HP OpenView Internet Services

User's Reference Guide

Manufacturing Part Number: J4511-90000

January 2003

Legal Notices

Warranty

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.

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

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 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices

Trademark Notices

Java™ is a trademark of Sun Microsystems, Inc. Microsoft Windows®, Windows NT®, MS Windows®, Windows 2000®, MS-DOS® and XP® 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 Ceticom Corp. Copyright

Support

Please visit the HP OpenView website at:

http://openview.hp.com/

There you will find contact information and details about the products, services, and support that HP OpenView offers.

The support area of the HP OpenView website includes:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information

contents

1

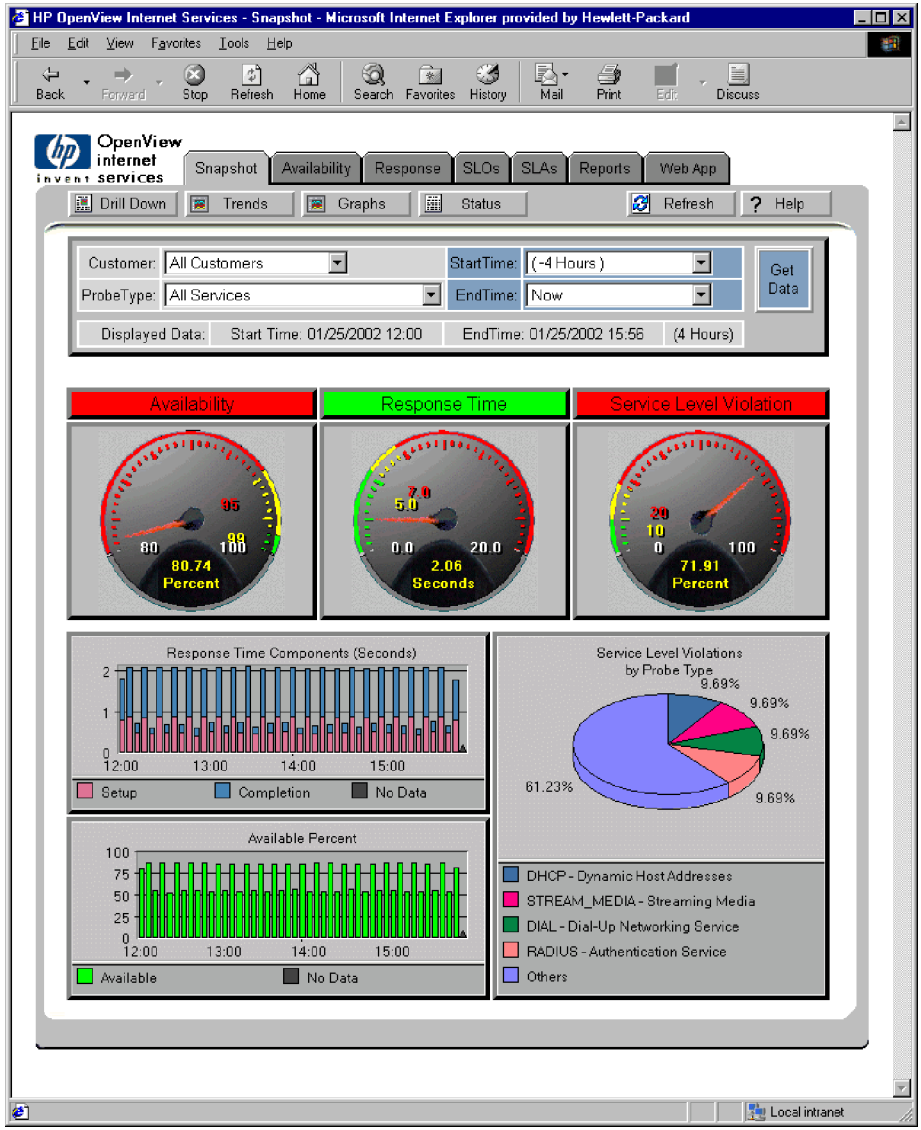
Introducing Internet Services

HP OpenView Internet Services (OVIS) 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.

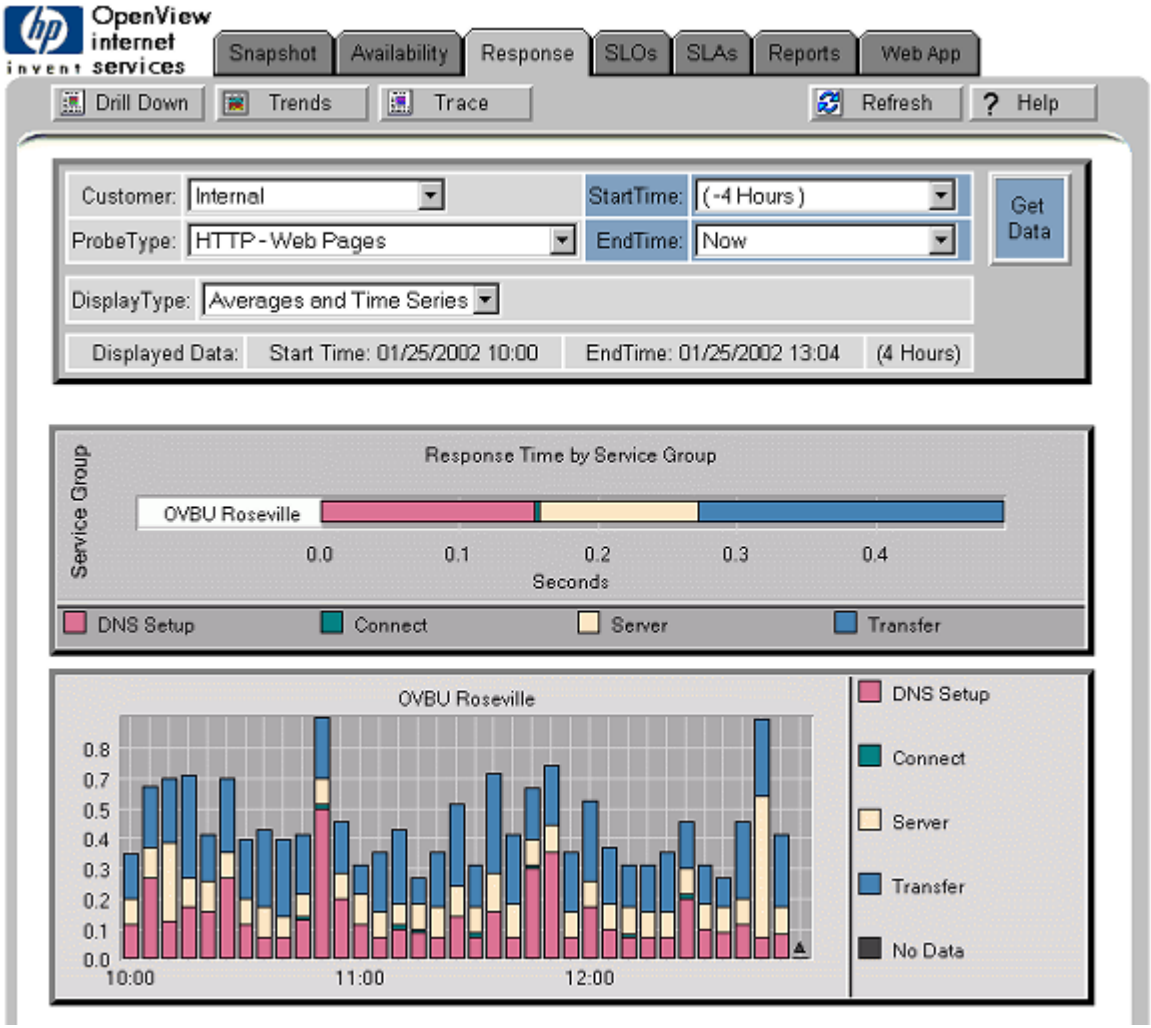
Internet Services uses software probes to simulate business activity. These probes measure availability, response time, and other performance metrics for your Internet and related services. In addition, service level violations and conformance to service level agreements are also monitored and reported. To view data from the probes and information about service levels, launch Internet Services Dashboard. The Dashboard is a collection of gauges, graphs, trend data you can view from a web browser.

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.



From the Dashboard display you can drill down into more detail. The example below shows the average time for each component of response time and shows response time component values at five minute intervals in the time series graph.



How Internet Services Works

Internet Services 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 Chapter 4, Descriptions of Service Types/Probes 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. There are also trend reports giving you a longer-term view of the data and out of the box **reports** that run nightly and summarize the data.

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 IT Operations), or any other event manager capable of receiving SNMP traps. These alarms, which take the form of regular updates and special alerts, will let you know whether a customer's services are performing adequately.

Data collected by OpenView Transaction Analyzer can be integrated with Internet Services and displayed on the Dashboard. Furthermore, if you define service level objectives and service level agreements for OVTA data, OVIS will forward OVTA alarms to OVO and NNM.

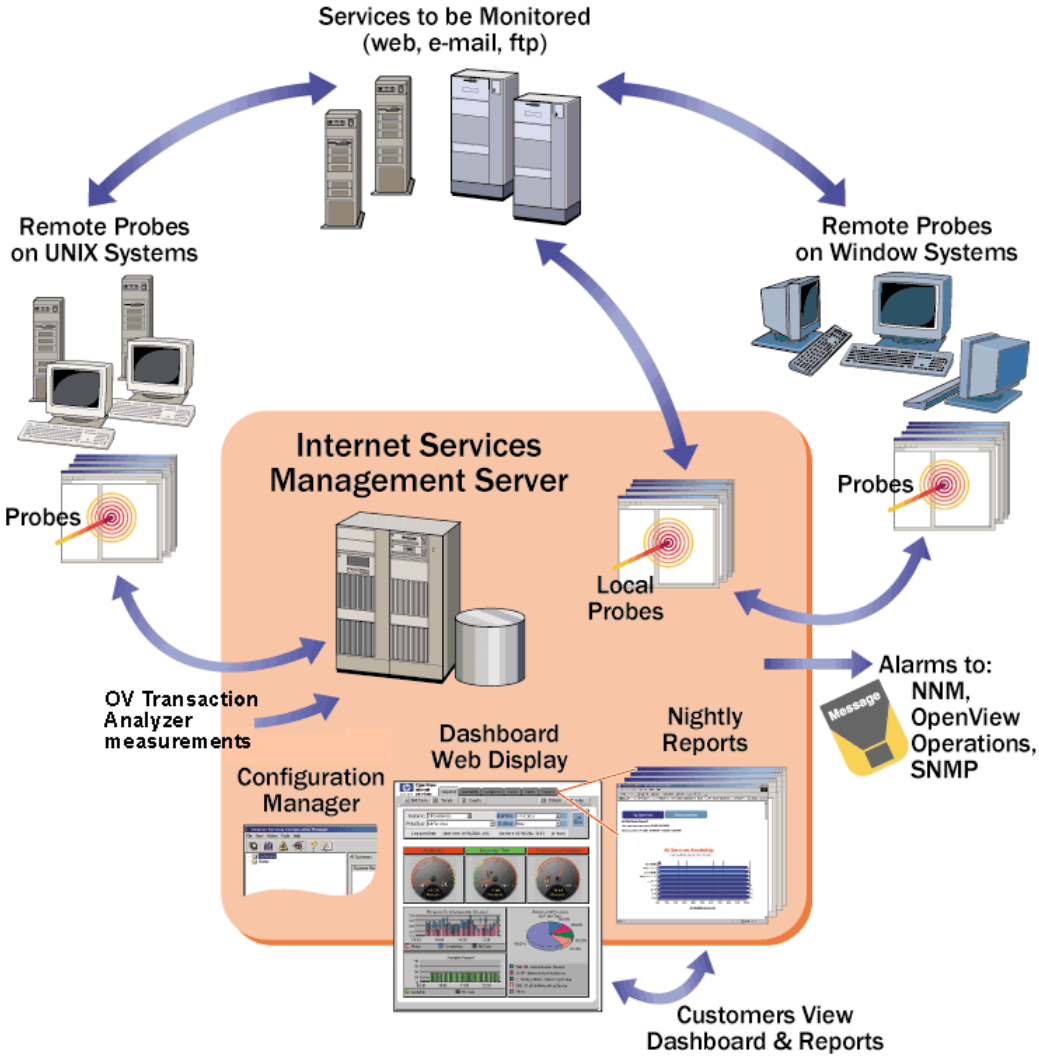


Figure 1 High Level Overview of the Internet Services Components

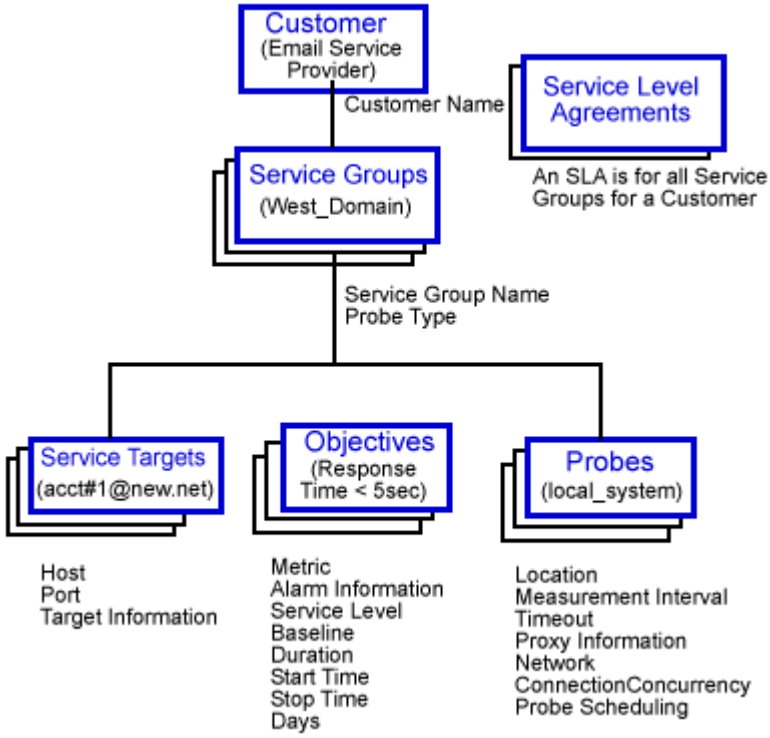
The Services Hierarchy

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:

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

3 Use the Internet Services Configuration Manager to define probe locations. You can set probes to monitor from the local Management Server system or you can deploy probes to remote systems.

4 Probes measure response time, availability and other performance metrics and send the data back to the Management Server. Use the status tab in the Configuration Manager to verify that the probes are working properly.

5 On the Management Server, data received from probes is consolidated for viewing in the OVIS Dashboard.

6 Service Level Agreement, Availability and Response Time reports are generated nightly.

7 Alarm events can be sent to NNM, OpenView Operations for UNIX, OpenView Operations for Windows or a generic SNMP management station.

Both Chapter 2, Getting Started with Internet Services and Chapter 3, Configuring Internet Services 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 Chapter 5, Integrating with OpenView Products, Internet Services can be configured to integrate with OpenView Transaction Analyzer, 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 to create custom reports for Internet Services and modify workshift 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 (formerly known as MeasureWare) 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.

If HP OpenView Performance Manager (OVPM) is installed on the same system as Internet Services, then Internet Services data can be viewed in the OVPM graphs and reports.

2

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. 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.

Installing and configuring Internet Services begins with the following tasks:

- Installation Considerations
- Installation Prerequisites
- Installing Internet Services
- Quick Start for Using Internet Services
- Uninstalling Internet Services

Installation Considerations

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.

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

Installation Prerequisites

The following recommendations represent minimum requirements for Internet Services.

See the OVIS Release Notes for detailed information on supported platforms, coexistence and integrations with other OpenView products

Hardware Requirements

Windows Management Server

- Intel Pentium III, 1 GHz or faster processor with 512 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 Probe System

- Intel Pentium, 500 MHz or faster processor with 256 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 Management Server

You must have one of the following operating system versions and IIS versions installed on the OVIS Management Server:

- Microsoft Windows 2000 Professional/ Server/Advanced Server with Service Pack 2 or 3
  (Note that Windows 2000 Advanced Server versions are supported but not advanced features of DataCenter Server.)

  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)

The OVIS Management Server has these additional software requirements:

- Internet Explorer 5.5 with the latest service pack or Internet Explorer 6.0 or 6.1. Internet Explorer 5.5 is required in order to support Restricted Views and IE 5.5 or 6.0, 6.1 for the Web Transaction Recorder
- IIS on the OVIS server must be configured to have all IP addresses assigned, especially 127.0.0.1 that is required for probe/server communication. In IIS configuration set the IP Address field to **All Unassigned**.
- 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, Windows Media Player or Real Player (basic version 8 or RealOne are required. By default, the Windows Media Player is installed with the probe. If you want to use Real Player you must install it. You can download a free version of Real Player from www.real.com.
- If you are using the HTTP_TRANS Web Recorder and Microsoft Script Debugger is installed, it is recommended that you turn off script debugging in Internet Explorer. For example, in IE select Tools > Internet Options > Advanced: and check “Disable Script Debugging”. Having script debugging enabled interferes with Web Recorder playback and recording in cases where the page contains a script with an error.

- Adobe Acrobat Reader 4.0 or higher is required to view the Internet Services User's Reference Guide and other documentation (in .pdf format). You can download the reader from http://www.adobe.com/products/acrobat/.
- If you use systems with different language settings, note that the same Locale setting must be used for the OVIS server, OVIS/Reporter database, remote probes. Also the same Locale setting must be used for OVO, OVO/Windows, NNM, SIP and other OpenView products if integrating OVIS with these products.

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 Probe System

- Microsoft Windows NT 4.0 Server or Workstation with Service Pack 6a; or Microsoft Windows 2000 with Service Pack 2 or 3; or Microsoft Windows XP with Service Pack 1.
- Internet Explorer 5.5 (with the latest service pack), IE 6.0 or 6.1.
- 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 are running the Streaming Media probe on the remote system, Real Player (basic version 8 or RealOne) for Windows or Windows Media Player is required. The Windows Media Player is installed automatically for you with the probe. If you want to use Real Player instead then you can download a free version from www.real.com.

DHCP is supported on remote probe systems.

UNIX Probe System

- HP-UX 11.0, 11.11, 11.22 Itanium
- Sun Solaris 2.7, 2.8, 9
- Linux Red Hat 7.0, 7.1, 7.2

Probes Not Available on UNIX Systems

- Streaming Media probe
- XSLAM CiscoWorks integration
- SMS probe
- ODBC probe
- Web App - OVTA integration
- 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 systems

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 7.0 requires ppp-2.3.11-7

Browser Requirements for Viewing the Dashboard

You must have a web browser to view the Dashboard and reports. Netscape 4.7, 6.1, 6.2, and 7 are supported along with Internet Explorer 5.5, 6.0 and 6.1.

Colors in the display settings on the system displaying the browser need to be set to High Color (16K) or more colors.

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. See the procedures below for setting this:

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**.

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 you log into the Dashboard when Restricted Views is enabled, you will be prompted to enter a user name and password before viewing the Snapshot display.

Installing Internet Services

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

If other OpenView products are installed on the system you will be using for the Management Server, you may not change the default drive and directory setting for the install or data directory. The OVIS installation will follow the path already established by these other OpenView products.

HP OpenView tools on Windows-based operating systems use registry entries in the `\HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard` hive during installation to tell if other OpenView tools are already installed and what the common directories are. The installation looks in this hive for `InstallDir` and `DataDir` keys underneath `HP OpenView`, or for a product name entry which contains a key named `RPM ID` and the path keys named `CommonApplicationPath` and `CommonDataPath` underneath `Current Version`.

Complete the installation as follows:

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

Probe Considerations

Probes must first be configured and saved before they can be installed. See "Quick Start for Using Internet Services" on page 33 for an example of probe configuration.

Probes can be run on the local OVIS management server system or they can be installed to run on remote Windows or UNIX systems. See "Configure Remote Probes" on page 91 for the steps to install and run remote probes.

License Key

You must have a license key password to use OVIS. At installation you are given a 60-day trial license. Within this 60 day period, you must obtain either a trial evaluation extension or a permanent license key password to continue to use OVIS.

To obtain your license key password, select the **License Wizard** button on the message box that appears on screen when you startup the OVIS Configuration Manager. It takes a minute or so for the **HP OpenView AutoPass** licensing program to launch.

You can skip obtaining your license by pressing OK in the initial message box. Later you can get your license key by selecting **File > Configure > License** in the Configuration Manager and selecting the **License Wizard** button on the dialog that is displayed.

Select the License Wizard button and follow the instructions in the **AutoPass** program to obtain and install permanent license keys. See the note on the following page if you are requesting a trial (evaluation) license extension, since this cannot be done via the OVIS License Wizard.

Follow these steps to obtain your permanent license key password:

1. In the License Wizard select either Direct Connection or enter your Proxy information in the dialog displayed.
2. Select Install Permanent Password in the dialog displayed and enter the HP OpenView Purchase Order information from your Entitlement Certificate.
3. Select the LTU (License To Use) products you have purchased.
4. Fill out the customer information form.
5. When finished, your password keys are installed.
6. Click OK to save the configuration changes before exiting the Configuration Manager.

If instead of the License Wizard, you used the www.webware.hp.com website to request a license key password, and have received it via email, you will need to import it into OVIS. Since this process is more complex, we recommend that you use the License Wizard to create and install the license key directly.

If you used the webware site to obtain your license keys, you will need to do the following to import the license keys you received via email into OVIS:

1. Access the www.webware.hp.com website and follow the instructions to request your license key passwords.
2. A License Key Password Certificate is then emailed to you.
3. Extract the passwords from the email attachment you receive and save just the license keys in a plain ASCII file. Save the file in a location available to the OVIS Management Server.
4. Run the Configuration Manager and select the License Wizard. Then select No Connection to the Internet in the dialog displayed.
5. Select Import Password in the dialog displayed. Then browse to find the password file you saved.
6. Each LTU license key from the password file is displayed. Select each and click the Import button.
7. Click OK to save the configuration changes before exiting the Configuration Manager.

If you need to request a **Trial (Evaluation) License Extension**, access the webware website to get contact information for evaluation software passwords. Contact the License Center in your region to request a Trial (Evaluation) License Extension. The Product Number and Name will be TRIAL-OVIS. This is a one-time 60-day extension. You'll receive your password key by email and install it using the importing a license key process above.

For information on the number of service targets you have set up, select **Tools > Probe Info** in the Configuration Manager and look at the number of Logical Targets. A logical target is calculated by adding up the total number of targets per probe location. To view specific information regarding installed licenses select the **View License Details** check box in the Configure License dialog.

For complete details about licensing OVIS, see the *HP AutoPass User's Manual* available on the OVIS product CD. You can download the manual from the Openview web site: ovweb.external.hp.com/lpe/doc_serv/.

If the Total Licensed Capacity is exceeded, data will not be gathered for the logical targets that are over the licensed capacity limit.

Quick Start for Using Internet Services

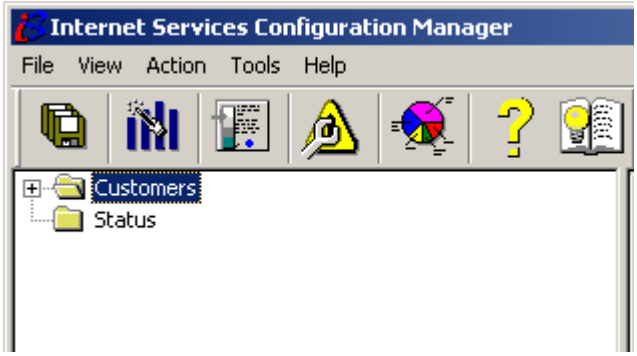
In this example you are going to configure the Web page www.hpshopping.com as a service target for the customer Hewlett-Packard. More detailed information on the process of configuring and installing probes is covered in Chapter 3, Configuring Internet Services.

The OVIS documentation set is available from the Help menu and the book icon.

Configure a Service Probe

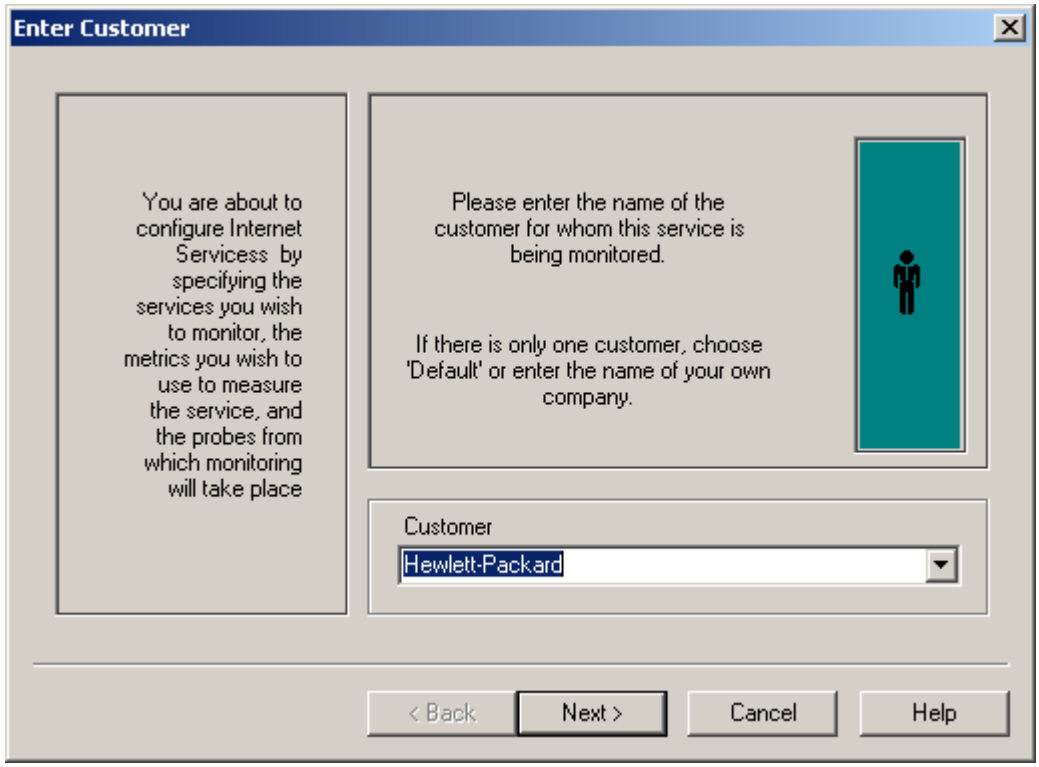
To create the local configuration on the Windows Internet Services Management Server:

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

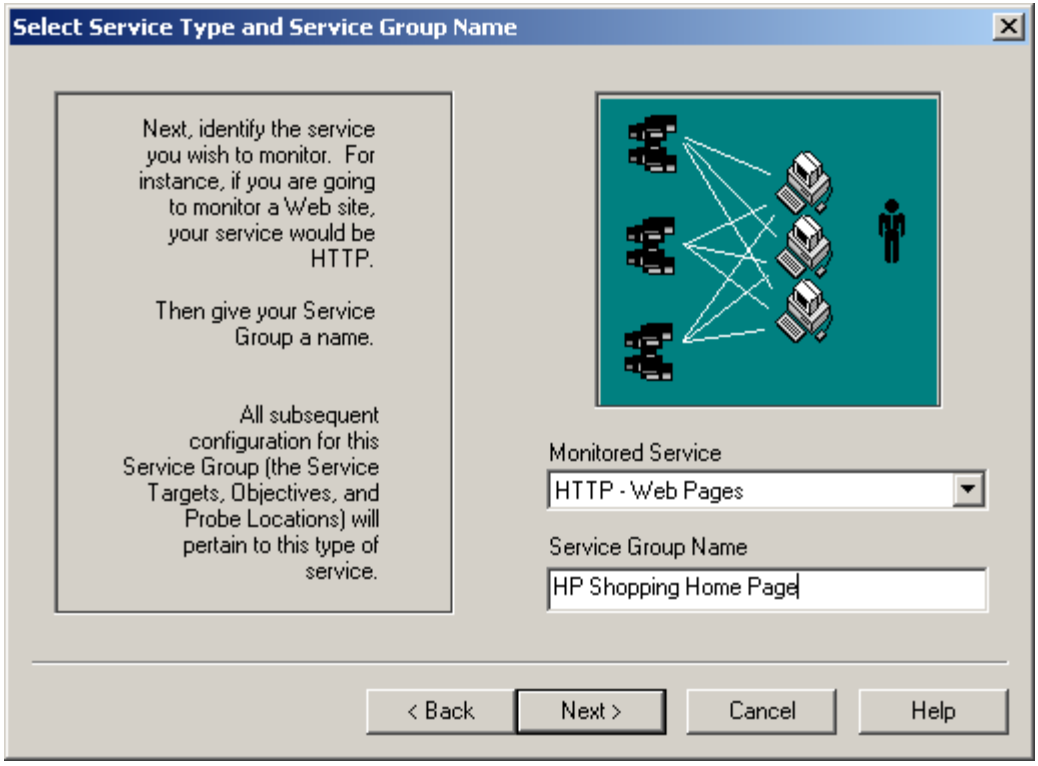


2 Select the **Configuration Wizard** toolbar button (second from left on the toolbar) or select **File>Configuration Wizard** from the menu.

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**.

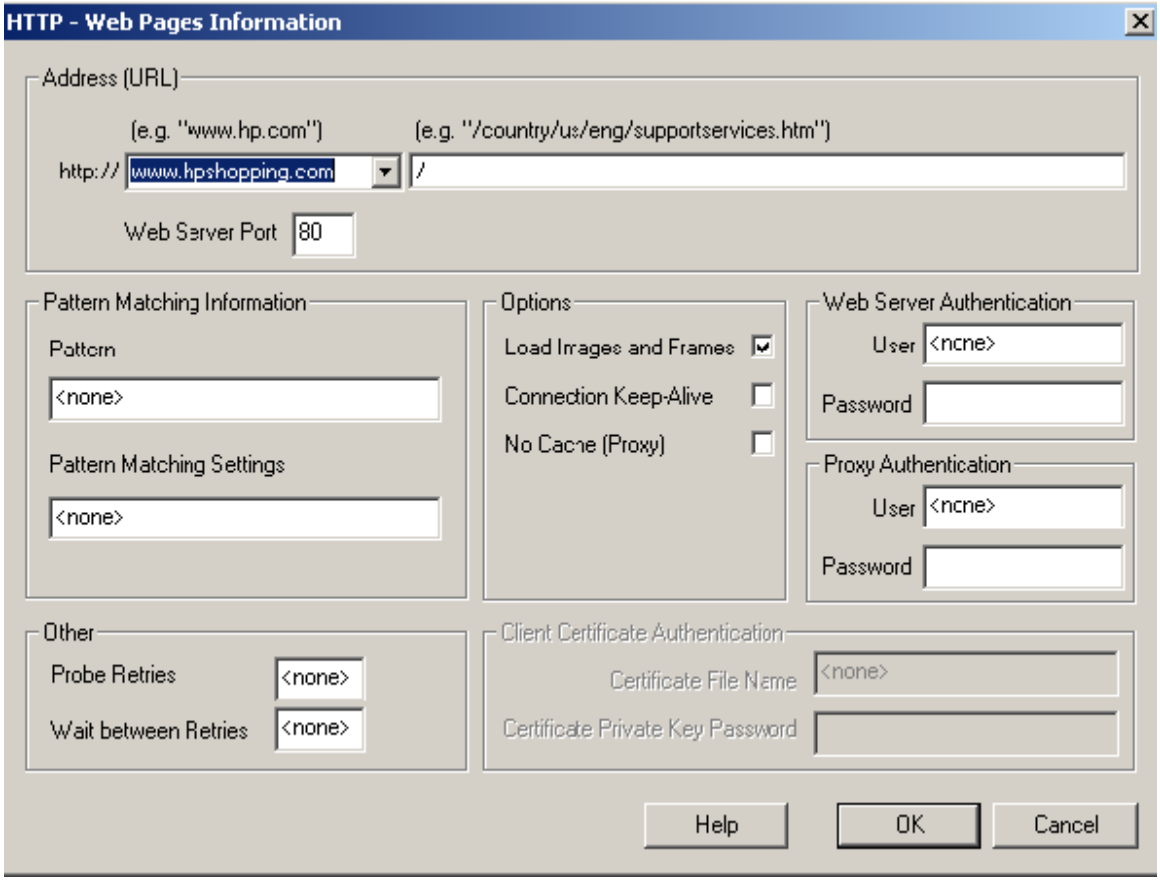


4 In the **Select Service Type and Service Group Name** dialog box, select **HTTP-Web Pages** as the service type, name the service group **HP Shopping Home Page**, and click **Next**.

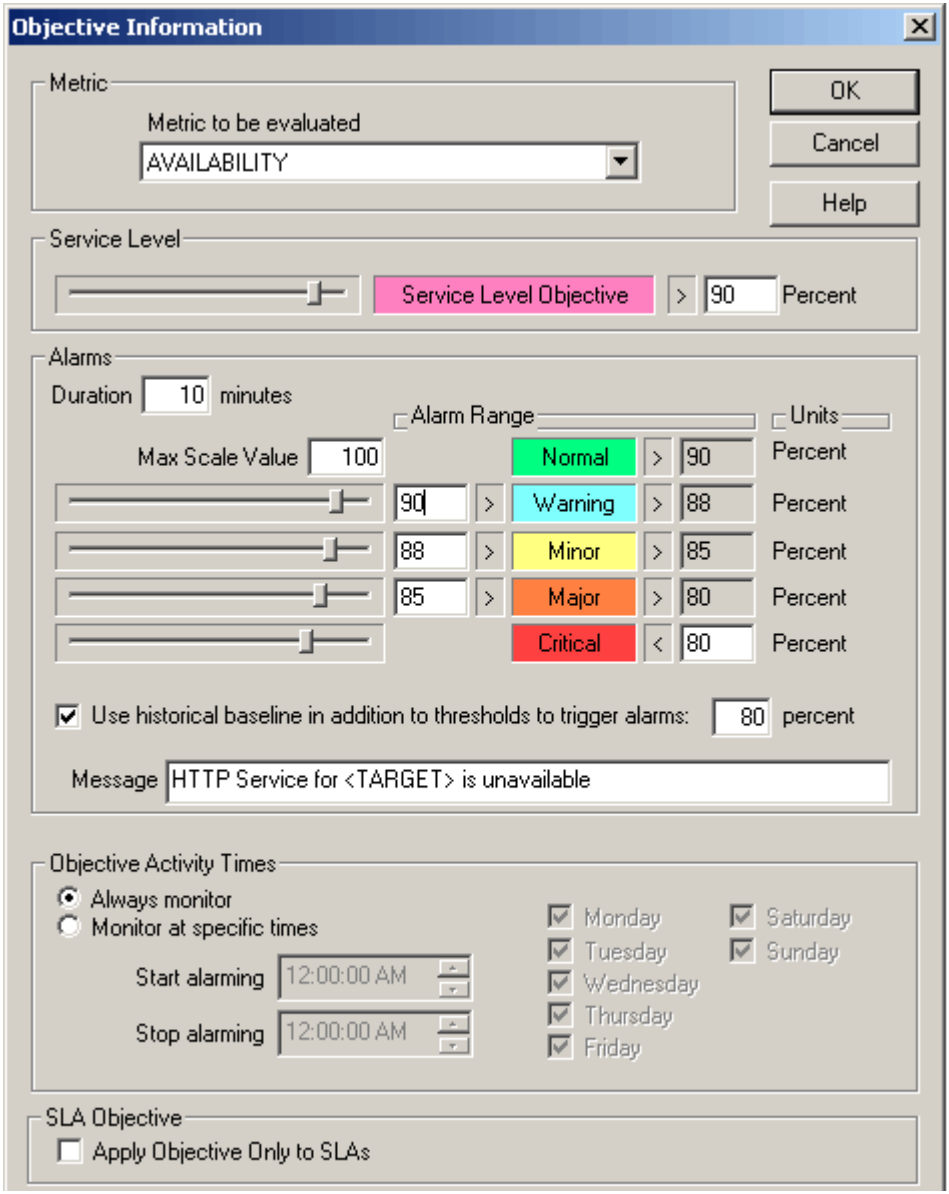


As you organize services, remember that service targets within a service group must be the same type: for example, HTTP (Web pages) is one type of service, while DNS (Domain Name Server) is another.

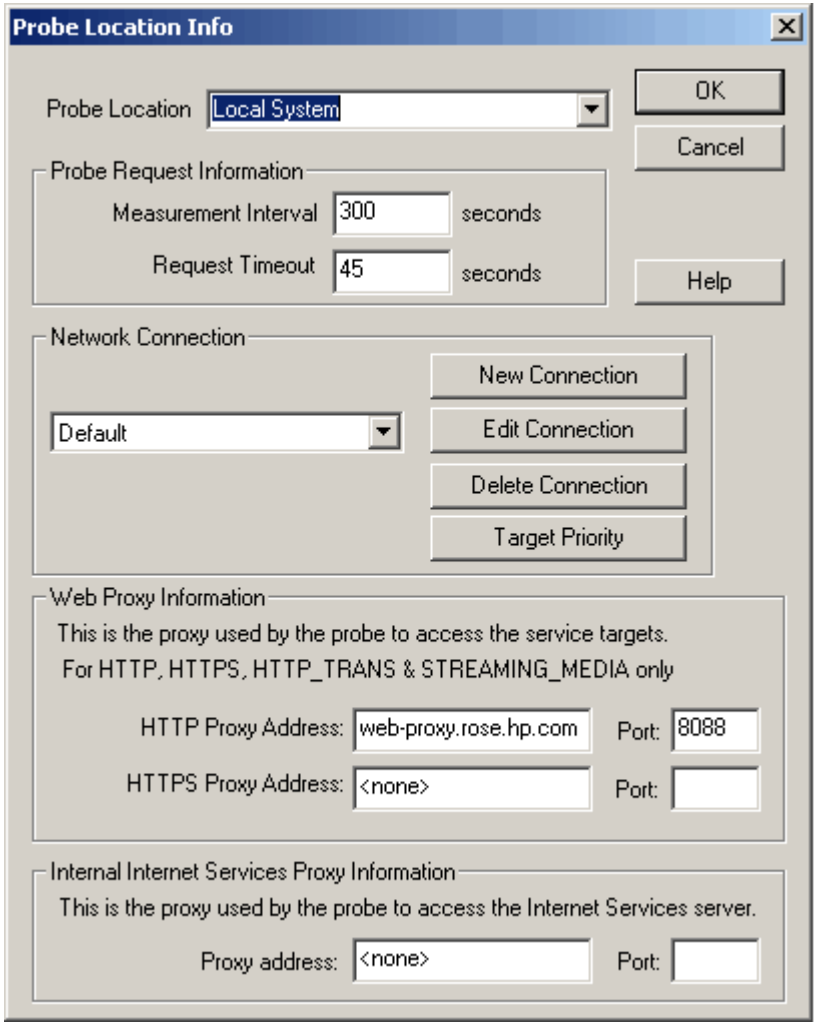
5 In the **Add Service Targets** dialog, select the **Add Service Target** button. The **HTTP WebPages Information** dialog opens. Enter **www.hpshopping.com** as the Service Target you want to monitor. Click **OK** and click **Next**.



6 In the **Add Objectives** dialog select **Add Service Objective.** In the **Objective Information** dialog, accept the default for an Availability objective, specifying that the service group should be available 90% of the time, click **OK** and **Next**.



7 When the **Add Probe Locations** dialog opens, select the **Add Probe Location** button. The **Probe Location Info** dialog opens.

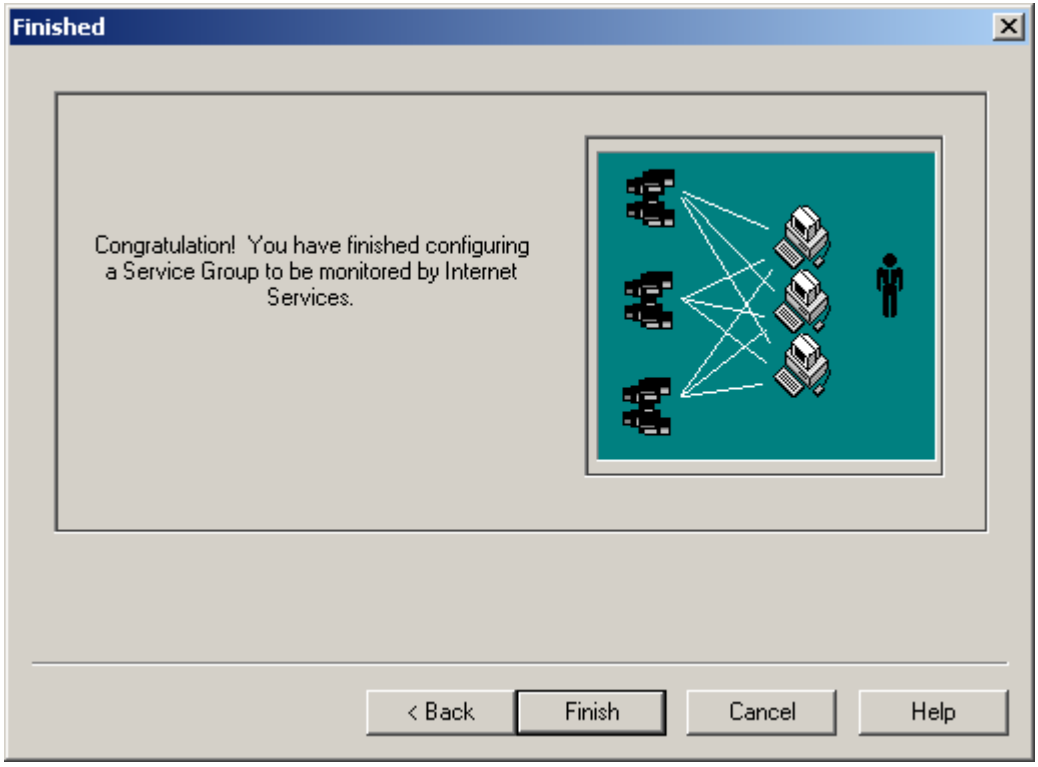


Accept all defaults EXCEPT for Proxy Information. If you use a web proxy to get access to a site like www.hpshopping.com, then you must enter the same proxy address and port number that is configured for your Web browser.

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**.

Note that this dialog is also used to specify probe timing (Probe Request Information), network connection to be used (such as Dial-Up), and target priority (for scheduling probes). See Chapter 3, Configuring Internet Services for more information on these.

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.

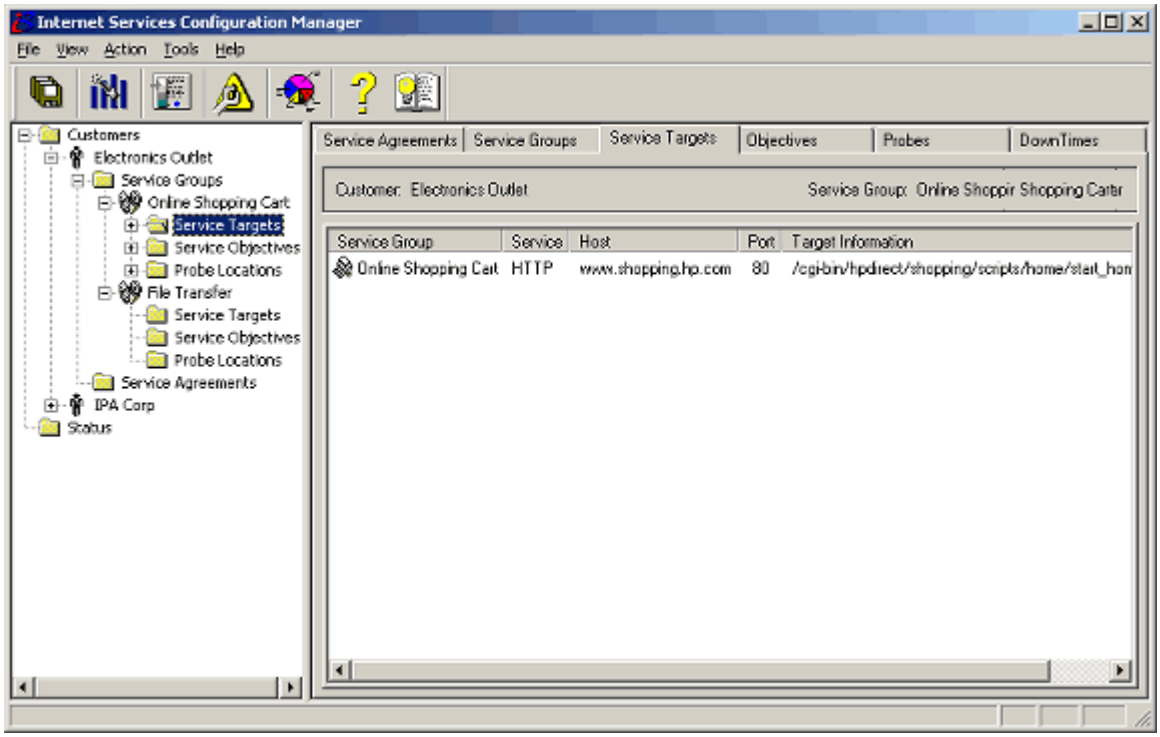
When the configuration setup is saved, all the probes specified for the local system are registered on the Internet Services Management Server and the associated configuration files are stored in the \probes directory. When the probe location is a remote system then the associated configuration files for the probes are created in the `\<install dir>\newconfig\` directory on the server and are then deployed to the remote system. See "Remote Probes" on page 91 for information on deploying probes to remote systems.

View Service Information in the Right Pane

In the Configuration Manager right pane you can view service information for the service targets you configure.

Select Customers at the top of the tree in the left pane of the Configuration Manager and a list of all customers you have configured is displayed in the right pane.

Select any of the other items in the service tree in the left pane and a series of tabbed displays is shown in the right pane. The tab that corresponds to the item you select in the left pane is displayed. For example if you click on a service target, the Service Target tab is displayed.

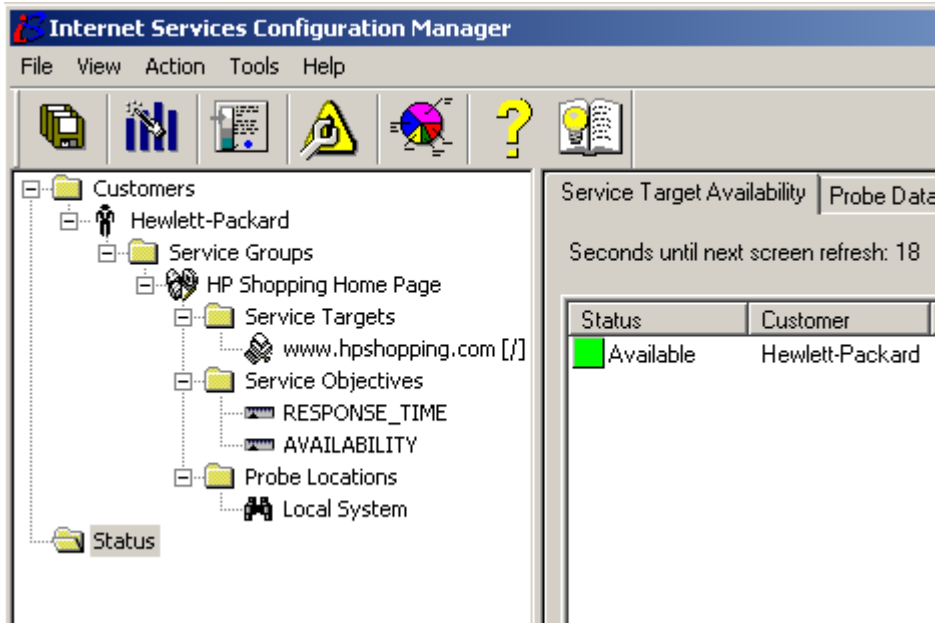


Tabs are as follows:

- Service Agreements
- Service Groups
- Service Targets
- Objectives
- Probes
- Downtimes

Check the Status of Data Collection for Configured Services

In the Configuration Manager left pane, select Status, at the bottom of the tree, 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 Chapter 6, Troubleshooting Information in this guide for what to do if the icons are not green.

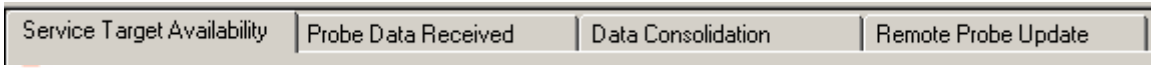


The **Service Target Availability** page show the status of the measurement or service target. It shows whether or not the probe data reached the temporary trace table storage area on the Internet Services Management Server and whether or not the service target is available. The reason for showing availability 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.



Red circles indicate the action was unsuccessful.

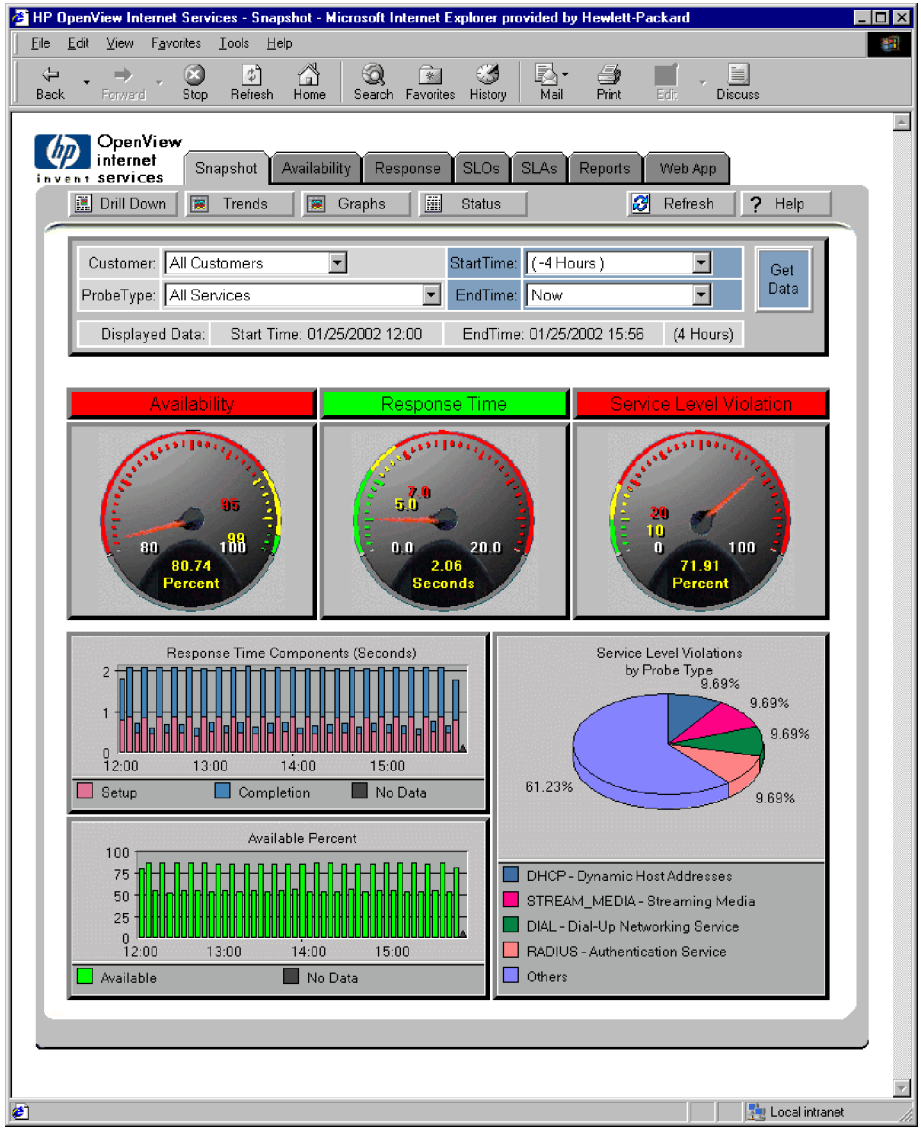
Yellow triangles indicate the action is not yet complete (trying to complete).

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.

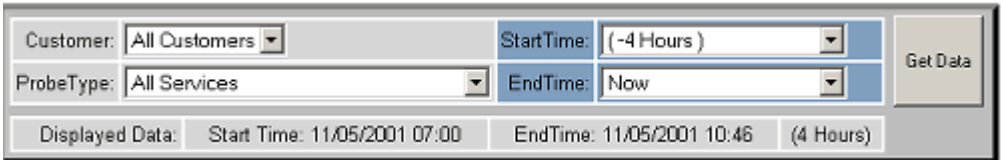
You can also start the Dashboard data display by selecting **Start>Programs>HP OpenView>internet services>Dashboard Display**.


HP OpenView Internet Services - Snapshot - Microsoft Internet Explorer provided by Hewlett-Packard
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
OpenView internet services
Snapshot Availability Response SLOs SLAs Reports Web App
Drill Down Trends Graphs Status Refresh Help
Customer: All Customers
ProbeType: All Services
StartTime: (-4 Hours)
EndTime: Now
Get Data
Displayed Data: Start Time: 01/25/2002 12:00 EndTime: 01/25/2002 15:56 (4 Hours)
Availability
80.74 Percent
Response Time
2.06 Seconds
Service Level Violation
71.91 Percent
Response Time Components (Seconds)
12:00 13:00 14:00 15:00
Setup Completion No Data
Service Level Violations by Probe Type
9.69%
9.69%
9.69%
61.23%
9.69%
DHCP - Dynamic Host Addresses
STREAM_MEDIA - Streaming Media
DIAL - Dial-Up Networking Service
RADIUS - Authentication Service
Others
Available Percent
12:00 13:00 14:00 15:00
Available No Data
Local intranet

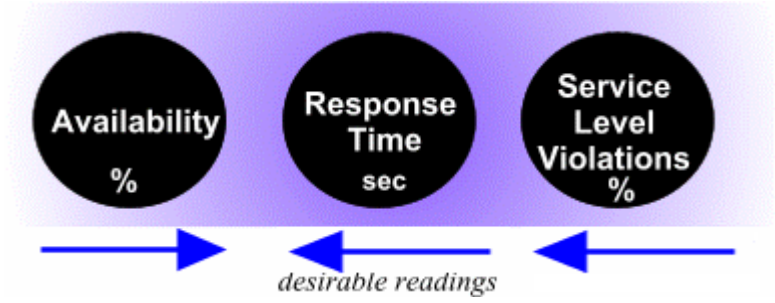
Snapshot Tab

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.



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.



- the **Availability gauge** 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 89
- The **Response Time gauge** shows the average number of seconds each service transaction needed to complete and the acceptability of that value.
- The **Service Level Violations gauge** 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 and SLA Tabs

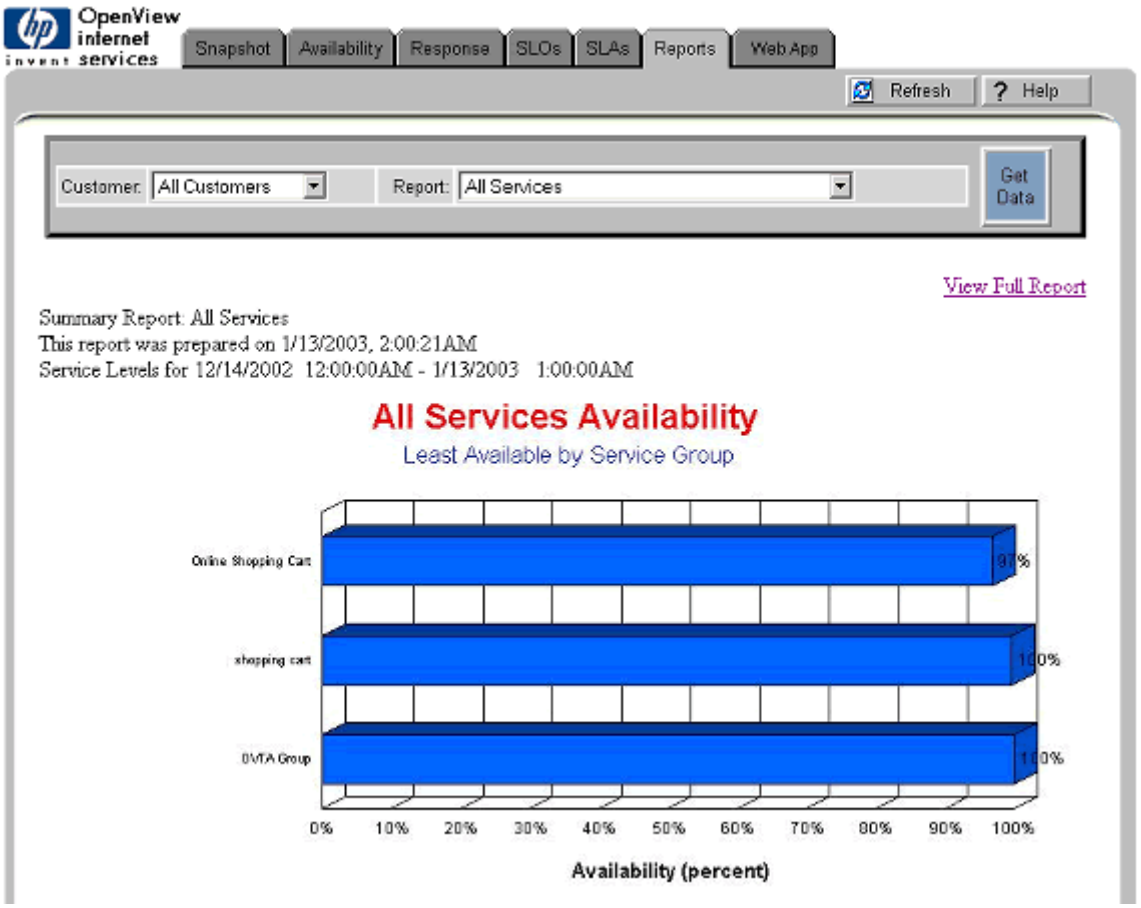
Next, look at the detail information contained in the Availability, Response Time, Service Level Objectives (SLO) and Service Level Agreements (SLA) tabs. Note that the first three tabs can also be viewed by clicking on the corresponding gauge in the Snapshot page. These pages show more detailed views 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

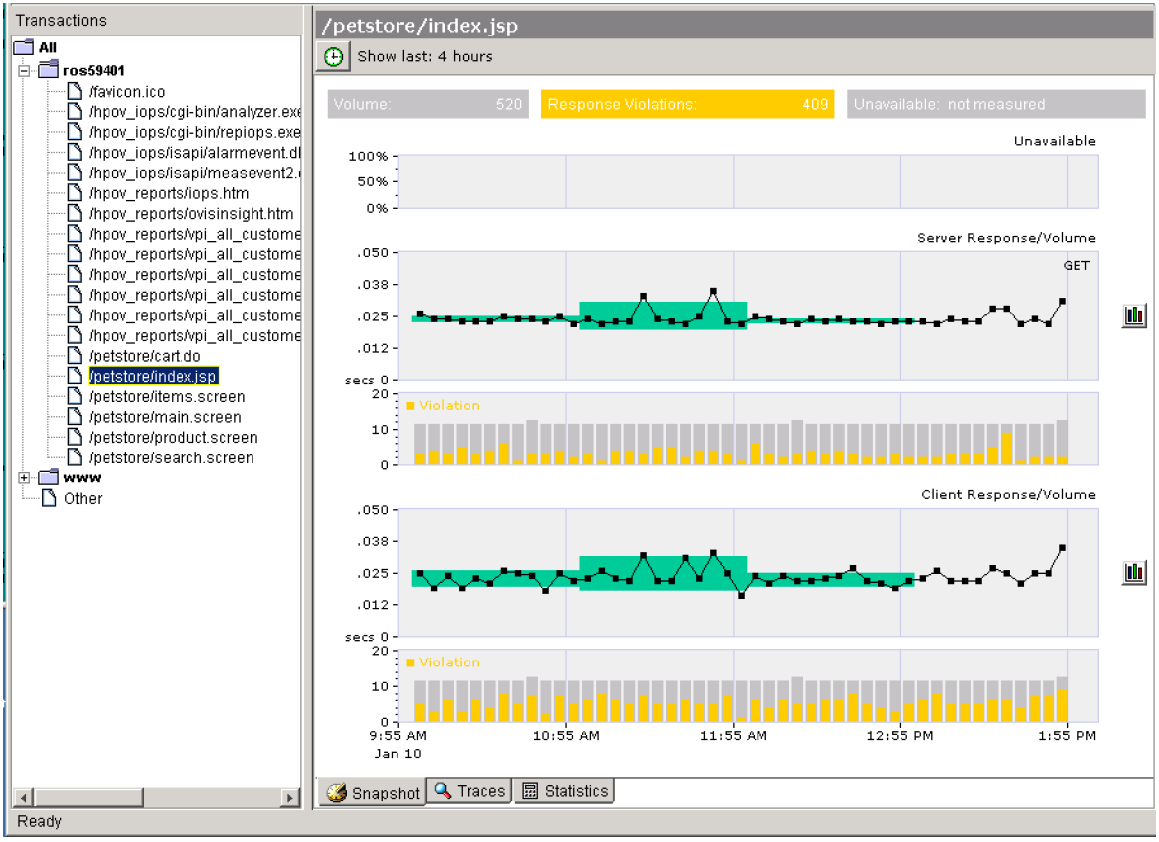
You can select the Reports tab to see long-term reporting. These reports are generated automatically every night and so will not be available until the day following installation and configuration. The out-of-the-box reports provided with OVIS are as follows. For the first three you can select all service types or a particular service and all customers or a particular customer

- Least Available by Service Group
- Highest Response Time by Service Group
- Highest Service Level Violations by Service Group
- Dial-Up Failures



Web App Tab

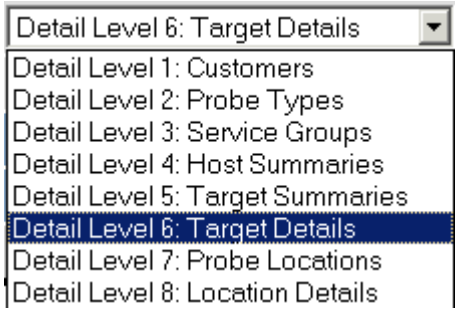
If you have integrated OVIS and OpenView Transaction Analyzer (OVTA) then you will see the Web App tab. You can launch the OVTA Console from this display. See Chapter 5, Integrating with OpenView Products for information about OVTA.



Common Dashboard Features

Drill Down Button

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. You can select different levels of drill down detail.



Trend Button

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.

Status Button

From the Snapshot display you can select the **Status** button which will display the status of service target availability.

Trace Button

If you have OpenView Transaction Analyzer (OVTA) configured to integrate with OVIS then you will see a **Trace** button in the Dashboard at the top of the page (except in the Snapshot and Reports pages). Trace shows HTTP and HTTP_TRANS service targets that are monitored by OVTA on the back-end web and application servers.

In the Trace page, clicking the Drill Down button launches the OVTA GUI, automatically selecting the corresponding transaction and showing the trace view for this transaction. See "Integrating with OpenView Transaction Analyzer" on page 178 for how to integrate with OVTA. Refer to the *OVTA User's Guide* for more information about the OVTA GUI.

Graphs Button

Select the **Graphs** button at the top of the page to draw additional graphs. If you use 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.
3. You should also uninstall any OVIS patches via Add/Remove programs, even those from previous releases.

3

Configuring Internet Services

Topics covered in this section are as follows:

- Configuring Services
- Configuration Manager
- Setting Objectives and Configuring Alarms
- Setting Up Service Level Agreements (SLAs)
- Probe Location Settings

  Configure the Network Connection

  Probe Timing and Scheduling
- Configuring Scheduled Downtime
- How Probes Work
- Remote Probes

  Configure Remote Probes

  Automatic Download of Updated Configuration

  Install and Remove Remote Probes
- Limiting Access to the Dashboard Data Display using Restricted Views
- Automating Configuration of Large Numbers of Service Targets

Configuring Services

As described in Chapter 1, the Internet Services service hierarchy provides a means of organizing the services on which you want to receive reports and problem notification.

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 location**: the service recipient's location (where the service request originates) and information about how to connect to this location.

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

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.

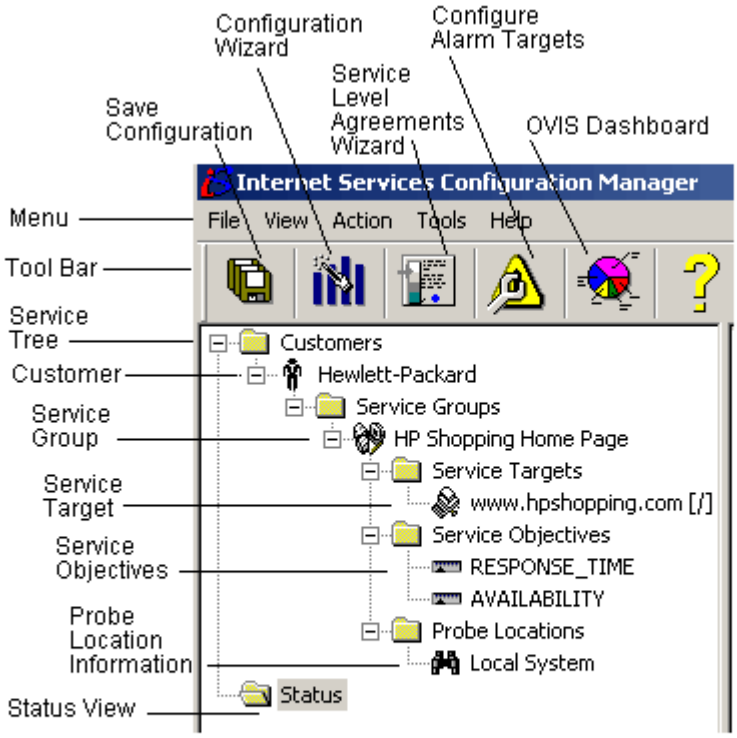
You can configure these services, using the **Configuration Manager** (see the sections below). And within the Configuration Manager you can use the **Configuration Wizard** to step you through setting up services.

As an alternative you can use the **Batch Configuration** 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 100).

Configuration Manager

You can use the Internet Services Configuration Manager to add, modify and delete services including: customers, service groups, service targets, service level objectives, probe locations, service level objectives and their settings.

To open the Configuration Manager window, select **Start > Programs > HP OpenView > internet services > Configuration Manager**.



The Configuration Manager facilitates the configuration process with a **Service Tree** display that shows how customers/service groups and their service targets, objectives, and probe locations are super- and sub-sets of each other.

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

You can access the **OVIS Dashboard** from the Configuration Manager toolbar. You can use the **Online Help** for details on using the Configuration Manager.

Using the Configuration Manager

To add, edit or delete items in the Configuration Manager you can right-click on the folder in the left pane tree view and select an action from the pop-up menu displayed. You can also run the wizards from these pop-up menus.

To configure a service you can use the Configuration Wizard or follow these general steps:

1. Create a customer
2. Create a service group and select the type of service to be monitored from the list displayed (for example HTTP, FTP, DNS services).
3. Define a service target. The information required depends on the service type.
4. Define service objectives for performance metrics such as availability and response time. You can also define service level agreements.
5. Define the probe location and any information needed to set up connections to remote systems. Also define probe timing and scheduling information as needed.

See "Quick Start for Using Internet Services" on page 33 for example of using the Configuration Manager to set up your services.

Also refer to the online help for detailed information on each of these steps and on the different service types.

Other Configuration Options

From the OVIS Configuration Manager **File > Configure** menu you can also configure the following:

- Alarm Destinations - Send alarms to OpenView Network Node Manager, OpenView Operations and OpenView Operations for Windows. You will also need to configure the integration between OVIS and NNM or OVO. See Chapter 5, Integrating with OpenView Products for details.
- Dashboard Settings - Configure default setting for the OVIS Dashboard such as what you want the default time span to be for the data display and what the minimum and maximum percentages should be in the Dashboard gauges.
- Database - Configure the database login and options for retaining data in the database.
- License - View license data and run the License Wizard to get license keys.
- OpenView Transaction Analyzer (OVTA) Measurement Server - Define the location of the OVTA measurement server to be used when configuring the integration of OVTA and OVIS.
- Restricted Views - Configure restricted views of the OVIS Dashboard data display by customer.
- Probe Scheduling Options - Set the probe scheduler to not restart after saving configuration changes and set the network connections to run one after the other (serialize).
- Schedule Downtime - Configure a new downtime value that can be applied to services.
- SLA Conformance Levels - Define service level agreement conformance levels such as Gold = 95%. These levels can be applied to SLAs.
- Tracing Levels - Specify more detailed server or probe tracing for use in troubleshooting.
- Web Server Properties - Configure communications between server and probe systems.

See the online help for more information on these items. Also in the Configuration Manager you can select **Tools > Probe Info** to get a report of how many service targets you have set up.

The rest of this chapter goes into more detail on the following:

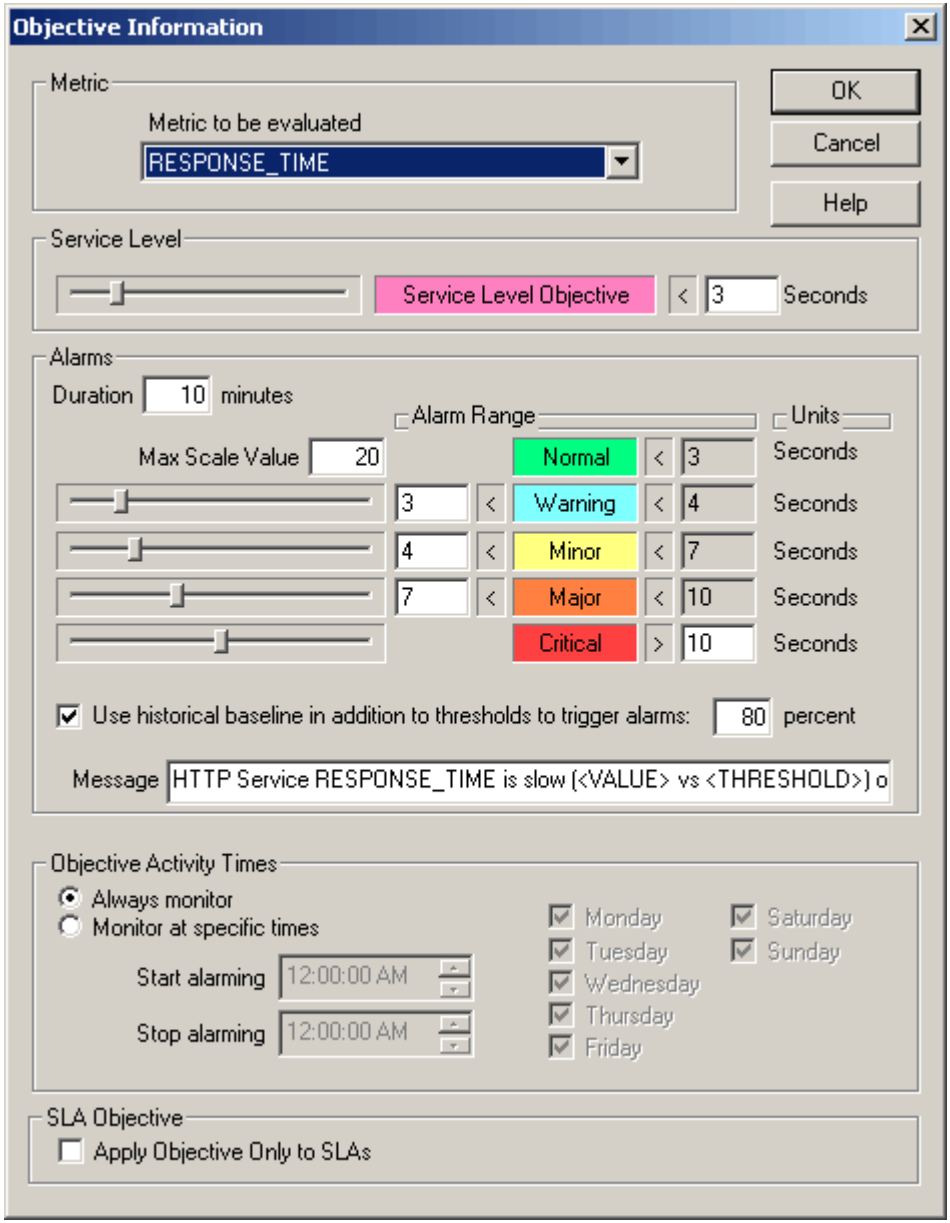
- Service level objectives and alarms
- Service level agreements
- How probes Work
- Probe timing, scheduling and defining the probe location
- Scheduled downtime
- Configuring and installing remote probes
- Restricted View.

Setting Objectives and Configuring Alarms

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

One criteria in deciding how to group targets in a service group is that they have similar expected performance characteristics. For example, grouping two HTTP targets with very different response times wouldn't be a good idea if you wish to set a response time SLO for the group or alarm on response time.

The Configuration Manager facilitates this process by providing the dialog that follows.


Objective Information
Metric
Metric to be evaluated
RESPONSE_TIME
OK
Cancel
Help
Service Level
Service Level Objective
< 3 Seconds
Alarms
Duration 10 minutes
Alarm Range
Units
Max Scale Value 20
Normal < 3 Seconds
3 < Warning < 4 Seconds
4 < Minor < 7 Seconds
7 < Major < 10 Seconds
Critical > 10 Seconds
Use historical baseline in addition to thresholds to trigger alarms: 80 percent
Message HTTP Service RESPONSE_TIME is slow (<VALUE> vs <THRESHOLD>) o
Objective Activity Times
Always monitor
Monitor at specific times
Start alarming 12:00:00 AM
Stop alarming 12:00:00 AM
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday
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 (previously known as ITO), OpenView Operations for Windows and other event managers that accept SNMP. See "Send Alarms" on page 69.

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. The settings provide a value against which the collected metric value for the service group is evaluated. See subsequent sections for details on these setting.

- **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 Dashboard display. Service level settings are *not* used for generating alarms.
- **In the Alarms section**, use the slider bar to define alarm event range values for each of the following categories:
  - WARNING
  - MINOR
  - MAJOR
  - CRITICAL
  - If the metric doesn't fall into any of these ranges, the status is considered to be NORMAL.

Note that in response time or other metrics where the values are less than a given value, you modify the values starting at the top (Warning). In the availability metric where the values are greater than a given value, you modify the values starting at the bottom.

In response time type metrics note that the range includes the higher number but not the lower number. For example: 2 < Warning < 5 would meaning warning for response times of 3, 4 and 5 seconds.

- **Duration**: Indicates that a probe metric value for a target 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 by not alarming unless a metric exceeds its configured threshold continuously for the duration configured.

  Setting a longer duration delays any actions until incoming metric values exceed the limits for the entire duration period. 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.

The Duration setting is for alarms only; service level violations are counted regardless and reported in the Internet Service Dashboard.

- **Use historical baseline...**: When unchecked, it is not used for alarms. Check Use historical baselines to restrict the number of alarms. The baseline value 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 hour of the day. A baseline normal range is calculated automatically. Baselines work well for high-use periods when metric values peak but are still considered normal.
- **In the Objective Activity Times sections**, you can filter the time periods you would like to alarm. This is useful to avoid false alarms during times when objectives are not expected to be met, such as backups.
- **SLA Objective:** Check this box if you want the objective applied ONLY to Service Level Agreements and not to alarming. See Setting Up Service Level Agreements (SLAs) for more information on SLAs.

When Availability is zero (that is, a target is unavailable), then all of its other metrics are considered invalid and not calculated for alarming. It makes no sense to consider response time when a target is unavailable. Also, availability is either 0 or 100% for a target in a given interval. Even though the slider bar allows settings between 0 and 100%, there is no difference for alarming or service level objectives between setting the availability metric objective at the default 90% level or at 100% since availability will always be either 0 or 100% for any target in the service group for a specific interval.

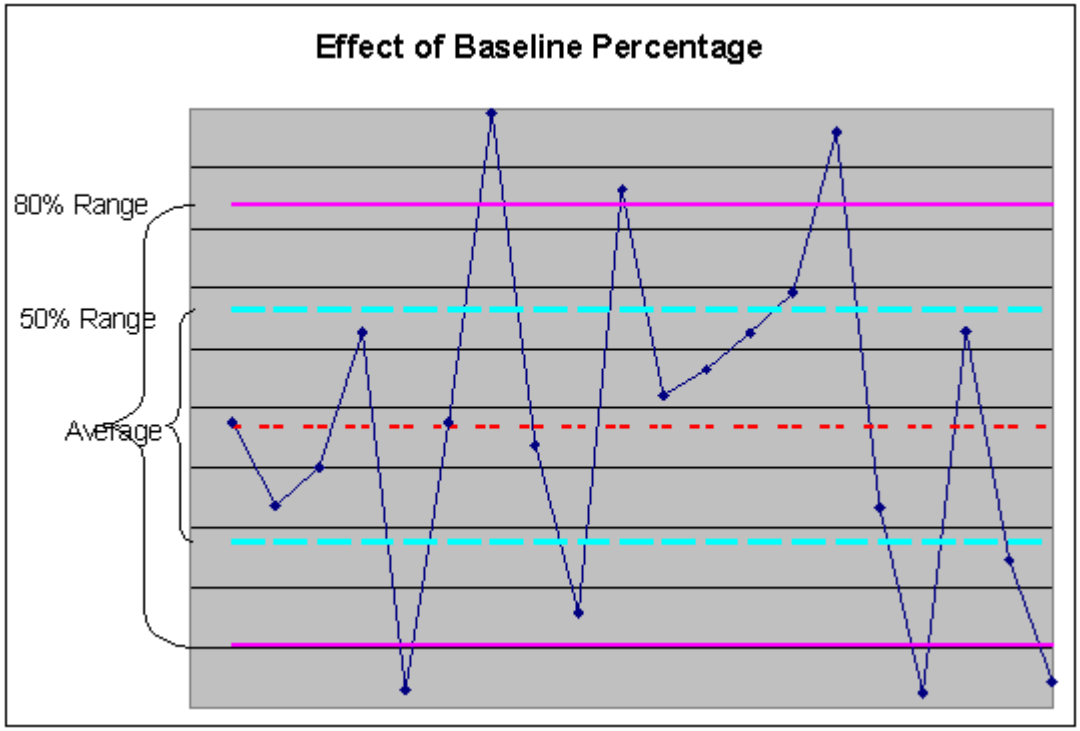
How Baselines Work

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.

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.

Caution: When trying to create alarms for test purposes, you should set baselines to off since it may inhibit the alarms you are trying to test.



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.

How Alarms are Triggered

The following process outlines how alarms are triggered based on settings in the Objective dialog:

1. Incoming measurements for each target in a service group are evaluated against the objectives specified. For each target, the objective starts out in the NORMAL state. As new data arrives from the probe, it is compared against the objective ranges.
2. If the value is within the ranged defined as NORMAL, then the objective state remains NORMAL and no alarm is triggered.
3. **Without Baselines:** An incoming metric value must exceed the threshold until the end of the interval for an action to occur. If the metric value falls within an alarm range (or severity, such as WARNING), the duration timer is reset. If the count exceeds the Duration defined, then the objective changes state to that of the alarm range. This is considered to be the START of the alarm event. Thus a target probed every 5 minutes with duration of 5 minutes would have to exceed the limit for 2 consecutive intervals to trigger an alarm.
4. **With Baselines:** 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.
5. If the metric value remains in the same range for another DURATION interval, this is considered to be a CONTINUED alarm event. If the metric value changes to another alarm range (either higher or lower) for the specified DURATION, the alarm event will START at the new severity.
6. When the metric value falls into the NORMAL category the alarm event will returns to the NORMAL status and this is the END of the alarm event.

Alarm Message

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)

Keyword	is replaced with
<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)
<ERROR_INFO>	Probe specific error information. For example, for HTTP_TRANS probes this will show the step where the failure occurred and the failed pattern and HTTP status code.
<METRIC1>	Metrics are probe specific. Refer to the List of Metrics in Chapter 4.
<METRIC2>	Metrics are probe specific. Refer to the List of Metrics in Chapter 4.
<METRIC3>	Metrics are probe specific. Refer to the List of Metrics in Chapter 4.
<METRIC4>	Metrics are probe specific. Refer to the List of Metrics in Chapter 4.
<METRIC5>	Metrics are probe specific. Refer to the List of Metrics in Chapter 4.
<METRIC6>	Metrics are probe specific. Refer to the List of Metrics in Chapter 4.
<METRIC7>	Metrics are probe specific. Refer to the List of Metrics in Chapter 4.
<METRIC8>	Metrics are probe specific. Refer to the List of Metrics in Chapter 4.

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:

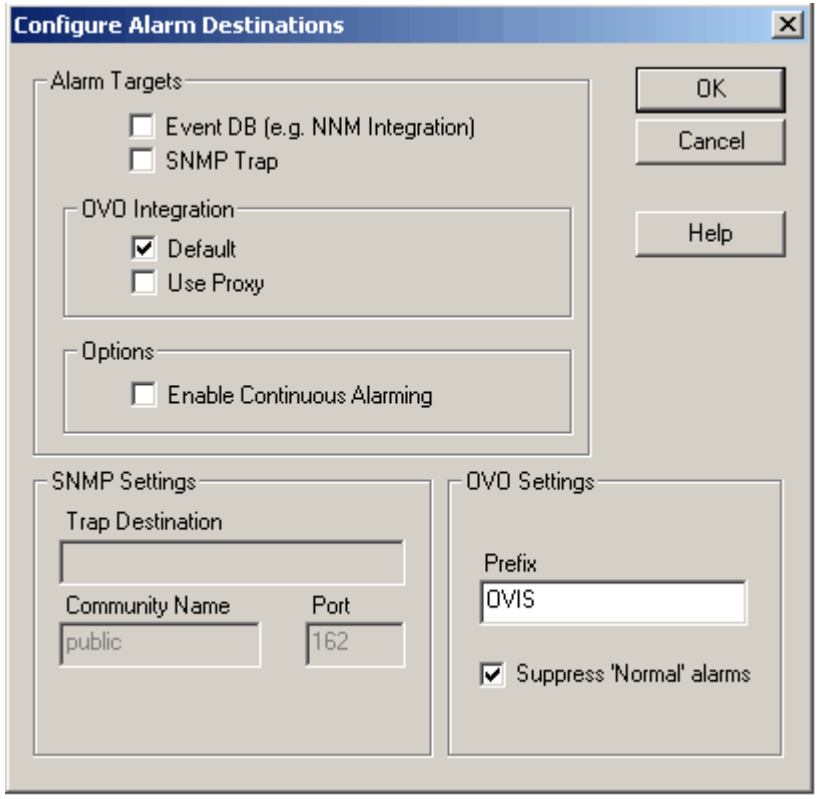
> HTTP response time from **curly.myhouse.com** to **webserver1.yourhouse.com** is 7 seconds (should be < **5.0** or between (**3.2** and **6.5**)

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

Send Alarms

Internet Services can send alarms to Network Node Manager (NNM), OpenView Operations for UNIX (previously known as ITO), OpenView Operations for Windows and other event managers that accept SNMP traps.

First you set up the Service Level Objectives that will trigger the alarms. Then you set up the alarm destinations using the Alarm Destinations dialog accessed from the Configuration Manager **File > Configure > Alarm Destinations**.



For details on integrating Internet Services with OpenView Operations (OVO) and/or NNM, please refer to Chapter 5, Integrating with OpenView Products.

When you save any configuration changes in the OVIS Configuration HP Internet Services service is restarted unless you have configured it not to do so. The OVIS component handling alarms and SLOs is restarted as well. This results in the current alarm state being lost during a restart.

Setting Up Service Level Agreements (SLAs)

You can configure Service Level Agreements in Internet Services.

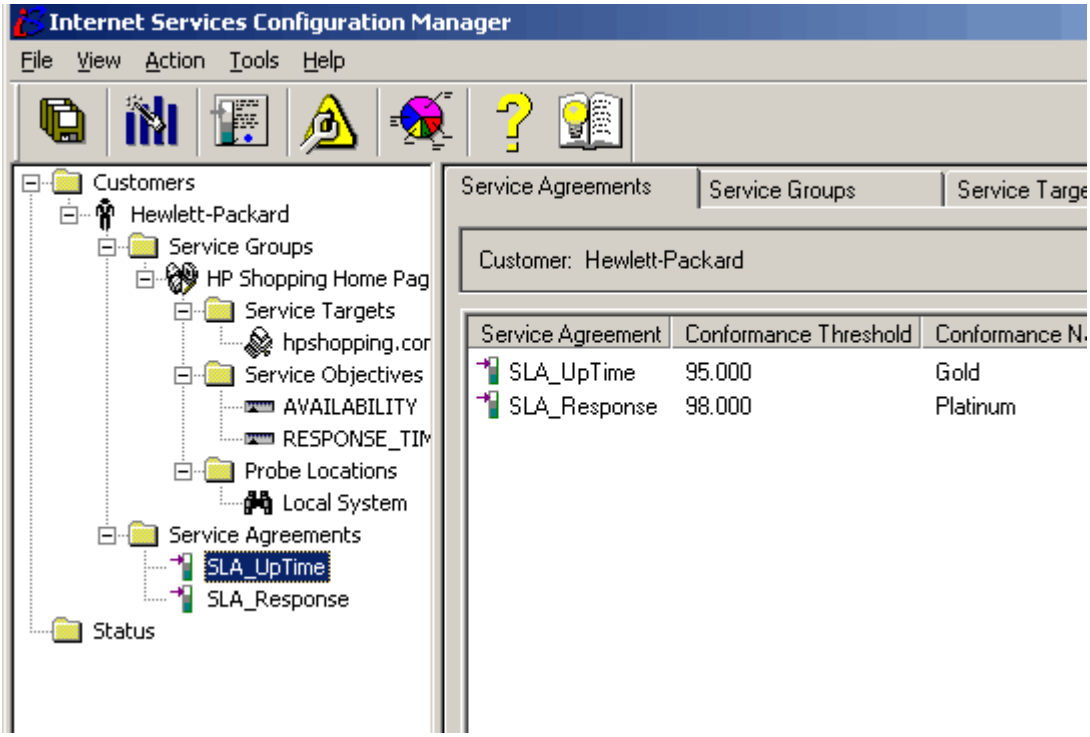
A Service Level Agreement (SLA) is based on a contract between the IT organization and the business customers. The SLA describes the quality level of IT service by defining service level objectives for a services in terms of availability and performance (based on metrics such as response time).

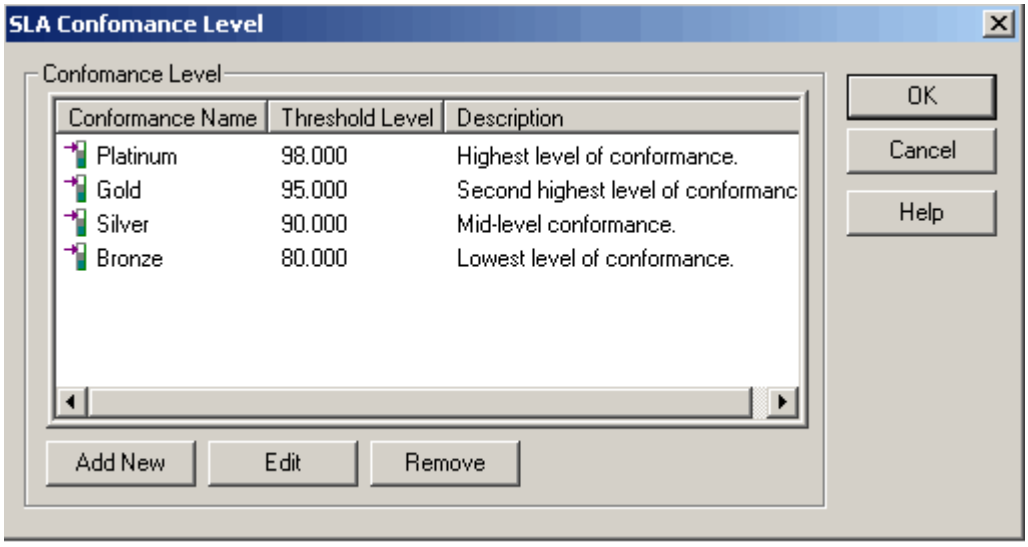
SLAs are created using either the SLA Configuration wizard (accessed from the **File>Configure** menu in the Configuration Manager) or by using the SLA Configuration dialog in the Configuration Manager. You set up the SLA for a customer and a set of service groups.

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.





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 an 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.

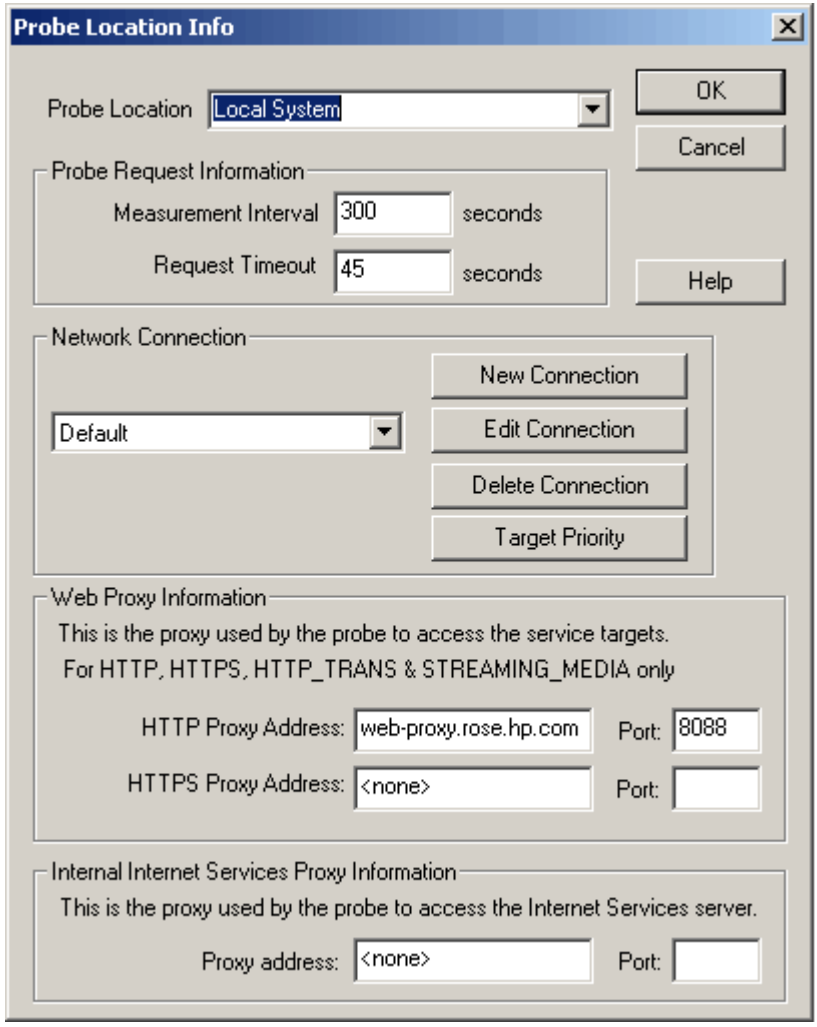
You can also set SLA conformance thresholds in the Configuration Manager (for example platinum = 98%, gold = 95%, silver = 90% and bronze = 80%). These are compared with the resulting SLA conformance at each hour. If an SLA does not meet or exceed the SLA conformance threshold, an alarm will be generated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

Probe Location Settings

The Probe Location dialog is used to specify a location where the probes will be running. But this same dialog is also used to configure the following:

- What kind of network connection the probe should use.
- How often you want the probe to initiate measurements.
- When the probe should retry and how often to retry before timing out.
- What the priority should be for the probe when scheduling measurements.



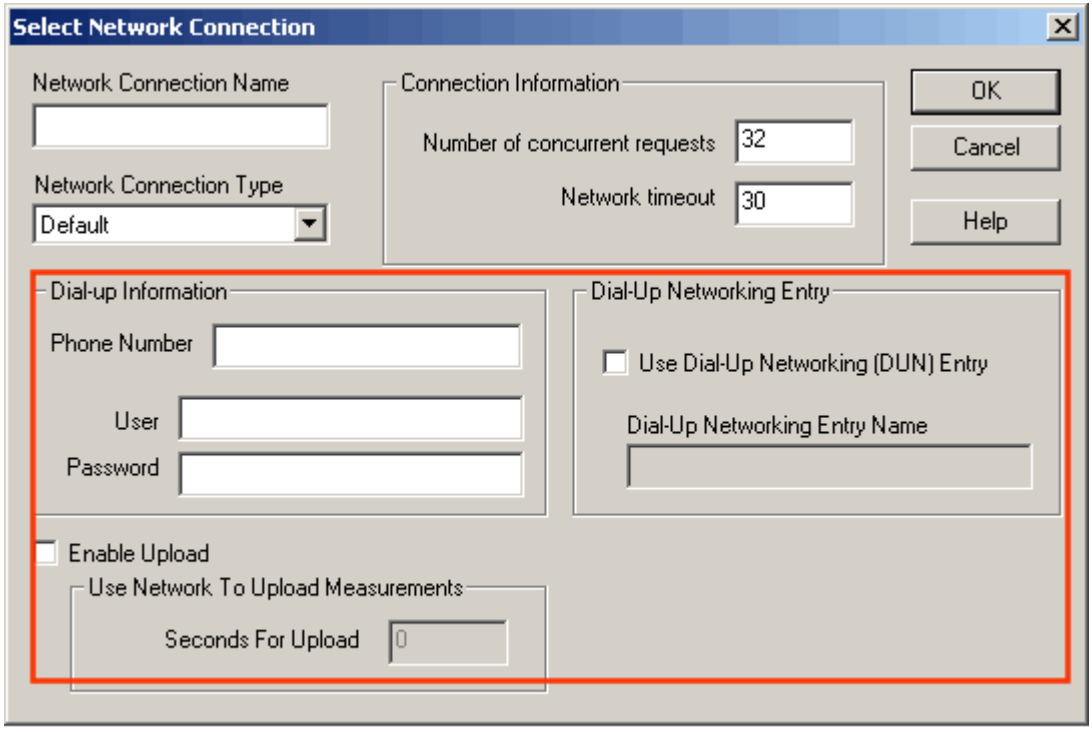
Configure the Network Connection

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, you can configure other network connections and define concurrency

for each connection using the Network Connection option. If any probes will use a Dial-Up connection to the service target, you can also configure that connection using the Network Connection option.

In the Probe Location Info dialog, you can press the **New Connection** button to Add/Edit/Delete a network 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.



To configure a Dial-Up network connection 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).

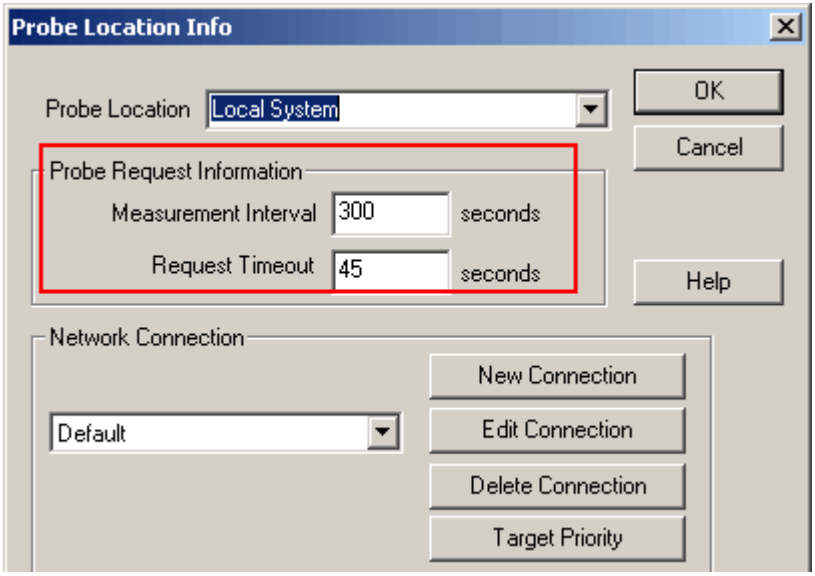
You can run multiple probes over this single Dial-Up connection and login. To do this for other probes under a Customer group, you open the Probe Location window and select the Dial-Up connection you just configured as the network connection.

The Dial-Up probe works in the background tracking the time it takes to dial and connect 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.

You can select **Enable Upload** to specify that probe data should be sent over a Dial-Up connection. Note that only one of your network connections may be enabled to send probe data over Dial-Up and it must be a dial-up connection on Windows.

Probe Timing and Scheduling

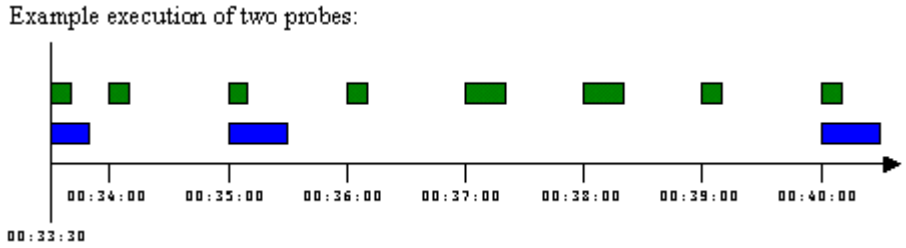
The scheduler component executes the probes at the intervals specified in the Probe Location dialog under the **Measurement Interval** field.



For example, the value 300 tells the scheduler to probe all targets that are contained in this Service Group for this probe location, every 300 seconds (5 minutes). The smallest value that can be specified is 60 seconds.

The time allowed for probing a target is specified in the **Request Timeout** field. A probe usually determines itself when it ran longer than the timeout. Depending on the probe type, it will determine that the target is unavailable when the timeout is exceeded.

Under certain circumstances, the scheduler will terminate a probe if it runs longer than the specified timeout (for example, if the timeout is 10 seconds, the scheduler will terminate the probe if it runs longer than 13 seconds). This ensures that only a certain number of probes are running at the same time. In these exceptional cases no data record is generated by the probe's execution.

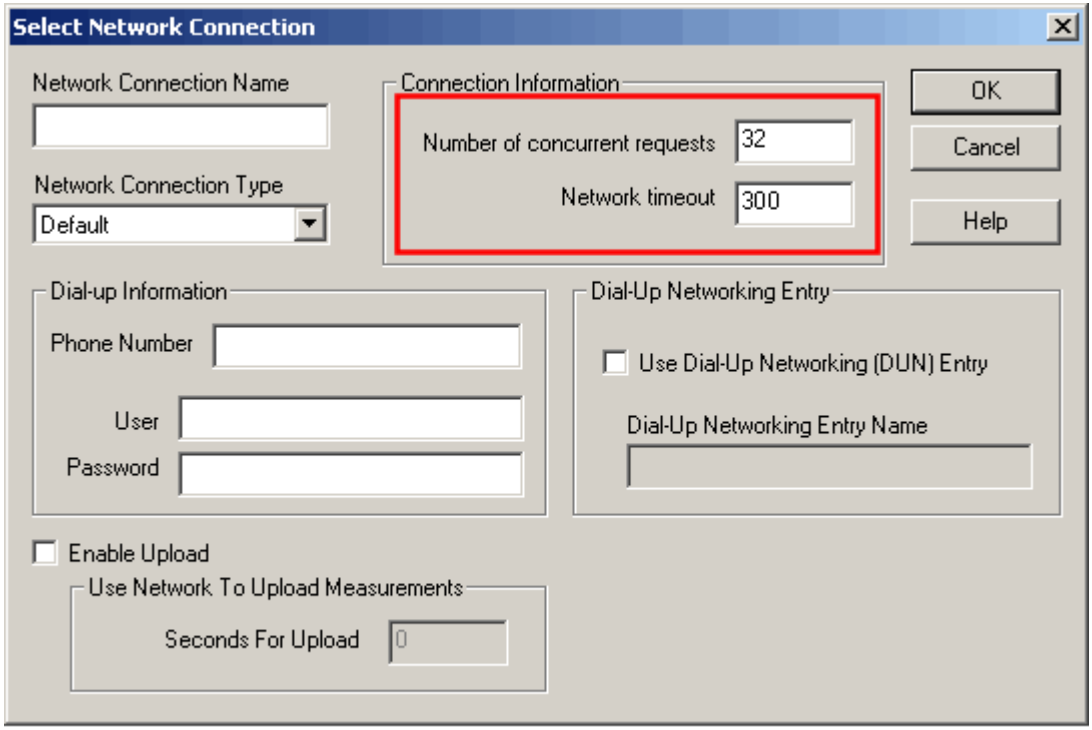


Example Execution of Two Probes: In the above example, there are two probes configured, one shown in the top row and the other shown in the bottom row. The probe in the top row has an interval of 60 seconds and a timeout of 20 seconds, and the probe in the bottom row has an interval of 300 seconds and a timeout of 30 seconds.

The scheduler is started at 00:33:30 and immediately executes all probes. This ensures that there is an immediate response when looking at the dashboard. The scheduler then tries to align the intervals. For example, a probe at a 300 seconds interval is always executed at xx:00:00, xx:05:00, xx:10:00,…, xx:55:00, where xx is any hour.

The scheduler may delay the execution of a probe for up to 10 seconds since it may take up to 10 seconds for the scheduler to see whether a probe is ready to run. So in the above example, the probe scheduled for xx:05:00 might actually start at xx:05:09.

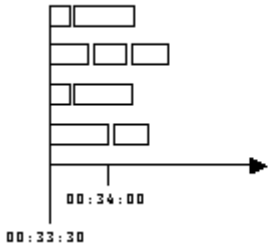
Set Number of Targets Probed Concurrently: The number of targets probed at the same time is specified in the **Number of concurrent requests** field, which is located in the Network Connection dialog (accessed from the Connection buttons in the Probe Location dialog).



The default is to probe 32 targets concurrently. This concurrency parameter is dependent on the probe type, network bandwidth and system performance. For more information, please refer to "Scalability Information" on page 266.

HTTP_TRANS heavyweight (IE mode) probe is much higher overhead than the other probes because each one is running a copy of Internet Explorer. A concurrency of 1 is best for this probe.

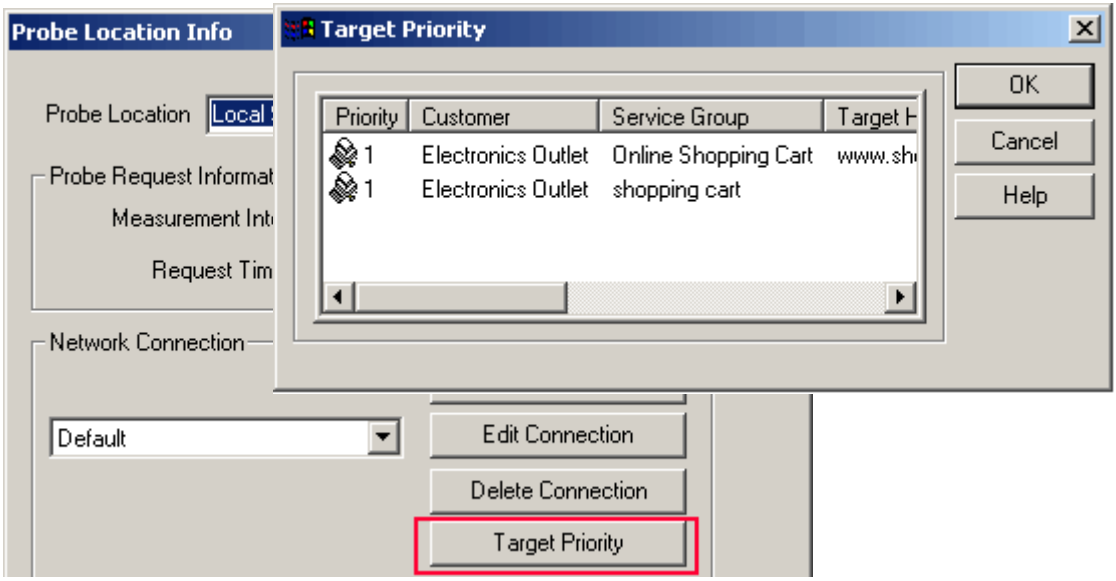
Example execution of 9 probes with concurrency of 4:



In the above example, the scheduler makes sure to only have 4 probes running at the same time. The concurrency and the timeout parameter will therefore determine the interval of the probes. For example, it is not possible to schedule 64 targets with concurrency of 32 every 60 seconds if the timeout of a target is 40 seconds since in the worst case, where all 64 targets time out, the total execution time for all probes will be 40 seconds + 40 seconds = 80 seconds which is greater than the interval of 60 seconds.

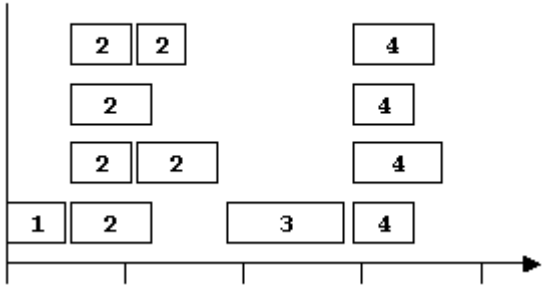
Set Target Priority for Probe Scheduling: The execution of targets can be ***prioritized***. This is helpful for load balancing executions where, for example, you want your HTTPTRANS probe to execute without other probes running in parallel, or when certain probe types need to be run first. If you do not specify the priority probes will run based on the concurrency setting and beyond that in order of configuration.

In the Configuration Manager Probe Location dialog select the **Target Priority** button to specify the priority of probes.



The Target Priority dialog lists all targets specified for this Probe Location and network connection as defined in OVIS. The lower the priority number associated with the target, the sooner the target will be probed. Targets with the same priority are executed in parallel within the specified concurrency limits.

Example execution of 12 probes with concurrency of 4 and priorities set:



In the above example, the target with priority 1 is probed first, then all targets with priority 2. Once all the targets with priority 2 have finished, the target with priority 3 is probed. Once the target with priority 3 is finished, all targets with priority 4 are probed.

The default priority is 1 unless changed in the Target Priority dialog. Please note that using priorities usually requires more time to execute all probes, which needs to be factored in when specifying the intervals. When new targets are added after changing the priority, the highest priority number will be used for this newly added target. For example, if the highest priority number is 3, a target that is added will also have priority 3.

Dial-Up and LAN Connections: Networks Connections can be used to execute probes over a Dial-Up connection. Dial-Up parameters such as DUN, username/password and phone number can be entered in the Select Network Connection dialog. The default network always probes using the LAN.

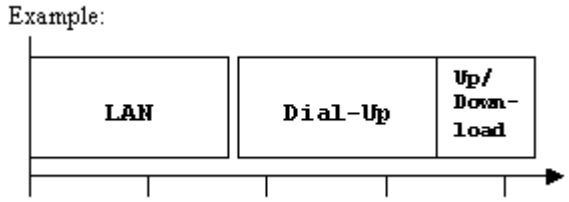
Usually, it is only necessary to have one or two network connections configured.

The combinations are the following:

- LAN
- Dial-Up
- LAN and Dial-Up

The LAN and Dial-Up option allows probing a LAN and uploading the measurements and downloading configuration through the Dial-Up connection.

Probe Data Over Dial-Up: The scheduler periodically checks for new configuration and uploads measurements that are stored in the queue directory. This behavior can be changed in the Select Network Connection dialog by checking the box for **Enable Upload** so that the new configuration download and measurement upload happens on a particular network after all targets have been probed. This allows the scheduler to use an established Dial-Up connection for communicating with the server.



In the above example, all targets associated with the default LAN network connection are executed. Then, the Dial-Up network is established and all targets associated with the Dial-Up network connection are executed. Once all targets have been executed, new configuration is downloaded and measurements are uploaded over the Dial-Up connection.

The maximum number of seconds that should be spent for the server communication can be specified in the Select Network Connection dialog. The default is 10 seconds, which may need adjustment depending on the number of targets that produce measurements. Further, the interval needs to be set so that no target is ready for execution while another network is still executing targets or performing server communication.

It is also possible to specify a network timeout which will not execute new probes once the timeout has been reached.

Things to watch out for:

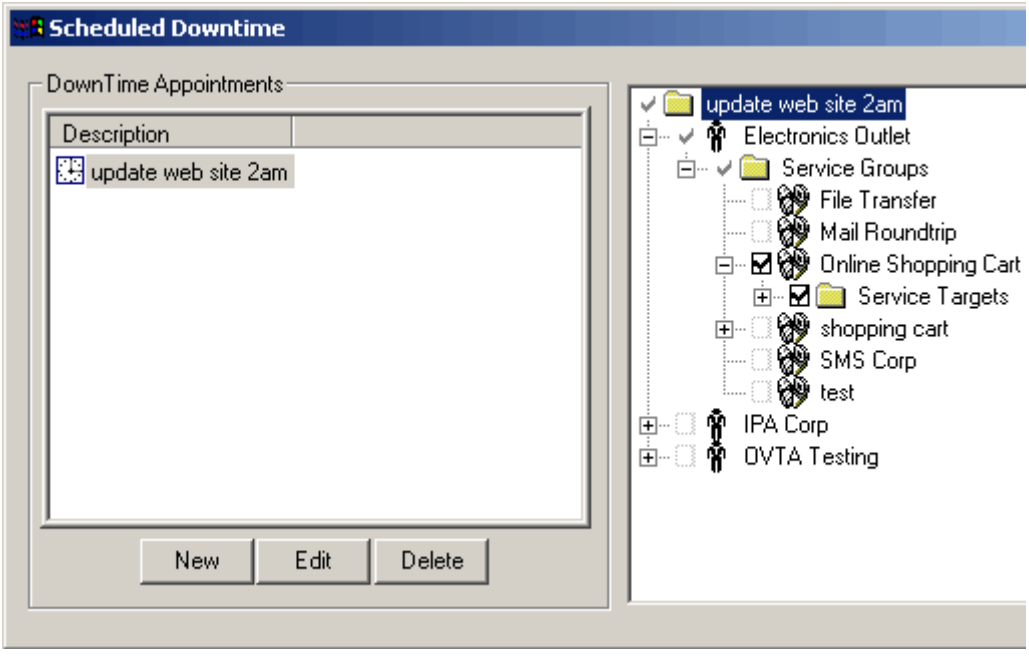
- Odd intervals such as 71, which don't fall on minute boundary, are possible as well but may have some of the following implications:
  - Cookie "scrubbing" for the heavy weight HTTPTRANS probe may not happen if the intervals are not multiples of five minutes (for example, 300, 600, etc).
  - In mixed LAN/Dial-Up network configuration, a LAN probe might be executed during Dial-Up
  - Probe sequencing can't be guaranteed for intervals which are not multiples of five minutes (for example, 300, 600, etc).
- A small network timeout can prevent probes from starting.

- A Dial-Up connection that is used for server communication might not be able to "catch up" with buffered measurements if the number of measurements is very high. Always allow enough communication time and use larger intervals (for example, 10 minutes).

Configuring Scheduled Downtime

You can set scheduled downtime for probes to prevent measurements from being gathered during specific time periods.

Set Downtimes by selecting from the **File > Configure > Schedule Downtime > Configure Downtime** menu. You can set up downtimes and apply selected downtimes to items in your service tree such as customers, service groups and service targets.



In the Scheduled Downtime dialog, create a downtime using the **New** button, edit an existing downtime using the **Edit** button, or delete an existing downtime using the **Delete** button.

The **New** and **Edit** button display the Scheduled Downtime Targets dialog where you enter the Time and Date for the downtime. You can also set up a Recurrence for the downtime. There are two basic forms of downtime, single instance and recurrence downtimes. Single instance occurrence downtime is a downtime that applies for a specific time and date. Recurrence downtimes are applicable for specific reoccurring time intervals (such as from 12:00 to 1:00 daily).

Once you have created the downtimes, you can schedule downtime for a particular item as follows:

1. Select any of the downtimes listed then check any item in the simplified tree in the right pane of the Scheduled Downtime dialog (that is a Customer, Service Group or Service Target). A check mark indicates the downtime has been applied. Only downtimes that are applied to an item have any effect.

2. Note that a downtime can be applied globally (like a template) by checking the box next to the downtime at the top of the tree in the right pane. A message prompts for if you want to make this a global template. Click **Yes** to apply this downtime globally to all customers, service groups and targets. Click **No** if you don't want it applied globally.

   Note that with a Global downtime template, this downtime will automatically be applied to any new service targets you add.

   Also with a Global downtime template, you won't be able to selectively check and uncheck the downtime for each item in the tree.

   If you have a large number of targets configured, it is better to use a global downtime template rather than applying downtimes individually, because the performance is better.

3. You can review the downtimes for a service target, service group or customer by going back to the main view in the Configuration Manager. Then select the item in the left pane and the information about this item is displayed in the right pane. Select the Downtime tab in the right pane to view any scheduled downtime for this item. Note that if the item is down now, the current downtime will be highlighted in blue. Also note that from the Downtime tab you can right-click to select Configure Downtime.

Note that downtimes can be applied to other customers, service groups or targets.

A special case you may want to configure is Always Down. You can create a scheduled downtime called "Disable - Downtime 24/7" with a start time of 12:00:00 AM and End Time of 11:59:59 PM. Once created this downtime can be applied to any service groups and their probes.This has the effect of the probes in a service group never running. Downtimes can be applied across the midnight boundary.

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 Chapter 4, Descriptions of Service Types/Probes 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 Configuration Manager on the Management Server reports **No Probe Info** from the probe system in its Status view rather than **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 availability of each target 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

Internet Services allows you to deploy probes to remote system locations. 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 probes send collected data back to the central Management Server for monitoring.

Configure Remote Probes

You create remote probes just as you would local probes, using the OVIS Configuration Manager to set up your service targets.

Then, using the Probe Location dialog, you define the remote system where you plan to deploy the remote probes.

When you save the configuration and exit the Configuration Manager, OVIS creates a `config_<system_name>.dat` file and stores this file in the `\<install dir>\newconfig` directory. The `<system_name>` must match the remote system name.

After the probes are configured to run remotely, you will need to install the probes on the remote systems. See "Install and Remove Remote Probes" on page 92 for how to install the remote probes.

Automatic Download of Updated Configuration

If you modify the configuration for a probe after the initial installation on a remote system, the updated configuration files will automatically be downloaded for you from the Management Server. And the changes will take effect.

The remote probes check every minute for new configuration on the Management Server. If new configuration file 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 of the Configuration Manager), 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.

Install and Remove Remote Probes

Once you have configured your remote probes and saved the configuration, you need to install them onto the remote Windows and UNIX systems. On Windows systems you can either install interactively or in silent mode.

Install Remote Probes Interactively on Windows Systems

To interactively install probes on remote Windows systems you must transfer the installation files to the remote system (you could use FTP) and execute the installation program. See "Install Remote Probes in Silent Mode on Windows Systems" on page 93 for silent install instructions.

1. Copy `\<install dir>\newconfig\remote_probes_install.exe` file to the remote probe system.
2. (Optional) If there are no other OpenView products are on the system including previous versions of the remote probes, you may change the drive and directory as described in this step.

   If there are already other OpenView products installed on the remote system you may NOT change the established install drive and directories (for example c:\rpmtools and c:\rpmtools\data) used during remote probe installation.

HP OpenView tools on Windows-based operating systems use registry entries in the `\HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard` hive during installation to tell if other OpenView tools are already installed and what the common directories are. The installation looks in this hive for `InstallDir` and `DataDir` keys underneath `HP OpenView`, or for a product name entry which contains a key named `RPM ID` and the path keys named `CommonApplicationPath` and `CommonDataPath` underneath `Current Version`.

To change the drive or directory, on the remote system, bring up a Command Prompt window and enter the following commands in the Command Prompt window

```
SET OVIS_INSTALLDIR=<install path>

SET OVIS_DATADIR=<installdata path>

remote_probes_install.exe
```

Where *<install path>* and *<installdata path>* are the drive and directory for the install directory and the data directory.

Note that the `remote_probes_install.exe` program must be run from the Command Prompt window for the SET commands to work.

3 If you haven't done so, execute `remote_probes_install.exe` from a Command Prompt window on the remote probe system. This will install the remote probe binaries. In the dialogs that display, enter the hostname of the Internet Services Management Server and other values as prompted. When the installation is complete the scheduler service is restarted with the new hostname of the Management Server.

Install Remote Probes in Silent Mode on Windows Systems

You can use silent mode to install probes on remote Windows systems as follows:

1 Copy the following files from the Management Server to the remote probe system:

```
\<install dir>\newconfig\remote_probes_install.exe

\<install dir>\newconfig\remote_probes_install.cmd

\<install dir>\newconfig\setup.iss
```

The .cmd file supplies replies for the questions asked interactively during install.

2 Edit the `remote_probes_install.cmd` file to supply appropriate values for your environment.

Environment variables are described in the remarks contained in the `remote_probes_install.cmd` file.

The Environment variables are as follows:

- OVIS_SILENT=TRUE
- OVIS_HOST=ManagementServer
- OVIS_PORT=80
- OVIS_PROXY=someproxy:8088
- OVIS_SSL=0
- OVIS_IGNORE_CERT_ERRS=1
- OVIS_CERT_FILE=mycert.txt
- OVIS_CERT_PASSWORD=somepassword
- OVIS_INSTALLDIR=c:\Program Files\HP OpenView
- OVIS_DATADIR=c:\Program Files\HP OpenView\data

Two of the variables (OVIS_INSTALLDIR, OVIS_DATADIR) are used to set the drive and directory for the install and data directories. Note that if there are other OpenView products already installed on the remote system you may NOT set these variables. In this case the remote probe installation will follow the path already established by these products.

3 Save your changes. Launch the `remote_probes_install.cmd` file from the Command Prompt window.

Remove Remote Probing Completely from a Windows Systems

You can remove all remote probes from Windows systems interactively as follows:

1 Delete the remote Probe Location from all Service Groups 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 on the remote system, double-click on **Add/Remove Programs**. Select **HP OpenView Internet Services Remote Probes** and click the **Add/Remove** button to remove.

Or you can remove remote probes from Windows systems in silent mode as follows:

1 Delete the remote Probe Location from all Service Groups in the Configuration Manager and save the change.

2 Copy the script `\<install dir>\newconfig\remote_probes_uninstall.vbs` from the Management Server into the `\probes` directory on the remote probe system.

3 Run the script from the Command Prompt window as follows:

```
cscript remote_probes_uninstall.vbs -s //T:999
```

The -s specifies silent mode. The //T:999 is a parameter to cscript that sets the timeout to 999 seconds.

You can check the return values for whether the uninstall succeeded.

Example

If you wanted to change the install directory on a remote system, you would do the following:

1 Uninstall the remote probes interactively or in silent mode.

2 Copy the following files from the Management Server to the remote probe system:

```
\<install dir>\newconfig\remote_probes_install.exe
\<install dir>\newconfig\remote_probes_install.cmd
\<install dir>\newconfig\setup.iss
```

3 Modify the OVIS_INSTALLDIR and OVIS_DATADIR environment variables in the `remote_probes_install.cmd` file on the remote probe system to reference a new drive or directory and save the file.

4 Launch the silent install by running the `remote_probes_install.cmd` program from a Command Prompt window.

Install Remote Probes on UNIX Systems

This section gives you instructions for installing remote probes onto HP-UX, Solaris, and Linux systems.

HTTP_TRANS probe in IE (heavyweight) mode is not available for UNIX systems, but the lightweight modes are available. Also the Streaming Media, Cisco Works XSLAM, SMS, and ODBC probes are not available for UNIX systems.

Stop Internet Services (if applicable).

You only need to stop Internet Services is 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 "Configuring Secure Communication" on page 250 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`.

Remove Remote Probing Completely from UNIX Systems

1. Delete the remote Probe Location for all Service Groups in the Configuration Manager and save the change.
2. Log on as root on the remote 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.

If you have configured integration between OVIS and OpenView Transaction Analyzer (OVTA) then in order to view OVTA data from the Web App tab or Trace button in the Dashboard, either restricted views must not be enabled or if restricted views is enabled, you must be logged in as All Customers.

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.

Using the batch configuration is complex and requires a through knowledge of probe configuration.

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 117 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.

Configuration Parameters that are set through **File->Configure** in the Configuration Manager are not saved in the XML.

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:

- **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.
- **Removeall** removes all of the configuration information in Internet Services.
- **Check** the syntax of a configuration file. Report any errors but do not affect the Internet Services configuration.
- **Info**, shows information on probe systems and probe target count.
- The following options are also included:
  - The **`-quiet`** option 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, a 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 **norestart** parameter specifies not to restart services when executing an IOPSload -load.

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

```
IOPSload -load [-quiet] [-norestart] configfilename
IOPSload -save [-quiet] configfilename
IOPSload -remove [-quiet] configfilename
IOPSload -removeall
IOPSload -check configfilename
IOPSload -info
```

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 UTF-8 encoded 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 104 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:

LOCATION	is the start token
id=	is an attribute token
"Denver"	is data that is associated with the id attribute. Note that the data is enclosed in double quotes.
</LOCATION >	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. For example, <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 reinstated prior to the data being used.

To render this character	Use this string
&	&amp;
<	&lt;
>	&gt;
"	&quot;

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>
```

```
        <PRIORITY></PRIORITY>
        </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. You can look at the file <install directory>\newconfig\packages\reload_IOPS.SRP for details.

<TARGET

(...) >Attributes vary depending on the type of probe for this service target.

Table 1 Probe attributes

PROBE	Attribute	Description
DHCP	host= port= clientPort= acceptOffer= pattern= patternConfig= chaddr= retries=	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 client hardware address number of retries
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)

Table 1 Probe attributes (cont'd)

PROBE	Attribute	Description
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
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

Table 1 Probe attributes (cont'd)

PROBE	Attribute	Description
HTTPS	host= port= urlfile= username= password= options 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 Keep Alive and No Cache 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
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

Table 1 Probe attributes (cont'd)

PROBE	Attribute	Description
MAILROUND TRIP	rhost= sprotocol= sender= datasize= rport= rprotocol= recipient= rusername= rpassword= susername= spassword= pollinterval= ESMTP	system name of the email server protocol used by the sending server email sender name message size port for receiving server protocol used by the receiving server email recipient fully qualified address username for the email account on the receiving server password for the email account on the receiving server username for the sending email server password for the sending email server interval to check receiving server for message receipt. indicates if an ESMTP/SMTP-A server is used
ODBC	host= query= username= password= pattern= patternConfig=	ODBC system DSN for the database select statement for the database query user name to log on to the database password to log on to the database pattern to be applied to the query 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

Table 1 Probe attributes (cont'd)

PROBE	Attribute	Description
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
SAP	sapprobetype= sapsystemid= saphostname= sapinstance= sapclient= sapuser= sappassword= sapgwhost= saphwservice= saptcode=	sap probe type unique 3 character name for the system within the system landscape system name for the SAP server SAP instance SAP client number user name to access the SAP transaction password to access the SAP transaction gateway host gateway service SAP transaction code
SMS	phoneno= smscno= query= pattern= patternConfig= deviceEntry=	target phone number for the service center number for the SMSC the information you want queried pattern to be applied to the SMS message pattern configuration parameters the specific SendModem/ReceiveModem pair
SMTP	host= port= recipient= sender= dataSize= ESmtp= username= password=	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 indicates if you are monitoring ESMTP/SMTP-A servers username to authenticate ESMTP/SMTP-A server password to authenticate the ESMTP/SMTP-A server

Table 1 Probe attributes (cont'd)

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

<Priority

priority=”1”
location=”Local System”
network=”Default”

- Attribute **priority=** the scheduled order within probe location/network that the service target should run.
- Attribute **location=** specifies probe location name of the service target’s service group.
- Attribute **network=** specifies the network name of the service target’s service group.

<Objective

objectiveid="id"
metric="metricname"
condition="comparison"
servicelevel="service level value"
warning="value for alarm severity level of warning"
minor="value for alarm severity level of minor"
major="value for alarm severity level of major"
critical="value for alarm severity level of critical"
baseline="baselinepercent"
duration="seconds"
starttime="hh:mm"
stoptime="hh:mm"
days="MTWTFSS"
message="textmessage">

- 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
<	&lt;	Less Than
>	&gt;	Greater Than
<=	<=	Less Than or Equal to
>=	>=	Greater Than or Equal to
=	=	Equal to
!=	!=	Not Equal to

- Attribute **servicelevel=** specifies the value defined for the service level objective for this metric. The value may be for example "90.000" for 90 percent or "2.000" for 2 seconds.
- Attributes **warning= minor= major= critical=** specifies the values that would trigger an alarm with severity of Warning (cyan), Minor (yellow), Major (orange), or Critical (red).
- 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 (0-23) 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 begin 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 (cont'd)

Symbol	Substitutes for
<THRUPUT>	Throughput value (if available from the probe)
<ERROR_INFO>	Probe specific 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)

<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. Blank if no customer specified for this network.
- Attribute **"service="** specifies the name of the Service Group associated with this Network. Blank if no service group specified for this network.
- Attribute **"type="** specifies the Type of this Network Entry. Valid values are Default, LAN, Dial-up.
- 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. For example 300.
- Attribute **"concurrency="** specifies the number of concurrent probes that will be executing at one time for this Network. For example 32.

<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="** should always be TRUE.

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="IPA Company">
    <SERVICE id="Dns Services" probe="DNS">
      <TARGET     host="15.351.193.31"
                  port="53"
                  query="34604.loc.hp.com"
                  retries="4"
                  comment="DNS Service Monitor Request"
                  disable="0"
       >
       <PRIORITY priority="1" location="Local System"
          network="Default"> </PRIORITY>
       </TARGET>
      <OBJECTIVE  objectiveid="3"
```

```
                    metric="AVAILABILITY"
                    condition="&gt;"
                    servicelevel="90.000"
                    warning="90.000"
                    baseline="0.000"
                    duration="600"
                    starttime="00:00"
                    stoptime="00:00"
                    days="MTWTFSS"
                    message="DNS for &lt;TARGET&gt; unavail"
      > </OBJECTIVE>
      <LOCATION   id="Local System"
                    interval="300"
                    timeout="20"
                    network="Default"
      > </LOCATION>
    </SERVICE>
  </CUSTOMER>
  <CUSTOMER name="Hewlett-Packard">
    <SERVICE id="HP Shopping Site" probe="HTTP">
      <TARGET     host="Sys5.loc.hp.com"
                    port="80"
                    urlfile="/"
                    password="##"
                    embedded="1"
                    proxypassword="##"
                    disable="0"
       >
       <PRIORITY priority="1" location="Local System"
           network="Default"> </PRIORITY>
       </TARGET>
      <TARGET     host="Sys66.loc.hp.com"
                    port="80"
                    urlfile="/hpov_reports/iops.htm"
                    password="##"
                    embedded="1"
                    proxypassword="##"
                    disable="0"
       >
       <PRIORITY priority="1" location="Local System"
          network="Default"> </PRIORITY>
       </TARGET>
      <OBJECTIVE  objectiveid="5"
                    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 for &lt;TARGET&gt; unavail"
     > </OBJECTIVE>
     <OBJECTIVE  objectiveid="2"
                    metric="RESPONSE_TIME"
                    condition="&lt;"
                    servicelevel="3.000"
                    warning="-91230000000000000000.000"
                    baseline="0.000"
                    duration="600"
                    starttime="00:00"
                    stoptime="00:00"
                    days="MTWTFSS"
                   message="HTTP RESPONSE_TIME slow
                      (&lt;VALUE&gt; vs &lt;THRESHOLD&gt;)
                        on &lt;TARGET&gt;"
     > </OBJECTIVE>
     <LOCATION   id="Local System"
                    interval="300"
                    timeout="45"
                    network="Default"
     > </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 conformance."
                    threshold="80.000"
> </CONFORMANCE_LEVEL>
<CONFORMANCE_LEVEL name="Gold"
                   description="Second highest conformance"
                    threshold="95.000"
> </CONFORMANCE_LEVEL>
<CONFORMANCE_LEVEL name="Platinum"
                    description="Highest 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;0,1,101
1118215,1,0,0;0,1011118215,0,0,0,0,0,0,0;0,0,0,0,0"
           applied="FALSE"
  > </DOWNTIME>
  <NETWORK name="Default" customer="" service=""
           type="LAN"
           executable=""
           phoneNumber=""
           user=""
           password=""
           DUNEntry=""
           timeout="300"
           concurrency="32"
           upload="0"
  > </NETWORK>
  <NETWORK name="ODBC" customer="" service=""
           type="Default"
           executable=""
           phoneNumber=""
           user=""
           password="##"
           DUNEntry=""
           timeout="30"
           concurrency="1"
           upload="0"
  > </NETWORK>
</CUSTOMERLIST>
```

4

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 165 for a complete list of the metrics collected for each probe type and a definition of each metric.

Internet Services Probes on Windows and UNIX Systems: Internet Services allows you to configure and monitor all service types listed below on Windows systems. On UNIX systems you can use all probes except for the HTTP_TRANS probe in Internet Explorer heavyweight mode, the Streaming Media probe and the ODBC probe.

- DHCP (Dynamic Host Configuration Protocol)
- DIAL (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 Recorder)
- ICMP (Internet Control Message Protocol—Ping)

- IMAP4 (Internet Message Access Protocol)
- LDAP (Lightweight Directory Access Protocol)
- MAILROUNDTRIP (Mail Round Trip)
- NNTP (Network News Transfer Protocol)
- NTP (Network Time Protocol)
- ODBC (Open Database Connectivity)
- POP3 (Post Office Protocol 3)
- RADIUS (Remote Authentication Dial In User Service)
- SAP
- SMS (Short Message Service)
- SMTP (Simple Mail Transfer Protocol)
- STREAM_MEDIA (Streaming Media)
- TCP (Transmission Control Protocol)
- WAP (Wireless Application Protocol)
- X_SLAM (CiscoWorks Integration)
- Your Own Custom Probes

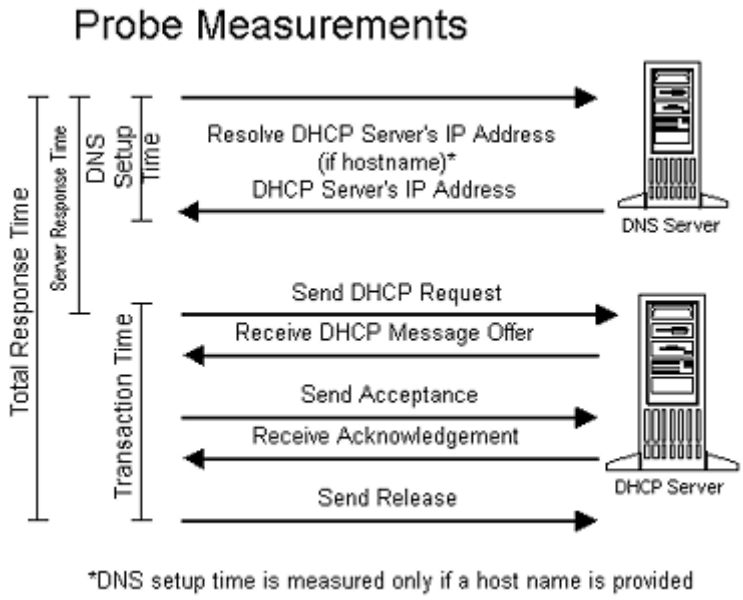
DHCP (Dynamic Host Configuration Protocol)

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.

If the probe has broadcast a request on the subnet, it accepts an offer from a DHCP server on a first come first serve basis. If the probe has sent the request to a specific host (when supplied), the probe only accepts an offer if it is made by that specific host.

After accepting the 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:



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 request is accepted by the DHCP 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 (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 dialog in the Configuration Manager and select the Dial-Up Network Connection. If a Dial-Up connection doesn't already exist, you can create one by selecting the New Connection button in the Probe Location dialog. 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 Dial-Up 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.

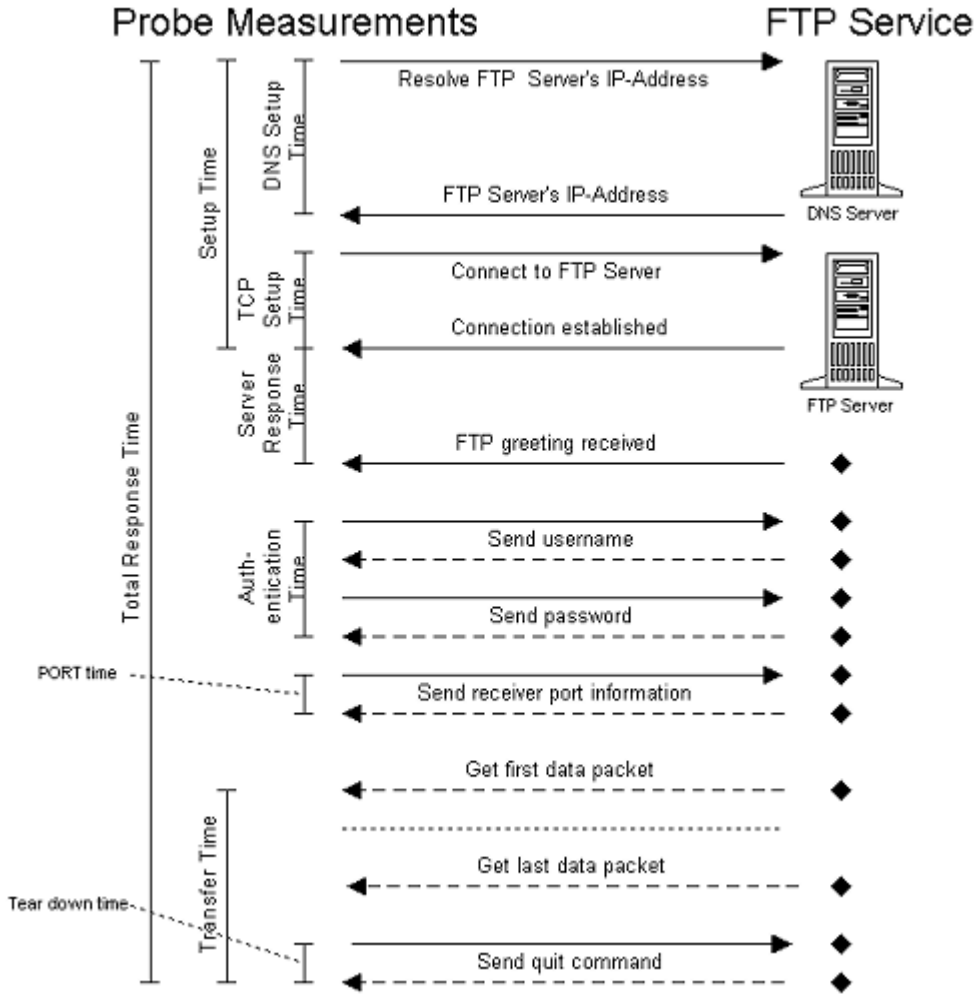
The DNS host system must be configured to resolve its own name and IP address in order for the DNS service target probe to work correctly.

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.

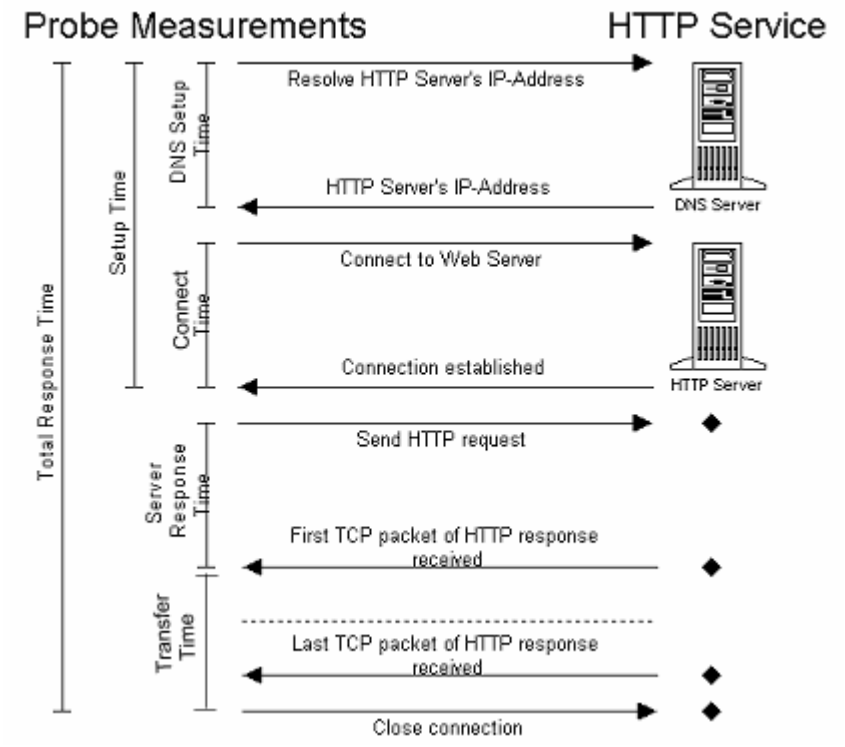
If no remote file is specified, the probe retrieves a directory listing using the ftp dir command.

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. 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.

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 which means the pattern must NOT occur. If the error text pattern match occurs then the target is marked unavailable.

Note that certain HTML characters are encoded (for example & is & and " is "). When setting up a pattern, look at the HTML source to see whether the string that is displayed in the browser contains any encoded characters. If encoded characters are part of the string then adjust the pattern accordingly.

Consider following examples:-

+"login successful" -error	For the target to be available, the word "login successful" must be contained in the HTML output but not 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 to OR in the Configuration Manager 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 HTTPS probe works the same as the HTTP probe (see above).

Parameters

Depending on the installed Windows 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 service target Trusted Root Certificate on the Management Server for the probe to use in validating the target server.

Exporting a Trusted Root Certificate

The service target Trusted Root Certificate must be exported in Base64 encoded X.509 (.CER) format and copied into the **trusted.txt** file located in the `\probes` directory. The `trusted.txt` file is used by the HTTPS probe to validate the target server.

For example, in Internet Explorer 5.5 export a Trusted Root Certificate as follows:

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

If the service target you are probing requires client authentication, you need to setup the client authentication and enter the certificate file and password under Client Authentication in the Web Service Target dialog.

HTTP_TRANS (Web Transaction Recorder)

The HTTP_TRANS probe is used to monitor multi-URL web transactions, such as catalog lookup, login/logout and shopping carts.

When you create an HTTP_TRANS service target, the Web Transaction Recorder is automatically launched. The Web Transaction Recorder allows you specify the user actions that you want to track and record them for the probe to play back on a regular basis, simulating typical end-user activity and collecting important availability and response time data.

Using the Web 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 Transaction 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.

Internet Explorer 5.5 or later (IE 6.0 with service pack 1, or 6.1 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.

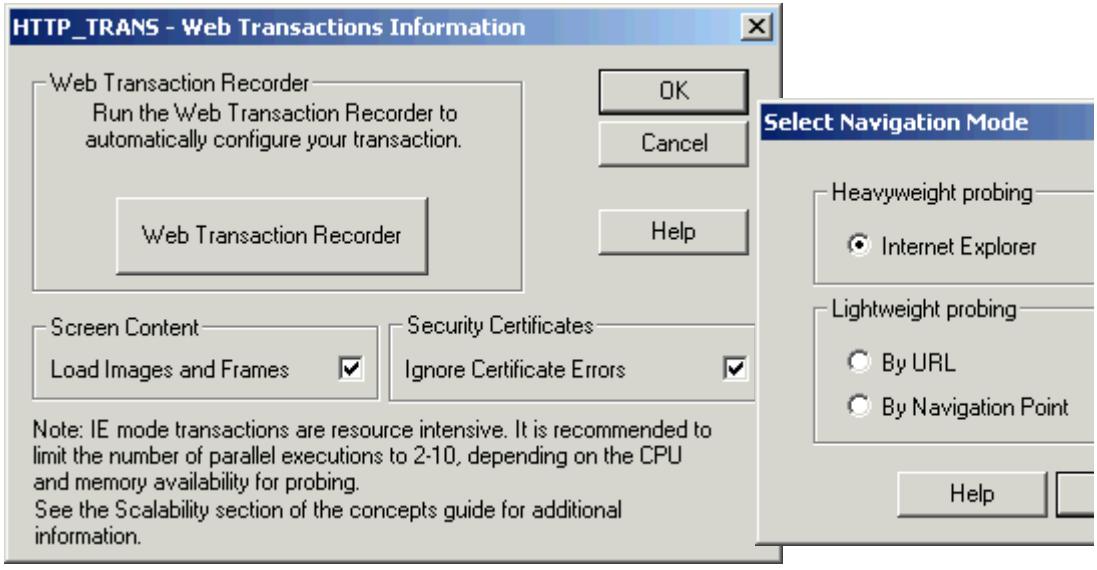
Web Transaction Recording Modes

In the Web Recorder there are three possible recording modes:

- Heavyweight probing - The heavyweight mode 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 or using the Target Priority option in the Probe Location dialog. Each heavyweight probe is then assigned to this network.

- Lightweight probing By URL - The Lightweight By URL mode 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.
- Lightweight probing By Navigation Point - The Lightweight Navigation Point mode should only be used when the other two cannot be used.



The difference is the technology used to do the probing and whether individual transaction steps are specified as a URL or as a navigation point used to determine the next URL to be loaded or the HTML element to be executed.

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

*** Through substitution rules

The Heavyweight mode does not support applications that create new dialogs with window.showModalDialog or window.showModlessDialog. These dialogs are not supported by the Internet Explorer API (see MSDN Q251128).

Quick Tips for Determining Which Mode to Use

Use IE Mode:

- When web pages contain Javascript or Java applets (such as online forms).
- When web transactions are complex.
- When web pages are generated dynamically each time the user visits.
- When input is coming from a program or script.
- When you desire your measurements to closely emulate a customer's browser.
- When unsuccessful using By URL mode.

- Note: The number of parallel IE mode transactions depend heavily on the performance of the probe system since significant resources (memory and CPU) are necessary.
- Note: Concurrency should be set to 1 for the probe.

Use By URL Mode:

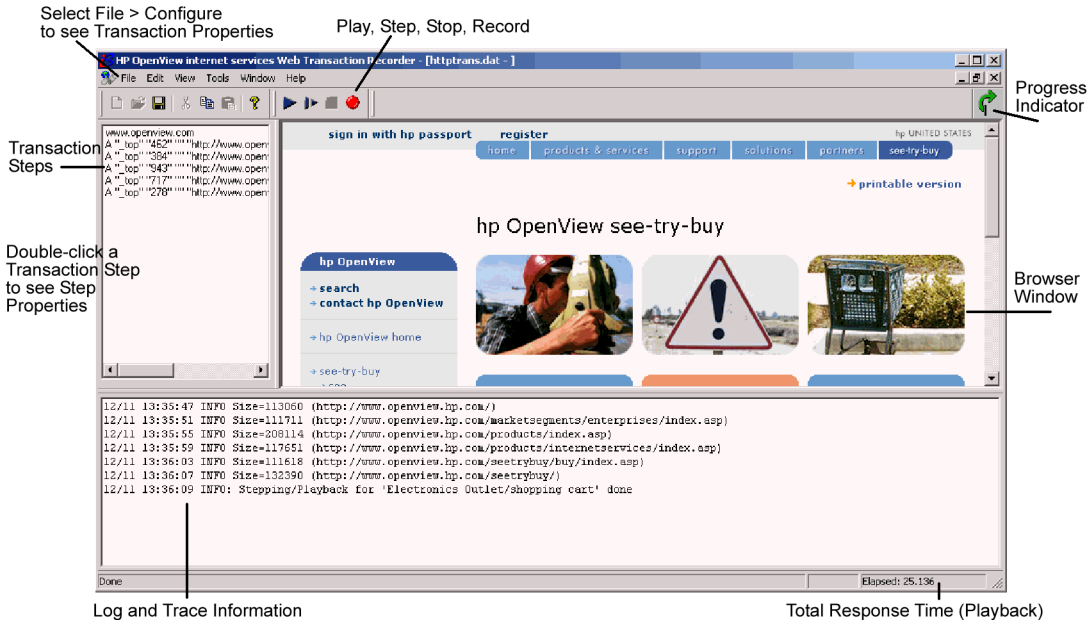
- When the probe runs from a UNIX, Linux or Windows system.
- When you want to simulate lots of transactions in parallel.

Use By Navigation Point:

- When the probe runs on UNIX or Linux and the By URL mode cannot be used (for example if the web pages are generated dynamically).
- Note: Transactions may need to be re-recorded when web pages change.
- Note: Frames are not detected.

Using the Web Transaction Recorder

The Web Transaction Recorder GUI used to record a web transaction is shown below.



The basic steps to recording a transaction are as follows **(please see the online Help for details)**:

1. Determine the web pages (and transaction steps within the pages) you want to record.
2. Use the **Tools > Cache Viewer** to delete cookies before recording your transaction.
3. Press the Record button to start recording the transaction steps.
4. Enter the starting URL (or navigation point).

5 After the web page has been completely loaded in the Browser Window in the right pane, you can navigate through the transaction steps in the web page displayed.

6 The transaction steps are shown in the left pane. Log and trace information for the transaction steps is shown in the lower pane.

7 Press Stop to end the recording.

8 Playback the recording to test whether all the steps you wanted were included. The total response time during playback is shown in the lower right corner.

9 Make any changes using the options in the web recorder. For example:

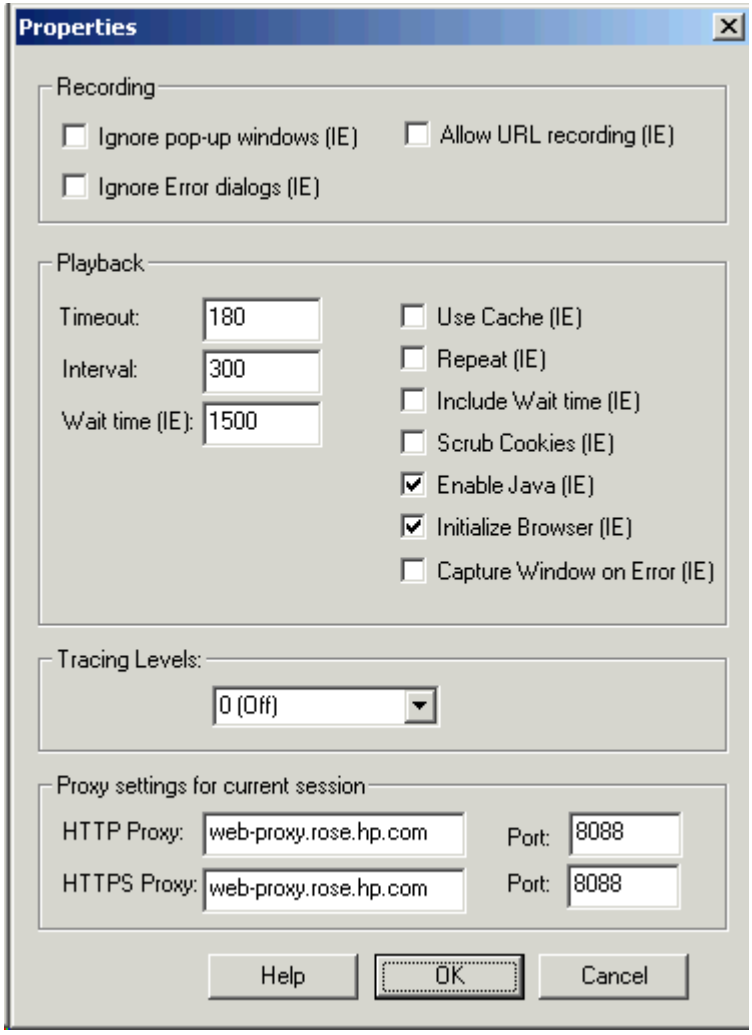
- Modify global transaction properties in the **File > Configure > Properties** dialog.
- Modify transaction step properties in the **Step Properties** dialog accessed by double-clicking on a transaction step in the left pane.
- Enter advanced scripting information in the **Advanced Step Properties** dialog. See the online help topic **Transaction Script Reference** for details.

10 Exit and save the probe changes in the Configuration Manager.

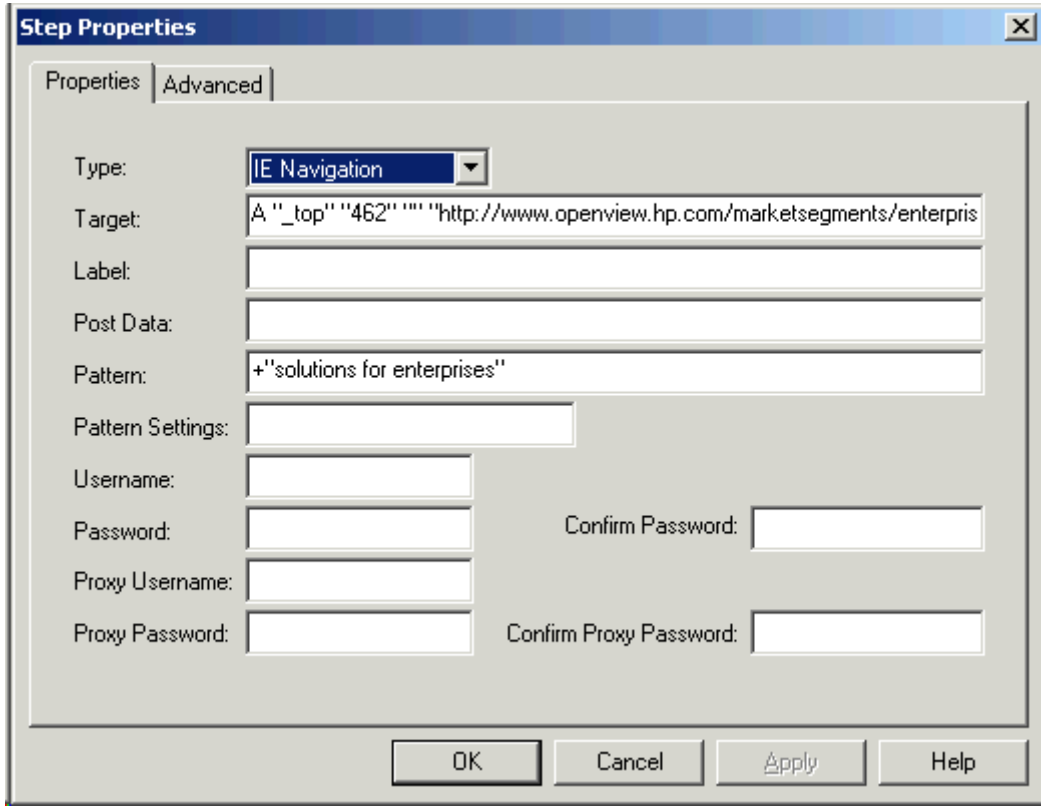
Advanced Usage

Selecting **File > Configure > Properties** dialog allows you to specify global transaction properties:

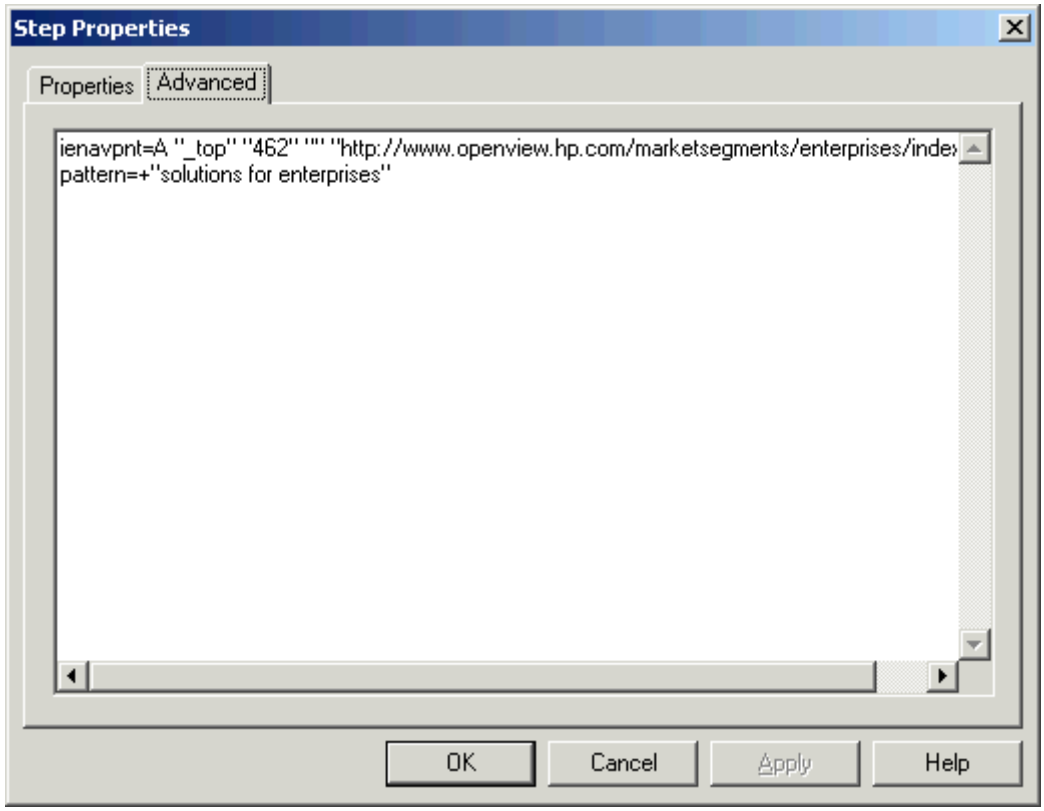
- Recording options
- Playback options
- Tracing levels
- Proxy settings (If you leave this blank the probe will run using the probe location's proxy settings.)


Properties
Recording
Ignore pop-up windows (IE)
Allow URL recording (IE)
Ignore Error dialogs (IE)
Playback
Timeout:
180
Interval:
300
Wait time (IE):
1500
Use Cache (IE)
Repeat (IE)
Include Wait time (IE)
Scrub Cookies (IE)
Enable Java (IE)
Initialize Browser (IE)
Capture Window on Error (IE)
Tracing Levels:
0 (Off)
Proxy settings for current session
HTTP Proxy:
web-proxy.rose.hp.com
Port:
8088
HTTPS Proxy:
web-proxy.rose.hp.com
Port:
8088
Help
OK
Cancel

Double-clicking on a transaction step displays the Step Properties dialog that allows you to view the details for each step and specify additional information needed for the probe to correctly execute the step.



Selecting the Advanced tab in the Step Properties dialog displays a window that allows you to set up advanced scripting options for the transaction step.



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 1.

Please refer to the following Web Recorder online help topics for detailed information on handling complicated or specialized web pages and solving recording problems:

- Advanced Topics
- Transaction Script Reference
- Web Recorder Tips
- Recording and Playback Issues
- Troubleshooting

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)

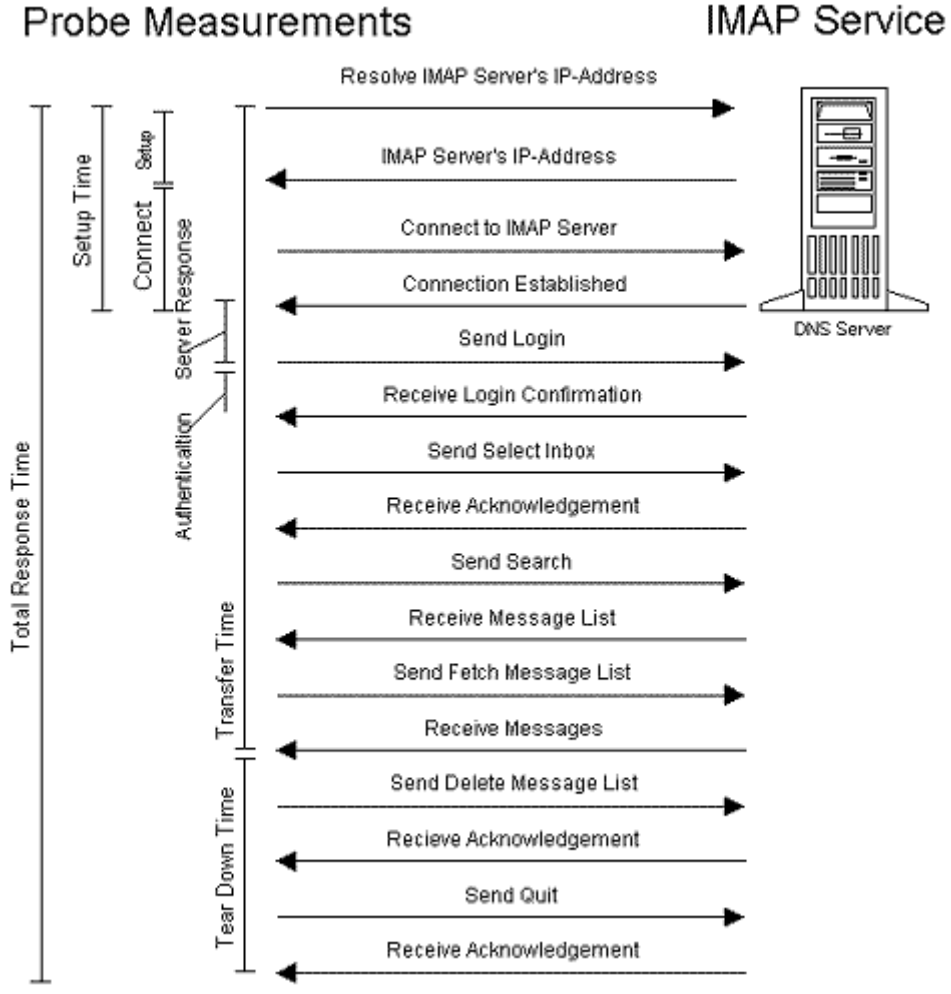
Internet Message Access Protocol (IMAP4) provides a method of accessing electronic mail or bulletin board messages that are kept on a (possibly shared) mail server. It permits a *client* email program to access remote message stores as if they were local. The IMAP probe measures the steps that occur in the client making its connection to the server and accessing messages.

It is highly recommended that you set up a mailbox specifically for the SMTP and IMAP4 probe.

The probe retrieves all mail in the mailbox and searches for all messages with the X-OVIS-Timestamp. This field is set by the SMTP probe. If this field is detected, the probe and marks the message for deletion. After all messages are read, the probe deletes the messages with the X-OVIS-Timestamp. This cleanup prevents filling up the mailbox with SMTP probe messages.

Note there are special considerations for using the IMAP probe to monitor the IMAP4 service as provided by Microsoft Exchange 2000 server. Please refer to the online help on the IMAP4 service target for more information.

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

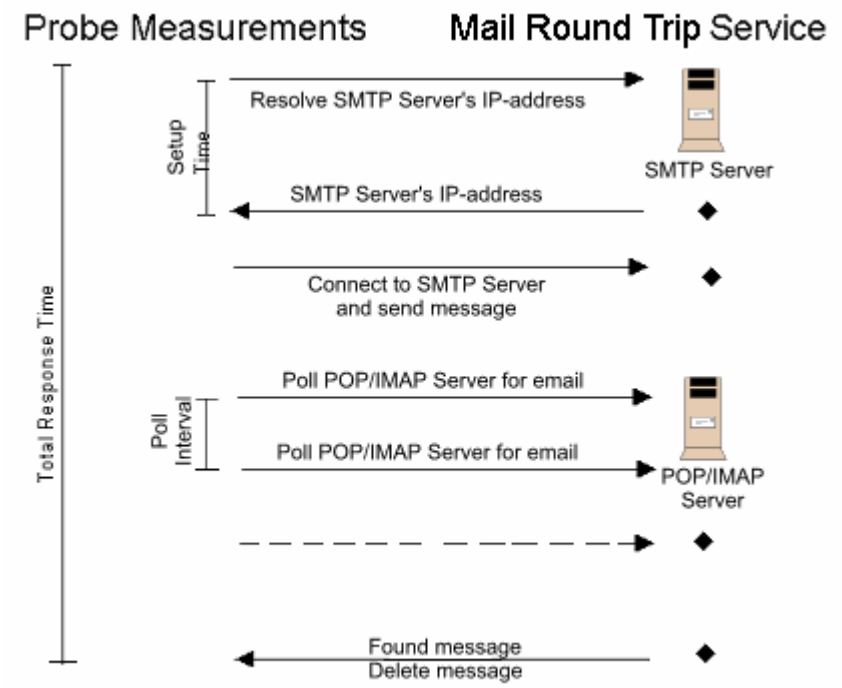
MAILROUNDTRIP (Mail Round Trip)

The Mail Round Trip mail service is monitored via the Internet Services Mail Round Trip (MAILRTRIP) probe. This probe connects to an email server (SMTP/ESMTP/SMTP-A), posts an e-mail message to the specified e-mail server, then polls on the (POP/IMAP) receiving server and measures how long it takes for the mail to complete the round trip journey. It sets message information such as the recipient and sender and posts a message body of the specified size. The probe also determines if the service is available and collects other information about this service as it executes. If no error is returned the message was successfully sent and received back.

Note there are special considerations for using the Mail Round Trip probe to monitor the mail service as provided by Microsoft Exchange 2000 server. Please refer to the online help on the Mail Round Trip service target for more information.

Parameters

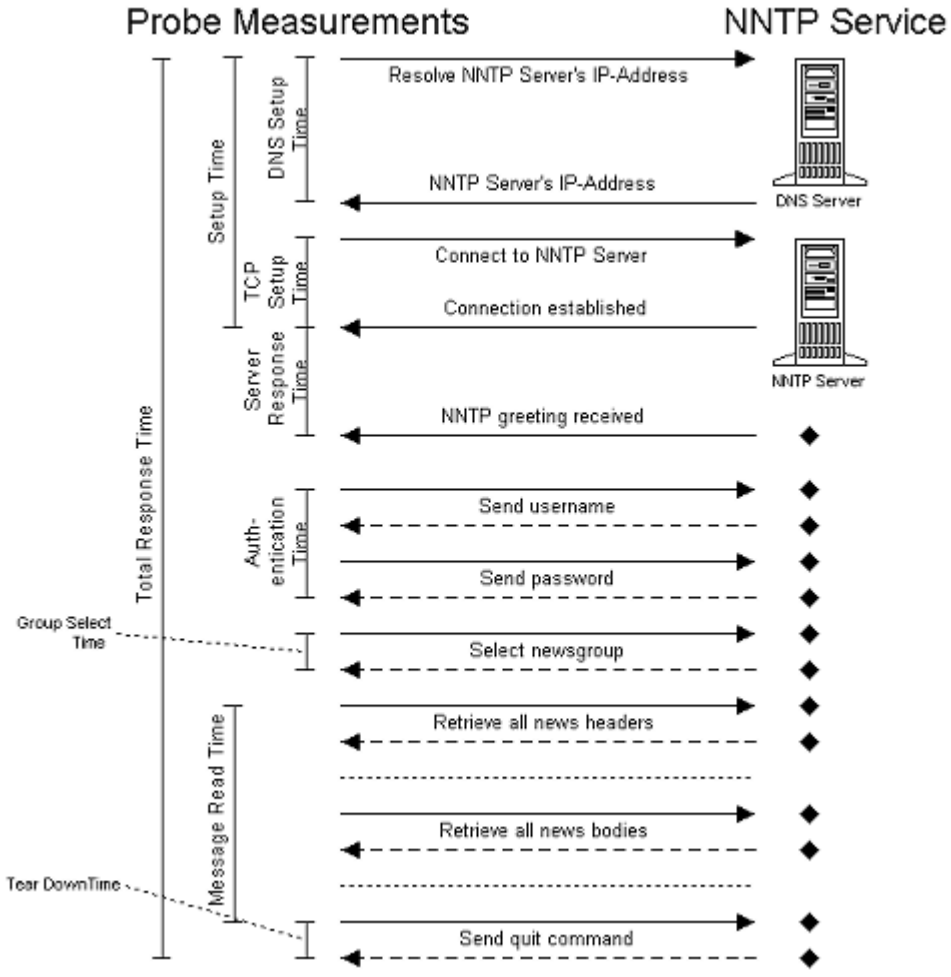
You must enter configuration information for both the email server that will send the message and the one that will receive the message. Then define the sender information to be used for sending the email and the protocol and email account information to be used for receiving the email. You can also specify message size and the interval at which to check for message receipt.



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:

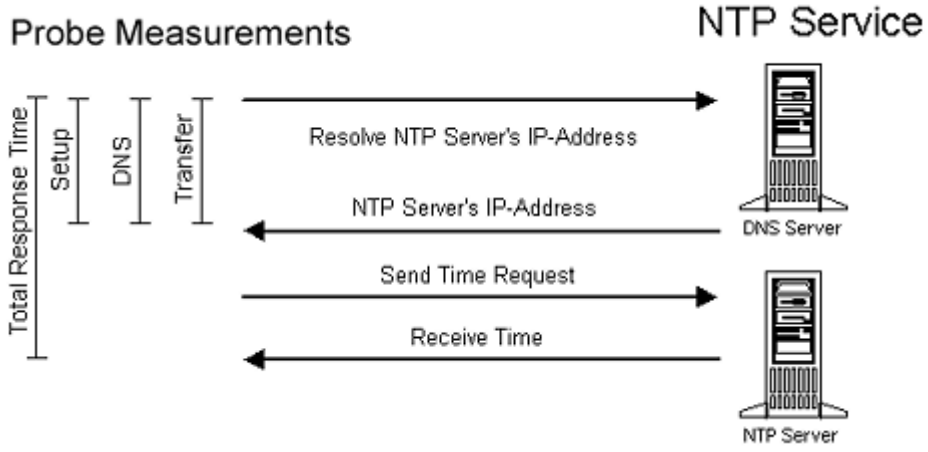


Parameters

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. The 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:



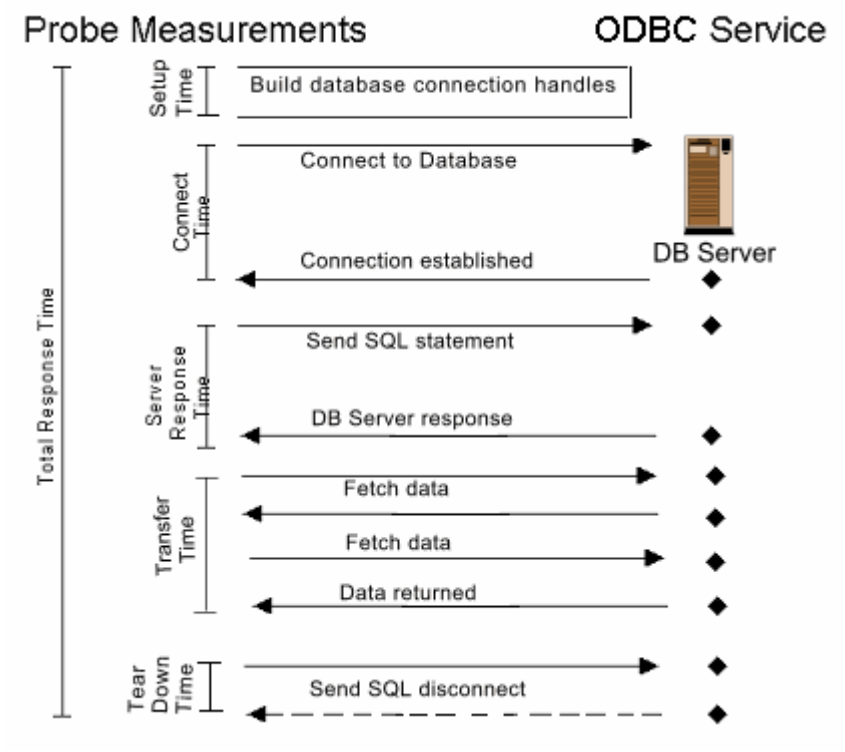
ODBC (Open Database Connectivity)

The ODBC (Open Database Connectivity) service is monitored via the ODBC Probe. The ODBC probe is a generic database probe that monitors the availability of a database with a user defined SQL select statement. **The probe runs on Windows systems only.**

The ODBC probe connects to a database via the configured System Data Source Name (DSN) set up in the ODBC Data Source Administrator on the local or remote system.

Note: if using NT Authentication for SQL Server, leave the user and password blank and set the HP Internet Service service to logon with the account that is setup to access the SQL Server database. This may also include setting up trust relationships for the account across domains. Furthermore, only one account may be used for all database probes if NT Authentication is used.

When setting up the probe location for the ODBC probe, create an ODBC network connection and **set the number of concurrent requests to 1**. This will prevent overloading of the ODBC Manager when launching multiple database probes.



POP3 (Post Office Protocol 3)

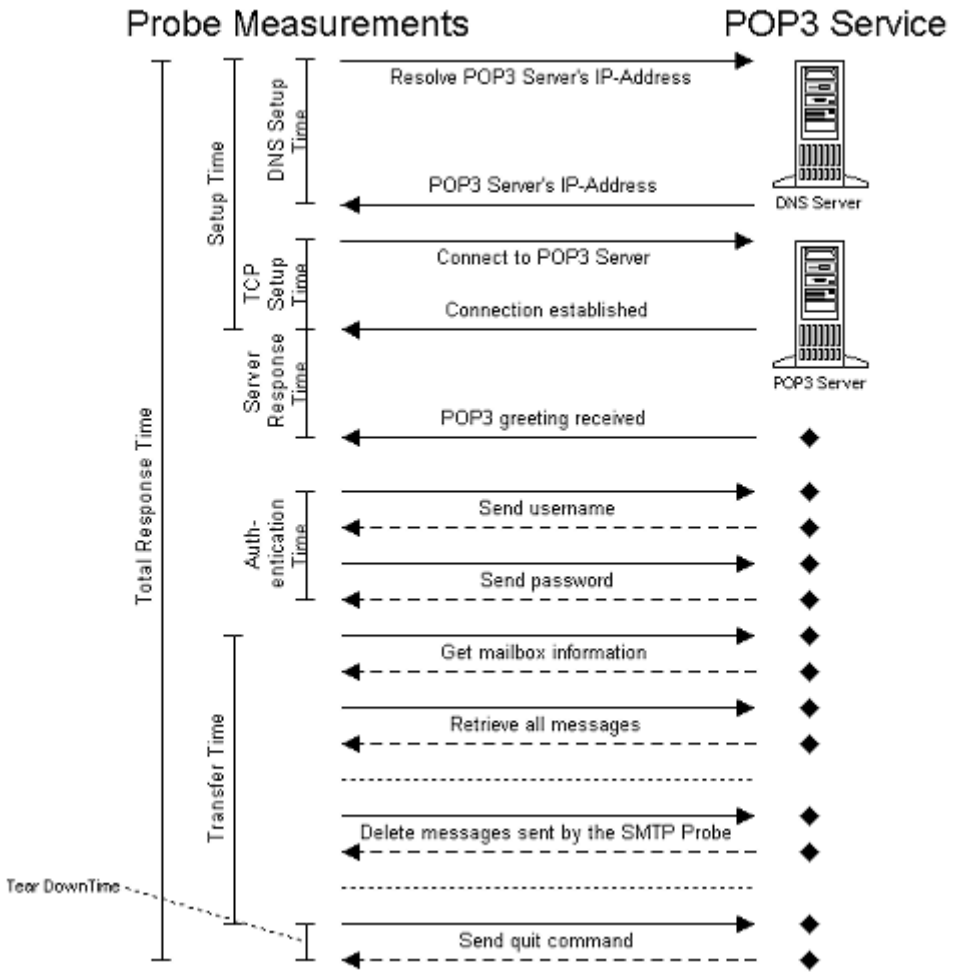
The POP3 probe emulates a user downloading email. After connecting to the POP3 server, the mailbox is authenticated by the specified username and password. On UNIX servers, this is typically the username and password of a local user. On Windows (for example, the Exchange Server), the username must include 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

Note there are special considerations for using the POP3 probe to monitor the mail service as provided by Microsoft Exchange 2000 server. Please refer to the online help on the POP3 service target for more information..

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:



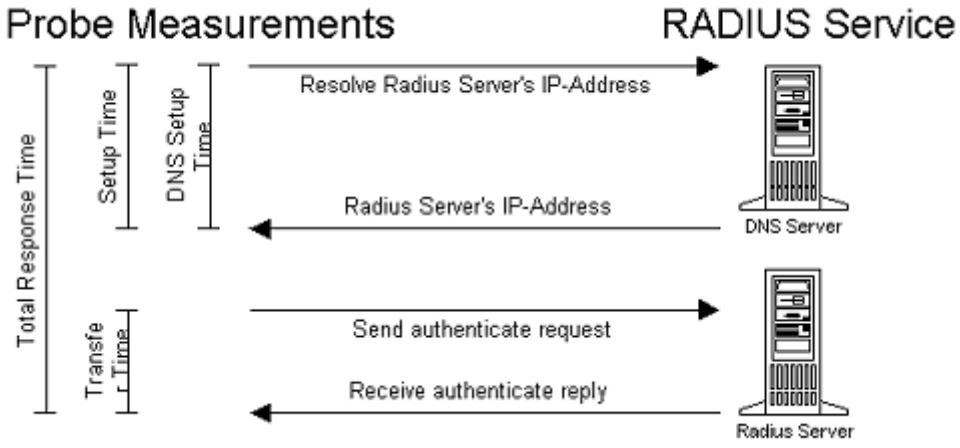
Parameters

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.

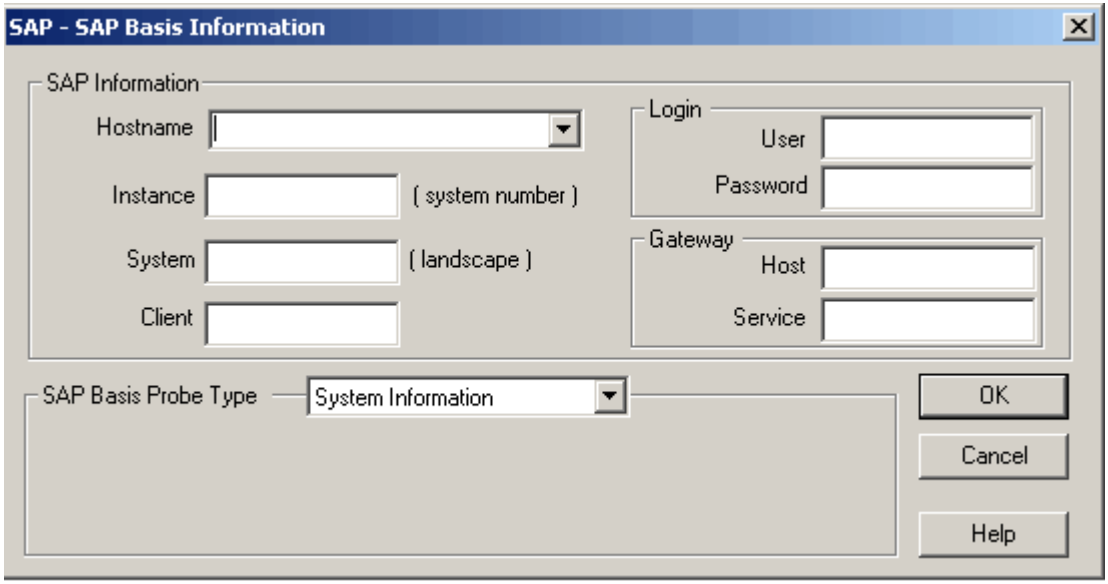
SAP

The SAP Basis (SAP_BASIS) Probe is used to monitor the availability of an SAP Application Server. The probe can access SAP servers running on Windows and UNIX platforms.

The probe can be configured to make two different types of SAP requests (SAP Basis Probe Type):

- **System Information** – When you select this type, the SAP ABAP/4 function RFC_SYSTEM_INFO (which is a simple command request) is made by the SAP probe. The RFC_SYSTEM_INFO command is used as a means of determining that the interface is working and if the SAP application server is available. The SAP ABAP/4 function RFC_SYSTEM_INFO should be contained on all SAP systems.
- **Transaction** – When you select this type, the probe is configured to accept a user specified SAP transaction code. The probe forwards this request (RFC_CALL_TRANSACTION_USING) to the server. The probe monitors the SAP transaction called.

The SAP Service Target dialog is shown below:



You need to set up or use an existing SAP user with specific attributes. See the instructions below for an example of setting up an SAP user. The S_A.ADMIN Authorization gives you the permissions you need for the System Information type SAP probe. Additional authorization to make RFC function calls is required for the Transaction type SAP probe.

Also note that for the Transaction SAP probe an RFC destination has to be defined in SAP transaction **sm59**. In this transaction, specify the SAP probe hosts that are allowed to do a RFC connection.

Set up an SAP User

1. Log on to SAP R/3.
2. Call the following transaction: **/nsu01**

3 Create a new user named ITOUSER with the following parameters. Note this example of ITOUSER is the same as for the OVO SAP SPI. If you have already configured this user you may use it. Or you may use a different user name as long as it as the following attributes:

User Type: CPIC/System. This user type, as opposed to Dialog, ensures the password will not expire.

I**nitial Password:** any SAP-admissable value *except* HPSAP_30 or whatever you will use as the password for the user. Note the password HPSAP_30 is the same as for the OVO SAP SPI. You may use a different password.

Authorization:

S_A.ADMIN (for SAP versions 3.1x, 4.x)

User Roles:

SAP_ALL_DISPLAY (SAP version 4.6C only)

Display authorization for all modules except BC, CA and HR

SAP_BC_BASIS_ADMIN (from SAP 6.10/6.20)

4 If you are using SAP version 6.10/6.20 (Web Application Server), then you need to perform the following additional actions:

a Call the following transaction: **/nsu02**.

b Generate a new profile with, for example, the name: ZSPIRFC is used with the OVO SAP SPI, and assign the following objects and authorizations to the newly create profile. This profile is needed because the OVIS SAP probe requires the authorization you define here to call SAP RFC functions during probe executions.

Object	Authorization Profile
S_RFC	S_RFC_ALL
S_RFC_TAB	&_SAP_ALL
S_C_FUNCT	&_SAP_ALL
S_DATASET	&_SAP_ALL

c Activate the profile and assign it to the SAP probe user which you already created.

5 Log on to SAP as user

6 SAP prompts you to change the password. Enter the following new password: HPSAP_30 or whatever you decide to use.

Parameters

In configuring the probe you need to enter an SAP instance (also referred to as system number). An instance is an administrative entity that combines components of SAP systems that offer one or more service. Within an instance, the services provided are started and stopped together. The default is 00.

In configuring an SAP probe, you enter the unique three-character name for the system within the system landscape. For example, DEV, QAS and PRD stand for Development, Quality Assurance and Production.

You also enter the client number. A client is an independent unit in a system. Each client has its own data environment and therefore its own master data and transaction data, assigned user master records and charts of accounts, and specific customizing parameters.

If you select the Transaction probe type described above, then you also specify an SAP transaction. A transaction code is assigned to each function in SAP R/3 systems. For example, to display the customer master data, the transaction code FD03 is used. Some example transactions for some modules:

SD (Sales and Distribution) - VA01, VA02, VA21

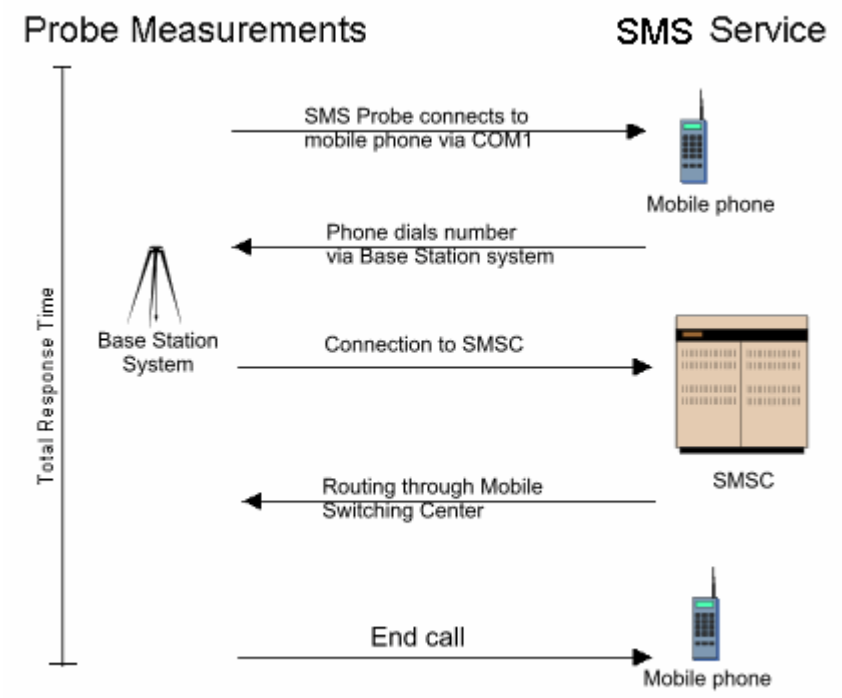
MM (Material Management) - MB51, MB59

SMS (Short Message Service)

The SMS (short message service) probe tests the time for a short text message to travel through the entire wireless infrastructure: from wireless phone, to tower, to SMSC, to the target tower, to target wireless phone. It uses the same phone for both sending and receiving messages.

The phone connects to the PC's COM port using a data cable. The probe can change the target SMSC of the sending phone on the fly, thus multiple SMSCs can be probed by the same wireless phone.

The probe can be configured to work with different mobile equipment vendors. You edit a configuration text file (`SMS2SMSConfig.txt` in the `\probes` directory) to set up the configuration for a specific vendor's phone.



Configuring the Probe to Work with Different Phones

The SMS probe can work with different vendor's phones. By changing the details in the SMS configuration text file (the `SMS2SMSConfig.txt` file is located in the `\probes` directory) you can easily set up probes using different phones and switch between vendors.

After you edit this text file it needs to be copied to the remote probe system. You can create different configurations for different remote systems and phones.

Here is an example and description of the different sections in the `SMS2SMSConfig.txt` file:

```
#Configuration file for sending SMS from SMS
[SendModem]
port = Com1
mode=pdu

#For Nokia phones
DevControlStr = 115200,n,8,1   #no spaces between control string fields
PduSendFormat = 001100%02X81%s0000A7%02X   #This is for Cingular,
Nokia phone
SetSmscFormat = "%s",145

#For Ericsson phones
#DevControlStr = 115200,n,8,1   #no spaces between control string fields
#PduSendFormat = 01801100%02X81%s0000A7%02X   #This is for Cingular,
Ericsson phone
#SetSmscFormat = "%s",145

#For Motorola phones
#baud = 57600, parity=N, data=8, stop=1
#DevControlStr = 57600,n,8,1    #no spaces between control string fields
#PduSendFormat = 0001FF%02X81%s0000%02X    #This is for Vodafone,
Motorola phone
#SetSMSCFormat = "%s"145

[ReceiveModem}
port = Com1
mode=pdu
#baud=57600, parity=N, data=8, stop=1
DevControlStr = 115200,n,8,1         #no spaces between control string fields
TargetMessageStore = "SM"
SetSmscFormat = "%s",145

#For Motorola phones
#baud = 57600, parity=N, data=8, stop=1
#DevControlStr = 57600,n,8,1    #no spaces between control string fields
#PduSendFormat = 0001FF%02X81%s0000%02X    #This is for Vodafone,
Motorola phone
#SetSMSCFormat = "%s"145
```

The file is divided into two sections: [SendModem] and [ReceiveModem]. Each contains name-value pairs describing various configuration attributes. The SendModem section contains configuration details for the phone sending the SMS message. The ReceiveModem section contains configuration details for the phone receiving the SMS message.

It is possible to support multiple device entries in the configuration file for this probe. Simply add the device entry name to the SendModem and ReceiveModem section name (for example, [SendModem:Nokia1] [ReceiveModem:Nokia1]). Then enter this as the **Device Name** in the Configuration Manager SMS Service Target dialog to specify which ports to send and receive on. If no Device Entry is specified in the SMS Service Target dialog, the probe will use the [SendModem], [ReceiveModem] entry.

Port. In both the sections, port describes the port on the PC to which the phone is connected. Valid values are COM1, COM2 etc.

DevControlStr. In both sections this represents the device control string for the phone. It is usually in the format: Baud-Rate,parity,number-of-data-bits,number-of-stop-bits. Commas separate these fields and no spaces are allowed.

PduSendFormat. In both sections this represents the format of the protocol data unit to be send in the SMS. It consists of two kinds of data: some fixed strings and some variable data. The fixed strings are mobile equipment specific. The variable data format is also mobile equipment specific, but the data itself is standard – the length of the called number, the called number itself, the length of the SMS message. The called number is input to the probe. The message is constructed within the probe software.

SetSMSCFormat. In both sections this represents the format of the SMSC number for the SMS message. It consists of the SMSC number, which is input to the probe, with a fixed string appended to the end. Depending on the wireless provider this string may be 145 or 129.

TargetMessageStore. In both sections this represents the SMS memory from which messages are read and deleted. Valid values are ME and SM.

SMTP (Simple Mail Transfer Protocol)

The SMTP/ESMTP/SMTP-A mail service is monitored via the SMTP probe. This probe creates a TCP connection to the SMTP port at the specified address, posts an e-mail message to the SMTP server and measures how long it takes. It sets message information such as the recipient and sender, and posts a message body of the specified size

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.

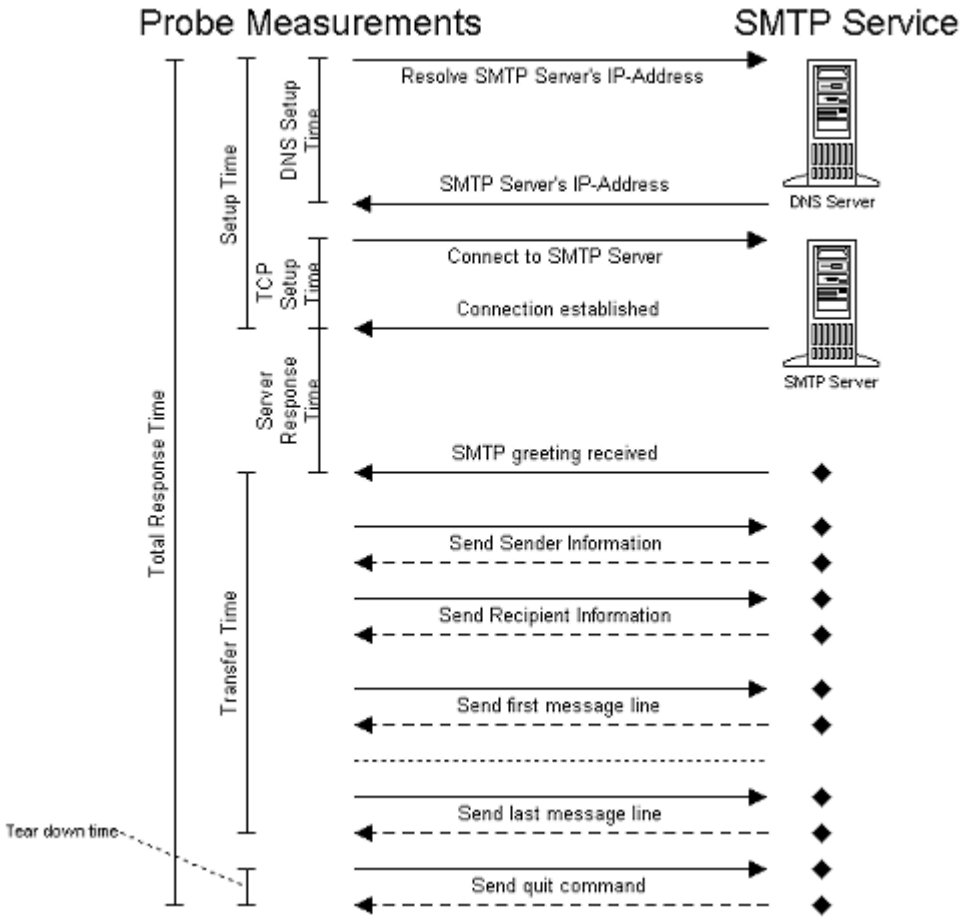
Make sure to use the POP3 or IMAP probe in conjunction with the SMTP probe. The POP3 or IMAP probes can delete the messages that are sent by the SMTP probe. Otherwise the recipient's mailbox will be flooded with messages.

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.

If you are probing an ESMTP/SMTP-A server, check Enable ESMTP Mode and enter the required username and password information to authenticate the mail send request.

The following diagram shows the protocol steps and measurements involved in posting the message:



STREAM_MEDIA (Streaming Media)

The Streaming Media probe streams file formats supported by Real Media Player (version Real8 Basic or RealOne) and Windows Media Player and monitors the performance.

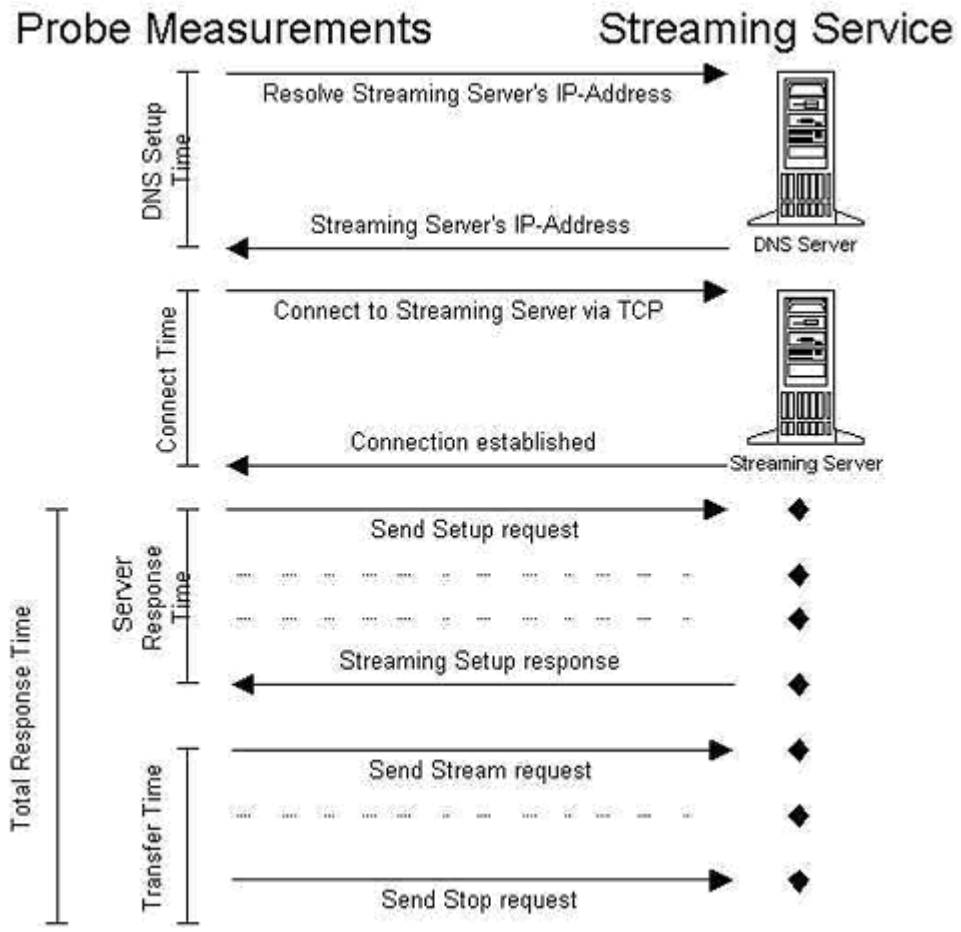
The Windows Media Player is installed automatically with the probe. If you want to use Real Player for Windows you will need to install it on whatever system you plan to run the probe. See the web site www.real.com. **The probe works on Windows platforms only.**

If the remote probe is behind a proxy and access to the server is through the proxy, then you may need to enable the proxy settings in the Player. You would also need to set up the proxy information in the Probe Location dialog in the Configuration Manager.

Parameters

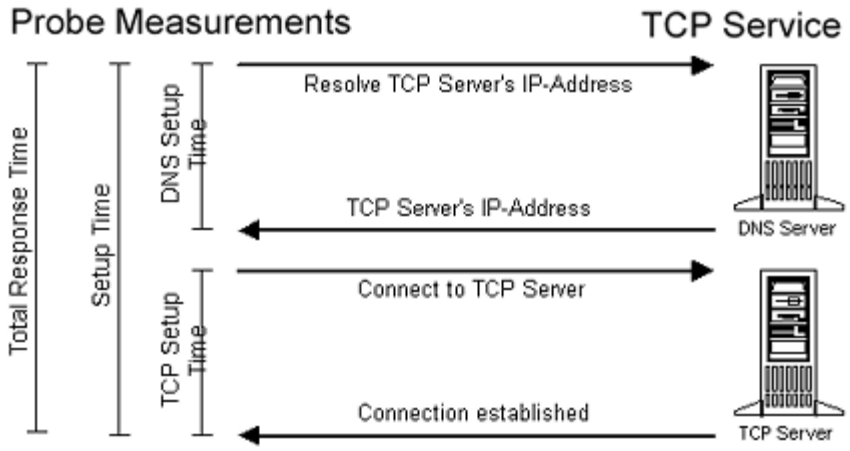
It is recommended that at least 60 seconds of sampling be performed for a streaming media target. See the online help for details on specifying **Play Time**.

The following diagram shows the protocol steps.



TCP (Transmission Control Protocol)

The TCP probe (ANYTCP) 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)

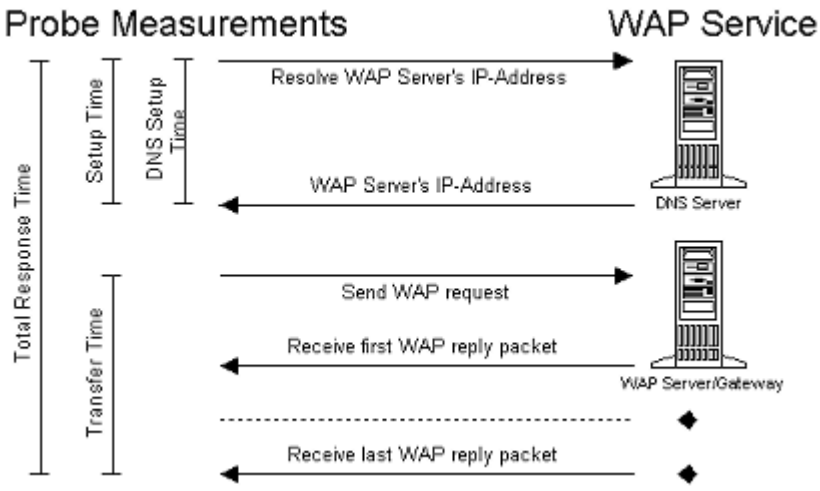
The WAP (Wireless Application Protocol) probe measures the total response time of an emulated WAP request. After the hostname or IP address is resolved, a WAP request for a document is sent to the WAP Server or WAP Gateway. Once the WAP server receives the request, it locates the requested document and 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).

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.

The following diagram shows the protocol steps:



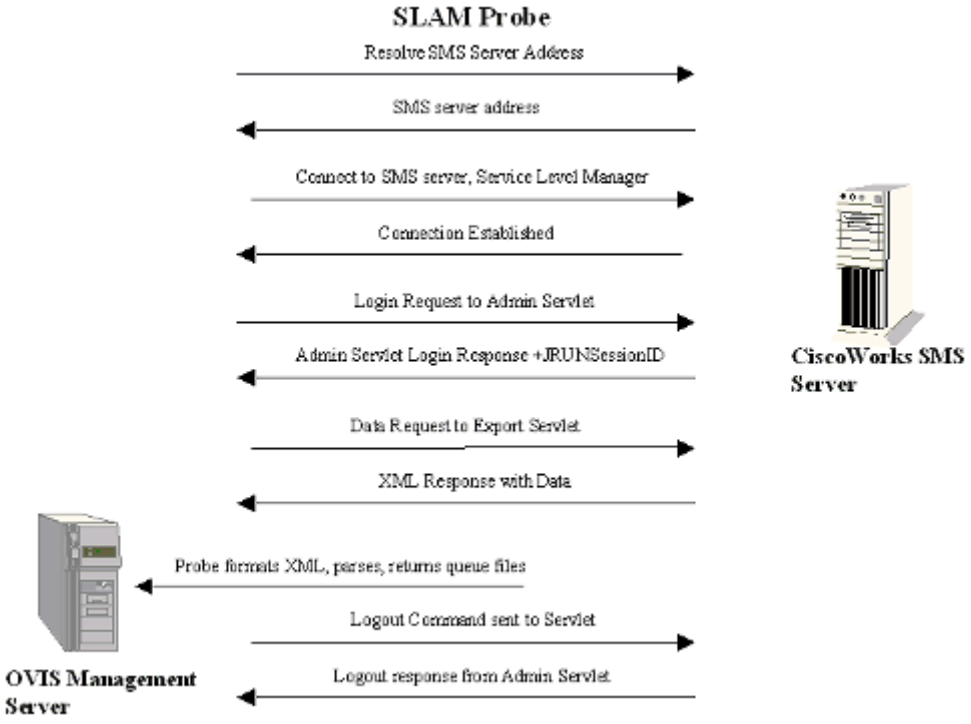
X_SLAM (CiscoWorks Integration)

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.

Note: The Cisco X_SLAM probes can only be run on the Management Server as a local probe, they are not part of the remote probes package.

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.



Your Own Custom Probes

You can use the Custom Probes feature and SDK in Internet Services to develop your own probes to probe services unique to your environment.

The Custom Probes feature is only supported with the English language version of Internet Services at this time.

The Custom Probe feature comes as 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. 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.

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

List of Metrics by Probe Type

You can look at the file `<install directory>\newconfig\packages\reload_IOPS.SRP` for a list of metrics by probe type.

DHCP

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

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

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

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

OFFER_TIME - Metric 1 - Time to first offer from server.

LEASE_TIME - Metric 2 - Time to lease offered IP address.

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

TRANS_BYTES - Metric 6 - The number of bytes transferred.

DIAL

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

RESPONSE_TIME - Time taken to establish PPP connection.

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

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

TOTAL_CONNECTION_TIME - Metric 3 - Total time connected.

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

DNS

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

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

ANSWER_DNS - Metric 1 - 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 set, 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).

SETUP_TIME - Time to resolve address and establish the connection.

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

DNS_SETUP_TIME - Metric 1 - Time to resolve hostname through DNS.

CONNECT_TIME - Metric 2 - Time to perform connect to FTP server.

SERVER_RESP_TIME - Metric 3 - Time it takes to receive the FTP start header (220).

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

PORT_TIME - Metric 5 - Time to send the client connection ports to the FTP server

TRANSFER_TIME - Metric 6 - Overall time to receive data on the data connection.

DATA_TRANS_BYTES - Metric 7 - The number of bytes transferred.

HTTP

AVAILABILITY - If a measurement could not be retrieved a 0 is set, 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).

SETUP_TIME - Time to resolve address and establish the connection.

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

DNS_SETUP_TIME - *Metric 1* - Time to resolve hostname through DNS

CONNECT_TIME - *Metric 2* - Time to perform connect to resolved IP address

SERVER_RESP_TIME - *Metric 3* - Time it takes to send HTTP Get request and receive first response packet.

TRANSFER_TIME - *Metric 4* - Time it took to send request and receive all reply packets.

TRANS_BYTES - *Metric 5* - The number of bytes transferred.

REQUESTS - *Metric 7* - Number of HTTP requests. For example, if the page was redirected or embedded objects are downloaded.

HTTP_TRANS

AVAILABILITY - If a measurement could not be retrieved a 0 is set, 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).

SETUP_TIME - Time to resolve address and establish the connection.

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

DNS_SETUP_TIME - *Metric 1* - Time to resolve hostname through DNS

CONNECT_TIME - *Metric 2* - Time to perform connect to resolved IP address

SERVER_RESP_TIME - *Metric 3* - Time it takes to send HTTP Get request and receive first response packet.

TRANSFER_TIME - *Metric 4* - Time it took to send request and receive all reply packets.

TRANSFER_BYTES - *Metric 5* - The number of bytes transferred.

REQUESTS - *Metric 7* - Number of HTTP requests. For example, if the page was redirected or embedded objects are downloaded.

HTTPS

AVAILABILITY - If a measurement could not be retrieved a 0 is set, 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).

SETUP_TIME - Time to resolve address and establish the connection.

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

DNS_SETUP_TIME - Metric 1 - Time to resolve hostname through DNS

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

SERVER_RESP_TIME - Metric 3 - Time it takes to send HTTPS Get request and receive first response packet.

TRANSFER_TIME - Metric 4 - Time it took to send request and receive all reply packets.

TRANSFER_BYTES - Metric 5 - The number of bytes transferred.

REQUESTS - Metric 7 - Number of HTTP requests. For example, if the page was redirected or embedded objects are downloaded.

ICMP

*AVAILABILITY - I*f a measurement could not be retrieved a 0 is set, otherwise availability is set to 1.

RESPONSE_TIME - Response time is the average roundtrip time for all ICMP packets.

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

MIN_RESPONSE - Metric 1 - Minimum roundtrip time of all ICMP packets.

MAX_RESPONSE - Metric 2 - Maximum roundtrip time of all ICMP packets.

PACKET_LOSS - Metric 3 - Number of packets lost.

IMAP4

*AVAILABILITY - I*f a measurement could not be retrieved a 0 is set, 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_TPUT - Transfer bytes/Transfer Time in kbytes/sec.

DNS_SETUP_TIME - Metric 1 - Time to resolve hostname through DNS.

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

SERVER_RESP_TIME - Metric 3 - Time for IMAP server to respond.

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

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

DATA_TRANS_BYTES - Metric 6 - The number of bytes transferred.

LDAP

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

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

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

DNS_SETUP_TIME - Metric 1 - Time to resolve hostname through DNS.

NUM_ENTRIES - Metric 2 - Number of returned entries.

CONNECT_TIME - Metric 3 - Time to perform connect to resolved IP address.

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

TRANS_BYTES - Metric 5 - The number of bytes transferred.

MAILROUNDTRIP

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

SETUP_TIME - Time to resolve address and establish the connection.

RESPONSE_TIME -Total response time for the SMTP mail send + the POP/IMAP receive.

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

NNTP

AVAILABILITY - If a measurement could not be retrieved a 0 is set, 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).

SETUP_TIME - Time to resolve address and establish the connection.

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

DNS_SETUP_TIME - Metric 1 - Time to resolve hostname through DNS.

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

SERVER_RESP_TIME - Metric 3 - Overall time to read the file (receive data on the data connection).

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

GROUP_TIME - Metric 5 - Time to select newsgroup and get request overview of last 100 articles.

READ_TIME - Metric 6 - Time to read articles with the overall size of 10000 bytes.

TEAR_DOWN_TIME - Metric 7 - Overall time to send the QUIT request and receive the response.

DATA_TRANS_TIME - Metric 8 - The number of bytes transferred.

NTP

AVAILABILITY - If a measurement could not be retrieved a 0 is set, 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_TPUT - Transfer bytes/Transfer Time in kbytes/sec.

DATA_TRANS_BYTES - Metric 5 - The number of bytes transferred.

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

ODBC

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

RESPONSE_TIME - Total response time for the ODBC service.

SETUP_TIME - Time to setup database connection handles.

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

CONNECT_TIME - Metric 1 - Time to connect to database.

SERVER_RESP_TIME - Metric 2 - Time to respond to the SQL statement.

TRANSFER_TIME - Metric 3 - Overall time it took for the data transfer.

DATA_TRANS_BYTES - Metric 4 - The number of bytes transferred.

POP3

AVAILABILITY - If a measurement could not be retrieved a 0 is set, 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).

SETUP_TIME - Time to resolve address and establish the connection.

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

DNS_SETUP_TIME - Metric 1 - Time to resolve hostname through DNS.

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

SERVER_RESP_TIME - Metric 3 - Time it takes to receive the POP3 start header (+OK).

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

TRANSFER_TIME - Metric 5 - Overall time to read all messages in the mailbox and delete the IOPS test messages.

DATA_TRANS_BYTES - Metric 6 - The number of bytes transferred.

RADIUS

AVAILABILITY - If a measurement could not be retrieved a 0 is set, 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_TPUT - Transfer bytes/Transfer Time in kbytes/sec.

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

DATA_TRANS_BYTES - Metric 5 - The number of bytes transferred.

SAP

AVAILABILITY - If a measurement could not be retrieved a 0 is set, otherwise availability is set to 1. Availability requires both a successful connection and a successful RFC call.

RESPONSE_TIME - Total response time for the SAP service. Setup Time + Completion which is the time to complete a successful RFC call (including logon check and logout).

SETUP_TIME - Time to get a successful connection with the RFC server.

SMS

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

RESPONSE_TIME - Total response time for the SMS service.

SMTP

AVAILABILITY - If a measurement could not be retrieved a 0 is set, 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).

SETUP_TIME - Time to resolve address and establish the connection.

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

DNS_SETUP_TIME - Metric 1 - Time to resolve hostname through DNS.

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

SERVER_RESP_TIME - Metric 3 - Time it takes to receive the SMTP start header (220).

TRANSFER_TIME - Metric 4 - Overall time to transfer the mail request (including SMTP responses to the requests such as MAIL FROM:, RCPT TO: DATA, QUIT.

TRANS_BYTES - Metric 5 - The number of bytes transferred.

TEAR_DOWN_TIME - Metric 6 - Overall time to send the QUIT request and receive the response.

STREAM_MEDIA

AVAILABILITY - If a measurement could not be retrieved a 0 is set, 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).

SETUP_TIME - Time to resolve address and establish the connection.

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

CONNECT_TIME - Metric 1 - The time to connect to the server. If a proxy is used then this is the time it takes to connect to the proxy.

SERVER_RESP_TIME - Metric 2 - The time it takes for the server to start sending packets. This includes the set up time for the various protocols.

TRANSFER_TIME - Metric 3 - The time it takes to transfer the data.

PACKETS_RECEIVED - Metric 4 - Total number of packets received.

PACKET_LOSS - Metric 5 - The percentage of packets lost.

LATENCY - Metric 6 - 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 - Metric 7 - 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 set, otherwise availability is set to 1.

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

SETUP_TIME - Time to resolve address and establish the connection

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

DNS_SETUP_TIME - Metric 1 - Time to resolve hostname through DNS.

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

WAP

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

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

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

DNS_SETUP_TIME - Metric 1 - Time to resolve hostname through DNS.

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

TRANS_BYTES - Metric 5 - The number of bytes transferred.

WEBAPP

Note: This service type is used in the integration with OpenView Transaction Analyzer. See Chapter 5, Integrating with OpenView Products for more information.

RESPONSE_TIME - Average response time of the successfully completed transactions during the last interval.

AVAILABILITY - The ratio of availability probe requests that failed, to the total attempts during the last interval.

TRANSACTION_RATE - Metric 1 - Total number of completed transactions per second over the last interval.

RESPONSE_TIME_VIOLATION_COUNT - Metric 2 - Number of successfully completed transactions in the last interval whose measured response time exceeded the response time threshold configured in OVTA.

RESPONSE_TIME_VIOLATION_PERCENTAGE - Metric 3 - Percent of successfully completed transactions in the last interval whose measured response time exceeded the response time threshold configured in OVTA.

TRANSACTION_SIZE - Metric 4 - Average size of the successfully completed transactions during the last interval.

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

5

Integrating with OpenView Products

You can integrate Internet Services (OVIS) with OpenView Transaction Analyzer (OVTA), OpenView Operations for UNIX (OVO for UNIX - formerly know as IT Operations), Network Node Manager (NNM), or Openview Operations for Windows (OVO for Windows). Integrating OVIS with OVTA provides a complete performance and availability management solution for web-based applications. Integrating OVIS with OVO or NNM 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 determine reported problems.

Additional information on configuring remote UNIX probes is also covered in chapter 3, "Install Remote Probes on UNIX Systems" on page 96.

OVIS also integrates with Service Information Portal (SIP), Reporter, Performance Manager and the Performance Agent. This chapter covers:

- Integrating with OpenView Transaction Analyzer (OVTA)
- Integrating with OpenView Operations for UNIX (OVO UNIX)
- Integrating with Network Node Manager (NNM)
- Integrating with OpenView Operations for Windows (OVO Windows)

Integrating with OpenView Transaction Analyzer

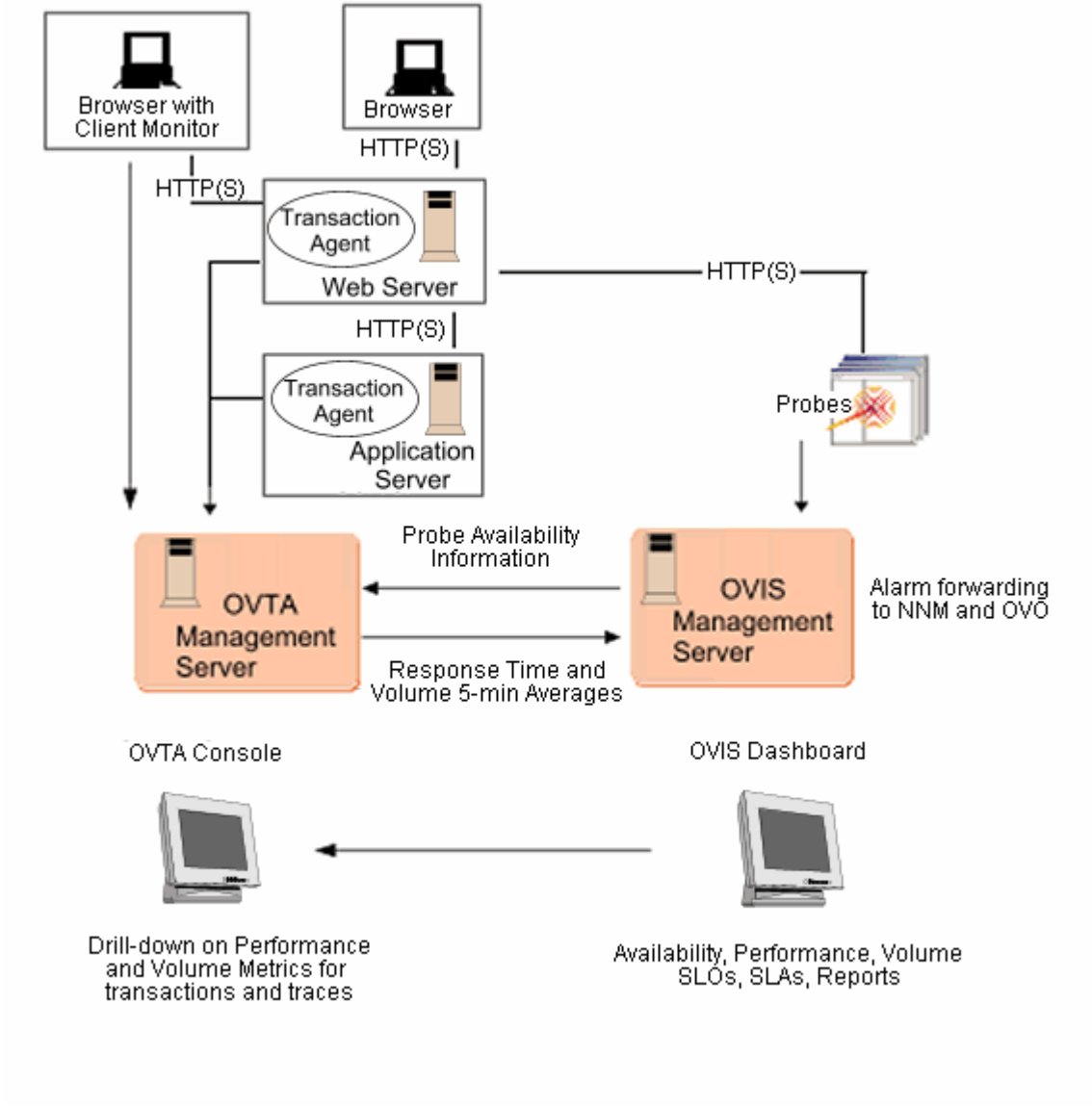
OVIS introduces the WEBAPP service type to import OpenView Transaction Analyzer (OVTA) transaction performance data summarized at reporting intervals (currently set at five minutes). OVTA measures and analyzes transaction volume and transaction response times for Web-based applications. OVTA uses transaction monitors to measure the real units of work submitted by end users. This gives you visibility into real end-to-end transaction response time as experienced by your end users. The transaction volume data provided by OVTA gives you a good picture of the actual usage of your web site.

Refer to the *OpenView Transaction Analyzer User's Guide* for more information. You can download the manual from the Openview web site: ovweb.external.hp.com/lpe/doc_serv/.

Note that the OVIS trial software you received with OVTA allows you to use the WEBAPP service type only. You need to purchase the OVIS product in order to use the HTTP/S, HTTP_TRANS or other probes.

The following diagram gives you a high level overview of the data flow in the OVIS/OVTA integration.

Figure 3 OVIS/OVTA Integration Data Flow



This integration provides the following features:

- More powerful service level objectives (SLOs) and service level agreements (SLAs) for performance and availability. The main areas of SLO/SLA enforcement center around availability, volume, and

responsiveness. OVIS HTTP/S and HTTP_TRANS probes provide availability and responsiveness measures. OVTA provides volume and response time measurements. The responsiveness measures from OVIS probes are limited in that they only include response time measurements taken from the synthetic probes. OVTA measurements complement the OVIS probe measurements by providing the volume and response time measurements of the real units of work submitted by end users. The combined OVIS and OVTA measurements allow you to set up and enforce SLO/SLAs for true performance and availability.

- Performance alarms can be configured for OVTA measurements and forwarded to NNM and OVO. This utilizes the existing SLO/SLA mechanism in OVIS. And it provides a common SLO/SLA and alarming solution for both OVIS and OVTA.
- Operations can view OVIS probe measurements and OVTA transaction measurements in a single pane - the OVIS Dashboard. In addition, you can launch the OVTA console from the OVIS Dashboard for further troubleshooting information.
- Reports are provided for OVTA measurement data.

Overview of the Integration

A brief overview of the OVIS - OVTA integration is described below. See "Integration and Configuration Steps" on page 184 for details on how to configure the integration.

1. OVIS automatically detects if an OVTA management server is installed on the same machine. For a remote OVTA management server, you will need to specify the hostname, port, username and password in the OVIS Configuration Manager.
2. Next you configure OVTA transactions like any other OVIS service target. Use the OVIS Configuration Manager to set up Customer and Service Groups for the OVTA integration. Select WEBAPP - Web Application as the Monitored Service when setting up the service group.

   Then in the OVIS Configuration Manager select the OVTA transactions you want imported as Service Targets in OVIS.

Be sure to configure the Probe Location as the default Local System, this is required in order for OVIS to collect data. Since the integration is only supported on the OVIS server (Local System), all you need to do is configure one default Local Probe Location.

3 Configure any Service Level Objectives (SLOs), Service Level Agreements (SLAs) for the Service Group. If you want alarms to be forwarded to OpenView Operations for UNIX, OpenView Operations for Windows or NNM then you need to set the alarm destination and configure OVIS integration with these products, too.

4 Save the configuration. Wait for data collection to begin and then check the status of the Web App service targets imported from OVTA.

5 Once data has been collected you can use the OVIS Dashboard to monitor the OVTA transactions you configured for import into OVIS. For more detailed analysis, you can launch the OVTA console from the OVIS Dashboard through the Web App tab.

6 In the OVIS Dashboard, you can click on the Trace button to show the HTTP and HTTP_TRANS probe traces that have additional drill-down data from OVTA. These are the traces from probes targeting Web servers on which OVTA transaction agents have been deployed. Clicking on the Drill Down button in this Trace display, launches the OVTA console which provides transaction sub-component detail.

7 After the nightly reports are generated in OVIS you can use the Reports tab in the OVIS Dashboard to see reports with information specific to OVTA.

8 Tune the SLO/SLA thresholds as needed to get more meaningful alarms and reports.

Metrics Collected

The following OVTA specific measurements are provided. These are summary statistics for the transactions imported into OVIS.

- Transaction rate (also referred to as Volume) - The total number of completed transactions per second over the last interval.
- Response Time Violation Count - The number of successfully completed transactions in the last interval whose measured response time exceeded the response time threshold configured in OVTA.

- Response Time Violation Percent - The percentage of successfully completed transactions in the last interval whose measured response time exceeded the response time threshold configured in OVTA.
- Transaction Size - The average size of the successfully completed transactions during the last interval.
- Response Time - The average response time of the successfully completed transactions during the last interval.
- Availability (see note below) - The ratio of availability probe requests that failed, to the total attempts during the last interval.

The availability metric is only meaningful if the transaction is also configured as a service target for an OVIS HTTP probe since the passive instrumentation provided by OVTA can't detect unavailability. It is recommended that an OVIS HTTP or HTTP_TRANS probe be configured for transactions that should include the availability measurement.

Usage Recommendations

It is recommended that only ***important*** transactions be configured. This avoids the extra overhead of importing OVTA transaction data that will not be used for alarms, service level agreements or OVIS data analysis.

When adding service level objectives (SLO), please adjust the SLO and alarm thresholds as needed for the transactions in the Service Group. Default objective thresholds are provided for each metric.

Use the OVTA console to monitor the response time averages, histograms, threshold violation counts, and transaction rates for the transactions of interest. This information can be used to override the defaults with more meaningful values.

If response time SLOs are configured, you may need to use the OVTA Configuration Editor to override the default response time thresholds. Note that the RESPONSE_TIME metric threshold applies to the average response time for the interval. As a result, SLOs using the RESPONSE_TIME metric are less effective. A more accurate response time SLO can be achieved by configuring a response time threshold in OVTA, then use the RESPONSE_TIME_VIOLATION_PERCENT or RESPONSE_TIME_VIOLATION_COUNT metrics when specifying SLOs in OVIS. See "Example SLOs and SLAs" on page 191 for examples.

The OVIS probe location contains the OVTA requesting node information. This allows an operator to use the OVIS Dashboard drill-down by Probe Location view to see the various requesting nodes for a transaction. If the requesting node is a probe, the probe location is the probe source system name. If the requesting node is a browser instrumented with the OVTA Browser Client Transaction Monitor, the probe location is a string indicating the time zone, connection type, and line speed used by the browser. See the *OVTA User's Guide* for more information on these values.

System Requirements

Both OVIS and OVTA must be installed and any initial configuration complete. They do not have to be installed on the same system. If you are not familiar with OVIS refer to Chapter 2, Getting Started with Internet Services for installation instructions and a getting started example you can go through.

If the OVTA and OVIS management servers are set up on the same system, be sure the system has adequate resources and is sized appropriately. Refer to the system requirements documentation for both OVIS and OVTA when sizing the common management server.

See the *OVTA Installation Guide*, "OVIS 4.x Integration" section for more on the configuration required to implement the Trace drill down feature in the OVIS Dashboard.

Limitations

- Measurements from OVTA may be delayed by as much as 15 minutes. This is due to the summarization algorithm using a timestamp that represents the start of a reporting interval for averaging the transactions. Therefore, it may take up to 10 minutes before the data from the managed nodes is available to the OVIS management server for alarming and another five minutes before the data is visible in the OVIS Dashboard.
- The OVIS status might display "No Probe Info" for certain transactions. This indicates that in the last reporting interval, the OVTA instrumentation monitors did not measure any transactions simply because these web pages were not accessed by any end users or OVIS HTTP/HTTP_TRANS probes.

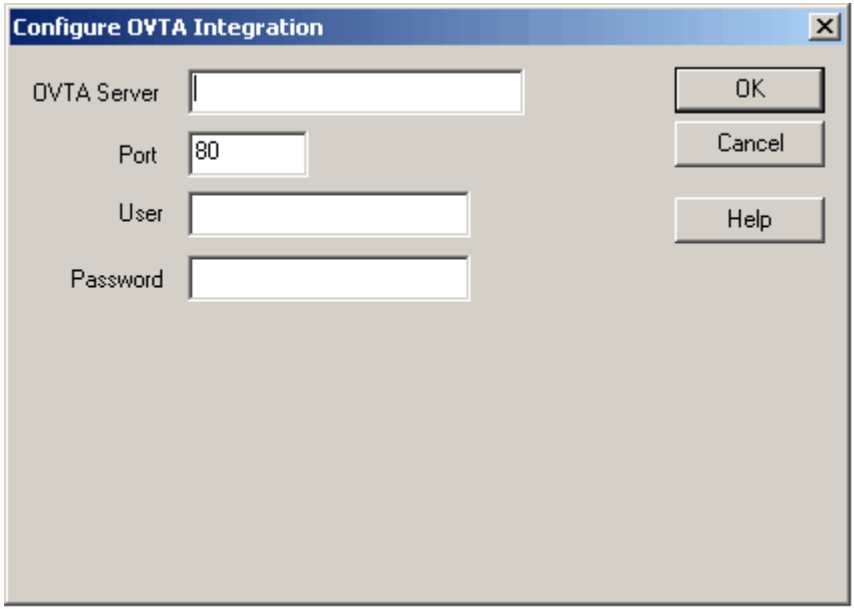
- The OVTA SLO Response time configuration is not integrated in the OVIS Configuration Manager. One must set these thresholds in the OVTA Configuration Editor for the transactions of interest. Refer to the *OVTA User's Guide* for further detail.
- Only one OVTA measurement server can be integrated with OVIS at a time.

Integration and Configuration Steps

The steps to integrate OVIS and OVTA are as follows.

Task 1: Configure OVTA Management Server

First identify the OVTA server (which can be local or remote). In the OVIS Configuration Manager, select **File > Configure > OVTA Measurement Server**. Enter the OVTA Server Name, Port Number and the OVTA User and Password for accessing the OVTA Configuration Editor. Note that if OVTA is installed on the same system as OVIS, the OVTA Server and Port is preset.



Task 2: Configure the Web Application Transactions

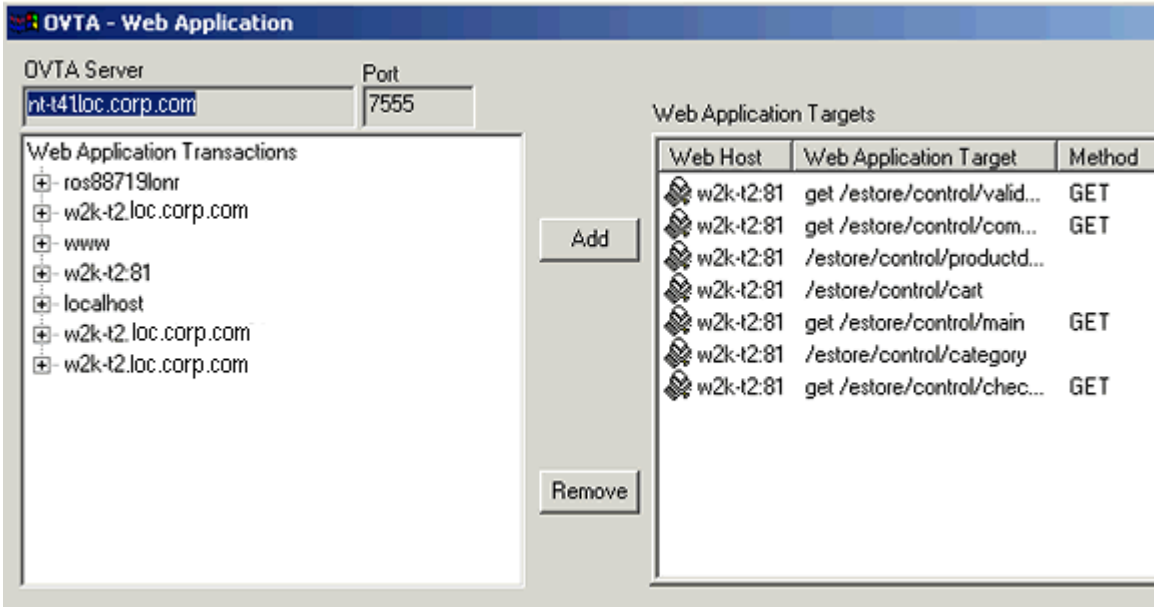
As with other OVIS services, simply create a new service group under which OVTA transactions should be grouped as service targets, and configure SLOs and a probe location.

In the OVIS Configuration Manager, either select the Configuration Wizard or set up the Service Group yourself by first selecting an existing Customer or right clicking on Customers and selecting New Customer to add a new Customer Name.

Then in the left pane, under the Customer name you will see the following listed: Service Groups, Service Level Agreements. Right click on Service Groups and select New Service Group.

Enter a name for this Service Group and select **WebApp - Web Application** from the drop down list as the Monitored Service. This adds a Service Group under the Customer name. You will then see the following listed under the Service Group: Service Targets, Service Objectives, Probe Location.

Right click on Service Targets and select New Service Target. The OVTA - Web Application dialog is displayed, which allows you to select the currently discovered transactions from the OVTA server.



Transaction types imported from OVTA have names derived from their corresponding URLs. The derivation is based on classification rules specified using the OVTA Configuration Editor. The following are some examples:

```
/estore/control/category

/estore/control/main

/estore/control/product

get /estore/control/main

get /estore/control/product
```

Note the some of the transaction names are prefixed with the http method "get" or "post". These are OVTA transactions measured at the web server using the OVTA Web Server Transaction Monitors. Transaction names without the http method prefix are those measured at the client. Client measurements can be measured by OVIS http probes or in the browser using the OVTA Browser Client Transaction Monitor.

Service groups can be used to logically group related transactions (e.g. shopping cart).

It is recommend that only the transactions of interest are configured for OVIS integration. Examples of interesting transactions:

- Transactions that need to be set up for alerts/alarms.
- Transactions that should be included in the nightly reports.
- Transactions that should appear in the OVIS Dashboard for high-level monitoring. This provides a single pane view of the OVTA transaction measurements along with the OVIS probe measurements. One uses the OVTA Console launch to drill down for more detailed transaction monitoring.

Make sure to add a Probe Location as this is required for OVIS to begin importing measurements from OVTA. For the OVTA integration select the default Local probe location.

You must save the configuration before exiting the OVIS Configuration Manager in order for measurements to be collected.

Task 3: Configure SLO and SLAs

The combined OVIS and OVTA measurements enable you to configure SLO/SLAs in the areas of availability, responsiveness, and volume. The latter provide the performance SLO/SLA capability by utilizing the OVTA measurement data.

Set SLOs: In the OVIS Configuration Manager left pane select Service Objectives, under the Service Targets you configured for the OVTA integration, and right click to select New Objective. In the Objective Information dialog set up Service Level Objectives for the OVTA based metrics collected. Refer to the online help for this dialog for how to set up SLOs.

Set Alarm Forwarding to OVO or NNM: If you want alarms to be forwarded to OVO or NNM then you need to configure the destination for the alarms. In the OVIS Configuration Manager select **File > Configure > Alarm Destinations** and select where you want the alarms to be sent. Note you will also need to configure the integration of OVIS with OVO or NNM if this has not already been done. See the later sections in this chapter for detailed steps.

Set SLAs: In the OVIS Configuration Manager left pane tree view under the same OVTA Service Group, right click on Service Level Agreements and select New Service Agreement to set up an SLA.

Be sure to save any changes you make to the configuration before exiting the Configuration Manager.

See "Example SLOs and SLAs" on page 191 for examples that show different SLO/SLAs you may want to set up for the OVTA data.

You may need to set up multiple Service Groups if SLOs need to be set on different transaction types. For example, one Service Group might include only transaction types measured at the web server for volume SLOs while another might include transaction types measured at the client for end-to-end responsiveness SLOs.

Task 4: Save the configuration and check status

You must save the configuration before exiting the OVIS Configuration Manager in order for measurements to be collected.

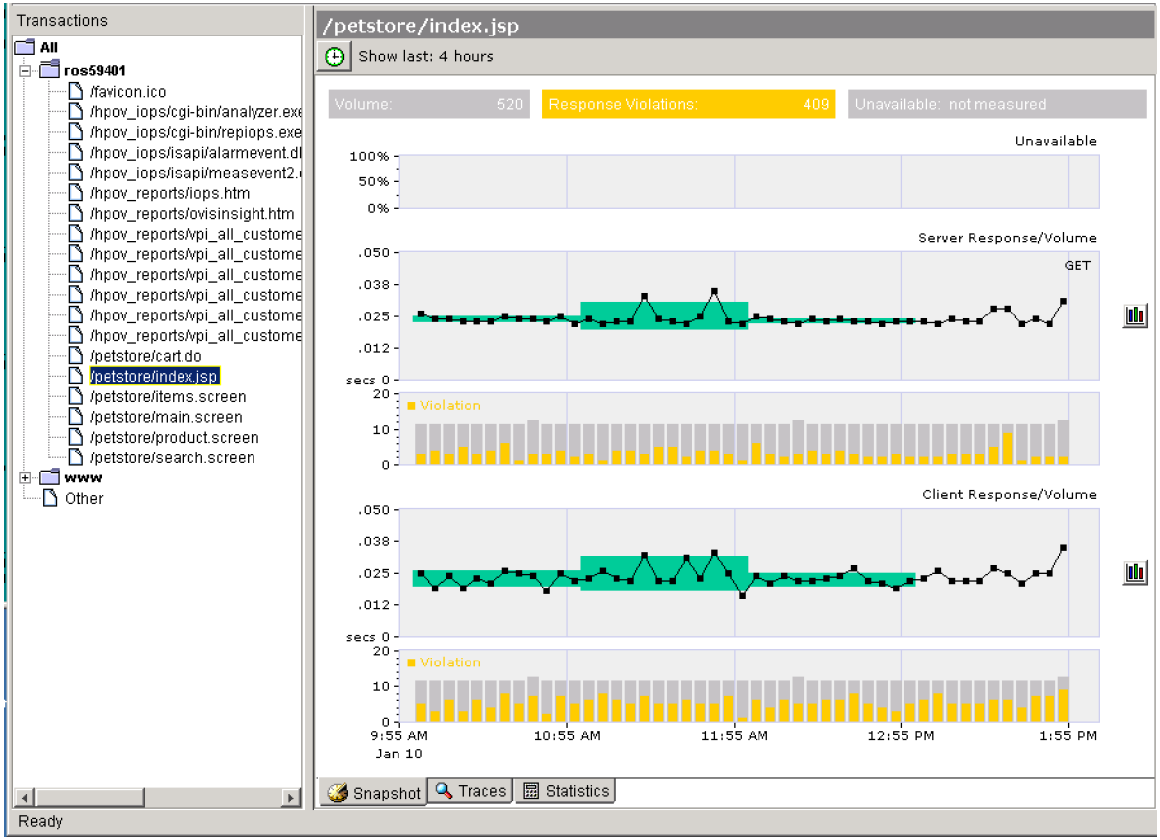
After saving the configuration, wait 10 - 15 minutes for the data to be collected. Then check the status of the new Web App service targets imported from OVTA. In the OVIS Configuration Manager select **Status** in the left

pane. The service targets will show status of green if the OVTA transaction monitor measured any transactions during the last reporting interval. If the status is red, it could be that the web pages that make up these transactions simply were not access, or the OVTA transaction monitors may not be enabled. Refer to Chapter 6, Troubleshooting Information for more information.

Task 5: Use the OVIS Dashboard to Monitor Web Application Transactions

The OVIS Dashboard can be used for high level monitoring of the OVTA Web Application Transactions configured in OVIS. When more detailed monitoring is needed, you can launch the OVTA Console from the OVIS Dashboard by selecting the Web App tab.

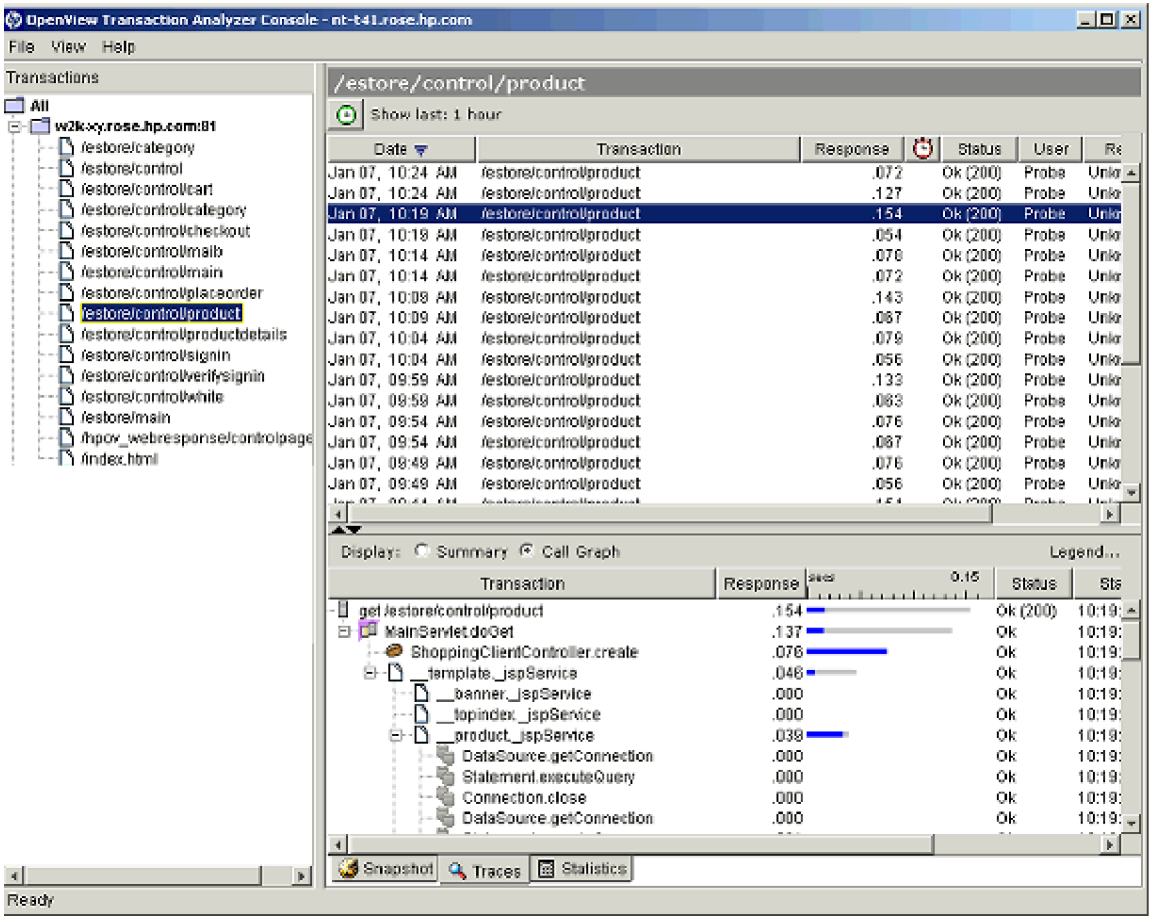
Note that in order to view OVTA data from the Web App tab or Trace button in the Dashboard, either restricted views must not be enabled or if restricted views is enabled, you must be logged in as All Customers. Restricted Views is configured in the OVIS Configuration Manager **File > Configure > Restricted Views**.



Task 6: Use the Trace function in the OVIS Dashboard to See Subtransaction Trace Data for HTTP and HTTP_TRANS Probes

The Trace button in the OVIS Dashboard shows HTTP and HTTP_TRANS service targets that result in transactions that are also monitored by OVTA on the web or application servers.

Clicking on the Drill Down button in the Trace display launches the OVTA GUI in context, automatically selecting the corresponding transaction and showing the trace view for this transaction.



Note that in order to view OVTA data from the Web App tab or Trace button in the Dashboard, either restricted views must not be enabled or if restricted views is enabled, you must be logged in as All Customers. Restricted Views is configured in the OVIS Configuration Manager **File > Configure > Restricted Views**.

Task 7: Web Application Transactions Reports

Reports with OVTA specific data are available in the OVIS Dashboard Reports page.

Task 8: Tune the SLO/SLA Thresholds

Based on your review of the alarms being generated and the data in the Dashboard and reports you may want to tune the thresholds for more meaningful alarms and reports. Use the OVIS Configuration Manager to change SLOs and SLAs. Use the OVTA Configuration Editor to set the response time thresholds.

Example SLOs and SLAs

Availability

While possible, there is really no need to configure availability SLO/SLAs using the OVTA measurement data. A more direct approach is to simply set up an OVIS HTTP service target in OVIS that corresponds to the OVTA transaction and configure the availability SLO/SLA using the OVIS http probe measurements.

Responsiveness

The RESPONSE_TIME metric for OVTA measurement data is a five minute average. As such, it is only useful for high-level monitoring. For responsiveness SLO/SLA enforcement, you need to set SLOs on the response time violation counts and/or percentages (RESPONSE_TIME_VIOLATION_COUNT and RESPONSE_TIME_VIOLATION_PERCENTAGE).

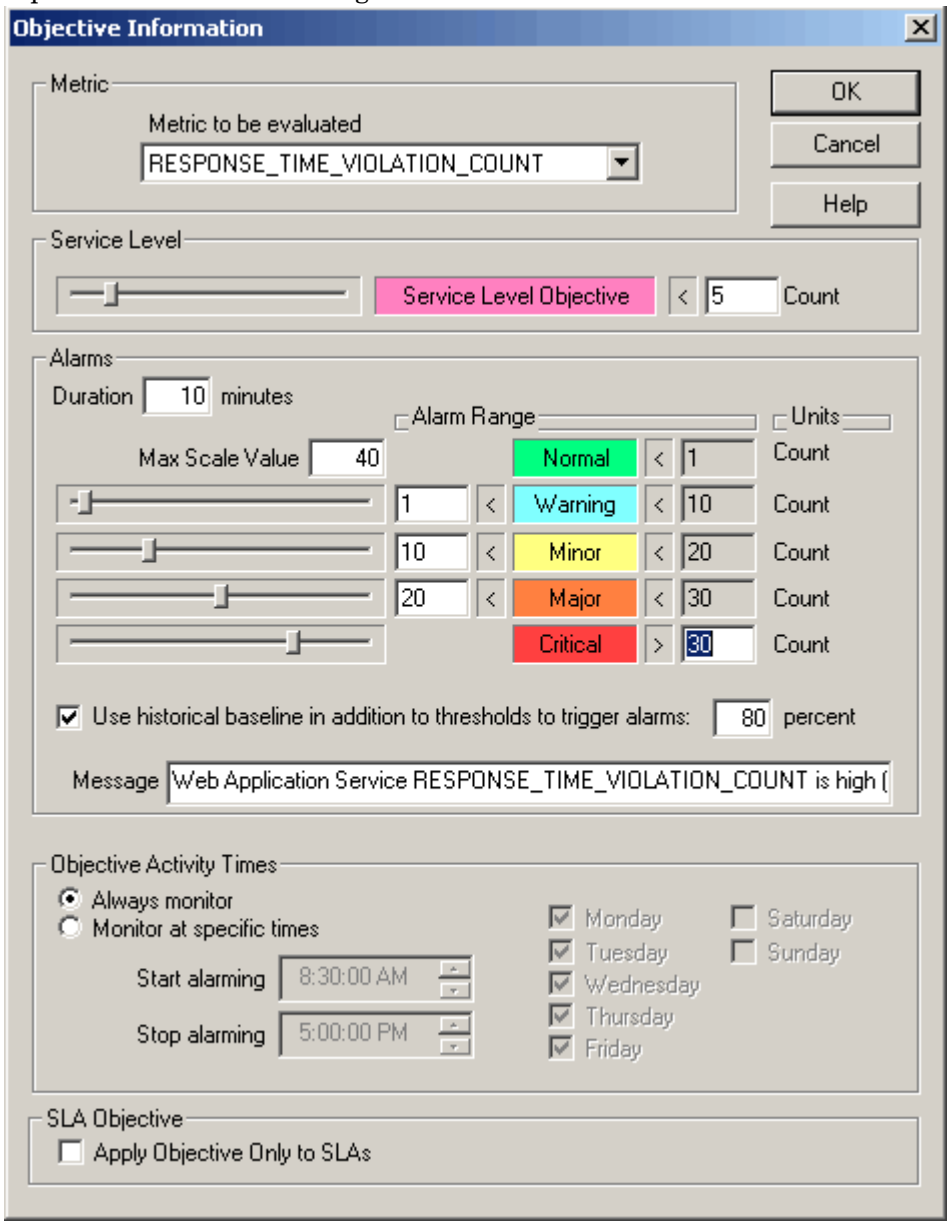
The response time violation threshold for OVTA transactions cannot be configured in the OVIS Configuration Manager. Use the OVTA Configuration Editor to set the thresholds on the transactions of interest. The

RESPONSE_TIME_VIOLATION_COUNT and RESPONSE_TIME_VIOLATION_PERCENTAGE metrics are measured in the OVTA Transaction Agent against these configured thresholds. Refer to the *OVTA Users Guide* for additional information.

The transaction types selected in the Service Group for responsiveness SLOs can be measured either at the client or at the web server. As discussed earlier, those measured at the web server are prefixed with the http method before the transaction name. If using the OVTA Browser Client Transaction Monitor, one can configure the responsiveness SLOs against the client transaction types. Note, however, that if this transaction type is also being probed, this SLO will be applied against the response time metrics measured by both the probe and the OVTA browser client monitors.

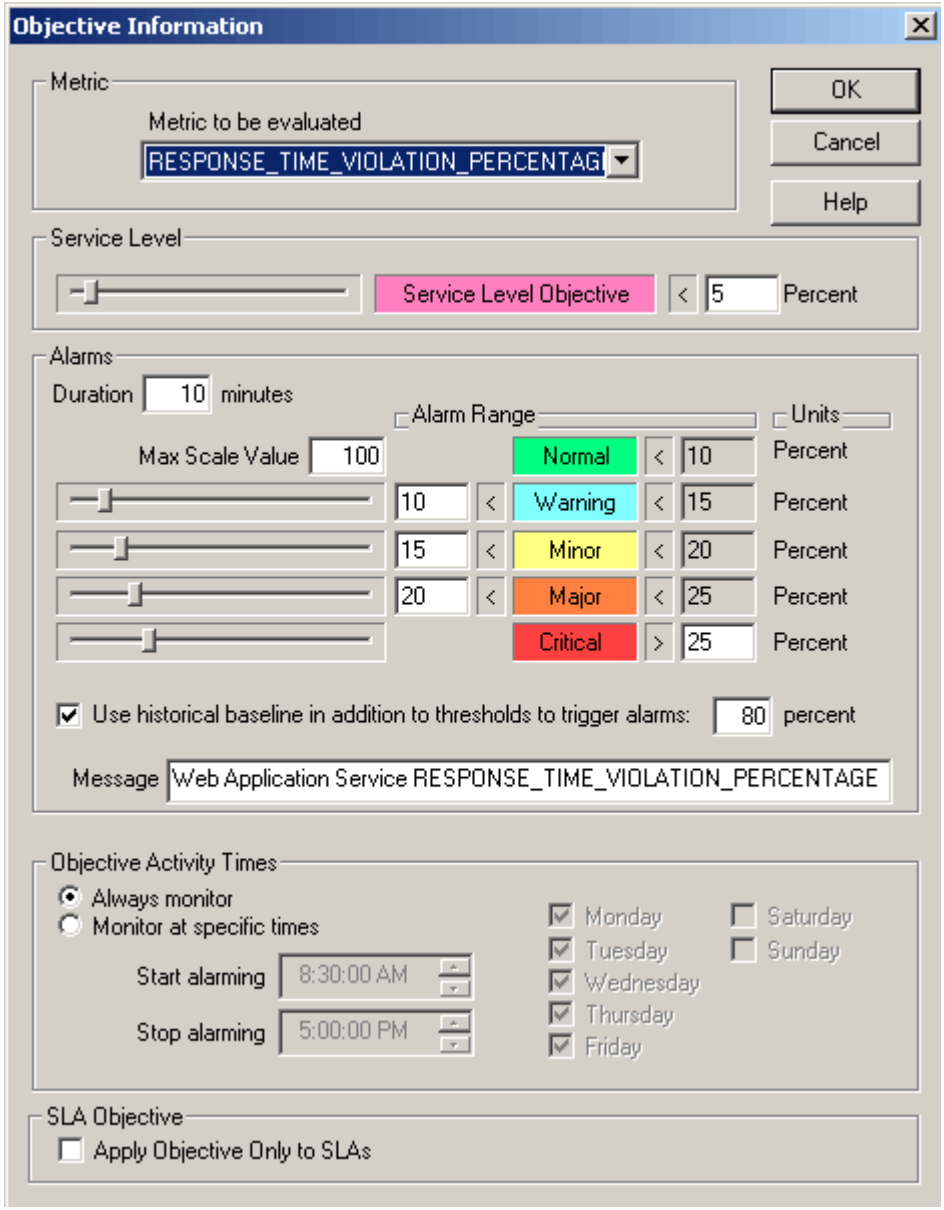
Responsiveness SLO Example #1

Ensure that fewer than 5 web page hits will have a response that exceeds the response time threshold configured in OVTA in a five minute interval.



Responsiveness SLO Example #2

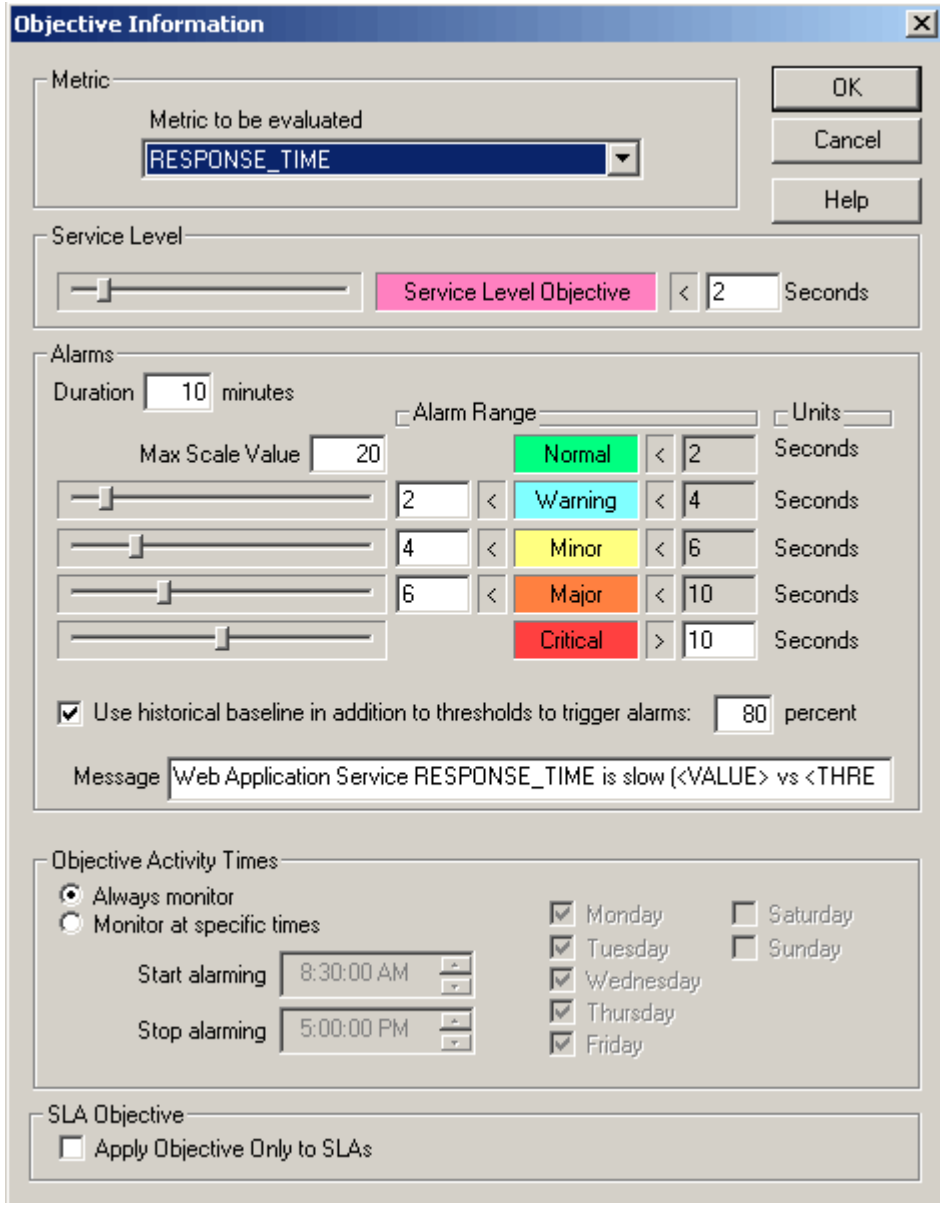
Ensure that no more than 5% of the web page hits have a response time exceeding the response time threshold configured in OVTA in the interval.



Responsiveness SLO Example #3

Ensure that the average response time is less than two seconds.

Note: This works best with a single transaction. Since the SLO is applied on a five minute average, some very high or low response time values from the individual transaction may skew the average. Even with a single transaction, the average may not be a good indicator of the true end-user experience. As mentioned earlier, the response time threshold count and percentage metrics are more useful for response time SLO enforcement.

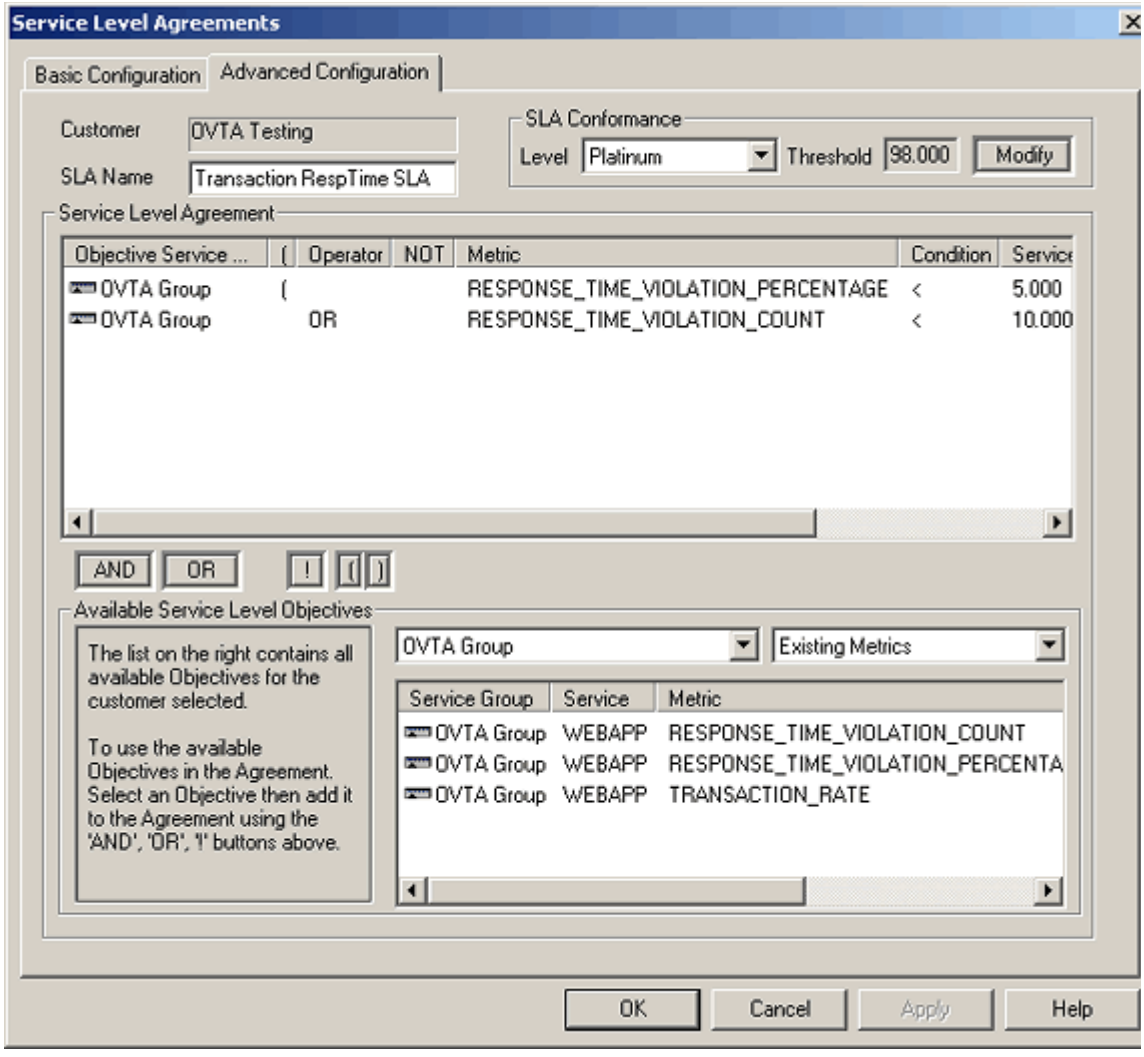

Objective Information
Metric
Metric to be evaluated
RESPONSE_TIME
OK
Cancel
Help
Service Level
Service Level Objective
< 2 Seconds
Alarms
Duration 10 minutes
Alarm Range
Units
Max Scale Value 20
Normal < 2 Seconds
2 < Warning < 4 Seconds
4 < Minor < 6 Seconds
6 < Major < 10 Seconds
Critical > 10 Seconds
Use historical baseline in addition to thresholds to trigger alarms: 80 percent
Message Web Application Service RESPONSE_TIME is slow (<VALUE> vs <THRE
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

Responsiveness SLA

Multiple SLOs can be combined for more powerful SLAs.

Use case: Ensure that no more than 5% of the web page hits will have a response time that exceeds the response time threshold configured in OVTA or the total number of response time threshold violations does not exceed 10 in a five minute interval.

Combining the response time violation count and percent SLOs in this manner prevents a high response time SLO violation percent from violating the SLA unless there are likewise a high number of total SLO violations (i.e., an adequate sample count).


Service Level Agreements
Basic Configuration
Advanced Configuration
Customer
OVTA Testing
SLA Name
Transaction RespTime SLA
SLA Conformance
Level
Platinum
Threshold
98.000
Modify
Service Level Agreement
Objective Service ...
(
Operator
NOT
Metric
Condition
Service
OVTA Group
(
RESPONSE_TIME_VIOLATION_PERCENTAGE
<
5.000
OVTA Group
OR
RESPONSE_TIME_VIOLATION_COUNT
<
10.000
AND
OR
!
(
)
Available Service Level Objectives
The list on the right contains all available Objectives for the customer selected.
To use the available Objectives in the Agreement. Select an Objective then add it to the Agreement using the 'AND', 'OR', '!' buttons above.
OVTA Group
Existing Metrics
Service Group
Service
Metric
OVTA Group
WEBAPP
RESPONSE_TIME_VIOLATION_COUNT
OVTA Group
WEBAPP
RESPONSE_TIME_VIOLATION_PERCENTA
OVTA Group
WEBAPP
TRANSACTION_RATE
OK
Cancel
Apply
Help

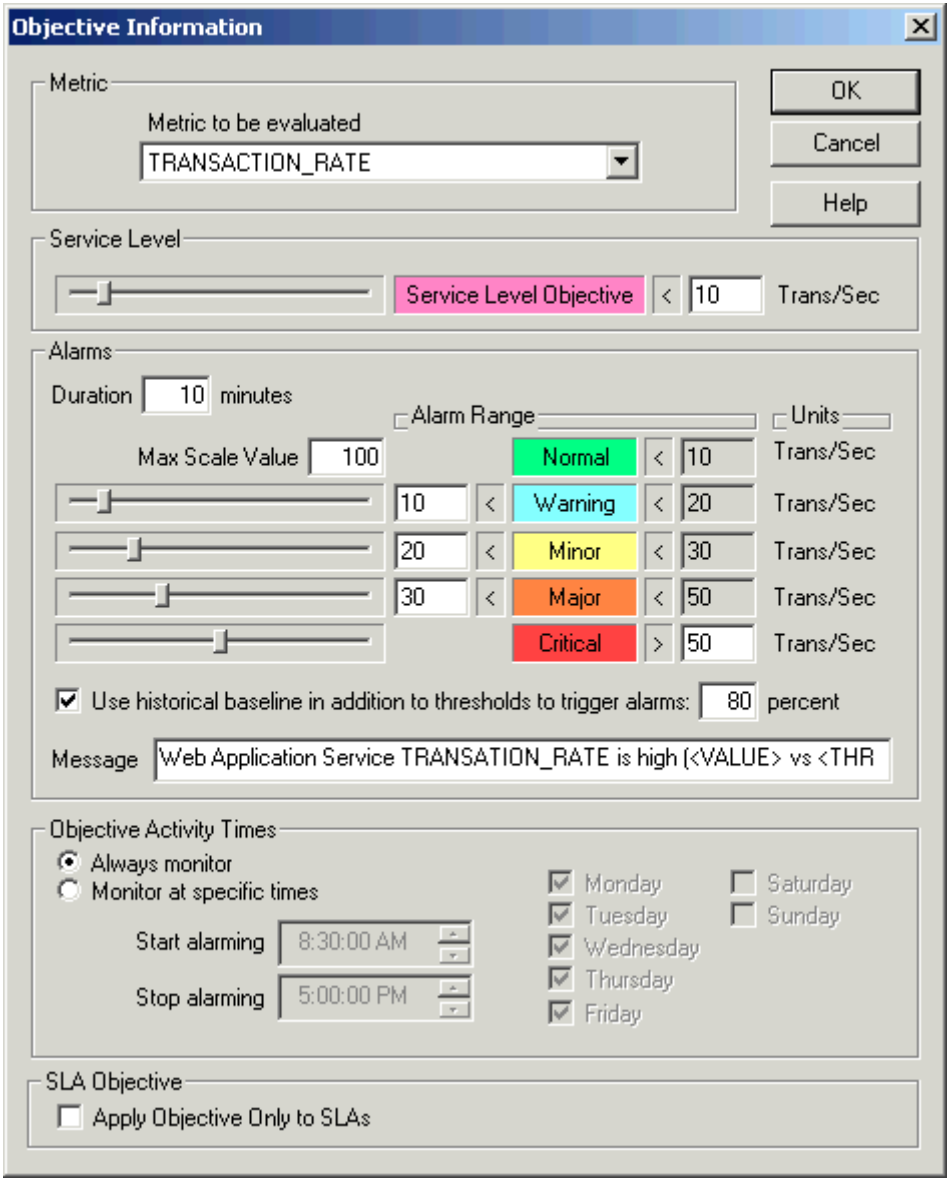
Volume

The TRANSACTION_RATE metric can be used to set volume SLOs. This can also be used in combination with responsiveness SLOs when configuring SLAs.

Note - True volume SLOs can only be measured at the web servers using the OVTA Web Server Transaction monitors. Therefore, the transactions in the service group for which volume SLOs are configured should be limited to the web server transactions. These are the transactions whose name contains the http method prefix (i.e. "get" or "post").

Volume SLO Example #1

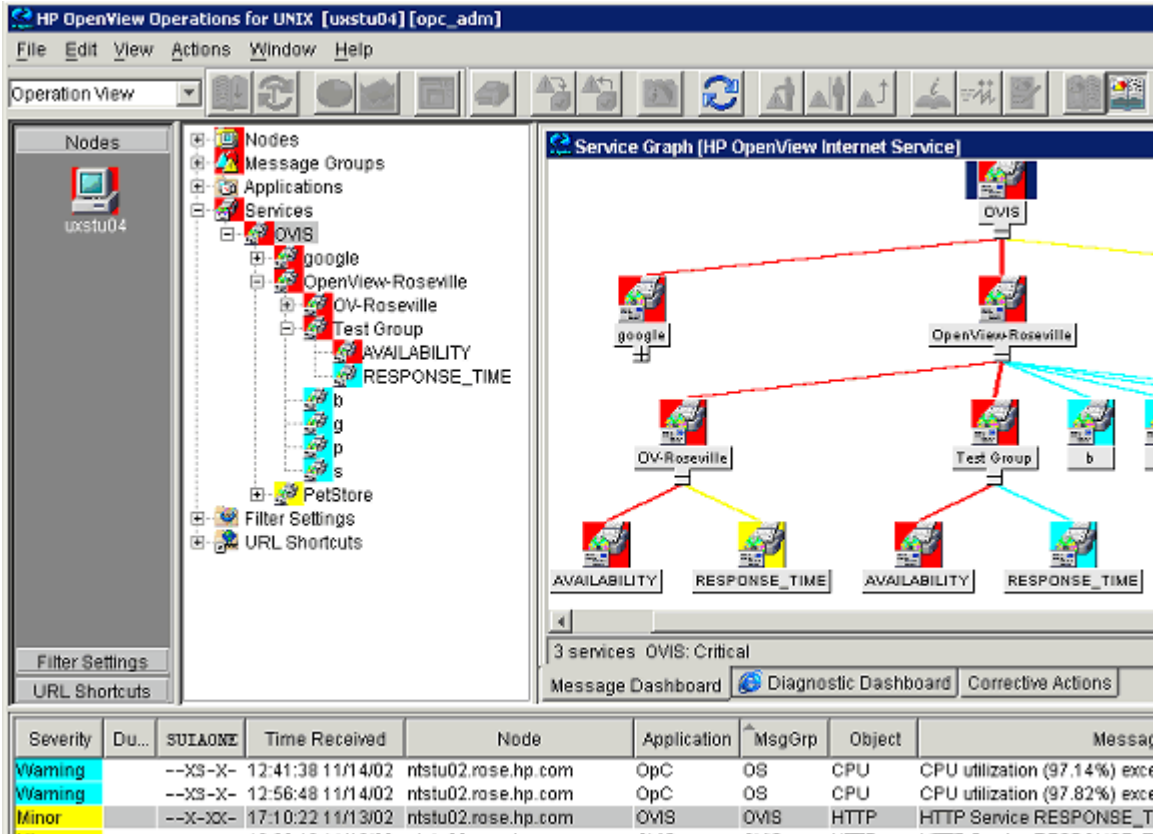
Use case: Ensure that there are no more than 10 hits per second.



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 (6 and 7). Note that templates are not yet localized.



Requirements

- Refer to the Internet Services release notes for OVO UNIX version requirements.
- 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 OVIS 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.). With OVO 7.x, both must be installed into C: drive unless you have installed the OVO NT agent patch.

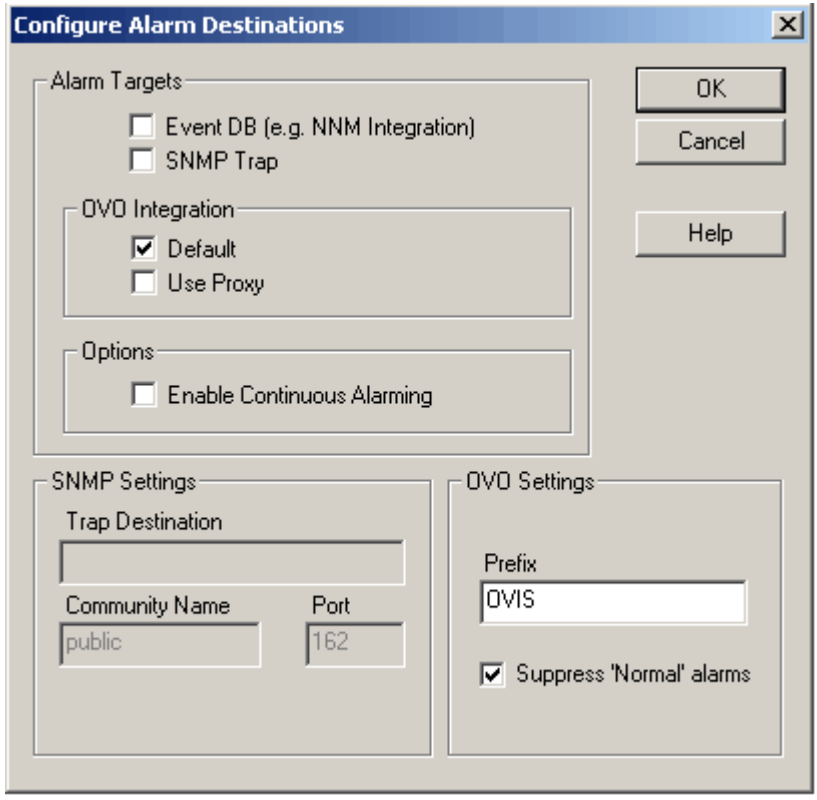
- A checkbox selection within the Internet Services Configuration Manager dialog to forward alarms to OVO.
- Installation of an OVO agent on the Internet Services server for forwarding alarm messages to OVO.
- If you are installing the integration on a Japanese OVO system, it is required that swagentd 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).

Integration Steps

Overview

To install Internet Services integration for use with OVO for UNIX, you need to perform the following tasks. See the tasks that follow for detailed steps.

- 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.
- 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 you need to remove the existing OVIS/OVO UNIX integration files.

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

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

   Internet Services

   OVIS Probe NT
   OVIS Probe Unix
   OVIS Server
   OVIS Server (2)
   OVIS ITO Mgmt Server

   If you are upgrading from OVIS 3.5 the groups include:

   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 OVIS and OVIS_Errors. If you are upgrading from OVIS 3.5 these groups are VP-IS and VP-IS_Errors.

5 Optional: If the passive monitoring components (OVIS 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. Refer to the installation instructions provided with the CD.

1 In the Internet Services Configuration Manager **Configure > Alarm Destinations** dialog the Prefix should be OVIS. Change from VP-IS to OVIS if needed.

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

Complete the following steps 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. Please refer to the *OVO for UNIX Administrator's Reference Guide* for OVO agent installation information. With OVO 7.x, both must be installed into C: drive unless you have installed the OVO NT agent patch.
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 system.

   If you plan to choose **OVO Integration-Use Proxy** in OVIS 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 OVO message browser. (Select **Window>User**

Bank and modify for appropriate operators to receive messages. 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 Note that there are two template groups, OVIS Server and OVIS Server (2). Only one of these needs to be assigned. Typically you would use the OVIS Server template group.
If you wish to use good/bad message correlation feature that comes with OVO 6 and higher, the OVIS Server (2) template version is recommended. In addition, the Suppress Normal Alarms checkbox in the OVIS Configuration Manager (select **File > Configure > Alarm Destinations**) Alarm Targets dialog needs to be unchecked if the good/bad message correlation is to be enabled.

Modify log files **OVIS Errors (Server - Reporter)** and **OVIS Errors (Server - OVIS)** to correctly refer to the OVIS installation directory. For example: `C:\Program Files\HP OpenView\Data` or `C:\rpmtools`.

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.

Modify **OVIS Errors** (Probe) log file to correctly refer to the OVIS installation directory. For example: `C:\Program Files\HP OpenView\Data` or `C:\rpmtools.`

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

1 Be sure a local OVO agent is running on the OVO Management Server.

2 Assign the **OVIS ITO Mgmt Serve**r 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 five 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

And select the **Update** button.

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 - See 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

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 Windows operating systems.

Requirements/Recommendations for NNM Integration

- Refer to the Internet Services release notes for NNM version requirements.
- 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-based NNM but is not the default for NNM on Windows. Setting submap persistence to **All Levels** in order to fully integrate Internet Services with NNM on Windows may cause NNM on Windows to require more memory (possibly much more) to function efficiently (see note below).
- Netscape (version 4.7 or greater) and/or Internet Explorer (version 5.5 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 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.

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 Windows 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 provided with the CD.** Installation differs depending on whether you are integrating with NNM on Windows, 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

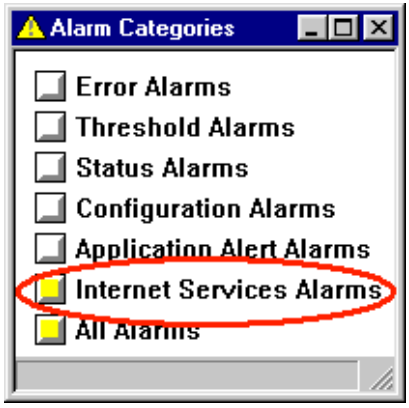
You will find several changes in NNM after you install the Internet Services integration:

- New alarm category: Internet Services Alarms appear 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.



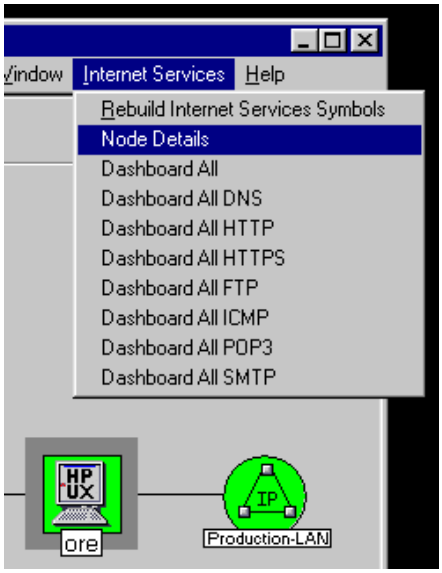
The alarms in this category originate from the Internet Services system. Internet Services alarms work the same as other NNM alarms so that you can expect to use standard NNM methods to configure and manage them as necessary:

- 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** - 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** - 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.

- T**he 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 following:

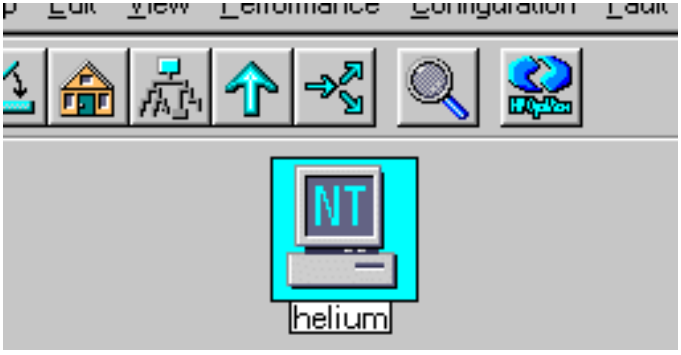
- **Customer(s)** served by the node.
- **Services monitored** - customers have child submaps that contain symbols representing the services monitored for them.
- **service objective alarms** - services also have child submaps that display the service objective alarms for the monitored service.

An illustration later in this chapter shows new symbols.

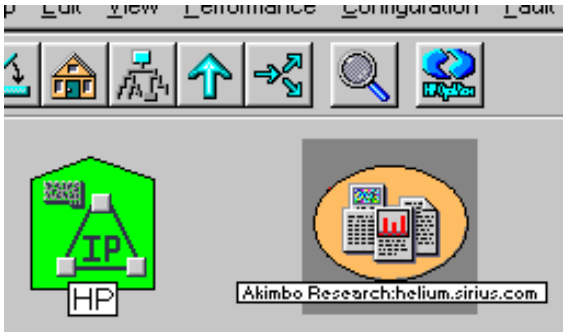
About Configuration Events

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:

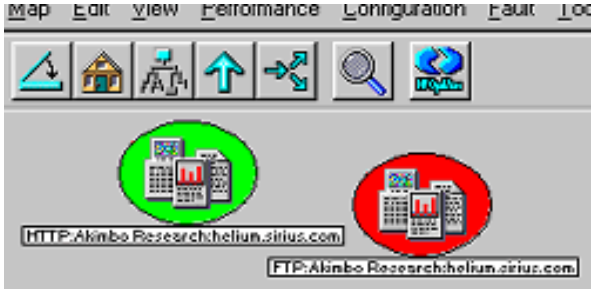
1 The status source of the object representing the target node (where the service is running) is set to **Compound (Propagated)**. Normally, nodes on the map determine their status from the interfaces on the node. Changing the status source to compound causes the node to use the status of all of its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

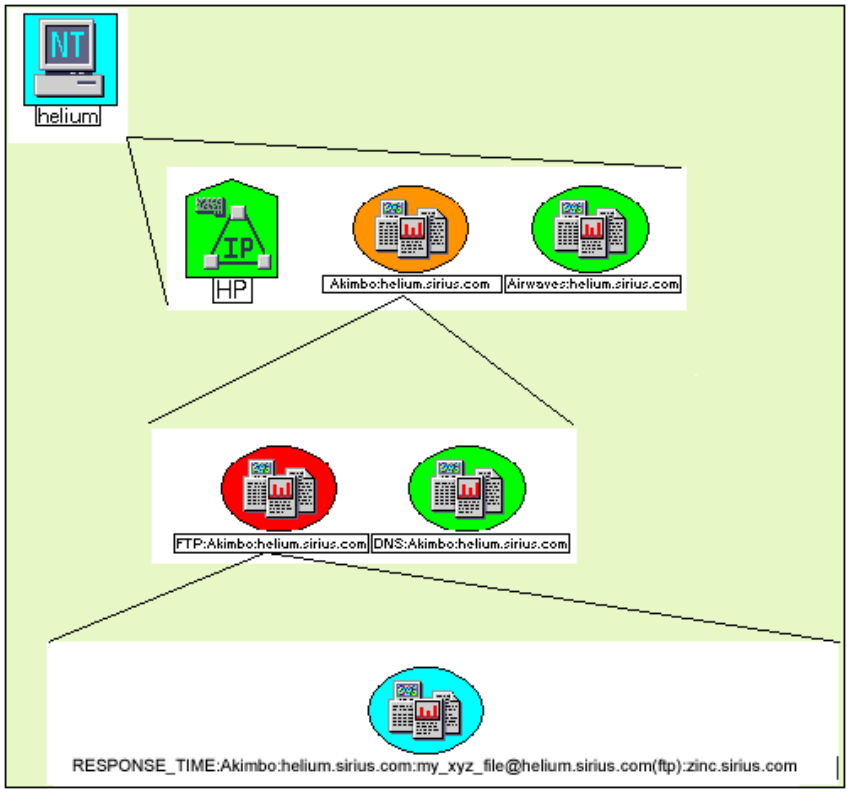
The name of the service objective symbol would then be:

RESPONSE_TIME:FTP:Akimbo:helium.sirius.com:my_xyz_file@helium.sirius.com:zinc.si rius.com

Service-objective symbol names can be lengthy. If necessary, use the Panner (or on Windows, 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:

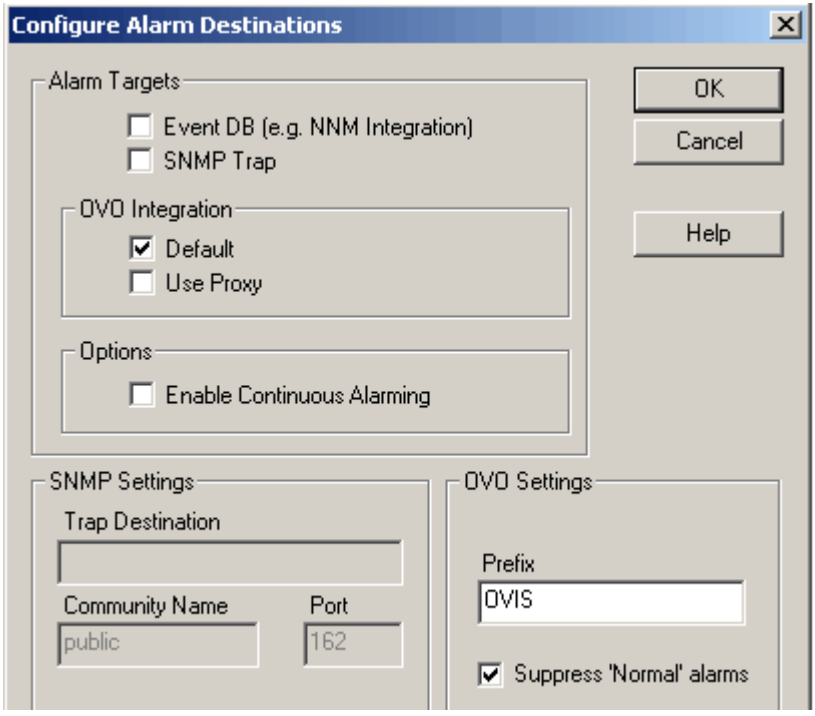
opcmsg a=OVIS o=OVIS_Test msg_text="Test".)

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 opcmsg policy, which flags all messages as "unmatched" because no specific condition was set up.

6

Troubleshooting Information

This chapter gives you basic troubleshooting information including the following:

- Troubleshooting Red Status Indicators
- Looking at OVIS Trace Files
- OVO for UNIX Integration Enabled but not Working Properly
- Troubleshooting the HTTP_TRANS Probe
- Troubleshooting the Streaming Media Probe
- Troubleshooting the TCP Probe
- Troubleshooting the OVIS to OVTA Integration

Refer to the Support folder on the Internet Services CD for a list of files with version information.

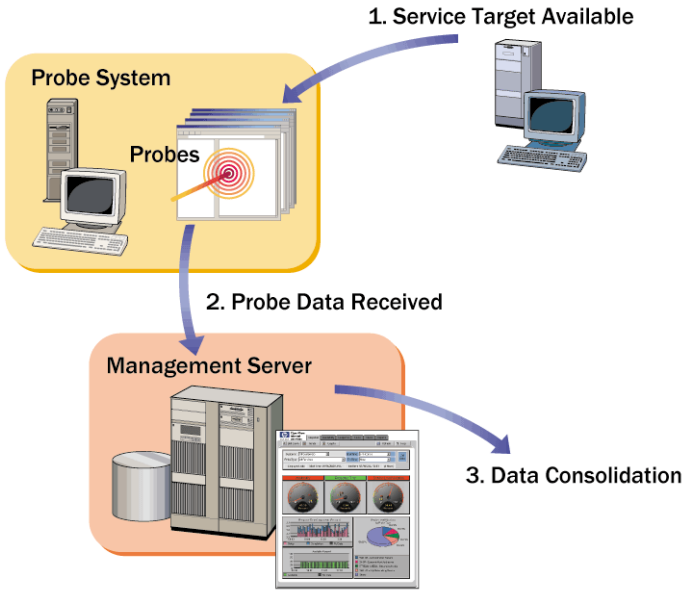
Troubleshooting Red Status Indicators

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 4 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 227
- **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 228
- **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 228

- **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 227.
- **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" on page 250 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 Windows 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: Verify your proxy information

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 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 Information section. You can consult the instructions in "No Probe Information" on page 226 in order to try to find the source of this problem.

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 easier to read.

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, summarizes it and puts it into the database has not done so. There are a couple of possible reasons for this.

- **There is no data to consolidate:** Consult the instructions in the previous section "No Probe Information" on page 226 to try to find the source of this problem.
- **The Reporter service is not running:** In the Windows Control Panel 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 **Administrative Tools > 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.

status.iops	Main status
status.PM	Embedded custom graphs status
status.Reporter	Embedded reporting status
trace.measEvent2	trace for the measEvent2.dll
trace.DllVersion	trace for Reporter DLLs
trace.iopscollector	trace for iopscollector
trace.IOpsConfig	trace for the Configuration Manager
trace.iopsmaint	trace for the data maintenance
trace.iopsslaevaluator	trace for the SLAs
trace.RepIOps	trace for the Dashboard
trace.RepCrys	trace for the nightly reports

trace.RepMaint	trace for the database maintenance
trace.ExportIOps	trace for the ExportIOps program
trace.IOpsLoad	trace for the IOpsLoad program
trace.Scheduler	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.

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:

If you are using OVO 7.x, be sure you have installed the OVO NT agent patch.

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.

Troubleshooting the Streaming Media Probe

For problems running the Streaming Media probe check the following:

Possible Cause: Media player can not reach the media target from the probe location.

Solution: Verify with the media player that your media target can be reached from the probe location and fix per any error messages.

Possible Cause: Media missing codecs/patches/updates.

Solution: Make sure you have the correct **codec(s)** installed for the media that you will be monitoring. Go to the Real Player 8 tool to the **View > Preferences** menu item and select the **Upgrade** tab box. Then select **Check for update now** in the **Update Notification** section. Be careful not to select any options that would install the latest "Real One" player. There may be many codecs/patches/updates that are suggested. Download the appropriate/ recommended codecs/patches/updates.

Troubleshooting the TCP Probe

Problem: While running the TCP probe, the number of connections to the TCP port in CLOSE_WAIT state keep climbing. You can check this with the netstat command.

Possible Cause: This may be caused by the port being probed not correctly shutting down the socket even though the probe requested it to do so. This is usually related to the application being probed not closing the socket correctly when requested by the probe.

Solution: Stop probing or increase the interval for probing.

Troubleshooting the OVIS to OVTA Integration

The following are some possible questions you may have in troubleshooting the OVIS to OpenView Transaction Analyzer (OVTA) integration.

Problem: The **Trace** button does not appear on the OVIS dashboard.

Solution: The registry entry for the OVIS-OVTA integration has not been set up on the OVIS measurement server. Check the OVTA User Guide for details on how to set this up.

Problem: Clicking the **Trace** button in the OVIS Dashboard results in a **Page Not Found** error.

Solution: Make sure that the file `CorrRecords.asp` has been copied to the right location under the OVIS Management Server install directories. Check the *OVTA User Guide* for details on how to set this up. Ensure that the references in this file to the OVIS Management Server, port number, and protocol in the line `<form action=` are correct.

Problem: The table displayed on the page loaded after clicking the **Trace** button in the OVIS Dashboard does not contain any data rows.

Solution: This implies that there are no records in the OVIS database with transaction breakdown data (from OVTA) available. This could be due to:

Using heavy weight probes which are not set up to integrate with OVTA breakdown data.

Using probe targets on web servers not running an OVTA Web Server Monitor.

Problem: The **Get Details** button in the OVIS Dashboard Trace display does not launch the OVTA GUI.

Solution: This could be due to:

Java WebStart is not installed. If it is not installed you will be re-directed to a page to download it. Follow the directions to download and install Java WebStart.

The OVTA measurement server is down.

Problem: I'm running OVIS 4.x on the same server as OVTA, but I don't see probe data in the OVTA Console. Why not?

Solution: Verify the following:

1. If the probe is hitting a web server that is not running an OVTA Web Server Monitor, an OVTA correlator will not be returned to the probe. The probe has an option to only forward probe data to the OVTA Measurement Server if a correlator is received back from the web server. By default, the behavior should be that all probe posts are forwarded regardless of the presence of an OVTA correlator. This can be overridden by setting the following registry key to a true (non-zero) value:

   HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\HP

   OpenView\IPA\CurrentVersion\PostOnlyIfCorr

   If this value is 0, all probe posts should forward to the OVTA Measurement Server.

2. When OVTA is installed, it sets an OVTA registry entry key for the URL path to the OVTA Measurement Server. The OVIS probe uses this to post (forward) the probe data to the OVTA Measurement Server. Verify that this is the correct URL to the OVTA Web Client Receptor Servlet.

   HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\HP

   OpenView\IPA\CurrentVersion\ClientReceptorURL

3. Make sure the version of OVIS is 4.0 or later.

4. If these items check out, check the log files in OVIS (the measevent2 component) for warnings or errors. If nothing comes up, enable diagnostic tracing in the OVIS measevent2 component following the instructions in the OVIS configuration manager online help.

7

Advanced Topics

This chapter includes advanced topics such as the following:

- Internet Services Architecture and Data Flow
- How to Move your Configuration to Another System
- Security
- Firewalls: Returning Data Through the Firewall
- How to protect the Probe System
- Configuring Communications Between Probe Systems and the Server
- Custom Reports
- Supported Databases
- Database Backup
- Starting Over
- 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 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:

- DHCP, Dial-Up Networking, DNS
- FTP File Transfer
- HTTP, HTTPS, Web Recorder (HTTP_TRANS)
- E-mail (IMAP4, POP3, Mail Roundtrip, SMTP)
- ICMP (ping)
- LDAP
- NNTP (Newsgroups)
- NTP
- ODBC
- Radius
- SAP
- SMS
- Streaming media
- TCP
- WAP
- X_SLAM (CiscoWorks Integration)

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.

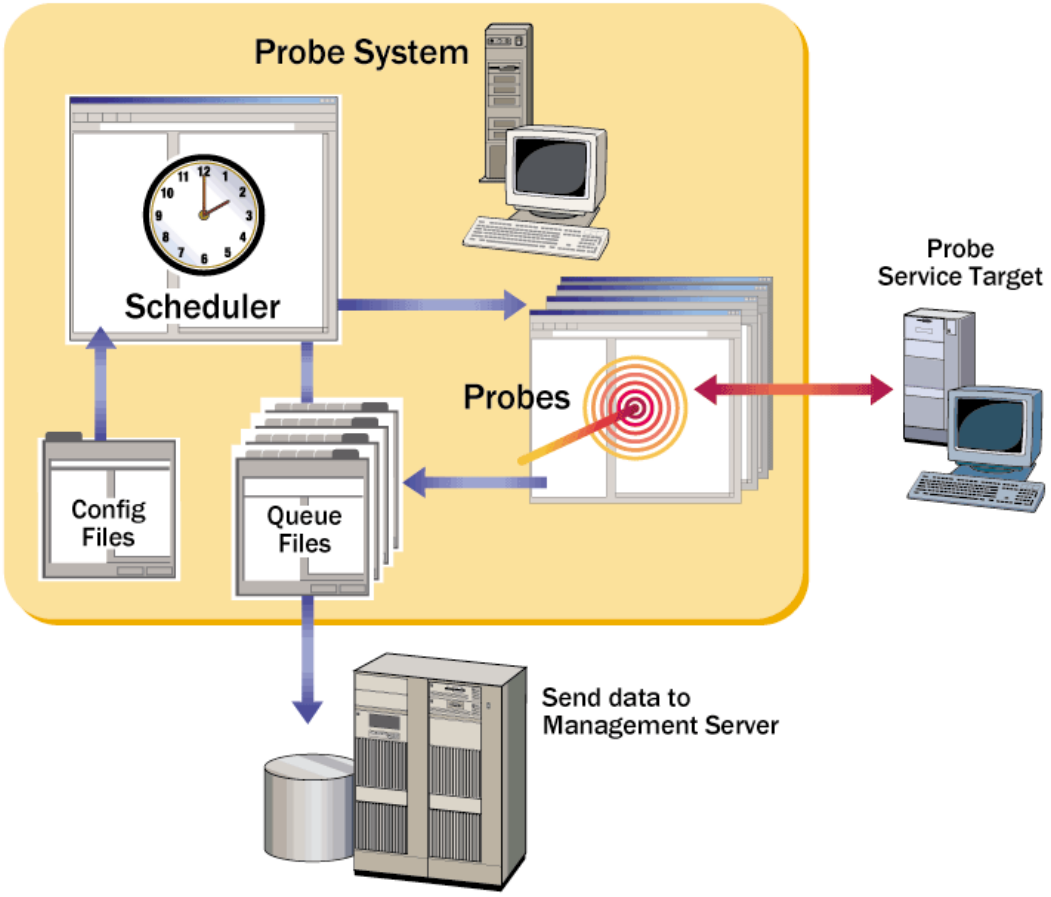


Figure 5 Data Diagram for the Probe Systems

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).

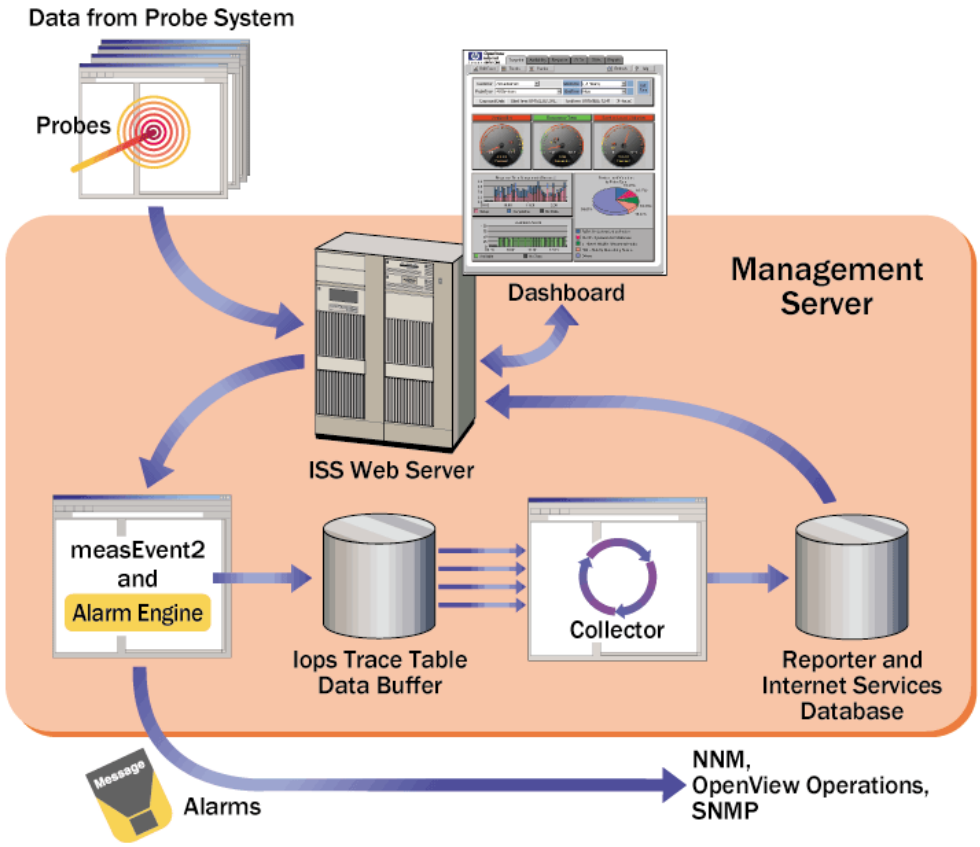
Periodically the collector component runs and does two things. It copies detail data from the IopsTraceTable into the Reporter database. And it aggregates IopsTraceTable data into service groups (based on the way you configured the services) and stores the data in the Reporter database. The data tables 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 6 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.

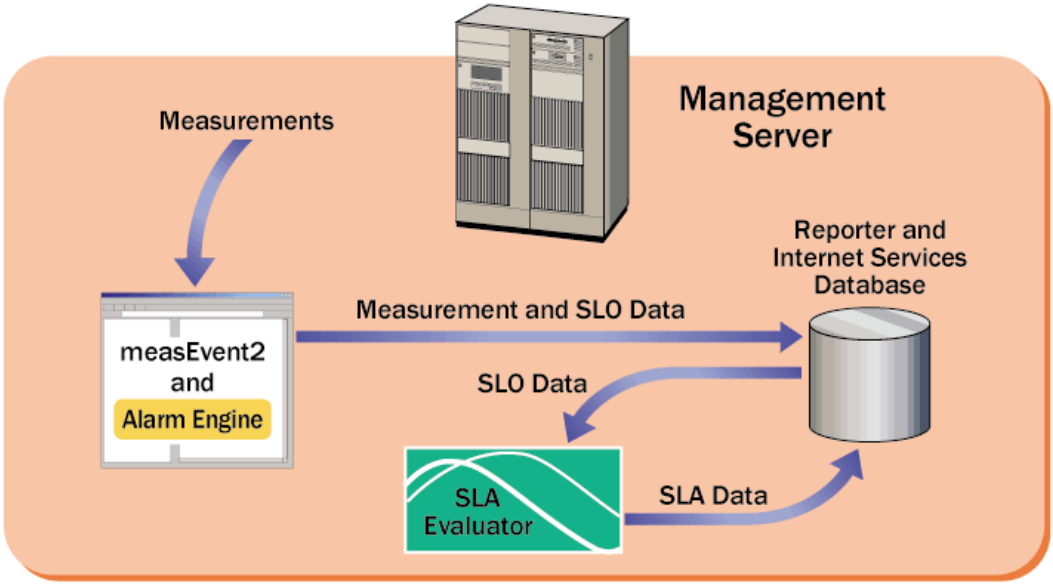


Figure 7 Data Diagram for Service Level Agreements

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 Windows probes) or stop the Scheduler (for 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.

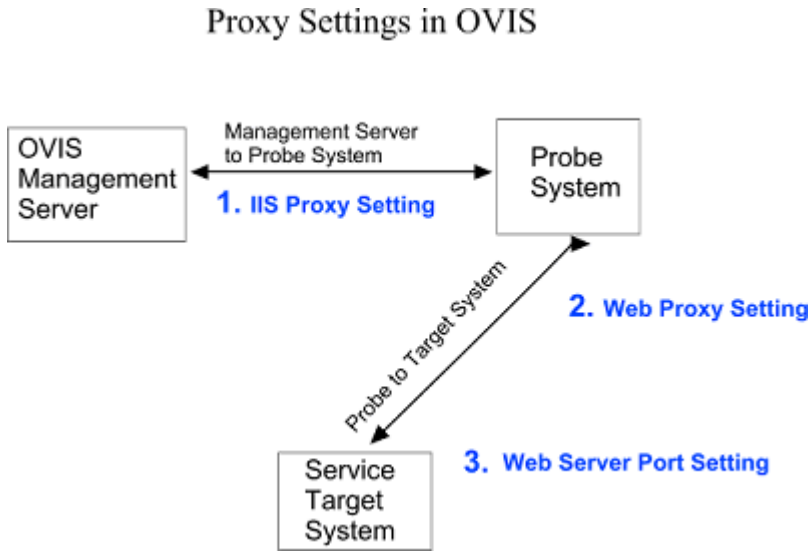
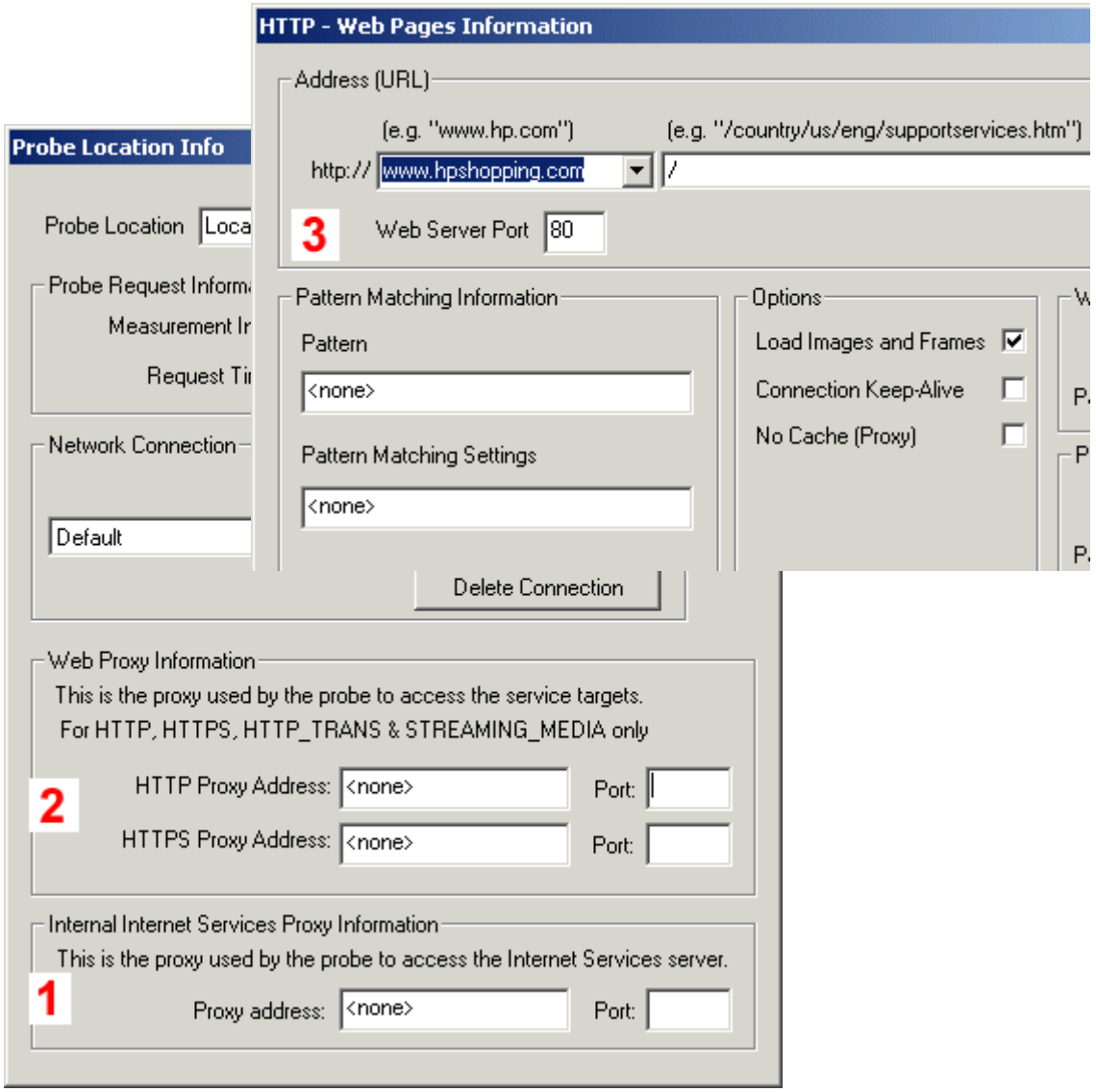


Figure 8 Proxy and Port Settings in Internet Services

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.

3 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.



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 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.

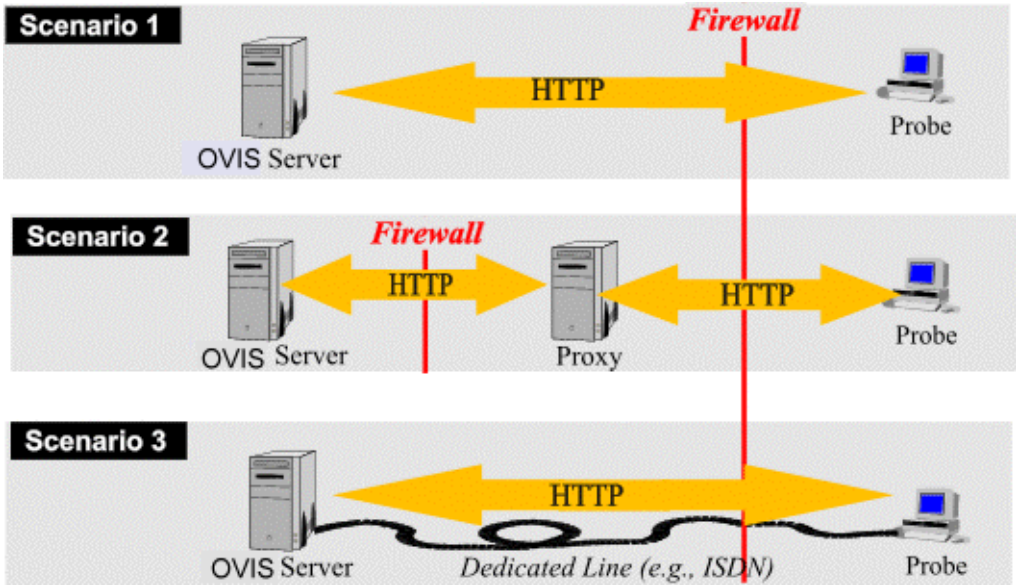
Firewalls: Returning Data Through the Firewall

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 >= 1024) to the Internet Services server.

Configuring Communications Between Probe Systems and the Server

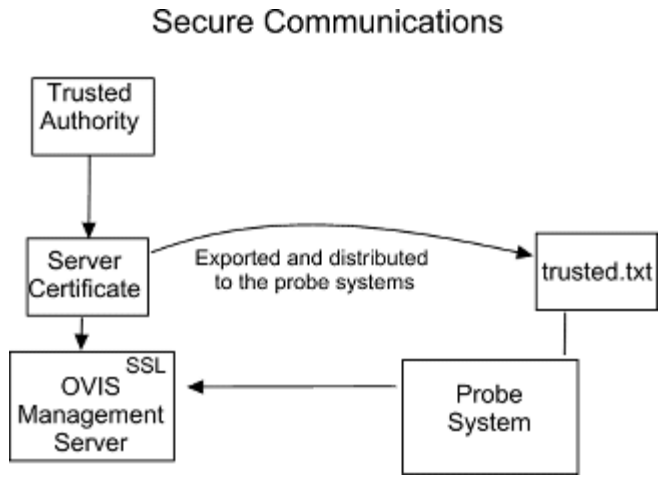
Data communication is required between the OVIS management server and the remote probe systems. See Internet Services Architecture and Data Flow for details on the data flow.

You can use the OVIS Configuration Manager, **File > Configure > Web Server Properties** dialog to set up data communications. You can specify the fully qualified hostname for the OVIS management server and define a timeout period for data transfer. You can specify the port number for the web server that displays the OVIS Dashboard and the port number for the OVIS management server.

You can also configure SSL secured communication between probe systems and the OVIS management server. This affects all the remote probes.

Configuring Secure Communication

Internet Services supports SSL secure communication between the probe system and the server. Basic secure communications only requires the server certificate to be exported into a trusted.txt file on the probe system. To further enhance security, a client certificate for the probe system can be installed.



Server Certificates

Follow the procedure below to export a server certificate. The certificate format for the trusted.txt file must be **Base64 encoded X.509**.

Once you have set up a secure server, ALL probe locations will have to use secure communication.

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. Set up the OVIS Management Server as a secure web server (see IIS product online help). To enable secure communication, create a server certificate for the IIS server on the OVIS Management Server system.
   a. Run Internet Service Manager (IIS) program. In the left tree pane right-click the Default Web Site and select Properties.
   b. Select the Directory Security tab and click the **Server Certificate** button.
   c. Follow the wizard to create a key or certificate. Forward the certificate request to your certificate authority. It may take several days to receive the certificate from the trusted authority.
   d. Once received from the trusted authority, process (or import) the certificate using the same wizard described above, except you select Process Certificate.
3. Once the certificate is processed you can set up the secure communications for two OVIS dlls as follows:
   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.dll` and select **Properties**.
   c. Go to File Security and click on the **Edit...** button under the Secure Communications group box.
   d. Click **Require Secure Channel when accessing this resource**. Press **OK** and exit the Internet Service Manager (IIS).

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

4 Now test secure access to `measEvent2.dll` with a browser.

In order to avoid authentication errors, import the server certificate and its CA certificate into your 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.

5 Export the server certificate and the CA certificate in Base64 encoded X.509 format through Internet Explorer.

- **a** In Internet Explorer on the OVIS 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).

6 In the Internet Services Configuration Manager, **File > Configure > Web Server Properties** dialog check the box to enable SSL Communication. **Save** the configuration change.

7 Distribute the **trusted.txt** file to EACH remote probe location. The other configuration files will be automatically distributed to remote probe systems.

8 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
```

9 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 4b, 4c and 4d 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, **File > Configure > Web Server Properties** dialog enter the certificate file name and location and set the password that is used to protect the **`clientcert`** file. **Save** the configuration change. 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 <pfx file> -out <ber file>`).

Custom Reports

If you want to create custom reports for your custom probes, 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. Refer to the *Internet Services Custom Probes API Guide* (CustomProbes.pdf) for more information on creating custom probes.

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.

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

The default database from OVIS 3.5 was MS Access and the default database is now Microsoft SQL Server Desktop Engine (MSDE). You may choose to change to one of the following supported databases:

- Oracle 8.1.7 for Solaris or HP-UX
- Oracle 9i for Solaris or HP-UX
- SQL Server 2000

Note that Oracle 8.0.6 and SQL Server 7 are only supported on an upgrade from an earlier version of OVIS.

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 for the first time	The MSDE default database is installed. You can later use instructions in the *OVIS Reporter Database Configuration Guide* provided with OVIS for configuring an Oracle or SQL Server 2000 database instead.

If you do not have Reporter and are updating from a previous version of Internet Services to this version of OVIS	The upgrade uses the existing database, it could be MS Access, Oracle 8.0.6, 8.1.6/7 or SQL Server 7 or 2000. With Access you can later use instructions in the *OVIS Reporter Database Configuration Guide* provided with OVIS to configure an Oracle 8.1.7 or SQL Server 2000 database instead.
If you do not have Reporter or OVIS on the system but for some reason you have SQL 7 installed but not configured for use with OVIS; and you install OVIS 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 you have OVIS and Reporter on the same system, attempting to migrate Reporter data to the new database may result in problems in OVIS.

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 suportability 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 Osql.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>EXEC sp_addumpdevice 'DISK', 'Reporter_BKUP',
'C:\Program Files\HP
OpenView\Data\Dataases\backup\Reporter_1.bak'
4>BACKUP DATABASE Reporter TO Reporter_BKUP WITH
INIT, STATS
5>EXEC 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\
Databases\backup\Reporter_1.bak' WITH RECOVERY,
REPLACE, STATS
```

```
3>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 Editio**n.
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 <openview>/<openview>.

Where <openview>/<openview> is the username and password for the OVIS Reporter database.

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

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. Windows, 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

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

Calculating the Number of Probes Systems Required

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.

$$\text{1 probe system} = \frac{\frac{NumTargets}{32} \times 20}{300}$$

The following examples show how the requirement for multiple probe systems is calculated.

targets = 3000
parallel = 32
timeout = 20 (seconds)
interval = 600 (seconds)

$$NumSystems = \frac{\frac{3000}{64} \times 20}{600} = 1.56 \Rightarrow 2$$

targets = 3000
parallel = 64
timeout = 20 (seconds)
interval = 600 (seconds)

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.

Actual results will vary depending on the targets being monitored.

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.

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.

Due to compaction of measurements that are older than one day, database growth is linear with "24 times number of service group" records.

OVIS 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.

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 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.

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 custom configuration of 10, 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 5 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 Configuration
\<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\	Edit	Yes	Read (RX)	
inetsrv\asp	Edit			*may not exist

Table 6 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 7 NTFS permissions explicitly for the "SYSTEM" account

Path	Edit/ Replace ACL	Include Sub Directories?	Permissions	Comments
\<Program Files\HP OpenView>	Edit	Yes	Full	

Table 8 Registry Settings

Path	Edit/ Replace ACL	Permissions	Comments
Path = HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\Reporter	Edit	Read (RX)	

Table 8 Registry Settings

Path	Edit/ Replace ACL	Permissions	Comments
Path = HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\IopsTraceTable	Edit	Read (RX)	

The Execute Permissions for Internet Services IIS Virtual Directories for the IUSR are as follows:

Table 9 IIS Permissions for the user IUSR

Path	Execute Permissions
HPOV_IOPS	Scripts only
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)

index

Symbols

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X