IBM FileNet Image Services
Version 4.2

SNMP Reference Manual

SC19-3319-00

IBM FileNet Image Services
Version 4.2

SNMP Reference Manual

SC19-3319-00

Note
Before using this information and the product it supports, read the information in "Notices" on page 117.

This edition applies to version 4.2 of IBM FileNet Image Services (product number 5724-R95) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this manual

Simple Network Management Protocol (SNMP) is a standard protocol for network management and is used primarily to monitor network-attached devices. Network administrators can use SNMP to export the statistics that comprise the IBM® FileNet® Management Information Base (MIB) to network management stations, through the SNMP agent.

You must already have an SNMP-based network management system in place for your FileNet Image Services system. The FileNet Image Services software does not include network management software.

To access the FileNet Image Services MIB information, you must be familiar with your implementation of SNMP .

To create an application to access the FileNet Image Services MIB information, you must also be familiar with the application-building utility on your particular network management system.

This manual discusses the following topics:

- SNMP overview
- SNMP traps
- SNMP port usage
- SNMP software configuration
- MIB organization and use
- SNMP components
- User configurable traps

- System monitor reports
- Appendix on SNMP daemon and trap configuration includes:
  - How to configure the Master SNMP Daemon
  - How to configure and use SNMP traps
  - How to read a trap
- Appendix with tables of the objects in the FileNet MIB file
- Appendix on SNMP services and functionality includes:
  - How to verify basic SNMP services and functionality
  - How to check FileNet SNMP functionality
- Appendix on SNMP processes and resources includes:
  - Platform-specific information
  - A bibliography of additional SNMP resources
- Appendix on support for SNMP version 3

To become familiar with SNMP, see the documentation that came with your network management software, or see the resources listed in the **"SNMP bibliography" on page 106**.

To become familiar with FileNet Image Services system operations and terminology, see the *FileNet Image Services System Administrator's Handbook*. To download IBM FileNet documentation from the IBM support page, see **"Accessing IBM FileNet Image Services documentation" on page 11**.

Document revision history

FileNet Image Services version	Date	Comment
4.2	May 2011	Initial release.

Accessing IBM FileNet Image Services documentation

To access documentation for IBM FileNet Image Services products:

1. On the **www/ibm/com** website, enter “FileNet Image Services Documentation” in the search box on the menu bar.
2. Select **IBM - Product Documentation for FileNet Image Services** from the list of search results.

IBM FileNet education

IBM provides various forms of education. Please visit the IBM Information Management support page at (**www.ibm.com/software/data/support**).

Feedback

We value your opinion, experience, and use of our products. Please help us improve our products by providing feedback or by completing a consumability survey.

Documentation feedback

Send comments on this publication or other IBM FileNet Image Services documentation by e-mail to **comments@us.ibm.com**. Be sure

to include the name of the product, the version number of the product, and the name and part number of the book (if applicable). If you are commenting on specific text, include the location of the text (for example, a help topic title, a chapter and section title, a table number, or a page number).

Product consumability feedback

Help us identify product enhancements by taking a **Consumability Survey**. The results of this comprehensive survey are used by product development teams when planning future releases. Although we are especially interested in survey responses regarding the most recent product releases, we welcome your feedback on any of our products.

The survey takes approximately 30 minutes to complete and must be completed in a single session; there is no option to save a partially completed response.

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is the industry-standard protocol for network management. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

Important

SNMP version 3 (SNMPv3) support has been tested on AIX 5.3 and AIX 6.1 over IPv4.

Other FileNet Image Services systems support only **SNMP version 1 (SNMPv1)**.

Through the FileNet Management Information Base (MIB), you can use your SNMP-compliant network management software to access a wide variety of information in your FileNet system.

Examples of network management software include BMC ProactiveNet Performance Management, HP OpenView, IBM NetView®, SunNet Manager, and CA Unicenter. FileNet Image Services does not include network management software.

Although the SNMP protocol is standard, there are many variations in specific implementations. Always see the manuals that came with your network management software for details.

For details, see the following topics:

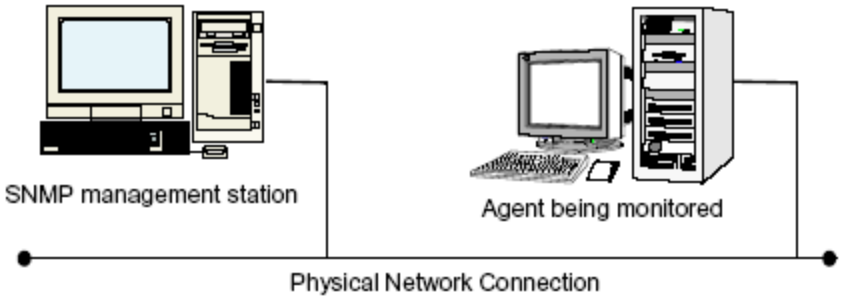
Overview

SNMP is a TCP/IP-based protocol for managing (monitoring and controlling) an enterprise's resources across the network. Examples of managed resources might include routers, switches (hardware), and FileNet Image Services servers (software).

Every SNMP communication takes place between two entities:

- A management station, which is a workstation running network management software
- An agent, which is the hardware or software being monitored by the management station

The following illustration shows the relationship between the SNMP management station and its monitored agent.



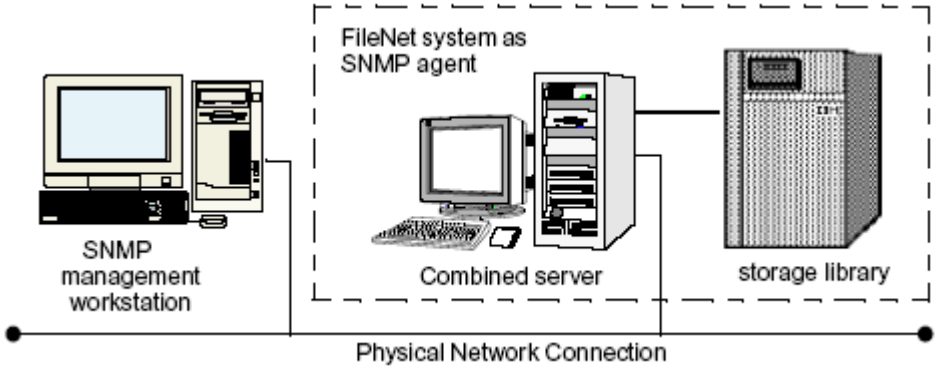
SNMP Management Station and Agent

The following topics illustrate the SNMP operations when configured to monitor a FileNet Image Services system:

SNMP monitoring a FileNet Image Services system

When configured to monitor a FileNet system, the SNMP management station sees the FileNet Image Services server as its agent.

The following illustration depicts a local area connection between the SNMP management workstation when a FileNet system is the monitored agent.



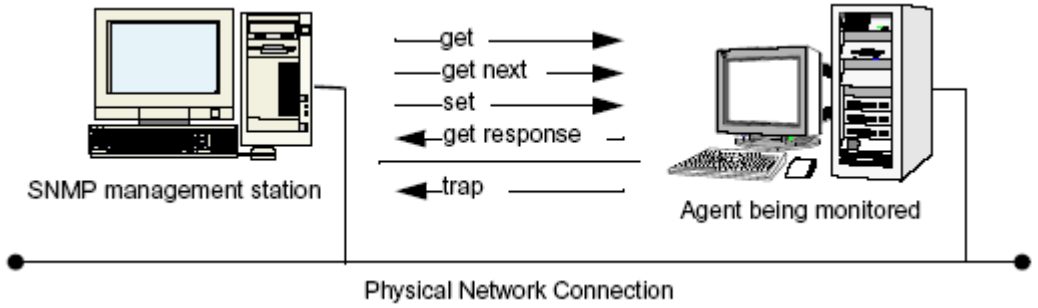
SNMP Management Station Monitoring a FileNet System

SNMP operations

SNMP uses five internal operations to exchange information:

get	Retrieves the values of specific objects from the MIB
get next	Retrieves the value of the next object in the MIB
set	Alters specific MIB objects' values
get response	Responds to get, get next, or set requests
trap	Generates unsolicited event notifications sent to network management stations For example, an SNMP agent issues a trap when it reinitializes itself, an attached interface status changes, or an error condition occurs.

The first three operations are issued from the management station and sent to the agent. The agent sends a response. The agent also initiates the trap operation and sends it to the management station.



SNMP Operations

How SNMP traps are issued

SNMP traps are alerts the agent software generates and sends to the third party SNMP-compliant network management system. When the FileNet Image Services server is the agent, there are seven possible default traps that can be sent:

- FileNet Image Services software stopped
- System aborted a process
- Signal killed a process
- SNMP has an internal error
- Server rejected an RPC connection due to a lack of service request handlers
- Error occurred, disabling the storage library or the optical drive
- Storage library needs operator intervention

Note The FileNet Image Services default implementation of SNMP does not issue a trap when a user disables a library or a drive.

You can also configure optional (fnPtt) traps.

The FileNet Image Services software has a trap table called fnPtt (“FileNet Poll Trap Table”). User-configured traps are enabled by adding entries to fnPtt. By default, fnPtt has no rows, which means no entries and no custom traps. Please note that the final row in the poll trap table fnPtt (see **“Poll Trap table group” on page 35**) always has an fnpttOID value of zero. This indicates “end of table.” Through your SNMP management software, you can add or delete values you want to monitor.

Users can add and delete entries to fnPtt (thereby enabling or disabling specific custom traps) through their SNMP management software, or by modifying the clear-text file /fnsw/etc/ptt.ini.

- See **"Configuring and using SNMP traps" on page 55** for examples of setting traps using an SNMP management console or manually editing the ptt.ini file with trap information using a text editor.
- See **"FileNet Poll Trap Table Group" on page 89** and **"User configurable traps" on page 37** for more information on customizing traps.

It is important to note that the information that appears in a particular trap message depends on how the fnptt trap table has been configured.

How SNMP software uses ports

Ports allow SNMP information to be sent to the correct application. Depending on the platform, FileNet Image Services uses two or more of the following SNMP ports.

Tip The following descriptions show file paths using the UNIX® format. If you are using a Windows® server, replace the forward slash (/) with a backward slash (\).

SNMP Ports

Name	Configurable	Description
SNMP	/etc/services Default=161/udp	An external SNMP manager uses this port to communicate with any/all SNMP agents on the host where FileNet Image Services resides.
FileNet Port	/fnsw/bin/ MasterSnmpd_ start	FileNet SNMP daemon, fn_snmpd, uses this port to listen for requests from the SNMP multiplexer. • FileNet Image Services for the HP-UX and the Solaris Operating Environment systems requires matching values for the FileNet_port variable in fn_snmpd_start and MasterSnmpd_start. The default port number is decimal 8001. • FileNet Image Services for Windows Server requires a hard-coded port number of 9002 hexadecimal. To change the port number, change the fn_snmpd/udp entry in the services file. • FileNet Image Services for AIX/6000 does not use this port.
Native Port	/fnsw/bin/ MasterSnmpd_ start ...AND... OS-specific (for example, /etc/rc3.d/ S76snmpdx)	Native OS SNMP daemon uses this port to listen for requests from the SNMP multiplexer. • FileNet Image Services for HP-UX has a default port number of 8000 decimal. To change this default value, you must change the native_port variable in MasterSnmpd_start, located in the /fnsw/bin directory. • FileNet Image Services for AIX/6000 and Windows Server systems does not use this port.

SNMP Ports, Continued

Name	Configurable	Description
FileNet Trap Daemon		FileNet trap daemon, fn_trapd, uses this port to listen for internal trap messages from fnsw. The port number is hard-coded to hexadecimal 8999. To change the port number, add an fn_trapd/udp trap entry in the /etc/services file.
Master-Snmpd Trap		MasterSnmpd multiplexer uses this port to listen for trap messages from fn_trapd. The port is hard-coded to hexadecimal 9001. To change the port number, add a master_trapd/udp entry in the /etc/services file. FileNet Image Services for AIX/6000 and Windows Server systems does not use this port.

The following table lists TCP Ports used by FileNet Image Services:

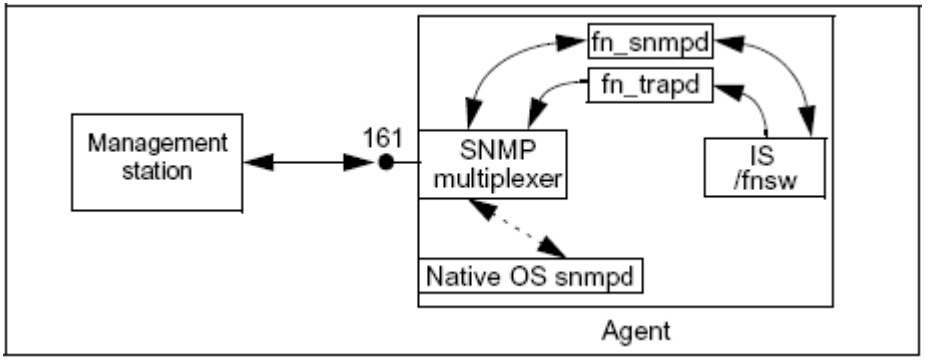
TCP Ports

Port	Description
32768/tcp	TMS
32769/tcp	COR
32770/udp	NCH
161/udp	fn_snmp
162/udp	snmp_trap
35225/udp	fn_trapd
8000/udp (HP only)	Native default SNMP port
8001/udp (HP and Solaris only)	FileNet-specific SNMP port
anonymous ports	Migration notify

How the SNMP software is configured

Software daemons on the agent listen for requests from the management station and send traps alerting the station to problems. Different operating systems provide different SNMP mechanisms and native software. FileNet Image Services is designed to work appropriately with the native OS SNMP capabilities.

The following diagram shows a generic SNMP configuration. An SNMP multiplexer opens and listens to standard port 161. FileNet daemons communicate between FileNet Image Services applications and the multiplexer.



Generic SNMP Configuration

FileNet Image Services for AIX/6000

The SNMP implementation on the FileNet Image Services for AIX/6000 systems uses the native AIX® SNMP daemon, /usr/sbin/snmpd, to communicate with the management station. The FileNet SNMP daemon, fn_snmpd, communicates with the native AIX daemon through the native AIX SNMP protocol information library, smux.lib.

AIX 5.2 and later

With AIX 5.2 and later, SNMPv3 has been introduced as the default SNMP version. See **"Appendix E – Support for SNMPv3" on page 107** for information on configuring SNMPv3.

Verifying the current SNMP version

1. Run the following command to verify the current SNMP version:

   ps –e | grep snmp

2. If you are running SNMP version 3 (SNMPv3), you can optionally switch to version 1 by entering:

   snmpv3_ssw –1

3. Also, edit the /etc/environment file and add the following environment variable:

   FDTABLENUM=1024

   The new FDTABLENUM environment variable will go into effect the next time you reboot the server.

Enabling traps

To enable traps, you must configure a line to the configuration file (/etc/snmpd.conf) specifying where to send the trap:

trap *community host view* fe

To allow users to change configurable MIB variables, configure the following line:

community *community host netmask* readWrite

For more detailed information, see **"Configuring the AIX operating system" on page 41**.

The native snmpd must be started at boot time. Beginning with AIX 4.1x, startup is no longer automatic; FileNet Image Services must ensure that snmpd starts. For architectural information concerning the SNMP processes, see **"AIX architecture" on page 99**.

FileNet Image Services for HP-UX and Solaris®

The FileNet SNMP implementation is similar on the FileNet Image Services for HP-UX and the Solaris Operating Environment systems. A FileNet master SNMP daemon, MasterSnmpd, acts as the SNMP multiplexer.

On both FileNet Image Services platforms, the MasterSnmpd_start script can start MasterSnmpd at boot time if it is configured to do so. When the FileNet Image Services server starts up, the fn_snmpd_start script starts both fn_snmpd and fn_trapd.

The MasterSnmpd_start script includes variables to let you specify the SNMP manager host name and community to which traps should be

sent. The default host name is “local,” which disables trapping. The MasterSnmpd_start script allows you to set the FileNet port number. The default FileNet port is 8001. If you change the FileNet port in MasterSnmpd_start, you must also change the FileNet port in fn_snmpd_start. For a complete list of MasterSnmp configurable parameters, see **“MasterSnmpd configurable parameters” on page 105**.

On the Solaris platform, the SNMP MIB2 standard requires support for certain operating system level MIBs (for example, #/bytes read, #/bytes written, etc.) by any agent. Since the FileNet software cannot assume the operating system has a native SNMP, FileNet Image Services for the Solaris Operating Environment implements the MasterSnmpd to handle these MIB2 counters if nobody else can. So, the FileNet software provides a standard MIB2, as well as the FileNet MIB. By default, the FileNet MIB2 processes non-FileNet requests. However, if you have customized the native OS MIB2 file, you must change this option to implement the customized values.

- On Solaris, MasterSnmpd_start defaults to **MIB2_flag=1**, meaning MasterSnmpd answers MIB2 queries.
- On Solaris, **MIB2_flag=0** means that the FileNet software defers to the Solaris snmpdx to answer MIB2 queries.

To use the MIB2 file provided with the Solaris OS:

1. Change the MIB_flag in MasterSnmpd_start to 0 (zero).
2. Change the snmp/udp entry in the /etc/services file to match the native port in the MasterSnmpd_start file.
3. Start the native snmpd before you start fnsw.

FileNet Image Services for HP-UX does not provide a standard MIB2. The native OS SNMP must process all non-FileNet requests. The default native port is 8000. For architectural information concerning the SNMP processes, see **“HP-UX architecture” on page 101** and **“Solaris architecture” on page 102**.

FileNet Image Services for Windows Server

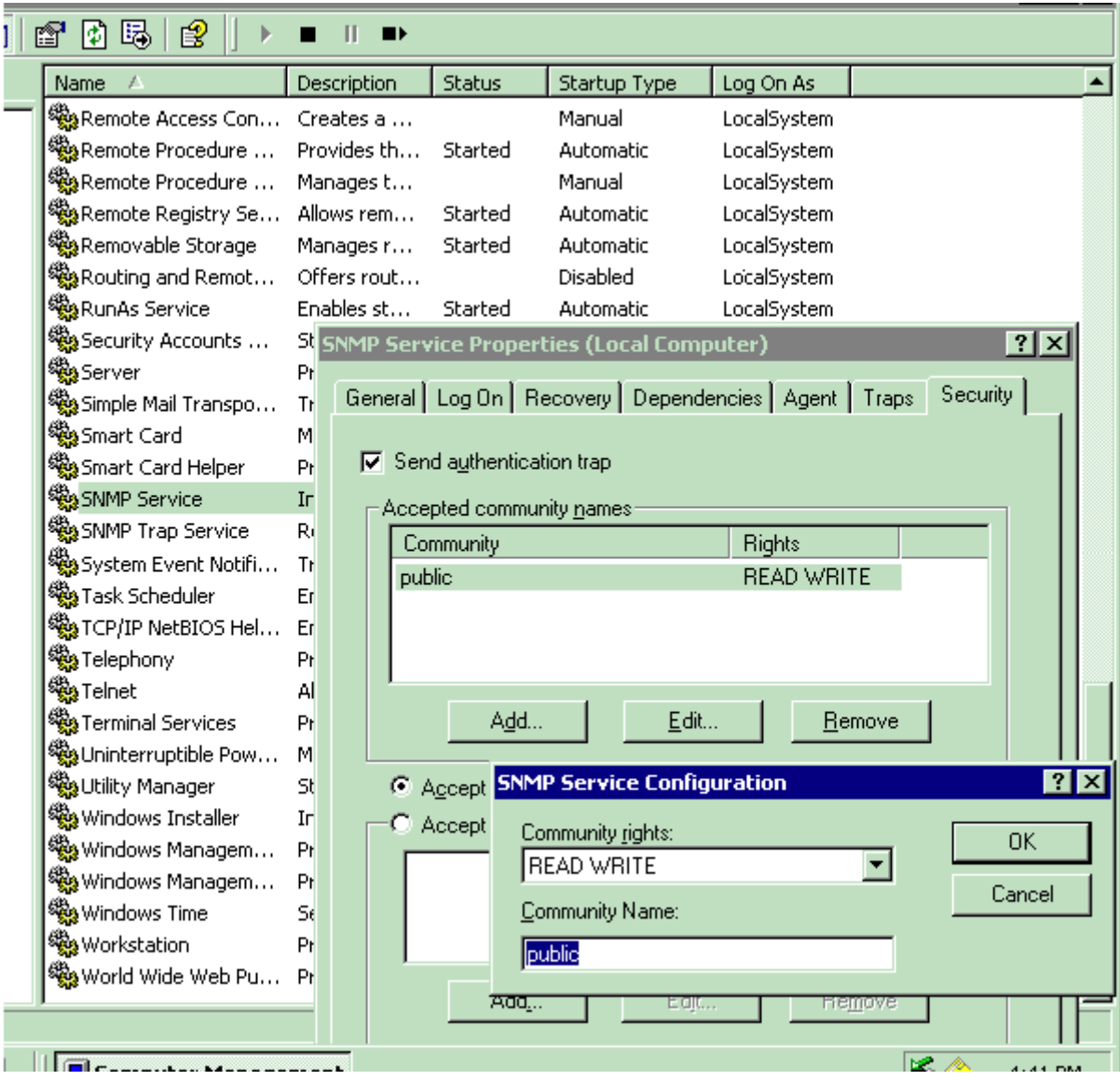
The FileNet SNMP implementation on the FileNet Image Services for Windows Server systems uses a dynamic link library, fn_snmpd.dll, to communicate between the FileNet daemons and the native Windows Server SNMP executable, snmp.exe. The FileNet daemons are fn_snmpd.exe and fn_trapd.exe.

The Windows SNMP Service (snmp.exe) must be installed before installing the FileNet Image Services software. See **"Determine if SNMP Services is installed on a Windows Server system" on page 94** for more details and options.

The FileNet SNMP agent uses the Native Windows SNMP services.

To use FileNet traps, you must first enable traps through the Windows Service SNMP configuration. Click on the icon and follow the directions provided. For architectural information concerning the SNMP processes, see **"Windows Server architecture" on page 104**.

The default SNMP security settings in Windows are **Read Only**. If you leave these defaults set, you cannot set custom SNMP poll traps. If you wish to use custom traps on an FileNet Image Services server running under Windows, you must set the security for your SNMP community to **Read Write**. You can do this from either the "Computer Management" or "Services" administrative applets, as shown in the following example:


Name
Description
Status
Startup Type
Log On As
Remote Access Con...
Creates a ...
Manual
LocalSystem
Remote Procedure ...
Provides th...
Started
Automatic
LocalSystem
Remote Procedure ...
Manages t...
Manual
LocalSystem
Remote Registry Se...
Allows rem...
Started
Automatic
LocalSystem
Removable Storage
Manages r...
Started
Automatic
LocalSystem
Routing and Remot...
Offers rout...
Disabled
LocalSystem
RunAs Service
Enables st...
Started
Automatic
LocalSystem
Security Accounts ...
Server
Simple Mail Transpo...
Smart Card
Smart Card Helper
SNMP Service
SNMP Trap Service
System Event Notifi...
Task Scheduler
TCP/IP NetBIOS Hel...
Telephony
Telnet
Terminal Services
Uninterruptible Pow...
Utility Manager
Windows Installer
Windows Managem...
Windows Managem...
Windows Time
Workstation
World Wide Web Pu...
SNMP Service Properties (Local Computer)
General
Log On
Recovery
Dependencies
Agent
Traps
Security
Send authentication trap
Accepted community names
Community
Rights
public
READ WRITE
Add...
Edit...
Remove
Accept
Accept
SNMP Service Configuration
Community rights:
READ WRITE
Community Name:
public
OK
Cancel

How the MIB Is organized and used

The Management Information Base (MIB) is a file stored on both the SNMP management station, as well as on the agent it monitors.

The MIB file contains a set of objects an SNMP management station can access through an IP-based network. A MIB defines the information exchanged between a management station and an agent. The MIB contains a uniquely identifiable field for each status or configuration parameter the SNMP manager can monitor.

If it has loaded the appropriate MIB file, the network management station, as well as its agent, can correctly identify and respond to messages sent between them.

MIB file location

When you install the FileNet software on the FileNet Image Services server, the installation program automatically copies the MIB file into the etc directory. For example, you'll find the FileNet MIB file using the default file path for your FileNet Image Services server's operating system:

For UNIX-based servers:	/fnsw/etc/filenet.my
For Windows-based servers:	\fnsw\etc\filenet.my

You must load a duplicate copy of this MIB file onto the workstation used as the SNMP management system that will monitor the FileNet system. The method used to load this file onto the SNMP management station varies, depending on the management software.

SNMP elements

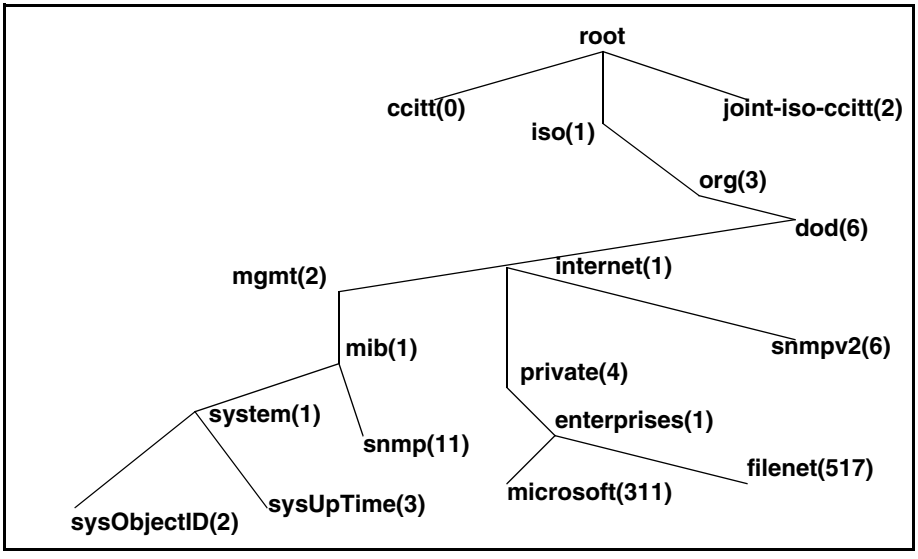
Note FileNet Image Services supports **SNMP versions 1 and 3 (SNMPv1 and SNMPv3)** on AIX 5.3 and AIX 6.1 and later over IPv4.

FileNet Image Services supports only **SNMP version 1 (SNMPv1)** on other operating systems.

The Internet Activities Board (IAB) defines SNMP elements using the OSI Abstract Syntax Notation One (ASN.1) format, a series of numbers separated by periods.

The IAB reserves the first six dotted notation numbers of **1.3.6.1.4.1** for assignment to hardware vendors requiring extensions for their SNMP MIB files. Adding a decimal digit to this numerical identifier, the IAB provides each of these private organizations with a unique enterprise-specific number that follows these first six numbers. See the following diagram for the SNMP section of the MIB naming tree.

The SNMP section of the MIB naming tree



The FileNet unique identifier is **517**. Therefore, the FileNet MIB definition file, named **filenet.my**, is **1.3.6.1.4.1.517**.

Every SNMP MIB item can be represented by a number like this, or a meaningful name. This series of numbers is the same as a path. Each branch of the tree is associated with a number. The first six numbers are standard and 517 is the FileNet MIB.

Each group and field defined in filenet.my has its own name and number. For example, FileNet Image Services system uptime (the number of seconds since FileNet Image Services was last initialized) is identified in filenet.my as fnsysUpTime, with the unique number:

1.3.6.1.4.1.517.1.5.0

Translated into text, this MIB file extension breaks into the following MIB file definitions:

1.3.6.1.4.1	=	SNMP MIB file
517	=	Enterprise-specific identifier, assigned to FileNet SNMP
1	=	FileNet system group
5.0	=	Time passed since last system start up.

You can program any network management software that recognizes the FileNet MIB-defined numbers to request information from the FileNet Image Services software and to respond to FileNet Image Services-generated trap messages.

For example, the network management software at a customer site has loaded filenet.my. As a result, with the appropriate programming, a management station can determine how many seconds the FileNet

Image Services software has been up by issuing the following command:

get (1.3.6.1.4.1.517.1.5.0)

If the FileNet system has been running 750 seconds when it receives the get command, FileNet Image Services sends the following response:

response, get, (1.3.6.1.4.1.517.1.5.0, value(750))

The network management software can process this information accordingly.

Monitoring groups

The FileNet MIB, filenet.my, allows you to monitor eight different groups of information, as described in the following table.

For detailed descriptions of each MIB entry in these groups, see **"Appendix B – Objects in the FileNet MIB" on page 71**.

FileNet MIB Groups

Group	Description	Information You Can Monitor
System	General information regarding the FileNet server on which the SNMP proxy agent is running For object descriptions, see **"FileNet System Group" on page 71**.	Network Clearing House (NCH) domain and organization names System serial number (SSN) Server type FileNet software uptime Information on last trap sent; various trap flags Table listing each service running on the server

FileNet MIB Groups, Continued

Group	Description	Information You Can Monitor
Cache	Information regarding each cache that resides on the server's hard disk This group applies only when the server's Cache Services sub-system is running. For object descriptions, see **"FileNet Cache Group" on page 76**.	Cache ID, name, and description Minimum and maximum number of sectors Number of sectors free, in use, or locked Number of objects in use or locked
Document Services	Document services statistics This group applies only when the server's document services sub-system is running. For object descriptions, see **"FileNet Document Services Group" on page 78**.	Number of pages and documents migrated from storage media to magnetic disk Number of calls for pages already in cache or on the disk in the drive Number of prefetch calls Total number of migration calls and calls using asynchronous notification Number of pages and documents committed Number of documents read and committed through import Number of batches, pages, and documents committed through Fast Batch Committal

FileNet MIB Groups, Continued

Group	Description	Information You Can Monitor
Storage Library	Statistics for each storage library configured on a FileNet Storage Library server. This group applies only when the server's storage library services subsystem is running. For object descriptions, see **"FileNet Storage Library Group" on page 82**.	Storage library ID, status, and type Number of times the arm has moved Number of times disks were loaded or unloaded Number of total drives and disabled drives
Courier	FileNet network connection management information For object descriptions, see **"FileNet Courier Group" on page 85**.	Number of connections approved, timed out, rejected, or aborted Number of client connections opened Number of failed client open calls
Database	Information on the databases in use on the FileNet server This group is mandatory. For object descriptions, see **"FileNet Database Group" on page 86**.	Database ID, description, location, and type FileNet application services that are clients of the database Total and in-use disk space for the database

FileNet MIB Groups, Continued

Group	Description	Information You Can Monitor
Security	FileNet security services information **“FileNet Security Group” on page 88**.	Number of users currently logged on Number of concurrent users licensed Number of rejected logon attempts
RSVP Group	Messages displayed on the FileNet Image Services console indicating when the storage library requires operator intervention **“FileNet RSVP Group” on page 90**.	When to replace new or existing surface When to remove current surface Operator intervention required

Poll Trap table group

The Poll Trap table permits user-configurable traps by setting thresholds against any MIB value in any of the eight FileNet MIB filenet.my allows you to monitor.

For detailed descriptions of each MIB entry in this group, see **“FileNet Poll Trap Table Group” on page 89**.

How the SNMP components work together

SNMP queries, responses, and traps pass through a number of layers of software, including several FileNet Image Services shared libraries. The Network Management Interface (NMI) and Simple Network Management (SNM) shared libraries provide most of the FileNet SNMP functionality.

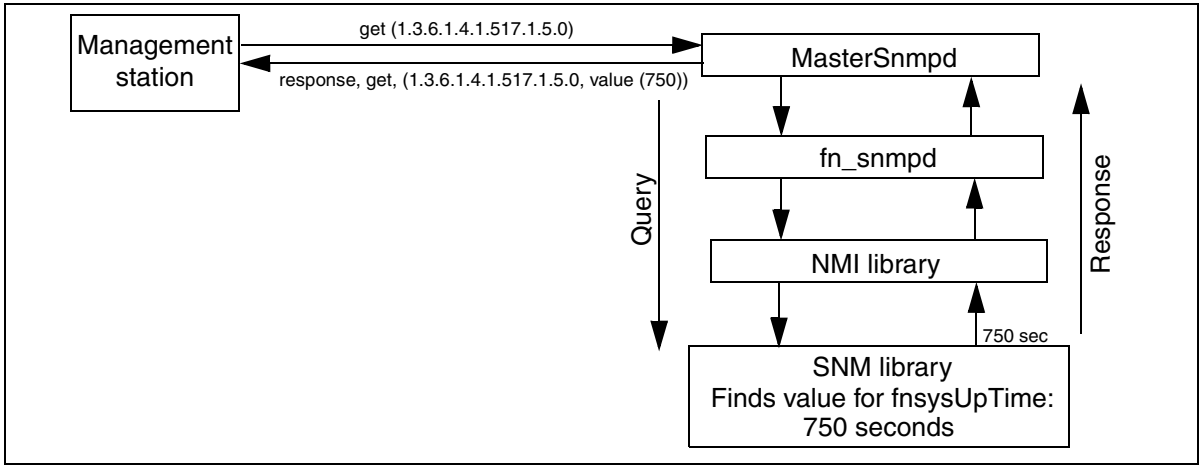
The NMI shared library retrieves FileNet MIB data, providing the following functions:

- Entry points holding all of the FileNet MIB data
- Links to SNM to get protocol process manager (PPM) and Courier (COR) statistics
- Links to performance counter (CNT), cache services manager (CSM), diagnostic interface (DIG), security (SEC), multi-keyed file (MKF), and the RDBMS database to collect statistics

The SNMP shared library provides the following functions:

- Holds COR statistics from the various COR_listen processes
- Holds PPM statistics from the various COR_listen processes
- Provides the PPM and COR statistics to clients

The following diagram illustrates the path of a query for the number of seconds the FileNet system has been up and the response of 750 seconds. The example is for an FileNet Image Services for HP-UX system. The interface daemons differ for other platforms.



Query and Response, FileNet Image Services for HP-UX

User configurable traps

FileNet SNMP gives you the ability to set up custom traps. You can monitor the value of any object in the FileNet MIB and configure the FileNet software to send a trap if that value exceeds a threshold.

To add a trap value, you must create a new row in the fnptt table. Change the value of the field **fnpttOid** (object ID of the FileNet MIB object) from zero (0) to the fnpttOid you want to monitor. Use your SNMP manager to do a **Set** of each of the following fnptt values:

1 **fnpttOID**: OID of the value you wish to monitor
MANDATORY
Must be the first value you set for the new row

2 **fnpttThreshold**: threshold for the object ID polled
MANDATORY

3 **fnpttInterval**: polling interval (in minutes)
MANDATORY
0 = disabled

4 **fnpttExact**: 0= normal checking, 1= exact match needed
OPTIONAL (default= normal)

5 **fnpttRepeatence**: #/times hitting a threshold generates a trap
OPTIONAL (default= 1)

6 **fnpttSeverity**: Severity level
OPTIONAL (default= 1)
Values= ok(1), warning(2), operator(3), severe(4)

To delete a trap value, change the **fnpttOid** field of the entry you want to delete to a value of zero (0); fn_snmpd deletes the entry and fn_trapd no longer checks the oid.

To disable monitoring temporarily, change the value of the **fnpttInterval** field of the entry to zero (0).

For each trap entry, fn_snmpd polls periodically, according to the value of fnpptOid. The fnpptOid is a dotted format Object ID entry, whose first digit starts after the FileNet MIB (1.3.6.1.4.1.517) subtree.

Note All FileNet traps conform to SNMP v1.0 syntax.

See **"Appendix A – SNMP daemon and trap configuration" on page 40** for a detailed, step-by-step example on setting up and using fnptt user-configurable traps.

System Monitor reports

The FileNet Image Services System Monitor displays read-only reports generated from data in the FileNet MIB.

The System Monitor reports include:

- General system status information
- General user security status information
- Storage use
- Network activity
- Document services activity

The System Monitor automatically redisplays report information at intervals appropriate for the type of information being displayed. You can print the reports and save each report to a file.

See your *System Administrator's Handbook* for detailed information about using the System Monitor. To download IBM FileNet documentation from the IBM support page, see **"Accessing IBM FileNet Image Services documentation" on page 11**.

Appendix A – SNMP daemon and trap configuration

An SNMP trap is an asynchronous message describing a predefined event sent by the SNMP agent (in our case FileNet Image Services) to a system managing SNMP. In other words, a trap has been sprung and an error or some other noteworthy event has occurred.

Traps are configurable using the **fnPttTable** in the FileNet MIB. This section will provide instructions for performing this configuration and using the trap data with HP OpenView's MIB browser utility. HP OpenView is a common SNMP Management program. At the end you will find a Microsoft® Network Monitor screen that allows you to read a trap once one has been created. As an alternative, this section will also provide instructions for configuring traps by manually editing the **ptt.ini** file.

Configuring the Master SNMP Daemon

The instructions for configuring the Master SNMP Daemon are quite different depending upon the operating system running on your FileNet Image Services server. Depending upon the operating system running on your server, click on the appropriate link:

Configuring the AIX operating system

Configuring SNMP Version 1

In AIX 5.2 and later, SNMPv3 is the default SNMP version.

For information on SNMPv3, see**"Appendix E – Support for SNMPv3" on page 107**.

1. Enter the following command to determine the SNMP version you are running:

   ps -e | grep snmp

2. If you are running SNMP version 3 (SNMPv3) and want to configure that version, skip to **"Appendix E – Support for SNMPv3" on page 107**,

   Otherwise, you can switch to version 1 by entering:

   snmpv3_ssw –1

3. Also, edit the /etc/environment file and add the following environment variable:

   FDTABLENUM=1024

   The new FDTABLENUM environment variable will take effect the next time you restart the server.

Configuring the SNMP version 1 Daemon

Ensure that the AIX SNMP daemon is configured to forward traps to the host computer running the SNMP Management software (for example, HP OpenView).

Note AIX uses /etc/snmpd.conf for its FileNet SNMP process.

1. Using your preferred editor (such as **vi**), prepare to make edits to the snmpd.conf file:

   vi /etc/snmpd.conf

   After Step 3, there is a sample snmpd.conf file with edits made for you to see as an example.

2. Edit the file and modify the **community public** line by making sure the line reads as in the following example. Note that “public” is the default.

3. Edit the file and modify the **trap** line by entering the IP address or the resolved name (in DNS) of the target host. The target host is the SNMP management system (for example, HP OpenView). In the example, **costa2** is the target.

The following sample output shows an snmpd.conf file with edits you made previously:

```
# THIS FILE FileNet Image Services MODIFIED TO SUPPORT SNMP TRAP TESTING.

Logging         file=/usr/tmp/snmpd.log  enabled
Logging         size=0                   level=0

Community       public  0.0.0.0  0.0.0.0    readWrite
Community       private  127.0.0.1  255.255.255.255    readWrite
Community       private  127.0.0.1  255.255.255.255    readWrite
1.17.2

view            1.17.2           system enterprises view

trap            public           costa2      1.2.3   fe      #  loopback
# snmp          maxpacket=1024 querytimeout=120 smuxtimeout=60

smux       1.3.6.1.4.1.2.3.1.2.1.2    gated_password # gated
smux   1.3.6.1.4.1.2.3.1.2.2.1.1.2  dpid_password  # dpid
smux             1.3.6.1.4.1.517                  fndp_password
# fnpd
```

Note The section of the snmpd.conf file shown in this example is the only part of this file that you can modify.

4. If the snmpd daemon is running, stop it by entering the following command:

   stopsrc -s snmpd

5. Start the AIX SNMP daemon by entering

   startsrc -s snmpd

6. Start the FileNet Image services software If it is not already started, by entering:

initfnsw start

7 Finally, verify the following processes are running:

- **snmpd** (The AIX SNMP master daemon)
- **fn_snmpd** (FileNet SNMP daemon)
- **fn_trapd** (FileNet SNMP Trap daemon)

Verify these processes are running by entering the following command:

ps -ef | grep nmp or **ps -ef | grep fn_**

The following is a sample output of the ps -ef | grep nmp command:

```
costa2(root)/> ps -ef | grep nmp
    root 3580  1 0 17:09:25 ?   0:00 /usr/sbin/snmpd
    fnsw 3860  1 0 17:10:33 ?   0:00 /fnsw/bin/fn_snmpd -f 8001
```

Important When FileNet Image Services is installed, the following files are automatically updated:

/etc/snmpd.peers: The following line is added at the end of the file:

"fnpd" 1.3.6.1.4.1.517 "fnpd_password"

/etc/snmpd.conf: The following line is added at the end of the file:

smux 1.3.6.1.4.1.517 fnpd_password # fnpd

If either of these lines is removed, SNMP will cause an error when FileNet Image Services is started.

Configuring the HP-UX and Solaris operating systems

Ensure the SNMP daemon is configured to forward traps to the host computer that is running the SNMP Management software (for example, HP OpenView).

Important HP-UX and Solaris use /fnsw/bin/MasterSnmpd_start as their FileNet SNMP process.

1. Using your preferred editor (for example, vi), edit /fnsw/bin/MasterSnmpd_start:

   vi /fnsw/bin/MasterSnmpd_start

   After Step 7, there is a sample MasterSnmpd_start file with edits made for you to see as an example.

2. Edit the file and modify the **trap_host=** line by entering the IP address or the resolved name (in DNS) of the target host. The target host is the SNMP management system running HP OpenView (for example, **hp9seal**).

3. Optionally, you can modify the **trap_community=** line by entering one of the following valid community names:

   public
   private
   regional
   proxy
   core

   The default is **public**. Using a communty name that is not one of the five valid names produces errors.

4. Save your changes and exit from the editor.

5 If the MasterSnmpd daemon is active, stop it by entering:

kill –9 $pid

6 Start the SNMP daemon by entering:

MasterSnmpd_start &

Note MasterSnmpd is started automatically at system boot by **/etc/rc.initfnsw**, if the file is set for “wait” or “boot” in the server configuration. The recommended setting is “wait.”

7 Start the FileNet Image Services software by entering:

initfnsw –y restart

The following display is a sample output of the MasterSnmpd_start file with edits made as previously directed:

```
#!/bin/sh
#
# This script starts FileNet MasterSnmpd called directly from reboot start up
# NOTE: User can direct change the following trap_host and trap_community
#       variables to refer to their snmp manager host name and community
#       name correspondingly. The "-t $trap_host" option can be used
#       multiple times to support multiple trap hosts, but "-c" option
#       only validate the last option value; The "-m $MIB2_flag" option
#       specify if fn_snmp need to support MIB2, while $MIB2_flag="1",
#       the fn_snmpd supports its own MIB2 implementation besides FileNet MIB;
#       and while $MIB_flag="0" the fn_dnmpd will only support FileNet MIB
#       and transfers non FileNet MIB query to the native snmpd (the native
#       snmpd can not use 161 port which was already used by MasterSnmpd,
#       you need to assign a nonused port number for native snmpd, start it
#       and replace the variable Native_port here; Also assign another non
#       used port number for fn_dnmpd. put it in file /fnsw/bin/fn_snmpd_start
#       and replace variable FileNer_port with it).
#
```

:

```
trap_host="hp9seal"
trap_community="private"
MIB2_flag="0"
Native_port="8000"
FileNet_port="8001"

pid='ps -ef | sed -n -e /grep/d -e/snmpdm/p | awk '{print $2}'
# check to see if the native snmpd is running
if test "" -ne "$pid" ; then
       kill -9 $pid
fi
if test "$MIB2_flag" -eq "0" ; then
   /usr/sbin/snmpd -P $Native_port
fi

# check to see if MasterSnmpd is running
pid='ps -ef | sed -n -e /grep/d -e/MasterSnmpd_start/d -e /MasterSnmpd/p | awk
'{print $2}'
if test "" -ne "$pid" ; then
  kill -9 $pid
fi

# now let's start the FileNet MasterSnmpd
/fnsw/bin/MasterSnmpd -t $trap_host -c $trap_community -m $MIB2_flag -n
$Native_port -f $FileNet_port &


#stamp
0G^RXCR5RwGpGW:T4KkE\BVNP5OfD[>U;a2IaC'=[MU1HcB^<S6_B[^C^CR<LcL]@WOX<KhM\?WAP7Ja
D]CV8T9I'EZ=e7N3HuW'BS6M
```

8 Finally, verify that the following processes are running:

- **MasterSnmpd** (the SNMP master daemon)

- **snmpdm** (an HP-UX process that should always be running, even when MasterSnmpd is down)(**HP Only**)
- **fn_snmpd** (FileNet SNMP daemon)
- **fn_trapd** (FileNet SNMP Trap daemon)

Verify these processes are running by entering the following command:

ps -ef | grep nmp

The following is a sample output of the ps -ef | grep nmp command:

```
Hpdoheny(root)/> ps -ef | grep nmp
    root 3580  1 0 17:09:25 ?   0:00 /usr/sbin/snmpdm
    fnsw 3860  1 0 17:10:33 ?   0:00 /fnsw/bin/fn_snmpd -f 8001
    root 3585  1 1 17:09:26 pts/tb   0:00 /fnsw/bin/MasterSnmpd -t hp9seal -c
public -m 0 -n 8000 -f 8001
```

Note The target host for the traps is displayed (**hp9seal**).

Solaris Host with snmpdx (Solaris 9 only)

Note Solaris 10 users should skip to the next section.

Solaris 10 has different functionality regarding the init.snmpdx file, which makes the modification to the init.snmpdx and MasterSnmp_ start files no longer necessary.

If your Solaris 9 host has **snmpdx** (the Solstice Enterprise Agents SNMP master daemon), complete the following steps:

1. Edit the /fnsw/bin/MasterSnmpd_start file:

   a. Change MIB2_flag from 1 to 0.

Example: **MIB2_flag=”0”**

b Change Native_port from 0 to 8000 (or any free UDP port):

Example: **Native_port=”8000”**

2 For Solaris 9 users, the port specified in the MasterSnmpd_start file must be added in the snmpdx startup file (for example, /etc/init.d/init.snmpdx file) as follows:

```
if [ -f ${SNMP_RSRC) -a -x /usr/lib/snmp/snmpdx l; then
                  if /usr/bin/egrep -v '^[            ]*(#|$)' ${SNMP_RSRC} > \
                      /dev/null 2&2l; then
                          /usr/lib/snmp/snmpdx -y -c /etc/snmp/conf -p 8000
          else
```

The necessary line is the one above the “else” condition. Notice that the **-p 8000** (meaning Port 8000) is at the very end of the line. Anywhere else and the port configuration will not take effect.

3 Stop the snmpdx and Master_Snmpd processes by entering the following command:

/etc/init.d/init.snmpdx stop

4 Restart the snmpdx process, then start the Master_Snmpd process by entering the following command:

/etc/init.d/init.snmpdx start

5 Verify that these processes are running by entering the following command:

ps –ef | grep nmp

The following sample shows the output of this ps -ef command:

```
# ps -ef | grep nmp
  root   533     1  0   Mar 24 ?   0:00 /fnsw/bin/MasterSnmpd -t local -c hp9seal
-m l -n 8000 -f 8001
  root   503     1  0   Mar 24 ?   0:00 /usr/lib/snmpx -y -c /etc/snmp/conf -p 8000
  nsw  2655     1  0 10:12:48 ?   0:00 /fnsw/bin/fn_snmpd -f 8001
```

The target host for the traps is displayed (**hp9seal**).

Solaris snmpXdmid process

The Solaris **snmpXdmid** process is a Solaris OS process that is not required by MasterSnmpd. The **snmpXdmid** process accepts SNMP requests from snmpdx and translates them into DMI requests that are serviced by the dmispd process. The existence of this process can make configuring MasterSnmpd problematic.

To disable the **snmpXdmi** daemon:

1. Prevent the daemon from starting up upon reboot.

   mv /etc/rc3.d/SXXdmi /etc/rc3.d/KXXdmi

2. Kill the currently running daemon.

   /etc/init.d/init.dmi stop`

3. Verify that the daemon is no longer active.

   ps –ef l grep dmi

4. As an additional measure, you can make the daemon non-executable.

   chmod 000 /usr/lib/dmi/snmpXdmid

Solaris 10 SMA process

On Solaris 10 with the System Management Agent (SMA) package installed, the default native master agent becomes **/usr/sfw/sbin/snmpd**. This agent is started by the script file /etc/init.sma start command. (This script file might also be in the **/etc/init.d** directory.) The agent does not use the **/etc/services** file, but it does use the **/etc/sma/snmp/snmpd.conf** file for community strings. The default port number for snmpd is 161.

To override the default port number, enter the following command:

/usr/sfw/sbin/snmpd udp:8000

If both SMA and SEA are present, then the SEA agent **snmpdx** becomes a proxy subagent to the SMA master agent **snmpd**. When SMA is present, **snmpd** is always the master agent.

The subagent **snmpdx** uses the default port 16161. To change this default port number, modify the **/etc/snmp/conf/snmpdx.reg** file.

To determine if ports 161 and 16161 are being used, enter the following command:

netstat –anv | grep 161

SMA also provides a trap listener service. To start this service, enter the following command:

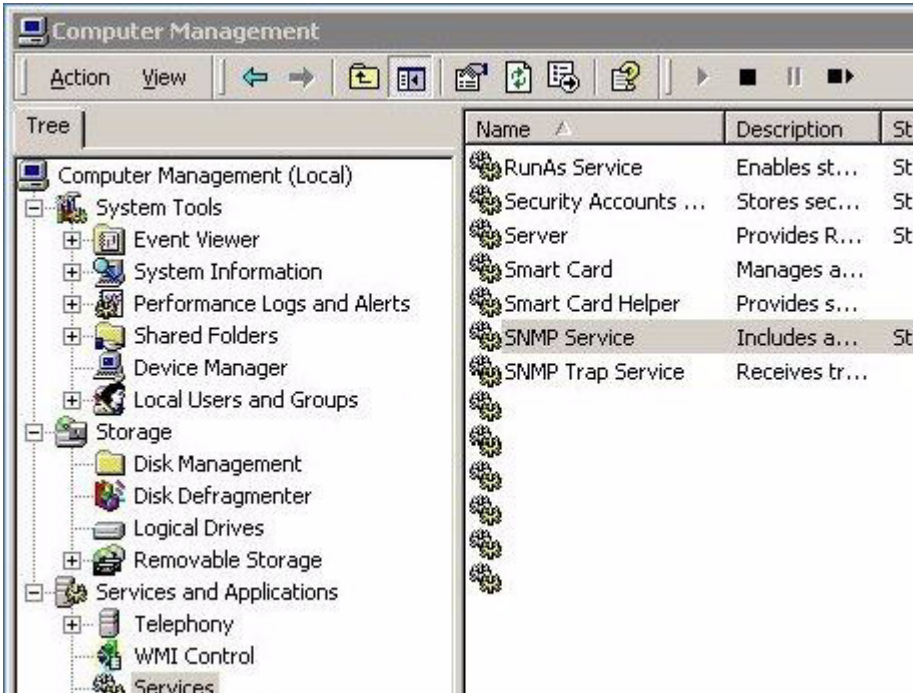
/usr/sfw/sbin/snmptrapd –O aen –P

Configuring the Windows Server operating system

Ensure the Windows SNMP daemon is configured to forward traps to the host computer running HP OpenView.

Note The Windows operating system uses the SNMP.EXE service as its FileNet SNMP process. The Windows SNMP Service (snmp.exe) must be installed before installing the FileNet Image Services software. See **"Determine if SNMP Services is installed on a Windows Server system" on page 94** for more details and options.

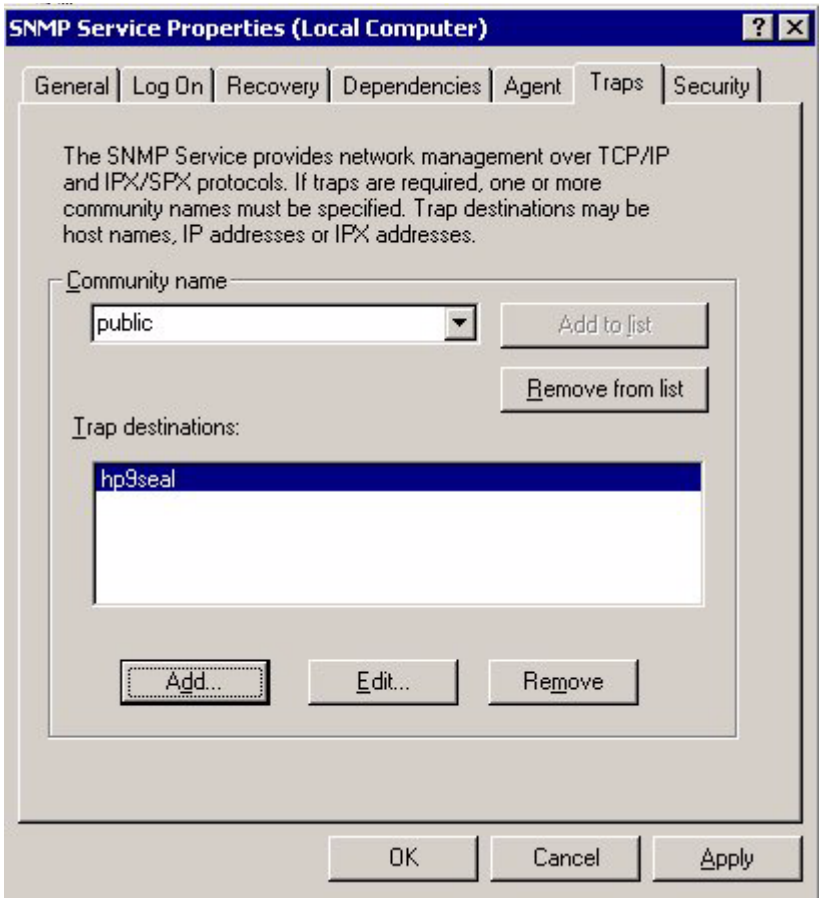
1 On your Windows server, open Services by using one of the usual Windows methods.



2 In the Computer Management window, double-click the **SNMP Service** option from the list in the right-hand pane.

3 On the General tab, stop the SNMP Service.

4 In the SNMP Service Properties window, select the Traps tab.



5 In the Community name field, enter a value. The default value is “public.” Also, enter the name of the target host on the Trap destinations field. The target host is the SNMP management system, such as HP OpenView. In this example, **hp9seal** is the name of the SNMP management system.

6 Select the Security tab.

7 Edit the Community entry (that is, “public”), and change the security to “READ WRITE.”

8 Ensure your “Accept SNMP packets ...” setting is correct for your security requirements.

9 Click **Apply**.

10 On the General tab, start the SNMP Service.

11 If “Startup type” is not set to “Automatic,” consider changing it to start the SNMP Service automatically whenever the server is restarted.

12 Click **OK** to close the SNMP Server Properties dialog box.

Configuring and using SNMP traps

This section describes how to test the SNMP trap mechanisms and then describes how to configure the fn_trapd daemon.

Testing the functionality of SNMP traps

To test the functionality of the SNMP traps, use the **traptest** utility, which exercises the SNMP trap mechanisms.

1. At the command prompt on your FileNet Image Services server, enter the following command:

   traptest

2. The output looks similar to the following example:

```
hpdpheny(root)/> # traptest
Entering traptest program!!
Sent trap successfully - leaving traptest program!!
hpdoheny(root)/>
```

3. Look at the system log and it should have an entry similar to the following:

```
2000/06/20 11:41:38.408 202,9,4 <root> traptest (5081) ...
An SNMP trap was issued for this error with trap code ce000002, trap severity '4'
Severe
```

4. Open the SNMP management software on the SNMP management system (for example, HP OpenView).

5 Look at the **All Alarms Browser**. If SNMP is configured and running correctly, the browser will show a **Normal** trap from the FileNet Image Services server where you earlier ran the traptest command.

Configuring SNMP Traps from within the FileNet MIB

Configuring the fn_trapd daemon can be done from within the FileNet MIB. This section describes the method for configuring the fn_trapd daemon using HP OpenView. For the purposes of this configuration, you will set a Poll Trap on the permanent database to be sent every five minutes. This trap will be one indicating the size of the database is larger than the specified Poll Trap threshold level.

Running the HP OpenView MIB Browser

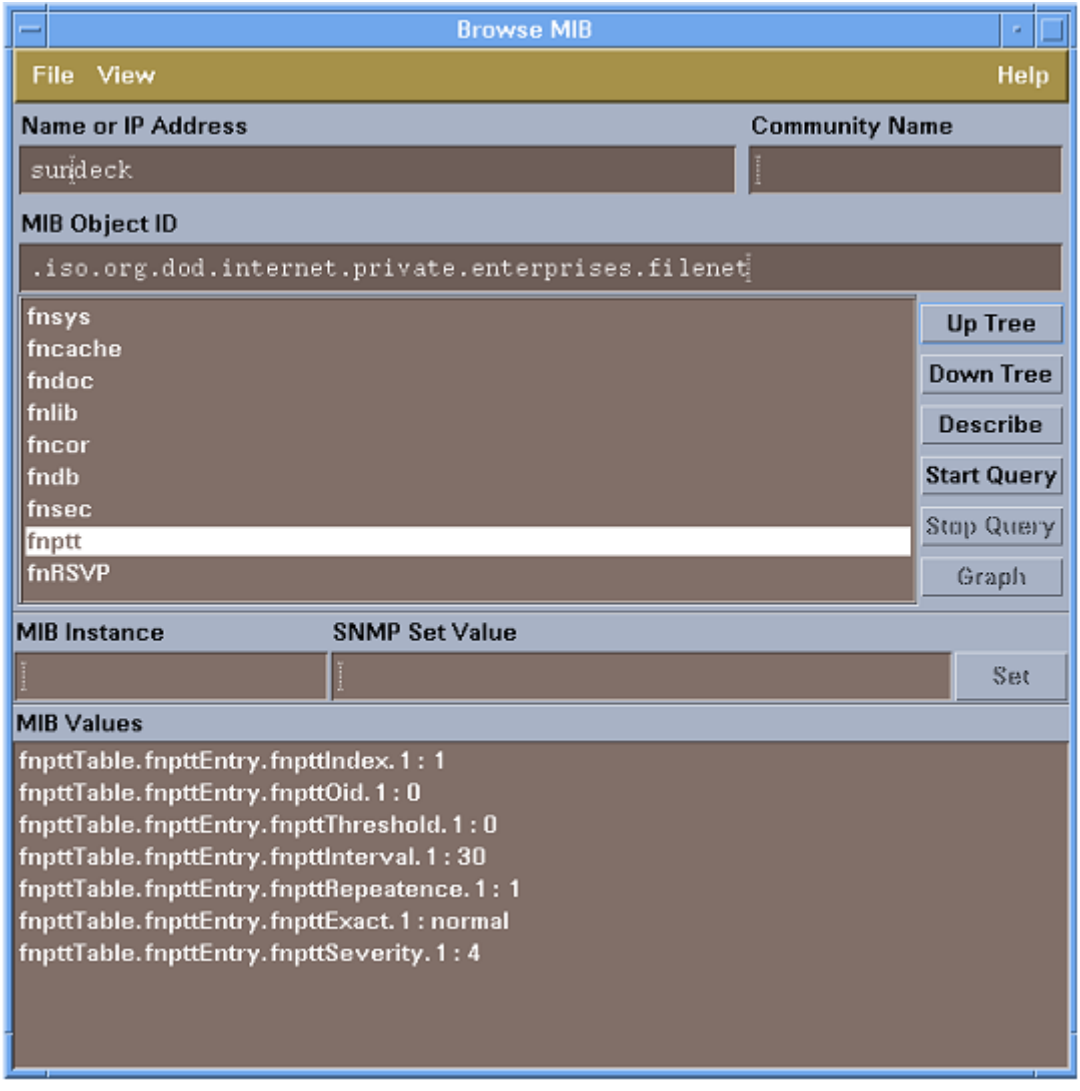
1 Activate HP OpenView on the SNMP management system.

2 Select the **Tools** option and then select the **SNMP MIB Browser** option.

3 In the Name or IP Address box, type in the name of the target FileNet Image Services server. Use the FileNet Image Services system's Root/Index server on multiple server systems.

4 Click the Down Tree button to move down the MIB naming tree through **Private**, through **enterprises** to **filenet**.

5 Highlight the fnptt MIB Object ID (OID) and click the **Start Query** button. You should see query result similar to the following example.

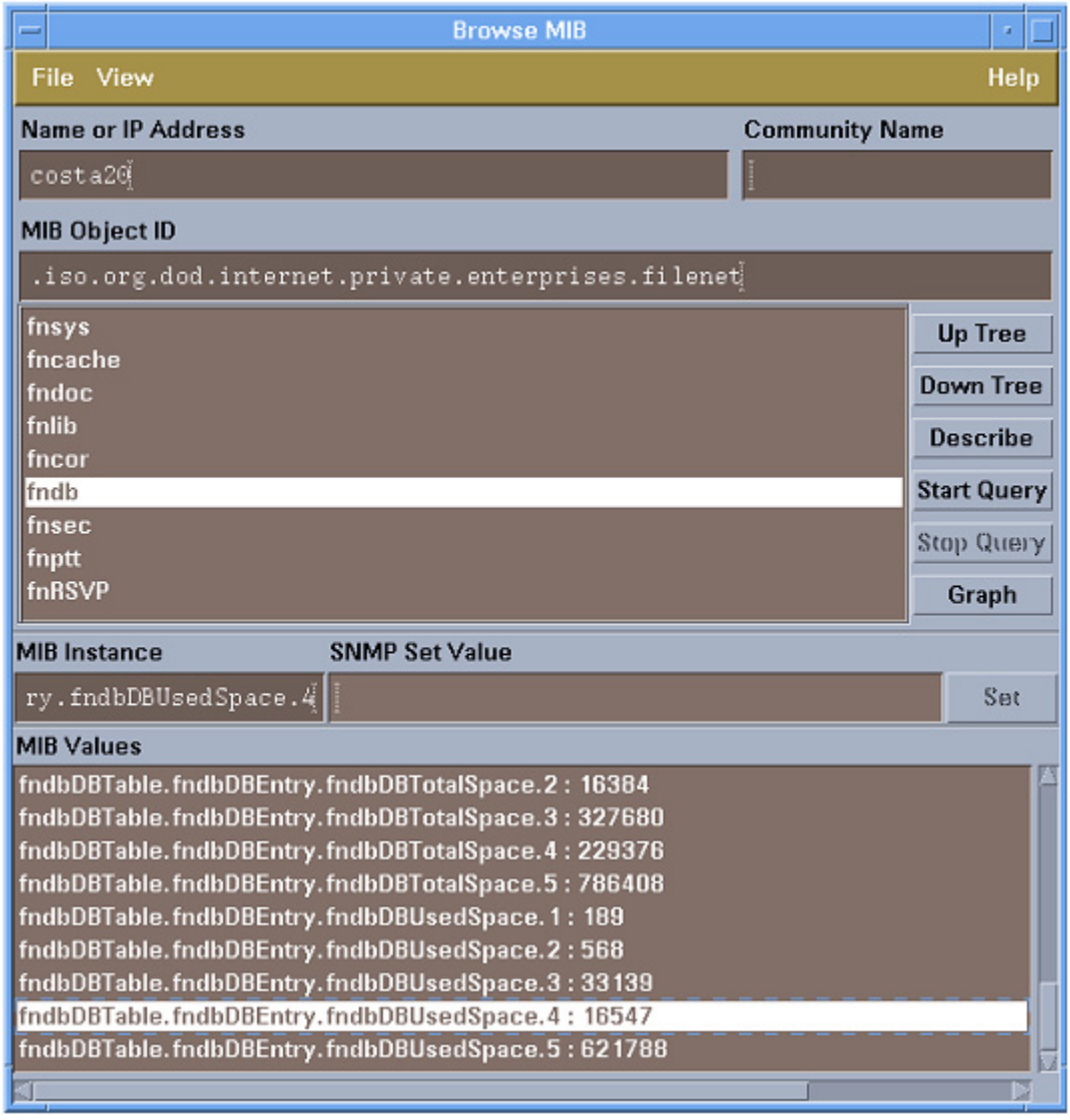

Browse MIB
File View Help
Name or IP Address
Community Name
sunideck
MIB Object ID
.iso.org.dod.internet.private.enterprises.filenet
fnsys
fncache
fndoc
fnlib
fncor
fndb
fnsec
fnptt
fnRSVP
Up Tree
Down Tree
Describe
Start Query
Stop Query
Graph
MIB Instance
SNMP Set Value
Set
MIB Values
fnpttTable.fnpttEntry.fnpttIndex.1 : 1
fnpttTable.fnpttEntry.fnpttOid.1 : 0
fnpttTable.fnpttEntry.fnpttThreshold.1 : 0
fnpttTable.fnpttEntry.fnpttInterval.1 : 30
fnpttTable.fnpttEntry.fnpttRepeatence.1 : 1
fnpttTable.fnpttEntry.fnpttExact.1 : normal
fnpttTable.fnpttEntry.fnpttSeverity.1 : 4

Note If you get an error, you must verify that everything is properly configured. Return to **"Configuring the Master SNMP Daemon" on page 40** to start troubleshooting the problem.

Configuring Poll Trap on the permanent database

1 From the same **SNMP MIB Browser**, run a MIB Query on the **fndb** MIB Object ID to discover the **DBUsedSpace** for the permanent database as shown in the following example.

In the following example, OID number **4** is the permanent database.


Browse MIB
File View
Help
Name or IP Address
Community Name
costa20
MIB Object ID
.iso.org.dod.internet.private.enterprises.filenet
fnsys
fncache
fndoc
fnlib
fncor
fndb
fnsec
fnptt
fnRSVP
Up Tree
Down Tree
Describe
Start Query
Stop Query
Graph
MIB Instance
SNMP Set Value
ry.fndbDBUsedSpace.4
Set
MIB Values
fndbDBTable.fndbDBEntry.fndbDBTotalSpace.2 : 16384
fndbDBTable.fndbDBEntry.fndbDBTotalSpace.3 : 327680
fndbDBTable.fndbDBEntry.fndbDBTotalSpace.4 : 229376
fndbDBTable.fndbDBEntry.fndbDBTotalSpace.5 : 786408
fndbDBTable.fndbDBEntry.fndbDBUsedSpace.1 : 189
fndbDBTable.fndbDBEntry.fndbDBUsedSpace.2 : 568
fndbDBTable.fndbDBEntry.fndbDBUsedSpace.3 : 33139
fndbDBTable.fndbDBEntry.fndbDBUsedSpace.4 : 16547
fndbDBTable.fndbDBEntry.fndbDBUsedSpace.5 : 621788

Tip For details on the FileNet MIB table, go to **"How the MIB Is organized and used" on page 29**.

2 In the previous example, the permanent database has a value of 16547, and you want to establish a Poll Trap threshold smaller than that number. Highlight the **fnptt** Mib **OID**, and then click the **Start Query** button.

3 Next, select the **fnpttTable.fnpttEntry.fnpttOid.1:0** entry.

4 In the SNMP Set Value box, input **6.1.1.7.4** and then click the **Set** button and click **Close** at the Information Window.

5 Start the query on the **fnptt** OID again by repeating Step 2. When this completes, you see that a new OID numbered 2 has been created with a value of 0. In this example, you will be working with OID number 1, which has a value of 6.1.1.7.4.

Tip There will always be an Object ID with a value of 0, by default. After recycling the FileNet software, this Object ID will become OID number 1 with a value of 0. When a new OID is entered, then there will be an OID number two with a value of 0 in addition to the new one just entered.

6 Next, select the **.fntppThreshold.1** MIB Value.

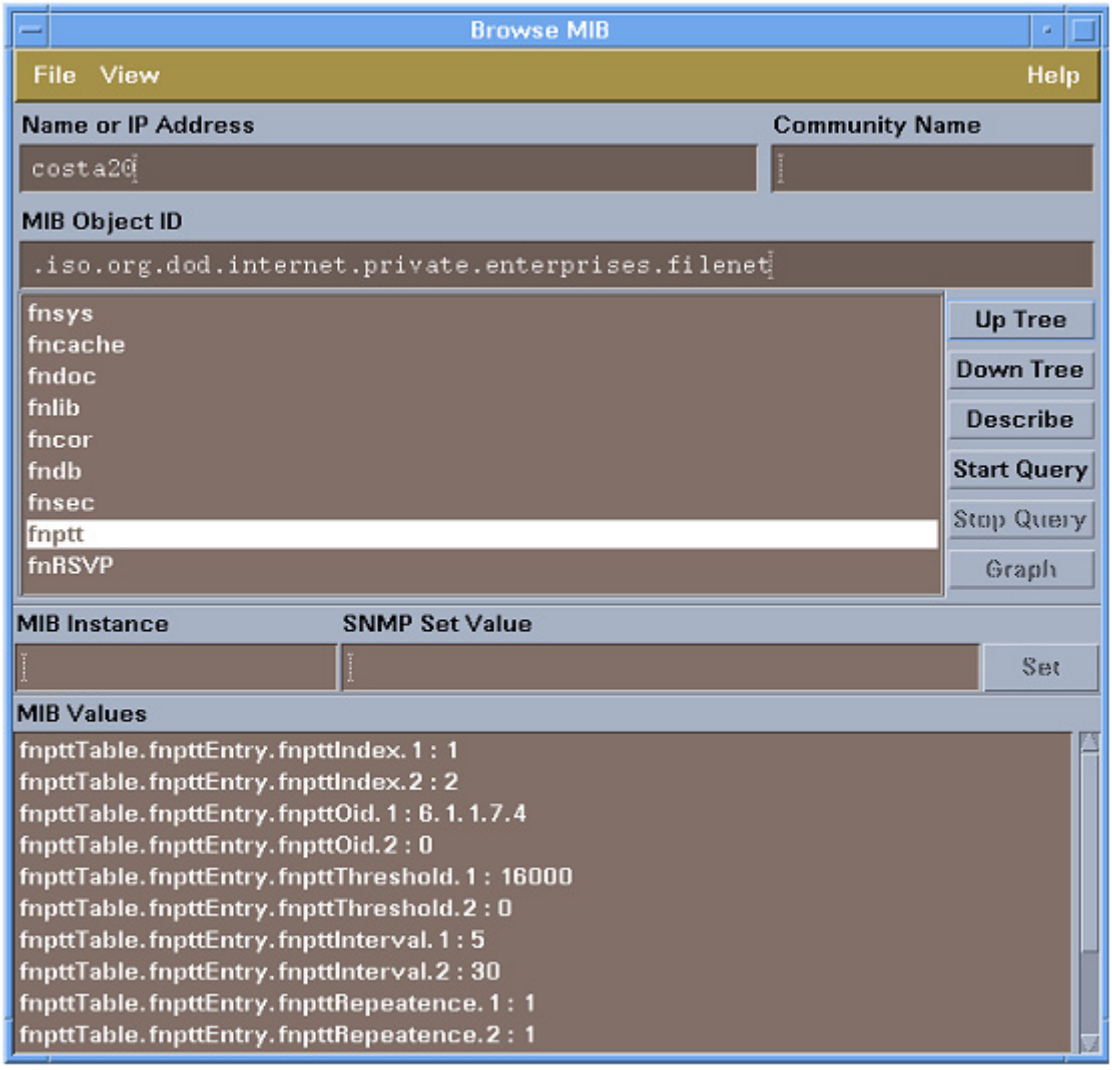
7 In the SNMP Set Value box, enter **16000** and then click the **Set** button and click **Close** at the Information Window.

8 Next, select the **.fnpttInterval.1** MIB Value.

9 In the SNMP Set Value box, enter 5 (for every 5 minutes) and then click the **Set** button and click **Close** at the Information Window.

Tip If you get a **Warning** window, click **Close**. This warning is common with the HP OpenView MIB Browser.

10 Select the **fnptt** MIB OID and then click the **Start Query** button. The query results should match the output shown in the following example:


Browse MIB
File View Help
Name or IP Address
Community Name
costa20
MIB Object ID
.iso.org.dod.internet.private.enterprises.filenet
fnsys
fncache
fndoc
fnlib
fncor
fndb
fnsec
fnptt
fnRSVP
Up Tree
Down Tree
Describe
Start Query
Stop Query
Graph
MIB Instance
SNMP Set Value
Set
MIB Values
fnpttTable.fnpttEntry.fnpttIndex.1 : 1
fnpttTable.fnpttEntry.fnpttIndex.2 : 2
fnpttTable.fnpttEntry.fnpttOid.1 : 6.1.1.7.4
fnpttTable.fnpttEntry.fnpttOid.2 : 0
fnpttTable.fnpttEntry.fnpttThreshold.1 : 16000
fnpttTable.fnpttEntry.fnpttThreshold.2 : 0
fnpttTable.fnpttEntry.fnpttInterval.1 : 5
fnpttTable.fnpttEntry.fnpttInterval.2 : 30
fnpttTable.fnpttEntry.fnpttRepeatence.1 : 1
fnpttTable.fnpttEntry.fnpttRepeatence.2 : 1

11 After a few moments, your SNMP Management system's Alarm Browser will start receiving Poll Trap Messages as shown in the following example:

```
Ack Cor Severity  Date/Time             Source        Message
         Normal  Tue Jun 20 15:25:26  Costa20       Received event 1.3.6.1.4.1.517
         Normal  Tue Jun 20 15:30:26  Costa20       Received event 1.3.6.1.4.1.517
         Normal  Tue Jun 20 15:35:26  Costa20       Received event 1.3.6.1.4.1.517
```

By scrolling to the right, you will see the Poll Trap shows the FileNet OID number, the Threshold and the Current data, indicating the size of the permanent database has become bigger than the specified Poll Trap threshold. This Poll Trap will occur every 5 minute as you specified earlier in the Poll Trap configuration.

Deleting the Poll Trap

1 From the same **SNMP MIB Browser**, select the **fnptt** MIB OID and then click the **Start Query** button.

2 Next, select the **fnpttTable.fnpttEntry.fnpttOid.1:6.1.1.7.4** entry.

3 In the SNMP Set Value box, enter **0** and then click the **Set** button and click **Close** at the Information Window.

4 Start the query on the **fnptt** Object ID again by repeating Step 2. Once this completes, you see that OID.2 still has a value of 0, indicating there are now no Poll Traps configured.

Configuring SNMP traps by editing the ptt.ini file

Configuring poll traps can be done by manually editing the **ptt.ini** file This section describes the method for configuring poll traps by editing the ptt.ini file using your preferred text editor. For the purposes of this configuration, you will set three Poll Traps: one for system uptime, one for library status, and one for used database space.

Important A ptt.ini file does not exist until a Poll Trap is configured, or until the file is manually created. Also, after it is created, the file is not automatically deleted.

1 Edit the ptt.ini by shutting down the FileNet software and then entering the following command:

vi /fnsw/etc/ptt.ini UNIX
edit \fnsw\etc\ptt.ini Windows

Because the ptt.ini file is periodically updated by the system, the software could need to be shutdown to ensure that your changes aren't overwritten while editing. Changes to the file will take effect immediately after FileNet Image Services is brought up or recycled. If you edit the ptt.ini file while FileNet Image Services is up, the changes will take effect on the next cycle of the Poll Trap Daemon.

2 Add a table to the file, similar to the following example:

```
#Oid Threshold Interval Repeatence Exact Severity
#--- --------- -------- ---------- ----- --------
1.5.1 0 2 0 2 4                #fnsysUpTime
4.1.1.3.2 2 10 0 1 4           #fnlibLibStatus (library 2 disabled)
6.1.1.7.4 100 5 0 1 4          #fndbDBUsedSpace (DB 4)
0 0 30 0 1 4
```

Keep all comments (“#”) at the top of the file and note that any in-line comments (comments to the right of the data values) can be erased if you mix manual updates with SNMP manager updates. Some important points to note:

- Deconfiguring all Poll Traps will result in a ptt.ini file with a default entry as shown in the last line in the previous example with the Interval value of 30.
- When using a MIB browser, you could see a ptt.ini file like the following:

```
#Oid Threshold Interval Repeatence Exact Severity
#--- --------- -------- ---------- ----- --------
#--- Everything below this line will be deleted ---
0 0 30 0 1 4
```

  This is not a cause for alarm. It is stating that everything below the line is subject to deletion. This occurs after removing all the OIDs using a MIB browser (such as the one in HPOpenView) rather than manually editing the file. Additionally, to get this deletion notification, a ptt.ini file with comments in it already must exist.

- The final row in the ptt.ini file always has an fnpttOID value of **zero**. This indicates “end of table”.

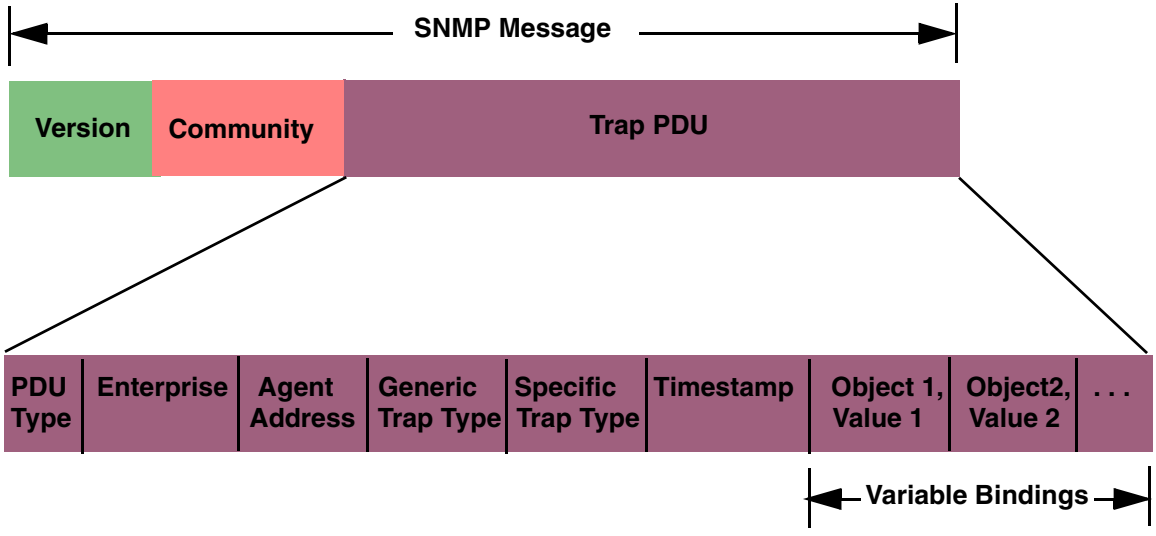
3 Save the file.

Reading a trap

PDU overview

An SNMP trap has a distinct Protocol Data Unit (PDU) with various fields, each with a purpose. The following graphic (Copyright © *Miller, Mark A, P.E., Managing Internetworks with SNMP, M&T Books, 1999*) illustrates the general contents of each of those fields.

SNMP Trap PDU Structure



Specific FileNet PDU formats

There are two types of FileNet PDU formats: poll traps and default traps.

Poll traps

Poll traps are user-configurable traps in the sense that you can set thresholds against any MIB value in any of the eight FileNet MIB filenet.my allows you to monitor. See **“FileNet Poll Trap Table Group” on page 89**.

The FileNet Poll Trap reports three objects in the trap PDU:

Object1	Poll Trap index
Object2	fnsysLastErrorSeverity
Object3	fnsysLastErrorText

Default traps

Default traps are traps that are not configurable by the user.

The FileNet default traps reports five objects in the trap PDU:

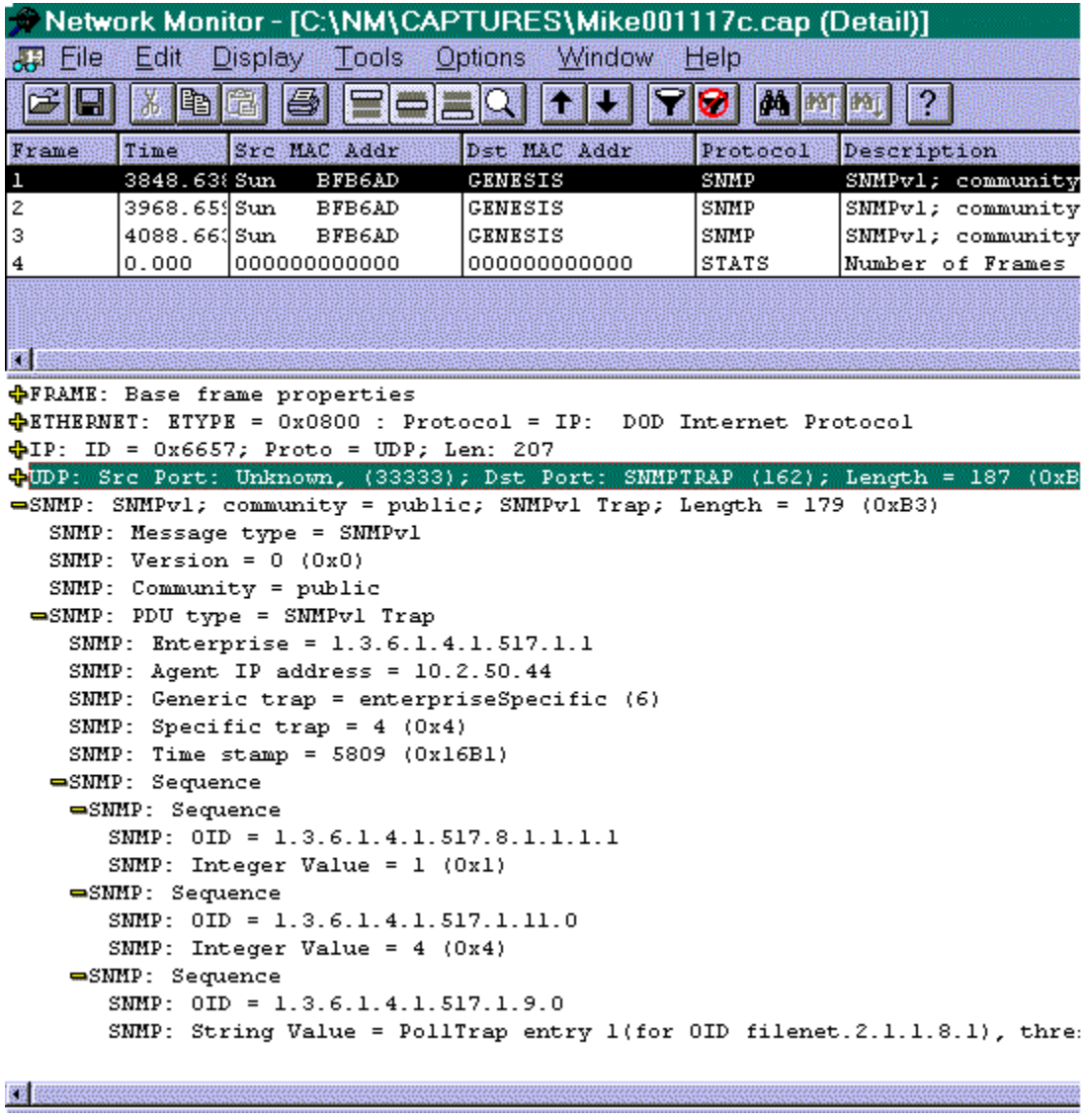
Object1	fnsysLastErrorCategory
Object2	fnsysLastErrorFunction
Object3	fnsysLastErrorNumber
Object4	fnsysLastErrorText
Object5	fnsysLastErrorSeverity

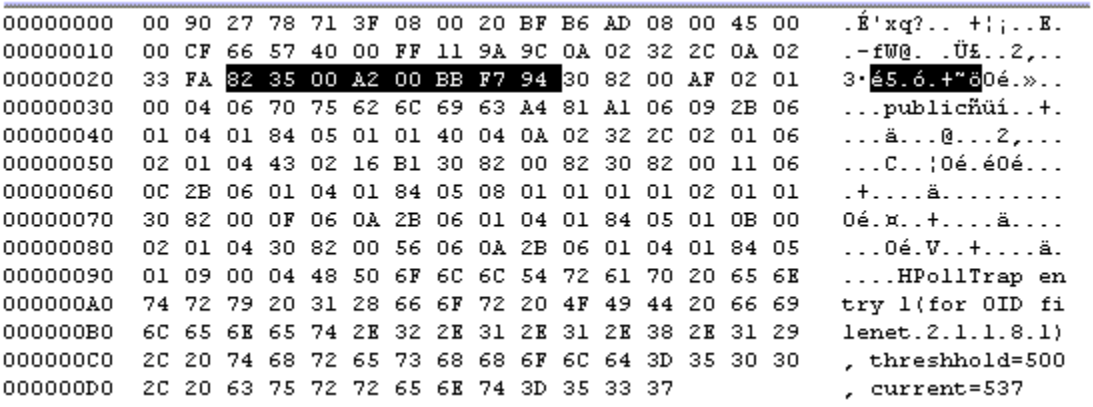
Default traps include:

- FileNet software stopped
- System aborted a process
- Signal killed a process
- SNMP has an internal error
- Server rejected an RPC connection due to a lack of service request handlers
- Error occurred, disabling the storage library or the optical drive
- Storage library needs operator intervention

PDU example

After a trap has been created, there are various third party tools that can be used to help you read and understand it. The following screens are just such an example using Microsoft's Network Monitor. Notice how the fields described earlier in the graphic on **page 66** are depicted in the following screens.


Network Monitor - [C:\NM\CAPTURES\Mike001117c.cap (Detail)]
File Edit Display Tools Options Window Help
Frame Time Src MAC Addr Dst MAC Addr Protocol Description
1 3848.63 Sun BFB6AD GENESIS SNMP SNMPv1; community
2 3968.65 Sun BFB6AD GENESIS SNMP SNMPv1; community
3 4088.66 Sun BFB6AD GENESIS SNMP SNMPv1; community
4 0.000 000000000000 000000000000 STATS Number of Frames
FRAME: Base frame properties
ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol
IP: ID = 0x6657; Proto = UDP; Len: 207
UDP: Src Port: Unknown, (33333); Dst Port: SNMPTRAP (162); Length = 187 (0xB
SNMP: SNMPv1; community = public; SNMPv1 Trap; Length = 179 (0xB3)
SNMP: Message type = SNMPv1
SNMP: Version = 0 (0x0)
SNMP: Community = public
SNMP: PDU type = SNMPv1 Trap
SNMP: Enterprise = 1.3.6.1.4.1.517.1.1
SNMP: Agent IP address = 10.2.50.44
SNMP: Generic trap = enterpriseSpecific (6)
SNMP: Specific trap = 4 (0x4)
SNMP: Time stamp = 5809 (0x16B1)
SNMP: Sequence
SNMP: Sequence
SNMP: OID = 1.3.6.1.4.1.517.8.1.1.1.1
SNMP: Integer Value = 1 (0x1)
SNMP: Sequence
SNMP: OID = 1.3.6.1.4.1.517.1.11.0
SNMP: Integer Value = 4 (0x4)
SNMP: Sequence
SNMP: OID = 1.3.6.1.4.1.517.1.9.0
SNMP: String Value = PollTrap entry 1(for OID filenet.2.1.1.8.1), thre:



```
00000000  00 90 27 78 71 3F 08 00 20 BF B6 AD 08 00 45 00   .É'xq?.. +¦¡..E.
00000010  00 CF 66 57 40 00 FF 11 9A 9C 0A 02 32 2C 0A 02   .-fW@. .Ü£..2,..
00000020  33 FA 82 35 00 A2 00 BB F7 94 30 82 00 AF 02 01   3·é5.ó.+˜ö0é.»..
00000030  00 04 06 70 75 62 6C 69 63 A4 81 A1 06 09 2B 06   ...publicñüí..+.
00000040  01 04 01 84 05 01 01 40 04 0A 02 32 2C 02 01 06   ...ä...@...2,...
00000050  02 01 04 43 02 16 B1 30 82 00 82 30 82 00 11 06   ...C..¦0é.é0é...
00000060  0C 2B 06 01 04 01 84 05 08 01 01 01 01 02 01 01   .+....ä.........
00000070  30 82 00 0F 06 0A 2B 06 01 04 01 84 05 01 0B 00   0é.¤..+....ä....
00000080  02 01 04 30 82 00 56 06 0A 2B 06 01 04 01 84 05   ...0é.V..+....ä.
00000090  01 09 00 04 48 50 6F 6C 6C 54 72 61 70 20 65 6E   ....HPollTrap en
000000A0  74 72 79 20 31 28 66 6F 72 20 4F 49 44 20 66 69   try 1(for OID fi
000000B0  6C 65 6E 65 74 2E 32 2E 31 2E 31 2E 38 2E 31 29   lenet.2.1.1.8.1)
000000C0  2C 20 74 68 72 65 73 68 68 6F 6C 64 3D 35 30 30   , threshhold=500
000000D0  2C 20 63 75 72 72 65 6E 74 3D 35 33 37            , current=537
```

Appendix B – Objects in the FileNet MIB

The tables in this appendix list the objects in the FileNet MIB that an SNMP-compliant network manager can monitor. Many of these MIBs can be configured for poll traps (page 35). For more information, go to "Configuring and using SNMP traps" on page 55. Using standard SNMP-management software, you can modify entries in the poll trap table (see "FileNet Poll Trap Table Group" on page 89) to customize traps.

Important

In these tables (except for the Poll Trap Table Group itself), you will see a column to the right of the OID column. This column is designed to help you set Poll Traps by adding either an additional **.1** as shown or a .number (**.#**) as shown that corresponds to the number of the specific database, cache, or library you want to be monitored and set the Poll Trap to. For example, on many FileNet Image Services systems the Permanent Database is number 4. So, any Poll Trap to be configured on the Permanent Database would have the OID end with "**.4**". For more detail, see "Configuring Poll Trap on the permanent database" on page 58.

FileNet System Group

Object	OID 1.3.6.1.4.1.517...	Poll Trap OID 1.3.6.1.4.1.517...	Description
fnsysDomain	...1.1	...1.1**.1**	Name of the domain to which this server belongs
fnsysOrganization	...1.2	...1.2**.1**	Organization to which this server belongs

FileNet System Group, Continued

Object	OID 1.3.6.1.4.1.517...	Poll Trap OID 1.3.6.1.4.1.517...	Description
fnsysSSN	...1.3	...1.3**.1**	System serial number for this server
fnsysServerType	...1.4	...1.4**.1**	Type of FileNet server
fnsysUpTime	...1.5	...1.5**.1**	Time (in hundredths of a second) since the FileNet system software was last re-initialized
fnsysLastErrorCategory	...1.6	...1.6**.1**	Category (upper 8 bits) of the FileNet error tuple corresponding to the last error for which a trap was sent A zero value is meaningless.
fnsysLastErrorFunction	...1.7	...1.7**.1**	The error function code (bits 16 through 23) of the FileNet error tuple corresponding to the last error for which a trap was sent This function code represents an area within a FileNet logical subsystem. A zero value is meaningless.
fnsysLastErrorNumber	...1.8	...1.8**.1**	The error number (least significant 16 bits) of the FileNet error tuple corresponding to the last error for which a trap was sent This error number represents a specific FileNet error condition. A zero value is meaningless.
fnsysLastErrorText	...1.9	...1.9**.1**	A human-readable description of the condition which caused the last trap to be sent and suggested corrective actions
fnsysLastErrorTime	...1.10	...1.10**.1**	The value of fnsysUpTime when the last FileNet trap was sent

FileNet System Group, Continued

Object	OID 1.3.6.1.4.1.517...	Poll Trap OID 1.3.6.1.4.1.517...	Description
fnsysLastErrorSeverity	...1.11	...1.11**.1**	The severity level of the last trap issued: ok (1): Normal status warning (2): Low resource condition or non-fatal error operator (3): Normal condition requiring operator intervention severe (4): Fatal error causing (or could soon cause) one or more services to become disabled invalid (100): Invalid entry—disregard
fnsysOKTrapFlag	...1.12	...1.12**.1**	Flag used to disable the cold start trap normally issued when the FileNet Proxy Daemon (fn_snmpd) process is started
fnsysWarningTrapFlag	...1.13	...1.13**.1**	Flag used to disable FileNet traps with a severity level of WARNING These traps normally indicate low resource conditions or non-fatal software problems. Low resource conditions could lead to error conditions if not attended to.

FileNet System Group, Continued

Object	OID 1.3.6.1.4.1.517...	Poll Trap OID 1.3.6.1.4.1.517...	Description
fnsysOperatorTrapFlag	...1.14	...1.14**.1**	Flag used to disable FileNet traps that indicate when a normal event which requires operator intervention has occurred
fnsysSevereTrapFlag	...1.15	...1.15**.1**	Flag used to disable FileNet traps that are very severe or fatal These traps normally indicate that one or more FileNet services has been shut down, or could soon be shut down, due to a fatal error or resource problem.
fnsysServiceTable	...1.16	Cannot set Poll Traps	The FileNet available services table This table contains one row for each FileNet service type that supports SNMP running on this server. The next two objects define the table: fnsysServiceEntry FnsysServiceEntry
fnsysServiceEntry	...1.16.1	Cannot set Poll Traps	An entry in the FileNet available services table

FileNet System Group, Continued

Object	OID 1.3.6.1.4.1.517...	Poll Trap OID 1.3.6.1.4.1.517...	Description
FnsysServiceEntry	- - - - - - - -	- - - - - - - -	The sequence of objects in the FileNet available services table: fnsysServiceIndex fnsysServiceType fnsysServiceDescription fnsysServiceProcesses fnsysServiceMaxProcesses fnsysServiceRejects
fnsysServiceIndex	...1.16.1.1	Cannot set Poll Traps	An index that uniquely identifies a service on a FileNet server
fnsysServiceType	...1.16.1.2	Cannot set Poll Traps	The type of FileNet service: nch, csm, doc, inx, pri, bes, osar, sec, sql, file, wqs
fnsysServiceDescription	...1.16.1.3	Cannot set Poll Traps	A human-readable description of a FileNet service
fnsysServiceProcesses	...1.16.1.4	Cannot set Poll Traps	The number of server processes running for this service type
fnsysServiceMaxProcesses	...1.16.1.5	Cannot set Poll Traps	The maximum number of server processes that could be started for this service type
fnsysServiceRejects	...1.16.1.6	Cannot set Poll Traps	The number of times connections were rejected because no processes of this server type were available

See the **Note** on page 71 for information on the use of **.#** in the OID.

FileNet Cache Group

Description	OID 1.3.6.1.4.1.517...	Poll Trap OID 1.3.6.1.4.1.517...	Object
fncacheTable	...2.1	- - - - - - - -	The FileNet available caches table
fncacheEntry	...2.1.1	- - - - - - - -	An entry in the FileNet available caches table
FncacheEntry	- - - - - - - -	- - - - - - - -	The sequence of objects in the FileNet available caches table: fncacheID fncacheName fncacheDescription fncacheMinSectors fncacheMaxSectors fncacheFreeSectors fncacheLockedSectors fncacheInUseSectors fncacheLockedObjects fncacheInUseObjects
fncacheID	...2.1.1.1	...2.1.1.1.#	The CSM cache ID of this cache
fncacheName	...2.1.1.2	...2.1.1.2.#	The NCH name of the FileNet cache
fncacheDescription	...2.1.1.3	...2.1.1.3.#	A human-readable description of the FileNet cache
fncacheMinSectors	...2.1.1.4	...2.1.1.4.#	The minimum number of sectors allocated for this cache
fncacheMaxSectors	...2.1.1.5	...2.1.1.5.#	The maximum number of sectors allocated for this cache

FileNet Cache Group, Continued

Description	OID 1.3.6.1.4.1.517...	Poll Trap OID 1.3.6.1.4.1.517...	Object
fncacheFreeSectors	...2.1.1.6	...2.1.1.6**.#**	The number of sectors reserved for this cache, but unused
fncacheLockedSectors	...2.1.1.7	...2.1.1.7**.#**	The number of sectors locked in this cache
fncacheInUseSectors	...2.1.1.8	...2.1.1.8**.#**	The number of sectors currently in use in this cache
fncacheLockedObjects	...2.1.1.9	...2.1.1.9**.#**	The number of CSM objects currently locked in this cache
fncacheInUseObjects	...2.1.1.10	...2.1.1.10**.#**	The number of CSM objects in use in this cache

FileNet Document Services Group

Object	OID 1.3.6.1.4.1.517...	Poll Trap OID 1.3.6.1.4.1.517...	Description
fndocPagesMigrated	...3.1	...3.1**.1**	Requested Pages Migrated to Magnetic Disk: • Reports the number of pages requested to be migrated to optical disk on this Storage Library server since FileNet Image Services was last recycled. • The number of pages will always be greater than or equal to the number of individual documents.
fndocDocsMigrated	...3.2	...3.2**.1**	Requested Documents Migrated to Magnetic Disk: • Reports the number of documents requested to be migrated to optical disk. • The number of documents will always be less than or equal to the number of individual documents.
fndocCacheHits	...3.3	...3.3**.1**	Magnetic Disk Cache Hits: Reports the number of times a request was satisfied by finding a document in cache.

FileNet Document Services Group, Continued

Object	OID 1.3.6.1.4.1.517...	Poll Trap OID 1.3.6.1.4.1.517...	Description
fndocDriveHits	...3.4	...3.4**.1**	Optical Drive Hits: • Reports the number of times a request was satisfied by finding a document on storage media already in a drive. • Disk loads are **not** counted when the requested platter is in a slot but needs to be loaded, or for RSVPs, the platter isn't in the library at all, and must be loaded by an operator. • Therefore, the number of Magnetic disk cache hits plus the number of Optical drive hits is less than or equal to the number of requested pages migrated to magnetic disk.
fndocPrefetchCalls	...3.5	...3.5**.1**	Number of DOC_prefetch_from_ optical_disk calls made
fndocAsyncMigrateCalls	...3.6	...3.6**.1**	Number of DOC_migrate_from_optical_ disk calls that used asynchronous notification
fndocMigrateCalls	...3.7	...3.7**.1**	Total number of DOC_migrate_from_ optical_disk calls
fndocPagesCommitted	...3.8	...3.8**.1**	Pages Committed: This field shows how many pages were committed to the permanent database.

FileNet Document Services Group, Continued

Object	OID 1.3.6.1.4.1.517...	Poll Trap OID 1.3.6.1.4.1.517...	Description
fndocDocsCommitted	...3.9	...3.9**.1**	Documents Committed: This field shows how many documents were committed to the permanent database.
fndocImportReads	...3.10	...3.10**.1**	Optical Disk Reads for Import • This counts the number of short descriptors read from storage media during import. • There can legitimately be multiple short descriptors in the optical disk directory per document. • Therefore, the optical disk reads per import is greater than or equal to the actual number of documents imported.
fndocImportedDocs	...3.11	...3.11**.1**	Documents Imported to System: • This field shows the number of documents committed to the permanent database by the import operation. • This is a count of the updates to the docs table database.
fndocFastBatches	...3.12	...3.12**.1**	This field shows how many batches committed used Fast Batch Committal. In addition to be a configuration option, remote committal and COLD both use Fast Batch Committal.

FileNet Document Services Group, Continued

Object	OID 1.3.6.1.4.1.517...	Poll Trap OID 1.3.6.1.4.1.517...	Description
fndocFastPages	...3.13	...3.13**.1**	This field shows how many pages used Fast Batch Committal.
fndocFastDocs	...3.14	...3.14**.1**	This field shows how many documents used Fast Batch Committal.

See the **Note** on page 71 for information on the use of **.#** in the OID.

FileNet Storage Library Group

Object	OID 1.3.6.1.4.1.517...	Poll Trap OID 1.3.6.1.4.1.517...	Description
fnlibLibTable	...4.1	- - - - - - - - -	The FileNet storage libraries table
fnlibLibEntry	...4.1.1	- - - - - - - - -	An entry in the FileNet storage libraries table
FnlibLibEntry	- - - - - - - - -	- - - - - - - - -	The sequence of objects in the FileNet storage libraries table: fnlibLibID fnlibLibType fnlibLibStatus fnlibLibTotalDrives fnlibLibDisabledDrives fnlibLibArmMoves fnlibLibLoads fnlibLibUnloads
fnlibLibID	...4.1.1.1	...4.1.1.1.#	Library services ID of this storage library

FileNet Storage Library Group, Continued

Object	OID 1.3.6.1.4.1.517...	Poll Trap OID 1.3.6.1.4.1.517...	Description
fnlibLibType	...4.1.1.2	...4.1.1.2.#	Type of a storage library. They are as follows: standard(1) - FileNet OSAR mini(2) - Hitachi Library (MOSAR) access(3) - Access Library rapidc(4) - Philips Rapid Changer LF4500 hp(5) - HP Library ibm(6) - IBM Library fnodset(7) - FileNet Optical Drive Set hitodset(8) - Hitachi Optical Drive Set hpodset(9) - HP Optical Drive Set ibmodset(10) - IBM Optical Drive Set rapidc2(11) - Philips Rapid Changer LF6600 rapidc3(12) - Philips Rapid Changer LF8600 msar(13) - MSAR ivalid(100) - Invalid value!
fnlibLibStatus	...4.1.1.3	...4.1.1.3.#	Status of a FileNet storage library: enabled, disabled, manual, invalid
fnlibLibTotalDrives	...4.1.1.4	...4.1.1.4.#	Number of drives in a FileNet storage library
fnlibLibDisabledDrives	...4.1.1.5	...4.1.1.5.#	Number of disabled drives in a FileNet storage library

FileNet Storage Library Group, Continued

Object	OID 1.3.6.1.4.1.517...	Poll Trap OID 1.3.6.1.4.1.517...	Description
fnlibLibArmMoves	...4.1.1.6	...4.1.1.6.#	Number of times this storage library's arm has moved
fnlibLibLibLoads	...4.1.1.7	...4.1.1.7.#	Number of times an operator loaded media into the storage library
fnlibLibUnloads	...4.1.1.8	...4.1.1.8.#	Number of times an operator unloaded media from the storage library

FileNet Courier Group

Object	OID 1.3.6.1.4.1.517...	Poll Trap OID 1.3.6.1.4.1.517...	Description
fncorApprConns	...5.1	...5.1**.1**	Number of connections approved by COR_ listen
fncorBadConns	...5.2	...5.2**.1**	Number of connections that timed out or terminated abnormally
fncorRejectConns	...5.3	...5.3**.1**	Number of connections rejected by COR_ listen/PPM
fncorAbortConns	...5.4	...5.4**.1**	Number of connections aborted by COR
fncorClientConns	...5.5	...5.5**.1**	The number of client connections opened through COR_Open
fncorClientFails	...5.6	...5.6**.1**	The number of client COR_Open attempts that failed for any reason

See the **Note** on page 71 for information on the use of **.#** in the OID.

FileNet Database Group

Object	OID 1.3.6.1.4.1.517...	Poll Trap OID 1.3.6.1.4.1.517...	Description
fndbDBTable	...6.1	- - - - - - - - -	The FileNet database table
fndbDBEntry	...6.1.1	- - - - - - - - -	An entry in the FileNet database table
FndbDBEntry	- - - - - - - - -	- - - - - - - - -	The sequence of objects in the database table: fndbDBID fndbDBType fndbDBClients fndbDBLocation fndbDBDescription fndbDBTotalSpace fndbDBUsedSpace
fndbDBID	...6.1.1.1	...6.1.1.1**.#**	The unique integer assigned to this row
fndbDBType	...6.1.1.2	...6.1.1.2**.#**	The type of the FileNet database: mkf, oracle, mssql, DB2®, or invalid
fndbDBClients	...6.1.1.3	...6.1.1.3**.#**	A value, indicating the set of FileNet services that store data in this database The services include inx, wqs, sqi, nch, doc, bes, csm, sec, pri.
fndbDBLocation	...6.1.1.4	...6.1.1.4**.#**	The file system pathname for the database file or partition
fndbDBDescription	...6.1.1.5	...6.1.1.5**.#**	A human-readable database description: permanent, transient, index, queue, sql, nch

FileNet Database Group, Continued

Object	OID 1.3.6.1.4.1.517...	Poll Trap OID 1.3.6.1.4.1.517...	Description
fndbDBTotalSpace	...6.1.1.6	...6.1.1.6**.#**	The total magnetic disk space (in KB) allocated to the database
fndbDBUsedSpace	...6.1.1.7	...6.1.1.7**.#**	The amount of magnetic disk space (in KB) currently in use in this database

FileNet Security Group

Object	OID 1.3.6.1.4.1.517...	Poll Trap OID 1.3.6.1.4.1.517...	Description
fnsecCurrentUsers	...7.1	...7.1**.1**	The number of connections approved by COR_ listen
fnsecLicenseLimit	...7.2	...7.2**.1**	The maximum number of concurrent users this security service is configured to support (and for which the service is licensed)
fnsecSoftLicenseLimit	...7.3	...7.3**.1**	The maximum number of concurrent users this security service is configured to support (and for which the service is licensed)
fnsecLogonRejects	...7.4	...7.4**.1**	The number of attempts to log onto Security Services which have been rejected due to the maximum number of concurrent users being exceeded. This value could be configured on a per-user basis in Xapex, Security Maintenance.
fnsecSoftHits	...7.5	...7.5**.1**	The number of attempts to log onto Security Services which soft_limit SLU is exceeded. This value is determined by your SLAC key and cannot be configured.

FileNet Poll Trap Table Group

Object	OID 1.3.6.1.4.1.517...	Description
fnpttTable	...8.1	The FileNet poll trap table
fnpttEntry	...8.1.1	An entry in the FileNet poll trap table
FnpttEntry	- - - - - - - - -	The sequence of objects in the poll trap table: fnpttIndex fnpttOid fnpttThreshold fnpttInterval fnpttRepeatence fnpttExact fnpttSeverity
fnpttIndex	...8.1.1.1	An index that uniquely identifies an entry in the FileNet poll trap table
fnpttOid	...8.1.1.2	The object ID for fn_snmpd to poll periodically The default is 0.
FnpttThreshold	...8.1.1.3	The threshold for the object ID polled
fnpttInterval	...8.1.1.4	The interval in minutes between two pollings (0 = disabled)
fnpttRepeatence	...8.1.1.5	The number of times polling results hitting a threshold generates a trap
fnpttExact	...8.1.1.6	Value for threshold checking (0 = normal checking; nonzero = exact match is needed to send a trap)
fnpttSeverity	...8.1.1.7	The severity level for a trap

FileNet RSVP Group

Object	OID 1.3.6.1.4.1.517...	Poll Trap OID 1.3.6.1.4.1.517...	Description
fnRSVPTable	...9.1	- - - - - - - - -	FileNet RSVP request entry table
fnRSVPEntry	...9.1.1	- - - - - - - - -	An entry in the FileNet RSVP entry table
FnRSVPEntry	- - - - - - - - -	- - - - - - - - -	Sequence of objects in the FileNet RSVP entry table: fnRSVPNum fnRSVPType fnRSVPAge fnRSVPTime fnRSVPSurfaceID fnRSVPMsg
fnRSVPNum	...9.1.1.1	...9.1.1.1**.1**	Index number that uniquely identifies one RSVP entry
fnRSVPType	...9.1.1.2	...9.1.1.2**.1**	RSVP request type (If RSVPs are enabled, every RSVP trap will be one of these types): mountNew(1) - Mount new surface mountExist(2) - Mount existing surface ejectMedia(3) - Eject one surface ejectFullTran(4) - Eject full tranlog surface ejectErrMedia(5) - Eject surface that contains errors libraryFault(6) - Operator intervention required errMsar(7) - MSAR-related error (specific MSAR error RSVPs) errSDS(8) - SDS-related error

FileNet RSVP Group, Continued

Object	OID 1.3.6.1.4.1.517...	Poll Trap OID 1.3.6.1.4.1.517...	Description
fnRSVPAge	...9.1.1.3	...9.1.1.3**.1**	Time (in hundredths of a second) since the RSVP was posted. This is an integer that says how old the RSVP is in 100s/second) This information available for any RSVP type.
fnRSVPTime	...9.1.1.4	...9.1.1.4**.1**	The absolute time the specified RSVP request was made or posted. This is a text string that says when the RSVP was initiated. This value is a string generated either by the FileNet “DTM_TimeToString()” entry or by the standard “ctime()”library function. This information available for any RSVP type.
fnRSVPSurfaceID	...9.1.1.5	...9.1.1.5**.1**	The surface ID to which the RSVP message refers This information available for any RSVP type.
fnRSVPMsg	...9.1.1.6	...9.1.1.6**.1**	The RSVP operator request text This information available for any RSVP type.

Appendix C – SNMP services and functionality

This Appendix provides basic information about SNMP services and functionality. It covers the following information:

- Determining whether SNMP services is installed and running on your system.
- Determining whether SNMP is functioning properly on your system in a basic sense and also specifically with FileNet Image Services.

Verify basic SNMP services

There is an easy, platform-specific way to verify SNMP is running on your system. Depending upon the type of FileNet Image Services system you have, you either need to run the appropriate **ps** command (UNIX) or navigate (Windows Server).

Determine if SNMP Services is installed on a UNIX system

Enter the following command to determine if SNMP is installed/running on your UNIX system:

ps eaf|grep -i -e snmp -e trap

If your system is an AIX system, you should receive output similar to the following:

```
root   9306  6448   0 17:09:31   - 0:00  /usr/sbin/snmpd
fnsw   8722     1   0 17:11:29   - 0:00  fn_snmpd
fnsw  18192     1   0 17:11:27   - 0:00  fn_trapd
```

Note fn_snmpd and fn_trapd are FileNet processes. fn_snmpd handles FileNet queries, and fn_trapd handles FileNet traps. These processes are started and stopped with the FileNet software. snmpd is the AIX SNMP daemon that comes up with the operating system.

If your system is an HP-UX system, you should receive output similar to the following:

```
root    3211     1    0 Feb 7 ?    - 0:12  /usr/sbin/snmpdm -P 8000
fnsw    3396     1    0 Feb 7 ?    - 0:01  /fnsw/bin/fn_snmpd -f 8001
fnsw    3397     1    0 Feb 7 ?    - 0:01  /fnsw/bin/fn_trapd
root    3226    1   0 Feb 7 ?   - 0:24  /fnsw/bin/MasterSnmpd -t local -c
public -m 1 -n 0 -f 8001
```

Note MasterSnmpd is another FileNet process for HP-UX and Solaris only. It is designed to multiplex all SNMP activities on the box, including FileNet-related SNMP traffic. On these two platforms, MasterSnmp is needed to verify that FileNet can coexist with SNMP services, because SNMP is sold separately from the base operating system (as opposed to AIX and Windows Server, where SNMP services are built-in). For a complete list of MasterSnmp configurable parameters, see **"Master-Snmpd configurable parameters" on page 105**.

snmpdm is the HP-UX SNMP daemon that comes up with the operating system. As with AIX, the fn_* processes are started and stopped with the FileNet software.

If your system is a Solaris system, you should receive output similar to the following:

```
fnsw   13204     1   0 13:57:34 ?       - 0:01  /fnsw/bin/fn_snmpd -f 8001
root   13437     1   0 15:55:58 pts/0   - 0:00  /fnsw/bin/MasterSnmpd -t
local -c public -m 1 -n 0 -f 8001
```

Determine if SNMP Services is installed on a Windows Server system

The Windows SNMP Service (snmp.exe) must be installed before installing the FileNet Image Services software. If the SNMP service must be installed after installing FileNet Image Services, skip to **"Create the SNMP reference registry entry" on page 95**. To determine if SNMP is installed/running on your Windows Server system, complete the following steps:

1. Right-click on your system's Network Neighborhood icon and click on Properties.
2. Click on the Services tab and you should see **SNMP Service** and be able to view its properties.
3. From the Taskbar, click on the **Start** button, point to Settings, and click on Control Panel.
4. From the Control Panel window, locate and double-click on the Services icon.

   The Services window displays. In the window, you should see both the **SNMP Service** and the **SNMP Trap Service** with a Status of **Started** and a Startup setting of **Automatic**.

You should also see **fn_snmpd.exe** and **fn_trapd.exe** in the Windows Server Process List.

5 Click **Close** to close the Services window.

Note You should be able to query non-FileNet SNMP MIBs whether or not FileNet Image Services is running. However, you do need to have FileNet Image Services running (along with the fn_snmpd process) in order to be able to query FileNet MIBs.

Create the SNMP reference registry entry

If the SNMP service must be installed after installing FileNet Image Services, complete the following steps to create the SNMP reference registry entry:

1 Install the SNMP Service on your server.

2 From a Command Prompt window, enter the following command to open the Registry editor:

REGEDT32

Tip You can also enter this command in the task bar Run dialog box.

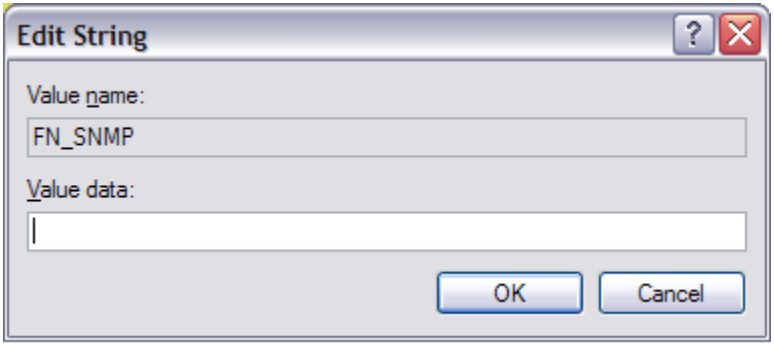
3 In the HKEY_Local_Machine on the Local Machine window, open the **System** folder and navigate to the ExtensionAgents folder using this path:

SYSTEM > CurrentControlSet > Services > SNMP > Parameters > ExtensionAgents

4 From the Edit Menu select New > String Value

5 Rename the new string entry **FN_SNMP**, and the type should be set to **REG_SZ** by default.

6 Double-click on the new entry and you will receive the following screen:



7 Enter **SOFTWARE\FileNet\IMS\CurrentVersion** in the Value Data field and click **OK**.

Check FileNet SNMP functionality

SNMP is used internally by FileNet Image Services (for example, some of the Xapex reports screens). In this section, you can check to see if this internal functionality is working by seeing if you can do FileNet SNMP queries on the same box. You can do this by using the **nmi_test** command.

1 Change directory to the **/fnsw/bin** and enter the nmi_test command:

nmi_test

2 You should receive output similar to the following:

```
NMI_get_system_info - completed successfully!
    Domain      : sas1
    Organization: FileNet
    SSN         : 1100106785
    ServerType  : Combined
    Uptime      : 62700 hundreths of a second
    LastTrapErr : <77,0,1>
    LastTrapText: You don't need a weatherman to know ...
    LastTrapTime: 62700
    LastTrapSev : Operator
    TrapFlags   : OK      : 0
                  Warning : 1
                  Operator: 1
                  Severe  : 1
    Service Table
    I Type        Prc Max Rej Desc
    - ----------- --- --- --- ------------------------------------ ...
```

Tip The information in **nmi_test** is exactly the same as the reports in Xapex.

Appendix D – SNMP processes and resources

This appendix is strictly a reference section detailing the processes and files associated with SNMP as well as providing other resources for you to look at. It is comprised of the following sections:

- SNMP Process and Files

  This section lists, by platform, all of the main SNMP-related processes and files on your system. Refer to **“SNMP processes and files” on page 99**.

- MasterSNMP Configurable Parameters

  This section lists the different parameters available with the MasterSnmpd_start script. Refer to **“SNMP processes and files” on page 99**.

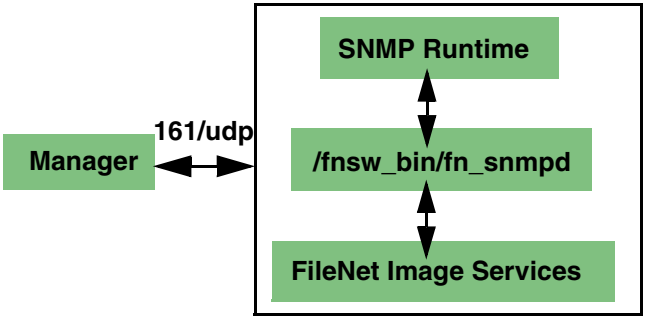
- SNMP Bibliography

  This section lists texts and URLs available to help you gain a greater understanding about SNMP. Refer to **“SNMP bibliography” on page 106**.

SNMP processes and files

The following sections illustrate each of the four supported FileNet Image Services platforms. Each section lists the processes created with SNMP and the files created by SNMP.

AIX architecture



AIX 5.1 processes

```
ps -eaf | grep -i -e snmp -e trapd =>
    root    9306  6448    0 17:09:31      - 0:00  /usr/sbin/snmpd
    fnsw    8722     1    0 17:11:29      - 0:00  fn_snmpd
    fnsw   18192     1    0 17:11:27      - 0:00  fn_trapd
```

Note No FileNet MasterSnmpd process on AIX (HP-UX and Solaris only).

AIX 5.2

With AIX 5.2 and later, SNMPv3 has been introduced as the default SNMP version. See **"Appendix E – Support for SNMPv3" on page 107** for information on configuring SNMPv3.

1. Run the **ps -e | grep snmp** command to check the SNMP version you are running.

2. If you are running SNMP version 3 (SNMPv3), you can optionally switch to version 1. For example, you might enter:

   snmpv3_ssw -1

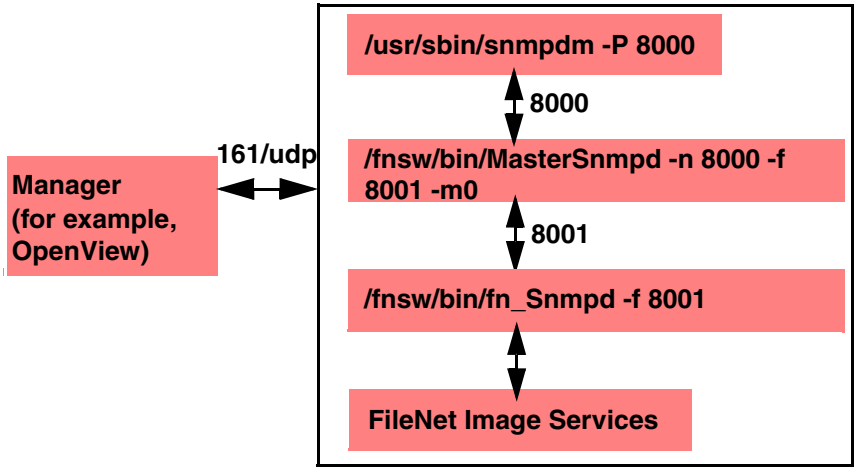
3. Also, edit the /etc/environment file and add the following environment variable:

   FDTABLENUM=1024

   When running SNMPv1 on AIX 5.2 and later, all other configuration details remain the same as they are in AIX 5.1.

   The new FDTABLENUM environment variable will go into effect the next time you reboot the server.

HP-UX architecture



Processes

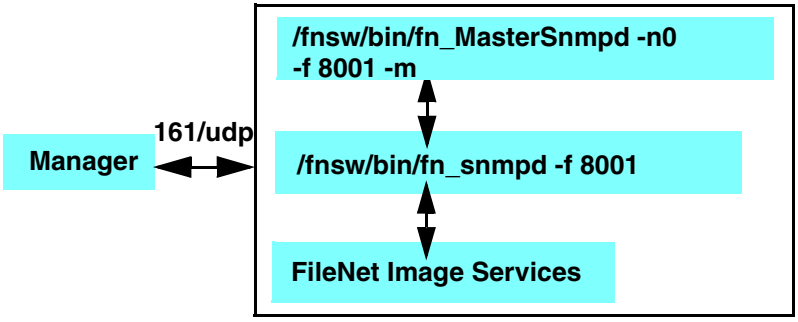
```
ps -eaf | grep -i -e snmp -e trapd =>
root    3211     1    0 Feb 7 ?              0:12  /usr/sbin/snmpdm -P 8000
fnsw    3396     1    0 Feb 7 ?              0:01  /fnsw/bin/fn_snmpd -f 8001
fnsw    3397     1    0 Feb 7 ?              0:01  /fnsw/bin/fn_trapd
root    3226     1    0 Feb 7 ?              0:24  /fnsw/bin/MasterSnmpd -t
   local -c public -m 0 -n 8000 -f 8001
```

Note traphost = local, community = public, .MIB2 = NO (using HP-UX MIBs Master), Native port = 8000 (matches snmpdm port), F/NET port = 8001

Files

/fnsw/bin/MasterSnmpd_start
/etc/rc.config.d/SnmpMaster, SnmpMib2, etc (HP-UX Master Agent config)
/etc/snmp.conf
/var/adm/snmpd.log
/etc/services => snmp 161 /udp, snmp-trap 162/udp (both HP-UX)

Solaris architecture



Processes

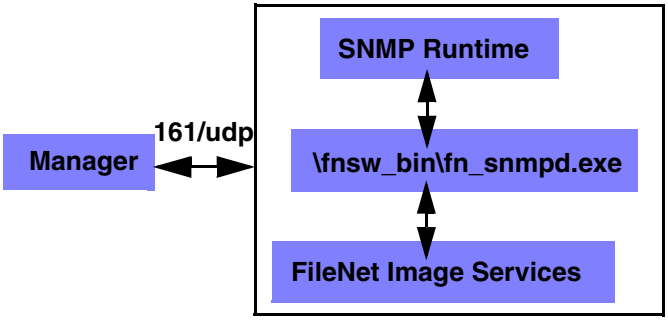
```
# ps -eaf | grep nmp -e =>
fnsw  660     1  0 10:21:19 ?          0:01  /fnsw/bin/fn_snmpd -f 8001
root  420     1  0 09:32:36 ?          0:00  /fnsw/bin/MasterSnmpd -t
hp9seal -c public -m 1 -n 8000 -f 8001
root  363     1  0 09:32:34 ?          0:00  /usr/lib/snmp/snmpdx -y -c /
etc/snmp/conf -p 8000
```

Note traphost = local, community = public, .MIB2 = YES (using F/NET as Master), Native port = 0 (F/Net is master), F/NET port = 8001

Files

/fnsw/bin/MasterSnmpd_start
/var/adm/messages*
/etc/services =>
fn_snmpd 161 /udp,
fn_trapd 35225/udp <- Default: Port 161 owned by FileNet

Windows Server architecture



Processes

```
snmp.exe (SNMP Service)
snmptrap.exe (SNMP Service)
fn_snmpd.exe
fn_trapd.exe
```

Files

Event Viewer

Note No FileNet MasterSnmpd process on Windows Server (HP-UX and Solaris only).

MasterSnmpd configurable parameters

Switch	MasterSnmpd_ Start	HP-UX	Solaris	Description
-t TRAPHOST	trap_host	“local”	“local”	Trap Destination
-c COMMUNITY	trap_community	“public” “private” “regional” “proxy” “core”	“public” “private” “regional” “proxy” “core”	SNMP Community
-m FLAG	MIB2_flag	0	1	1 = Use FN MasterSnmp 2 = Use OS MasterSnmp
-n NATIVE_PORT	Native_port	8000	0	Native port
-f FN_PORT	FileNet_port	8001	8001	FileNet port
-p TRAP_PORT	None	None	None	Trap port
-d	None	None	None	DEBUG: dump packets
-a	None	None	None	DEBUG: log addresses

Examples:

HP-UX: /fnsw/bin/MasterSnmpd -t local -c public -m 0 -n 8000 -f 8001

Solaris: /fnsw/bin/MasterSnmpd -t local -c public -m 1 -n 0 -f 8001

SNMP bibliography

The following list of texts and URLs can help you gain a better understanding of SNMP.

Texts

Miller, Mark A, P.E., Managing Internetworks with SNMP, M&T Books, 1999, ISBN 0-7645-7518-X

Covers SNMP and network management in general, includes CD

Murray, James D., Windows NT SNMP, O'Reilly, 1998, ISBN 1-56592-338-3

Covers both SNMP Architecture and Win 32 APIs, includes CD

URLs

http://www.ietf.org/rfc.html (SNMP RFCs)

http://docwiki.cisco.com/wiki/Simple_Network_Management_Protocol (Tutorial)

Appendix E – Support for SNMPv3

SNMPv3 support has been tested on AIX 5.3 and AIX 6.1 over IPv4. This appendix contains the configuration details that were used for each of the available SNMPv3 configuration options.

After making any change to the SNMPv3 configuration files, you must complete the following steps:

- Stop the FileNet Image Services software.
- Run the **stopsrc –s snmpd** command.
- Run the **startsrc –s snmpd** command.
- Start FileNet Image Services.

Ensure that SNMPv3 is enabled

Enter the following command to determine the version of SNMP that is currently running:

ps –e | grep snmp

Command Output	SNMP Version
snmpd64v1	SNMP v1
snmpdv3ne	SNMPv3 Non-Encryptiont
snmpdv3el	SNMPv3 Encryption (AIX Encryption Pack must be installed)

To change SNMP version, use the appropriate snmpv3 command:

Command	Purpose
snmpv3_ssw -e	Switch to encrypted version of snmpdv3 agent
snmpv3_ssw -n	Switch to non-encxrypted version of snmpdv3 agent
snmpv3_ssw -l	Switch to snmpdv1 agent

Important

When FileNet Image Services is installed, the following files are automatically updated:

/etc/snmpd.peers: The following line is added at the end of the file:

"fnpd" 1.3.6.1.4.1.517 "fnpd_password"

/etc/snmpd.conf: The following line is added at the end of the file:

smux 1.3.6.1.4.1.517 fnpd_password # fnpd

Since SNMP v3 does not use the /etc/snmpd.conf file, it is important to add the "fnpd" data where indicated in the following section. Failure to do so causes SNMP errors when FileNet Image Services is started.

SNMP v1 Communities configuration within SNMPv3

It is possible to configure the legacy SNMP v1 Communities from within the SNMPv3 environment. The following example illustrates how this is configure in the /etc/snmpdv3 file:

- For “read/write” add “defaultView” to the VACM_ACCESS line
- For a Poll Trap target, put the target system’s IPv4 IP address in the TARGET_ADDRESS line
- Add the SMUX line for the fnpd_password at the bottom of the file. This line is automatically installed in the \etc\snmpd.conf file when FileNet Image Services is installed, but it is not added to the snmpdv3.conf file.

```
VACM_GROUP group1 SNMPv1  public -

VACM_VIEW defaultView        internet                          - included
-

# exclude snmpv3 related MIBs from the default view
VACM_VIEW defaultView        snmpModules                       - excluded
-
VACM_VIEW defaultView        1.3.6.1.6.3.1.1.4                 - included
-
VACM_VIEW defaultView        1.3.6.1.6.3.1.1.5                 - included
-

# exclude aixmibd managed MIBs from the default view
VACM_VIEW defaultView        1.3.6.1.4.1.2.6.191               - excluded
-

VACM_ACCESS  group1 - - noAuthNoPriv SNMPv1  defaultView
defaultView defaultView -

(Continued on next page)
```

```
(Continued from previous page)

NOTIFY notify1 traptag trap -

TARGET_ADDRESS Target1 UDP 9.39.41.103  traptag trapparms1 - - -

TARGET_PARAMETERS trapparms1 SNMPv1 SNMPv1 public  noAuthNoPriv -

COMMUNITY public   public   noAuthNoPriv 0.0.0.0   0.0.0.0 -
logging         file=/usr/tmp/snmpdv3.log       enabled

DEFAULT_SECURITY no-access - -

logging         file=/usr/tmp/snmpdv3.log       enabled
logging         size=100000                     level=0

smux            1.3.6.1.4.1.2.3.1.2.1.2         gated_password #
gated

smux 1.3.6.1.4.1.2.3.1.2.3.1.1 muxatmd_password #muxatmd
smux 1.3.6.1.4.1.517           fnpd_password    # fnpd
```

These setting provide for fully functional SNMPv1 capabilities, including the ability to MIB browse and set FileNet Image Services Poll Traps using the “public” community.

SNMPv1 User Authentication configuration within SNMPv3

It is possible to configure SNMP v1 using SNMPv3 User Authentication. The following configuration entries in the /etc/snmpdv3.conf file provide an example:

```
VACM_GROUP group1 SNMPv1  private  -

VACM_VIEW group1view         internet                    - included -

VACM_ACCESS  group1 - - noAuthNoPriv SNMPv1  group1view group1view
group1view -

NOTIFY notify1 traptag trap -

TARGET_ADDRESS Target1 UDP 9.39.41.103       traptag trapparms1 - - -

TARGET_PARAMETERS trapparms1 SNMPv1  SNMPv1  private noAuthNoPriv -

COMMUNITY private   private     noAuthNoPriv 0.0.0.0     0.0.0.0 -

DEFAULT_SECURITY no-access - -

logging         file=/usr/tmp/snmpdv3.log       enabled
logging         size=100000                     level=0

smux            1.3.6.1.4.1.2.3.1.2.1.2         gated_password # gated

smux 1.3.6.1.4.1.2.3.1.2.3.1.1 muxatmd_password #muxatmd
smux 1.3.6.1.4.1.517           fnpd_password    # fnpd
```

These settings provide for a community called “private” and a group called “group1” to have privileges to MIB browse and set FileNet Image Services Poll Traps.

SNMPv3 User Authentication configuration non-encrypted

It is possible to configure SNMPv3 User Authentication without encryption. The following configuration entries in the /etc/snmpdv3.conf file provide an example:

```
USM_USER u1 - HMAC-MD5 1a4b5ea9746e247dc2ac0ec8ccf43b7d - - L -

VACM_GROUP group1 USM  u1  -

VACM_VIEW group1View        internet             - included -

# Include FileNet Image Services MIB
VACM_VIEW group1View            1.3.6.1.4.1.517    - included -

VACM_ACCESS  group1 - - AuthNoPriv USM  group1View group1View
group1View -

NOTIFY notify1 traptag trap -

TARGET_ADDRESS Target1 UDP 9.39.41.103       traptag trapparms1 - - -

TARGET_PARAMETERS trapparms1 SNMPv3  USM  u1  AuthNoPriv -

DEFAULT_SECURITY no-access - -

logging         file=/usr/tmp/snmpdv3.log       enabled
logging         size=100000                     level=0

smux            1.3.6.1.4.1.2.3.1.2.1.2         gated_password  # gated

smux 1.3.6.1.4.1.2.3.1.2.3.1.1 muxatmd_password #muxatmd
smux 1.3.6.1.4.1.517           fnpd_password    # fnpd
```

You must also configure the /etc/clsnmp.conf file:

```
user1 9.39.47.174 snmpv3 u1 - - AuthNoPriv HMAC-MD5
8b70fe477f4914667eeb702ebe05e535
 - -
```

Use the “pwtokey” command to generate the Authentication keys that are used in the snmpdv3.conf and clsnmp.conf files.

This example provides for a user called “u1” and a group called “group1” which have privileges to MIB browse and set FileNet Image Services Poll Traps.

SNMPv3 User Authentication configuration with encryption

It is possible to configure SNMPv3 User Authentication with encryption. The following configuration entries in the /etc/snmpdv3.conf file provide an example:

```
USM_USER u1 - HMAC-MD5 739ebd6792075348ab189d23a3a7b1e4 DES
739ebd6792075348ab189d23a3a7b1e4 L -

VACM_GROUP group1 USM  u1 -
VACM_GROUP group2 SNMPv1  regional -

VACM_VIEW group1View        internet            - included -

# Include FileNet Image Services MIB
VACM_VIEW group1View            1.3.6.1.4.1.517    - included -

VACM_VIEW group2view         internet                   - included -

# exclude snmpv3 related MIBs from the default view
VACM_VIEW defaultView        snmpModules                - excluded -
VACM_VIEW defaultView        1.3.6.1.6.3.1.1.4          - included -
VACM_VIEW defaultView        1.3.6.1.6.3.1.1.5          - included -

# exclude aixmibd managed MIBs from the default view
VACM_VIEW defaultView        1.3.6.1.4.1.2.6.191        - excluded -

VACM_ACCESS  group1 - - AuthPriv USM group1View group1View group1View -
VACM_ACCESS  group2 - - noAuthNoPriv SNMPv1  group2view - group2view -

NOTIFY notify1 traptag trap -

TARGET_ADDRESS Target1 UDP 9.39.41.103       traptag trapparms1 - - -
TARGET_ADDRESS Target2 UDP 9.39.41.107       traptag trapparms2 - - -

(Continued on next page)
```

```
(Continued from previous page)

TARGET_PARAMETERS trapparms1 SNMPv3  USM  u1  AuthPriv -
TARGET_PARAMETERS trapparms2 SNMPv1  SNMPv1  regional  noAuthNoPriv -

COMMUNITY regional  regional   noAuthNoPriv 0.0.0.0       0.0.0.0   -

DEFAULT_SECURITY no-access - -

logging         file=/usr/tmp/snmpdv3.log       enabled
logging         size=100000                     level=0

smux            1.3.6.1.4.1.2.3.1.2.1.2         gated_password  # gated

smux 1.3.6.1.4.1.2.3.1.2.3.1.1 muxatmd_password #muxatmd
smux 1.3.6.1.4.1.517           fnpd_password    # fnpd
```

You must also configure the /etc/clsnmp.conf file:

```
user1 9.39.46.71 snmpv3 u1 - - AuthPriv HMAC-MD5
8b70fe477f4914667eeb702ebe05e535 DES 8b70fe477f4914667eeb702ebe05e535
```

After generating the Authentication Keys and Privacy Keys with the “pwtokey” command, you might need to do the following steps:

- Stop the SNMP daemon:

  stopsrc –s snmpd

- Rename the /etc/snmpd.boots file:

  mv /etc/snmpd.boots /etc/snmpd.boots.backup

- Start theSNMP daemon:

  startsrc –s snmpd

In the previous example of the /etc/snmpdv3.conf file, the result is both SNMP v1 and SNMPv3 functionality. This provides for an SNMPv3 user called “u1” and a group called “group1” with privileges to MIB browse and “set” Poll Traps. The Poll Traps will be encrypted (unreadable text) and will be sent to IPv4 address 9.39.41.103.

This configuration also provides for an SNMP v1 community called “regional” and a group called “group2” with privileges to MIB browse and “get” Poll Traps (no “set” rights). Poll Traps will be encrypted and will be sent to IPv4 address 9.39.41.107.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Corporation
J74/G4
555 Bailey Avenue
San Jose, CA 95141
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS FileNet Image Services” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims

related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "**Copyright and trademark information**" at www.ibm.com/legal/copytrade.shtml.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

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

Other company, product, and service names might be trademarks of IBM or other companies.

U.S. Patents Disclosure

This product incorporates technology covered by one or more of the following patents: U.S. Patent Numbers: 6,094,505; 5,768,416; 5,625,465; 5,369,508; 5,258,855.

Index

Product Number: 5724-R95

Printed in USA

SC19-3319-00