

hp OpenView internet services

User's Reference Guide



Manufacturing Part Number: J5108-90000
January 28, 2002

Notice

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty. A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend. All rights are reserved. No part of this material may be copied, reproduced, or translated to another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights In Technical Data and Computer Software clause in DFARS 252.22707013 for DOD agencies, and subparagraphs (c)(1) and (c)(2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

HEWLETT-PACKARD COMPANY

United States of America

Copyright Notices. © Copyright 2002 Hewlett-Packard Company, all rights reserved. Reproduction, adaptation, or translation of this material without prior written permission is prohibited, except as allowed under the copyright laws of the United States.

Trademark Notices. Java™ is a trademark of Sun Microsystems, Inc. Microsoft Windows®, Windows NT®, MS Windows®, and Windows 2000® MS-DOS® are U.S. registered trademarks of Microsoft Corporation. Netscape™ and Netscape Navigator™ are U.S. trademarks of Netscape Communications Corporation. Oracle®, and Oracle7™, are trademarks of Oracle Corporation. OSF/Motif® and Open Software Foundation® are trademarks of Open Software Foundation. Pentium® is a registered trademark of Intel Corporation. UNIX® is a registered trademark of The Open Group. Adobe® and Acrobat® are registered trademarks of Adobe Inc. Certicom, the Certicom logo, SSL Plus, and Security Builder are trademarks of Certicom Corp. Copyright © 1997-2000 Certicom Corp. Portions are Copyright 1997-1998, Consensus Development Corporation, a wholly owned subsidiary of Certicom Corp. All rights reserved. Contains an implementation of NR signatures, licensed under U.S. patent 5,600, 725. Protected by U.S. patents 5,787,028; 4,745,568; 5,761,305. Patents pending. All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

- Chapter 1 Introducing Internet Services 9**
 - How Internet Services Works 12
 - The Services Hierarchy 14
 - Implementation Sequence 16
 - Integration with other OpenView Products 16

- Chapter 2 Getting Started with Internet Services 19**
 - Installation Considerations 20
 - Installation Prerequisites 20
 - Hardware Requirements 20
 - Windows Management Server 20
 - Windows NT/2000 Probe System 20
 - UNIX Probe System 21
 - Software Requirements 21
 - Windows NT/2000 Management Server 21
 - Windows NT/2000 Probe System 22
 - UNIX Probe System 23
 - Browser Requirements for Viewing the Dashboard 24
 - Platform Support 25
 - Install Internet Services 26
 - Quick Start for Using Internet Services 27
 - Probe Configuration 27
 - Check the Status of Data Collection for Configured Services 34
 - View the Data using the Dashboard Webpage display 35

Snapshot Tab	37
Availability, Response, SLO, SLA Tabs	38
Reports Tab	39
Drill Down and Trend Data.	39
Graphs Web Form	39
Uninstalling Internet Services.	40
Chapter 3 Configuring Internet Services	41
Configuring Services.	42
Default Configuration Settings	42
Using the Configuration Manager (and wizard).	43
Setting Objectives, Baselines and Alarms for the Service Group.	45
Setting Alarm Event and Service Level Objectives Only.	49
Setting Baseline Objectives Only	50
Setting Baseline and Alarm Objectives.	53
Alarm Events	53
Setting Up Service Level Agreements (SLAs).	56
How an SLA is Evaluated	58
Configuring the Network Connection (optional).	60
How Probes Work	62
How Service Target Availability is Determined.	62
Remote Probes.	64
Configuring and Installing Remote Probes for Windows NT/2000	64
Additional steps for remote probe deployment.	64
Automatic Download	65
To remove remote probe(s) from a Windows system	65
Configuring and Installing Remote Probes on UNIX Systems.	66
Stop Internet Services (if applicable).	66
Install Internet Services	66
Start Internet Services	68
Automatic Download	68
To remove probe(s) from UNIX Systems	69
Limiting Access to the Dashboard Data Display using Restricted Views	70

Automating Configuration of Large Numbers of Service Targets	71
How Batch Configuration Works	71
Syntax for the Configuration File (general)	73
Structure of the Configuration File	75
Tokens or Elements in the Configuration File	76
Create a Sample Batch Configuration File	87
Example Batch Configuration File	88
Chapter 4 Descriptions of Service Types/Probes	91
DHCP (Dynamic Host Configuration Protocol)	93
Dial-Up Networking Service	94
DNS (Domain Name System)	95
FTP (File Transfer Protocol)	96
HTTP (Hypertext Transfer Protocol)	98
HTTPS (Hypertext Transfer Protocol Secure)	100
HTTP_TRANS (Web Transaction probe)	101
ICMP (Internet Control Message Protocol—Ping)	105
IMAP4 (Internet Message Access Protocol)	105
LDAP (Lightweight Directory Access Protocol)	107
NNTP (Network News Transfer Protocol)	107
NTP (Network Time Protocol)	109
POP3 (Post Office Protocol 3)	109
RADIUS (Remote Authentication Dial In User Service)	112
SMTP (Simple Mail Transfer Protocol)	114
Streaming Media	115
TCP (Transmission Control Protocol)	117
WAP (Wireless Application Protocol)	117
X_SLAM (CiscoWorks Integration)	118
Creating your Own Custom Probes	119
List of Metrics by Probe Type	121
Chapter 5 Integrating with Other OpenView Products	131
Integrating with OpenView Operations for UNIX	132

Requirements	132
Configuration Options	133
Integrating with Network Node Manager (NNM)	140
Requirements/Recommendations for NNM Integration.	140
How to Integrate with NNM	141
Features in NNM after Integration with Internet Services.	142
Internet Services Alarms.	143
The Internet Services Menu	144
Internet Services Symbols in NNM	145
About Configuration Events	145
About Alarm Events.	147
Simple Troubleshooting for NNM Integration	148
Integrating with OpenView Operations for Windows.	150
Configuration Tasks	150
Chapter 6 Troubleshooting Information.	153
Troubleshooting Red Status Indicators	154
Service Target Availability Displays Red Circle.	155
Target Status Unavailable	155
No Probe Information	156
Possible Cause: Local Web server connection failed	157
Possible Cause: Invalid URL (IOPS 1-11)	158
Possible Cause: Proxy Information Incorrectly Configured	158
Possible Cause: Connection to Web proxy Timed Out.	158
Probe Data Received Displays Red Circle.	159
Data Consolidation Displays Red Circle	159
No Data Appears in the Dashboard.	159
Looking at OVIS Trace Files	160
Database running out of space.	161
OVO for UNIX Integration Enabled but not Working Properly.	162
Troubleshooting the HTTP_TRANS Probe	163

Chapter 7	Advanced Topics	165
	Internet Services Architecture and Data Flow	166
	Probes	166
	Management Server	168
	Service Level Agreements	170
	How to Move your Configuration to Another System.	172
	Security	174
	Configuring Proxy/Port Settings	174
	How Internet Services Handles Security	176
	Firewalls: Returning Data Through the Firewall	176
	How Probes Can Communicate through a Firewall.	176
	How to protect the Probe System	178
	Using Secure Probe/Server Communication.	178
	Configuring Secure Communication - Probe and Management Server.	179
	Server Certificates	179
	Client Certificates	181
	For 403.7 Forbidden: Client certificate required in IE	182
	For Microsoft Certificate Server	183
	Custom Reports.	183
	Supported Databases	184
	Database Backup	186
	For the default database	186
	Example Backup Steps if you have only MSDE installed.	187
	Example Restore Steps	187
	Starting Over.	189
	Recreating MSDE Database	190
	Recreating SQL Server Database	191
	Recreating the Access Database	192
	Recreating the Oracle Database	193
	OVIS Version 3.5 Scalability Information.	195
	Probe System	195

Examples:	196
Management Server	198
Network Usage	200
OVIS Version 4.0 Scalability Information	201
Standalone OVIS	201
Distributed OVIS: Remote Probes	202
Distributed OVIS: Remote Probes and Remote SQL Server	202
Conclusions	203
NTFS Security Settings	205

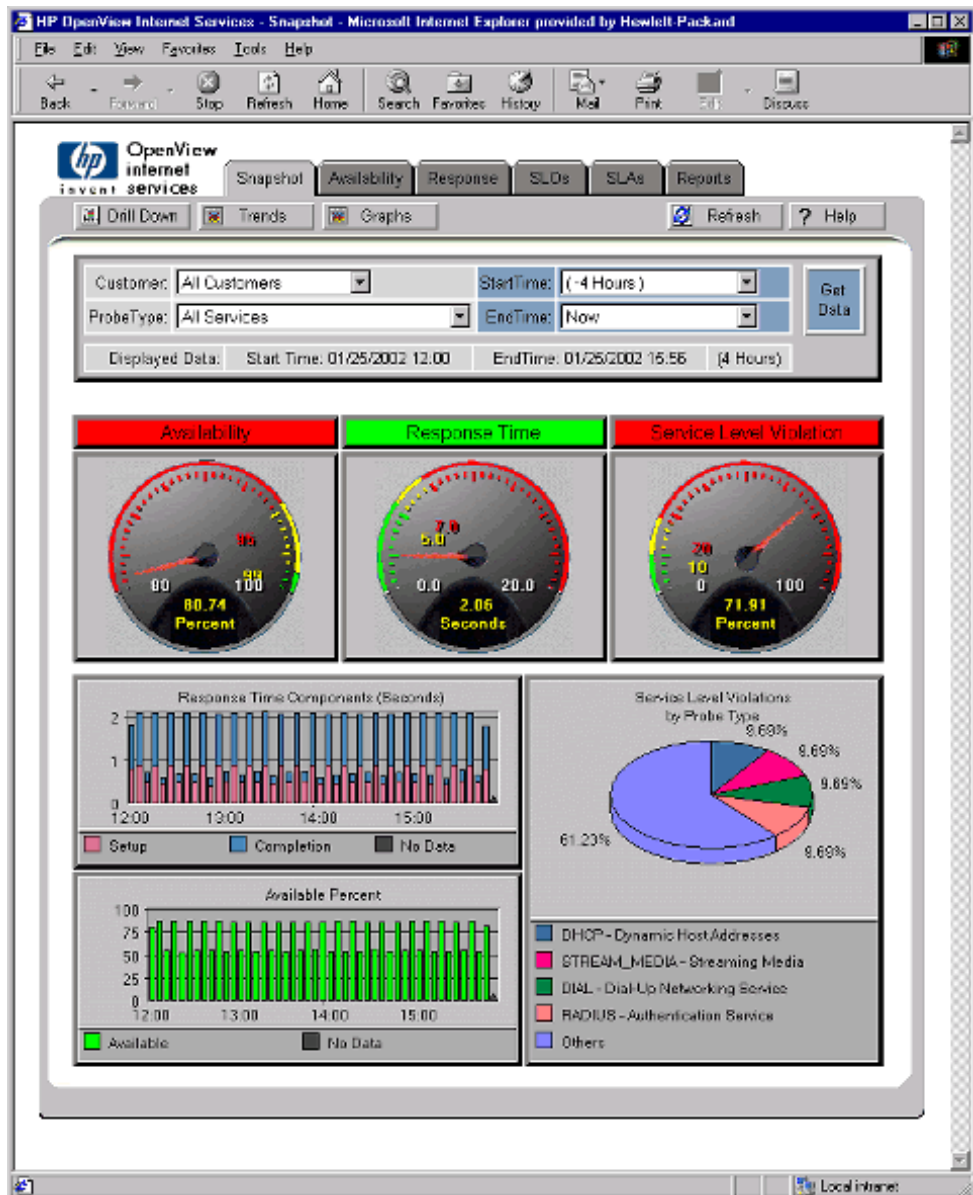
Introducing Internet Services

HP OpenView Internet Services provides a single integrated view of your Internet and related services. It is designed to help IT staff efficiently predict, isolate, diagnose and troubleshoot problems, anticipate capacity shortfalls, and manage and report on service level agreements.

HP OpenView Internet Services uses software probes to simulate business activity. These probes measure the availability, response time, service level conformance and other performance metrics for your Internet and related services. In addition service level violations and conformance to service level agreements is also monitored and reported. Data from the probes and service level calculations can be viewed in the Internet Services Dashboard web display, which includes gauges, graphs, trend data, drill down data and reports.

Internet Services can also generate alarms and make them available to other hp OpenView products. These alerts and regular information updates keep you informed as to whether or not a customer's Internet and related services are performing efficiently

The Internet Services Dashboard Snapshot is displayed below.



In the Dashboard display you can drill down into more detail as shown in the example below showing time series data for Response Time measurements.



How Internet Services Works

HP OpenView Internet Services (OVIS) allows you to monitor a customer's Internet services in an organized way. Once installed and configured Internet Services measures the availability, response time, service level conformance and other metrics of specific service activity.

Internet Services provides you with a view of the Internet and service provider world, which consists of customers and the services they access. Services and protocols such as HTTP, HTTPS, ICMP, FTP, DNS, E-mail, Dial-up, TCP access, Radius, WAP, Streaming media and more can be monitored with Internet Services. See [“Descriptions of Service Types/ Probes” beginning on page 91](#) for a complete description of all the services monitored.

With Internet Services, you configure **probes** that measure the performance and availability of these services. A probe tests service performance by executing typical transactions.

Measurements from the probes are forwarded to the **Internet Services management server** where they are stored in a database. Data is consolidated for reporting in the Internet Services Dashboard web display.

From the Internet Services **Dashboard**, you can look at a snapshot of the current status of the services and also get more detailed data on availability, response time, service level violations and conformance to service level agreements. Even more detail is available in the drill down reports. And you can get a view longer-term trends and look at nightly run **reports**.

Service Level Agreements can be created using the Internet Services Configuration Manager and conformance to these agreements can be reported in the Dashboard.

Service **alarms** can be forwarded to Network Node Manager, OpenView Operations for Windows and OpenView Operations for UNIX (also known as VantagePoint Operations), or any other event manager capable of receiving SNMP traps. These alerts and regular information updates keep you informed as to whether or not a customer's Internet services are performing efficiently.

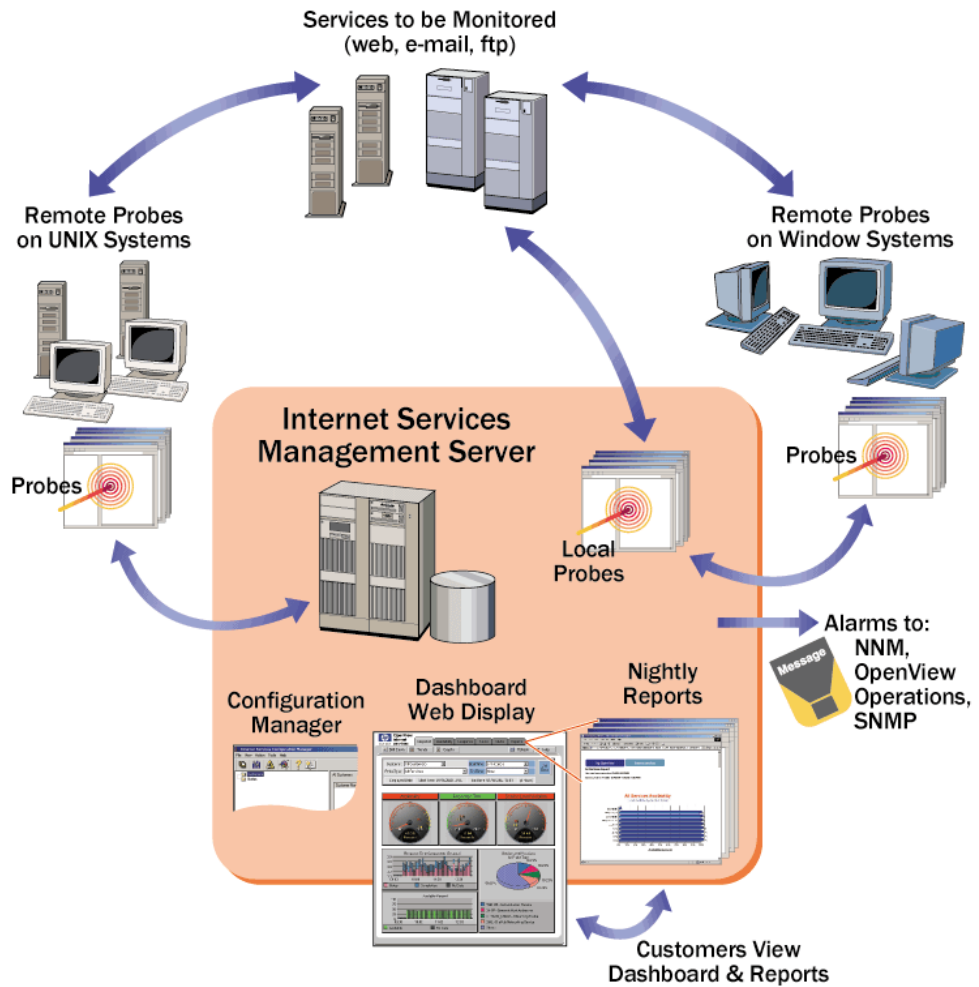


Figure 1 High Level Overview of the Internet Services Components

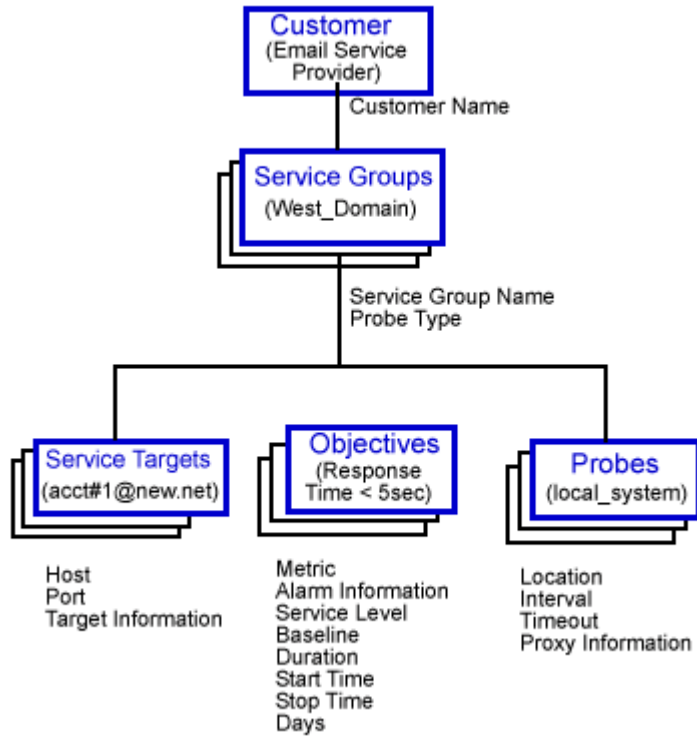
The Services Hierarchy

You use the Internet Services Configuration Manager to configure each service target you want to monitor. You group the service targets under service groups for each customer forming a service hierarchy. This structure allows you to view data by service type and customer.

At the top of the services hierarchy is the customer, which could be the name of a company, Internet service provider, or any entity within a company. Below the customer is the service group. One customer may have one or more service groups; each service group should contain services of the same type. Below every service group are the three components that allow Internet Services to measure, interpret, and thereby generate reports and alarms. Those three components are:

- the **service target**: the service to measure and the location of the service.
- the **service objective**: the value that the service must comply with in order to meet the service goal (objective).
- the **probe location**: where the probe is deployed.

Figure 2 Service Hierarchy



Implementation Sequence

The steps to using Internet Services are as follows

- 1 Install the software.
- 2 Use the Internet Services Configuration Manager to configure, customers, service groups, service targets to be probed, service level objectives and service level agreement conformance levels and define the probe location. Probes can be set to monitor from the local Management Server system or the probe software can be deployed to remote systems.
- 3 The probes measure response time, availability and other performance metrics.
- 4 The probes send data back to the Management Server.
- 5 On the Management Server, data is consolidated for viewing in the Dashboard and for generating alarm events that can be sent to NNM, OpenView Operations for UNIX, OpenView Operations for Windows or a generic SNMP management station.

Both the [“Getting Started with Internet Services” beginning on page 19](#) and [“Configuring Internet Services” beginning on page 41](#) chapters provide you with information for configuring the services you want to monitor. These chapters show how to organize the services, set up service level objectives, service level agreements and alarms. Online Help and a Configuration Wizard are available to guide you through your initial configurations.

Integration with other OpenView Products

As described in [“Integrating with Other OpenView Products” beginning on page 131](#), Internet Services can be configured to integrate with OpenView Operations for UNIX and for Windows, Network Node Manager, or any event manager capable of receiving SNMP traps.

If installed on the same system as Internet Services, HP OpenView Reporter also integrates with Internet Services. All of the enterprise reporting, including Internet Services, is viewable in the same set of Web pages. This allows you to see both the user view of Internet service performance as well as any performance problems on the server itself. In addition, having hp OpenView Reporter installed on the same system as Internet Services allows you capabilities such as creating custom reports for Internet Services and modifying shift definitions. If Reporter is configured to use an Oracle or SQL Server database, then when Internet Services is installed on the same system it will use the same database.

If HP OpenView Performance Agent (MeasureWare/NT) is installed on the same system as Internet Services, then Internet Services data is automatically logged using ARM so that it can be viewed through PerfView.

Getting Started with Internet Services

This chapter introduces you to the simple steps you need to take in order to install and start using Internet Services (OVIS). An example takes you through a quick start to using Internet Services. It is strongly recommended that you follow the steps in the example to become familiar with configuration and monitoring. After completing all steps in the example, you should find it easy to configure and monitor your own service targets.

Initial tasks involve **Installing** and **Configuring** Internet Services as follows:

- “Installation Considerations”
- “Installation Prerequisites”
- “Install Internet Services”
- “Quick Start for Using Internet Services”
- “Uninstalling Internet Services”

Installation Considerations

If you have a version of Internet Services already installed, please refer to the Release Notes for important information on upgrading the software.

Before you begin, you need to ensure that the system on which you install Internet Services meets the minimum requirements. Then you are ready to complete the simple installation and start configuring services.

Installation Prerequisites

The following recommendations represent minimum requirements for Internet Services.

Hardware Requirements

Windows Management Server

- Intel Pentium III, 500 MHz or faster processor with 256 MB of memory or more are recommended.
- 200 MB of disk space is required initially, with increases as more data is added.
- Temporary disk space during report generation may range from 50-1000 MB, depending on the number of services being probed.

Windows NT/2000 Probe System

- Intel Pentium, 200 MHz or faster processor with 64 MB of memory or more are recommended. This depends on the number of probes that should run in parallel. For most efficient execution and metric accuracy, it is recommended that the system be dedicated to probing.
- 10 MB of disk space for probes and configuration files, plus an additional 10- 100 MB of disk space to hold probe data in queue files in case the network goes down. Space required is dependent on the number of probe targets and length of network downtime you wish to accommodate.

UNIX Probe System

- 128 MB of memory or more is recommended.
- 10 MB of disk space for probes and configuration files, plus an additional 10- 100 MB of disk space to hold probe data in queue files in case the network goes down. Space required is dependent on the number of probe targets and length of network downtime you wish to accommodate.

Software Requirements

Windows NT/2000 Management Server

- Microsoft Windows 2000 Professional or Server with Service Pack 1 or 2 (Service Pack 2 is highly recommended for security reasons)

Microsoft IIS 5.0 Web Server.

OR

- Microsoft Windows NT 4.0 Server with Service Pack 6a

Microsoft IIS 4.0 Web Server

OR

- Microsoft Windows NT 4.0 Workstation with Service Pack 6a

Microsoft IIS 4.0 Personal Web Server (available on Windows NT option pack 4.0)

AND

- Internet Explorer 5.5 or greater. Internet Explorer 5.5 is required in order to support Restricted Views and for the Web Transaction Recorder
- NTFS file system is required
- Virtual memory should be set to an initial size of 512 MB or larger on the system running Internet Services. Systems running other applications may require larger virtual memory settings to accommodate Internet Services in addition to the other applications.
- DHCP is not supported on the management server (but it is supported on remote probe systems)

- For probes running on the local system, if you use the Dial Up probe, or configure other probes (such as a WAP probe) to run over a Dial Up Network Connection, RAS (Remote Access Server) and a minimum of one phonebook entry must be configured on the management server.
- For Streaming Media probes running on the local system, you must install Real Player (basic or higher) for Windows. You can download a free version of Real Player from www.real.com.
- Adobe Acrobat Reader 4.0 or higher is required to view the Internet Services User's Reference Guide (in .pdf format). You can download the reader from <http://www.adobe.com/products/acrobat/>.

See the Internet Services Release Notes for requirements for integration with OpenView Operations for Windows.



On systems running Business Transaction Observer (BTO), do not install Internet Services server components. BTO requires a dedicated system in order to operate as expected.

Windows NT/2000 Probe System

- Microsoft Windows NT 4.0 Server or Workstation with Service Pack 6a; or Microsoft Windows 2000 with Service Pack 1 or 2 (Service Pack 2 is highly recommended for security reasons).
- Internet Explorer 5.5 or higher.
- If you use the Dial Up probe, or configure other probes (such as a WAP probe) to run over a Dial Up Network Connection, then RAS (Remote Access Server) and a minimum of one phonebook entry must be configured on the Windows probe system.
- If you have the Streaming Media probe on the remote Windows system, you must install Real Player (basic or higher) for Windows. You can download a free version of Real Player from www.real.com.



DHCP is supported on remote probe systems.

UNIX Probe System

HP-UX 11.0, 11.11, 11.20
Sun Solaris 2.6, 2.7, 2.8
Linux Red Hat 6.0, 6.2, 7.0

The HTTP_TRANS probe in Internet Explorer heavyweight mode is not available on UNIX systems but is available in URL and Navigation Point modes on UNIX system.

The Streaming Media probe is not available on UNIX.

Dial-Up Probe Requirements on UNIX Systems

If you are using the Dial-Up probe on a UNIX system the following software is required.

Solaris

Solaris (for all supported versions) the following must be installed:

SUNWbnur Networking UUCP Utilities (Root)
SUNWbnuu Networking UUCP Utilities (Usr)

Solaris 8 and Solaris 7 (11/99) also require the following to be installed:

SUNWapppr PPP/IP Asynchronous PPP daemon configuration
SUNWapppu PPP/IP Asynchronous PPP daemon and PPP login service
SUNWpppk PPP/IP and IPdialup Device Drivers

Solaris, earlier versions of Solaris 7 require the following to be installed:

SUNWpppk Solstice PPP Device Drivers
SUNWapppu PPP/IP Asynchronous PPP Daemon and PPP login service
SUNWapppr PPP/IP Asynchronous PPP daemon configuration files

If you have 64-bit Solaris 7 or 8 installed you should also have the following package installed:

SUNWpppkx PPP/IP and IPdialup Device Drivers (64-bit)

HP-UX (11.0 and 11.11)

PPP-RUN software is required. Note you do not need to manually install the PPP software if you have the following:

- The LAN/9000 networking products was pre-installed on your system (instant ignition).
- You used the HP-UX swinstall program to install the Core Networking Bundle. The PPP-RUN fileset is part of this software bundle.

Linux

The following versions of PPP are required:

Linux RedHat 6.0 requires ppp-2.3.7-2

Linux RedHat 6.2 requires ppp-2.3.11-4

Linux RedHat 7.0 requires ppp-2.3.11-7

Browser Requirements for Viewing the Dashboard

A web browser for viewing the HTML reports (Netscape 4 or later, or Internet Explorer 5 or later).

When viewing Dashboard reports, you must have your browser configured to check for newer versions of stored pages in order for all the report images to update properly.

For example, in IE 5.5 select **Tools > Internet Options > General Tab** then click the **Setting** button under Temporary Internet Files. Be sure that **Every Visit to the Page** is selected and then click **OK**.

For example, in Netscape 4.7 select **Edit > Preferences** and in the dialog box expand the tree to select **Advanced > Cache**. Then select **Every time I view the page** setting under **Document in cache is compared to document on network**.

If Restricted Views has been enabled, then when logging into the Dashboard you will first be prompted to enter a user name and password before viewing the Snapshot display.

Platform Support

Internet Services has four components that span a variety of platforms.

Component	Platform
Internet Services Management Server	Windows NT and Windows 2000
Internet Services Database	<p>MSDE (default).</p> <p>MS Access and SQL 7 are supported on updates from previous versions of OVIS where MS Access or SQL 7 were already configured.</p> <p>Internet Services can be configured to use Oracle 8.0.6, 8.1.6, 8.1.7 database on HP-UX or Sun Solaris or SQL Server 2000 database.</p> <p>If Reporter is installed on the same system, Internet Services will use its database.</p>
Probes	<p>Windows and UNIX platforms: HP-UX, Solaris, and Linux</p> <p>HTTP_TRANS in IE mode is not available on UNIX but is available in URL and Navigation Point modes. The Streaming Media probe is not available on UNIX.</p>
Service Targets	All supported platforms above

Install Internet Services



If you are upgrading from a previous version of Internet Services please first refer to the Internet Services Release Notes for important information on upgrading.

- **Insert the CD in the CD-ROM drive and follow the online instructions.**
- **Reboot the system after the installation is complete.**

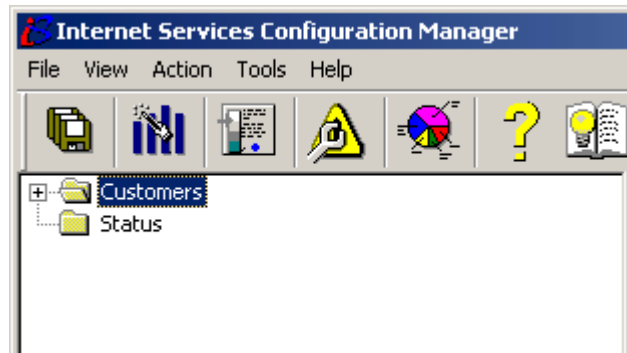
Quick Start for Using Internet Services

In this example you are going to configure the Web page www.hpshopping.com as a service target for the customer Hewlett-Packard.

Probe Configuration

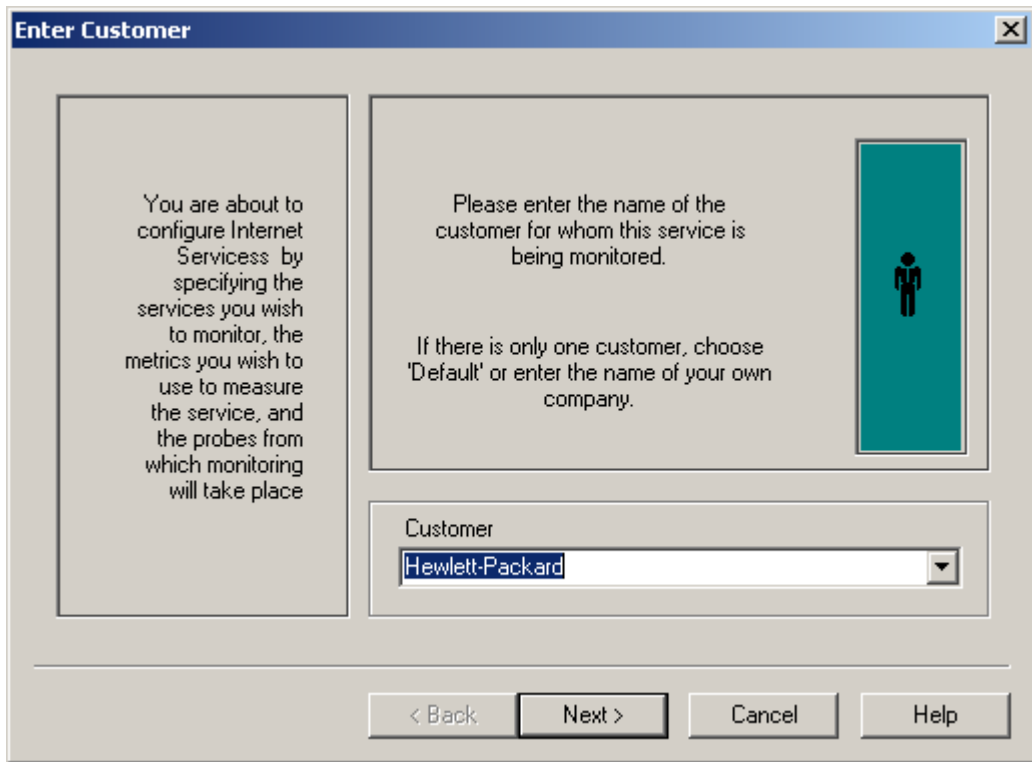
To create the local configuration on the Windows Internet Services Management Server:

- 1 Open the Configuration Manager by selecting **Start>Programs>HP OpenView>internet services>Configuration Manager**.

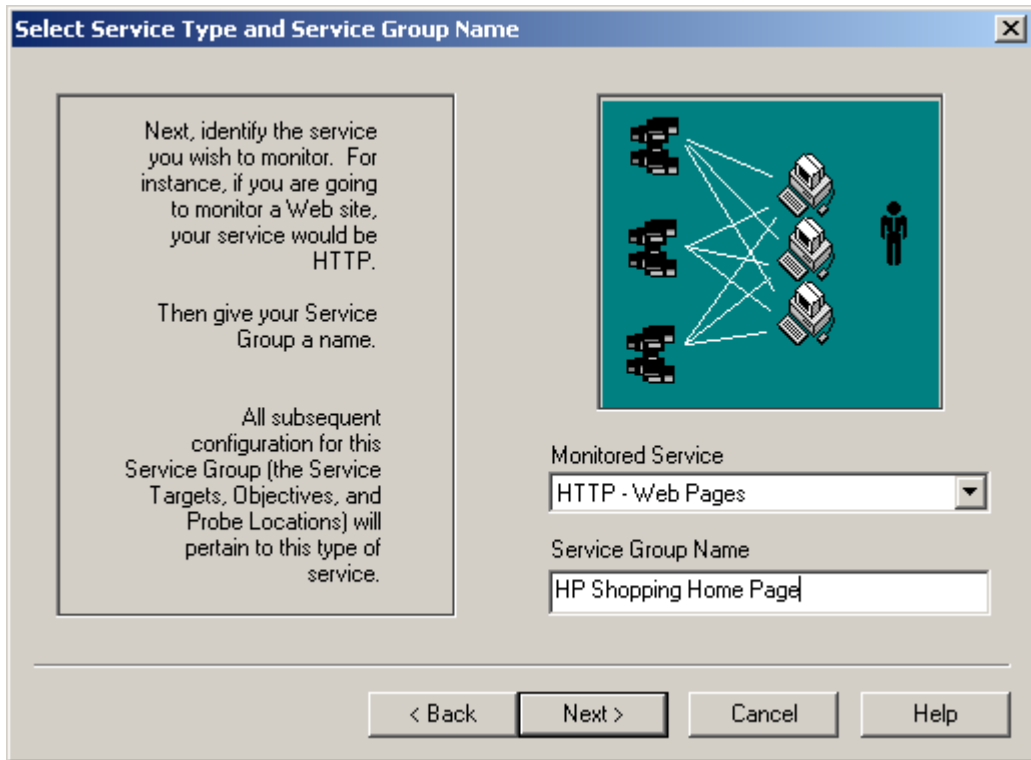


- 2 Select the **Configuration Wizard** toolbar button (second from left on the toolbar) or select **File>Configuration Wizard** from the menu.

- 3 The Configuration wizard begins with the **Enter Customer** dialog enter **Hewlett-Packard** for this example. The Customer Name identifies the customer who has the service target(s) to be monitored. Click **Next**.



- 4 In the **Select Service Type and Service Group Name** dialog box, select **HTTP-Web Pages** as the service type, name the service group **HP Shopping Home Page**, and click **Next**.



As you organize services, remember that service targets within a service group must be the same type: for example, HTTP (Web pages) is one type of service, while DNS (Domain Name Server) is another.

- 5 In the **Add Service Targets** dialog displayed select the **Add Service Target** button to open the **HTTP WebPages Information** dialog box and enter **www.hpshopping.com** as the Service Target you want to monitor. Click **OK** and click **Next**.

HTTP - Web Pages Information

Address (URL)

(e.g. "www.hp.com") (e.g. "/country/us/eng/supportservices.htm")

http:// /

Web Server Port

Pattern Matching Information

Pattern

Pattern Matching Settings

Options

Load Images and Frames

Connection Keep-Alive

No Cache (Proxy)

Web Server Authentication

User

Password

Proxy Authentication

User

Password

Other

Probe Retries

Wait between Retries

Client Certificate Authentication

Certificate File Name

Certificate Private Key Password

Help OK Cancel

- 6 In the **Add Objectives** dialog select **Add Service Objective**. In the **Objective Information** dialog, accept the defaults, which specify that the service group should be available 90% of the time, click **OK** and **Next**.

Objective Information

Metric
Metric to be evaluated
AVAILABILITY

OK
Cancel
Help

Service Level
Service Level Objective > 90 Percent

Alarms
Duration 10 minutes
Max Scale Value 100
Alarm Range Units
Normal > 90 Percent
Warning > 90 Percent
Minor > 90 Percent
Major > 90 Percent
Critical < 90 Percent
 Use historical baseline in addition to thresholds to trigger alarms: 80 percent
Message HTTP Service for <TARGET> is unavailable

Objective Activity Times
 Always monitor
 Monitor at specific times
Start alarming 8:30:00 AM
Stop alarming 5:00:00 PM
 Monday
 Tuesday
 Wednesday
 Thursday
 Friday
 Saturday
 Sunday

SLA Objective
 Apply Objective Only to SLAs

- 7 In the **Add Probe Locations** dialog that appears, select the **Add Probe Location** button to open the **Probe Location** dialog.

Probe Location Info

Probe Location: Local System

Probe Request Information:

Measurement Interval: 300 seconds

Request Timeout: 45 seconds

Network Connection:

Default

New Connection

Edit Connection

Delete Connection

Web Proxy Information:

This is the proxy used by the probe to access the service targets.
For HTTP, HTTPS, HTTP_TRANS & STREAMING_MEDIA only

HTTP Proxy Address: <none> Port: <none>

HTTPS Proxy Address: <none> Port: <none>

Internal Internet Services Proxy Information:

This is the proxy used by the probe to access the Internet Services server.

Proxy address: <none> Port: <none>

OK

Cancel

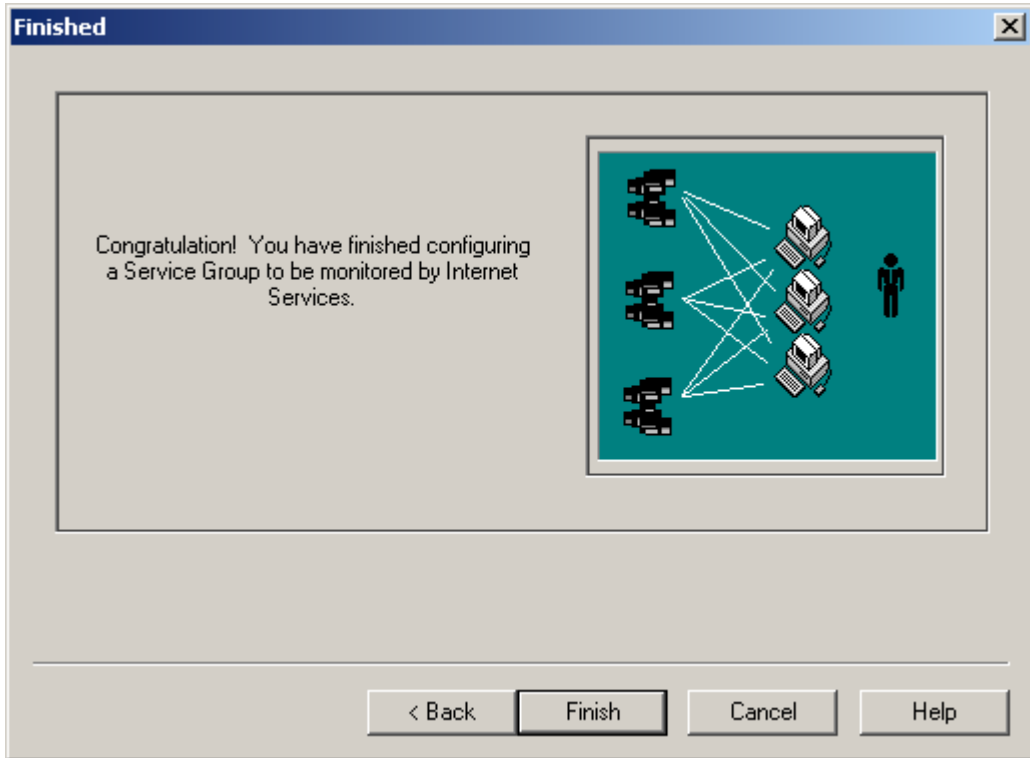
Help

Accept all defaults EXCEPT for Proxy Information. If you use a web proxy to get access to a site like www.hpshopping.com, then you must enter the same proxy address and port number that is configured for your Web browser.

For Internet Explorer you can typically find this information under the main menu selections under **Internet Options>Connection tab>LAN settings**. **For Netscape** you can find this information under

the main menu selections, where you choose **Preferences** and expand the **Advanced** area of the tree and select **Proxies**.

- 8 Click **OK** and click **Next**. Click **Finish** to complete the wizard-guided setup.

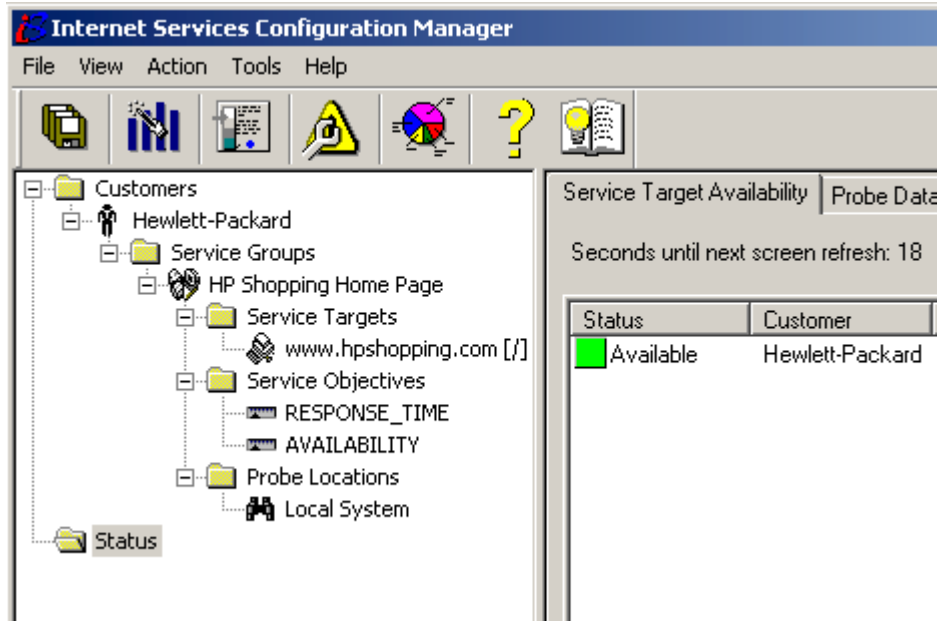


- 9 From the Configuration Manager click the **Save** toolbar button or select **File>Save** from the menu.

▶ It is important to save your configuration as no service monitoring occurs until you do.

Check the Status of Data Collection for Configured Services

In the Configuration Manager left pane, select Status to check for success in contacting the service target. If you configured the service target correctly, the icons should turn green within five minutes. Refer to the chapter “[Troubleshooting Information](#)” beginning on page 153 of this guide for what to do if the icons are not green.






The **Service Target Availability** page shows the status of the measurement or service target. It shows whether or not the probe data reached the temporary trace table storage area on the Internet Services Management Server and whether or not the service target is available. The reason for showing availability is that if a server name or Web page is misspelled, or more importantly, if the service is really down, that target will show up as unavailable. This may happen within five minutes of saving the configuration (before the probe has had a chance to gather measurements) and indicates by showing availability whether the target is configured correctly and available.

The **Probe Data Received** page shows whether or not the probe successfully transferred its measurement data to the temporary trace table storage area on the Internet Services Management Server. This normally happens within five minutes of saving the configuration and displays by the next screen refresh.

The **Data Consolidation** page shows whether or not collected data was transferred from the temporary trace table storage area to the reporting database for display in the Dashboard Snapshot page and in reports. This normally happens within ten minutes of saving the configuration.

The **Remote Probe Update** page shows when the remote probe system contacted the server the last time for new configuration information.

Service Target Availability	Probe Data Received	Data Consolidation	Remote Probe Update
-----------------------------	---------------------	--------------------	---------------------

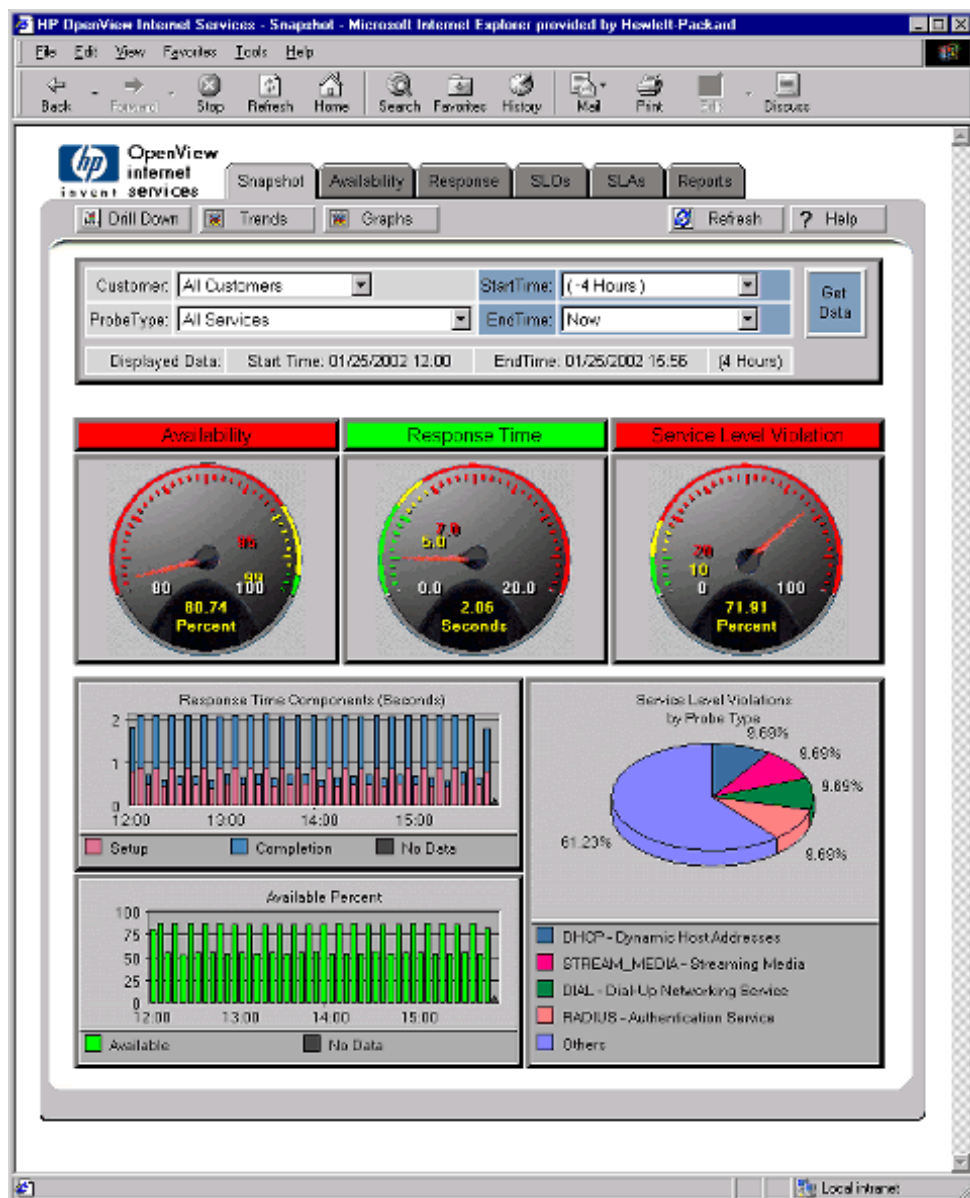
-  Red circles indicate the action was unsuccessful.
-  Yellow triangles indicate the action is not yet complete (trying to complete).
-  Green squares indicate the action was successful.

View the Data using the Dashboard Webpage display.

From the Configuration Manager select the Launch Internet Services Dashboard (pie chart) toolbar button or from the menu you can select **Action>Run>Dashboard** to launch the Dashboard Web pages that display Internet Services data.

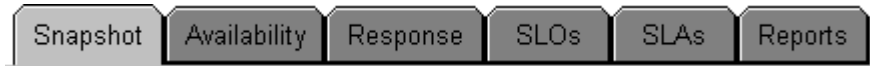


You can also start the Dashboard data display by selecting **Start>Programs>HP OpenView>internet services>Dashboard Display**.



Snapshot Tab

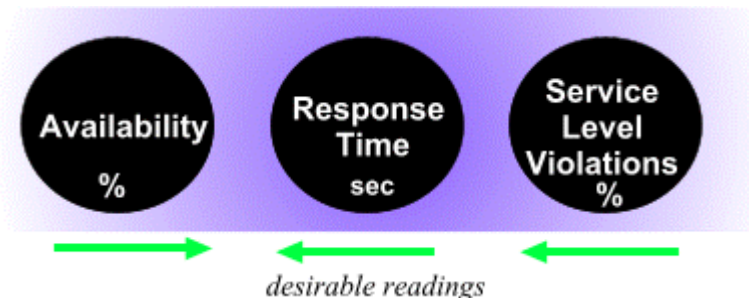
Select the Snapshot tab to display a summary of your monitored Internet Services.



Data Selection in the Dashboard: The data is narrowed (or broadened) by the data selections at the top of the current page. By default you see data for all customers and all service types for the last four hours. These selections pertain to all tabbed pages, except the Reports page, which shows longer term data. To change the data display, select the Customer, Probe Type, StartTime and EndTime and press the **Get Data** button. On some pages you can also select whether to display the data as averages or time series.

Customer:	All Customers ▾	StartTime:	(-4 Hours) ▾	Get Data
ProbeType:	All Services ▾	EndTime:	Now ▾	
Displayed Data:	Start Time: 11/05/2001 07:00	EndTime: 11/05/2001 10:46	(4 Hours)	

The Dashboard's service Snapshot page contains three round gauges that graphically represent the performance for the selected service type. These gauges provide an overview of how the selected service type is performing in terms of: availability, response time, service level objective violations.



- **Availability:** shows the percentage available and acceptability of that value; the default setting means that the service must be available 95% or more of the time; green indicates acceptable, yellow, a warning; and red, unacceptable. See [“How Service Target Availability is Determined” on page 62](#)
- **Response time:** shows the average number of seconds each service transaction needed to complete and the acceptability of that value.
- **Service level violations:** shows the percentage of service level objectives which were violated. For example if you configured response time SLOs, this would show the total service response times that exceeded their configured thresholds and the acceptability of that value.

The **pie chart** (if displayed) offers a quick look at service types in violation of their configured thresholds. For example, if three service types are in violation, the chart shows by percentage which are in violation to a greater or lesser degree. If only one service type is in violation, the pie chart will represent that service type as being 100% of the service level violators. If you see no pie chart below the gauges, Internet Services has detected no service violations from any configured service type. Note: if you have selected a specific probe type (for example HTTP) then this pie chart will show the individual service group contribution to the service level violation percentage.

Availability, Response, SLO, SLA Tabs

Next, look at the detail information contained in the Availability, Response Time, Service Level Objectives (SLO) and Service Level Agreements (SLA) tabs. Note that the first three can also be viewed by clicking on the corresponding gauge in the Snapshot page. These pages show more detailed views of the data. Each one contains three views: the first is a horizontal bar chart showing either availability, response time, or service level violation for each service group. The second view shows these metrics by customer, and the third view shows them by shift (for example, Prime and Offshift). Again, this data can be narrowed or broadened with the data selections at the top of the page.

Time Series: If you wish to view this data over time, you may select Averages and Time Series in the data selections at the top of the page. This useful view allows you to see how the selected service(s) has been performing at each individual period over the timespan selected.

Reports Tab

You can select the Reports tab to see long-term reporting. These reports are generated automatically every night and so will not be available until the day following installation and configuration.

Drill Down and Trend Data

If you want to see information on the individual targets or probes within a service group, select the **Drill Down** button at the top of the page. This accesses information from the detailed data tables. It is useful for drilling down to get a more detailed view of individual targets and probes, helping to find the source of potential problems. To return from the Drill Down page, select the appropriate tab.

If you want to see information regarding trend data, select the **Trend** button. This gives you both hour-of-the-day and day-of-the-week trending information based on all data collected since Internet Services installation.

Graphs Web Form

You can select the Graphs button at the top of the page. This allows you to draw additional graphs, and with the custom graphs function, you can create your own graphs based on Internet Services data.

The standard graphs available from the Graphs web form are:

- Internet Response Time
- Snapshot Gauges
- Snapshot Five Gauges
- Snapshot Response
- Snapshot Availability
- Snapshot SLO Violations
- Availability by Service Group
- Availability by Customer
- Availability by Work Shift
- Response by Service Group
- Response by Customer
- Response by Work Shift
- Service Level by Service Group

Service Level by Customer
Service Level by Work Shift
Trend Availability
Trend Response
Trend Service Level

Uninstalling Internet Services

To uninstall Internet Services:

- 1 Stop the Internet Services components:
 - a Reporter Service
 - b "HP Internet Services"
 - c World Wide Web Publishing Service
- 2 Go to **Add/Remove Programs** in the Control Panel and select to uninstall/remove the HP OpenView Internet Services product.

Configuring Internet Services

Topics covered in this section are as follows:

- “Configuring Services”
- “Using the Configuration Manager (and wizard)”
- “Setting Objectives, Baselines and Alarms for the Service Group”
- “Setting Up Service Level Agreements (SLAs)”
- “Configuring the Network Connection (optional)”
- “How Probes Work”
- “Configuring and Installing Remote Probes for Windows NT/2000”
- “Configuring and Installing Remote Probes on UNIX Systems”
- “Automating Configuration of Large Numbers of Service Targets”

Configuring Services

Internet Services provides a means of organizing the services on which you want to receive reports and notifications of problems.

At the top of the services hierarchy is the customer, which could be the name of a company, Internet service provider, or any entity within a company. Below the customer is the service group. One customer may have one or more service groups; each service group may only contain services of the same type. For each customer you can add Service Level Agreements that can be applied to that customer's service groups.

Below every service group are the three components that allow Internet Services to measure, interpret, and thereby generate reports and alarms. Those three components are:

- the **service target**: the service to measure and its location (where the service originates)
- the **service objective**: the value that the service must comply with in order to meet the service goal (objective)
- the **probe**: the service recipient's location (where the service request originates)

Also for a customer you can configure Service Level Agreements (SLAs) and set a conformance level for each SLA.

Default Configuration Settings

Internet Services allows you to organize your service monitoring based on individual customers, each with its own set of service groups, targets, etc. If there is only one customer, or if you do not want to use this capability, you can create a default customer, under which you can place all service groups.

You can add service level agreements, service groups, their service targets, service objectives, and probe locations, using the Configuration Manager (see the sections below). Or you can use a program that is designed for automating configuration of large numbers of service targets at once (see “Automating Configuration of Large Numbers of Service Targets” on page 71).

The section “Using the Configuration Manager (and wizard)” on page 43 shows how to start the Configuration Manager. Subsequent sections describe service level objectives, service level agreements, how service probes work and how the service performance levels are established.

Initially you may choose to accept the suggested values that populate many of the settings within the dialogs that appear as you step through the setup using the Configuration wizard. With service level settings established, services that do not meet acceptable performance goals can generate reports and/or alarm events and messages, depending on how you choose to configure them.

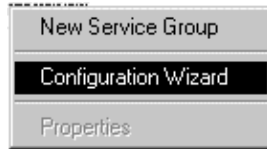
Using the Configuration Manager (and wizard)

You can use the Internet Services Configuration Manager to add and modify customers, service level agreements, service groups, service targets, and their settings. The Configuration Manager facilitates the process with a display that shows how customers/service groups and their service targets, objectives, and probes are super- and sub-sets of each other. Online Help is also available from the Configuration Manager window and is context sensitive within the dialogs.

Within the Configuration Manager, you can view default settings or change the settings, once you have established what the desired service levels are. To open the Configuration Manager window, select **Start>Programs>HP OpenView>internet services>Configuration Manager**.



The Configuration Manager also includes a wizard, accessible through a toolbar button or on the **File>Configuration Wizard** menu. The Configuration Wizard steps you through the process of establishing customers, service groups, targets, service level objectives, alarms (thresholds and baselines), and probe locations.



You can also access the Configuration Wizard by right-clicking any item in the hierarchy and selecting Configuration Wizard.

Setting Objectives, Baselines and Alarms for the Service Group

When you set up a service group, you can establish an expected service level objective (SLO) for performance for the group.

The Configuration Manager facilitates this process by providing the dialog pictured below.

Objective Information
✕

Metric

Metric to be evaluated

AVAILABILITY ▾

OK

Cancel

Help

Service Level

Service Level Objective > 90 Percent

Alarms

Duration 10 minutes

Alarm Range Units

Max Scale Value 100

	90	>	Normal	>	90	Percent
	90	>	Warning	>	90	Percent
	90	>	Minor	>	90	Percent
	90	>	Major	>	90	Percent
			Critical	<	90	Percent

Use historical baseline in addition to thresholds to trigger alarms: 80 percent

Message HTTP Service for <TARGET> is unavailable

Objective Activity Times

Always monitor

Monitor at specific times

Start alarming 8:30:00 AM ▾

Stop alarming 5:00:00 PM ▾

<input checked="" type="checkbox"/> Monday	<input type="checkbox"/> Saturday
<input checked="" type="checkbox"/> Tuesday	<input type="checkbox"/> Sunday
<input checked="" type="checkbox"/> Wednesday	
<input checked="" type="checkbox"/> Thursday	
<input checked="" type="checkbox"/> Friday	

SLA Objective

Apply Objective Only to SLAs

The information you enter in this dialog pertains to the service group. The settings will affect the results displayed in the Internet Services Dashboard, and the Service Level Agreement (SLA) evaluation.

Alarms are for integration with event managers and apply to every target in the service group. Although the settings for the Service Level and Alarms are typically determined for two distinct purposes, it is useful to have them in the same dialog box so that alarms can be sent before service level violations are reached. This allows the operational group to react before contractual commitments are violated.



Internet Services can send alarms to Network Node Manager (NNM), OpenView Operations for UNIX (also known as ITO), and OpenView Operations for Windows (also known as VantagePoint for Windows). For integrating Internet Services to with OpenView Operations (OVO) and/or NNM, please refer to [“Integrating with Other OpenView Products” on page 131](#) for more information.

Many of the boxes within this dialog show suggested values, which you can accept or modify. No setting is finalized until the service group configuration has been saved. Each Objective setting defines the expected limits for a specific metric. These limits are applied to every Service Target in the Service Group. The settings provide a value against which the collected metric value for the service group is evaluated.

- **In the Metric section**, select the desired metric.
- **In the Service Level section**, accept the default for the metric or set a threshold against which to compare all incoming values for the metric. Incoming values that exceed this threshold are counted as violations and are reported within the Internet Services data display (Snapshot, bar chart summaries, and drill down reports). Service level settings are *not* used for generating alarms.
- **In the Alarms section**, define alarm event range values for the metric selected. Then, in order for alarms to be send to NNM or OVO or via SNMP, you also need configure the alarm destination. This can be done in the Configuration Manager by selecting **File>Configure>Alarm Destinations** or by selecting the Configure Alarm Targets toolbar button. See the online Help for details. See [“Integrating with Other OpenView](#)

Products” beginning on page 131 for details on the integration with NNM, and OVO.

- **Duration:** Indicates that a probe metric value can exceed expected limits for a short period of time and not generate an alarm. This setting is useful to reduce the number of alarms caused when one incoming metric value exceeds limits but others are generally acceptable. Setting a longer duration delays any actions until incoming metric values exceed the limits for the entire duration period. (Setting duration value at less than that of the probe sampling interval disables the feature.) The default probe sampling interval is 5 minutes (300 seconds), so you should consider setting duration in increments of 5 minutes (5, 10, 15, etc.). Setting Duration to zero generates alarms right away.
- **Use historical baseline...:** When unchecked, it is disabled. Use this setting to restrict the number of alarms as it specifies the percentage of returned values that are expected to fall within the *normal* range. This setting will override the alarm settings for the metric if it falls within 80% of the values for that day of the week and time of day. A normal range is calculated automatically over time if a value is present in this text box. This setting works well for high-use periods when metric values peak but are still considered normal.

For example, between 10 AM and 12 PM on Monday, a stock trading page gets many purchase orders and experiences its *peak* period. Response times for web page loading are between 4-6 seconds, values which exceed the alarm threshold of <3 seconds. However, the historical baseline calculates that during this high-use period, response times average within a 4-6 second range fall within 80% of the incoming values. As a result, because the baseline was set to 80%, alarms are not generated for these values. Values at a higher level that fall outside this range make up the other 20% of the response times measured, and these values which could be anywhere from 7 seconds and up generate alarms and signify a true violation of an acceptable service level.

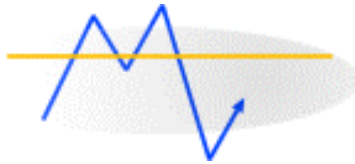
- **In the Objective Activity Times sections**, you can filter the time periods you would like services monitored.

You can choose to use one, some, or all the settings for Service Level, Alarms, Use historical baseline..., Objective Activity Times. You get different effects, depending on the settings you use as explained below.

Note: There is a fundamental difference between Availability and other metrics like Response Time. For instance, for a specific time period, if the target service is unavailable, then Availability for that time period will have an availability value of zero, while Response Time will have a value of No Data or the time period. This is because the service was unavailable, and so there is No Data for Response Time for the time period.

Setting Alarm Event and Service Level Objectives Only

The fixed values for alarm events and service level violations are unlike the baseline value, which can fluctuate. Whenever an incoming metric value does not meet the alarm or service level value, a violation occurs. If the violation continues to occur for the number of seconds specified for the duration, an alarm event occurs. If at any time during the interval the metric value returns to an acceptable level, the interval time span is reset and starts over.



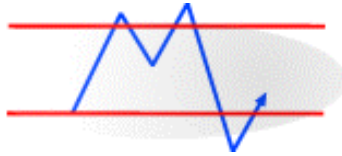
How alarm events work with duration settings: An incoming metric value must exceed the threshold until the end of the interval for an action to occur. After an event occurs, the duration timer is reset. If the incoming metric value continuously exceeds the threshold value over the course of another duration interval, an event occurs again. Once an event occurs, incoming values for the metric continue to be monitored, and when the value drops below the threshold an Alarm Finished event can occur.



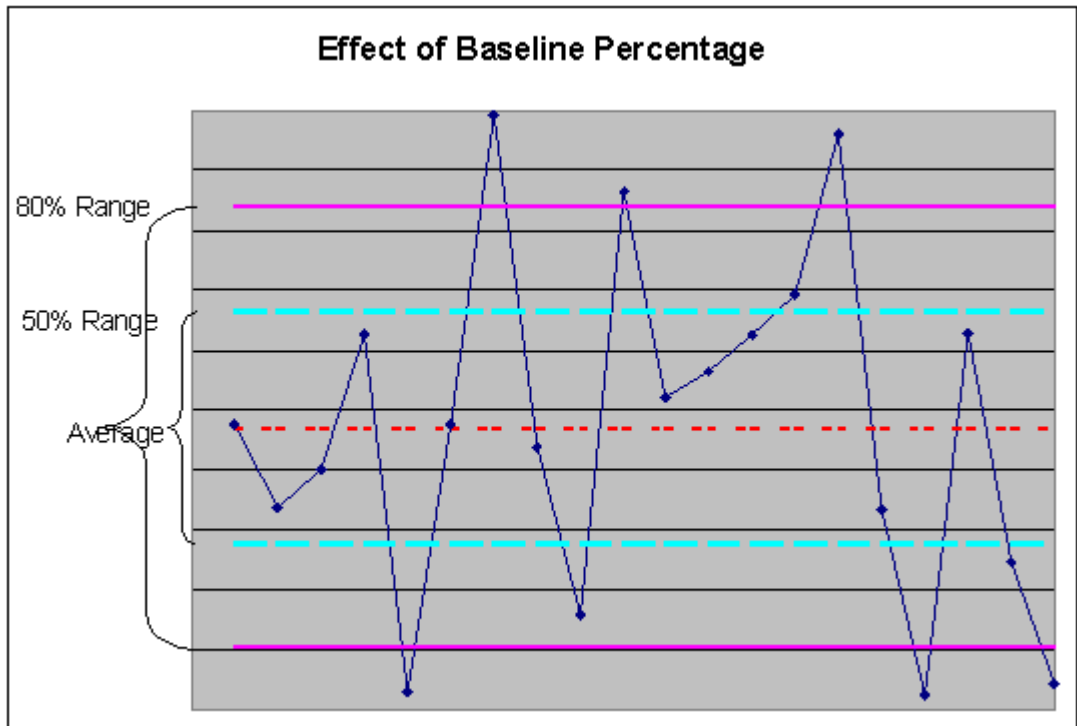
The Duration setting is for alarms only; service level violations are counted regardless and reported in the Internet Service data display (Snapshot and reports).

Setting Baseline Objectives Only

The baseline comparison value is automatically calculated by watching incoming probe metric values. Once a sufficient number of values accumulate, a predictable range of values can be established for the metric.



Alarm events occur according to the value(s) set for various levels, but instead of using a fixed value, the metric value is compared against the expected high (or low) value from the baseline. The value set in the Baseline dialog box is not a fixed value. The baseline value is a percentage (from 1 to 100) that determines how loose or tight you expect the predicted *normal* range to be. The value indicates the percentage of all metric values that are expected to lie within the normal range. A value of 80 for the Baseline says that 80% of all metric values should lie between the expected low and high values of the range. Likewise, a value of 80% also indicates that you expect 20% of the metric values to fall outside the baseline range. The larger you set the baseline percentage value, the fewer events that will occur, since a larger percentage of metric values will be considered normal.



Baseline values will be adjusted to one of the values in this table:

Baseline Value	Standard Deviations from Average
50	0.6745
68.27	1.000
75	1.150
80	1.281 (default)
90	1.650
95	1.960
95.43	2.000

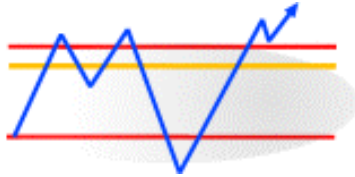
Baseline Value	Standard Deviations from Average
99	2.580
99.73	3.000
99.9	3.290
99.999	99.999

Some special features of baseline objectives:

- The time it takes to establish a baseline can vary: Baseline events are disabled until a sufficient number of metric values are processed so that a realistic prediction range can be made. If incoming metric values are fairly constant, the baseline can be established after only a few metric values are received. If, on the other hand, metric values vary significantly, more metric values may be needed to determine a realistic prediction range. The validity of a prediction is known by the baseline, and objective events cannot occur until the predictions are feasible.
- Baselines can differ for various times of the day: Since activity can vary throughout the day and on different days of the week, the baseline can be calculated to handle separate prediction ranges for each hour of each day of the week. Events may occur at a very low value Sunday morning at 4:00 AM when values are regularly low. On Monday at 9:00 AM, it may require a much higher value to cause an event if the incoming metric values are regularly much higher at that time.
- Baseline prediction ranges may differ between service groups. If the targets in one service group normally have a different value from those in a different service group, the same value in the baseline field will result in events occurring at different levels for each service group.
- A single baseline is maintained for all targets in a service group. All target values will contribute to setting the expected baseline range. Each target will be individually compared against the service group's baseline when evaluating the objectives. For this reason, targets in a service group should be expecting roughly the same metric values.

Setting Baseline and Alarm Objectives

If a Service Objective contains Alarms and Baseline settings, both settings are considered in alarm events. In order for an alarm event to occur, the probe metric value must violate the configured alarm value AND fall outside the baseline metric range. If the metric value violates the alarm setting, but falls within what is normal for the time of day, no alarm event occurs. If the metric value is outside the expected range from the baseline, but it does not exceed the alarm setting, the alarm event is suppressed.



Setting combined (Alarm and Baseline) thresholds/values should generate the fewest events since alarm events occur only when a metric value exceeds an alarm threshold at a time when it is not expected to.

Alarm Events

When an alarm threshold is violated, an alarm can occur. The purpose of this alarm would be to notify someone for purposes of correcting the situation. An alarm can include an indication of its severity as well as a message with additional information. Severity levels are chosen from the list provided and can be used by operators to prioritize their actions. The message describes the alarm and can contain information captured from the alarm.

To include data captured from an alarm into a message, add special keywords to your message. As an alarm is processed, these key words are replaced with the information indicated:

Keyword	is replaced with
<SERVICE>	The name of the Service Group to which this objective belongs
<CUSTOMER>	The customer name that owns this objective
<PROBETYPE>	The type of probe measuring the data (HTTP, ICMP, DNS, etc.)
<PROBESYS>	The name of the system where the probe was executing
<TARGET>	The objective target (URL, hostname, etc.)
<HOST>	The name of the system which was being measured
<THRESHOLD>	The objective fixed threshold value
<BASELINE>	The objective baseline percentage value
<DURATION>	The number of seconds an objective must be violated before an alarm
<VALUE>	The value of the metric in this objective at the time of the alarm
<BASELOW>	The lower limit of the baseline expected range for this hour
<BASEHIGH>	The upper limit of the baseline expected range for this hour
<RESPONSE_TIME>	The response time metric value (if this probe supplies it)
<AVAILABILITY>	The availability metric value (if this probe supplies it)
<SETUP_TIME>	The setup time metric value (if this probe supplies it)
<THRUPUT>	The throughput metric value (if this probe supplies it)

For example, the message string:

<PROBETYPE> response time from **<PROBESYS>** to **<HOST>** is
<VALUE> seconds (should be **<THRESHOLD>** or between
(**<BASELOW>** and **<BASEHIGH>**))

would appear with values inserted for the keywords which could be something like the following:

HTTP response time from **curly.myhouse.com** to
webserver1.yourhouse.com is **7** seconds (should be **< 5.0**
or between (**3.2** and **6.5**))

Emphasis is added to highlight keywords in the message string and the replacing values in the actual message.

Setting Up Service Level Agreements (SLAs)

You can configure Service Level Agreements in Internet Services.

A Service Level Agreement (SLA) is based on a contract between the IT organization and the business customers. The SLA describes the quality level of IT service by defining service level objectives for a services in terms of availability and performance (based on metrics such as response time).

SLAs are created using either the SLA Configuration wizard (accessed from the **File>Configure** menu in the Configuration Manager) or by using the SLA Configuration dialog in the Configuration Manager. You set up the SLA for a customer and a set of service groups.

The wizard steps you through creating a custom SLA based on Availability or Response Time. Once this is set up Internet Services tracks the service availability and conformance to agreed upon levels and reports on the SLA conformance.

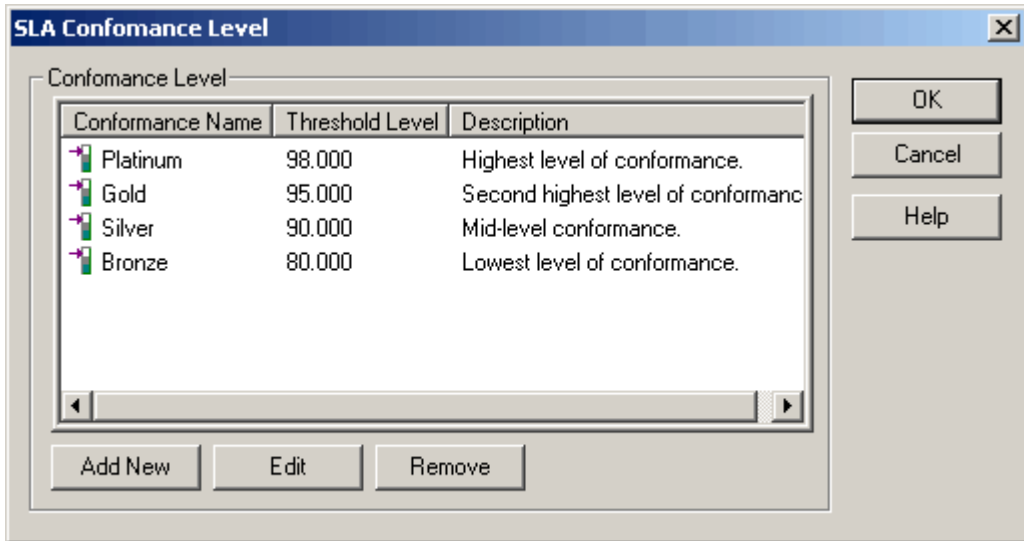
You can also use the SLA Configuration dialog to set up SLAs. Within this dialog, it is possible to set up Basic SLAs or Advanced SLAs. Basic SLAs are essentially a collection of service level objectives, which are evaluated together to form an SLA. Advanced SLAs allow for the creation of more complex logical combinations of objectives, and are evaluated differently than basic SLAs. Note that the wizard creates Basic SLAs for either Availability or Response Time.

The screenshot shows the Internet Services Configuration Manager interface. The left pane displays a tree view of the configuration hierarchy:

- Customers
 - Hewlett-Packard
 - Service Groups
 - HP Shopping Home Pag
 - Service Targets
 - hpshopping.com
 - Service Objectives
 - AVAILABILITY
 - RESPONSE_TIM
 - Probe Locations
 - Local System
 - Service Agreements
 - SLA_UpTime
 - SLA_Response
 - Status

The right pane shows the configuration details for the selected SLA. The "Customer" is Hewlett-Packard. The table below lists the service agreements and their configurations:

Service Agreement	Conformance Threshold	Conformance N.
SLA_UpTime	95.000	Gold
SLA_Response	98.000	Platinum



How an SLA is Evaluated

The basic idea of an SLA is that you combine a number of service level objectives (SLOs) into a single SLA. Then, Internet Services evaluates those SLOs to determine what percentage of them were met. The resulting value is called the SLA conformance. For example, if you have five SLOs in a SLA, and one of them results in an SLO violation but the other four met the SLO criteria, then the SLA conformance would be 80 percent.

SLAs are evaluated every hour. For basic SLAs, all of the measurements received for that hour are examined, and weighed against the number of SLO violations. The resulting SLA conformance can be viewed in the Dashboard and Reports. There is also an additional Dashboard view which allows you to examine the SLA to see which SLOs contributed most heavily to the non-conformance of that SLA.

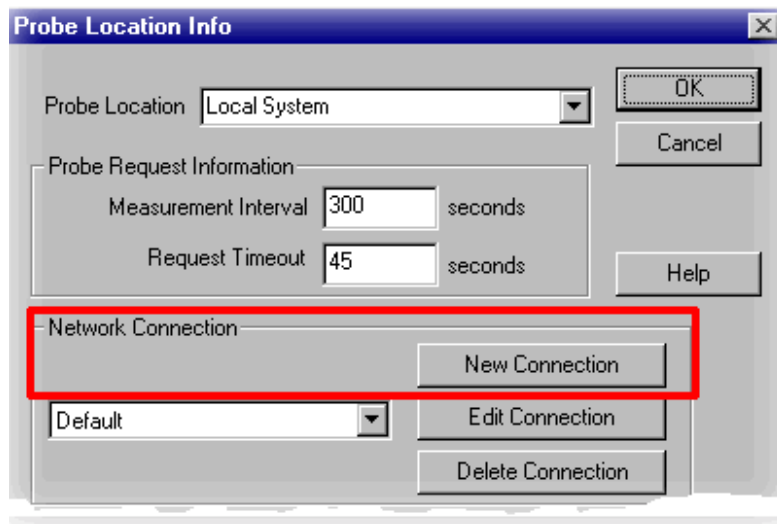
You can also set SLA conformance thresholds in the Configuration Manager (for example platinum = 98%, gold = 95%, silver = 90% and bronze = 80%). These are compared with the resulting SLA conformance at each hour. If an SLA does not meet or exceed the SLA conformance threshold, an alarm will be generated which alerts you to this SLA performance problem.

Note also that there is a fundamental difference between Availability and Response Time metrics and objectives, and hence these metrics may not be mixed when creating SLAs. You should create two separate SLAs if you wish to have both metrics evaluated. Availability is calculated as a percentage over time SLA, wherein a large number of measurements must be collected before they can be evaluated. Response Time (and the other metrics) can be evaluated individually on a per-measurement basis, and these results are collected and evaluated at the end of each hour. So if you do wish to have SLA evaluations of both Availability and Response Time metrics, just create two SLAs, one for Availability and one for Response Time.

Configuring the Network Connection (optional)

As you step through configuring a probe within the Configuration Manager, you have the option of configuring the probe's network connection. The default configuration has the probe connecting to the target through the LAN. However, if the probe will use a dial-up to connect to the service target, you can configure that connection using the Network Connection option.

In the Probe Location Info dialog (pictured below), you can press the New Connection button and configure the dialup connection.



In the dialog that follows (the Select Network Connection window) you name the connection so that you can see it referenced as a Service Group in the Internet Services data display and select Dial-Up as the Network Connection Type. Then you either set up the probe by entering dial-up information directly (phone number, user name and password) or by using a Dial-Up Networking entry (DUN entry). You set up a DUN entry outside of Internet Services. For example on Windows you use the Dial-Up Networking window accessed from **Start > Programs > Accessories**.

Using a DUN entry is preferable because it allows more extensive configuration options and you can set it up, check the connection and make changes without reconfiguring your probe.

Once you configure a Dial-Up network connection - a Dial-Up probe is created automatically (you will see the Dial-Up probe within the same Customer folder as the probe it works with).

You can run multiple probes over this single dial-up connection and login. To do this for other probes under a Customer group, you open the Probe Location window and select the dial-up connection you just configured as the network connection.

The Dial-Up probe works in the background tracking the time it takes to dial and connection to the service target. It creates a connection and after the connection has been successfully established, all probes that belong to the network connection are run in parallel over this connection.

How Probes Work

You can use the Configuration Wizard to set up the various service probes for the service targets you want to measure. It is helpful, though, to understand how probes work and what you need to consider in accepting or changing the default settings assigned to a probe. See [“Descriptions of Service Types/Probes” beginning on page 91](#) for more details on each probe type.

A probe tries to emulate someone using a service. It checks the service’s availability and measures certain service protocol characteristics. For example, the HTTP probe requests a Web page from a Web server and measures (among other protocol steps) the setup time (hostname resolution and server connect time) and total response time to process the request. A throughput calculation is performed from the number of bytes exchanged and the time to transfer them.

Measurements of protocol steps (such as host name resolution and connect time) are helpful for determining bottlenecks and troubleshooting. For example, if most of the total response time is spent in the name resolution, the problem is likely to be a problem in the name server (DNS).

How Service Target Availability is Determined

By the Probe:

A service target is available if the probe completes the full operation before the timeout you’ve specified. For example if a web page does not complete the download before the timeout of 45 seconds the availability for the interval is 0%. If only some of the page was downloaded the availability is 0%.

Note: If for some reason a probe cannot send the data back to the Internet Services Management Server, the probe puts the data into queue files until it can reach the Management Server. When this connection comes back up the data from the queue files is processed. Until then the probe reports No Probe Info from the probe system, it correctly, does not report the service as unavailable.

In a web transaction if any steps is unavailable, then the transaction as a whole is unavailable.

By the Management Server:

If there is more than one target in a service group, availability is calculated by the number of targets in the data. For instance if there are 5 targets in a service group and 4 are available and one is not for an interval, the service group has 80% availability for that interval.

If in a single service group the same target is probed from 4 different places, then availability of the service group is the sum of the availabilities of the targets divided by the number of targets. So if the target is available from 2 of 4 probe sites, then the service group is considered 50% available.

Remote Probes

Deploying remote probes allows you to place probes in locations more representative of the user experience that you want to monitor and easily compare them to probe results local to the servers providing these services. The remote probe sends its data to the central Internet Services management server, where you can centrally monitor many remote probed targets. After installing the remote probe, it automatically receives updated configuration files from the Management Server, when you make and save changes in the Configuration Manager.

Configuring and Installing Remote Probes for Windows NT/2000

You configure remote probes the same as local probes, and the Configuration Manager handles the difference as follows:

- 1 Use the Internet Services Configuration Wizard and online Help to set up the service target(s) with service objective, probe location (remote system name), and other information.
- 2 Click the **Save** toolbar button to store the probe configuration. (Internet Services creates a `config_<system_name>.dat` file and stores the file in the `\<install dir>\newconfig` directory. The `<system_name>` must match the remote system name.

Additional steps for remote probe deployment

The difference in the remote probe configuration is that you need to complete a few additional steps. You must manually transfer the installation program to the remote target probe system (you could use FTP).

- 1 Copy `\<install dir>\newconfig\remote_probe_install.exe` file to the remote probe system.
- 2 Execute `remote_probe_install.exe`. This will install the remote probe binaries.

- 3 After installation, enter the hostname of the Internet Services Management Server in the `ovisactivate` dialog. This will restart the scheduler service with the new hostname of the Management Server.

Automatic Download

If you modify the configuration for a probe after the initial installation on a remote system, the configuration files will be automatically downloaded for you.

The remote probes check every minute for new configuration at the Management Server. If new configuration is available (`\newconfig\config_<system_name>.dat`), it will be downloaded by the remote probe and activated for the next interval.

In the Configuration Manager the remote probe status screen (select the Status folder in the left pane), shows, for each probe system, the last time the probe checked for new configuration and when the last configuration was downloaded.

Please note that when the Distribution Manager (part of IIS) is restarted, the status will temporarily show "No data waiting for update" until the remote probe contacts the Distribution Manager again.

Also note: If the remote probe system has a DNS name and/or IP address that the Internet Services Management Server is not able to resolve, the automatic update of probe configuration might not work. In that case, either manually distribute the configuration file `\newconfig\config_<system_name>.dat` or create the file `\probes\nodeid.dat` with the IP address that the Management Server knows of the remote probe system.

To remove remote probe(s) from a Windows system

- 1 Delete the Service Target for the probe in the Configuration Manager and Save the change.
- 2 Stop the Scheduler server on the remote probe system by entering the following on the command line:


```
net stop "HP Internet Services"
```

(Alternatively, you can stop the scheduler by opening the Control Panel, double-clicking Services, selecting HP Internet Services, and clicking Stop).

- 3 In the Control Panel, double-click on **Add/Remove Programs**. Select "HP OpenView Internet Services Remote Probes" and click the Add/Remove button to remove.

Configuring and Installing Remote Probes on UNIX Systems

As with an Windows probe you use the Configuration Manager to set up the UNIX probe. However, remote probe deployment for UNIX systems differs from remote probe deployment for Windows systems (as explained above). The section below gives you instructions for HP-UX, Solaris, and Linux.



HTTP_TRANS probe in IE (heavyweight) mode is not available for UNIX systems, but the lightweight modes (URL and Navigation Point) are available.

Stop Internet Services (if applicable).

You only need to stop Internet Services if you are deploying to a system where probes were previously installed.

- 1 Check if the two Scheduler processes are running by entering:

```
ps -ef | grep scheduler
```
- 2 Change to the probes directory containing the Internet Services executables by entering:

```
cd /opt/OV/VPIS/probes
```
- 3 Stop Internet Services

```
./Scheduler -k
```

Install Internet Services

- 1 Log on to the UNIX system as `root`.

- 2 Insert the CD into the CD-ROM drive and mount the disk by typing:

```
/etc/mount /dev/dsk/<device_name> /cdrom
```

where the *<device_name>* is the specific name of your CD-ROM drive

- 3 Change to the directory where the installation program is located by typing:

```
cd /cdrom/SETUP/Remote_Probes_Unix
```

- 4 Type:

```
./install
```

- 5 After successful installation, enter the Internet Services management server host name and any other parameter changes in the dialog that is displayed.

Hostname. This is the Internet Services management server hostname. You are required to enter a value.

Port. This an optional entry, only needed if the web server is not running on port 80.

Proxy. Enter the proxy if communications should to through a proxy.

Secure. Set this to enable or disable secure communications. The default is **Off**.

Ignore Certificate Errors. These next three settings are the same as defined in the **Configure > Web Server Properties** dialog in the Configuration Manager. Set this to **On** if you want probe systems to ignore any errors relating to the server certificates (for example if certificate information such as server hostname or issuer cannot be resolved on the probe system). If you want to require certificate validation, then you can set Ignore Certificates to Off. Then for the probe to work you must set up the certificate for the probe to use in accessing the host and validating the certificate from the target. And you need to enter the certificate file and password as described below. See the [“Configuring Secure Communication - Probe and Management Server”](#) on page 179 for details.

Certificate Password. Enter the password that is used to protect the certificate file.

Certificate File. Enter the file name and location for the client certificates. The Base64 encoded X.509 formatted certificate must be

installed in the `/<install_dir>/probes` directory with the specified name (**clientcert**). All probe locations share the same certificate file name and password.

When you've made necessary changes, select number **10** to Save and Exit. The scheduler is automatically started.

Start Internet Services

This normally happens automatically, but manual procedures are provided here for your information.

- 1 On the UNIX system, change to the directory containing Internet Services executables by entering:

```
cd /opt/OV/VPIS/probes
```

- 2 Start Internet Services by entering:

```
./Scheduler
```

- 3 Verify that two Scheduler processes are running by entering:

```
ps -ef | grep Scheduler
```



In the future if you need to stop Internet Services on the UNIX system, use the command: `./Scheduler -k`.

Automatic Download

If you modify the configuration for a probe after the initial installation on a remote system, the configuration files will be automatically downloaded for you.

The remote probes check every minute for new configuration at the Management Server. If new configuration is available (`\newconfig\config_<system_name>.dat`), it will be downloaded by the remote probe and activated for the next interval.

In the Configuration Manager the remote probe status screen (select the Status folder in the left pane), shows, for each probe system, the last time the probe checked for new configuration and when the last configuration was downloaded.

Please note that when the Distribution Manager (part of IIS) is restarted, the status will temporarily show "No data waiting for update" until the remote probe contacts the Distribution Manager again.

Also note: If the remote probe system has a DNS name and/or IP address that the Internet Services Management Server is not able to resolve, the automatic update of probe configuration might not work. In that case, either manually distribute the configuration file `\newconfig\config_<system_name>.dat` or create the file `\probes\nodeid.dat` with the IP address that the Management Server knows of the remote probe system.

To remove probe(s) from UNIX Systems

- 1 Delete the Service Target for the probe in the Configuration Manager and Save the change.
- 2 Log on as root on the UNIX system.
- 3 Change to the probes directory by entering:

```
cd /opt/OV/VPIS/probes
```
- 4 Stop Internet Services (if necessary) above.
- 5 Start the removal script by entering:

```
./remove.vpis
```

Limiting Access to the Dashboard Data Display using Restricted Views

After you have configured customers and service groups, you may optionally decide that you want to restrict access to the Dashboard Web page data display. You can easily do this in the Configuration Manager by first enabling **Restricted Views**, then selecting each customer and assigning the customer a password. This feature can be found within the Configuration Manager main window under **File>Configure>Restricted Views**. When you enable this feature, anyone logging in must enter a user name/password (which have been defined in the Configuration Manager) to see the Dashboard's Snapshot page.

You can also create a superuser account that has access to all customers and reports by creating a user named "All Customers" and assigning it a password. The superuser account then allows anyone using it access to the Dashboard data display that shows data for all customers.



The Dashboard data display Web pages are stored by default to be accessible from

`http://<Web_server_system>/hpov_reports/iops.htm`.

Customers accessing the display from other systems will need to enter this URL in their browser. If you have enabled Restricted Views, the customer is required to enter a password within the Internet Services Dashboard Web page that appears.

Automating Configuration of Large Numbers of Service Targets

If you have large numbers of services to target and these targets are already available in some machine-readable form, Internet Services includes a way to configure those service targets as a batch file. To configure multiple service targets, you can write a program or script to reformat the targets and feed them into a batch configuration interface. You might also want to save configurations you created with the Configuration Manager and make those configurations available to another installation of Internet Services.

This section discusses a batch configuration interface that can serve these purposes. Not everyone will need to use the batch configuration interface. It requires programmatic or script-generated input compared with the Configuration Manager user input and does not tolerate errors as well. Still, it provides a way to add a large amount of information into the Internet Services configuration in an automated manner.

Note: the easiest way to understand the syntax for the configuration file is to use the Configuration Manager to create a single configured service target of the type you are interested in and then look at the resulting XML formatted configuration file. See [“Create a Sample Batch Configuration File” on page 87](#) for details.

How Batch Configuration Works

The batch configuration facility uses a simple character file containing XML formatted text. XML is an emerging industry standard format for representing data in text files and is being driven by Internet extensions to HTML. This discussion does not cover XML syntax in general but rather covers how it is used in configuring multiple service targets (batch configurations) for Internet Services.

The **IOPSLoad** program supports the batch configuration facility. This program can be found in the `c:\<install dir>\bin\` directory on your Internet Services management server. The program can:

- **Check** the syntax of a configuration file. Report any errors but do not affect the Internet Services configuration.
- **Load** the information from a configuration file into the Internet Services product.
- **Save** the information currently in the Internet Services product into a configuration file. This file is suitable for subsequent load operations.
- **Remove** information from the Internet Services product that matches information in the configuration file.
- **Info**, shows information on probe systems and probe target count.

To run the IOPSLoad program, you open a Command Prompt window and enter syntax as follows:

```
IOPSLoad [-check] [-quiet] configfilename
IOPSLoad -load [-quiet] configfilename
IOPSLoad -save [-quiet] configfilename
IOPSLoad -remove [-quiet] configfilename
IOPSLoad -info
```

The **-quiet** parameter directs the operation to execute with no output to the console window. If you do not specify **-quiet**, the program output is written to a console window. In either case, you can find a summary of the operation in the `status.iops` file in the `c:\<install dir>\data` directory.

The **configfilename** is the name of the character file containing the XML format configuration information. An entry for this parameter is required; no default is supplied.

The remaining parameters select the operation to be performed. **-check**, **-load**, **-save**, **-remove**, and **-info** will check the syntax of a configuration file, load information from a configuration file, save information into a configuration file, remove data which matches a configuration file and show information on probe systems respectively. Only one of these parameters should be provided. If none is provided then **-check** is assumed.

Syntax for the Configuration File (general)

The configuration file is a simple text file containing ASCII character data (not UNICODE data) that is terminated by a line feed (newline) character. Optionally a carriage return character may also be included at the end of each line. The line spacing is not critical except that a line split cannot occur in the middle of a token.

Tokens are reserved words that identify configuration information. These tokens are described in the section [“Tokens or Elements in the Configuration File” on page 76](#) and must be entered exactly as shown. Case is important, so be sure to match upper case and lower case as shown in the tokens. Generally, XML syntax provides for a start token, intermediate attribute tokens, and an end token.

For example: `<LOCATION id="Denver"></LOCATION>`

In this example:

<code>LOCATION</code>	is the start token
<code>id=</code>	is an attribute token
<code>"Denver"</code>	is data that is associated with the name attribute. Note that the data is enclosed in double quotes.
<code></LOCATION ></code>	is the end token.

Please note the placement **angle brackets** "<" and ">". Their placement is critical to the proper interpretation of the XML codes. A start token must match a corresponding end token. `<LOCATION>` with no corresponding `</LOCATION>` will produce an error.

For advanced usage: It is often possible to combine the start and end tokens using a special syntax. The previous example could also be represented as:

```
< LOCATION id="Denver"/>
```

Note the slash preceding the closing angle bracket. If you are just getting started in XML, you might want to avoid this construct until you are familiar with using start and end tokens.

Certain characters are used in interpreting the XML syntax and so are not allowed in the data fields. If one of these characters is needed then a special string must be substituted in its place. The original character will be re- instated prior to the data being used.

To render this character Use this string

&	&
<	<
>	>
"	"

Structure of the Configuration File

The first two lines in the configuration file identify the file as XML syntax and specify its options. If generating your own configuration file, copy these lines precisely.

```
<?xml version="1.0" encoding="ASCII" standalone="yes" ?>
<!-- @version: -->
```

The rest of the file consists of nested token pairs. The outermost token pair specifies the configuration file contents and must be:

```
<CUSTOMERLIST>
</CUSTOMERLIST>
```

All configuration information must fall after the `<CUSTOMERLIST>` token and before the `</CUSTOMERLIST>` token. Tokens for the Configuration file must follow a specific nesting pattern as shown below:

```
<CUSTOMERLIST>
  <CUSTOMER>
    <SERVICE>
      <TARGET></TARGET>
      <OBJECTIVE></OBJECTIVE>
      <LOCATION></LOCATION>
    </SERVICE>
    <SLA></SLA>
  </CUSTOMER>
  <CONFORMANCE_LEVEL></CONFORMANCE_LEVEL>
  <NETWORK></NETWORK>
  <DOWNTIME></DOWNTIME>
</CUSTOMERLIST>
```

This indicates that:

A CUSTOMERLIST consists of zero or more CUSTOMERS.

(You may start another `<CUSTOMER>` immediately following the end of the previous one `</CUSTOMER>`.)

A CUSTOMER consists of zero or more SERVICES. (also referred to as a service group)

And within a CUSTOMER you can have the SLA.

A **SERVICE** consists of zero or more **TARGETS**, **OBJECTIVES** and **LOCATIONS**.

Within a **SERVICE**, **TARGETS**, **OBJECTIVES** and **LOCATIONS** may occur in any order and be repeated as many times as necessary.

A **SERVICE** does not have to have all three components (**TARGET**, **OBJECTIVE** and **LOCATION**).

Also within a **CUSTOMERLIST**, after **CUSTOMER**, you can have **CONFORMANCE_LEVEL**, **NETWORK**, and **DOWNTIME** in any order and they may be repeated as necessary.

Tokens or Elements in the Configuration File

This section covers the batch configuration file syntax details. Please consult the preceding sections for further information on how these configuration elements should be used.

<CUSTOMERLIST>

No attributes.

<CUSTOMER

```
name="customername">
```

- Attribute "name=" specifies the customer name and cannot be omitted.

<SERVICE

```
id="servicegroupname"  
probe="probename">
```

- Attribute "**id**=" specifies the name of the service group and can not be omitted.
- Attribute "**probe**=" specifies the name of the service probe that will measure targets in this service group. This name must match one of the probe names that are known to the Internet Services product.

<TARGET

(...) >Attributes vary depending on the type of probe for this service target.
For probes not listed, see the individual probe documentation:

Table 1 Probe attributes

PROBE	Attribute	Description
DHCP	host= port= clientPort= acceptOffer= pattern= patternConfig=	system name of DHCP server TCP/IP port default=67 client port to use whether to accept offered address pattern to find pattern configuration parameters
DIAL	phoneNumber= username= password= phoneEntryName= stayConnected=	phone number to dial user name password DUN entry file name stay connected (1) after dial or not (0)
DNS	host= port= query= retries=	system name of Domain Name Server TCP/IP port default=53 system name to be resolved by DNS number of retries
FTP	host= port= file= username= password= mode=	system name of FTP Server TCP/IP port default=21 name of file to transfer user name password Automatic, Passive, or Active

Table 1 Probe attributes (Continued)

PROBE	Attribute	Description
HTTP	host= port= urlfile= username= password= options pattern= patternConfig= embedded= proxyusername= proxypassword= retry= waittime=	system name of Web Server TCP/IP port default=80 reference string for the web page user name password Keep Alive and No Cache pattern to find pattern configuration parameters load images and frames? user name for proxy server password for proxy server number of times to retry request time to wait between retries
HTTPS	host= port= urlfile= username= password= pattern= patternConfig= embedded= ignore= proxyusername= proxypassword= clientcertfile= clientcertpassword= retry= waittime=	system name of Secure Web Server TCP/IP port default=443 reference string for the secure web page user name password pattern to find pattern configuration parameters whether to load images and frames ignore flag (0 or 1) user name for proxy server password for proxy server client certificate file used in authentication client certificate password number of times to retry request time to wait between retries
HTTP_TRANS	transFile= embedded= ignore=	name of transaction file (httptrans.dat) load images and frames? ignore flag (0 or 1)
ICMP	host= packetsize= requests=	system or TCP/IP address to be polled bytes to be sent number of requests

Table 1 Probe attributes (Continued)

PROBE	Attribute	Description
IMAP4	host= port= username= password=	system name of IMAP4 mail server TCP/IP port default=143 user name password
LDAP	host= port= distinguishedName= filter= scope= pattern= patternConfig=	system name of LDAP server TCP/IP port default=389 LDAP distinguished name parameter filter LDAP_SCOPE_SUBTREE, LDAP_SCOPE_ONELEVEL, or LDAP_SCOPE_BASE pattern to find pattern configuration parameters
NNTP	host= port= group= username= password= maxBytes=	system name of NNTP news server TCP/IP port default=119 news group name user name (if server requires authentication) password (if server requires authentication) Maximum number of bytes downloaded
NTP	host= port=	system name of NTP server TCP/IP port default=123
POP3	host= port= username= password=	system name of POP3 mail server TCP/IP port default=110 user name password
RADIUS	host= port= username= password= protocol= sharedSecret= NASPort= retries	system of remote authentication server TCP/IP port default=1645 user name password PAP or CHAP shared secret between user and RADIUS server Network Access Server port number of times to retry request

Table 1 Probe attributes (Continued)

PROBE	Attribute	Description
SMTP	host= port= recipient= sender= dataSize=	system name of SMTP mail server TCP/IP port default=25 mail user to whom the mail will be sent mail user that is sending the mail number of bytes in the message
Streaming Media	host= port= file= protocol= PlayType= PlayTime=	system name of server Streaming media port default=80 Media file to be played on server (HTTP, RTSP) Protocol to be used for playing the media clip Format of media file Time (in seconds) the clip is to be played
TCP	host= port=	system name of server TCP/IP port to access
WAP	host= port= url= pattern= patternConfig=	system name of WAP server TCP/IP port default=9200 reference string for the Web page pattern to find pattern configuration parameters

Table 1 Probe attributes (Continued)

PROBE	Attribute	Description
X_SLAM_DNS	port=	port number of the Cisco SMS port
X_SLAM_HTTP	host=	Cisco SMS server name
X_SLAM_ICMP	SLC=	SLC Handle from Cisco SLM server
X_SLAM_UDP	SLA=	SLA Handle from Cisco SLM server
X_SLAM_TCP	Username=	user name
X_SLAM_VoIP	Password=	password
	SLCName=	if SLC handle is not available then the exact name can be used
	SLAName=	if SLA handle is not available then the exact name can be used
	serviceid=	combination of service id, target id, and probe id separated by a semi-colon, for example 41;44;42
	sourceDevice=	NOTE: Use sourceDevice and targetDevice when specifying a device pair combination. exact SLM source device from RME Inventory Database
	targetDevice=	exact SLM target device

<OBJECTIVE

```

objectiveid="id"
metric="metricname"
condition="comparison"
threshold="fixedthreshold"
baseline="baselinepercent"
duration="seconds"
starttime="hh:mm"
stoptime="hh:mm"
days="MTWTFSS"
message="textmessage"
severity="severitycode">

```

- Attribute **objectiveid**= specifies a unique numeric id representing this specific objective.

- Attribute "**metric**=" specifies the name of the metric that will be used on this objective. The metric name must match a metric that is provided by the service probe for this service.
- Attribute "**condition**=" specifies the comparison of the metric value to the threshold values. The following conditions are allowed:

Table 2 Comparison conditions allowed

Symbol	in Config file	Description
<	<	Less Than
>	>	Greater Than
<=	<=	Less Than or Equal to
>=	>=	Greater Than or Equal to
=	=	Equal to
!=	!=	Not Equal to

- Attribute "**threshold**=" specifies that a fixed threshold will be used for the comparison. The <fixedthreshold> is a number and may include decimals.
- Attribute "**baseline**=" specifies that a baseline comparison will be used, based on the expected normal values for the metric. The <baselinepercent> is a number between 0 and 100 and may include decimals.
- Attribute "**duration**=" specifies the number of seconds that an objective must be true before triggering an alarm. The value is an integer number and is most useful when it is a multiple of the probe sampling interval.
- Attribute "**starttime**=" is used together with "**stoptime**". If both these attributes are supplied then no alarms will be triggered unless they fall between the start and stop times. The values for both these attributes are hour (0-24) a colon ":" and minute (0-59). For example: 08:00 is eight in the morning, 17:30 is five thirty in the evening.
- Attribute "**days**=" specifies the days of the week that alarms can be triggered for this objective. The value consists of seven characters, each representing a day of the week. If the character is blank, no alarms can be triggered. If the character is not blank, alarms can be triggered. The character positions beginning with Monday, then Tuesday, ... and end with

Sunday. A value which allows alarms only Monday, Wednesday and Friday would be "M W F " or "X X X ".

- Attribute "**message=**" specifies the text for the message that is sent along with any alarm that is generated for this objective. The message may contain special codes that substitute data from the measured data. Remember that all data fields must contain substitutions for the special formatting characters <, >, &, ". See the table above.

Table 3 Symbol Substitutes

Symbol	Substitutes for
<SERVICE	Service Group name
<CUSTOMER>	Customer name
<PROBETYPE>	Type of Service Probe (HTTP, DNS, etc.)
<PROBESYS>	Location of Probe that took the measurement
<TARGET>	Target (depending on probe type)
<HOST>	System name where the target resides
<THRESHOLD>	Fixed threshold for the objective
<BASELINE>	Baseline percent for the objective
<DURATION>	Objective duration in seconds
<VALUE>	Latest metric value
<BASELOW>	Expected low value based on baseline information
<BASEHIGH>	Expected high value based on baseline information
<RESPONSE_TIME>	Response Time value (if available from the probe)
<AVAILABILITY>	Service Availability (if available from the probe)
<SETUP_TIME>	Setup Time value (if available from the probe)

Table 3 Symbol Substitutes (Continued)

Symbol	Substitutes for
<THRUPUT>	Throughput value (if available from the probe)
<METRIC1>	Probe Specific value (if available from the probe)
<METRIC2>	Probe Specific value (if available from the probe)
<METRIC3>	Probe Specific value (if available from the probe)
<METRIC4>	Probe Specific value (if available from the probe)
<METRIC5>	Probe Specific value (if available from the probe)
<METRIC6>	Probe Specific value (if available from the probe)
<METRIC7>	Probe Specific value (if available from the probe)
<METRIC8>	Probe Specific value (if available from the probe)

- Attribute "**severity**=" specifies the alarm severity and must be chosen from the following list:

Normal	Green
Warning	Cyan
Minor	Yellow
Major ()	Orange
Critical ()	Red
Service Level	

<LOCATION

```
id="locationname"
interval="seconds"
timeout="seconds">
```

- Attribute "**id**=" specifies the name of the system where the probe agent will reside. Specifying `id="Local System"` will indicate that the probe agent resides on the same system as the Internet Services management Server.
- Attribute "**interval**=" specifies the number of seconds between measurements.
- Attribute "**timeout**=" specifies the number of seconds before a measurement is "timed out" and recorded as unavailable.

<SLA

```
id="slaname"
type="slatype"
equation="slaequation"
threshold="thresholdvalue"
conformance_name="conformancename"
```

- Attribute "**id**=" specifies the name of the Service Level Agreement (SLA)
- Attribute "**type**=" specifies the type: 0 = basic, 1 = advanced.
- Attribute "**equation**=" specifies the SLA equation itself.
- Attribute "**threshold**=" specifies the SLA conformance threshold value.
- Attribute "**conformance_name**=" specifies the name of the conformance threshold (for example: platinum, gold, silver, bronze).

<CONFORMANCE_LEVEL

```
name="conformancelevelname"
description="description"
threshold="thresholdvalue"
```

- Attribute "**name**=" specifies the name of the conformance level (for example: platinum, gold, silver, bronze).
- Attribute "**description**=" is a text description.

- Attribute "**threshold**=" is the numeric threshold value associated with this conformance level. You would set up separate conformance level statements if you have more than one threshold value.

<NETWORK

```
name="networkname"  
customer="customer name"  
service="service name"  
type="network type"  
executable="probe executable name"  
phonenumber="dialphone"  
user="DIALuser"  
password="DIALpassword"  
dunentry="dial-up Net Entry"  
timeout="seconds"  
concurrency="num concurrent probes"
```

- Attribute "**name**=" specifies the name of the Network
- Attribute "**customer**=" specifies the Customer associated with the Network. If there is no specific Customer for this Network, it is -9999.
- Attribute "**service**=" specifies the name of the Service Group associated with this Network. If there is no specific Service Group for this Network, this value is -9999.
- Attribute "**type**=" specifies the Type of this Network Entry. Valid values are Default, LAN, DIAL.
- Attribute "**executable**=" specifies the executable to be launched to invoke this Network. For normal purposes, this value is empty, since no special executable is required to access the network. However, for dial-up connections this value will be probeDial.exe.
- Attribute "**phonenumber**=" specifies the phone number to be used for dial-up connections.
- Attribute "**user**=" specifies the user name for this dial-up connection.
- Attribute "**password**=" specifies the password to be used for this dial-up connection.
- Attribute "**dunentry**=" specifies the user-defined DUN (dial-up network) entry to be used for this dial-up connection.

- Attribute "**timeout**=" specifies the elapsed time after which probes will be terminated for this network.
- Attribute "**concurrency**=" specifies the number of concurrent probes that will be executing at one time for this Network.

<DOWNTIME

```
description="description"
downtimestring="downtime"
applied="appliedflag"
```

- Attribute "**description**=" is the text description for this downtime.
- Attribute "**downtimestring**=" specifies a string representing all the settings of this downtime including start, stop, recurrence.
- Attribute "**applied**=" specifies TRUE if this downtime is applied, FALSE if this downtime is not applied.

Create a Sample Batch Configuration File

You can create your own sample XML configuration file, to examine and perhaps use as a basis for the real XML configuration file that you will complete later. You can do this by performing the following steps:

- 1 Open the **Configuration Manager**, and create a configuration based on your environment, including a customer, one or more service groups, and the associated service targets, objectives, and probe locations.
- 2 Open a Command Prompt window, change to the subdirectory where you want to save your XML configuration file, and enter: `IOPSLoad -save myconfig.txt`

At this point, you have an XML configuration file, based on the information you entered through the Configuration Manager. This file is named `myconfig.txt`, and is located in the subdirectory where you ran the IOPSLoad program. You can examine and modify the configuration file using the text editor of your choice.

Later if you modify the configuration file and you want those changes updated in Internet Services, open a Command Prompt window and enter: `IOPSLoad -load myconfig.txt`

Example Batch Configuration File

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<!-- @version: -->

<CUSTOMERLIST>

  <CUSTOMER name="Hewlett-Packard">

    <SERVICE id="HP Shopping Home Page" probe="HTTP">

      <TARGET  host="hpshopping.com"
        port="80"
        urlfile="/"
        password="##"
        embedded="1"
        proxypassword="##"

      > </TARGET>

      <OBJECTIVE objectiveid="1"
        metric="AVAILABILITY"
        condition="&gt;"
        servicelevel="90.000"
        warning="90.000"
        baseline="80.000"
        duration="600"
        starttime="00:00"
        stoptime="00:00"
        days="MTWTFSS"
        message="HTTP Service for &lt;TARGET&gt; is unavailable"

      > </OBJECTIVE>

      <OBJECTIVE objectiveid="2"
        metric="RESPONSE_TIME"
        condition="&lt;"
        servicelevel="3.000"
        warning="-9123000000000000000.000"
        baseline="0.000"
        duration="600"


```



```

        starttime="00:00"
        stoptime="00:00"
        days="MTWTFSS"
        message="HTTP Service RESPONSE_TIME is slow
(&lt;VALUE&gt; vs &lt;THRESHOLD&gt;) on &lt;TARGET&gt;";
    > </OBJECTIVE>

    <LOCATION id="Local System"
        interval="300"
        timeout="45"
        network="Default"
        httpproxy="web-proxy.rose.hp.com:8088"

    > </LOCATION>

</SERVICE>

<SLA id="SLA_Name"
    type="0"
    equation="([1])"
    threshold="95.000"
    conformance_name="Gold">

    <SLO objectiveid="1"> </SLO>

</SLA>

<SLA id="SLA_Name2"
    type="0"
    equation="([2])"
    threshold="98.000"
    conformance_name="Platinum">

    <SLO objectiveid="2"> </SLO>

</SLA>

</CUSTOMER>

<CONFORMANCE_LEVEL name="Bronze"
    description="Lowest level of conformance."
    threshold="80.000"

```

```
> </CONFORMANCE_LEVEL>

<CONFORMANCE_LEVEL name="Gold"
    description="Second highest level of conformance."
    threshold="95.000"

> </CONFORMANCE_LEVEL>

<CONFORMANCE_LEVEL name="Platinum"
    description="Highest level of conformance."
    threshold="98.000"

> </CONFORMANCE_LEVEL>

<CONFORMANCE_LEVEL name="Silver"
    description="Mid-level conformance."
    threshold="90.000"

> </CONFORMANCE_LEVEL>

<DOWNTIME description="SchedDown"

downtimestring="1011118202,1011118202,0;1;1011118202;0,1,101111821
5,1,0,0;0,1011118215,0,0,0,0,0,0;0,0,0,0,0"
    applied="FALSE"

> </DOWNTIME>

<NETWORK name="Default" customer="" service=""
    type="LAN"
    executable=""
    phoneNumber=""
    user=""
    password=""
    DUNEntry=""
    timeout="300"
    concurrency="32"

> </NETWORK>

</CUSTOMERLIST>
```

Descriptions of Service Types/Probes

Every service group that you configure is made up of a particular service type. When you set up service targets and objectives, it is helpful to understand how each service type works.



Refer to [“List of Metrics by Probe Type” on page 121](#) for a complete list of the metrics collected for each probe type and a definition of each metric.

Internet Services Probes on Windows NT/2000 and UNIX*

Systems: Internet Services allows you to configure and monitor all service types listed below on Windows NT systems. On UNIX systems you can use any probe except for the HTTP_TRANS probe in Internet Explorer heavyweight mode and the Streaming Media probe. Click on any item to jump to the section for a description of that particular service type.

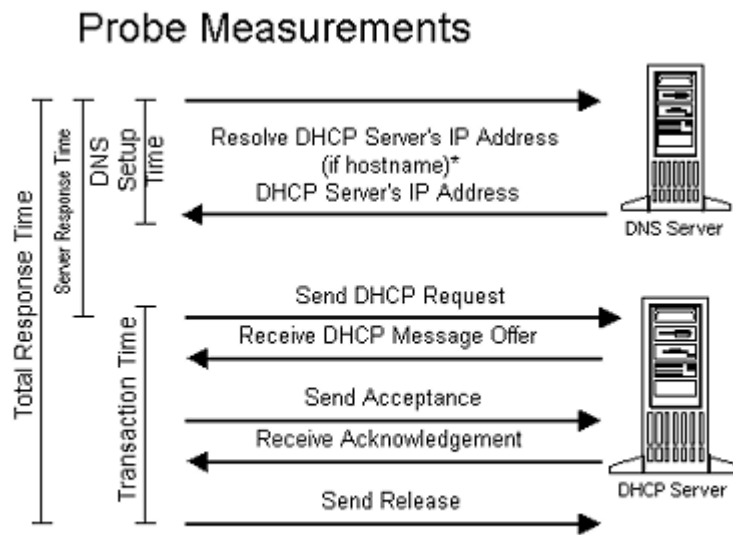
- “DHCP (Dynamic Host Configuration Protocol)”
- “Dial-Up Networking Service”
- “DNS (Domain Name System)”
- “FTP (File Transfer Protocol)”
- “HTTP (Hypertext Transfer Protocol)”
- “HTTPS (Hypertext Transfer Protocol Secure)”
- “HTTP_TRANS (Web Transaction probe)”

- “ICMP (Internet Control Message Protocol—Ping)”
- “IMAP4 (Internet Message Access Protocol)”
- “LDAP (Lightweight Directory Access Protocol)”
- “NNTP (Network News Transfer Protocol)”
- “NTP (Network Time Protocol)”
- “POP3 (Post Office Protocol 3)”
- “RADIUS (Remote Authentication Dial In User Service)”
- “SMTP (Simple Mail Transfer Protocol)”
- “Streaming Media”
- “TCP (Transmission Control Protocol)”
- “WAP (Wireless Application Protocol)”
- “X_SLAM (CiscoWorks Integration)”
- “Creating your Own Custom Probes”

DHCP (Dynamic Host Configuration Protocol)

The DHCP probe measures the time it takes the DHCP server to return an IP address. The probe sends a request to a specific host (if supplied) or broadcasts the request to the network. The probe then waits for an offer of an IP address from a DHCP server. More than one server may respond with offers. After accepting the first offered IP address, the probe then waits for acknowledgement from the server. After receiving acknowledgement, the probe releases the IP address.

The following diagram shows the protocol steps:



*DNS setup time is measured only if a host name is provided

To avoid tying up IP addresses, the probe does not, by default, actually reserve offered IP addresses. Although some DHCP servers reserve offered leases for up to two minutes after making the offer, they are free to give them away to other requesters as needed. If the probe's offer is accepted by the DNS server, the probe then officially requests the offered

IP address from the server and waits for the DHCP server to acknowledge the request. If the server acknowledges the request, the probe then immediately releases the offered IP address back to the server.

Dial-Up Networking Service

The Dial-Up (DIAL) probe establishes a point-to-point-protocol (ppp) connection over a modem to a remote server. It works in the background, measuring the amount of time that it took to dial, handshake, and complete the ppp connection protocol. Although this probe most often works in conjunction with other probes, you may configure it separately if you would like to create a special service group.



If you use the Dial Up probe, or configure other probes to run over a Dial Up Network Connection, RAS (Remote Access Server) and a minimum of one phonebook entry must be configured on the probe system.

Once a Dial-Up probe has been created, it can be used by any number of other probes making dial-up connections to access their service targets. To configure other probes to use the dial-up probe you go to the Probe Location windows in the Configuration Manager and select the Dial-Up Network Connection. If a Dial-Up probe doesn't already exist, you can create one by selecting the New Connection button in the Probe Location windows. After you set up the dial-up network connection a Dial-Up probe is automatically created (you will see it in the same customer folder as the probe it works with).

This background dial-up probe also has a service group automatically created for it as well. You will see it within the same customer folder under which you configured its partner service. The DIALUP service group allows you to set service level objectives and/or thresholds for triggering alarms in other OpenView products.

DNS (Domain Name System)

The DNS probe measures the total response time to resolve a hostname or IP address. It uses the UDP protocol to talk to the DNS server. The DNS server is considered available when the DNS probe gets an answer back. Please note that the answer might indicate that the hostname or IP-address could not be resolved but the DNS server is still considered to be available because it was processing the request and returning a valid reply.

Parameters

In the Configuration Manager, you can right-click the Service Group you have created for DNS and select **New Service Target**. In the dialog that appears, you specify the hostname or IP address. The retry field specifies the number of times the probe resends a request. The DNS probe adjusts the retries so that they will fit within the Request Timeout value (20 seconds or as specified in the Probe Location window for the DNS probe).

Retries is calculated as follows: The default timeout between requests is 5 seconds, which is the standard DNS resolver library timeout setting. The probe sends a request and waits for 5 seconds. If the request isn't completed, the timeout between requests is doubled to 10 seconds and so on. But the total time cannot exceed the Request Timeout value.

For example, if the Request Timeout is 20 seconds, the DNS probe will do a maximum of 2 retries (5 seconds + 10 seconds = 15 seconds). It could not do three retries in 20 seconds (5 + 10 + 20 = 35 seconds) since this is longer than the Request Timeout of 20 seconds.



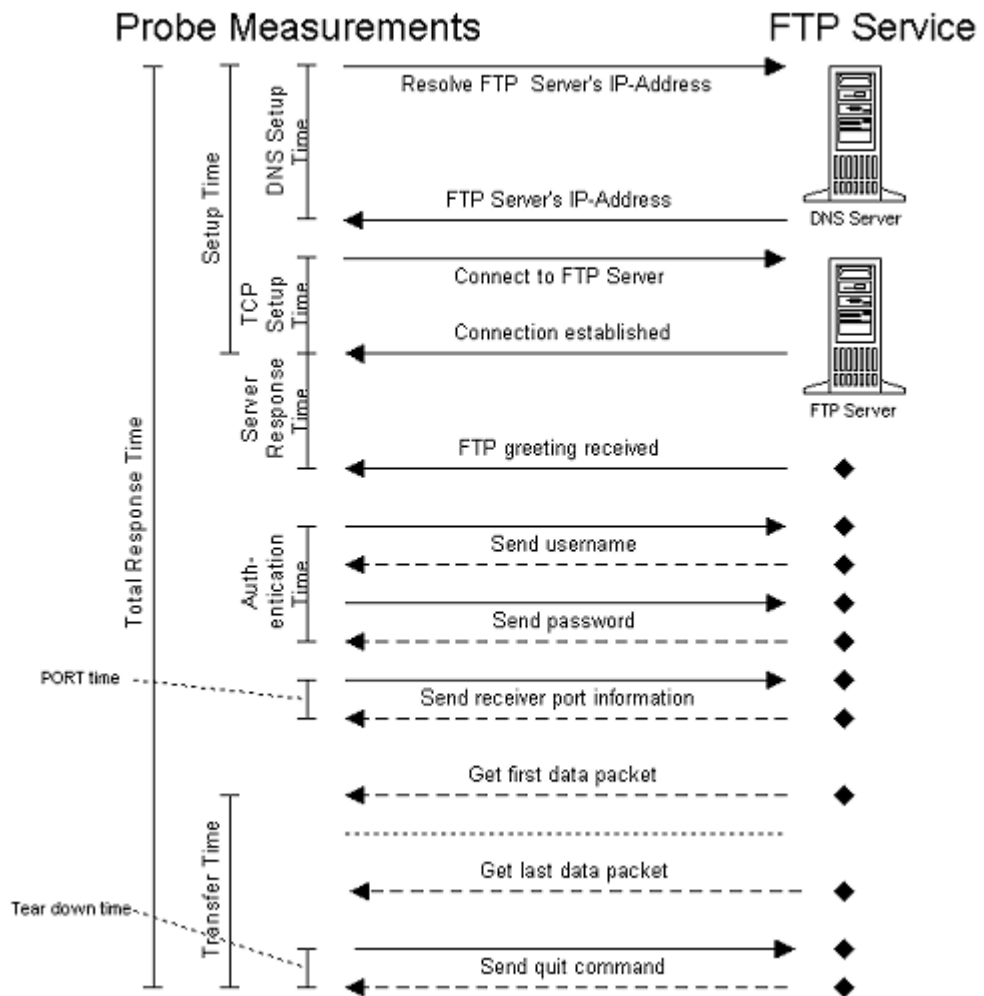
The DNS host system must be configured to resolve its own name and IP address in order for the DNS service target probe to work correctly.

FTP (File Transfer Protocol)

The FTP probe performs a simple file retrieval or directory listing. It authenticates itself with the specified username and password and downloads the specified file.

The FTP protocol uses two connections, one to exchange command information and one to download the data. A new socket is opened by the probe for the data connection and the socket is sent to the FTP server through the command connection (PORT protocol step).

The following diagram describes the various protocol steps and measurements that are taken:



Parameters

Username and password are required for authentication. The default username is `anonymous` and password is `VPIS@VPIS`. Note, these defaults do not work if anonymous FTP is disabled.

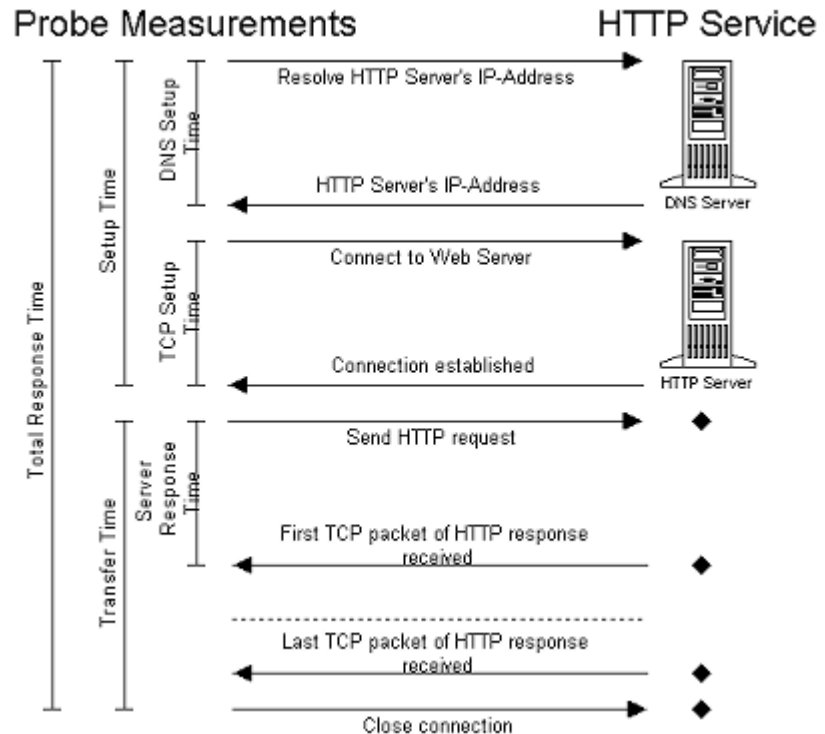
If no remote file is specified, the probe retrieves a directory listing (FTP DIR command).

HTTP (Hypertext Transfer Protocol)

Web Page Setup/Loading Time

The HTTP probe emulates a typical HTTP request. It supports proxies, basic authentication and download of forms and images. Additionally, a search pattern can be configured which is applied to the returned HTML output of the web page.

The following diagram shows the emulated protocol steps and its measurements:



Parameters

By default, the HTTP probe downloads the specified document with embedded images and frames.

The check box **Connection Keep-Alive** can be checked if you want the connection to stay open after each request within a page (HTTP 1.0 keep alive). By default this is set to off. Note this may not be available on all servers.

The check box **No Cache (Proxy)** can be checked if you want the probe to always go to the service target instead of using cached pages.

To use proxies: The probe can relay the request to a proxy if specified. In the Probe Location dialog you enter the proxy information in the Proxy Address and Port fields.

To download targeted web pages protected by authentication: You must specify web server username and password.

To use pattern matching to check successful or unsuccessful Web page downloads: A pattern can be applied to the returned HTML output to check whether or not the probe returned the desired Web page or returned a Web page with an error message. You can insert text that is present in the page preceded by a plus(+) sign as the pattern to match. If the target successfully matches the pattern, the page is considered available; if the pattern does not match, the target is marked unavailable. You could, on the other hand, include error text as the pattern to match preceded by a minus(-) sign as the pattern to match for showing that the Web page is not available. The pattern follows the standard WWW search engine format, where a "+" in front of a word means that the word has to be matched, and a "-" means that the word must not occur. Consider following examples:-"connect to database"

- | | |
|----------------------------|---|
| +"login successful" -error | For the target to be available, the word "login successful" must be contained in the HTML output but no the word "error". |
| -"connect to database" | For the target to be available, the word "connect to database" must not be contained in the HTML output. |

The default operator for word concatenation is AND. This can be changed by the pattern configuration where it can be set to OR in the HTTP Web Pages Information dialog box, where you add the service target. A word compare is case sensitive. This can be changed by the pattern configuration option to be case insensitive.

To simulate user input with the HTTP probe, the standard HTTP parameter passing mechanism must be used where form input parameters are appended to the URL. For example, if the form tags for two HTML text fields are "username" and "password", the document needs to be entered the following way: /
login.PL?username=me&password=secret

HTTPS (Hypertext Transfer Protocol Secure)

The service probe works the same as HTTP (see above).

Parameters

Depending on the installed Windows NT encryption strength (export or US domestic), the probe can access SSL secured HTTP servers. Please note, that the probe might fail if it runs on a system with export encryption strength and tries to access an HTTPS server secured with US domestic encryption strength.

The check box **Ignore Certificates** can be checked if certificate information such as the hostname or issuer cannot be resolved on the probe system.

If you don't set Ignore Certificates, then you need to set up the Trusted Root Certificate for the probe to use in accessing the host and validating the Certificate from the target. The HTTPS probe uses the file trusted.txt located in the probes directory to do the validation. This file contains exported certificates in Base64 encoded X.509 (.CER) format.

In order for the probe to be able to validate the certificate sent by the target, you need to first be sure the Certificate from the target server is installed on the Internet Services management server and then you need to export the Certificate to a format usable by the trusted.txt file and the probe.

Exporting a Root Certificate in Internet Explorer 5.5

- 1 From the Menu Tools->Internet Options...
- 2 Select the Content Tab, In the Certificates Section, Select Certificates...
- 3 Select the Trusted Root Certification Authorities Tab, and Select the Certificate for export
- 4 Select Export, which bring up the Certificate Manager Export Wizard, and Select Next
- 5 Select the Format Base64 encoded X.509 (.CER) for export, and Select Next
- 6 Choose a file name c:\<my_cert>.cer (note: the .cer extension will be added automatically), Select Next
- 7 Select Finish, The message "The export was completed successfully." should be displayed, and Select OK
- 8 Open the file c:\my_cert.cer with Notepad, and copy the entire contents of the file (from -----BEGIN CERTIFICATE----- to -----END CERTIFICATE-----) into trusted.txt
- 9 Repeat steps for multiple certificates
- 10 Comments may be added above the -----BEGIN CERTIFICATE----- to identify the name of the certificate and its expiration date.

For example: RSA Commercial CA - exp. Jan 7, 2010

-----BEGIN CERTIFICATE-----

...

-----END CERTIFICATE-----

HTTP_TRANS (Web Transaction probe)

The HTTP_TRANS probe is used to track specific user actions that occur within Web applications, such as the use of catalog lookup, login/logout, shopping carts, etc.

To specify the actions that you want to track, you use the Configuration Manager. As with the other Internet Services probes, you create a customer and choose the service group for probe type HTTP_TRANS

which launches the Web Recorder. As you will see, using the transaction recorder for configuring the HTTP_TRANS probe(s) alleviates the likelihood of errors and accelerates configuration steps.

Instead of manually typing numerous URLs or page references, the Web Recorder allows you to go through each step of a typical end-user transaction, while it automatically captures your actions and the sequence of accessed pages and links to which you navigate. Later you can test and verify the transaction and make additional modifications on the recorded transaction steps.

Once you configure the HTTP_TRANS probe it then replays the recorded transaction on a regular basis, simulating typical end-user activity and collects important availability and response time data.



Internet Explorer 5.5 or later (IE 6 provides the capability to intercept and log HTTP status codes) is required for use with the Web Transaction Recorder.

You are allowed only one web transaction service target per service group.

Key Concepts

In the Web Recorder, a transaction is composed of individual transaction steps. A step can be a **URL**, or it can be a **navigation point** that is used to determine the next URL to be loaded or the HTML element to be executed. Navigation points are independent of the URL and allow the playback of sties where the URL changes every time (dynamic URLs).

There are two recording types in the Web Recorder: **Lightweight** and **Heavyweight**. This difference is the technology used to do the probing.

- The heavyweight type uses Internet Explorer (also called IE mode) to playback the recorded transaction. Since this probe uses the IE engine, functionality such as JavaScript and screen rendering is supported. The screen rendering draws the web page and executes scripts and embedded objects such as Java and other Plug-ins, thus providing response time measurements that are very close to the ones experienced by an end-user. Note the Heavyweight probe is best run only one at a time, by setting up a network connection with concurrency of 1. Each heavyweight probe is then assigned to this network.

- The lightweight type uses a custom probe that only downloads the URLs and doesn't attempt to render the content which makes it ideal to simulate lots of transactions in parallel to verify the availability of a web site. In addition the lightweight probe is platform independent, whereas the heavyweight probe only runs on Windows.

The following table provides an overview of the supported features for the lightweight recording type and the heavyweight recording type

Table 4 Web Recorder Recording Modes

Recording Type	Mode	Java Script	Java	Dynamic URLs	Plug-ins	Screen Rendering
Light-weight	URL	No	No	Yes	Yes *	No
Light-weight	Navigation Point	No	No	Yes	No	No
Heavy-weight	IE Mode	Yes	Yes **	Yes	Yes *	Yes

* Only Plug-Ins that load URLs

** Loads and executes Java applets but doesn't record interactions

Since the probe for IE mode uses the Microsoft Internet Explorer engine, functionality such as JavaScript and screen rendering is supported. The screen rendering draws the web page and executes scripts and embedded objects such as Java and other Plug-Ins, thus providing response time measurements that are very close to the ones experienced by an actual user.

The number of parallel IE mode transactions depend heavily on the performance of the probe system since significant resources (memory and CPU) are needed for concurrent IE executions.

In contrast, the lightweight modes simulate the transaction without the screen rendering and script execution overhead, which makes it ideal to simulate lots of transactions in parallel to verify availability of an application. The lightweight modes are also platform independent.

In addition, the web site may dictate which mode can be used. If a lot of JavaScript functionality is involved (e.g. filling out multiple forms), selecting the IE mode may be the best approach.

Plug-Ins (such as Flash) are supported as long as they load new pages. For example, a Flash menu would navigate to a new URL when a certain menu item has been selected.

Dynamic URLs are supported through substitution rules and implicitly by the IE mode (see Advanced Topics - Dynamic URL Substitution).

Steps to Using the Web Transaction Recorder

The following outlines the series of steps you would go through to use the web transaction recorder. **Please see the online Help for details.**

- 1 Determine the transaction steps you want to record.
- 2 Configure an HTTP_TRANS service target, which will start the web recorder dialog.
- 3 Select the recording or navigation mode (lightweight or heavyweight).
- 4 Press the Record button to start recording the transaction steps. After the web page has been completely loaded in the window in the right pane, you can navigate through the transaction steps.
- 5 Press Stop to end the recording.
- 6 Playback the recording to test whether all the steps you wanted were included.
- 7 Make any changes using the options in the web recorder.
- 8 Exit and save the probe changes in the Configuration Manager.



The HTTP_TRANS probe in Internet Explorer (IE Heavyweight) mode requires significant CPU and memory resources which can limit the number of parallel executions of this probe type. Too many parallel executions may cause aborts of the probe program `probehttptrans2.exe`. In such a case limit the concurrency in the Probe Location dialog of the Configuration Manager to 2 or create a new network connection. Network connections are executed separately, one after the other, and allow you to control the concurrency of probe executions.

ICMP (Internet Control Message Protocol—Ping)

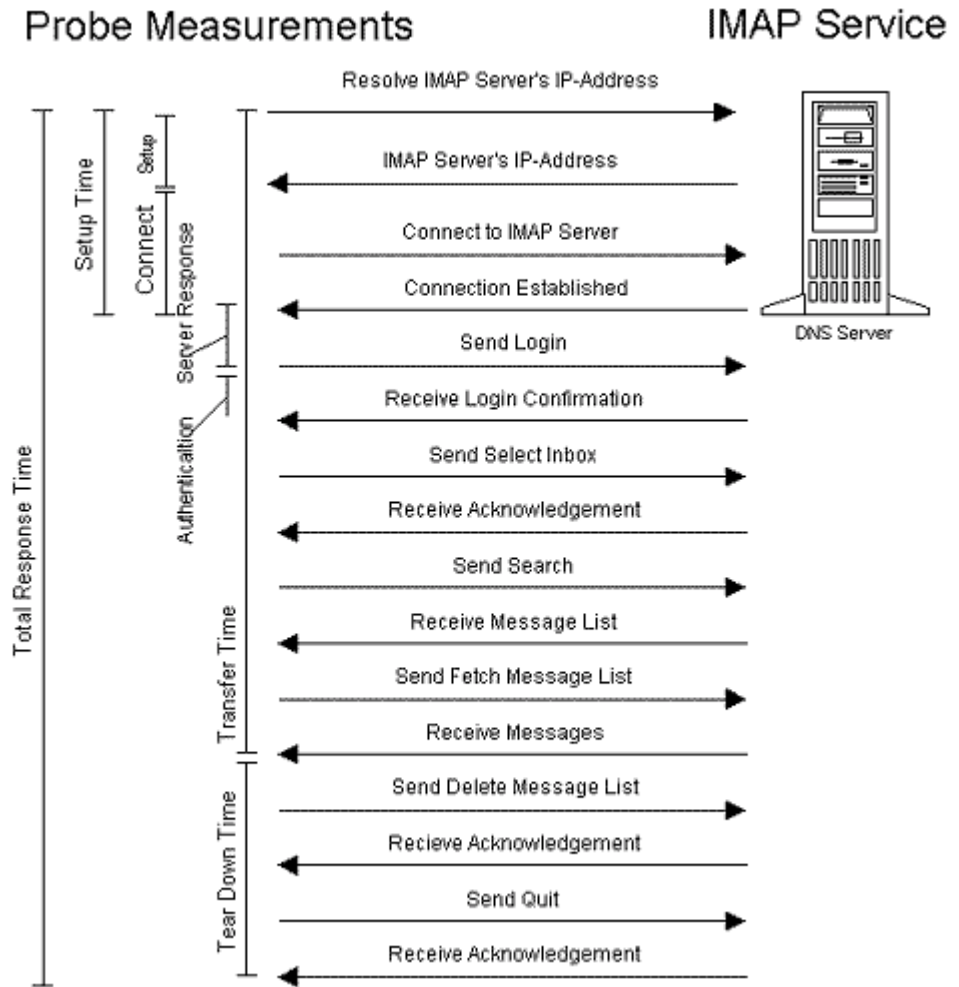
The ICMP probe sends ICMP Echo Requests to the specified host once a second and measures the response time for each request/reply. The total response time returned by the probe is the average of the individual request/reply response times.

Parameters

In the Configuration Manager, you can right-click the Service Group you have created for ICMP and select New **Service Target**. In the **Number of Requests** field you designate how many requests you want sent to the TCP/IP address. When you set up the Probe Location, in the **Request Timeout** field you designate the number of seconds for all requests to wait before timing out.

IMAP4 (Internet Message Access Protocol)

IMAP provides a method of accessing electronic mail or bulletin board messages that are kept on a (possibly shared) mail server. It permits a *client* email program to access remote message stores as if they were local. The IMAP probe measures the steps that occur in the client making its connection to the server and accessing messages. The following diagram shows the protocol steps:



LDAP (Lightweight Directory Access Protocol)

The LDAP probe measures time to connect to an LDAP server and return matching data to a specific distinguished name (supplied by the user). After all the entries matching the search criteria are returned, the probe terminates its connection to the LDAP server. Note that the LDAP probe does not support Windows 2000 active directory LDAP or Microsoft Exchange 2000.

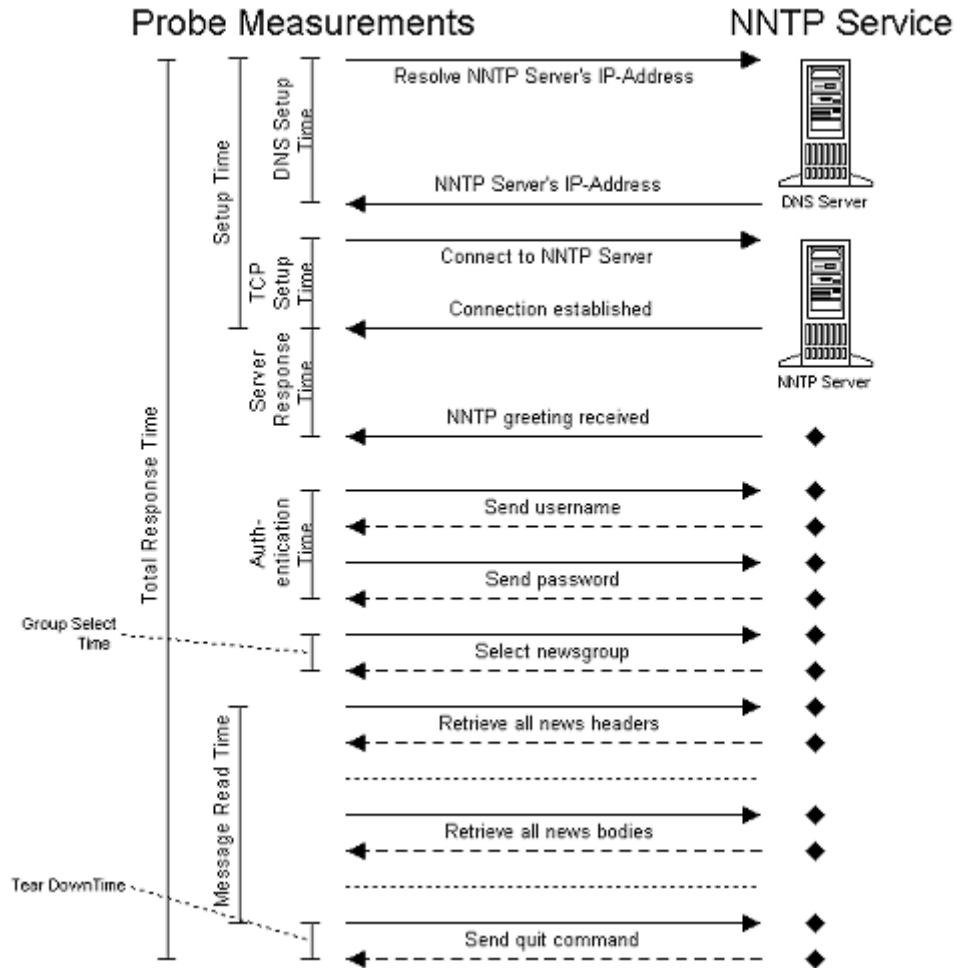
In order to configure the LDAP probe, you must know the structure of the database that the LDAP server accesses. An example of how a specific LDAP configuration might appear within the config.dat file is as follows:

```
[LDAP]
distinguishedName=emailaddress=j_jones@corp.com,ou=employees,o=corp.com
host=ldap.corp.corp.com port=389 scope=LDAP_SCOPE_SUBTREE
```

NNTP (Network News Transfer Protocol)

The NNTP probe emulates a typical news reader. After authenticating to the server (which is optional), the probe selects the specified news group and retrieves all message headers. A user generally uses headers to display the subject lines and get the message attributes (size, identifier, etc.). After downloading headers, the probe retrieves the corresponding message text, simulating a user reading messages.

The following diagram shows the protocol steps of the NNTP probe:

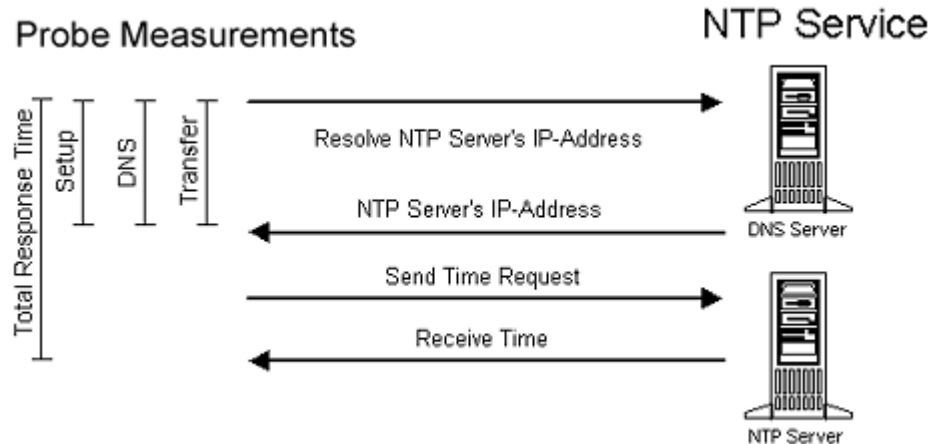


Parameters

The username and password are optional if the NNTP server does not require authentication. The news group must always be specified.

NTP (Network Time Protocol)

Network Time Protocol (NTP) is used to synchronize the time of a computer client or server to another server or reference time source, such as a radio or satellite receiver or modem. This NTP probe measures the time it takes to send a time request to the configured NTP host and receive the current time according to the NTP host. The following diagram shows the protocol steps:



POP3 (Post Office Protocol 3)

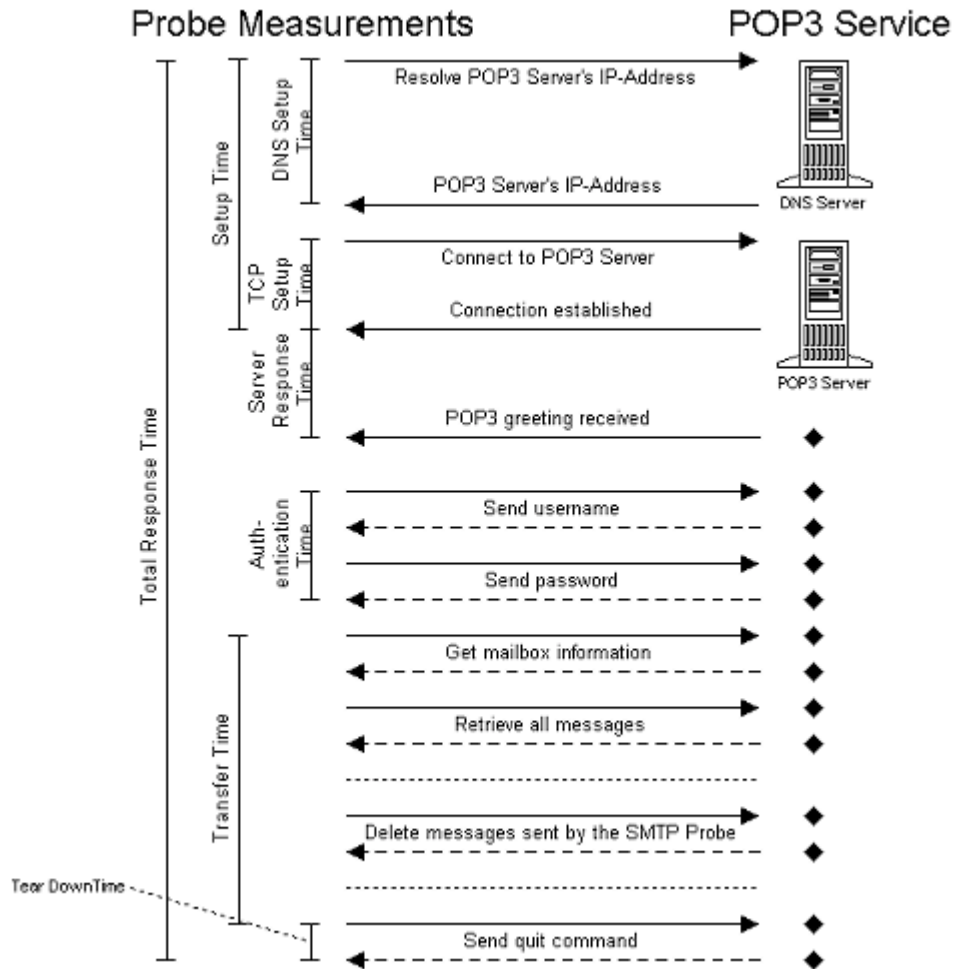
The POP3 probe emulates a user downloading email. After connecting to the POP3 server, the mailbox is authenticated by the specified username and password. On UNIX servers, this is typically the username and password of a local user. On NT (for example, the Exchange Server), the username must include the mailbox name and the account name (as: `MyAdminMailbox\Administrator`).

The probe retrieves all mail in the mailbox and scans for the X-IOPS-
Timestamp header field. This field is set by the SMTP probe. If this field is
detected, the probe adds this message to its internal list for deletion. After
all messages are read, the probe deletes the messages that contain the X-
IOPS- Timestamp. This cleanup mechanism prevents filling up the
mailbox with SMTP probe messages.



It is highly recommended to set up a mailbox specifically for use with
the SMTP and POP3 probe.

The following diagram shows the protocol steps of the POP3 probe:



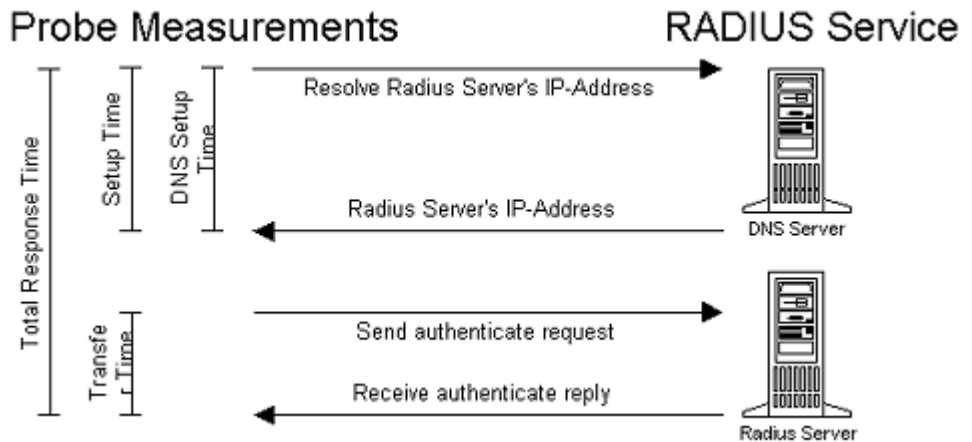
Parameters

Both username and password must be a valid account on the POP3 server system.

RADIUS (Remote Authentication Dial In User Service)

The RADIUS probe measures the total response time of a RADIUS authentication request. After the hostname or IP address is resolved, an authentication request containing a username and encrypted password is sent to the RADIUS server. When the RADIUS server receives the request, it determines if the sending host is authorized to make requests and, if so, it attempts to authenticate the given user. The RADIUS server will acquire the user's password from a well-known source, such as a trusted database, and then use the shared secret to encrypt that password. If this encrypted password created by the RADIUS server matches the encrypted password sent in the authentication request, an access-accept message is sent back to the probe.

The following diagram shows the protocol steps:



The RADIUS probe measures both the time necessary to resolve the hostname/IP address and the time it takes to send and receive the access-accept message. If an "access-rejected" message is sent back to the probe, response time is still measured, even though the RADIUS server is considered unavailable.



The official port for RADIUS is 1812, however many RADIUS servers commercially available use port 1645, which was the port originally chosen (in error) for RADIUS.

The probe currently supports the following protocols:

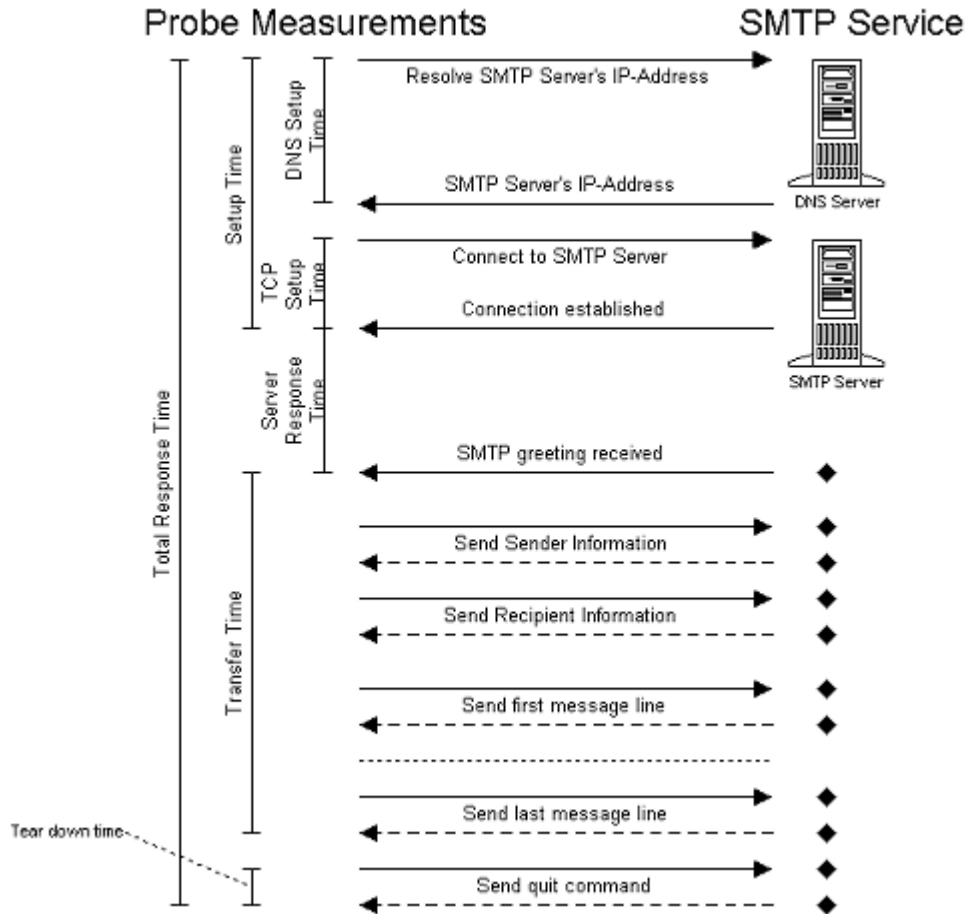
- PAP (Password Authentication Protocol)
- CHAP (Challenge Handshake Authentication Protocol)

Parameters

The shared, secret username and password must be specified.

SMTP (Simple Mail Transfer Protocol)

The SMTP probe posts an e-mail message to the SMTP server. It sets message information such as the recipient and sender, and posts a message body of the specified size. The following diagram shows the protocol steps and measurements involved in posting the message:





Some SMTP servers do not allow forwarding of messages ("relaying"). Forwarding occurs when the recipient's address cannot be resolved by SMTP to a local mailbox. In such a case, the service is considered unavailable. Also, some SMTP servers require a domain extension for the sender.



Make sure to use the POP3 probe in conjunction with the SMTP probe. The POP3 probe can delete the messages that are sent by the SMTP probe. Otherwise the recipient's mailbox will be flooded with messages.

Parameters

The recipient field specifies the email address, which must be resolvable by the SMTP server. Usually, it is in the form <username>@<server>.<domain> (e.g. info@hp.com). The default for the sender field is <> (no user specified). The message size field determines the number of characters with which the message body is filled. A default of 0 does not add any characters to the message body.

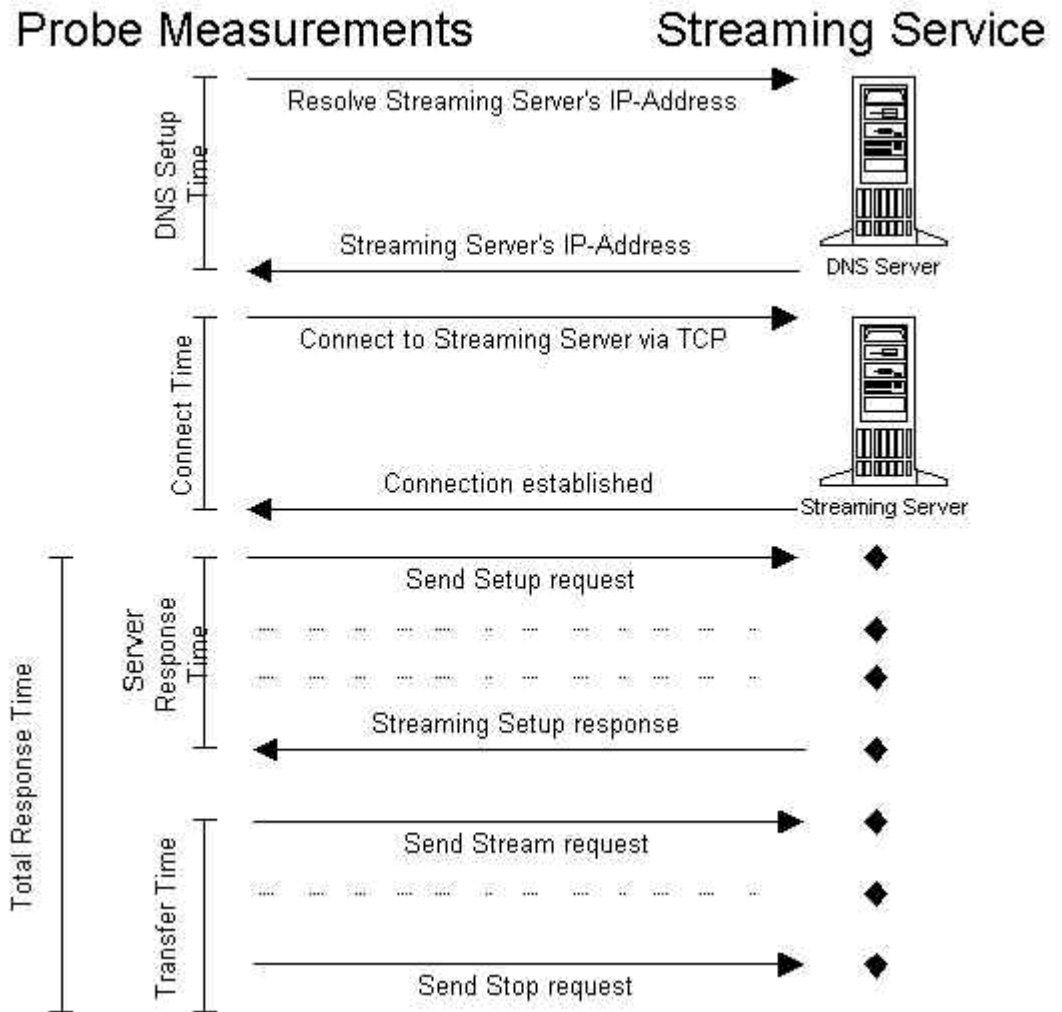
Streaming Media

The Streaming Media probe streams file formats supported by Real Media and monitors the performance.

Real Player (basic Version No. 8 or higher) for Windows is required on whatever system you plan to run the probe. The probe works on Windows NT/2000 platforms only.

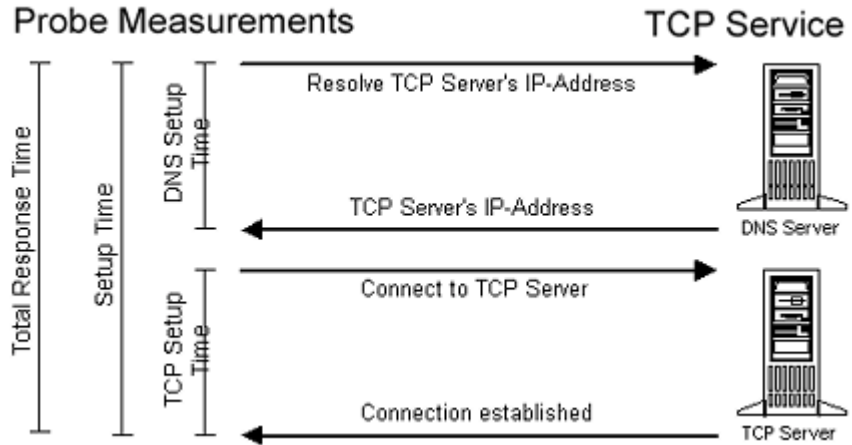
If the probe is behind a proxy and access to the server is through the proxy, then you need to enable the proxy settings in the Real Player. To do this go to **Control Panel > Real Player > Settings** and enable the player to handle proxies. You also need to set up the proxy information in the Probe Location dialog in the Configuration Manager.

The following diagram shows the protocol steps.



TCP (Transmission Control Protocol)

The TCP probe simply measures the time it takes the TCP steps to complete to connect client to the specified host at the specified port. The following diagram shows the protocol steps:

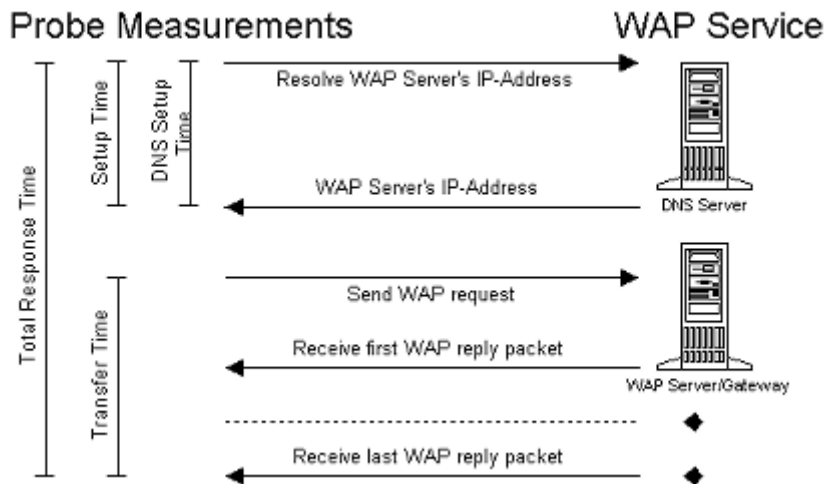


WAP (Wireless Application Protocol)

The WAP (Wireless Application Protocol) probe measures the total response time of an emulated WAP request. After the hostname or IP address is resolved, a WAP request for a document is sent to the WAP Server or WAP Gateway. Once the WAP server receives the request, it locates the requested document and sends it back to the probe. The probe measures both the time necessary to resolve the hostname/IP address and the time it takes to send and receive the specified file.

Currently, the probe supports only WSP (connection-less protocol).

The following diagram shows the protocol steps:



Parameters

The default port number for WAP is 9200. Currently, the WAP probe downloads only the document without embedded images. Note that if you configure the WAP probe to run over a Dial Up Network Connection, RAS (Remote Access Server) and a minimum of one phonebook entry must be configured on the probe system.

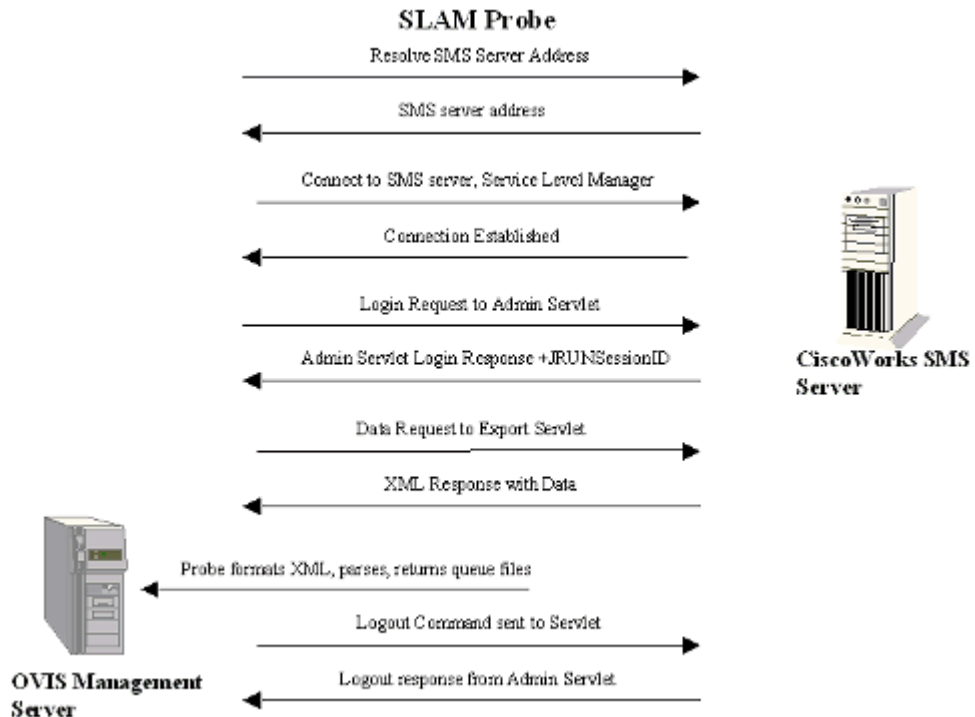
X_SLAM (CiscoWorks Integration)

The X_SLAM series of probes connects to and downloads metrics gathered by synthetic probes on a CiscoWorks server. The information the X_SLAM probe returns from the server is dependent on the CiscoWorks Service Level Contract (SLC) and the Service Level Agreement (SLA) values entered for the probe.

When setting up the probe it is recommended that the probe location be set up for the Service Group before entering the Service Target. This will allow the Service Target dialog to use the proxy and port entered in the

Probe Locations dialog to retrieve the SLC/SLA configurations from the CiscoWorks server. Also it is recommended that you set the Probe Location configuration to retrieve the information on one hour intervals with a 300 second timeout.

The following diagram shows the protocol steps.



Creating your Own Custom Probes

You can use the Custom Probes feature in Internet Services to develop your own probes to probe services unique to your environment. Custom Probes comes is a set of Application Programming Interfaces (APIs) that support development of Custom Probes to probe user specific services, and forward measurements back to the Internet Services Management Server.

The APIs primarily provide functionality for command line parsing, time measurement, probe tracing, error logging and data logging to the Internet Services Management Server.

Technical support for Internet Services custom probes is only available through the **purchase** of hp Partner Care Extended (U2461AA). For more information on hp Partner Care, contact your hp sales representative or hp sales office. Additional information can be found at the Partner Care web site: www.hp.com/go/partnercare.



Warning: Support for the Internet Services custom probes feature is **NOT** available through standard support channels.

See the *Internet Services Custom Probes API Guide* (CustomProbes.pdf) for more information.

List of Metrics by Probe Type

DHCP

Availability - If a measurement could not be retrieved a 0 is logged otherwise availability is set to 1.

Response Time - Total response time for the DHCP service. (Setup Time + Transaction Time)

Transfer Throughput - Transfer bytes/Transfer Time in kbytes/sec.

Setup Time Time to resolve address and establish the connection if host is specified.

Metric 1 - Time to first offer from server.

Metric 2 - Time to lease offered IP address.

Metric 3 - IP address of server.

Metric 4 - Offered IP Address.

Metric 5 - Time to complete entire transaction (discover, offer, request, acknowledge and release)

Metric 6 - The number of bytes transferred.

Dial Up

Availability - If a measurement could not be retrieved a 0 is logged otherwise availability is set to 1.

Response Time - Time taken to establish PPP connection.

Metric 1 - Error returned by RAS Dial. Will be 0 for successful connection.

Metric 2 - Baud Rate - Transfer rate as reported by the modem.

Metric 3 - Total time connected.

Metric 4 - True (1) for abnormal termination of connection, otherwise false (0).

DNS

Availability - If a measurement could not be retrieved a 0 is logged otherwise availability is set to 1.

Response Time - Execution time of the query to a hostname/IP address.

Answer DNS - Answer DNS is set to 0 if the hostname cannot be resolved, and 1 if it can. In either case Availability will be 1 (or true) because the server is doing its job answering the query, whether the name can be resolved or not.

FTP

Availability - If a measurement could not be retrieved a 0 is logged, otherwise availability is set to 1.

Response Time - Total response time of the FTP request (DNS Setup Time + Connect Time + Server Response Time + Setup Time + Authentication Time + Port Time + Data Transfer Time).

DNS Setup Time - Time to resolve hostname through DNS.

Connect Time - Time to perform connect to FTP server.

Server Response Time - Time it takes to receive the FTP start header (220).

Setup Time - Time to resolve address and establish the connection.

Authentication Time - Time to authenticate user (time to send username/password and receive response).

Port Time - Time to send the client connection ports to the FTP server

Transfer Time - Overall time to receive data on the data connection.

Data Trans Bytes - The number of bytes transferred.

Transfer Throughput - Transfer bytes/Transfer Time in kbytes/sec.

HTTP

Availability - If a measurement could not be retrieved a 0 is logged, otherwise availability is set to 1.

Response Time - Total response time for the web page access (DNS Setup Time + Connect Time + Server Response Time + Transfer Time).

DNS Setup Time - Time to resolve hostname through DNS

Connect Time - Time to perform connect to resolved IP address

Server Response Time - Time it takes to send HTTP Get request and receive first response packet.

Transfer Time - Time it took to send request and receive all reply packets.

Setup Time - Time to resolve address and establish the connection.

Transfer Bytes - The number of bytes transferred.

Requests - Number of HTTP requests. For example, if the page was redirected or embedded objects are downloaded.

Transfer Throughput - Transfer bytes/Transfer Time in kbytes/sec.

HTTP_TRANS

Availability - If a measurement could not be retrieved a 0 is logged, otherwise availability is set to 1.

Response Time - Total response time for the web page access (DNS Setup Time + Connect Time + Server Response Time + Transfer Time).

DNS Setup Time - Time to resolve hostname through DNS

Connect Time - Time to perform connect to resolved IP address

Server Response Time - Time it takes to send HTTP Get request and receive first response packet.

Transfer Time - Time it took to send request and receive all reply packets.

Setup Time - Time to resolve address and establish the connection.

Transfer Bytes - The number of bytes transferred.

Requests - Number of HTTP requests. For example, if the page was redirected or embedded objects are downloaded.

Transfer Throughput - Transfer bytes/Transfer Time in kbytes/sec.

HTTPS

Availability - If a measurement could not be retrieved a 0 is logged, otherwise availability is set to 1.

Response Time - Total response time for the secure web page access (DNS Setup Time + Connect Time + server Response Time + Transfer Time).

DNS Setup Time - Time to resolve hostname through DNS

Transfer Time - Time it took to send request and receive all reply packets.

Setup Time - Time to resolve address and establish the connection.

Transfer Bytes - The number of bytes transferred.

Requests - Number of HTTP requests. For example, if the page was redirected or embedded objects are downloaded.

Transfer Throughput - Transfer bytes/Transfer Time in kbytes/sec.

ICMP Network Service

Availability - If a measurement could not be retrieved a 0 is logged, otherwise availability is set to 1.

Response Time - Response time is the average roundtrip time for all ICMP packets

Min/Max Response Time - Minimum and maximum roundtrip time of all ICMP packets

Packet Loss - Number of packets lost

Transfer Throughput - Transfer bytes/Transfer Time in kbytes/sec.

IMAP4

Availability - If a measurement could not be retrieved a 0 is logged otherwise availability is set to 1.

Response Time - Total response time for the IMAP4 service. (Setup Time + Connection Time + Server Response Time + Authentication Time + Transfer Time).

Setup Time - Time to resolve address and establish the connection

Transfer Throughput - Transfer bytes/Transfer Time in kbytes/sec.

DNS set up time - Time to resolve hostname through DNS.

Metric 2 - Time to perform connect to resolved IP address.

Metric 3 - Time for IMAP server to respond.

Metric 4 - Time to authenticate user (time to send username/password and receive response).

Metric 5 - Overall time it took for the data transfer only.

Metric 6 - The number of bytes transferred.

LDAP

Availability - If a measurement could not be retrieved a 0 is logged otherwise availability is set to 1.

Response Time - Total response time for the LDAP service. (Setup Time + Data Transfer Time).

Transfer Throughput - Transfer bytes/Transfer Time in kbytes/sec.

DNS Setup Time - Time to resolve hostname through DNS.

Metric 2 - Number of returned entries.

Metric 4 - Overall time it took for the data transfer only.

Metric 5 - The number of bytes transferred.

NNTP

Availability - If a measurement could not be retrieved a 0 is logged, otherwise availability is set to 1.

Response Time - Total response time for NNTP (DNS Setup Time + Connect Time + Server Response Time + Authentication Time + Group Time + Read Time + Tear Down Time).

DNS Setup Time - Time to resolve hostname through DNS.

Connect Time - Time to perform connect to resolved IP address.

Server Response Time - Overall time to read the file (receive data on the data connection).

Setup Time - Time to resolve address and establish the connection.

Authentication Time - Time to authenticate user (time to send username/password and receive response).

Group Time - Time to select newsgroup and get request overview of last 100 articles.

Read Time - Time to read articles with the overall size of 10000 bytes.

Tear Down Time - Overall time to send the QUIT request and receive the response.

Data Trans Bytes - The number of bytes transferred.

Transfer Throughput - Transfer bytes/Transfer Time in kbytes/sec.

NTP

Availability - If a measurement could not be retrieved a 0 is logged otherwise availability is set to 1.

Response Time - Total response time for the NTP service. (Setup Time + Transfer Time).

Setup Time - Time to resolve address and establish the connection

Transfer Throughput - Transfer bytes/Transfer Time in kbytes/sec.

Metric 1 - NTP receive timestamp (integer part).

Metric 2 - NTP receive timestamp (fraction part).

Metric 3 - NTP transmit timestamp (integer part).

Metric 4 - NTP transmit timestamp (fraction part).

Metric 5 - The number of bytes transferred.

Metric 6 - Overall time it took for the data transfer only.

POP3 Mail Server

Availability - If a measurement could not be retrieved a 0 is logged, otherwise availability is set to 1.

Response Time - Total response time for the POP3 Mail delivery (DNS Setup Time + Connect Time + Server Response Time + Authentication Time + Data Transfer Time).

DNS Setup Time - Time to resolve hostname through DNS.

Connect Time - Time to perform connect to resolved IP address.

Server Response Time - Time it takes to receive the POP3 start header (+OK).

Setup Time - Time to resolve address and establish the connection.

Auth Time - Time to authenticate user (time to send username/password and receive response).

Transfer Time - Overall time to read all messages in the mailbox and delete the IOPS test messages.

Data Trans Bytes - The number of bytes transferred.

Average Mail Deliver - Average mail delivery time.

Max Mail Deliver - Maximum mail delivery time.

Transfer Throughput - Transfer bytes/Transfer Time in kbytes/sec.

Radius

Availability - If a measurement could not be retrieved a 0 is logged, otherwise availability is set to 1. If the server is successfully contacted but returns an Access-Reject packet (because of a bad password, secret, etc.) the Availability will be 0.

Response Time - Total response time for the RADIUS service (DNS Setup Time + Data Transfer Time).

Setup Time - Time to resolve address and make connection.

Transfer Time - Overall time it took for the data transfer only.

Data Trans Bytes - The number of bytes transferred.

Transfer Throughput - Transfer bytes/Transfer Time in kbytes/sec.

SMTP Mail Server

Availability - If a measurement could not be retrieved a 0 is logged, otherwise availability is set to 1.

Response Time - Total response time for the SMTP mail request (DNS Setup Time + Connect Time + Server Response Time + Transfer Time + Tear Down Time).

DNS Setup Time - Time to resolve hostname through DNS.

Connect Time - Time to perform connect to resolved IP address.

Server Response Time - Time it takes to receive the SMTP start header (220).

Setup Time - Time to resolve address and establish the connection.

Transfer Time - Overall time to transfer the mail request (including SMTP responses to the requests such as MAIL FROM:, RCPT TO: DATA, QUIT).

Trans Bytes - The number of bytes transferred.

Tear Down Time - Overall time to send the QUIT request and receive the response.

Transfer Throughput - Transfer bytes/Transfer Time in kbytes/sec.

Streaming Media

Availability - If a measurement could not be retrieved a 0 is logged otherwise availability is set to 1.

Response Time - Total response time for the Streaming Media service (which includes the time it takes to transfer the data and the set up time).

Server Response Time - The time it takes for the server to start sending packets. This includes the set up time for the various protocols.

Connect Time - The time to connect to the server. If a proxy is used then this is the time it takes to connect to the proxy.

Transfer Time - The time it takes to transfer the data.

Transfer Throughput - The average bandwidth used in data transfer in Kbytes/sec.

DNS Set Up time - Time to resolve hostname through DNS.

Total Packets Received - Total number of packets received.

Packet Loss - The percentage of packets lost.

Latency - The latency in data transfer in seconds. The server responds at set intervals so after a request is sent there may be some wait time before the next interval.

Congestion - The percentage of time spent in buffering data vs. the total time for playing the streams. This includes the initial buffering time.

TCP

Availability - If a measurement could not be retrieved a 0 is logged otherwise availability is set to 1.

Response Time - Total response time for the TCP service. (Setup Time + Connection Time).

Transfer Throughput - Transfer bytes/Transfer Time in kbytes/sec.

Setup Time - Time to resolve address and establish the connection

DNS Setup Time - Time to resolve hostname through DNS.

Metric 2 - Time to perform connect to resolved IP address.

WAP

Availability - If a measurement could not be retrieved a 0 is logged, otherwise availability is set to 1.

Response Time - Total response time for the WAP service (DNS Setup Time + Data Transfer Time).

DNS Setup Time - Time to resolve hostname through DNS.

Transfer Time - Overall time it took for the data transfer only.

Data Trans Bytes - The number of bytes transferred.

Transfer Throughput - Transfer bytes/Transfer Time in kbytes/sec.

X-SLAM

The protocols supported for SMS 1.0 are: DNS, ICMP, HTTP, UDP, and VoIP. For SMS 2.0 the protocols supported are: DNS, ICMP, HTTP, TCP, UDP, and VoIP.

Protocol	ProbeType
DNS	X_SLAM_DNS
ICMP	X_SLAM_ICMP
HTTP	X_SLAM_HTTP
TCP	X_SLAM_TCP
UDP	X_SLAM_UDP
VoIP	X_SLAM_VoIP

List of metrics, and data parsed from data retrieved from SLM server.

X_SLAM_DNS

Availability
Response Time

X_SLAM_HTTP

Availability
Response Time
HTTP Time
Connect Time
Transact Avg
Transfer Bytes
Setup Time
Transfer TPut

X_SLAM_ICMP

Availability
Response Time

X_SLAM_UDP

Availability
Response Time

X_SLAM_TCP

Availability
Response Time

X_SLAM_VoIP

Availability
Response Time
FWDLOSS
BWDLOSS

Integrating with Other OpenView Products

You can integrate Internet Services (OVIS) with OpenView Operations for UNIX (OVO for UNIX - formerly know as VantagePoint Operations or as IT/O), Network Node Manager (NNM), or Openview Operations for Windows (OVO for Windows - formerly known as VantagePoint for Windows). Integrating Internet Services with any of these products enables the integrated product to retrieve alarms and messages generated within Internet Services. At the console of the integrated product, you are alerted to those Internet Services-configured services that are not meeting specified objectives. With the integration you expand your performance monitoring area and are able to quickly to determine reported problems.



Additional information on configuring remote UNIX probes is also covered in chapter 3, [“Configuring and Installing Remote Probes on UNIX Systems”](#) on page 66.

Internet Services also integrates with Service Information Portal (SIP), Reporter and the OpenView Performance Agent. This chapter covers the following:

- “Integrating with OpenView Operations for UNIX”
- “Integrating with Network Node Manager (NNM)”
- “Integrating with OpenView Operations for Windows”

Integrating with OpenView Operations for UNIX

To integrate Internet Services with OpenView Operations for UNIX (OVO), you must install the Internet Services integration package on the OVO management server. Then from the OVO console you can distribute the Internet Services templates to the Internet Services Management Server and probe systems so that probe data can be forwarded to OVO. OVO integration offers you the following:

- Within the OVO Message Browser, display of Internet Services service objective violations as alarms.
- Within the OVO console, consolidation of alarms under the OVIS message group and consolidation of errors for the Internet Services server and probe under the OVIS_Errors message group.
- Within the OVO Service Navigator, display of Internet Services Customer/Service Group/Service Objective tree.
- Within the OVO Message Browser, ability to launch the Internet Services Dashboard as part of an operator action in the opcmsg template.
- Additional information from Internet Services status log files (status.reporter and status.iops) originating from log file templates on the Internet Services server.
- Self-monitoring for the Internet Services scheduler and IIS Web Server
- A new message interceptor templates (OVIS Alarms (2)) provides correlation of failure alarms (critical, minor major and warning) with normal alarms. This means a critical unavailability alarm is automatically acknowledged and put in the history browser when a normal alarm is received indicating the service is available again.
- The integration package is installable on Japanese systems running Japanese OVO for UNIX (5 and 6). Note that templates are not yet localized.

Requirements

- Internet Services integration with OVO is supported on ITO A.05.XX and VPO A.06.XX.

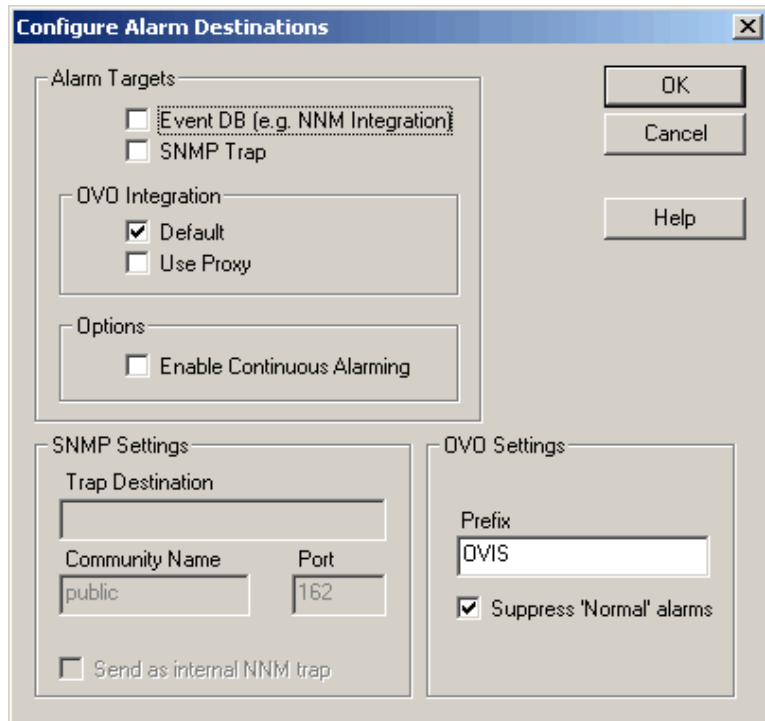
- Netscape (version 4.x) is required on the OVO management server for displaying the Internet Services dashboard web display. The browser is launched with the **ovweb** command. Please refer to the **ovweb** man-page for correct setup.
- An OVO agent must be installed and running on the OVO management server for the Internet Services dashboard integration and the Service Navigator integration. (Please refer to the OpenView Operations manuals and swinstall man page for more information about OpenView Operations, Service Navigator, and swinstall.)
- A checkbox selection within the Internet Services Configuration Manager dialog to forward alarms to OVO.
- Installation of an OVO agent on the Internet Services server for forwarding alarm messages to OVO.
- If you are installing the integration on a Japanese OVO system, it is required that swagentd was started under LANG=ja_JP.SJIS.
As root:
export LANG=ja_JP.SJIS
swagentd -r

Configuration Options

Using the Internet Services Configuration Manager, you can choose between two options for forwarding Internet Services data to OpenView Operations for UNIX. The options (accessed by selecting **File>Configure>Alarm Destinations**) are as follows:

- **OVO Integration - Default:** By accepting the default, you choose to allow identification of Internet Services messages sent to OVO for UNIX as having originated from the Internet Services server. This configuration requires that the Internet Services server be added as a managed node in

OVO for UNIX and that the Internet Services server be running an OVO agent.



OR

OVO Integration—Use Proxy: By selecting this mode, you choose to identify the origin of each Internet Services message according to the monitored Internet Services service target node. This configuration requires that you add the Internet Services server, Internet Services probe-installed systems, and the Internet Services service targets nodes to a Node Bank in OVO for UNIX. You are not required to install an OVO for UNIX agent on the service target nodes.

- **OVO Settings—Prefix:** By entering a prefix (such as OVIS), you automatically create a message group for the OVIS monitored services. Uncheck the Suppress Normal alarms check box for automatic acknowledgement for failure messages (requires OVIS Alarms (2) template).

To install Internet Services integration for use with OVO for UNIX (version 4.0), you need to perform the following tasks:

- Uninstall the existing integration (Note that all modifications to the templates you have made are not saved)
- Use the Internet Services installation CD to install the Internet Services components on the OVO management server. Refer to the installation instructions provided with the CD (Internet Services Components for OVO for UNIX integration).
- From the OVO for UNIX console, assign and distribute the now available OVIS templates.

Task 1: Prepare for Upgrade of Previous Version

Upgrade from Previous Version: Before installing the new integration (version 4.0), you need to remove the existing integration files.



Any modifications you have made to the templates will not be saved.

- 1 Un-assign all VPO templates (active monitoring templates) from Internet Services server and all probe systems
- 2 Distribute templates to all nodes
- 3 Delete all VPO template (active monitoring templates) groups and group members including these groups:

Internet Services

VP-IS Probe NT

VP-IS Probe Unix

VP-IS Server

VP-IS ITO Mgmt Server



A deletion of a group will only delete the group and NOT the group members; continue to delete the group members.

- 4 Delete message groups VP-IS and VP-IS_Errors

- 5 Optional. If the passive monitoring components (version 3.5) are not used, deinstall the integration package:

```
swremove HPVPIS
```

Task 2: Install the Integration Package

Once the existing integration is removed, you can install the new integration (version 4.0). Refer to the installation instructions provided with the CD (Internet Services Components for OVO for UNIX integration).

- 1 In the Internet Services Configuration Manager **Configure > Alarm Destinations** dialog change Prefix from VP-IS to OVIS.

- 2 Install depot

HP-UX

- a Insert the CD.

- b As root, find the CD-ROM drive device name:

```
#ioscan -fn | more
```

Example: /dev/dsk/c1t2d0

- c Create the /cdrom directory under root (/)

```
# mkdir /cdrom
```

- d As root, mount the CD onto /cdrom directory

Example: # mount /dev/dsk/c2t2d0 /cdrom

- e Install the software

```
# swinstall -s /cdrom/SETUP/Ovo_Unix/hpdepot
```

Solaris

- a Insert the CD (mounted automatically to /cdrom/cdrom0).

- b Install the software

```
# swinstall -s /cdrom/cdrom0/SETUP/Ovo_Unix/sundepot  
OVIS-SP
```

Then continue to the next task to distribute the new templates.

Task 3: Distribute Templates for Internet Services Probe-based Active Monitoring

To set up Internet Services systems to be monitored for alarms/messages for display within specified OVO for UNIX admins'/operators' Message Browsers

- 1 Launch the OVO Console as Administrator (for example: `opc -user opc_adm -passwd OpC_adm`)
- 2 Set up and configure the Internet Services server system as an OVO managed node (**Action>Add Node**).
- 3 Install an OVO agent on the Internet Services server.
- 4 Set up and configure all Internet Services probe-installed systems as OVO managed nodes and be sure an OVO agent is installed and running on each probe- installed systems.
 - ▶ If you plan to choose OVO Integration-Use Proxy as the alarm- forwarding mode, set up all Internet Services service target nodes as OVO nodes. In this case, you do not need to install an OVO agent on these nodes.
- 5 Add Internet Services nodes to an OVO node group (**Window>Node Group Bank**).
- 6 Assign the OVO node group (with Internet Services nodes) and the OVIS and OVIS-Error message groups to the OVO user(s) (operator and/or administrator) who will be responsible for responding /monitoring Internet Services services. Making these assignments ensures that OVIS messages appear in the user's OVO message browser. (**Window>User Bank** and modify for appropriate operators to receive message; for example, `opc_adm`; select the **Responsibility** button to assign the OVIS and OVIS Error message groups).
- 7 Select **Actions: Agents -> Assign Templates...** and assign the **OVIS Server** Template group to the OVIS server.
 - ▶ If you are not using the OVIS default installation directory, modify log files **OVIS Errors (Server - Reporter)** and **OVIS Errors (Server - OVIS)** to correctly refer to the installation directory.

- 8 Assign either the **OVIS Probe UNIX** or **OVIS probe NT** template group to each of the probe-installed systems. If the Internet Services server is also used as a probe system, assign the **OVIS Probe NT** template group to it as well.



If you are not using the Internet Services default installation directory, modify **OVIS Errors** (Probe) log file to correctly refer to the installation directory.

Task 4: (optional) To integrate Internet Services with the OVO for UNIX Service Navigator (VPO A.06.xx):

- 1 Be sure a local OVO agent is running on the OVO Management Server.
- 2 Assign the **OVIS ITO Mgmt Server** template group to the OVO Management Server.
- 3 In the **OVIS ITO Mgmt Server** template group, select the **OVIS Service Sync** scheduled action template and add the Internet Services server name to the command line. (Include the fully qualified hostname of the Internet Services server; for example, /opt/OV/OVIS/bin/vpispull.sh jester.dev.hp.com. This script synchronizes the Internet Services customer/service group/objective hierarchy to Service Navigator every 5 minutes. As default, it assigns the Internet Services service to the `OVO administrator opc_adm`. Additional operators must be assigned with `opcservice` command (see OpenView Operations for UNIX documentation.)
- 4 Select **Actions: Agents -> Install/Update SW & Config** from the menu.
- 5 In the **Install/Update VPO Software and Configuration window**, select the following options:
 - Actions
 - Monitors
 - Commands
 - Templates
 - Force
 - Update
- 6 Press **OK**.

(If the distribution was successful, you receive appropriate messages in the OVO message browser.)

- 7 In the Internet Services Configuration Manager, select **File>Configure>Alarm Destinations**, and under **OVO Integration**, check

Default (please read previous section on Configuration Options for an explanation)

OR

Use Proxy (requires that you set up all Internet Services service target nodes as OVO nodes, but does not requires that you install an OVO agent on the nodes.

Task 5: If an OVO agent is re-installed on the Internet Services Management Server:

- 1 First stop IIS and hp OpenView Reporter:
net stop iisadmin /y
net stop reporter
- 2 Then re-install the agent and start IIS and Reporter again:
net start W3SVC
net start reporter

Integrating with Network Node Manager (NNM)

After you integrate Internet Services with NNM, NNM receives configuration and event information from the Internet Services database that adds to two areas of NNM:

- 1 **Alarms/messages**, which are automatically forwarded to the NNM alarm system, where they appear in a new Internet Services alarm category. These alarms, like any alarms in NNM, can trigger automatic actions, such as launching an external script or paging an operator.
- 2 **New submap symbols** for NNM managed nodes that have Internet Services- configured service targets. The new symbols represent customers to which the node provides services, services provided those customers, and performance objectives of each service.

With a check box selection in the Internet Services Configuration Manager (accessed from the menu: **File>Alarm Destinations**), Internet Services can generate alarms. The alarms, once forwarded into NNM, appear in the now added "Internet Services" alarm category.

The first task for initiating the Internet Services integration is to install the Internet Services software on the NNM management station. The media you received with Internet Services contains integration software for NNM on Sun Solaris, HP-UX, or Microsoft NT operating systems.

Requirements/Recommendations for NNM Integration

- Internet Services can be integrated with NNM version 6.1 (HP-UX 10.20 and 11.0, Solaris 2.7 and 2.8, Windows NT and 2000) and 6.2 (HP-UX 10.20, 11.0 and 11.11, Solaris 2.6, 2.7 and 2.8, Windows NT and 2000), or later.
- If you also have HP OpenView Customer Views for Network Node Manager, Internet Services automatically integrates to add organizations/customers defined in Internet Services as well as associating their corresponding targets.
- Successful integration with NNM requires that IP submaps be persistent to all levels, which is the default for UNIX(r)-based NNM but is not the default for NNM on Microsoft(r) NT. Setting submap persistence to "All Levels" in order to fully integrate Internet Services with NNM on NT may

cause NNM on NT to require more memory (possibly much more) to function efficiently (see note below).

- Netscape (version 4.5 or greater) and/or Internet Explorer (version 5.0 or greater) are supported browsers on the management server for the Internet Services dashboard integration



Before you install NNM Integration software, it is recommended that you first configure the NNM IP Map application so that submaps are persistent to all levels. Completing this step now saves you from having to complete a manual step later when you start NNM after the integration.

For information on submap persistence, consult the NNM A Guide to Scalability and Distribution. Chapter 2 provides information about on-demand submaps and persistence. Chapter 4 provides simple instructions on how to check and reset the level of your submap persistence if necessary.

How to Integrate with NNM

Task 1: Ensure Internet Services is installed and operational on the management server.

Until Internet Services is successfully installed and operating on the NT system as a stand-alone application, NNM integration cannot take place.

Task 2: At the NNM management station(s) that will integrate with Internet Services, perform the remaining steps



You can have multiple NNM stations pulling information from the Internet Services system. If you have more than one NNM management station available and you would like Internet Services information sent to these stations, perform the following steps on each of those NNM stations.

- 1 Set the submap persistence as noted above in "Requirements/ Recommendations for NNM Integration."** If submap persistence is not set to All Levels, NNM will log errors relating to its inability to create

necessary symbols. These errors are informational only and do not affect NNM's ability to function.

- 2 Follow the NNM Integration installation instructions on the CD-ROM jacket.** Note that there is separate media for the UNIX(r)-based platforms. Installation differs depending on whether you are integrating with NNM on Windows NT, Sun Solaris, or HP-UX.
- 3 Follow the on-screen instructions during installation.** You must provide the fully qualified name (for example, ovis.testlab.megacorp.com) of the Internet Services management station that you are integrating with.
- 4 Start NNM.** If you have not already set the submap persistence to All Levels, do so now. Then selected Rebuild Internet Services Symbols from the (new) Internet Services menu.

Task 3: At the Internet Services management server, configure NNM integration.

In the Internet Services Configuration Manager select File>Configure>Alarm Destinations and check Event DB (e.g., NNM Integration).

Features in NNM after Integration with Internet Services

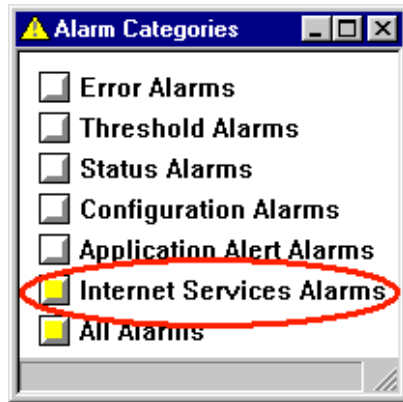
You'll find several changes in NNM after you install the Internet Services integration:

- New alarm category-Internet Services Alarms-appears in the NNM Alarm Categories window.
- New menu-Internet Services-appears on the menu bar.
- New symbols that represent customers, services, and service objectives within NNM submaps.
- New, defined customers-If you have HP OpenView Customer Views for NNM, customers defined in Internet Services appear in the "Customers" view of CV-NNM with their Servers and Access Links submaps populated with the nodes and interfaces supplied by Internet Services.
- New communication mechanism between Internet Services management server and NNM console, which does not **lose** messages (like SNMP) if the NNM console is down for any reason. This mechanism uses an HTTP

protocol, which communicates through port 80, which can be important to know if the two consoles are separated by a firewall.

Internet Services Alarms

The NNM Alarm Categories window shows a new category: Internet Services Alarms.

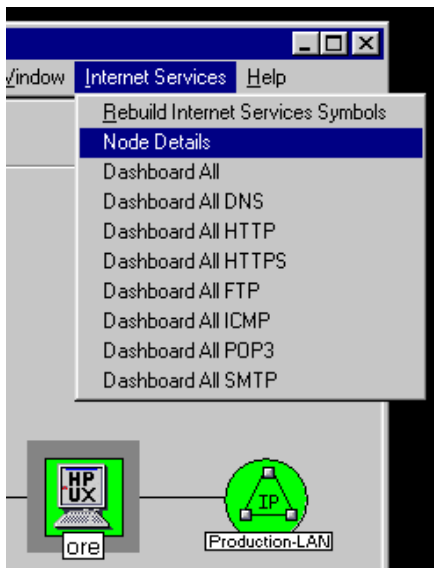


The alarms in this category originate from the Internet Services system. Internet Services alarms work the same as other NNM alarms so that you can expect to use standard NNM methods to configure and manage them as necessary:

- You can configure a script to be launched when certain Internet Services alarms arrive.
- You can acknowledge or delete the alarms in the usual way. However, note that simply removing an alarm will not change the status of the associated service objective symbol in the map (see "Internet Services Symbols" below). That status is updated by Internet Services according to the data it is collecting.

The Internet Services Menu

The NNM menu bar has a new menu after integration with Internet Services: Internet Services.



- **Rebuild Internet Services Symbols** (first item)- enables you to rebuild the Internet Services-added symbols in the map according to the current data in Internet Services. You may find this action necessary only on rare occasions if Internet Services symbols are out of sync with Internet Services.
- **Node Details** (second item)-is extremely useful when you need to know all the detail Internet Services has about a selected node. Clicking this menu item launches the Internet Services Reports page, with the currently selected node.
- **The remaining items** launch the Internet Services dashboard as indicated in the text of the menu item.

Internet Services Symbols in NNM

Any node in the NNM management domain with a service target has three submaps added to it. These submaps contain symbols that represent the **1) Customer(s)** served by the node; customers have child submaps that contain symbols representing the **2) services monitored** for them; services also have child submaps that display the **3) service objective alarms** for the monitored service. An illustration later in this chapter shows new symbols.

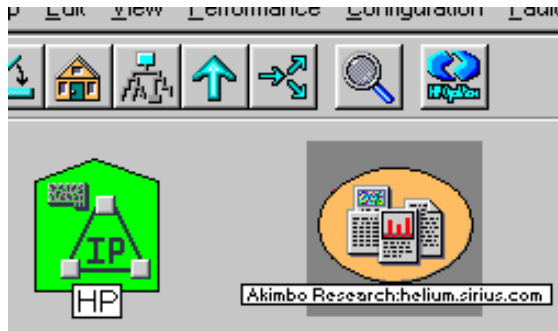
About Configuration Events

A Internet Services configuration change is an event that results in a change to the NNM display. In this way, NNM is updated to reflect the new Internet Services information. For example, configuration events could cause the following behaviors in NNM:

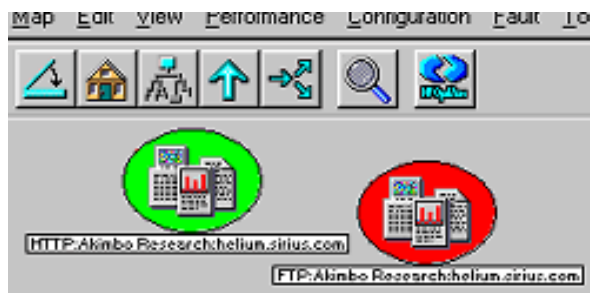
- 1 The status source of the object representing the target node (where the service is running) is set to **Compound (Propagated)**. Normally, nodes on the map determine their status from the interfaces on the node. Changing the status source to compound causes the node to use the status of all of its child objects to determine its status.



- 2 Creates a symbol representing the customer as a child of the target node. The name of the symbol is "customer_name:node_name". For example, suppose you have a node named "helium.sirius.com" which provides a service for a customer named "Akimbo Research". NNM creates a new symbol under "helium.sirius.com" (next to the node's network interface symbols) and names that symbol Akimbo Research:helium.sirius.com



- 3 For each customer symbol created in the previous step, NNM creates one or more symbols representing the service(s) provided to customers by the node. The name of a service symbol is "service_name:customer_name:node_name". For example: "HTTP:Akimbo Research:helium.sirius.com".



- 4 Sets the appropriate service capability to TRUE. For example, a target node that provides the DNS service is (by definition) a DNS server, and so NNM sets the ovisIsDNSServer capability of the node to TRUE

About Alarm Events

After configuration and in response to an alarm from Internet Services, NNM performs the following steps:

- 1 Creates a symbol representing the service objective as a child of the service symbol. The name of the symbol has this format:

```
metric_name:service_name:customer_name:node_name:target_info:probe_location
```

For example, suppose the alarm represents a violation of the following service objective:

Customer:	Akimbo
Service:	FTP
Target Node:	helium.sirius.com
Target Info:	my_xyz_file
Metric:	RESPONSE_TIME
Probe Location:	zinc.sirius.com

The name of the service objective symbol would then be:

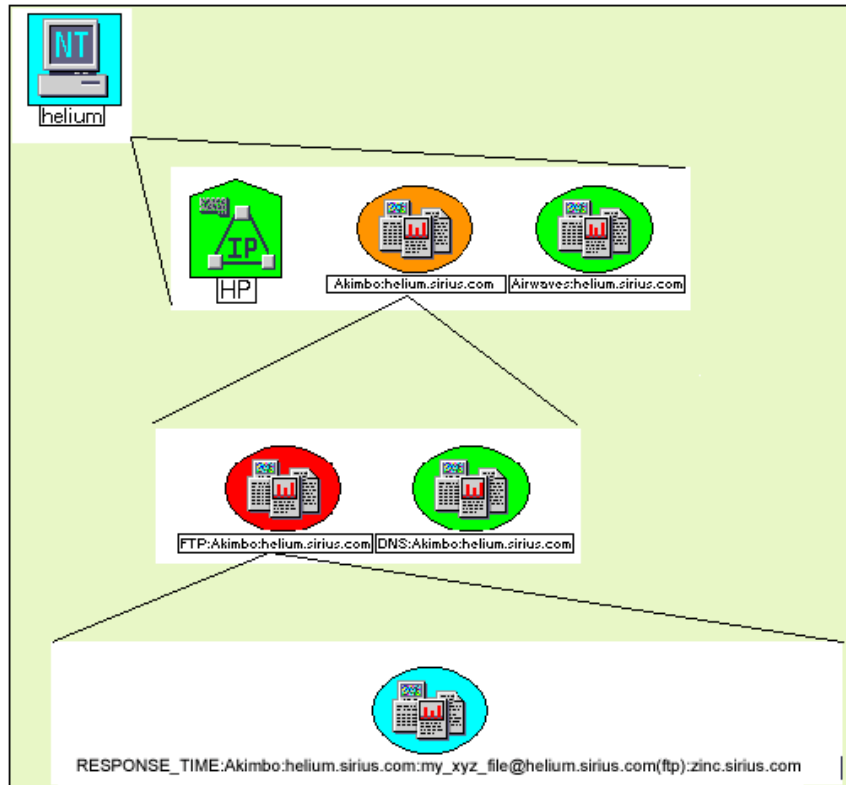
```
RESPONSE_TIME:FTP:Akimbo:helium.sirius.com:my_xyz_file@helium.sirius.com:zinc.sirius.com
```



Service-objective symbol names can be lengthy. If necessary, use the Panner (or on NT, right-click the symbol) to obtain a larger, readable view of the name.

- 2 Sets the status of the service objective symbol to the severity of the alarm.

The illustration below shows examples of symbols with user-defined names.



Simple Troubleshooting for NNM Integration

If you suspect that NNM is not synchronized with Internet Services, you may want to perform a total re-set of the integration data.



All ovw sessions must be closed before running ovisclean.ovpl

The NNM integration package provides a script for that purpose:

\$OV_BIN/ovisclean.ovpl

You can use `ovisclean.ovpl` to completely clear the NNM VP-IS command database, and then retrieve all the latest configuration and alarm data from the VP-IS station. The script also causes a rebuild of all Internet Services symbols within NNM maps.

Integrating with OpenView Operations for Windows

Internet Services integration with OpenView for Windows (OVO for Windows) results in Internet Services threshold violations forwarded as alarm messages to OpenView Operations for Windows for display in the console message browser. Using the Internet Services Configuration Manager, you can choose between two options for forwarding Internet Services data to OVO for Windows. The options (accessed by selecting **File>Configure>Alarm Destinations**) are as follows:

- **OVO Integration—Default:** By leaving this mode (default) checked, you choose to allow identification of Internet Services messages sent to OVO for Windows as having originated from the Internet Services server. This configuration requires only that the Internet Services server be configured as a node in OVO for Windows.

or

- **OVO Integration—Use Proxy:** By selecting this mode, you choose to identify the origin of each Internet Services message according to the Internet Services service target node being monitored. This configuration requires that you add all Internet Services service target nodes to the Nodes folder in OVO for Windows console.

Configuration Tasks

Before starting, configure all Internet Services service targets and objectives in the Internet Services Configuration Manager and then verify that data comes in and that graphs and reports are generated.

- 1 In the OVO for Windows console and add the Internet Services server to the OVO for Windows Nodes folder.

(Please refer to the OVO for Windows online Help for more information on configuring managed nodes and other related topics.)
- 2 Deploy an OVO for Windows agent to the Internet Services server.

- 3 If you plan to choose **OVO Integration—Use Proxy** as the alarm-forwarding mode, add all Internet Services service target nodes to the Nodes folder in OVO for Windows.
- 4 Double-click the Open Message Interface policy group, select the **opcmsg message** policy, and deploy it to the Internet Services server node (and/or all service target nodes if you added them to the OVO for Windows Nodes folder).

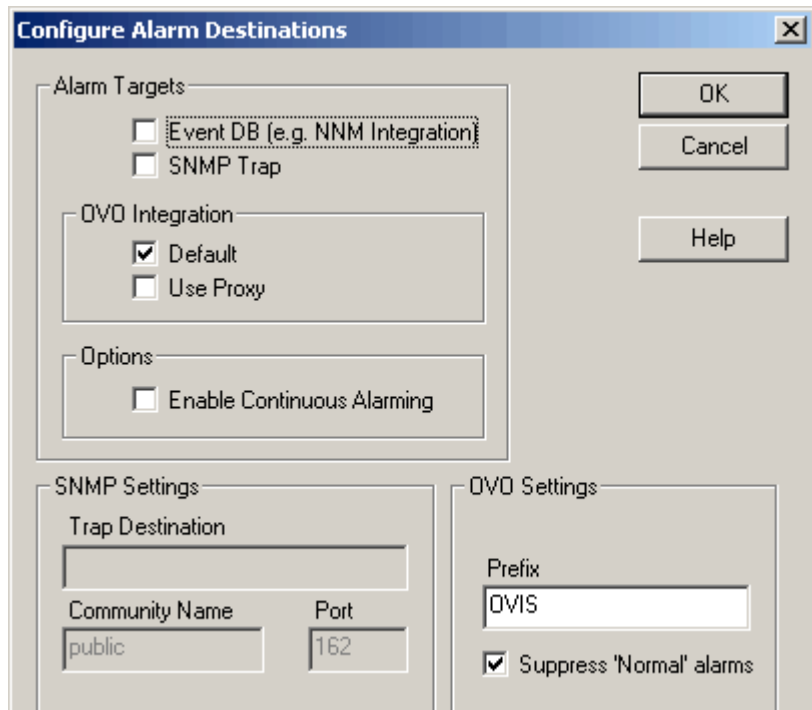
(To make sure that messages are forwarded as expected, on the Internet Services server open a Command Prompt window and enter: `opcmsg a=OVIS o=OVIS_Test msg_text="Test".`)

- 5 In the Internet Services Configuration Manager, select **File>Configure>Alarm Destinations**, and check

OVO Integration—Default

OR

OVO Integration—Use Proxy (requires that you add all Internet Services service target nodes to the OVO for Windows Nodes folder).



Alarm messages should now be forwarded to OVO for Windows. The object field in the OVO for Windows View Message Browser - Active Message window will show the service target and the probe installed system from which the message originated. The basic integration uses the default opcmmsg policy, which flags all messages as "unmatched" because no specific condition was set up.

Troubleshooting Information

This chapter gives you basic troubleshooting information including the following:

- “Troubleshooting Red Status Indicators”r
- “Looking at OVIS Trace Files”
- “Database running out of space”
- “OVO for UNIX Integration Enabled but not Working Properly”
- “Troubleshooting the HTTP_TRANS Probe”

Refer to the Internet Services Release Notes for a list of files with version information.

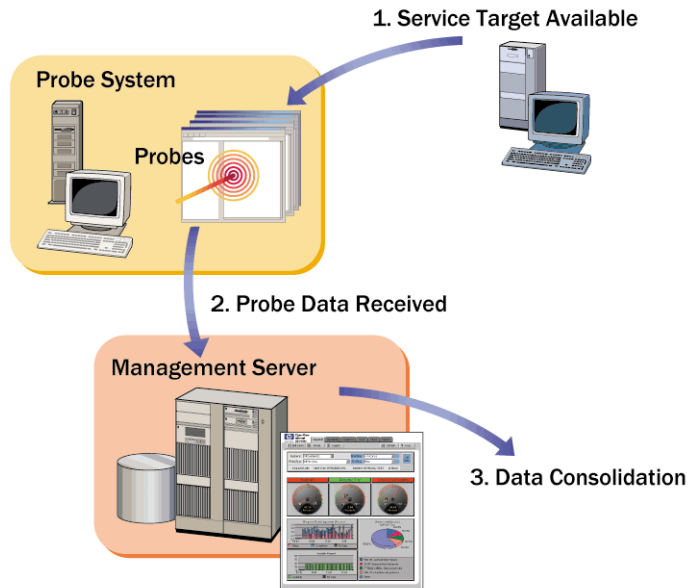
Troubleshooting Red Status Indicators

This section deals with problems that are indicated through the status window of the Configuration Manager, where you see a red circle next to the items listed in the Service Target Availability, Probe Data Received, and Data Consolidation tabbed pages.

If you are not receiving data regarding a service target you have configured, any one of three areas could be the cause.

- 1 Service Target Availability
- 2 Probe Data Received
- 3 Data Consolidation

Figure 3 Flow of Probe Data





Prerequisite: You have configured service groups using the Configuration Manager and you know that probes are deployed to the correct locations.

Service Target Availability Displays Red Circle

If a target in the Service Target Availability column of the status display is red, there can be two reasons: either the target is **Unavailable**, or there is **No Probe Info** (these states are shown in the **Status** column of the screen).

- **Unavailable:** If the target status is **Unavailable**, this means that the probe executed, tried to access the target, and determined that the target was unavailable for some reason, and has informed OVIS of this fact.
- **No Probe Info:** If the target status is **No Probe Info**, this means that OVIS has not received any measurement information from the probe. This indicates either the probe has not had enough time to run and return data to OVIS, or else there is a problem in the communication between the probe and the OVIS management server.

Target Status Unavailable

When a target is unavailable, there are a number of possible causes:

- Mis-typed target information. For instance, the URL for an HTTP target was typed incorrectly, or the server for an FTP target is not correctly qualified. For an HTTP example of how to check this, see [“Possible Cause: Invalid URL \(IOPS 1-11\)” on page 158](#)
- Missing proxy information. For example, if your site requires the use of a web proxy to get at certain web sites outside your intranet, you must enter this information when configuring the Probe Location. For how to check this see [“Possible Cause: Proxy Information Incorrectly Configured” on page 158](#)

Proxy not working. Possibly, the web proxy is not functioning properly. You can verify this using a browser, or you can ping the proxy and see if it

responds. For an example see [“Possible Cause: Connection to Web proxy Timed Out” on page 158](#)

- Unable to resolve name or IP address. Sometimes, the DNS server is unable to resolve the target host name. Verify that the host name or IP address is resolvable by using the `nslookup` command (e.g. `nslookup web.alt.hp.com`). If you do not receive an IP-address, the system is not registered with the DNS server or the DNS server you are accessing is slow or down.
- Service unavailable. This is actually one of the things that OVIS is designed to do -- discover when the service is down! Make sure the service is really up and functioning (for example, for HTTP, visit the web site using a browser, or for other probes FTP a file, send an e-mail message).

No Probe Information

When there is no probe info, and the probe should have had enough time to gather information and send it to OVIS, there must be a problem in the communication between the probe and the OVIS management server. Here are some possible causes and action to take:

- The Web Server on the OVIS system is not running and operational. See [“Possible Cause: Local Web server connection failed” on page 157](#).
- Proxy required between the probe system and the OVIS management server. Don't forget to make sure that this has been configured, if required, in the Probe Locations dialog.
- Security settings incorrect for communication between the probe system and the OVIS management server. If you are using secure communication between the probe systems and the OVIS management server, make sure that the certificates and web server configuration are set up correctly. See the section on [“Configuring Secure Communication - Probe and Management Server” on page 179](#) in Chapter 7.
- HP Internet Services (the probes) service is not running. Make sure (using the Services dialog of Windows) that the HP Internet Services service is started.

Here are some clues to help you understand what the No Probe Info problem might be:

- On the probe system, if there are no queue files in the `<installdir>\probes\queue` (or `<installdir>\Data\queue`

directory (if the probes are running locally), this probably means that the probe service ('HP Internet Services') is not running. Verify this by checking the timestamp of the SEQ file in this directory; if it is not up-to-date, then the probes are not running. Stop and start the service to see if this alleviates the problem.

- On the probe system, if there are queue files building up in the <installdir>\probes\queue directory, this means that the probe service ('HP Internet Services') is probably running fine, but the OVIS management server is not accepting the measurement data. Just to make sure that the probe service is running okay, stop and start the service.

Possible Cause: Local Web server connection failed

Action

Verify the local Web server is correctly configured and running

- 1 Open your Web browser and in the Address bar enter:

```
<system_name>/HPOV_IOPS/  
for example: nt-t30.xsys.corp.com/HPOV_IOPS/
```

- 2 An example of a successful response:

```
[To Parent Directory]  
Wednesday, January 08, 2002 10:56 AM <dir> cgi-bin  
Wednesday, January 08, 2002 10:56 AM <dir> isapi  
Wednesday, January 08, 2002 10:56 AM <dir> java
```

If you get an error like HTTP 404 (page not found), the Web service may not be started, so to start the service:

- a Open the NT Control Panel, select **Services**, highlight **World Wide Web Publishing Service**, and press the **Start** button.
- b Close the Control Panel
- c Open your Web browser and in the Address bar enter:

```
<system_name>/HPOV_IOPS/  
for example: nt-t30.xsys.corp.com/HPOV_IOPS/
```

Possible Cause: Invalid URL (IOPS 1-11)

Socket error 11001 in 'gethostbyname' due to a typing error in service target information.

Action

Verify the URL is available through the Web browser

- 1 Open the Configuration Manager.
- 2 Highlight the Service Target you are checking, right-click, and select **Edit Service**.
- 3 Copy the host URL into your Web browser Address bar.
- 4 If an error appears, such as HTTP 404 (page not found), the URL may have been mis-typed.
- 5 Enter the correct URL by editing the Service Target

Possible Cause: Proxy Information Incorrectly Configured

Action

Check the proxy information in the Probe Locations dialog in the Configuration Manager for the service target and compare to the LAN settings in Internet Explorer **Internet Options>Connection tab>LAN settings**. Make changes to the proxy settings as needed.

Possible Cause: Connection to Web proxy Timed Out

Action

Verify the web proxy can be resolved.

- 1 From a command prompt, enter **ping** followed by the Web proxy server address, for example: `ping web-proxy.xsys.corp.com`
- 2 If you get a Timed out or Bad IP address response, contact your network administrator.

Probe Data Received Displays Red Circle

If there is a red circle in this column in the status display, the reason is that no data has been received from this probe, very similar to the No Probe Info section in the previous section. One additional piece of information on this screen is the time since the last data has been received, which may be useful to determine when probe data stopped being received. This information is also organized and summarized by Service Group, so it is somewhat easier to read.

If there is a red circle, you can consult the instructions in the previous section “[No Probe Information](#)” on page 156 in order to try to find the source of this problem.

Data Consolidation Displays Red Circle

If there is a red circle in this column in the status display, it means that the OVIS program which takes the incoming probe data and summarizes it and puts it into the Reporter Database has not done so. There are a couple of possible reasons for this.

- There is no data to consolidate. This goes back to the other status screens -
 - no data has been received from the probes.
- The Reporter service is not running. In the Windows 'Services' dialog, make sure that the Reporter service is running. You may want to stop and start the service to make sure that it is operational.
 - Open the Windows Control Panel and select **Services**.
 - Highlight the **Reporter Service** and press the **Start** button.

No Data Appears in the Dashboard

If no data appears in the Dashboard display, go into the Configuration Manager and check the status display. If you see green icons under Probe Data Received but red circles under Data Consolidation, your Reporter service may not be running correctly. Make sure the Reporter service is running by checking the **Services** dialog found in the Control Panel.

Looking at OVIS Trace Files

If the preceding troubleshooting has been unsuccessful, you may wish to turn on tracing and look at the OVIS trace files to look for potential problems. While these trace files are primarily for internal use, and a complete description is beyond the scope of this document, you may be able to discern some useful information by examining the text.

There are two types of trace files:

- Probe trace files
- OVIS Management Server trace files

The Probe trace files may be found in `<installdir>\probes\log` (or `<installdir>\Data\log` if the probes are running locally). They are called `error.log` and `trace.log`.

The OVIS Management Server trace files are found in the in the `<installdir>\Data` directory, and are named `trace.<programname>`. For example, the trace file for the OVIS module which receives the probe data via the web server would be called `trace.measEvent2`. The trace file for the program which moves data from the local storage (IOpsTraceTable) to the Reporter database is called `trace.iopscollector`. These files aid your Support representative in isolating OVIS issues and are primarily for their use.

<code>status.iops</code>	Main status
<code>status.PM</code>	Embedded custom graphs status
<code>status.Reporter</code>	Embedded reporting status
<code>trace.measEvent2</code>	trace for the measEvent2 dll
<code>trace.DllVersion</code>	trace for Reporter DLLs
<code>trace.iopscollector</code>	trace for iopscollector
<code>trace.IOpsConfig</code>	trace for the Configuration Manager
<code>trace.iopsmaint</code>	trace for the data maintenance
<code>trace.iopsslaevaluator</code>	trace for the SLAs
<code>trace.RepIOps</code>	trace for the Dashboard
<code>trace.RepCrys</code>	trace for the nightly reports
<code>trace.RepMaint</code>	trace for the database maintenance
<code>trace.ExportIOps</code>	trace for the ExportIOps program
<code>trace.IOpsLoad</code>	trace for the IOpsLoad program
<code>trace.Scheduler</code>	trace for the Scheduler program

trace.webrecorder trace for the Web Transaction Recorder

You can turn on tracing using the Internet Services Configuration Manager, under **File > Configure > Tracing**.

To do probe troubleshooting set tracing to 9, save the configuration, the modified configuration files will automatically be redeployed and the probes will log more information for use in troubleshooting. Be sure to set the tracing level back after you have completed the troubleshooting.

In the resulting trace file search for ERROR or WARNING and examine the text following for help in resolving the error. For example IOPS 1-11...gethostbyname indicates a typing error in the URL, IOPS 1-15 connection to web proxy or service target timed out indicates a problem reaching the web proxy or service target.

Database running out of space

If the database is getting too large, you can perform the following procedure.

Compressing the database

1 Stop the services used by Internet Services and find System DSN tab:

For Windows NT:

- a Open the **Control Panel** and double-click **Services**.
- b Select **HP Internet Services**, **IIS Admin Services**, and **Reporter Service** and click the **Stop** button.
- c Open the Control Panel, choose **Data Sources (ODBC)**

For Windows 2000:

- a Open the **Control Panel**, double-click **Administrative Tools** and double-click **Services**.
- b Right-click each service and select Stop.
- c Open the **Control Panel**, double-click **Administrative Tools**, and **Data Sources (ODBC)**.

- 2 Select the **System DSN** tab and highlight **Reporter Microsoft Access Driver (*.mdb)**.
- 3 Select the **Configure...** button and in the next window the **Compact...** button.
- 4 Restart all services.

OVO for UNIX Integration Enabled but not Working Properly

Symptom: OVO for UNIX integration enabled but no message shows up in the OVO Browser. Or the following message is logged in status.iops:
measEvent2 ERROR: Unable to locate VPO agent API - no VPO alarming possible (ret=1)

Resolution:

First make sure that the OVO for UNIX agent is installed and that the integration templates are working:

In OVIS:

- Make sure that the OVO for UNIX integration is enabled (in the Configuration Manager select **Configure > Alarm Destinations**).
- Make sure that an objective is set-up in the Configuration Manager that can trigger alarm messages (note, for testing, disable baselining (set to 0) and duration set to 1).

In OVO for UNIX:

- Verify that **OVIS Server Template Group** is assigned and distributed to the OVIS Management Server.
- Make sure that OVIS server node is part of a node group.
- Make sure that OVIS and OVIS_Err message groups are part of operators responsibility.

On the command line on the OVIS Management Server, run

```
opcmsg a=OVIS o=o msg_t=Test
```

This should produce a message in the OVO message browser.

If it doesn't, make sure that the system Path includes the location of the `opcapi.dll` (usually in `\usr\OV\bin\OpC` and/or `\usr\OV\bin\OpC\intel` directory). OVIS needs the OVO API library `opcapi.dll` in the system Path environment variable.

Settings > Control Panel > System applet: Environment

Add `\usr\OV\bin\OpC` and `\usr\OV\bin\OpC\intel` to the Path for the System Variables and reboot the system. Note, you may need to move the `\usr\OV\bin\OpC` and `\usr\OV\bin\OpC\intel` path components further towards the front of the Path statement.

If messages are still not forwarding to OVO, install the OVO agent, OVIS and IIS all on the same drive (for example C:).

Troubleshooting the HTTP_TRANS Probe

For problems encountered when using the Web Transaction Recorder to configure an HTTP_TRANS probe, please refer to the Web Recorder online help topics on Recording and Playback Issues and Web Recorder Tips.

Advanced Topics

This chapter includes advanced topics such as the following:

- “Internet Services Architecture and Data Flow”
- “Security”
- “How Internet Services Handles Security”
- “How to protect the Probe System”
- “Configuring Secure Communication - Probe and Management Server”
- “Supported Databases”
- “Database Backup”
- “Starting Over”
- “OVIS Version 3.5 Scalability Information”
- “NTFS Security Settings”

Internet Services Architecture and Data Flow

The following pages give a view of the basic data flow for each component of Internet Services.

Probes

Probes can be run locally on the Internet Services Management Server or be deployed, along with configuration information, to remote UNIX or Windows NT/2000 systems. Using remote probes allows you to measure service levels from different locations. The probes work by executing typical actions and measuring the response time, availability and other performance metrics for each service.

Types of probes include:

- HTTP, HTTPS, Web Recorder (HTTP_TRANS)
- ICMP (ping)
- FTP File Transfer
- DNS, DHCP, LDAP
- E-mail (POP3, SMTP, IMAP4)
- NNTP (Newsgroups)
- Radius
- Dial-up
- NTP
- TCP
- Streaming media
- Cisco X_SLAM

On the probe system, a scheduler component runs and decides when to launch the probes. Each probe is a separate executable that gets launched by the scheduler with appropriate service target information that comes from the configuration files.

The probe then takes measurements and saves the measurements in a queue file. Queue files are sent to the Internet Services Management Server using HTTP or HTTPS protocol.

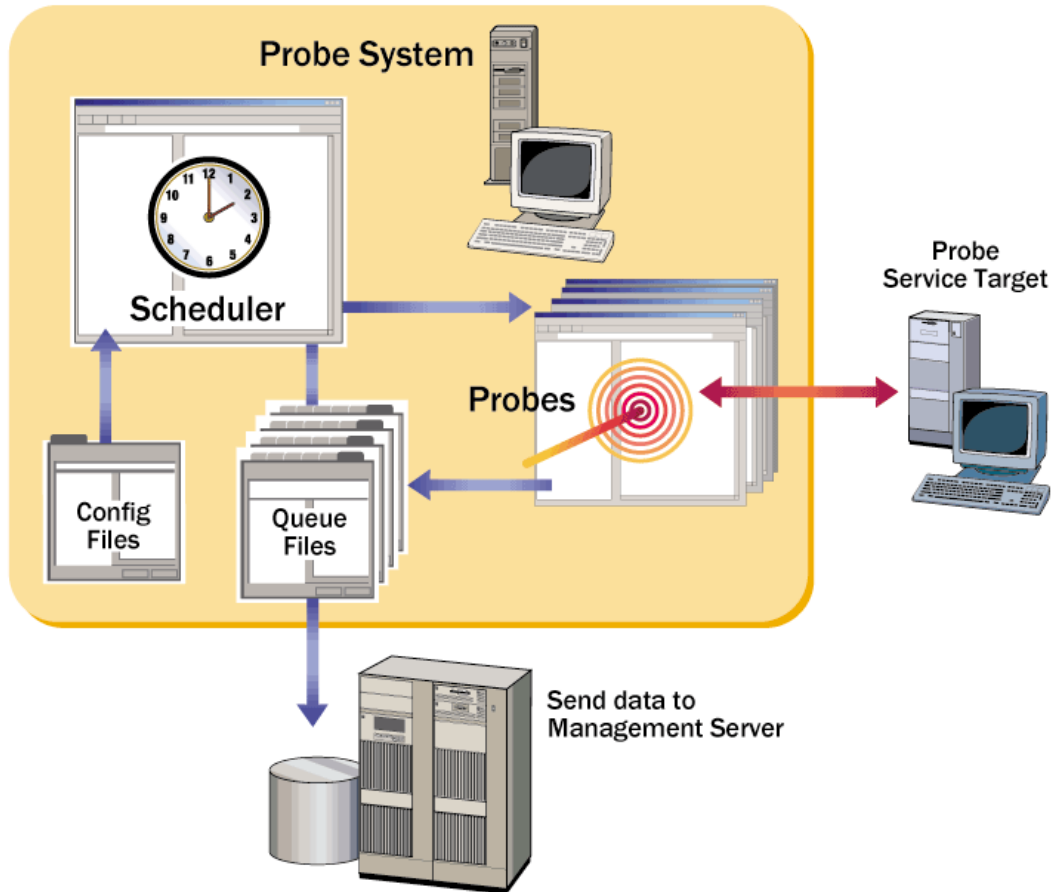


Figure 4 Data Diagram for the Probe Systems

Management Server

The probe sends the data it has gathered back to the Internet Services Management Server. The measurement receiver `measEvent2` writes the data to the measurement trace table `IopsTraceTable` data buffer (a transient data store).

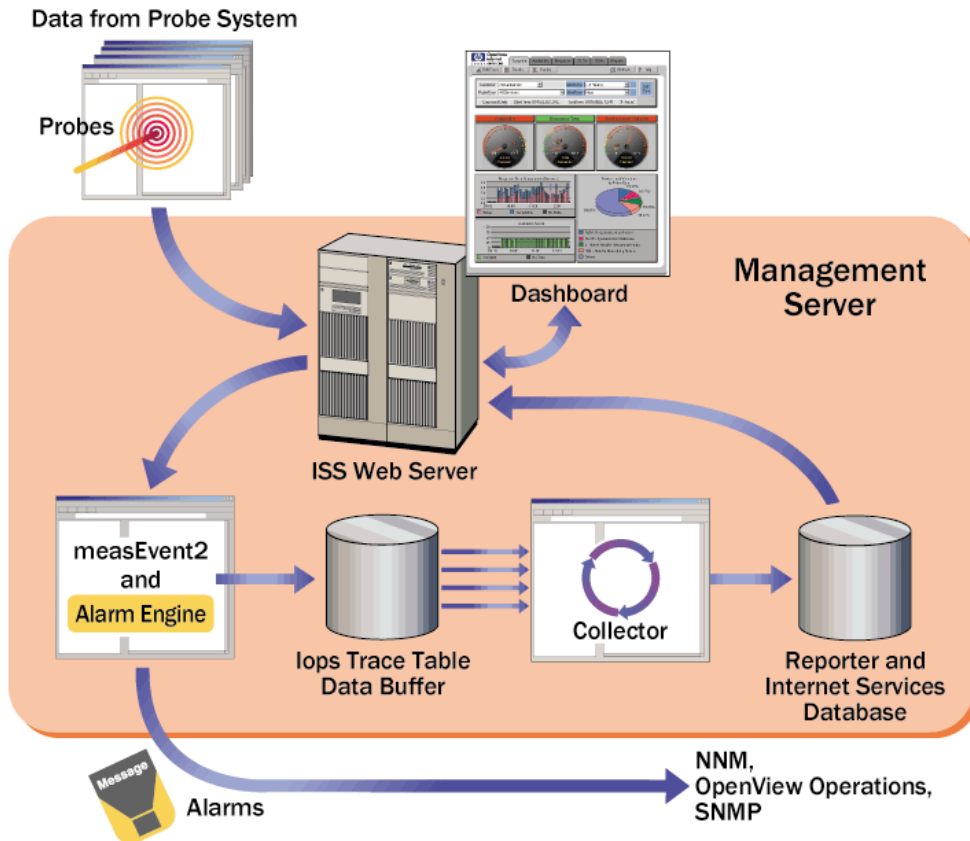
Periodically the collector component runs and does two things. It copies detail data from the `IopsTraceTable` into the Reporter database. And it aggregates `IopsTraceTable` data into service groups (based on the way you configured the services) and stores the data in the Reporter database. The data tables are as follows:

- `IOPS_DETAIL_DATA` for 5 minute probe/target level data
- `IOPS_DETAIL_DATA_HOURLY` for hourly probe/target level data
- `IOPS_DETAIL_DATA_DAILY` for daily probe/target level data
- `IOPS_PROBE_DATA_CACHE` for 5 minute service group level data
- `IOPS_PROBE_DATA` for hourly service group level data
- `IOPS_PROBE_DATA_DAILY` for daily service group level data

Alarms and messages are generated from the Alarm Engine within `measEvent2`, as the data comes in from the probes. Alarms are sent to other OpenView applications like Network Node Manager, OpenView Operations for UNIX and OpenView Operations for Windows, or any event manager capable of receiving SNMP traps.

The data from the Reporter database is displayed in the Internet Services Dashboard web interface in near real time graphs and nightly reports. Drill down data in the Dashboard comes from the IOPS_DETAIL_DATA table and the IOPS_DETAIL_DATA_HOURLY table.

Figure 5 Data Diagram for the Management Server



Service Level Agreements

A Service Level Agreement (SLA) is set based on service level objectives (SLOs) and evaluated to determine compliance. For example an SLA might indicate that response time for a service target must be less than 4 seconds. As another example, to set an availability SLA, you choose the service groups to monitor for this SLA, set an SLA conformance threshold to the total availability percent you wish to achieve.

SLAs are set up in the Internet Services Configuration Manager as are the SLOs.

The SLA evaluator evaluates incoming measurements and service level objectives and determines the SLA and SLO compliance. This compliance information is stored in the Reporter database.

As measurements arrive, the Alarm Engine (within MeasEvent2) evaluates each data point against the configured SLOs. The Alarm Engine logs this information about failed objective evaluations in the IOPS_SLO_VIOLATIONS_DATA table.

The SLA evaluator runs hourly and evaluates SLA conformance using this SLO information as well as information from the IOPS_PROBE_DATA table. The SLA and SLO conformance percentages for each interval are then stored in the IOPS_SLA_CONFORMANCE_DATA and IOPS_SLO_CONFORMANCE_DATA tables in the Reporter database..

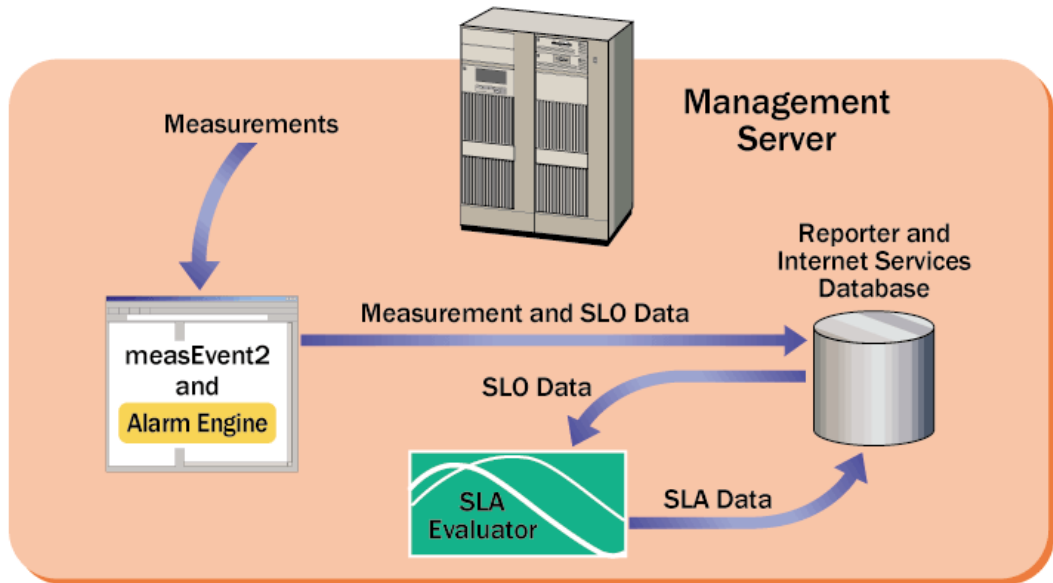


Figure 6 Data Diagram for Service Level Agreements

How to Move your Configuration to Another System.

Follow these steps to move your configuration from one system to another:

On the system you wish to copy the configuration from:

From a command prompt window, enter:

```
cd <installdir>\probes  
  
iopsload -save config.sysname.xml
```

Transfer the `config.sysname.xml` and the `httptrans.dat` file to the system where you wish to import the configuration in the `<install dir>\probes`. On that system:

From a command prompt window, enter:

```
net stop "HP Internet Services"  
  
net stop "IIS Admin Service" /y
```

NOTE: You will be informed that associated subservices are being stopped. Note down those names for use later.

NOTE: Pause 5 minutes to give Reporter Service a chance to do its last consolidation.

```
net stop "Reporter Service"  
  
iopsload -load config.sysname.xml
```

WARNING: If you have any remote probe systems in the configuration being transferred, you should stop HP Internet Services (for NT probes) or stop the Scheduler (Unix probes) on all those systems before proceeding.

```
net start "Reporter Service"
```

```
net start "World Wide Web Publishing Service"
```



The previous command will implicitly start IIS Admin Services. You may also wish to start any other subservice of IIS Admin Services that was stopped above.

Now enter the Configuration Manager and check that the configured customers and services have been successfully transferred. If so, press the **Save Configuration** (diskette) icon, and you should begin probing those targets.



If the configuration includes remote probes, you will have to redeploy the config.dat and httptrans.dat file from this system since the name of the system they are supposed to send their data to has now changed.

Security

Configuring Proxy/Port Settings

There are a number of places where a proxy or port can be used in Internet Services.

Proxy Settings in OVIS

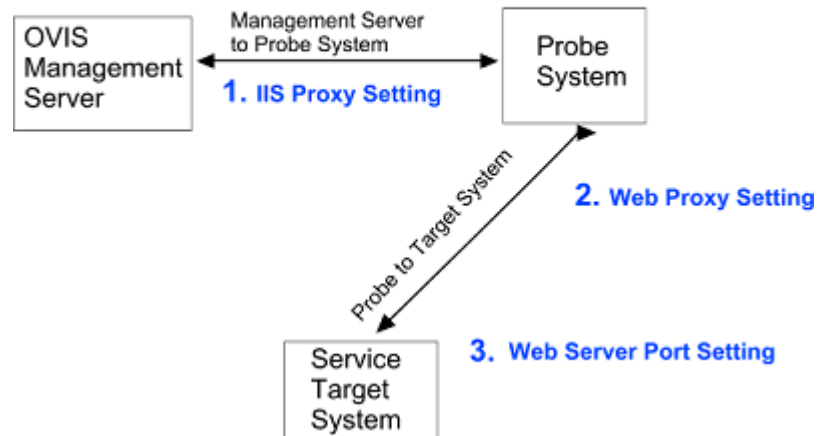


Figure 7 Proxy and Port Settings in Internet Services

The diagram shows the following:

- 1 You could have a firewall between your OVIS Management Server and your remote probes. In this case you need to go into the Probe Location Information dialog and change the Internal Internet Services Proxy information so that the OVIS management server and the remote probe system can send each other data.
- 2 You could have a firewall between the probe (local or remote) system and the service target system. In this case, if you are using HTTP, HTTPS, and/or HTTP_TRANS probes, you need to go into the Probe Location dialog and change the Web Proxy Information to the correct proxy and port for the data to flow between the systems.

- The target system may have a different port than the default port 80 in its TCP Port in IIS' Web Site Identification. In this case you need to go into the Web Pages Information dialog and change the Web Server Port to match the TCP Port in IIS.

HTTP - Web Pages Information

Address (URL)

(e.g. "www.hp.com") (e.g. "/country/us/eng/supportservices.htm")

http:// **www.hpshopping.com** /

3 Web Server Port **80**

Pattern Matching Information

Pattern

<none>

Pattern Matching Settings

<none>

Options

Load Images and Frames

Connection Keep-Alive

No Cache (Proxy)

Web Proxy Information

This is the proxy used by the probe to access the service targets.
For HTTP, HTTPS, HTTP_TRANS & STREAMING_MEDIA only

2 HTTP Proxy Address: <none> Port:

HTTPS Proxy Address: <none> Port:

Internal Internet Services Proxy Information

This is the proxy used by the probe to access the Internet Services server.

1 Proxy address: <none> Port:

Delete Connection

Probe Location Info

Probe Location **Local**

Probe Request Information

Measurement Interval

Request Timeout

Network Connection

Default

How Internet Services Handles Security

Internet Services installs with maximum restrictive security settings. Working with MS Internet Information Server (IIS), Internet Services probes for data and stores the values it retrieves in an MS Access database. For Internet Services to work with IIS in this way, the Internet Services DLLs must have the appropriate permissions. Internet Services uses both NTFS and IIS security settings to allow data to be retrieved/stored and can also prevent unauthorized access to the data. The Windows NT or Windows 2000/IIS administrator can adjust security settings if less security is desired. But be aware that lowering security settings or allowing anonymous access to additional functionality can have serious implications as it could allow users access to sensitive data. Security for IIS is handled at two levels, the NTFS (NT Filesystem) level and the IIS level. Using FAT (File Allocation Table) file systems is not supported as it does not allow specific permissions to be set. Also, note that in order to reflect changes to NTFS permissions in IIS, you need to stop and restart IIS.

Firewalls: Returning Data Through the Firewall

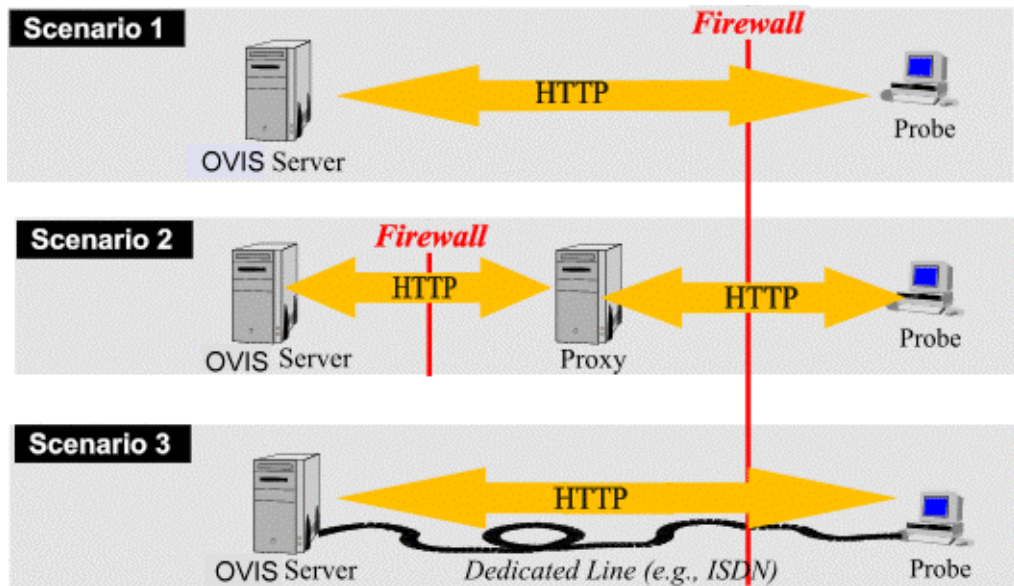
Internet Services probes use standard HTTP protocol to send measurements to the Internet Services server. Probes send HTTP POST requests, using port 80 on the Internet Services server as the default. The Management Server's URL as:

http://<management server>/HPOV_IOPS/isapi/measEvent2.dll

How Probes Can Communicate through a Firewall

Internet Services probes use HTTP POST to send data back to the Internet Services Management Server. If a firewall exists around the server, the probe must have an open port through which it can return its

collected data. The following scenarios show three common configurations for how a probe might return data through a firewall to the Internet Services server:



In Scenario 1, the Internet Services Management Server sits right behind the firewall. This setup requires that the probe talk to the Management Server on port 80 (which is configurable). It is recommended that you set up the firewall to block anything that comes to the Management Server except TCP packets originating from the probe system with the Management Server/port 80 as destination.

In Scenario 2, a proxy server can be used to relay probe data to the Management Server residing inside the firewall. This effective security scenario requires only that a simple proxy server be setup. A compromised proxy server does not affect the rest of the ISP because the proxy runs a simple HTTP forwarder process.

In Scenario 3, the probe uses a dedicated line, such as ISDN, to send measurements to the Internet Services server. This setup makes spoofing of IP packets more difficult since the dedicated line is not vulnerable to attacks from the Internet.

How to protect the Probe System

If the probe system is outside the firewall or in an unprotected site, it should be protected from attacks that can come from the Internet. A probe system has basically two ways to send measurements back to the Internet Services server:

- Through the Internet (scenarios 1 and 2)
- Through a dedicated line into the Intranet (no route between Internet and Intranet).

The first two scenarios allow attacks on the returned data, such as in cases where packets can be intercepted and altered. However, since no sensitive information is transmitted, such an attack is not too critical. The third option, is where a dedicated line such as ISDN is used to send measurements from the probe system to the Internet Services server. This makes spoofing of IP packets harder since a separate line into the Intranet exists. However, since a dedicated line exists into the Intranet, this may circumvent security measures taken on the outside firewall.

With all options, it is recommended that the probe system be secured by a personal firewall product and/or that no system ports (ports <1024) are open on the probe system. This eliminates attacks on standard services such as HTTP, FTP, etc.

With the second option, the outside firewall should only allow packets from the probe system that come from the dedicated line (port \geq 1024) to the Internet Services server.

Using Secure Probe/Server Communication

Internet Services supports SSL secured communication between the probe system and the server. The basic security only requires the server certificate to be installed on the probe system. To further enhance security, a client certificate for the probe system can be installed. The certificate format used by the probe system must be **Base64 encoded X.509**. See chapter 7 “[Configuring Secure Communication - Probe and Management Server](#)” on page 179 for more information.

Configuring Secure Communication - Probe and Management Server

Internet Services supports SSL secure communication between the probe system and the server. The basic security only requires the server certificate to be installed on the probe system. To further enhance security, a client certificate for the probe system can be installed.

The certificate format used by the probe system must be **Base64 encoded X.509**.

Server Certificates



Please follow the IIS documentation for setting up a secure web server. Once you have set up a secure server, ALL probe locations will have to use secure communication.

A client certificate will also be required by the Configuration Manager if communication is further secured by the use of Client Certificates.

- 1 Stop all probing on each of the probe locations (local and remote).
 - On Windows:** `net stop "hp internet services"`
 - On UNIX systems:** `cd /opt/OV/VPIS/probes`
 `./Scheduler -k`
- 2 To enable secure communication, create a server certificate for IIS server on the Internet Services Management server system (see IIS product online help).
 - a Run Internet Service Manager (IIS) program and navigate to `HPOV_IOPS/isapi` in the left tree pane under Default Web Site.
 - b Right click `measEvent2.d11` and select **Properties**.
 - c Go to File Security and click on the **Key Manager** button.
 - d Create a key and forward the key request to your certificate authority.
 - e Once the server certificate has been imported, click **Edit...** under the Secure Communications group box.

- f Click **Require Secure Channel when accessing this resource**. Press **OK** and exit the Internet Service Manager (IIS).

Repeat Step 2b and 2f above for `DistribMgrExt.dll` (right-click `DistribMgrExt.dll` and select **Properties** then Click **Require Secure Channel** when accessing this resource).

- 3 Now test secure access to `measEvent2.dll` with a browser. In order to avoid authentication errors, import the server certificate and its CA certificate in the browser. When accessing the following URL, you should not get a security warning in Internet Explorer:

https://<ovis_server>/HPOV_IOPS/isapi/measEvent2.dll?Refresh

An empty page should be shown in Internet Explorer as the result of the above URL.

- 4 Export the server certificate and the CA certificate in Base64 encoded X.509 format through Internet Explorer.
 - a In Internet Explorer on the Internet Services Management Server, select **Tools->Internet Options->Content->Certificates...**
 - b Find and select the server certificate and export it in Base64 encoded X.509 format.
 - c Do the same for the CA certificate.
 - d Append the two exported certificates to the file **trusted.txt** in the `<install_dir>\probes` directory (create it if it is not present).
- 5 In the Internet Services Configuration Manager, enable secure communication (**File->Config->Web Server Properties**). Press **Save**. Distribute the **trusted.txt** file to EACH remote probe location. The other configuration files will be automatically distributed to remote probe systems.
- 6 Restart the Internet Services services on each probe location (local and remote).

On Windows:	<code>net start "hp internet services"</code>
On UNIX systems:	<code>cd /opt/OV/VPIS/probes</code>
	<code>./Scheduler</code>
- 7 In the Internet Services Configuration Manager, verify in the **Status** view that probe measurements are received.

Client Certificates

Security can be further strengthened by installing client certificates on each probe location. Client certificates must be in Base64 encoded X.509 format and MUST contain the private key. Creation of client certificates depends on the certificate server or authority you are using.

- 1 Stop all probing on each probe system (local and remote):

```
On Windows systems: net stop "hp internet services"
On UNIX systems:    cd /opt/OV/VPIS/probes
                   ./Scheduler -k
```

- 2 Create client certificate and be sure it is Base64 encoded X.509 format. Then be sure it is installed in the `<install_dir>\probes` directory with the name `clientcert`. All probe locations shared the same certificate file name and password! However, the certificates can be different.
- 3 The client certificate is required by the Configuration Manager. Add the client certificate to the certificates of all users using the Configuration Manager. This can be accomplished by loading the client certificate in Internet Explorer.
- 4 Once the certificates are in place (`<install_dir>\probes\clientcert`), enable client certificate checking in Internet Service Manager (IIS).
 - a Navigate to **HPOV_IOPS/isapi** in the left tree pane under Default Web Site.
 - b Right click on `measEvent2.dll` and select **Properties**.
 - c Go to File Security and click on the **Edit** button in the Secure Communications group box.
 - d Click **Require Client Certificate**. Press **OK** and exit the Internet Service Manager.

Repeat Step 3b, 3c and 3d above for `DistribMgrExt.dll`.

- 5 Import the client certificate in Internet Explorer and access

https://<ovis_server>/HPOV_IOPS/isapi/measEvent2.dll?Refresh

The imported certificate should pop-up in a select box with the client certificate name and access to the URL should be granted (empty page, no error).

- 6 In the Internet Services Configuration Manager, set the password that is used to protect the `clientcert` file (**File->Config->Web Server Properties**). Press **Save**. Distribute the `clientcert` file to each remote probe location.
- 7 Restart the Internet Services services on each probe location (local and remote).
On Windows: `net start "hp internet services"`
On UNIX systems: `cd /opt/OV/VPIS/probes`
 `./Scheduler`
- 8 In the Internet Services Configuration Manager, verify in the **Status** view that probe measurements are received.

For 403.7 Forbidden: Client certificate required in IE

When you test your client certificate in Internet Explorer and get the above error, verify that the client certificate is present in the browser.

If an empty selection box pops-up, it may be that the server doesn't have the root CA certificate installed that signed the client certificate. To install the root CA certificate, run Internet Explorer on the web server system. During the second step of the Install Wizard, select the radio button **Place all certificates into...**, then press **Browse**. A window with the certificate stores opens. Click on the check box **Show physical store** and select **Trusted root certificate authority**. Then select the node local computer and continue with the installation.

See also Q218445 in Microsoft's Support Database.

For Microsoft Certificate Server

With Microsoft Certificate Server 1.x, there is no way of getting the private key included in the client certificate export. Therefore, import the key in Internet Explorer and export it from Internet Explorer in PKCS #12 format (make sure to click on Export private key). Then use the openssl tool (www.openssl.org) to convert the PKCS #12 format into Base64 encoded X.509 format (`openssl pkcs12 -in <pxf file> -out <ber file>`).

Custom Reports

If you want to create your own custom reports for display in the Dashboard Reports tab, you need to use Crystal Decisions Crystal Reports version 8.5 or higher (www.crystaldecisions.com) and the hp OpenView Reporter product version A.03.00 or higher.

Use Crystal Reports to create the custom report and hp OpenView Reporter to configure the report to be viewed in Internet Services. Documentation on setting up reports to be generated and viewed is provided in the Reporter Concepts Guide. Also refer to the Reporter online help topic *Add report definition* for details.

Once you've created a custom report, then to integrate a custom report into Internet Services do the following:

- 1 To integrate a custom report template put the custom report template in the `data/reports/iops/` folder.
- 2 Use hp OpenView Reporter to add your custom report. Be sure to set the following:


```
CATEGORY = 190 Internet Services
HTML_DIRECTORY = webpages\<a\_custom\_report\_1>
```

 Where `<a_custom_report_1>` is the report name in the webpages relative directory. Refer to the Reporter documentation for how to do this.
- 3 Let your custom probe run overnight. Next day the nightly report for your custom probe should show up under the Reports tab of the Internet Services Dashboard.

Supported Databases

Internet Services and Reporter share the same database for storing performance and reporting information. The default database from OVIS 3.5 was MS Access and the default database from the OVIS 4.0 release is MSDE. You may choose to change to one of the following supported databases:

- Oracle 8.0.6 for Solaris or HP-UX
- Oracle 8.1.6/8.1.7 for Solaris or HP-UX
- SQL Server 7 (if already setup with a previous version of OVIS) or 2000

There are several databases scenarios possible depending on which OpenView products you have installed.

If you have Reporter on the same system as Internet Services is already or will be installed:

When you install OVIS, it will detect whatever database is configured for Reporter and use this same database. The OVIS installation configures a connection to this database and adds table entries for OVIS as needed.

If you do not have Reporter and are installing Internet Services 4.0 for the first time

The MSDE default database is installed. You can later use instructions in the *Reporter Database Configuration Guide* provided with Internet Services for configuring an Oracle or SQL Server database instead.

If you do not have Reporter and are updating from a previous version of Internet Services to OVIS version 4.0

The upgrade to 4.0 uses the existing database, it could be MS Access, Oracle or SQL Server 7. With Access, you can later use instructions in the *Reporter Database Configuration Guide* provided with Internet Services for configuring an Oracle or SQL Server database instead.

If you do not have Reporter on the system but for some reason you have SQL 7 installed but not configured for use with OVIS and install Internet Services 4.0 for the first time.

The install will install MS Access as the database not the typical default MSDE. This is because SQL 7 and MSDE are not compatible.



WARNING: Migration of data from your old database to the new database is not supported for Internet Services. And if Internet Services is on the same system as Reporter, attempting to migrate data to the new database will result in problems in Internet Services.

See the *Reporter Database Configuration Guide* (Reporter_Database_Config.pdf) for instructions on configuring Oracle and SQL Server databases. For your convenience this document pulls the information on database configuration out of the *OpenView Reporter Installation and Special Configuration Guide* and includes it with your Internet Services product.

Database Backup

We recommend that you follow your usual procedures for backing up the Reporting database used by Internet Services.

First stop the following services:

- Reporter Service
- "HP Internet Services Service"
- World Wide Web Publishing Service

Then backup the database according to your usual procedures. Some suggested procedures are provided below for MSDE.

For the default database

If you use the default MSDE database, backup procedures are available and described on the Microsoft Web site. The below mentioned options use Microsoft utilities. Please refer to the Microsoft documentation for supportability issues or errors that may occur when using these procedures.

Option #1, for MSDE using SQL Client tools:

If SQL 2000 Client Tools are installed, use SQL Enterprise Manager to back up you MSDE database.

Option #2, for MSDE using neither Access 2000 nor SQL Enterprise Manager:

If you have only MSDE installed, you can use the TSQL BACKUP DATABASE command and execute with Osq.exe (command line Query tool).

MSDN as well as the SQL online books provide detail on how to use the stored procedures outlined below. Create a backup/detach/restore, etc. procedure, by enter syntax as described below.

NOTE: The steps below provide an example of how to use the various stored procedures with MSDE to perform a backup or restore. You may want to customize the steps for your particular environment. Some additional things you might want to do are to create a daily backup job, or

to produce a daily backup report. Refer to Microsoft (MSDN) documentation on the `osql` utility, `BACKUP DATABASE` and `RESTORE DATABASE` for other options and features. Be sure and verify that you backup and restore work correctly.

Certain defaults have been chosen in this example. You may be required to change the directory name, user name and password.

Example Backup Steps if you have only MSDE installed

- 1 Stop the "Reporter", "HP Internet Services", and "W3SVC" services and make sure that no other client tools are accessing the Reporter/Internet Services MSDE database.
- 2 Create a backup device and then backup the MSDE database as follows:
From a command prompt

```
c:\>osql -S.\OVOPS -Usa -P
1>USE Reporter
2>BACKUP LOG Reporter WITH TRUNCATE_ONLY
3>sp_addumpdevice 'DISK', 'Reporter_BKUP',
'C:\Program Files\HP Ope-
niew\Data\Dataases\backup\Reporter_1.bak'
4>BACKUP DATABASE Reporter TO Reporter_BKUP WITH
INIT, STATS
5>sp_dropdevice 'Reporter_BKUP'
6>go
The database will be backed up...
1>exit
```

- 3 Re-start the "Reporter", "HP Internet Services", and "W3SVC" services.

Example Restore Steps

- 1 Stop the "Reporter", "HP Internet Services", and "W3SVC" services and make sure that no other client tools are accessing the Reporter/Internet Services MSDE database.
- 2 Restore the backup of the MSDE database as follows:
From a command prompt

```
c:\>osql -S.\OVOPS -Usa -P
1>USE Master
2>RESTORE DATABASE Reporter FROM DISK='C:\Program Files\HP OpenView\Data\Data-
bases\backup\Reporter_1.bak' WITH RECOVERY,
REPLACE, STATS
3>go
4>BACKUP DATABASE Reporter TO Reporter_BKUP WITH
INIT, STATS
5>sp_dropdevice 'Reporter_BKUP'
6>go
The database will be restored...
1>exit
```

- 3** Re-start the "Reporter", "HP Internet Services", and "W3SVC" services.

Starting Over

This section covers how to return Internet Services to its original state. You can use this procedure to remove trial configurations and "start over." You can also use it to preserve your configuration but rebuild the database. Rebuilding the database may be required if the database becomes corrupted or if you want to remove all data that was collected and start again.

The current release of Reporter and Internet Services use MSDE as the default database, while previous releases used MS Access. Removing all data from either default database differs. The differences are noted in the procedure below.

Restarting other products running the reporting services

THIS PROCEDURE RESTARTS OTHER PRODUCTS RUNNING THE REPORTING SERVICES. IF YOU HAVE REPORTER OR WEB TRANSACTION OBSERVER INSTALLED, CONSULT THE PRODUCT DOCUMENTATION BEFORE PERFORMING THIS PROCEDURE.



This procedure will permanently remove Internet Services data.

Before you begin you may want to save the current Service configuration information so it can be reloaded later. Open an MS DOS Command Prompt window. Enter the following to transfer all the current configuration data to an xml file:

```
iopsload -save myconfig.xml
```

where you substitute a file name for *myconfig.xml*. This file is created and filled with an XML description of your configuration information.

Recreating MSDE Database

The following steps cover deleting an existing MSDE Reporter/Internet Services database and recreating a new MSDE database. The script that you run must be executed from the `../bin` directory where `newdb.exe` resides.

- 1 Stop the Internet Services components:
 - a Reporter Service
 - b "HP Internet Services"
 - c World Wide Web Publishing Service
- 2 Be sure the Reporter GUI and Internet Services Configuration Manager, and Dashboard are closed.
- 3 Open an MS-DOS command window.
- 4 Use the change directory (`cd`) command to change to the `<install dir>/bin` directory.
- 5 Type the following command at the command prompt:
`cscript RecreateMSDEDB.vbe`
- 6 Check the `<install dir>/Data/status.Reporter` file for the status of `newdb`.
- 7 **Optional:** restore the saved configuration information.
 - a start an MS DOS Console window
 - b run the `iopsload` program to transfer the xml file back into the database `iopsload -load myconfig.xml` where `myconfig.xml` is the same file name used earlier.
- 8 From the Start menu select **Settings>Control Panel>Services** and restart Internet Services components:
 - a Reporter Service
 - b "HP Internet Services"
 - c World Wide Web Publishing Service

Recreating SQL Server Database

The following steps cover deleting an existing SQL Server Reporter/Internet Services database and recreating a new SQL Server database. The script that you run must be executed from the `../bin` directory where `newdb.exe` resides.

- 1 Stop the Internet Services components:
 - a Reporter Service
 - b "HP Internet Services"
 - c World Wide Web Publishing Service
- 2 Be sure the Reporter GUI and Internet Services Configuration Manager, and Dashboard are closed.
- 3 On the database system, select the following from the control panel: **Start> Programs> Microsoft SQL Server> Enterprise Edition.**
- 4 In the dialog that is displayed open the tree in the left pane to: **Microsoft SQL Servers> SQL Server Group> <your server machine name> Database> Reporter** and right-click **Delete**. This will delete the database.
- 5 To recreate the database open the tree in the left pane as described above and right-click **New Database**. Enter Reporter and an initial size, and the database is recreated. Refer to the instructions in the database configuration documentation for more information (`Reporter_Database_Config.pdf`).
- 6 Open the Configuration Manager on the Management Server and this will run the `NewDB.exe` program to rebuild the Internet Services tables.
- 7 **Optional:** restore the saved configuration information.
 - a start an MS DOS Console window
 - b run the `iopsload` program to transfer the xml file back into the database `iopsload -load myconfig.xml` where `myconfig.xml` is the same file name used earlier.
- 8 From the Start menu select **Settings>Control Panel>Services** and restart Internet Services components:
 - a Reporter Service

- b "HP Internet Services"
- c World Wide Web Publishing Service

Recreating the Access Database

The following steps cover deleting an existing Access Reporter/Internet Services database and recreating a new Access database. The script that you run must be executed from the `../bin` directory where `newdb.exe` resides.

- 1 Stop the Internet Services components:
 - a Reporter Service
 - b "HP Internet Services"
 - c World Wide Web Publishing Service
- 2 Be sure the Reporter and Internet Services Configuration Manager and Dashboard are closed.
- 3 If you want to save existing data, rename the database; if you do not need to save existing data, delete the file `\<install dir>\data\datafiles\Reporter.mdb`
- 4 For Windows 2000 systems: Select **Start>Settings>Control Panel>Administrative Tools>Data Sources (ODBC)**
or
For Windows NT systems: Select **Start>Settings>Control Panel>Data Sources (ODBC)**
- 5 Select the System DSN tab and within the System Data Sources: select Reporter and click the Configure... button.
- 6 In the window that appears click the Create... button.
- 7 In the New Database window browse to the `\<install dir>\data\datafiles\` directory and in the Database Name text box type Reporter and click OK.
- 8 Now create the Reporter tables within the database by running the `\<install dir>\bin\NewDB.exe` program.
- 9 **Optional:** restore the saved configuration information.
 - a start an MS DOS Console window

- b run the `iopsload` program to transfer the xml file back into the database `iopsload -load myconfig.xml` where `myconfig.xml` is the same file name used earlier.
- 10 From the Start menu select **Settings>Control Panel>Services** and restart Internet Services components:
 - a Reporter Service
 - b "HP Internet Services"
 - c World Wide Web Publishing Service

Recreating the Oracle Database



This will remove the Internet Services specific tables only. Additional Reporter tables will not be removed. Refer to the *Reporter Installation and Special Configuration Guide* for more on removing data from the Oracle database. And if you have other OpenView products using this same reporting database, refer to their product documentation for how to remove tables specific to these products.

- 1 Stop the Internet Services components:
 - a Reporter Service
 - b "HP Internet Services"
 - c World Wide Web Publishing Service
- 2 Be sure the Reporter and Internet Services Configuration Manager and Dashboard are closed.
- 3 On the Windows systems where Internet Services is installed copy the file `<install dir>\newconfig\oracle\hp-ux or sun directory\DropIOPS.sql` (entering either the `hp-ux` or the `sun` directory) to the UNIX system in the directory `$ORACLE_HOME/dbs/`
- 4 On the UNIX system where the Oracle database is installed, verify that for the current Oracle session, the `ORACLE_SID=REPORTER`.
- 5 Log on as `oracle` and at the oracle prompt, enter `svrmgrl` to start the Oracle Server Manager program.
- 6 At the `SVRMGR>` prompt, enter `connect internal`.

- 7 Enter the following to remove data from the database:
`@ORACLE_HOME/dbs/dropIOPS.sql`
- 8 Now create the Reporter and Internet Services tables within the database by running the `\<install dir>\bin\NewDB.exe` program.
- 9 **Optional:** restore the saved configuration information.
 - a start an MS DOS Console window
 - b run the `iopsload` program to transfer the xml file back into the database `iopsload -load myconfig.xml` where `myconfig.xml` is the same file name used.
- 10 From the Start menu select **Settings>Control Panel>Services** and restart Internet Services components:
 - a Reporter Service
 - b "HP Internet Services"
 - c World Wide Web Publishing Service

OVIS Version 3.5 Scalability Information

Scalability consideration is divided between (remote) probe system and the central management server. The following sections will provide some hardware configurations and sizing information.

In general, Internet Services scalability depends on

- The number of individual targets
- The number of customers and service groups
- The number of targets within a service group
- CPU speed and number of processors
- Speed of the network and hard disks
- The database product (Access, SQL Server, Oracle)
- Number of remote probes
- OS configuration (e.g. NT 4.0/Windows 2000, Unix kernel configuration such as number of processes, open files per process etc.)
- Memory, CPU and network bandwidth requirement of the probe
- The HTTP_TRANS probe in Internet Explorer (IE Heavyweight) mode requires significant CPU and memory resources which can limit the number of parallel executions of this probe type. Too many parallel executions may cause aborts of the probe program probehttptrans2.exe. In such a case limit the concurrency in the Probe Location dialog of the Configuration Manager to 2 or create a new network connection. Network connections are executed separately, one after the other, and allow you to control the concurrency of probe executions.

Probe System

The probe system is responsible for probing all configured targets. The limiting factors are:

- The performance of the system
- The number of parallel probe executions

- The speed of the network equipment

With parameters such as the number of targets, the number of probes executed in parallel, the interval and timeout, it is possible to calculate the number of required probe systems. The model assumes the worst-case scenario where all probe executions time out and report unavailability.

The following equation can be used to calculate the number of probe systems needed to support a given number of targets:

$$NumSystems = \frac{\frac{targets}{parallel} \times timeout}{interval}$$

The result of the above equation must be rounded to the next integer.

Examples:

In the following example it would take .20 probe systems to run 100 targets in a five minute interval with a 20 second per target timeout. You round the .20 up to 1 probe system required.

$$NumSystems = \frac{\frac{100}{32} \times 20}{300} = 0.20 \Rightarrow 1$$

targets = 100
 parallel = 32
 timeout = 20 (seconds)
 interval = 300 (seconds)

In the following example you want to find out how many targets can you have running on one probe system. If the number of probes that could execute in parallel was 32 (the default) and you had a 20 second timeout per target, then you solve the equation for the number of targets. You could run 480 targets in 5 minutes on a single system.

$$1 \text{ probe system} = \frac{\text{NumTargets}}{32} \times 20$$

$$= \frac{3000}{32} \times 20$$

The following examples show how the requirement for multiple probe systems is calculated.

targets = 3000
 parallel = 32
 timeout = 20 (seconds)
 interval = 600 (seconds)

$$\text{NumSystems} = \frac{\frac{3000}{64} \times 20}{600} = 1.56 \Rightarrow 2$$

targets = 3000
 parallel = 64
 timeout = 20 (seconds)
 interval = 600 (seconds)



The other factors such as network bandwidth and OS overhead can influence the result. For example, some probes are more demanding than others (e.g. FTP uses two network connections whereas most of the other probes use only one or HTTPS requires more CPU cycles for the encryption and decryption of data packets). Also HTTP_TRANS probe in IE mode requires significantly more resources than a regular probe.

The following table lists three typical hardware configurations and the max parallel probe execution that can be achieved on those systems with OVIS version 3.5 (see OVIS 4.0 Scalability for details on that release):

Table 5 Parallel probe execution hardware configurations

Hardware	Max. Parallel probe execution
Pentium Pro/150 MHz, 128 MB, single processor, NT 4.0	32
Pentium III/500 MHz, 256 MB, single processor, NT 4.0	128
HP 725/100, 128 MB, single processor, HP-UX 11.0	128

Management Server

Sizing the management server for scalability depends on the number of customers, service groups, targets and remote probe systems. The more customers and service groups, the greater are the performance demands on the system. It is always recommended to exclusively use the management server system for Internet Services and to use either SQL Server or Oracle databases.

The following table lists some typical configurations with OVIS version 3.5 (see OVIS 4.0 Scalability for details on that release):

Table 6 Management server configurations

Hardware	Configuration
Pentium III/500 MHz, 256 MB, single processor, NT 4.0	<ul style="list-style-type: none"> • Database: Access • Customers: 15 • Service Groups: 44 (total) • Targets: 100 (total) • Probe Systems: 1 (local), 5-minute interval

Table 6 Management server configurations (Continued)

Hardware	Configuration
Pentium III/733 MHz, 650 MB, two processors, Windows 2000	<ul style="list-style-type: none"> • Database: SQL Server 7 • Customers: 10 • Service Groups: 20 • Targets: 100 (total) • Probe Systems: 5 (remote), all 5 probe systems are probing the same targets every 5 minute
Pentium III/700 MHz, 1 GB, four processors, Windows 2000 (Datacenter)	<ul style="list-style-type: none"> • Database: SQL Server 2000 • Customers: 2000 • Service Groups: 6000 (total), 3 per customer • Targets: 6000 (total), • Probe Systems: 2 (remote), 10-minute interval, each system handles 3000 targets (1000 customers, 3000 service groups)

Due to compaction of measurements that are older than one day, database growth is linear with "24 times number of service group" records.

A variety of scenarios could occur with Internet Services probes, all of which cannot be covered in this short section. To date, Internet Services has been tested extensively on systems with the following hardware:

- 600 MHz Pentium III single processor
- 256 MB Memory

Probe stress factors

The number of probes that successfully monitor services from a single Internet Services server are affected by the following:

- service target availability (unavailable service targets cause probes to timeout, slowing the succession of sequentially executed probes)

- timeout value (longer timeouts can decrease scalability; see preceding point)
- measurement Interval (longer measurement intervals increase scalability; fewer data samplings allow more sequential data gathering)
- local or remote probe location

Network Usage

Each HTTP probe over a five-minute interval created approximately 65 Kb of network traffic. Actual network usage is dependant on the size of the Web page being monitored. For example, 500 HTTP targets create approximately 32 MB of network traffic during a five-minute internal.

Testing Scenario

The example below with OVIS version 3.5 (see OVIS 4.0 Scalability for details on that release) shows testing of 32 concurrent processes which included the conditions as listed and showed results as follows:

- All the configured URL service targets are unavailable all of the time.
- The configured Measurement interval /timeout value
- $32 = \text{number of targets measured (per Monitored Service) is } 300 \text{ seconds} / 45 \text{ seconds} * 32 = 213 \text{ URLs.}$
- Actual test results include only Web page-loading measurements with availability of 90%.
- 2000 HTTP targets in 5 minutes, probe running on local system.



Remote probe scalability tests are not yet complete.

Across the various NT/UNIX environments results are likely to vary due to the service target availability, remote/local probe locations, length of the measurement interval, network performance, Internet traffic, proxy server performance, and Internet Services Management Server performance. The above results shown in the maximum testing scenario apply only to HTTP targets.

OVIS Version 4.0 Scalability Information

OVIS version 4.0 can scale to meet a number of different requirements, depending on the size of the network being monitored, and the systems available to perform the probing and consolidated data collection. The following examples describe the load placed on OVIS systems under a number of different environments.

Standalone OVIS

Table 7 Standalone Configurations

System	Targets	CPU Utilization	Memory Required	Cycle Time*	Con-currency
Dual 400MHz PII 256MB	550	15%	300MB	2.0 Minutes	32
Dual 400MHz PII 256MB	1050	33%	350MB	3.0 Minutes	32
Dual 400MHz PII 256MB	1550	52%	400MB	3.5 Minutes	32
Single 1.7GHz P4 512MB	1550	42%	400MB	3.0 Minutes	32
Single 1.7GHz P4 512MB	1550	48%	400MB	2.2 Minutes	64

* Cycle Time refers to the time it takes to perform all probing.

Distributed OVIS: Remote Probes

- Probe System 1: Dual 400MHz PII 256MB
- Probe System 2: Dual 200MHz PII 256MB
- Probe System 3: Single 1.0GHz Celeron 1.0GB
- Server System: Single 1.7GHz P4 512MB

Table 8 Distributed Configuration - Remote Probes

Targets	CPU (Server)	Memory Required	CPU (Probe 1)	CPU (Probe 2)	CPU (Probe 3)
550	3.5%	300MB	13%		
1250	5%	400MB	35%		
2700	15%	650MB	35%	45%	
4000	30%	725MB	35%	45%	50%

Distributed OVIS: Remote Probes and Remote SQL Server

- Probe System 1 (Pr1) (1500 targets): Dual 400 MHz PII 256MB
- Probe System 2 (Pr2) (1500 targets): Dual 200MHz PII 256MB
- Probe System 3 (Pr3) (1500 targets): Single 1.0GHz Celeron 1000MB
- Probe System 4 (Pr4) (1500 targets): Single 500MHz PIII 256MB
- Probe System 5 (Pr5) (1500 targets): Single 500MHz PIII 256MB
- Probe System 6 (Pr6) (1500 targets): Single 733MHz PIII 256MB
- Probe System 7 (Pr1) (1500 targets): Single 350MHz PII 196MB
- Server System: Single 1.7GHz P4 512MB
- SQL Server System: Single 1.7GHz P4 1000MB

Table 9 Distributed Configuration - Remote Probes and Remote SQL Server

Targets	OVIS Server CPU	DB Server CPU	Pr1 CPU	Pr2 CPU	Pr3 CPU	Pr4 CPU	Pr5 CPU	Pr6 CPU	Pr7 CPU
4500	7.5%	8.0%	45%	54%	64%				
6000	9.0%	10.5%	45%	54%	64%	62%			
7500	11.5%	13.0%	45%	54%	64%	62%	84%		
9000	13.5%	15.5%	45%	54%	64%	62%	84%	51%	
10500	15.5%	17.0%	45%	54%	64%	62%	84%	51%	93%

Notes:

- Remote probes required approximately 180MB of memory for 1500 targets.
- Memory requirements on the system running SQL Server depend on the SQL configuration.
- Dashboard response time is optimized in the distributed solution.
- SLA evaluation takes place once an hour and uses a moderate amount of the CPU of both the OVIS management server and the DB server.
- For very large environments, the status screens in the Configuration Manager take a very long time to complete.

Conclusions

The optimal hardware configuration is to have all probes be remote; and to use separate systems for the OVIS Management Server and for the Database Server. This offloads and distributes the most CPU-intensive task, which is the probing. It allows the database overhead to be offloaded to the Database Server, as well. This leaves the OVIS Management Server free to receive and summarize the data, and to present the data via the Dashboard.

CPU and bus speed can be misleading indicators of the actual performance of a system. In our tests, there was not a huge difference in the standalone dual 400MHz PII system versus the 1.7GHz P4. The 1.0 GHz Celeron was a poor performer for the probes, compared to other Pentium systems.

Having a dual-processor system was a real advantage for the probe system, where process switching takes up a large amount of CPU time. Having two processors limited the amount of process switching required in order to handle higher concurrency in the probes, thus reducing the CPU utilization and cycle time.

In probe environments where the probes spend a significant amount of time waiting for responses from the target, cycle time can be decreased significantly by increasing the concurrency. However, in environments with little wait time, the process switching overhead incurred with increased concurrency may actually decrease overall performance.

The more Service Level Objectives configured, and the more alarms and SLO violations triggered, the more overhead is incurred for the processing of each incoming measurement.

The responsiveness of the Dashboard will vary in direct relation to the amount of data being requested. Requests for "All Customers" will take considerably longer than requests for a single customer (e.g., with a 10 custom configuration, it will take up to 10 times longer for All Customers). Likewise, requests for "All Services" and "All Metrics" (in Drill Down) will take longer to process. Also, the time taken to create and transmit all of the graph images may be prohibitive (especially if time series graphs are requested). However, in the distributed system described above, with all probes remote, and the Database on a separate system, the Dashboard was quite responsive, and scales quite well, especially when looking at a subset of the data (e.g., a specific Customer and a specific Probe Type).

It is probably wise to allow for some available CPU utilization time on the OVIS Management Server, in order to catch up in cases where the probes have been gathering data, but the OVIS Management Server has not been receiving the measurements (e.g., if the IIS web server is down for some reason, for a period of time). In those cases, the probes will queue up their data, until the Management Server begins to retrieve measurements

again. When this retrieval resumes, the Management Server will take some time to catch up, as it downloads large numbers of these queued files and processes them into the appropriate database tables.

The SLA Evaluator runs once every hour. The amount of time consumed will depend on the number of Service Level Objectives being evaluated, and the number of SLAs configured. These values are not part of the calculations given above, but since it runs once per hour the impact should not be large.

With a very large number of targets, the Reporter database in which all of this OVIS data resides can become quite large. Make sure that the database is configured to grow to the size you desire, and use the OVIS database configuration dialog in the Configuration Manager to insure that the OVIS tables contain the appropriate number of days worth of data.

NTFS Security Settings

Some files and directories must be accessible and/or modifiable by the anonymous Internet user account (IUSR_<machine name>). Note that the path <Program Files\HP OpenView> is the default directory, you may override this default at installation. The Internet Services install program sets the following NTFS permissions explicitly for the user IUSR_<machine name>:

Table 10 NTFS permissions explicitly for the user IUSR

Path	Edit/ Replace ACL	Include Sub Directories?	Permissions	Comments
\<Program Files\HP OpenView>	Edit	Yes	Read (RX)	
\<Program Files\HP OpenView>\data	Edit	Yes	Change (RXWD)	
\<Program Files\Common Files\	Edit	Yes	Read (RX)	ODBC Configurati on

Table 10 NTFS permissions explicitly for the user IUSR (Continued)

Path	Edit/Replace ACL	Include Sub Directories?	Permissions	Comments
\<Temp>	Edit	No	Change (RXWD)	
\<Winnt>\system32	Edit	No	Read (RX)	
\<Winnt>\system32*.*	Edit	No	Read (RX)	
\<Winnt>\system32\inetsrv	Edit	No	Read (RX)	
\<Winnt>\system32\ inetsrv\asp	Edit	Yes	Read (RX)	*may not exist

Table 11 NTFS permissions explicitly for the local "Administrator" group:

Path	Edit/Replace ACL	Include Sub Directories?	Permissions	Comments
\<Program Files\HP OpenView>	Edit	Yes	Full	
\<Program Files\HP OpenView>\data	Edit	Yes	Full	
\<Temp>	Edit	Yes	Full	

Table 12 NTFS permissions explicitly for the "SYSTEM" account

Path	Edit/ Replace ACL	Include Sub Directories?	Permissions	Comments
\<Program Files\HP OpenView>	Edit	Yes	Full	

Table 13 Registry Settings

Path	Edit/ Replace ACL	Permissions	Comments
Path = HKEY_LOCAL_MACH INE\SOFTWARE\ ODBC\ODBC.INI\R eporter	Edit	Read (RX)	
Path = HKEY_LOCAL_MACH INE\SOFTWARE\ ODBC\ODBC.INI\Io psTraceTable	Edit	Read (RX)	

The Execute Permissions for Internet Services IIS Virtual Directories for the IUSR are as follows:

Table 14 IIS Permissions for the user IUSR

Path	Execute Permissions
HPOV_IOPS	Scripts only

Path	Execute Permissions
HPOV_IOPS\cgi-bin	Scripts and Executables
HPOV_IOPS\isapi	Scripts and Executables
HPOV_IOPS\java	Scripts and Executables
HPOV_reports	Scripts only (includes all subdirectories)
HPOV_Help	Scripts only (includes all subdirectories)

Numerics

- 403.7 Forbidden
 - Client certificate required, 182

A

- Access
 - recreating database, 192
- access, restricting, 70
- active monitoring, distributing templates, 137–138
- Alarm Engine, 168
 - logging, 170
- alarm message keywords, 54
- alarms
 - configuring events, 53–55
 - description, 12
 - events, 147
 - NNM, 143
 - setting, 45–55
 - setting events, 49
 - setting objectives, 53
- ARM, using, 17
- availability gauge, 38

B

- baseline= attribute, 82
- baselines
 - setting, 45–55
 - setting objectives, 53
 - value calculation, 50–52

- batch configuration facility, 71
- Batch Configuration File
 - creating sample, 87
- browser requirements, 24
- Business Transaction Observer (BTO)
 - installation restriction, 22

C

- Certificate File, 67
- Certificate Password, 67
- characters, XML usage restrictions, 74
- CiscoWorks server, 118
- client certificates, creating, 181–183
- clientcert, 68
- collector, functions, 168
- communications
 - secure
 - configuring, 179–183
 - preparing, 179–180
 - secure to server, 178
- components, platforms, 25
- condition= attribute, 82
- conditions, comparing metric and threshold values, 82
- configfilename, 72
- configuration
 - automating, service targets, 71–90
 - file syntax, 73–86
 - OpenView Operations for UNIX, 133
 - OVO for Windows, 150–152

- removing trial, 189
- Configuration Manager
 - description, 14
 - using, 43–44
- Configuration Manager window, 34
- Configuration Wizard
 - using, 43–44
- configuring, 41–44
 - default settings, 42–43
 - NNM integration, 141–142
 - services, 42–44
- conformance level
 - SLA, 58
- Crystal Reports, 183
- Custom Probes API, 119
- custom reports
 - creating your own, 183

D

- Dashboard
 - data selection, 37
 - reports, viewing requirements, 24
 - viewing data, 35
 - viewing requirements, 24
 - web interface, 169
- data
 - collection, checking status, 34–35
 - consolidation displays red hexagon, 159
 - display restricting access, 70
 - tables, 168
 - web page display, viewing, 35
- Data Consolidation page, 35
- database
 - backup, 186
 - compressing, 161
 - configuring, 184
 - maintaining, 184
 - platforms supported, 25
 - possible configurations, 184
 - rebuilding, 189
 - running out of space, 161
 - types supported, 184

- database documentation, 185
- days= attribute, 82
- description, OVIS, 12
- DHCP (Dynamic Host Configuration Protocol)
 - probe attributes, 77
 - service description, 93
- DIAL (Dial-Up Networking Service)
 - probe attributes, 77
 - service description, 94
- Dial Up probe, 22
- DNS
 - probe attributes, 77
 - service description, 95
- Domain Name System, *see* DNS
- Drill Down page, 39
- duration settings, 49
- duration= attribute, 82

E

- Echo Requests, 105
- events
 - alarms, 147
 - configuring in NNM, 145–148

F

- firewalls, communicating through, 176–177
- FTP (File Transfer Protocol)
 - probe attributes, 77
 - service description, 96–98

H

- hardware requirements, 20–21
- heavyweight recording mode, 102
- HP OpenView Performance Agent (MeasureWare/NT), 17
- HP OpenView Reporter, integration, 17
- HTTP
 - probe attributes, 78
 - service description, 98–100
- HTTP_TRANS
 - service description, 101

- HTTPS
 - probe attributes, 78
 - service description, 100–101
- I**
- ICMP (Internet Control Message Protocol-Ping)
 - probe attributes, 78
 - service description, 105
- id= attribute, 76, 85
- Ignore Certificate Errors, 67
- IIS level security, 176
- IMAP (Internet Message Access Protocol)
 - service description, 105
- IMAP4 probe attributes, 79
- installation
 - considerations, 20
 - prerequisites, 20–25
 - procedure, 26
- integration
 - other OpenView products, 131–152
- Internet Service Manager (IIS) program, 179
- interval= attribute, 85
- IOPS 1-11, socket error, 158
- IOPSLoad program, 71
- IopsTraceTable data buffer, 168
- L**
- LDAP (Lightweight Directory Access Protocol)
 - probe attributes, 79
 - service description, 107
- lightweight recording mode, 102
- M**
- Management Server
 - description, 12
 - function, 168
 - hardware requirements, 20
 - platforms, 25
 - software requirements, 21
- measEvent2 dll, 168
- message= attribute, 83
- metric descriptions
 - by probe type, 121
- metric= attribute, 82
- Microsoft Certificate Server, 183
- MSDE database
 - recreating, 190
- MSDE default database, 184
- N**
- Network Connection
 - configuring, 60–61
- Network Node Manager (NNM)
 - integration, 140–149
 - interface and features, 142–148
 - troubleshooting, 148
- news reader, 107
- NNM Alarm Categories window, 143
- NNM Internet Services symbols, 145
- NNM menu bar, 144
- NNTP (Network News Transfer Protocol)
 - probe attributes, 79
 - service description, 107–108
- NTFS
 - permissions, 205–208
 - registry settings, 207
 - Security Settings, 205–207
- NTFS level security, 176
- NTP (Network Time Protocol)
 - probe attributes, 79
 - service description, 109
- O**
- Objective Activity Times, 48
- objectives
 - setting, 45
- objectives dialog, 46
- OpenView Operations for UNIX. integrating, 132
- OpenView Operations for Windows
 - integration, 150–152
- Oracle

- recreating database, 193
- Oracle and SQL Server database, 184
- OVO for UNIX integration
 - enabled, not working, 162
- OVO for UNIX Service Navigator,
 - integrating, 138
- OVO Integration Package, installing, 136
- OVO Integration-Default option, 133
- OVO Integration-Use Proxy option, 134
- OVO Settings-Prefix option, 134
- OVO UNIX upgrading previous version,
 - preparing, 135

P

- password, 70
- password, viewing Dashboard, 70
- pattern matching, using in HTTP, 99
- platforms
 - support, 25
- POP3 (Post Office Protocol 3)
 - probe attributes, 79
 - service description, 109–111
- prerequisites, installation, 20–25
- Probe Data Received page, 35
- Probe Location Info dialog, 60
- Probe System
 - UNIX
 - hardware requirements, 21
 - software requirements, 23
 - Windows
 - hardware requirements, 20
 - software requirements, 22
- probe= attribute, 76
- probes
 - architecture and data flow, 166
 - attributes, 76–83
 - configuring, 27–33
 - UNIX systems, 66–69
 - custom development, 119
 - description, 12
 - locations, 14
 - NT systems
 - configuring remotes, 64
 - deploying remotes, 64–66
 - outside of firewall, protecting, 178
 - platforms supported, 25
 - services structure, 42
 - Windows system
 - removing remotes, 65
- procedures
 - active monitoring, distributing
 - templates, 137–138
 - batch configuration, creating, 87
 - client certificates, creating, 181–183
 - database, compressing, 161
 - events
 - configuring in NNM, 145–148
 - local web server, verify running correctly, 157
 - NNM integration, configuring, 141–142
 - NNM, integrating, 140–149
 - OVO for UNIX Service Navigator,
 - integrating, 138
 - OVO for Windows, configuring, 150–152
 - OVO Integration Package, installing
 - OVO integration package, 136
- probes
 - removing remotes, 65
 - UNIX, removing, 69
- remote probes
 - deploying, 64–66
- Root Certificates, exporting, 101
- secure communications, preparing, 179–180
- software, implementing, 16
- software, installing, 26
- tracing, checking for error text, 161
- upgrading previous versions OVO UNIX, 135

- proxies, using in HTTP, 99
- proxy and port settings, 174

Q

- queue files, 167

-quiet parameter, 72

R

RADIUS (Remote Authentication Dial In User Service)

probe attributes, 79

service description, 112–113

RAS (Remote Access Server), 22

Real Player, 22

Remote Probe Update page, 35

removal, 69

Reporter

database, 169

reports, 39

long-term, viewing, 39

requirements

browser, 24

Dashboard

reports, viewing, 24

hardware, 20–21

NNM integration, 140–141

OpenView Operations for UNIX, 132

software, 21–23

response time gauge, 38

restoring database, 189

S

scalability

calculate number of probe systems, 196

scalability 4.0, 201

scalability 3.5, 195

scheduler, description, 166

secure communication, *see* communications

security, 174

security settings, 176

service groups, components, 14

Service Level Agreements (SLAs), 170

setting up, 56

service level objectives, 45

service level objectives (SLOs)

compliance, 170

service level violations gauge, 38

Service Level, violations, 49

service objective, 42, 53

description, 14

service target, 42

description, 14

Service Target Availability page, 34

service targets

automating configuration, 71–90

configuring, 27

platforms supported, 25

probe type descriptions, 91–120

services

configuring, 42–44

severity= attribute, 84

SLA configuration wizard, 56

SLA conformance level, 59

SLA evaluator, 170

frequency, 171

SMTP (Simple Mail Transfer Protocol)

probe attributes, 80

service description, 114–115

Snapshot page, gauges, 37

socket error, IOPS 1-11, 158

software

implementation, 16

requirements, 21–23

SQL Server

recreating database, 191

starttime= attribute, 82

Streaming Media

probe attributes, 80

service description, 115–116

Streaming Media probe, 22

symbols, XML substitutions, 83–84

T

TCP (Transmission Control Protocol)

probe attributes, 80

service description, 117

threshold= attribute, 82

timeout= attribute, 85

tokens, XML, 73

Trend Report button, 39
trial configurations, removing, 189
troubleshooting, 153–206
Trusted Root Certificate, 100

U

UNIX Probe System, *see* Probe System
UNIX

V

virtual memory, software requirements, 21

W

WAP (Wireless Application Protocol)
probe, 22
probe attributes, 80

service description, 117–118
web pages, downloading of protected in
HTTP, 99

web recorder, 102
steps to using, 104

Windows Management Server, *see*
Management Server

Windows Probe System, *see* Probe System
Windows

X

X_SLAM
probe attributes, 81
service description, 118–119
XML syntax, 71–76