td>NetView Server</td>
<td>Upgrade from V5.x</td>
<td>310 MB</td>
</tr>
<tr>
<td>AIX</td>
<td>NetView Client</td>
<td>Fresh Installation</td>
<td>150 MB</td>
</tr>
<tr>
<td>AIX</td>
<td>NetView Client</td>
<td>Upgrade from V6.0</td>
<td>35 MB</td>
</tr>
<tr>
<td>AIX</td>
<td>NetView Client</td>
<td>Upgrade from V5.x</td>
<td>100 MB</td>
</tr>
<tr>
<td>Solaris</td>
<td>NetView Server</td>
<td>Fresh Installation</td>
<td>530 MB</td>
</tr>
<tr>
<td>Solaris</td>
<td>NetView Server</td>
<td>Upgrade from V6.0</td>
<td>265 MB</td>
</tr>
<tr>
<td>Solaris</td>
<td>NetView Server</td>
<td>Upgrade from V5.x</td>
<td>370 MB</td>
</tr>
<tr>
<td>Solaris</td>
<td>NetView Client</td>
<td>Fresh Installation</td>
<td>220 MB</td>
</tr>
<tr>
<td>Solaris</td>
<td>NetView Client</td>
<td>Upgrade from V6.0</td>
<td>65 MB</td>
</tr>
<tr>
<td>Solaris</td>
<td>NetView Client</td>
<td>Upgrade from V5.x</td>
<td>165 MB</td>
</tr>
</tbody>
</table>

The optional online books component requires 60 MB of disk space in the /usr/OV directory.

The optional relational database component requires 15 MB of disk space in the /usr/OV directory. Additional disk space is required for the relational database that you plan to use. See the appropriate relational database documentation for additional disk space requirements.

Every 200 nodes requires 1 MB of disk space. This assumes you have one read-write map. Each additional read-write map requires 1 MB of disk space.

**NOTE:** Do not install the Tivoli NetView program in a network file system (NFS)-mounted /usr/OV file system, because the results will be unpredictable.

**NOTE:** Depending on the network size and management load, your system may require additional resources. Managers of moderate-sized networks should consider adding up to 512 MB of additional space in the partition containing the /usr/OV directory.
Additional Requirements

Disk Space

<table>
<thead>
<tr>
<th>File Systems</th>
<th>Minimum Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>/var</td>
<td>8 MB</td>
</tr>
<tr>
<td>/tmp</td>
<td>5 MB</td>
</tr>
<tr>
<td>$BINDIR</td>
<td>100 MB</td>
</tr>
<tr>
<td>/etc/lpp</td>
<td>4 MB</td>
</tr>
<tr>
<td>/etc</td>
<td>1 MB</td>
</tr>
</tbody>
</table>

*The $BINDIR file system refers to the disk where the Tivoli Management Framework is installed. A minimum of 256 MB of paging space is required if the Tivoli Management Framework is used.

Paging Space

A minimum of 256 MB of paging space is required.

See "Appendix A, Memory, Paging Space, Tuning, and Sizing Considerations" in the Tivoli NetView for UNIX Configuration Guide for more information about estimating paging space requirements.

Determine how much paging space is available as follows:

<table>
<thead>
<tr>
<th>For...</th>
<th>Enter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>l s p s . s</td>
</tr>
<tr>
<td>Solaris</td>
<td>s w a p . s</td>
</tr>
</tbody>
</table>

Use the above commands to determine the amount of paging space that is currently available on your system, as well as the total amount.

Color Display

A color display supporting X Window System, Version 11 Release 5 (or OpenLook for Solaris) and OSF/Motif, Version 1 Release 2 and meeting the following requirements:
A network adapter (a PCI adapter is strongly recommended for best performance)

A mouse

To use the optional host connection feature, which is available only on AIX, you must have the following software:

One of the following host 390 programs:

-- TME 10 NetView for OS/390 Version 1 Release 1 or Release 2 or Tivoli NetView for OS/390 Version 1 Release

-- NetView Version 3 Release 1

-- NetView Version 2 Release 4

AIX NetView Service Point Version 1 Release 2 Modification 2 with PTF U459153 program or later to use with SNA Server/6000

Communications Server for AIX Version 4 or Version 5

Optionally, Graphic Monitor Facility host subsystem (GMFHS). Refer to the Tivoli NetView for OS/390 library for more information.

To use the optional host connection feature, which is available only on AIX, the AIX NetView Service Point Version 1 Release 2 Modification 2 with PTF U459153 program or later and one of the following is required:

IBM Token Ring High-Performance Network Adapter (#2970)

IBM X.25 Interface Co-Processor/2 (#2960)

IBM 4-Port Multiprotocol Communication Controller (#2700)

<table>
<thead>
<tr>
<th>Features</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum number of colors</td>
<td>256</td>
</tr>
<tr>
<td>Depth</td>
<td>8 planes</td>
</tr>
<tr>
<td>Bits in color</td>
<td>8 bits</td>
</tr>
<tr>
<td>Dimensions</td>
<td>1280x1024 pixels</td>
</tr>
<tr>
<td>Resolution</td>
<td>91x92 dots per inch</td>
</tr>
<tr>
<td>Video memory on adaptor</td>
<td>1 MB minimum</td>
</tr>
</tbody>
</table>
© Ethernet High Performance Network Adapter

**Browser Requirements**

© Netscape Version 4.5.1 or higher for AIX, Netscape Version 4.7 or higher for Solaris.

**NOTE:** You might encounter display problems with the Web Console if you use Netscape Version 6.01a on Solaris.

**TCP/IP Connection Requirements**

As a network manager, the Tivoli NetView program depends on access to the network, even during installation. To ensure that the TCP/IP communications between the system to be installed and the rest of the network are working correctly, perform the following system commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ping 127.0.0.1</code></td>
<td>To check communications on the system</td>
</tr>
<tr>
<td><code>nslookup 127.0.0.1</code></td>
<td>To check connection to the nameserver</td>
</tr>
<tr>
<td><code>nslookup &lt;local IP address&gt;</code></td>
<td>To check name resolution</td>
</tr>
<tr>
<td><code>hostname</code></td>
<td>To check host name resolution</td>
</tr>
<tr>
<td><code>ping &lt;local system name&gt;</code></td>
<td>To check communications to the system</td>
</tr>
<tr>
<td><code>ping &lt;another system name&gt;</code></td>
<td>To check connectivity to another system</td>
</tr>
<tr>
<td>`ps -ef</td>
<td>grep snmpd`</td>
</tr>
</tbody>
</table>

The above commands assume that your system is configured to use a domain name server (DNS). If your system does not use a domain name server, the host names should be resolved in the `/etc/hosts` file.

Also, ensure that all ports required by the Tivoli NetView program are not already in use. Use this command to check the status of ports:

```
netstat -a
```
Close any programs that are using these ports. The Tivoli NetView installation program will fail if any of the following ports are in use:

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Port/Protocol</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>nvtr pd-trap</td>
<td>162/tcp</td>
<td>Tivoli NetView trapd monitor trap port</td>
</tr>
<tr>
<td>nvtr pd-trap</td>
<td>162/udp</td>
<td>Tivoli NetView traps monitor trap port</td>
</tr>
<tr>
<td>nvtr pd-client</td>
<td>1661/tcp</td>
<td>Tivoli NetView trapd client application port</td>
</tr>
<tr>
<td>gtmd</td>
<td>2112/tcp</td>
<td>Tivoli NetView General Topology Manager port</td>
</tr>
<tr>
<td>xxmd</td>
<td>3113/tcp</td>
<td>Tivoli NetView General Topology Manager child process port</td>
</tr>
<tr>
<td>cmot_manager</td>
<td>163/tcp</td>
<td>Tivoli NetView CMOT Manager port</td>
</tr>
<tr>
<td>cmot_manager</td>
<td>163/udp</td>
<td>Tivoli NetView CMOT Manager port</td>
</tr>
<tr>
<td>cmot_agent</td>
<td>164/tcp</td>
<td>Tivoli NetView CMOT Agent port</td>
</tr>
<tr>
<td>cmot_agent</td>
<td>164/udp</td>
<td>Tivoli NetView CMOT Agent port</td>
</tr>
<tr>
<td>ovwdb</td>
<td>9999/tcp</td>
<td>Tivoli NetView Object Database daemon</td>
</tr>
<tr>
<td>ovtopmd</td>
<td>8888/tcp</td>
<td>Tivoli NetView IP Topology daemon</td>
</tr>
<tr>
<td>pmd</td>
<td>2113/tcp</td>
<td>Tivoli NetView Postmaster daemon port</td>
</tr>
<tr>
<td>nvsecd</td>
<td>1663/tcp</td>
<td>Tivoli NetView Security daemon port</td>
</tr>
<tr>
<td>nvcorrd</td>
<td>1666/tcp</td>
<td>Tivoli NetView Correlation daemon port</td>
</tr>
<tr>
<td>actionsvr</td>
<td>1670/tcp</td>
<td>Tivoli NetView Correlation Action daemon port</td>
</tr>
<tr>
<td>nvcold</td>
<td>1664/tcp</td>
<td>Tivoli NetView SmartSet facility</td>
</tr>
</tbody>
</table>
You can also run the Tivoli NetView prerequisite script (**NVprereq.sh**) to determine whether your system meets all requirements and is ready to install the Tivoli NetView program. This script is included on the Tivoli NetView CD-ROM in the **TOOLS** directory. To run this script enter the following:

```
cd  cdmountpoint/TOOLS
NVprereq.sh  <  server | server_update | client | client_update  >
```

Where **cdmountpoint** is the directory where the Tivoli NetView CD-ROM is mounted and **server | server_update | client | client_update** specifies which kit you are planning to install.

### About the Tivoli NetView Software Components

The Tivoli NetView program consists of required and optional software components.

The following software components are required:

**Tivoli NetView Server**

Provides the required code for Tivoli NetView operation.

The following software components are optional:
Tivoli NetView Books

Provides the Tivoli NetView online books. You must have the Netscape Navigator or Netscape Communicator browser to view the online books.

NOTE: To access books, you must have exported the MOZILLA_HOME variable with the location of the Netscape binary file. Also, ensure that the xhost + command has been run on the server.

Tivoli NetView Database

Provides relational database support. If you have a relational database installed, installing the relational database component enables you to store IP topology, the trapd log, and snmpCollect data in the relational database. Refer to the Tivoli Management Framework Reference for the latest supported databases.

Refer to the Tivoli NetView for UNIX Database Guide for information about configuring the Tivoli NetView program to use a relational database.

Tivoli NetView Client

Provides the Tivoli NetView client. This component cannot be installed on a system where the Tivoli NetView server is installed.

See “Installing the NetView Server, Clients, and Books” on page 98 for instructions on how to install your clients.

Installation and Configuration Considerations

Tivoli NetView Server Considerations

In choosing hardware for the Tivoli NetView Server, you should consider a number of capacity and workload issues, such as:

- Size of the managed network
- Number (and types) of Tivoli NetView operators
- Desired polling intervals for status monitoring and SNMP collections
- Speed of the network connections between the Tivoli NetView program and the managed resources
- Whether to use Tivoli NetView Mid-Level Managers
Whether to use Tivoli NetView client systems

For small networks, you could use entry-level workstations from a variety of vendors as Tivoli NetView servers. But as a network grows in size, the number of operators increases, and other major applications are added to the system, the memory and CPU capacity needs increase substantially.

For larger networks, systems with multiple CPUs are strongly recommended and, in some cases, multiple systems must be used to distribute the management workloads. Refer to “Appendix A, Memory, Paging Space, Tuning, and Sizing Considerations” in the Tivoli NetView for UNIX Configuration Guide.

An entry-level system to support a small IP network is defined here as a network that includes 5000 objects or 2000 interfaces and one local operator, with network response times of 4-10 microseconds for an ICMP ping and default polling intervals defined.

Suggested systems for this small, entry-level Tivoli NetView server include:

- For AIX, a RISC/6000 7043-150 or 7043-260
- For Solaris, an Ultra 10 or Ultra 2

**NOTE:** Specific models from vendors change frequently. A suggested entry-level system should be considered as a class of machine.

**Tivoli NetView Client Considerations**

The Tivoli NetView client is typically deployed as the number of operators or size of managed network increases. The reason for deploying the Tivoli NetView client is to remove the memory and CPU capacity requirements for supporting operators from the Tivoli NetView server and distribute them to another system. When you are selecting hardware for the Tivoli NetView client, questions about capacity are limited to memory needs and number of operators.

To install the Tivoli NetView client in a small network, entry-level workstations from a variety of vendors are acceptable. As the number of operators increases, the memory and CPU capacity needs increase substantially. For larger numbers of operators (10 or more simultaneously active), systems with multiple CPUs are strongly recommended. A single system with adequate memory and CPU capacity may be used to support multiple operators. Another alternative is to use multiple entry-level systems as a combination Tivoli NetView client and operator workstation.
For detailed information, Refer to “Appendix A, Memory, Paging Space, Tuning, and Sizing Considerations” in the Tivoli NetView for UNIX Configuration Guide.

An entry-level system supporting a small network is defined here as a two-operator Tivoli NetView client system that is part of a 5000-object IP network.

Suggested systems for this small, entry-level Tivoli NetView client include:

© For AIX, a RISC/6000 7043-150 or 7043-260
© For Solaris, an Ultra 10 or Ultra 2

**NOTE:** Specific models from vendors change frequently. A suggested entry-level system should be considered as a class of machine.

### Fresh Installation vs. Update Installation

The Tivoli NetView program provides two types of installations: Fresh Installation and Update Installation.

Use the Fresh Installation when the Tivoli NetView program is not currently installed and you are not migrating any previously-saved Tivoli NetView backup directories.

Use the Update Installation to migrate from a previous version of the Tivoli NetView program (whether or not the NetView program is currently installed). For the Update Installation to succeed, either the Tivoli NetView program must be installed, or a Tivoli NetView migration backup directory must exist. Refer to “Appendix H, Files That Migrate” in the Tivoli NetView for UNIX Configuration Guide for information about creating a migration backup directory.

If you are not migrating files from a previous version of the Tivoli NetView program, skip to “Installing the NetView Program in a non-Tivoli Management Framework Environment” on page 98 or “Installing a Tivoli NetView Server or Client” on page 103. Otherwise, continue to the next section for information about tasks that you should perform before upgrading the Tivoli NetView program.
Tasks to Complete Prior to Upgrade Installation

Backing up the Tivoli NetView Database

Before you install any application, Tivoli strongly recommends that you back up your Tivoli database. This makes it possible to return to the pre-application database if, for some reason, you encounter a problem while installing a particular application.

In a non-Tivoli Management Framework Environment

To back up the Tivoli NetView databases, follow these steps:

1. Exit all copies of the Tivoli NetView user interface using the File..Exit menu item.
2. Stop all the Tivoli NetView daemons.
3. Create a tar file of the Tivoli NetView databases with the command:

   ```
   tar -cvf /dev/rmt0 /usr/OV/databases
   ```

4. Type `netview` to restart the Tivoli NetView program.

Of course, you can replace `/dev/rmt0` with whatever destination you want to use for backups. If you just want to back up the topology information, which includes `ovwdb` objects, `ovw` map information, and IP and non-IP topology information, use `tar` the information in `/usr/OV/databases/openview`.

If you want to back up information other than the Tivoli NetView databases, such as registration files, configuration files, and application defaults, it is best to use `mksysb` to back up your entire manager station.

In a Tivoli Management Framework Environment

From the Tivoli Management Framework desktop Desktop menu, select Backup to perform a backup of the Tivoli server and clients. The `wbkupdb` command can also be used, as shown below:

1. Estimate the size of the backup and ensure there is enough room by using the `-e` option on the `wbkupdb` command as follows:

   ```
   wbkupdb -e
   ```

2. Back up the database using the `-d` option of the `wbkupdb` command:

   ```
   wbkupdb -d <pathname>
   ```
In the previous example, `<pathname>` is the fully qualified path name of the file in which the backed-up data is to be placed.

If no node name is given, the `wbkupdb` command assumes that all managed nodes on this server are to be backed up.

To restore a system when from a backup, use the `-r` option of the `wbkupdb` command as follows:

```
wbkupdb -r -d <backupfilename>
```

For more information about the `wbkupdb` command, refer to the *Tivoli Management Framework Reference, Version 3.6*.

**Migrating RDBMS from 6.x to 7.1**

When doing a migration installation with NetView databases, perform the following procedure for a successful migration:

1. Convert the Topology data back to flat files.
2. Back up the NetView program as described in the previous sections (In a non-Tivoli Management Framework Environment and In a Tivoli Management Framework Environment).
3. De-install the NetView program.
4. Install the NetView Version 7.1 program.
5. Drop the 6.x topology tables.
6. Create Topology tables using the 7.1 database schema.
7. Convert the flat files back to RDBMS.

The SNMP Collect and TRAPD data should be accessible as before.

**Files Migrated during Upgrade Installation**

During an upgrade installation to NetView Version 7.1, the following files are now migrated:

```
/usr/0V/conf/location.conf
/usr/0V/conf/netmon.seed
```

Other configuration file migration occurs as in previous versions of the NetView program.
To Ensure A Smooth Migration

Follow these steps to ensure a smooth migration:

1. Determine whether third-party applications will be migrated with the NetView program (for example Nways®, CiscoWorks®, or Optivity©). Deinstall any applications that will not be migrated, and verify that all deinstalled software has been deleted.

2. Verify that all Tivoli NetView and third-party application daemons start without error. Remove any daemons from startup that do not start correctly, or correct the reason for the failure. All daemons must start without error for a successful Tivoli NetView migration.

   In general, verify that all of the NetView program and its associated applications are running correctly at the current installed level.

3. For a client, remove the server using the Tivoli Desktop or the Client Setup application (clientsetup). Select **Configure –> Remove Server**. The client upgrade installation will fail if a server is still set for the client.

   After the installation, reset the server for each client using clientsetup (select **Configure –> Add/Change Server**).

4. Stop all Tivoli NetView windows.

5. Turn off Tivoli NetView security, if it is currently turned on, because the installation will fail if security is turned on.

6. Stop all Tivoli NetView daemons by entering the following:

   ```bash
   /usr/OV/bin/ovstop
   /usr/OV/bin/ovstop nvsecd
   ```

7. Run the `chktrapd` script to determine whether any lines or sections of the `trapd.conf` file are too long (more than 99 fields). This script is included on the Tivoli NetView CD-ROM in the `TOOLS` directory. Use the following command to run this script:

   ```bash
   chktrapd /usr/OV/conf/C/trapd.conf
   ```

   Errors found by the script are saved in the `/tmp/trapd.confchk` file. Correct any errors in the `trapd.conf` file before performing an upgrade installation of the Tivoli NetView program.

Now you are now ready to perform an upgrade Installation of the Tivoli NetView program. Proceed to the next section for instructions on installing or upgrading a Tivoli NetView server or client.
Setting the LANG and LC_MESSAGES Variables

The default setting for the LANG variable and the LC_MESSAGES variable is C. The LANG and LC_MESSAGES environment variables must be set to the U.S. English language locale at the time the Tivoli NetView base product or any associated patches are installed.

After installation, to get full message function, set the LANG and LC_MESSAGES environment variables to the LANG value appropriate for your system.

These are the valid values for the U.S. English locale:

<table>
<thead>
<tr>
<th>For...</th>
<th>The U.S. English Locale is...</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>En_US</td>
</tr>
<tr>
<td>Solaris</td>
<td>en_US.ISO8859-1</td>
</tr>
</tbody>
</table>

On an AIX system using a Bourne or Korn shell, enter the following:

```
export LANG=en_US
export LC_MESSAGES=en_US
```

On a Solaris system using a C shell, enter the following:

```
setenv LANG en_US
setenv LC_MESSAGES en_US
```

**Attention:** If the LANG and LC_MESSAGES variables are set to C or are not set, messages are not displayed correctly and the NetView program might not run correctly.

The Tivoli NetView program has algorithms for finding language-sensitive files. An attempt is made to locate the files based on the value of the LANG environment variable. However, the Tivoli NetView program defaults to operating as though the LANG environment variable is set to C if one of the following happens:

- The LANG variable is not set.
- The value of the LANG variable is not a recognized locale.
- A required file is not found in the path referenced by the LANG variable.
NOTE: If the LANG and LC_MESSAGES variables are not set, you will see the following information when you start the NetView application from the command line:

\textit{LC_MESSAGES set to en\_US because it was unset or set to C}
\textit{LANG set to en\_US because it was unset or set to C}

### Installing the NetView Program in a non-Tivoli Management Framework Environment

#### Installing the NetView Server, Clients, and Books

The NetView program no longer needs to be installed using the Tivoli Management Framework. You can easily install NetView servers, clients, and books using the new scripts, `instalnv` and `uninstnv`, without using the Tivoli Management Framework. Both these scripts are available in the top-level directory of the installation CD.

The `uninstnv` script uninstalls previously-installed versions of the NetView program. At a command prompt on the machine to be deinstalled, change the directory (`cd`) to the installation media and type:

```
uninstnv
```

To install the NetView program without using the Tivoli Management Framework, change the directory (`cd`) to the installation media and type:

```
instalnv -k KIT [-u]
```

where `KIT` is the type of installation required: `CLIENT`, `SERVER`, or `BOOKS` and `-u` is the update flag to designate an upgrade installation rather than a fresh installation.

After invoking the `instalnv` script, you are prompted to continue. If you select Yes, prerequisite checking occurs, the installation continues, and progress is displayed in the window from which it was initiated. The message `Install finished` is displayed in the window when the installation is complete.

Two files are displayed on the machine being installed: `Readme` and `update.log`. These files contain installation information and any error messages that resulted from the installation.
When the installation is complete, you must stop and restart the daemons using netnmrc. To do this, follow these steps:

### On AIX, type...

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>cd /usr/OV/bin</td>
</tr>
<tr>
<td>ovstop</td>
</tr>
<tr>
<td>ovstop nvsecd</td>
</tr>
<tr>
<td>ps</td>
</tr>
<tr>
<td>/etc/netnmrc</td>
</tr>
</tbody>
</table>

### On Solaris, type...

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>cd /usr/OV/bin</td>
</tr>
<tr>
<td>ovstop</td>
</tr>
<tr>
<td>ovstop nvsecd</td>
</tr>
<tr>
<td>ps</td>
</tr>
<tr>
<td>/etc/init.d/netnmrc</td>
</tr>
</tbody>
</table>

- The `uninstnv` script replaces the cleanup script that was available in the Tools directory in previous releases.
- Before installing the NetView program, it is always good practice to reboot the machine that you plan to install the NetView program on.
- A non-Tivoli Management Framework installation might still show Tivoli Management Framework-related errors during installation, start-up, and deinstallation. These are harmless.
- NetView relational database support is not provided with non-Tivoli Management Framework installations. To use a NetView relational database, the Tivoli NetView program must be installed using the Tivoli Management Framework.
- The Database kit can be installed only through the Tivoli Management Framework because it requires RIM support.

## Installing the NetView Program in a Tivoli Management Framework Environment

If you plan to use the Tivoli Management Framework to install the NetView program, first verify that the correct version of the Tivoli Management Framework is installed on your machines. See “Software Requirements” on page 84 for the required Tivoli Management Framework version.
Licensing Note: The Tivoli NetView program includes a Tivoli Management Framework license at no additional charge. Customers can use the Tivoli Management Framework on the Tivoli NetView server and Tivoli NetView clients only for enabling the use of the Tivoli NetView program.

Managing Tivoli NetView Installation from the Tivoli Desktop

The NetView program can be installed from the Tivoli desktop on a TMR server residing on any of the following platforms and operating systems:

⊙ IBM RS/6000 Systems running AIX 4.3.3 or higher
⊙ Sun SPARC or ULTRA Systems running Solaris 2.7 or higher
⊙ HP 9000 Systems running HP-UX 10.20 or higher
⊙ Intel 486 or Pentium Systems running Windows NT 4.0 or Windows 2000.

Refer to “Software Requirements” on page 84 for the supported versions of the operating systems and required software for the remote installation.

Tivoli NetView can be installed on a TMR server or Tivoli managed node residing on an AIX or Solaris UNIX system. Refer to “Hardware Requirements” on page 83 and “Software Requirements” on page 84 for supported hardware platforms and operating system versions.

Tivoli Management Framework Installation

The Tivoli Management Framework can be used to install the NetView program and its features, to install any patches required by the NetView program, and to provide relational database support for the NetView program.


Install the Tivoli Management Framework Version 3.7 on the machine that is to be your Framework server. When installing the Tivoli Management Framework, use a valid license key. If you do not have a valid license key, contact your Tivoli support representative. Refer to the Tivoli Management Framework Planning and Installation Guide Version 3.7 and Tivoli
NOTE: The Tivoli NetView program includes a Tivoli Management Framework license at no additional charge. Customers can use the Tivoli Management Framework on the Tivoli NetView server and Tivoli NetView clients only for enabling the use of the Tivoli NetView program. For any use beyond this scope, a valid license key is required.

NOTE: If you want to use RIM with NetView 7.1 on Solaris you must use Tivoli Management Framework 3.6.3, not the 3.7 version.

Starting the Tivoli Desktop

Use the following steps to set up the UNIX system environment and display the Tivoli desktop:

1. Log in to a Tivoli client or the Tivoli server on which your Tivoli administrator has an alias with a super user role for the TMR. Refer to the Tivoli Management Framework Planning and Installation Guide for information about creating administrators with authorization roles for the TMR.

2. Run one of the following environment initialization and setup scripts:

<table>
<thead>
<tr>
<th>For...</th>
<th>Enter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bourne or Korn shell</td>
<td>./etc/Tivoli/setup_env.sh</td>
</tr>
<tr>
<td>C shell</td>
<td>source ./etc/Tivoli/setup_env.csh</td>
</tr>
</tbody>
</table>

3. Start the Tivoli desktop by entering tivoli in a terminal window (you must be logged in as root).

NOTE: When using the Tivoli Management Framework Desktop, no NetView menu help is available from the icon for a managed node if NetView has not been installed on that node.

Tivoli NetView Framework Patch

The Tivoli NetView Framework patch provides the Tivoli NetView configuration menus and enables the Tivoli Management Framework to
recognize the presence of the Tivoli NetView program. You must install this patch before you can install the NetView program through the Tivoli Management Framework.

The Tivoli NetView Framework patch is included on the Tivoli NetView CD-ROM. It must be installed before using Tivoli Management Framework to install the Tivoli NetView program.

**NOTE:** If you are migrating from a previous version of the Tivoli NetView program and want to back up your Tivoli NetView data before migrating, perform this task before installing the patch. Refer to “Backing up the Tivoli NetView Database” on page 94 for information about saving your customized data for migration. Backing up your data is a precautionary measure. The Tivoli NetView Update Installation automatically backs up and migrates your customized Tivoli NetView data.

To install the patch, follow these steps:

1. From the command line, mount the Tivoli NetView CD-ROM.
   
   Refer to “Additional AIX Information” on page 106 for instructions about how to mount a CD-ROM on AIX. On Solaris, the CD-ROM is automatically mounted for you. Use the `df` command and look for the file system beginning with `/cdrom`.

2. Start the Tivoli desktop. Refer to “Starting the Tivoli Desktop” on page 101.

3. Select **Install -> Install Patch...** from the Desktop pull-down menu. The Install Patch dialog is displayed.

4. Click **Select Media...** to display the File Browser dialog.
   
a. Set the Path Name to where the Tivoli NetView CD-ROM is mounted.

   b. Click **Set Path** to change to the specified directory.

   c. Click **Set Media & Close** to save the new media path and return to the Install Patch dialog.

5. Select the appropriate patch from the **Select Patch to Install** list. (If this list is empty or lists the wrong patches, refer to the *Tivoli Management Framework Planning and Installation Guide* for information about setting media.)

   For a server or client Update Installation from NetView Version 5.1 and 6.x, select the following:
For a fresh installation, select:

Tivoli NetView Framework Patch - 7.1 (NVF71)

6. Select the Tivoli clients on which to install the patch. If necessary, move clients from the Clients to Install On list to the Available Clients list. To move more than one client at a time, press the Ctrl key when you select the clients.

7. Click Install & Close to install the patch and close the Install Patch dialog.

The installation process displays a Patch Install dialog that lists the operations will occur during the installation. This dialog also warns you about problems that you may want to correct before installing the patch. Click Cancel if you need to end the installation.

8. Click Continue Install to start the installation. The status of the installation is displayed in the Patch Install dialog.

9. Click Close to close the dialog.

10. Reexecute the Tivoli server by entering the following command:

   `odadmin reexec`

**Installing a Tivoli NetView Server or Client**

The Tivoli NetView program can be installed on either a Tivoli Management Framework server or a managed node. Follow these steps to install a Tivoli NetView server or client:

1. Start the Tivoli Management Framework by entering `tivoli` in a terminal window.

2. Select Install from the Desktop menu. Choose Install Product.... The Install Product dialog is displayed.

3. Click Select Media... to display the File Browser dialog. Set the path name to the directory where the Tivoli NetView CD-ROM is mounted. Click the Set Media & Close button.

4. Select the appropriate product from the Select Product to Install list. (If this list is empty or lists the wrong products, refer to information about set media in the Tivoli Management Framework User’s Guide.)
NOTE: The Tivoli NetView server and Tivoli NetView client cannot be installed on the same system.

The list of products to install, for both AIX and Solaris, is:

<table>
<thead>
<tr>
<th>Type of Installation</th>
<th>Kit Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Fresh Installation</td>
<td>Tivoli NetView Server 7.1</td>
</tr>
<tr>
<td>Server Update Installation</td>
<td>Tivoli NetView Server 7.1 Update</td>
</tr>
<tr>
<td>Client Fresh Installation</td>
<td>Tivoli NetView Client 7.1</td>
</tr>
<tr>
<td>Client Update Installation</td>
<td>Tivoli NetView Client 7.1 Update</td>
</tr>
</tbody>
</table>

5. Select the clients on which to install the product. If necessary, move clients from the **Clients to Install On** list to the **Available Clients** list.

6. Click **Install & Close** to begin the installation process and close the Install Product dialog. The installation process displays a Product Install dialog that lists the operations that will occur during the installation. This dialog also warns you about problems that you may want to correct before installing the product. Click **Cancel** if you want to end the installation.

7. Click **Continue Install** to start the installation. The status of the installation is displayed in the Product Install dialog.

8. Click **Close** to close the dialog.

To install the Tivoli NetView online books, follow Step 1-8 above, but in Step 4, choose **Tivoli NetView Books 7.1** from the **Select Product to Install** list. This component is optional and can be installed on top of any of the server or client kits.

If you wish to install the Tivoli NetView database component, follow Steps 1-8 above, but in Step 4, choose **Tivoli NetView Database 7.1** from the **Select Product to Install** list. This component can be installed on top of either the Server Fresh Installation or Server Update Installation kits. Refer to the **Tivoli NetView Database Guide** for information about configuring Tivoli NetView to use a relational database.
Installation Problems

- Whether you are installing the NetView program through the Tivoli Management Framework or not, prerequisites are checked before any new files are installed. If a prerequisite is not met, the installation will stop and a message will be displayed in the Tivoli Desktop under the heading Distributing Architecture Specific NetView Prerequisites.

Look at the /tmp/NVS_71_BIN_before.output file to find out which prerequisites failed. Fulfill the missing prerequisites and then reinstall. Refer to TCP/IP Connection Requirements for information on the NVprereq.sh script that determines whether the prerequisites are satisfied. You can run this script before installing the Tivoli NetView program to determine whether all prerequisites are met.

If the installation fails in a later section (after prerequisite checking) look in the /tmp/update.log and /tmp/NVS_71_*.error files for information about the error. Solve the problem and deinstall Tivoli NetView by running the clean-up script located on the Tivoli NetView CD-ROM. Do this by typing:

cd <mountpoint>
./uninstnv

After running this script, install Tivoli NetView again.

- On Solaris, the installation might fail because ports are still in use. This information will be shown in the /tmp/NVS_71_BIN_before.output file. If this happens, wait a minute or so before trying the installation again.

- On Solaris, the installation might show a failure starting nettl tracing and logging (ERR_bcfg_200). This is because the tracing and logging facilities could not allocate a system semaphore. Contact your system administrator to remove any unneeded semaphores (if any) by running the following commands:

  ipcs -s
  ipcrm -s <sem_id>

  where <sem_id> is the value in the ID column after calling ipcs. If the problem persists, contact your support representative with the following information:

  (semget, errno 28)

- After integrating Nways 2.1 Element Manager, Generic Java-based Graphical Manager for non-SNMP devices, some NetView daemons will
not run. This is because Nways adds a trap called newflow which is already defined in the NetView program’s trapd.conf file.

The workaround for this issue is to comment out line number 437 in the /usr/OV/conf/C/trapd.conf file.

**NVenvironment script**

There is a new script in /usr/OV/bin called NVenvironment. This shell script initializes the NetView runtime environment. You should source this script from your login script. For example, Bourne shell users would add this line to their .profile file: . /usr/OV/bin/NVenvironment to source the proper NetView environment.

**Additional AIX Information**

This section contains additional information for users of Tivoli NetView on an AIX platform.

**Mounting a CD-ROM on AIX**

Following is additional information about mounting a CD-ROM on AIX:

1. Create a CD-ROM file system. If this has already been done, proceed to step 2. To create a CD-ROM file system:
   a. Start SMIT using the following command:
      ```bash
      smit crfs
      ```
   b. Select Add a CDROM File System from the SMIT menu. Complete the fields in this dialog.
      The DEVICE Name is likely to be cd0 (check for the file /dev/cd0; if it does not exist, determine the name of your cdrom device).
      A suggested name for MOUNT POINT is /cdrom. Ensure that the directory specified exists and that it is an empty directory.
   c. Click OK to add the CD-ROM file system and then exit from smit.

2. Insert the CD-ROM in the drive and execute the following command:
   ```bash
   mount /cdrom
   ```
   Where /cdrom is the CD-ROM file system.
NOTE: To unmount a CD-ROM on AIX, execute the command:

`unmount /cdrom`

**Tuning Suggestions for AIX Systems**

This section describes miscellaneous AIX tuning recommendations to improve your performance.

- Be aware of these changes to the AIX buffers for network adapter cards:
  
  PCI adapters allow larger buffers than MCA adapters.

  Tivoli recommends that you set transmit and receive buffers for your network adapter card as large as allowed for your Tivoli NetView server and Tivoli NetView client systems. Follow these steps to increase the size of these buffers. This example assumes that the adapter is active and for the tr0 token ring.

  1. Enter `ifconfig tr0 detach`.

  2. Make the adjustments using `smit`. The smit fast path commands are `smit tradap` or `smit ethernet`.

  3. Enter `ifconfig tr0 hostname up`.

- The TurboDatabase speed option has been shown to reduce I/Os and improve network discovery response times. Refer to "Appendix G, NDBM Database Enhancements" in the [Tivoli NetView for UNIX Configuration Guide](#) (AIX only) for more information on this utility.

- Increase the **Processes per user** to 1024. Use the smit utility to make this change.

- The ARP Cache is used to translate IP addresses to hardware addresses on the same subnet. A good example is the default router address. The default (175 for AIX Version 4) is usually acceptable.

  - Use `arp -an | wc -l` to check cache usage counts.

  - Use `no -a` to view the `arptab_nb` (number of "buckets") and `arptab-bsiz` (size of "buckets") settings.

    The cache size is equal to the product for these two values. Change with the `no -o arptab_nb=293` (prime #) command, add this change to the `/etc/rc.net` file (careful with placement), and confirm that the size is adequate.

- The ARP cache is less interesting in routed networks.
The ARP cache is more interesting in switched networks.

**Recommended AIX Machine Types**

Contact your Tivoli Representative for information on the recommended AIX machine type for the size of your network.

**Tuning AIX for Tivoli NetView**

For information about AIX tuning and the Tivoli NetView program, refer to "Appendix A, Memory, Paging Space, Tuning, and Sizing Considerations" in the *Tivoli NetView for UNIX Configuration Guide*.

**AIX 4.3.3 Support**

APM distribution may hang for AIX users when running `bos.net.tcp.client` at the 4.3.3.10 code level. Applying the latest `bos.net.tcp.client` patch resolves this issue.

**Additional Solaris Information**

This section contains additional information that you should be aware of if you are a Sun Solaris user.

**Solstice Enterprise Agent (SEA) Issues**

In order to fix SEA problems on Solaris 2.8, the latest Solaris 2.8 kernel patches must be installed on both the client and server machines.

The following problems may occur when the NetView server is on a machine running Solaris 2.7 and SEA 1.0.3:

1. The NetView graphical user interface does not come up on the client system, or the client cannot connect to the server. The error message `ERROR: Cannot connect to server daemons` or `Cannot contact the mgrantd daemon for daemon status. Make sure that the mgrantd daemon is running on the server` may display on the client.

2. NetView server machines are not recognized as NetView managers (isManager field is not set to TRUE). The NetView SmartSet is not populated when this occurs.
To fix these problems, install the latest version of the Solaris 2.7 kernel patch and the SEA 1.0.3 patch on both the client and server machines.

Reboot your system after installing these patches.

It is always advisable to install the latest patches for the SEA, available at the following URL:


**MLM Issues**

If you have an MLM installed on the same machine as the NetView server, then you must also make the following change to the `midmand.acl` file:

Change:
```
  acl = {
    communities = public, private
    access = read-write
    managers = *
  }

  }
```

to
```
  acl = {
    communities = private
    access = read-write
    managers = *
  }

  {
    communities = public
    access = read-only
    managers = *
  }
```

Installing the NetView Web Console

Installing the Web Console from the Server

To install the NetView Web Console application, enter the following URL in your browser:

http://<server>:8080/download

where <server> represents the name of the NetView Web Server.

Select the appropriate Web Console kit from among the following:

<table>
<thead>
<tr>
<th>Kit Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nvwc.tar</td>
<td>full console for Unix, without JRE (for use on AIX or Solaris)</td>
</tr>
<tr>
<td>nvwc_thin.tar</td>
<td>thin console for Unix (uses Web Server’s Java environment)</td>
</tr>
<tr>
<td>nvwc_solaris_jre_1_3.tar</td>
<td>full console for Solaris, including Java 2 Runtime Environment</td>
</tr>
<tr>
<td>nvwc_aix_jre_1_3.tar</td>
<td>full console for AIX, including Java 2 Runtime Environment</td>
</tr>
<tr>
<td>nvwc_thin.zip</td>
<td>thin console for Windows (uses Web Server’s Java environment)</td>
</tr>
<tr>
<td>nvwcinstall.exe</td>
<td>Windows self-extracting installation</td>
</tr>
</tbody>
</table>

You can decide which kit you need by typing java -fullversion in a command line.

<table>
<thead>
<tr>
<th>Platform</th>
<th>You should see...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>j2re 1.3.0 ibm build cn130-20010502</td>
</tr>
<tr>
<td>AIX</td>
<td>j2re 1.3.0 ibm build ca130-20010615a</td>
</tr>
<tr>
<td>Solaris</td>
<td>1.3.1·b24</td>
</tr>
</tbody>
</table>
If the response is other than the above, or if you get no response at all, you should use the full console kit for the applicable operating system.

Save the appropriate zip kit to disk and extract the zip file. On Windows, you can use the JAR tool (jar xvf filename.zip) or any file extraction tool (like WinZip). On UNIX, you can use the jar, unzip, gzip, or gunzip commands. The JAR tool is available from the Solaris or IBM web sites. The gzip executable is available from the GNU website.

Additional Information:

© If you are prompted for a Java plug-in to start the Web Console in a browser, they can be found at the following URLs.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>Not currently available.</td>
</tr>
</tbody>
</table>

Installing the Windows Web Console from the CD

From the Tivoli NetView Installation window, select Install Web Console Only. Answer Yes to the dialog that asks if you wish to continue with the installation.

The InstallShield Wizard extracts the web console files and a progress bar shows the installation progress.

At the Tivoli NetView Web Console welcome window, select Next to continue after reading the information.

By default, the Tivoli NetView Web Console application is placed in the C:\Program Files\Tivoli Systems\Tivoli NetView Web Console directory. If this directory does not exist, it can be automatically created. You can also specify a different installation directory. Select Browse to look for a different directory to install in or press Next to continue.
A progress bar shows installation progress. The final installation window allows you to launch the Tivoli NetView Web Console. Select Finish to complete installation of the Web Console application.

**Using the Self-extracting Windows Web Console Script from the Server Download Area**

A self-extracting InstallShield® Web Console application installation is now available for Windows 98, NT, and Windows 2000. It is located in the Web Server’s download area. In your browser, go to http://<hostname>:8080/download and select the `nvwcinstall.exe` script.

Depending on which browser you are using, one of two things will happen when you choose the `nvwcinstall.exe` kit:

1. A File Download dialog appears. Select Run this program from its current location and click OK.
   
   A harmless Security Warning dialog appears:
   
   Do you want to install and run “nvwcinstall.exe from <hostname>”?  
   The publisher cannot be determined due to the problems below:  
   Authenticode signature not found.

2. You are prompted to save the file. When it is saved, go to the directory where it was saved and double-click on the `nvwcinstall.exe` file.

   Click Yes to continue installation.

   The InstallShield program will guide you through the installation. By default, the Tivoli NetView Web Console application is placed in the `C:\Program Files\Tivoli Systems\Tivoli NetView Web Console` directory. If this directory does not exist, it can be automatically created. The user can also specify a different installation directory. When the installation is complete, the user can start the Web Console application.

**Starting the Web Console on Windows**

The Web Console application is started from the Windows Start menu by selecting Programs, then selecting Tivoli NetView -> NetView Web Console or by using the `bin\nvwc.bat` script (located under the installation directory).
Starting the Web Console on UNIX

Start the Web Console with the `nvwc.sh` script located in `nvwc/bin` under the directory where the kit was extracted.

Installing the Tivoli NetView Mid-Level Manager

If you want to install the Tivoli NetView Mid-Level Manager (MLM), do so after you install the Tivoli NetView program. The MLM kit is included on the Tivoli NetView CD-ROM in the `MLM` directory. For information about installing MLM, refer to the `readme` files in the appropriate platform subdirectory under the MLM directory on the Tivoli NetView CD-ROM. For example, the AIX MLM kit and readme files are located in the `<mountpoint>/MLM/AIX` subdirectory.

Additional Information:

© The MLM Administrative functions are available only from the NetView configuration menus in the Tivoli Management Framework. These functions are not available from the Server Setup window after a non-Tivoli Management Framework installation.

Installing the Tivoli Integration Pack for Tivoli NetView (TIPN)

The Tivoli Integration Pack for NetView (TIPN) provides integration between the Tivoli NetView program and the Tivoli Management Framework, Tivoli Inventory, and Tivoli Enterprise Console. The TIPN software is provided on the Tivoli Integration Pack for NetView CD-ROM, which is included with the Tivoli NetView program distribution.

Refer to the Tivoli Integration Pack for NetView User’s Guide and the readme file included on the TIPN CD-ROM for information on installing and using TIPN.

© The Tivoli Event Console integration functions previously packaged in the Tivoli Integration Pack for NetView (TIPN) are now incorporated in the base NetView package. These functions include the ability to display TEC events from the NetView user interface and create TEC events groups.
Based on NetView SmartSet membership. Both the Tivoli Management Framework and the TEC Console must be installed on the NetView server for these functions to work.

Due to changes to Inventory 4.0, there is an incompatibility between the TIPN NetView/Inventory Integration adapter or profile and the Tivoli Management Framework 3.71/Inventory 4.0 environment. This is a permanent restriction.