netmon

6.1

User Guide

Contents

Introduction

Terminology

Trackers

Netmon uses the concept of a *tracker* to indicate some specific object, service, application or performance metric that it is observing. There are many different types of trackers in Netmon, and each has a specific purpose, including:

- Tracking the response to ping requests;
- Tracking the response to network service handshakes;
- Tracking the resulting content of an HTTP request;
- Following the values of SNMP managed objects;
- And more…

Philosophy

Netmon's primary goal is to provide you with complete visibility into, and awareness of, your server, network and datacenter infrastructure. It does this by collecting and exposing a variety of key performance metrics, and brings them all together into an integrated set of tools and views.

Home Dashboard

The first screen you will see after logging into the system is the Netmon Home Dashboard. This screen is designed to provide you with a high-level, up-to-the-moment overview of your network. To see this screen, click the **Home** button in the top toolbar.

The home dashboard consists of two tab views: Dashboard and Recent Activity. You can toggle between each view by clicking on the associated tab at the top of the home dashboard screen.

Dashboard Tab

The dashboard tab has a number of sections:

Recent Alerts

This section is located on the left side of the screen, below the Dashboard tab. It shows, in table format, a list of recently-issued alerts. The following information is provided for each alert:

Date and Time: A timestamp when the alert was issued.

Alert Type: The type of alert that was triggered.

Alert Details: When available, additional information about the conditions surrounding the alert will be shown here.

Performance Trackers

This section is located on the left side of the screen, below the Recent Alerts section, and shows line charts for certain SNMP object trackers.

The charts displayed here have the “Display on Home Dashboard” flag set in their Device Settings. In a brand new installation of Netmon, nothing is displayed in this section. You have to choose which trackers to display via Devices > *Select a Device* > Device Settings.

You can interact with these charts with your mouse: hovering over data points will expose additional detail in a tooltip.

Network Traffic Graphs

This section is located on the top right side of the screen. It shows a bar chart for each traffic analyzer or collector that is configured in the system. The chart represents the last 2 hours of network activity for each analyzer or collector, broken down into 2-minute slices. Each slice indicates the total amount of bandwidth utilized during that time interval, and is broken down into different colors, each of which represents a specific port or protocol. Netmon will attempt to identify this traffic using its internal port label database.

You can interact with these charts with your mouse: hovering over data points will expose additional detail in a tooltip.

Bandwidth Graphs

This section is located on the right side of the screen, below the Network Traffic Graphs section. It is similar to the Performance Trackers section in that it shows SNMP object trackers. However, this section is specifically provisioned to show bandwidth utilization charts for network interfaces.

The charts displayed here have the “Display on Home Dashboard” flag set in their Network Interface settings. In a brand new installation of Netmon, nothing is displayed in this section. You have to choose which trackers to display via Devices > *Select a Device* > Device Settings

You can interact with these charts with your mouse: hovering over data points will expose additional detail in a tooltip.

Recent Activity Tab

The Recent Activity tab shows top statistics in a table format:

Top Activity Snapshot

This panel gives you a high-level overview of the 10 most active client-server conversations over the last 5 minutes, and also shows the TDP/UDP port of each conversation. If Netmon recognizes the port being used, you’ll see a friendly name instead of the actual TCP/UDP port.

Top Web Destinations

This panel shows the top web destinations (based on HTTP requests), averaged over the last 5 minutes. A web destination is simply the recipient (i.e. the server) of HTTP requests. This could be any or all of the following:

- Public websites like www.google.com or www.amazon.com
- Local intranets and web based applications
- Non-Web HTTP traffic (i.e. SOAP or XML-RPC calls)

Top Web Users

This panel displays the top local hosts which are requesting HTTP web traffic. Traffic rates (averaged over the last 5 minutes) are also provided for reference.

Recently Discovered Hosts

The Netmon network auto discovery service detects new MAC/IP pairs on your network, and displays recent discoveries in this table.

Netmon uses the Address Resolution Protocol (ARP) to probe for new hosts on your local segment(s). It issues periodic ARP broadcast requests, and checks the responses it receives against its database of known MAC addresses.

Monitoring Network Activity

Using the Visual Network Explorer

The Visual Network Explorer (VNE) component gives you a network-oriented view of your environment. It provides a near real-time graphical view of your current network activity on local or remote segment(s). You can customize this view in many different ways to find information of interest.

In order to use the Visual Network Explorer, you must have one or more of the following:

- A network device which supports NetFlow or sFlow protocols, and is configured to send these packets to the Netmon server appliance;
- A network switch which is capable of sending a copy of all network traffic to a specific physical port, a feature known variably as port mirroring, port monitoring or port spanning. The Netmon appliance must be connected to this port through one of its physical interfaces.

If you do not have the above configurations in place, you will be unable to view network traffic in the VNE. Refer to the Setup and Installation Guide for guidance on this topic.

Customizing the VNE View

Zoom and Pan Support

You can zoom the VNE view in or out by using the scroll wheel of your mouse while hovered over the view, or by clicking either of the zoom buttons located in the top left part of the VNE, just below the Network Explorer toolbar.

You can also pan the view up or down, left or right by doing a click-and-drag over any empty area in the view.

Moving or Repositioning Hosts

You can move or reposition a host in the VNE view by doing a click-and-drag on the host's name or icon. The position of hosts is partially controlled by the VNE itself, and other hosts will be automatically repositioned during any move. Hosts are also affected by a gravitational effect: your ability to move a particular host will depend on how many other hosts are connected to it. Hosts with a large number of connections to other hosts will be easier to move than those with only 1 or 2 connections.

Selecting a Traffic Source

The VNE displays network traffic from one NetFlow source, sFlow Source, or physical source at a time. To switch between traffic sources, locate the **Traffic Sources** drop-down menu in the Network Explorer toolbar, and select the source you wish to view.

By default, Netmon will display at least one source in this list: the Local IP Packet Analyzer. If you have additional physical interfaces configured for traffic analysis, or if Netmon is collecting sFlow or NetFlow data from remote devices, you will see them in this list.

Absolute vs. Relative Traffic View

Depending on your requirements, you can view network connections in one of two different ways, by adjusting the **Traffic View** drop-down menu in the Network Explorer toolbar:

Absolute View displays all network traffic on an absolute scale. Each packet stream is displayed according to the maximum speed your infrastructure can support — usually 100 Mbps or 1 Gbps. For a reference on what each style of line represents, see the Activity Legend. Using Absolute View is usually the best way to monitor traffic if you're trying to understand your overall network load.

Relative View displays traffic according to the most active packet stream on the network. In this scenario, the most active conversation on your network is displayed with a thick, bright red line (see the Activity Legend) and all of the other conversations are scaled in a linear fashion according to this host.

Relative View is the best option to use when you want to compare your network traffic to other network traffic. It allows you to see how traffic from individual hosts compares against the traffic between other active hosts.

Viewing Fewer or More Connections

By changing the selection in the **Max Conversations** drop-down menu, you can customize your view to show the anywhere from 16 to 128 network conversations. Viewing fewer conversations at once can simplify the view, while viewing many conversations at once can give you a broader perspective.

Viewing Hosts by Name or IP Address

You can choose to view individual hosts by their IP address or by their host name by adjusting the selection in the **View Hosts By** drop-down menu in the Network Explorer toolbar.

If you choose to view by Host Name, Netmon displays the host using its friendly name, if one is available. If a friendly name is not available, Netmon selects the first entry in its name database (giving preference to NetBIOS names, followed by DNS names)

Identifying Specific Network Traffic through Traffic Filters

Traffic filters allow you to refine the VNE view to look for specific types of network traffic. By adjusting the selection in the **Apply Traffic Filter** drop-down menu, the VNE will only show the network activity that's been defined in the associated filter.

Viewing Specific Hosts through Host Filters

Host filters allow you to refine the VNE view to look at a specific device, or group of devices. By adjusting the selection in the **Selected Hosts** drop-down menu, the VNE will only show the hosts that have been defined in the associated filter.

Freezing the View

Due to the dynamic nature of the VNE, it can sometimes be beneficial to freeze the view in place to permit further analysis or investigation. You can then work with the view as it was when the freeze took place, click on hosts to view their connection details, etc.

To freeze the view, click the Pause button in the Network Explorer toolbar. To un-freeze the view, click this button again.

Interacting with Individual Hosts in the VNE

Selecting a Host

Clicking on any individual host icon in the VNE will populate two panels on the right side of the VNE. You can expand or collapse each panel by clicking on the gray title bar.

Resolved Hostname(s)

In many cases, a single IP address can resolve to many different DNS names, or you may have applied a friendly label to this host. This panel shows a list of all resolved names for the selected host.

Connections

This panel shows a list of all connections for the selected host from the past 20 seconds in table format, with the following data columns:

> **Direction:** An upward-pointing arrow indicates that the selected host is sending data to the destination host. A downward-pointing arrow indicates that the selected host is receiving data from the destination host.
>
> **Source Host:** The resolved name or IP address of the host on the other side of the connection.
>
> **Port:** The TCP or UDP port number of the connection. If Netmon is able to resolve the protocol using its port label database, the name of the protocol will appear here.
>
> **Speed:** The rate of transfer of the connection, averaged over the 20-second time span when the host was selected.

Data in the Connections table can be sorted by clicking the column heading.

To refresh the Connections view with up-to-date data, simply re-click on the host in the VNE view.

Monitoring Devices

Simple Network Management Protocol (SNMP)

Effective network monitoring encompasses a broad range of responsibilities. You need to understand your network traffic from several vantage points, but it also becomes important to monitor the health, availability and load of many different kinds of mission-critical devices.

The solution is the Simple Network Management Protocol (SNMP): a widely supported monitoring and management protocol for network-aware devices. Managed devices, as SNMP-capable devices are otherwise known, can include things like switches, routers, multi-function printers, fax stations, firewalls, thin clients, wireless transmitters, and much more. Thousands of different devices support the SNMP protocol.

SNMP provides the ability to query and update a managed device remotely. Using this protocol, you can retrieve a potentially rich set of information about a particular device: data such as inbound and outbound traffic levels, current connections, CPU load, memory status, usage history, error messages, device status, and countless other details. This is really nice stuff to know. Furthermore, SNMP ’write’ operations can even allow devices to be configured and managed remotely.

Devices can also be configured to automatically ’push’ SNMP data to a remote monitoring or management system. For example, you might configure a laser printer to send information about current toner level. These UDP datagrams are known as SNMP traps, and they’re generally sent to a remote monitoring system where they’re collected and handled appropriately.

The SNMP Protocol

The SNMP protocol itself is a relatively simple request-response protocol. It works at the application layer, and typically utilizes UDP ports 161 and 162.

The choice of UDP may seem a bit unusual for a request-response protocol, but SNMP was designed from the outset to move across the network as ’non-critical’ traffic. In high load situations, UDP packets that are dropped from the network are not resent by the originating host. This reduces network congestion in critical load situations. To ensure that SNMP traffic doesn’t unnecessarily burden a network, its designers skipped the higher overhead of a full-blown TCP connection in favor of a more graceful failure scenario.

Every managed device keeps a hierarchical database of values, known as a Management Information Base (MIB). These MIBs are sent as numerical indexes (known as object identifiers, or OIDs) in the SNMP packet payload, and each one represents some type of configuration detail. Each MIB has an associated meaning, such as the following:

MIB: Cisco Router OID: 1.3.6.1.4.1.9.1.1

Netmon can monitor object identifiers, plot numerical values on a graph, and issue email alerts when OID values meet a defined criteria.

Using the Devices Explorer

The Devices Explorer gives you a device-oriented perspective of your environment, and is designed to help you see a large number of devices at once, and focus on problem areas quickly.

Each device is contained in a rounded box which displays key identifiers and status information in a compact space. The following data is displayed:

- the IP address of the device
- the resolved hostname of the device, if available
- icon and text which identifies the type of device
- a status icon which indicates if Netmon currently detects a problem condition with the device
- A brief description of the problem condition detected, if any

To open the Devices Explorer, click on the Devices button in the top toolbar.

Organizing the Device Explorer View

You can re-order the boxes in the Device Explorer to make it easier to locate specific devices. By making a selection in the **Order By Status** button, which is located in the Device Explorer toolbar. The available options are:

IP Address: Order the view by device IP address

Status: Order the view so that devices with problem conditions float to the top

Name: Order the view by the resolved hostname of the device

Group: Order the view by the Device Group to which this device belongs

Dashboard: Order the view by the type of device (i.e. server, switch, router, UPS)

Searching for Devices by Name, Label or IP Address

You can use the search bar in the Device Explorer toolbar to locate devices by DNS name, label or IP address. Enter a search string in this box and press Enter to show only devices which match your search criteria.

To clear your search, empty the search box and press Enter.

Add a New Device

In most cases, devices will be added to your Netmon database automatically via its automatic discovery services. However, there may be cases where you wish to add a new device to Netmon that is outside of your monitored ranges, or has not been discovered by automatic discovery services.

To add a new device to the Device Explorer, press the **New Device** button in the Device Explorer toolbar. This will open a window where you can specify the details of the device you'd like to add.

IP Address: The IP address of the host or device you wish to add.

Device Group: If you'd like to assign this device to an existing Device Group, select it here.

Device Label: Provide a friendly name for this host or device. This label will take precedence over any resolved names in the Netmon user interface.

Device Type: The Device Type helps Netmon to classify a particular host, and is used to determine which device dashboard to display. You can make a selection from the available list, or choose **Default** if your device doesn't match any of the types in this list.

Enable NetFlow: Checking this box tells Netmon to accept NetFlow packet streams from this device. If you do not specifically enable it here, Netmon will not accept NetFlow packet streams from this device.

Enable sFlow: Checking this box tells Netmon to accept Flow packet streams from this device. If you do not specifically enable it here, Netmon will not accept sFlow packet streams from this device.

Enable SNMP: Checking this box tells Netmon that this device supports SNMP and can be polled via SNMP GET or WALK requests. Selecting this option exposes 3 more fields for the device polling interval, the SNMP community string to supply when authenticating to the device, and the SNMP port number to use when making SNMP requests.

Enable Syslog: Checking this box tells Netmon to accept syslog messages from this device. If you do not specifically enable it here, Netmon will not accept syslog messages from the device. Selecting this option exposes 2 additional fields, where you can specify the message facilities to accept (with a default of all messages) and the minimum severity level to accept (with a default of ERROR level severity).

Once you've filled out each of these fields, press the **Save Changes** button to add your device to Netmon's database.

Removing a Device

To remove a device from Netmon's database, locate it in the Device Explorer, and click on it to view the device dashboard. Look for the **Delete Device** button on the right side of the main toolbar. Click on this button to being the removal process, which you'll be asked to confirm via a pop-up dialog window.

Note: Removing a device in this fashion will free up a device license, which can then be re-used on another device.

Viewing Device Details

To view a detail window for any device, simply click on it in the Device Explorer. This will open a new screen which shows everything Netmon knows about the host.

At the top of this screen is the Device toolbar. From this toolbar, you can add a new device, run commands against the currently highlighted device, and make adjustments to device settings.

Beneath this toolbar is a multi-tabbed interface. You can click on the individual tabs, identified as follows:

Dashboard: A high level performance-oriented dashboard. Depending on the type of device, the contents of this tab can vary considerably.

Network: View the status of network service, network interfaces and other network performance metrics in this tab.

Event Logs: See syslog or event log data from this device that has been forwarded to Netmon.

Notes: View and manage notes that have been recorded for this device. Notes are useful for recording maintenance activities or storing configuration details.

Command Output: This tab is empty by default, but will be populated with information when certain commands are executed, such as SNMP walk, Port Scan or Traceroute.

Adding a New Tracker

There are multiple ways to add a new tracker. You can:

- Use the **Add New Tracker** button on the device toolbar.
- Click on any performance metric in the device's Dashboard Network, and Event Logs tabs.
- Perform an SNMP walk on the device via the **SNMP Walk** button on the device toolbar, and click on any of the resulting SNMP objects to create a new tracker for that object.

Performing a Port Scan

Netmon can determine which TCP ports are open and responding to connections with its built-in port scanner.

To run a port scan on any device, first locate it in the Device Explorer and click on it. Then click the **Port Scan** button in the device toolbar.

The results of the port scan will appear in the **Command Output** tab of the device profile.

Performing a Traceroute

Netmon can determine the network path between itself and a host via its built-in traceroute utility. To run a traceroute on any device, first locate it in the Device Explorer and click on it. Then click the **Traceroute** button in the device toolbar.

The results of the traceroute will appear in the **Command Output** tab of the device profile.

Performing an SNMP Walk

Netmon uses the SNMP Walk facility to explore the exposed Management Information Base (MIB) tree for a particular device.

Caution: SNMP Walks can be very resource-intensive operations, and have been known to crash some older devices. You should always exercise caution when walking mission-critical devices, especially ones which are already under a heavy workload.

What is a MIB?

A Management Information Base (MIB) generally defines the set of parameters that an SNMP management station can query (or set) in in an SNMP-enabled device. It is essentially a collection (or more than one) of information that can be gathered from an SNMP-enabled device.

Common MIB Data Types

Netmon automatically recognizes the following common MIB data types:

32 Bit: Any 32-bit value. This value is generally expressed as an integer.

Gauge: Any 32-bit value. This value is generally expressed as an integer.

Hex: A 32-bit hexadecimal number.

Integer: Any valid integer.

Host Address: An IP address.

OID: A numeric OID reference string.

String: A string value.

Timeticks: usually expressed in milliseconds or microseconds.

Using the OID Tracker Service

Netmon's SNMP OID tracker service allows you to watch a specific OID management point for changes. This is an extremely flexible service that can be used to monitor hundreds or thousands of different performance metrics from SNMP-capable devices.

When tracking OIDs, Netmon renders Integer, Counter and Gauge data types in a similar fashion. Text data types are displayed as a small datagrid. When you find an OID of interest in the MIB Browser, you can click on it to have Netmon watch that object at any desired interval. You will then be prompted to enter the following information:

Label: Apply a descriptive label to this OID Tracker. Netmon will suggest a label based on the OID you have selected, but it can often be beneficial to add additional information here. This label is the main descriptive field used for Netmon's email and pager alerts.

Sampling Interval: The number of seconds between successive polls. Be sure to choose an appropriate value here.

Enable Logging: When this box is checked, it tells Netmon to record all historical poll results for the specified OID Tracker. If the box is left unchecked, Netmon simply records the latest result to the database.

Display on Home Dashboard: If this is an important OID Tracker, you can display it on the Netmon Home Dashboard. Depending on the logging selection you have made (see above) this tracker will appear as a line chart or a single-value panel.

Network Tab

The contents of this tab reflect what Netmon knows about the devices network interfaces and network services.

Network Services

Network services (i.e. open TCP ports, responsiveness to PING requests) which have been detected or manually configured on this host will appear in this section, along with a summary of the status of each, as follows:

Service Name: The friendly label applied to the service.

Port: For TCP services, the port number will be listed here. ICMP will simply specify ‘ICMP’.

Status: If the service is up, this label will be green. If the service is unresponsive, this label will be red. If Netmon is able to detect the latency (in milliseconds) of requests to this service, they’ll be displayed here.

Time Polled: The date and time of the most recent status check on this service.

Actions: You can update Netmon’s monitoring parameters of this service by clicking the **Edit** button, alerts for this service via the **Alerts** button, and remove this service from Netmon’s monitoring through the **Delete** button.

Bandwidth Trackers

If you’ve configured Netmon to track the bandwidth utilization of any interface(s), you’ll see a line chart for each interface in this section.

To configure Netmon to track the bandwidth utilization of a particular interface and see the chart here, see Network Interfaces below.

Network Interfaces

Each row in this table represents a physical or virtual network interface on the host. Information about each interface is displayed in columns, as follows:

Interface Icon: An icon indicating the numeric identifier of the interface, along with red/green indicators which display the status of the interface. Green indicates an active interface, while red indicates a disconnected or misconfigured interface.

Interface Name: A friendly name for the network interface (example: Default Gateway). Clicking on this label opens a window where you can update the friendly name.

In: The latest inbound traffic throughput metric for the interface.

Out: The latest outbound traffic throughput metric for the interface.

Speed: The configured speed of the interface (often 100Mbps or 1Gbps).

Connected IP / Mac: In the case of switches or routers, Netmon will attempt to identify the device which is connected to this interface. If it's able to resolve the devices identity, its hostname, friendly name or IP address will be displayed here. If Netmon cannot resolve the host, the MAC address of the interface itself will appear here.

Errors: If any errors have been detected on the interface, they are displayed here.

Actions: You can set up bandwidth alerts for this interface by clicking the **Alerts** button here.

Displaying Bandwidth Graphs for Network Interfaces

To display a line graph in the Bandwidth Trackers section, click on the interface icon, or the interface friendly label. This opens a window where you can choose some of the monitoring parameters for this interface. Ensure the **Enable Logging** checkbox is checked if you'd like to see a bandwidth graph for this interface.

Displaying Bandwidth Graphs on the Home Dashboard

To display bandwidth utilization for a network interface on Netmon's home dashboard, click on the interface icon, or the interface friendly label. Ensure the **Display on home dashboard** checkbox is checked.

Event Logs Tab

Netmon's built-in SYSLOG server allows you to manage SYSLOG and event log data from a variety of hosts in a single, integrated console.

Collecting Syslog Data

In order to manage log data in Netmon, you must first configure your SYSLOG-capable clients to send log messages to Netmon's IP address. This process will vary depending on the type of device or server you are sending from.

Important: Netmon expects to receive log data over UDP port 514. Most SYSLOG message systems are configured by default to send messages over this port. However, if you're not seeing expected SYSLOG data in Netmon, you may want to ensure that your client software is configured to use this protocol/port combination.

Once you have configured your client device(s), Netmon will automatically start collecting event log data that it receives from that device, and log data will be visible in the **Event Logs** tab of the device dashboard.

Windows Event Logs

Netmon can monitor Event Logs on Windows systems, and collect these logs in the same way that SYSLOG messages are handled. The same alerting and reporting facilities are also available. A software agent is required to facilitate this task.

Considerations for Event Log Monitoring

SYSLOG is a 'push' oriented format, so most systems that support it are capable of sending log data to a monitoring system with a few small configuration changes.

Windows Event Logs, on the other hand, were not designed to be forwarded to other systems, but are instead are stored only locally in the file system. An agent is therefore required to retrieve these logs and perform the task of sending them to a remote system.

Using the SNARE Windows Agent

Netmon recommends (and distributes with all Netmon products on its website – Netmon.ca) the SNARE for Windows Agent, which gathers Event Log data and sends it in a SYSLOG-compatible format to your Netmon system.

The SNARE Windows Agent is highly respected open-source package, which has no licensing costs (so you can deploy it on as many systems as you desire) and is also supported by Netmon technical staff. You can download a copy on our website at http://netmon.ca/support.

Install and configure the SNARE agent to forward event logs to Netmon over UDP port 514. Once you have configured the SNARE agent, Netmon will automatically start collecting event log data that it receives from that device, and log data will be visible in the **Event Logs** tab of the device dashboard.

Event Log Alerts

Netmon can send email alerts when log messages that fit a pre-determined criteria arrive. To manage these alerts, click the **Manage Alerts** button in the Event Logs tab. A dialog window will appear.

If there are any previously-configured event log alerts for this device, they'll appear at the top of this window. Existing alerts can be reconfigured by clicking on them, or removed by clicking the **Delete** button under the Actions column next to them.

To configure a new event log alert, or if you're modifying an existing one, enter the following information in the form:

> **Label:** Provide a friendly label for this alert. This label is displayed first in the management window.
>
> **Recipient:** Select a Netmon user account to be the recipient of alert email messages.
>
> **Notification Method:** Choose from the available options of email or pager.
>
> **Severity:** Enter the minimum severity level to accept. This can be useful for filtering unwanted matches from low-severity log entries.
>
> **Pattern:** Enter a string of text here, or a regular expression pattern, and Netmon will use this pattern to filter incoming log data. Log entries which match the specified pattern will trigger an alert; those that don't will not.

Disk Drives

Netmon provides system administrators with the ability to monitor the amount of free space on network-connected disks and partitions. Netmon can keep track of disks on Windows systems, as well as Linux or Unix-like hosts.

It can alert you when occupied space exceeds your defined threshold, and can also help you monitor volume growth over time, which helps in capacity planning. Custom alert thresholds and notification parameters can be set for each share or partition, along with custom monitoring intervals and timeout periods.

How does Netmon monitor disks and partitions?

On Windows systems, Netmon uses the Server Message Block (SMB) protocol to connect to your shared folders. The SMB protocol returns information to Netmon about the amount of free space on the disk.

On Linux and Unix type systems, Netmon uses the df utility to work with inetd or xinetd super servers. Netmon connects to the specified port number, parses the df output, and extracts the necessary disk information.

Monitoring Windows Volumes

Netmon can monitor public or administrative shares on Windows servers and workstations.

Security Considerations for Monitoring Windows Shares

Monitoring a shared Windows folder requires that Netmon log in to the remote system with a valid username and password. Since the transmission of a non-encrypted user-name and password across the network is a security risk, use the following technique to ensure that Netmon can monitor remote Windows shares safely:

1. Create a new, empty share on the drive or partition you wish to monitor, and set the access privileges for this share to read-only. Do not place any data in this folder.
2. Create a separate user account on the target machine with the minimum access privileges required to access the monitoring share.

Monitoring UNIX Drives

On Unix type systems, Netmon uses the df utility to work with inetd or xinetd super servers. Netmon connects to the specified port number, parses the df output, and extracts the necessary disk information.

Note: If you wish to monitor Netmon's own disk, it is recommended you follow this method instead of the one described below.

On Solaris 10, inetd has become part of the "smf " service management system. See below for details on this.

Adding a New Unix Partition (inetd Method)

Use this method if your system uses inetd. Monitoring a Unix partition requires a minor change to two configuration files on the remote system. These files are called /etc/services and /etc/inetd.conf.

1. Insert the following line into /etc/services:

```
df 5001/tcp #DF
```

(We have specified port 5001 here, but you can actually choose any port number you wish. However, you'll have to remember to specify the same port number when adding this information to Netmon.)

2. Insert the following line into /etc/inetd.conf:

```
df stream tcp nowait root /usr/bin/df df -k
```

On some systems, the “df ” utility will not be located at /usr/bin/df. Search for the location of this utility with “which”:

```
which df
```

If the output of this command does not match “/usr/bin/df ” then replace this bit of text in step 2 with the output of this command. For example, if the output of “which” is:

```
/bin/df
```

You would modify the configuration line for /etc/inetd.conf to read as follows:

```
df stream tcp nowait root /bin/df df -k
```

3. Restart inetd with the following command:

```
killall { HUP inetd
```

Alternatively, you can use the following command:

```
kill-HUP <inetd PID>
```

On a Solaris 10 system, restarting inetd will have no effect, you must instead convert the inetd.conf entries into the new format:

```
inetconv
```

This will convert your service definition to the smf format.

Adding a New UNIX Partition (xinetd Method)

Use this method if your system uses xinetd. Monitoring a Unix partition requires a minor change to two configuration files on the remote system. These files are called /etc/services and /etc/inetd.conf.

1. Insert the following line into /etc/services:

```
df 5001/tcp #DF
```

(We have specified port 5001 here, but you can actually choose any port number you wish. However, you’ll have to remember to specify the same port number when adding this information to Netmon.)

2. Create the ’df ’ script in /etc/xinetd.d with the following content:

```
service df
{
disable = no
flags = REUSE
socket_type = stream
wait = no
user = root
server = /bin/df
}
```

3. Restart xinetd with the following command:

```
killall { HUP inetd
```

Alternatively, you can use the following command:

```
kill-HUP <inetd PID>
```

Adding a Disk Tracker

Once you've configured your server, it's time to add the disk to Netmon. To do so, take the following steps:

1. Locate the device in the Device Explorer and click on it.
2. Click the **Add New Tracker** button in the Device toolbar, which opens a window.
3. Choose one of the two disk tracker types (Windows or Linux/Unix).
4. Depending on your choice of disk type, you'll see different fields, which are described below.
5. Once all information has been entered, click the **Save Changes** button.

Disk Tracker Fields

Label: (Windows, Unix/Linux) Enter a friendly label for this disk tracker.

Sampling Interval: (Windows, Unix/Linux) Specify how frequently, in seconds, Netmon should check the remote partition. The default interval is 300 seconds (5 minutes) but this can be set to any interval you choose.

Port: (Unix/Linux only) Specify the port number to which Netmon must connect. This should be the same port number as entered in Step 1 above.

Partition: (Unix/Linux only) Enter the device name of the partition (i.e. /dev/sda1 or /dev/hda1).

Timeout: (Windows, Unix/Linux) Specify how long, in minutes, Netmon should spend trying to connect to the remote host. The default timeout period is 5 minutes, but this can be set to any interval you choose.

Alarm Threshold: (Windows, Unix/Linux) When this amount of space is ex-ceeded, Netmon will trigger an alert. The default threshold is 90%, but this can be set to any amount you choose.

Share: (Windows) Enter the SMB share name here.

Username: (Windows) Enter a Windows user name here.

Password: (Windows) Enter a Windows password here.

Monitoring SNMP Objects with OID Trackers

Netmon can track the values of SNMP Object Identifiers (OIDs), plot scalar values on a graph, and send alerts if the results of an SNMP GET request meet a specific criteria.

Device dashboards contain a pre-defined selection of OIDs. You can add trackers to any of these by clicking on the OID description and/or value. This will open a pop-up window where you can add new trackers, or manage existing ones.

Notes Tab

You can add notes to any device in Netmon's database. Notes are useful for logging maintenance activities or holding other data about the host that isn't tracked elsewhere in Netmon.

To view and manage notes for a selected device, click the **Notes** tab in the Device Dashboard view.

Adding a new note can be accomplished by clicking the **New Note** button, which opens an editing window. Enter a subject for your note in the **Subject** field, and add your note details in the **Note** field. To save your new note, click the **Save Note** button.

New Host Discovery

Netmon uses the Address Resolution Protocol (ARP) to probe for new hosts on your local segment(s). It issues periodic ARP broadcast requests, and checks the responses it receives against its database of known MAC addresses. When a new MAC address is detected, Netmon can be configured to send an alert message.