HP OpenView Internet Services

User’s Reference Guide

Manufacturing Part Number: J4511-90006

April 2005

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 US trademark of Sun Microsystems, Inc.

Microsoft Windows® (Windows NT®, Windows® 2000, MS-DOS®, Windows Server™ 2003 and Windows® XP) is a US registered trademark of Microsoft Corporation.

Oracle®, and Oracle7™, are registered US trademarks of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of The Open Group.
Linux is a US registered trademark of Linus Torvalds

Adobe® and Acrobat® are trademarks of Adobe Systems Inc.

open-source Notices

Additional open-source licenses can be found under `<install dir>\license-agreements`.

Support

Please visit the HP OpenView web site at:

http://www.managementsoftware.hp.com/

This web site provides contact information and details about the products, services, and support that HP OpenView offers.

You can also go directly to the support web site at:

http://support.openview.hp.com/

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valuable support customer, you can benefit by being able to:

- Search for knowledge documents of interest
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and log in. Many also require a support contract.

To find more information about access levels, go to the following URL:

http://support.openview.hp.com/access_level.jsp

To register for an HP Passport ID, go to:

https://passport.hp.com/hpp2/newuser.do

contents

1

Introducing Internet Services

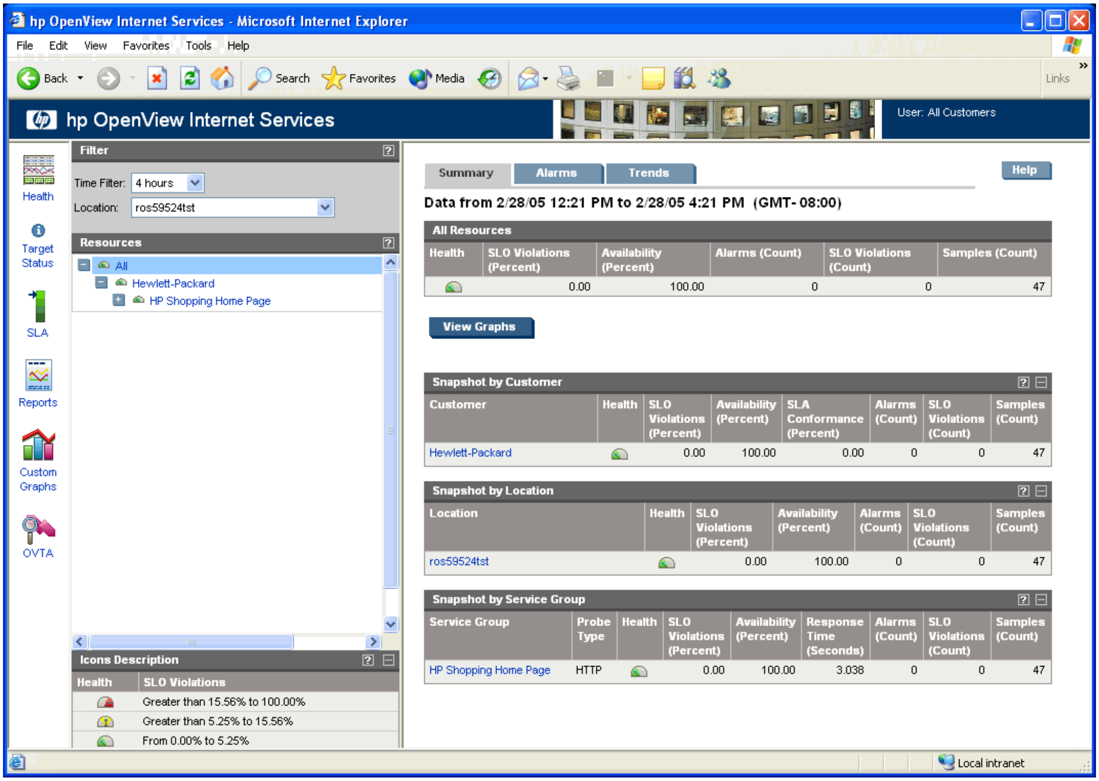
HP OpenView Internet Services (OVIS) provides a single integrated view of your IT and business services. It is designed to help IT staff efficiently predict, isolate, diagnose and troubleshoot problems, anticipate capacity shortfalls, and manage and report on service level agreements.

Services supported by the traditional client-server application architecture are also beginning to require much more proactive management for meeting service level agreements. Poor availability or performance of these services can dramatically affect a business. So IT departments need to provide business owners with clear service level guarantees on the availability and responsiveness of these services, along with notifications and resolutions of outages and slowdowns. When things go wrong, OVIS can be used by IT and network operations staff to isolate and solve problems quickly and communicate with impacted customers and end users in a timely manner.

OVIS 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 view information about service levels, launch the Internet Services Dashboard. The Dashboard is a collection of graphs, snapshot and detail metrics, and trend data you can view from a web browser.

OVIS 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 IT and business services are performing efficiently.

The Internet Services Dashboard is displayed below.


hp OpenView Internet Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Links
hp OpenView Internet Services
Health
Target Status
SLA
Reports
Custom Graphs
OVTA
Summary
Alarms
Trends
Help
View Graphs
Local intranet

User: All Customers

Filter

Time Filter: 4 hours

Location: ros59524tst

Resources

- All
  - Hewlett-Packard
    - HP Shopping Home Page

Icons Description

Health	SLO Violations
◒	Greater than 15.56% to 100.00%
◒	Greater than 5.25% to 15.56%
◒	From 0.00% to 5.25%

Data from 2/28/05 12:21 PM to 2/28/05 4:21 PM (GMT-08:00)

All Resources

Health	SLO Violations (Percent)	Availability (Percent)	Alarms (Count)	SLO Violations (Count)	Samples (Count)
◒	0.00	100.00	0	0	47

Snapshot by Customer

Customer	Health	SLO Violations (Percent)	Availability (Percent)	SLA Conformance (Percent)	Alarms (Count)	SLO Violations (Count)	Samples (Count)
Hewlett-Packard	◒	0.00	100.00	0.00	0	0	47

Snapshot by Location

Location	Health	SLO Violations (Percent)	Availability (Percent)	Alarms (Count)	SLO Violations (Count)	Samples (Count)
ros59524tst	◒	0.00	100.00	0	0	47

Snapshot by Service Group

Service Group	Probe Type	Health	SLO Violations (Percent)	Availability (Percent)	Response Time (Seconds)	Alarms (Count)	SLO Violations (Count)	Samples (Count)
HP Shopping Home Page	HTTP	◒	0.00	100.00	3.038	0	0	47

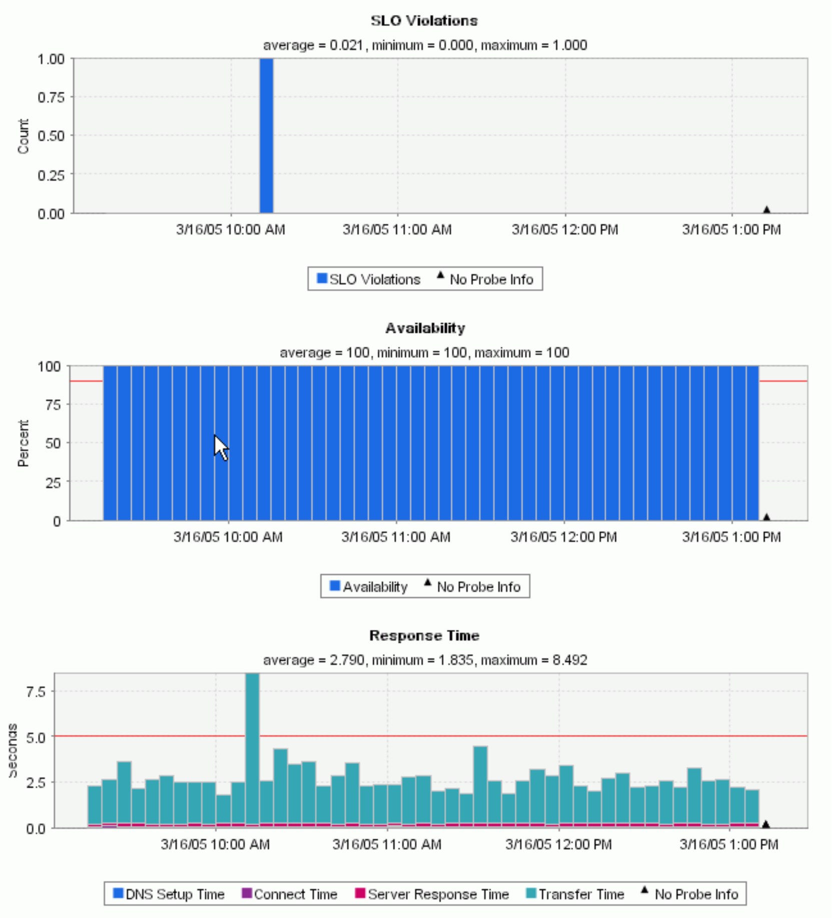
The Dashboard gives you the following:

- High level view of service health.
- Access to additional functions like SLAs, nightly reports and a custom graph builder.
- Summary of the health for All resources, by customer, service group, probe location and targets.
- Time series data in table and graphical form of key measurements like availability and response time.
- List of alarms generated.

- Trend and baseline graphs.
- Access to diagnostic tools and commands (Troubleshooting Insight Packages TIPs) you can run to analyze problems (select a target in the tree view to access the TIPs link or select the Alarms tab to access a TIP for an alarm).

See View the Data using the Dashboard on page 55 for details on the Dashboard.

From the Dashboard you can view time series graphs for a particular target showing SLO violations, availability, response time and other probe specific metrics. Note that you can see the Service Level Objective as a red horozontal line on the graph. If you hover the mouse over a bar on the graph you see a pop-up box with the metric value and the time interval.



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 monitors services and protocols (called **Service Types**) such as HTTP, FTP, DNS, E-mail and more. See Chapter 4, Descriptions of Service Types/Probes for a complete description of all the services monitored.

You use the Internet Services **Configuration Manager** to create/configure **probes** that simulate the use of a service, such as accessing a web page on a web server, and measure the performance and availability of the service. Probes are then deployed to Windows or UNIX **probe locations** from which, they probe the service automatically at set intervals.

Measurements from the probes are sent back 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 **Dashboard**, you can look at the current health of all the services you are probing and get more detailed data on availability, response time and service level violations. There are also trend graphs giving you a longer-term view of the data and out-of-the-box **reports** that run nightly and summarize the data. From the Dashboard, you can run diagnostic tools and commands called **Troubleshooting Insight Packages** (**TIPs**) to analyze service problems and alarms.

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

Service **alarms** to alert you when a customer's services are experiencing problems are generated by OVIS based on measurement thresholds you configure. These alarms can be forwarded to Network Node Manager (NNM), OpenView Operations for Windows (OVO/Windows) and OpenView Operations for UNIX (also known as IT Operations or OVO), or any other event manager capable of receiving SNMP traps. These alarms, can also be viewed in the Dashboard.

Data collected by OpenView Transaction Analyzer (OVTA) can be integrated and displayed on the Dashboard. Furthermore, if you define service level objectives and service level agreements for OVTA data, OVIS will forward alarms on this data.

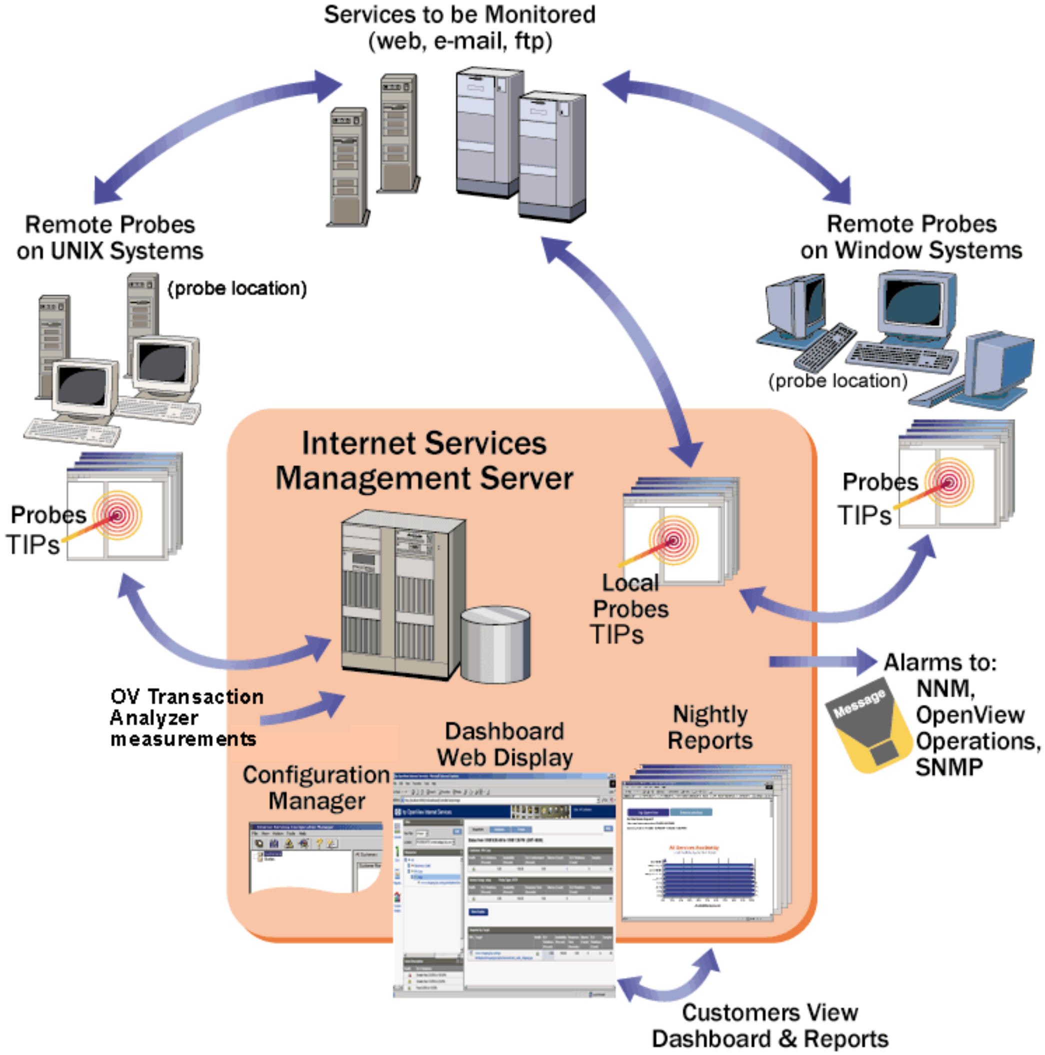


Figure 1 High Level Overview of the Internet Services Components

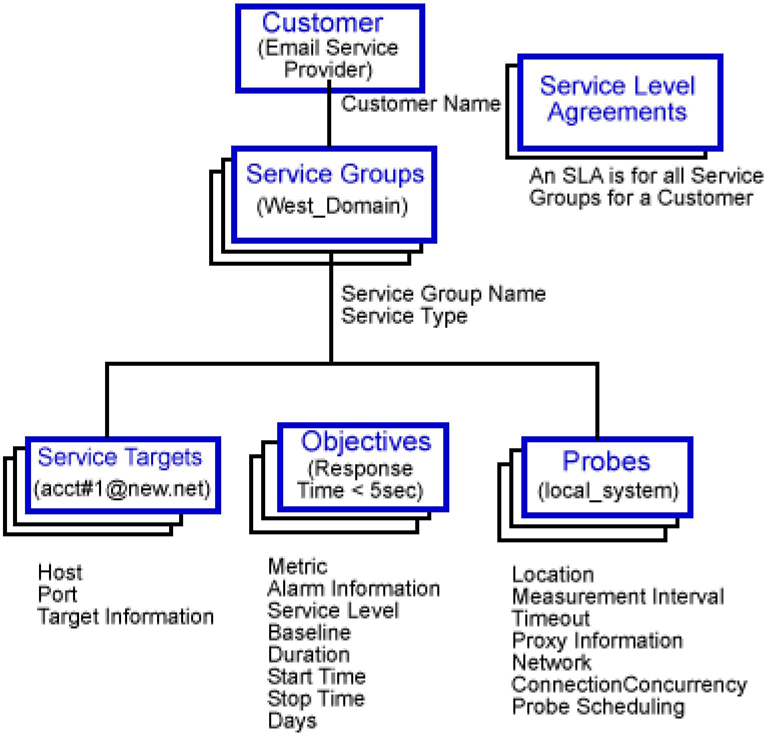
The Services Hierarchy

You use the Internet Services Configuration Manager to configure service targets for each service 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 service type. Below every service group are the three components that allow Internet Services to create probes to measure the service, evaluate the data received from the probes, and consolidate/group the data in order to 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 (service level objective or SLO).
- **Probe location**: where the probe is deployed. The probe may be run on the local OVIS Management Server system or deployed to remote Windows and UNIX systems. Deploying to remote systems allows you to gather measurement data from different locations within your enterprise.

Figure 2 Service Hierarchy



Implementation Sequence

The steps to using Internet Services are as follows

1 Install the OVIS software from the OVIS CD.

2 Use the Internet Services Configuration Manager to create probes by configuring customers, service groups, service targets to be probed, service level objectives (SLOs) and service level agreement (SLA) conformance levels.

3 Use the Internet Services Configuration Manager to define probe locations. You can configure probes to monitor from the local OVIS Management Server system or you can configure probes to run from remote Windows or UNIX systems.

4 Install remote probe software from the OVIS CD onto remote systems where you plan to run the probes. The probe configuration files can then be deployed to remote systems and the probes can begin collecting data.

5 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.

6 On the Management Server, data received from probes is consolidated for viewing in the OVIS Dashboard. Analyze the data displayed to verify that the probes are collecting the data you need. Note that Service Level Agreement, Availability and Response Time reports are generated nightly.

7 If desired, install integration components from the OVIS CD, for integrating OVIS with OpenView Operations for UNIX (OVO), OpenView Operations for Windows (OVO/Windows), and Network Node Manager (NNM). Follow the steps in Chapter 5, Integrating with OpenView Products to set up the integration with these other OpenView products.

8 If desired, configure alarm events to be sent to NNM, OVO, OVO/Windows or a generic SNMP management station.

Chapter 2, Getting Started with Internet Services, Chapter 3, Configuring Internet Services and Chapter 4, Descriptions of Service Types/Probes provide you with information for configuring probes to monitor various services. These chapters show how to organize the services, create probes, set up service level objectives, service level agreements and alarms. In addition, 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 the following products:

- OpenView Transaction Analyzer
- OpenView Operations for UNIX
- OpenView Operations for Windows
- Network Node Manager (or any event manager capable of receiving SNMP traps)

Internet Services also includes embedded components from OpenView Reporter and OpenView Performance Manager (OVPM) that provide basic reporting and custom graphing functions. The full version of Reporter or OVPM can be installed on the same system as OVIS providing you additional functionality as described below.

Reporter: 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, will then be 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 or system itself. In addition, having Reporter allows you to create custom reports for Internet Services and modify workshift definitions through the Reporter GUI. 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.

OVPM: 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. The newer OVPM versions can display system performance data plus OVIS data directly.

Note that for older versions of OVPM (PerfView), you can still get this view of OVIS data and system performance data, using OpenView Performance Agent (OVPA) and Application Response Measurement (ARM), see the section below.

OVPA and ARM: ARM is an industry-standard technology for measuring the response time of critical transactions within an application. OVPA, formerly known as MeasureWare Agent supports the ARM 2.0 standard and collects performance metrics for ARM instrumented applications. OVIS has ARM-instrumented all its probes so that if OVPA is installed on the same system as OVIS this transaction data is automatically logged. The OVIS ARM data collected via OVPA can be used in traditional OVPA facilities such as extract, can be exported to other tools such as SAS and be viewed through PerfView. This OVIS data can then be viewed right alongside system performance data.

The following chart shows the OVPA metrics with descriptions as they relate to OVIS.

OVPA Metric	Description as relates to OVIS
TT_APP_NAME	OVIS customer name.
TT_NAME	OVIS service group name.
TT_WALL_TIME_PER_TRAN	This is the response time for the probe. Instead of using the arm_start and arm_stop calls, OVIS uses the arm_complete_transaction call. This allows OVIS to feed a pre-calculated response time to OVPA for this metric, rather than have OVPA calculate it using the start and stop. As a result the TT_WALL_TIME_PER_TRAN is the same as the response time data in OVIS.
TT_SLO_COUNT	This is the number of probe response times that exceeded the defined SLO. It is important to remember that the SLO for ARM transaction data is defined in OVPA, and has nothing to do with the SLO/SLA information configured in OVIS.
TT_USER_MEASUREMENT_*	Availability.
TT_USER_MEASUREMENT_*_2	Setup Time.
TT_USER_MEASUREMENT_*_3	Transfer Throughput.
TT_USER_MEASUREMENT_*_4	OVIS probe metric 1.
TT_USER_MEASUREMENT_*_5	OVIS probe metric 2.
TT_USER_MEASUREMENT_*_6	OVIS probe metric 3.

See the *OVPA Metrics Dictionary* and the *OVPA Tracking Your Transactions Guide* for more information on these metrics.

If the ARM library is not found, OVIS uses a NO-OP library, which causes the arm_* calls to return immediately without error and taking no action.

By default this ARM transaction data is collected. The overhead associated with the data collection is on average extremely low. You can refer to an OVIS White Paper on ARM integration for more information.

Service Desk: Internet Services can be integrated with OpenView Service Desk to do the following:

- Provide current service status information with incident and problem management.
- Synchronize service hierarchy information between business service management (Service Desk) and operational service management (Internet Services).
- Report on services in the context of SLAs agreed upon with the customer.
- Launch the Dashboard from a service call by invoking a smart action.

See the *Service Desk Administrator's Guide* for details on how to configure this integration.

Systems Insight Manager: Internet Services can be integrated with HP Systems Insight Manager (SIM) using the SNMP `ovis.mib` in the OVIS `<install dir>\contrib` directory.

OpenView Business Process Insight (OVBPI): OVIS 6.0 integrates with OVBPI 1.1.

Documentation

OVIS documentation is available on the CD or installed in `<install dir>\help\iops\c\` directory. The documents include:

- OVIS User's Reference Guide (`IS_User_Ref_Guide.pdf`)
- OVIS Web Transaction Recorder Guide (`webrecorder.pdf`)
- OVIS SQL Server and Oracle Database Configuration Guide (`Reporter_Database_Config.pdf`)
- OVIS Custom Probes API Guide (`CustomProbes.pdf`)
- OVIS Release Notes (`IOpsReleaseNotes.pdf`)
- What's New - OVIS Dashboard (`OVIS 60-dashboard.pdf`)
- What's New - OVIS Troubleshooting Insight Packages (TIPs) (`ovis60-tips.pdf`)
- hp OpenView Tracing Concepts Guide (`ov_tracing.pdf`)
- hp OpenView AutoPass Licensing Guide (`AutoPass-guide.pdf`)

This documentation is also available online at this URL:

`http://ovweb.external.hp.com/lpe/doc_serv/.`

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 examples to become familiar with configuring probes, monitoring probe status and using the Dashboard to view performance data. After completing all steps in the examples, you should find it easy to configure your own service targets and analyze performance data.

Installing and configuring Internet Services begins with the following tasks:

- Installation Considerations
- Installation Prerequisites
- Installing Internet Services
- Quick Start for Configuring Internet Services

  Check the Status of Probe Data Collection
- View the Data using the Dashboard

  Quick Start to Using the Dashboard
- More Details on the Dashboard
- 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 *OVIS 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

Minimum Hardware Requirements

Please see the Scalability Information on page 478 for more information on system sizing.

Windows Management Server

- Intel Pentium IV, 2 GHz or faster processor with 1 GB of memory or more are recommended.
- 600 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.
- The recommended minimum display resolution is 1024 x 768.

Windows Probe System

- Intel Pentium IV, 1 GHz or faster processor with 512 MB of memory or more are recommended. These requirements vary depending on the number and type of probes that run in parallel. For most efficient execution and metric accuracy, it is recommended that the system be dedicated to probing.
- 100 MB of disk space for probes and configuration files, plus an additional 10- 100 MB of disk space to hold probe data in temporary 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

- 512 MB of memory or more is recommended.
- 100 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 4 (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 XP Professional with minimum of Service Pack 1.

  Microsoft IIS 5.1 Web Server.

  OR

- Microsoft Windows Server 2003 Standard and Enterprise editions.

  Microsoft IIS 6.0 Web Server.

The OVIS Management Server has these additional software requirements:

- Systems with Windows 2000 or Windows XP also require Microsoft Windows Script 5.6. You can download this from the Microsoft Download Center at www.microsoft.com/downloads.
- Internet Explorer 6.0 with the latest Security Update and Service Pack.
- 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. You do this in IIS configuration Web Site tab in the IP Address field by either selecting this IP address to be assigned to the port shown or by selecting [All Unassigned] in the IP Address field to indicate that all unassigned IP addresses should be assigned to the port shown.
- 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 as long as the hostname stays the same).
- 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 (version 8 or higher) or Real Player (version Real8 basic 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 Web Transaction Recorder (HTTP_TRANS) probe 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 Transaction 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 default Locale setting must be used for the OVIS server, OVIS/Reporter database and 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. At this time, OVIS does not support databases that have been configured to use the UTF-8 character set.

See the OVIS Release Notes for requirements for integration with other OpenView products.

‼ Installing OVIS and a clustered OVO for Windows server (7.5 or higher) on the same system is not supported. Also integration between OVIS and a clustered OVO for Windows implementation is not supported.

‼ 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 2000 with Service Pack 4; or Microsoft Windows XP Professional with Service Pack 1; or Microsoft Windows Server 2003 Standard and Enterprise editions.
- Internet Explorer 6.0 with the latest Security Update and Service Pack.
- 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 (Real8 Basic or RealOne) for Windows or Windows Media Player (version 8 or higher) is required. The Windows Media Player is installed automatically for you with the probe. If you want to use Real Player instead, you can download a free version from www.real.com.

➤ DHCP is supported on remote probe systems as long as the hostname stays the same.

UNIX Probe System

- HP-UX 11.0, 11.11, 11.22 and 11.23 (runs on Itanium in PA-RISC emulation mode)
- Sun Solaris 2.8 (requires patch 110934), Sun Solaris 9
- Linux Red Hat 8.0, 9.0, ES 2.1, ES 3.0, note that Red Hat Linux requires compat-libstdc++7.3-2.96 or higher
- SUSE Linux Enterprise Server 8 & Professional 8.1 (32 bit)

➤ See the OVIS release notes for important information on other required patches for UNIX systems.

Probes Not Available on UNIX Systems

- Streaming Media probe
- SMS probe
- ODBC probe
- Exchange probe
- SYS_BASIC_WMI probe
- 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
- The Dial probe is on all supported versions of UNIX except SuSE Linux

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

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 is required: ppp-2.3.11-7

Browser Requirements for Viewing the Dashboard

The OVIS Dashboard can be viewed from the OVIS management server or any other system with a browser. You must have a web browser to view the Dashboard and reports. Internet Explorer 6.0 with the latest Security Update and Service Pack, and Mozilla 1.7.2 (HPUX Mozilla is version 1.6) are supported.

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 examples below of how to set this:

> In IE 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**.

If you log into the Dashboard when Restricted Views is enabled in OVIS, you will be prompted to enter a user ID and password before viewing the main Dashboard display (see Dashboard Login using Restricted Views on page 131).

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`.

⚠ Installing OVIS on a clustered OVO for Windows server (7.5 or higher) is not supported.

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.

A number of ports are used by OVIS. During installation, the following default ports are used in the Tomcat Servlet Container Configuration:

— 8080 (HTTP - OVIS Dashboard)

— 8009 (JK2 - AJP communication via Apache)

— 8005 (Shutdown)

If any of these ports are not available, the installation program will prompt you to select a different port. You can run `netstat -an` to see what ports are in use. In addition, you may change these and other ports used by OVIS later, after installation (see Configuring and Changing Ports in OVIS on page 445).

Probe Considerations

Once you install OVIS, you use the Configuration Manager to create probes for the services you want to monitor. See Quick Start for Configuring Internet Services on page 43 for an example of probe configuration.

Then the probes can either be run on the local OVIS management server system or they can be deployed to run on remote Windows or UNIX systems. See Installing and Removing Remote Probe Software on page 159 for the steps to install the remote probe software from the OVIS CD and deploy probe configuration files to remote systems.

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 license extension (see If you need to Obtain an Extension Trial License on page 41) or a permanent license key password.

Selecting the OVIS License Wizard

When you first open the OVIS Configuration Manager you will see the OVIS Configure License dialog which displays information on the current license status. You'll see the licensed capacity for Standard OVIS targets and the licensed capacity for Custom targets (configured targets from user-built probes using the custom probe SDK or the Probe Builder) . The dialog box also has a button to start the License Wizard, which runs the HP AutoPass licensing program and allows you to request a permanent license key.

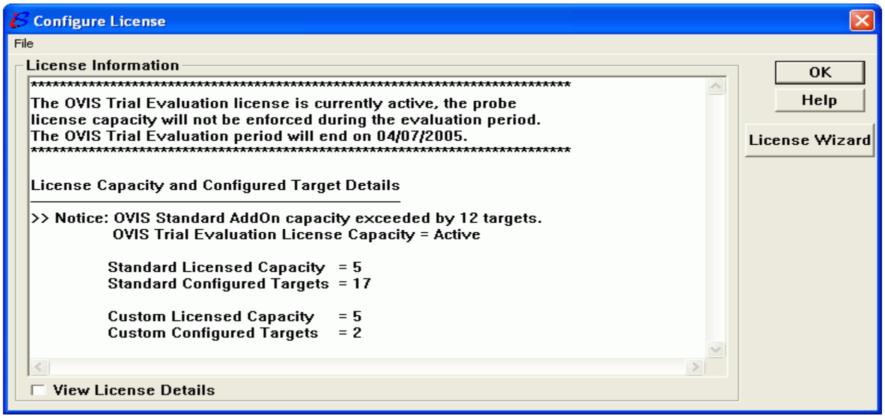
Licenses for Standard configured targets and Custom configured targets are tracked separately.

The text in this dialog may also contain warning messages notifying you if your configured targets exceed licensed capacity for either Standard targets or Custom targets.

⚠ Once your trial license expires, if the Standard Licensed Capacity is exceeded or the Custom Licensed Capacity is exceeded, data will not be gathered for the targets that are over the licensed capacity limit.

➤ OVIS 6.0 license enforcement was updated, preventing OVIS Standard Capacity licenses from being used for Custom targets. Upgrade customers that do not have the correct number of Custom Licensed Capacity should contact their HP Sales Representative.

At installation you are given a 60-day trial license. Within this 60-day period, you must obtain a trial extension or a permanent license key password to continue to gather data for OVIS targets not appropriately licensed beyond the 60 day period.



```
*****************************************************************************
The OVIS Trial Evaluation license is currently active, the probe
license capacity will not be enforced during the evaluation period.
The OVIS Trial Evaluation period will end on 04/07/2005.
*****************************************************************************

License Capacity and Configured Target Details

>> Notice: OVIS Standard AddOn capacity exceeded by 12 targets.
           OVIS Trial Evaluation License Capacity = Active

          Standard Licensed Capacity   = 5
          Standard Configured Targets  = 17

          Custom Licensed Capacity     = 5
          Custom Configured Targets    = 2
```

□ View License Details

To obtain your license key password for products purchased, select the **License Wizard** button on the Configure License dialog 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 License dialog 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.

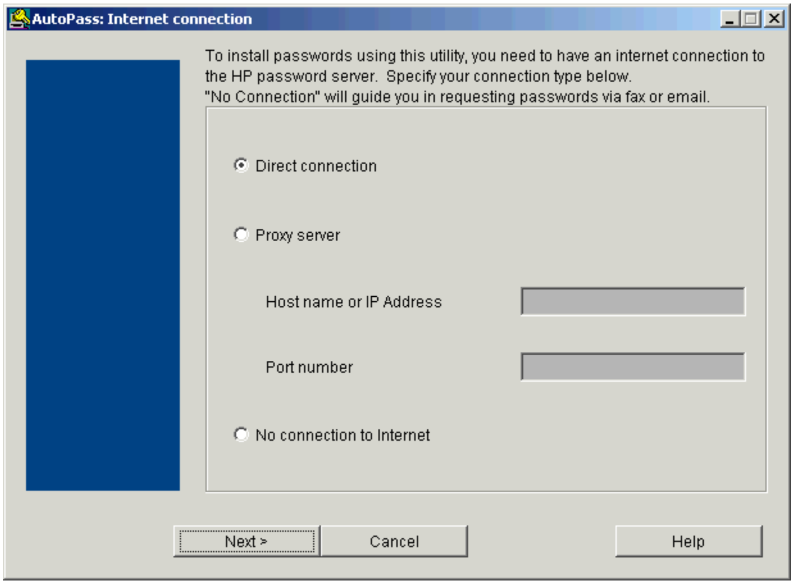
After selecting the **License Wizard** button, follow the instructions in the **HP AutoPass** program to obtain and install permanent license keys.

See If you need to Obtain an Extension Trial License on page 41 if you are requesting a trial (evaluation) license extension, since this cannot be done via the OVIS License Wizard.

If you have an Entitlement Certificate and Access to the Internet

If you have purchased the OVIS software, received your entitlement certificate and have access to the Internet from the system where OVIS server is installed, follow these steps to enter your permanent license key password:

1. After selecting the License Wizard in OVIS, the opening dialog of the AutoPass program is displayed, click **OK**.
2. In the next dialog displayed, select either Direct Connection or enter your Proxy information.



AutoPass: Internet connection

To install passwords using this utility, you need to have an internet connection to the HP password server. Specify your connection type below.
"No Connection" will guide you in requesting passwords via fax or email.

● Direct connection

○ Proxy server

Host name or IP Address

Port number

○ No connection to Internet

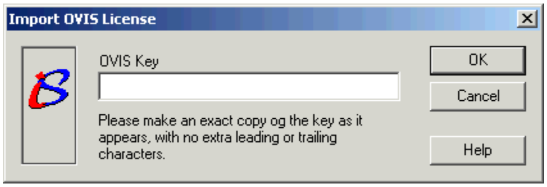
3. In the next dialog displayed, select Install Permanent Password and enter the HP OpenView Purchase Order number from your Entitlement Certificate.
4. Select the LTU (License To Use) products you have purchased.
5. Fill out the customer information form.
6. When finished, your password keys are installed.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

If you have Received a License Key by Email

If instead of the License Wizard, you used the www.webware.hp.com website or phone to request a license key password, and have received it via email, you will need to import it into OVIS as described below. (Note that we recommend that you use the License Wizard to create and install the license key directly.)

To obtain your license keys via e-mail and import them into OVIS, you will need to do the following:

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. Save the file in a location available to the OVIS Management Server.
3. Run the Configuration Manager and select **File > Configure > License**. In the License dialog, select **File > OVIS License > Enter License Directly**. Then copy the license password/key from the file you saved and paste into the OVIS Key field. It is important to not include leading or trailing spaces, quotes or other non-license-key value characters. Select OK and the license is imported into OVIS.



Import OVIS License

OVIS Key

Please make an exact copy og the key as it appears, with no extra leading or trailing characters.

If you need to Obtain an Extension Trial License

If you need to request a **Trial (Evaluation) License Extension**, access the www.webware.hp.com website to get contact information for evaluation software passwords. Contact the License Center in your region (select the Evaluation Extension Licenses link in the website) to request a Trial (Evaluation) License Extension. Note that evaluation extension licenses are grated only once per customer (one 60 day extension) and after that a permanent license must be purchased to continue to use the product. You may contact one of the password centers outside our local area if necessary.

The password center will ask you for the following information:

Software product number. Use TRIAL-OVIS.

IP address or Host name. This is the system where the evaluation software is installed.

Contact information. Company, name, address, phone number, email address.

You'll receive your password keys by email. You'll see two lines in the .txt file, one for Standard targets and one for Custom targets. You install them using the If you have Received a License Key by Email on page 41. You will need to do two copy/paste actions, one for each trial license extension, and after each paste, select OK to import the license. These extension trial licenses will allow a virtually unlimited number of targets.

View License Information

To view specific information regarding installed licenses select the **View License Details** check box in the Configure License dialog. For additional information on the number of probes you have configured by probe location, select **Tools > Probe Info** in the Configuration Manager.

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: http://ovweb.external.hp.com/lpe/doc_serv/.

Quick Start for Configuring 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 probe software is covered in Chapter 3, Configuring Internet Services.

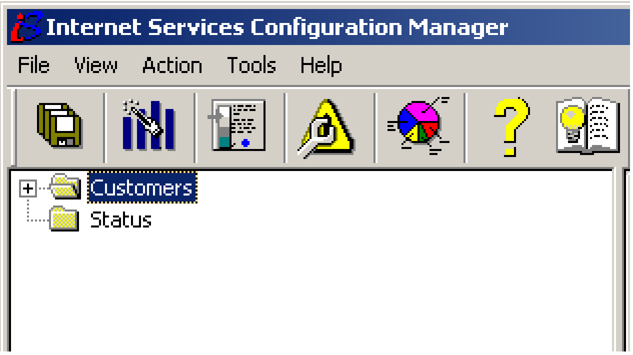
➤ The OVIS documentation set is available from the Help menu and the book icon in the Configuration Manager.

Configure a Service Probe

To configure a probe on the Windows Internet Services Management Server:

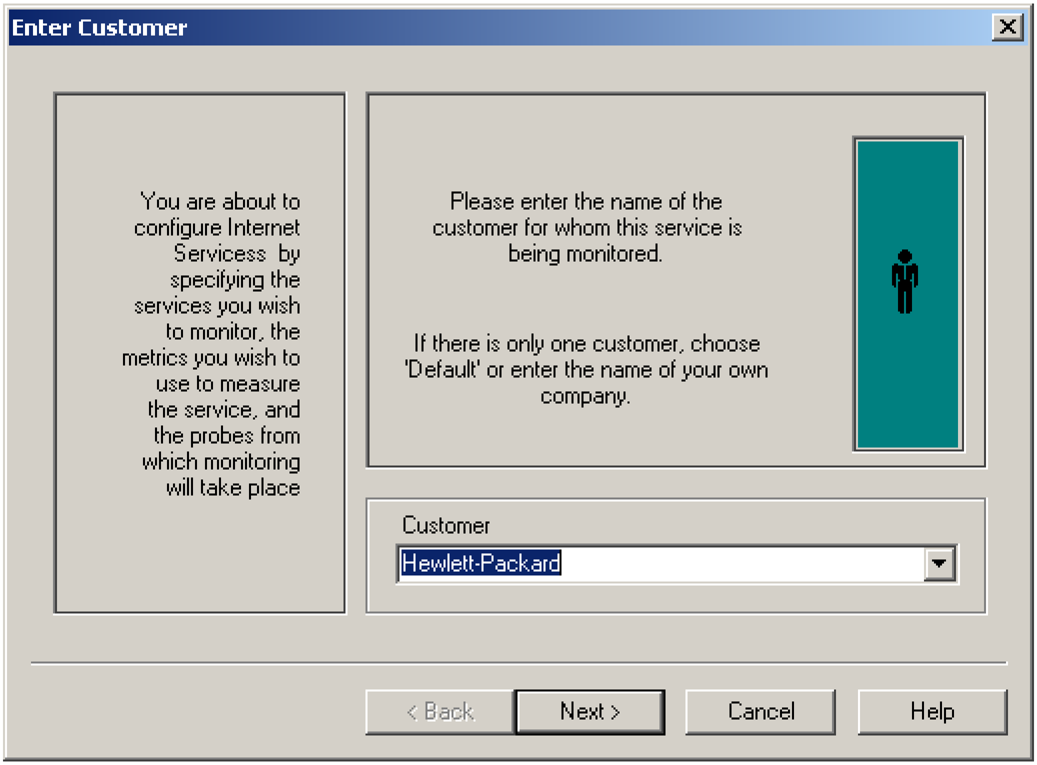
1 Open the Configuration Manager by selecting **Start>Programs>HP OpenView>Internet Services>Configuration Manager**. Multiple User options can be configured to specify whether locking should occur when multiple users are trying to add/update/delete/save the same item (see Other Configuration Options on page 96 for additional requirements for using Multiple User locking).

Use of the OVIS Configuration Manager requires Administrator user.



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**.



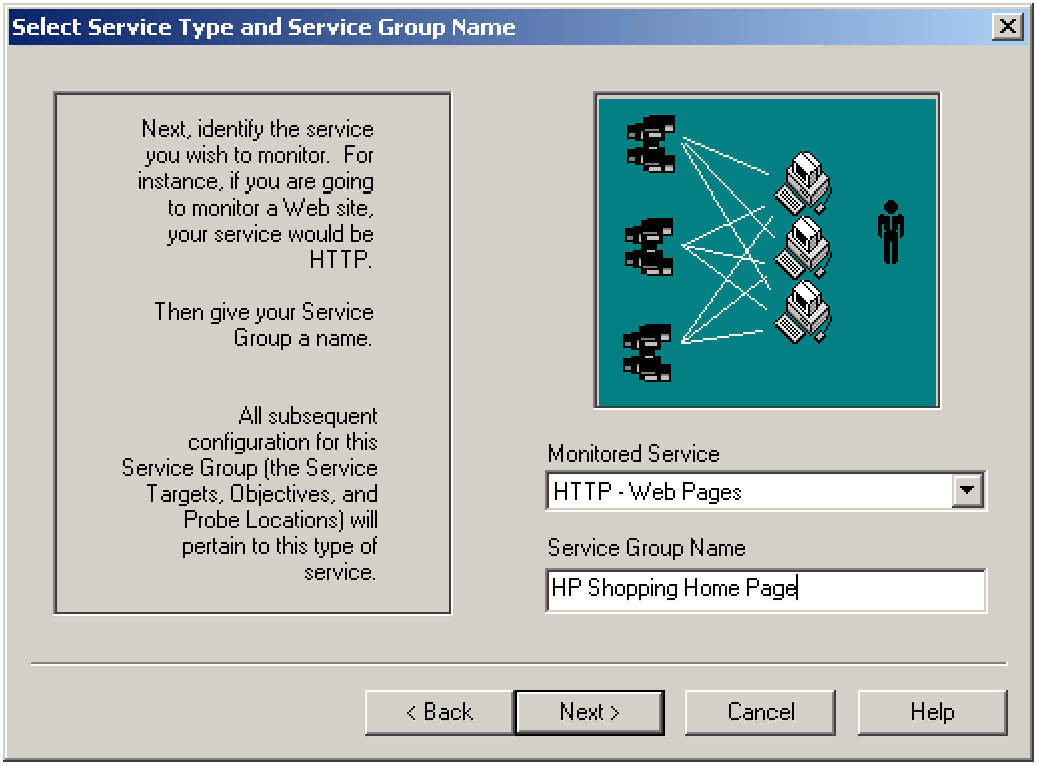
You are about to configure Internet Servicess by specifying the services you wish to monitor, the metrics you wish to use to measure the service, and the probes from which monitoring will take place

Please enter the name of the customer for whom this service is being monitored.

If there is only one customer, choose 'Default' or enter the name of your own company.

Customer: Hewlett-Packard

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



Select Service Type and Service Group Name

Next, identify the service you wish to monitor. For instance, if you are going to monitor a Web site, your service would be HTTP.

Then give your Service Group a name.

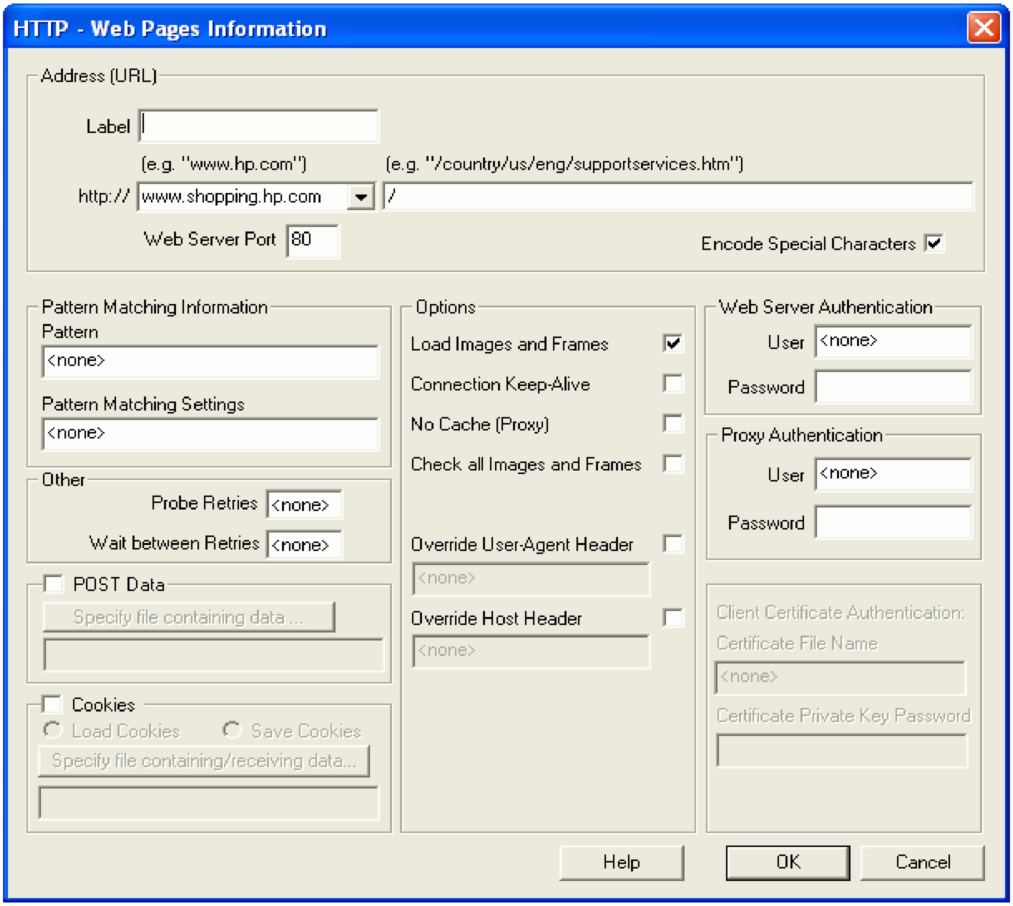
All subsequent configuration for this Service Group (the Service Targets, Objectives, and Probe Locations) will pertain to this type of service.

Monitored Service: HTTP - Web Pages

Service Group Name: HP Shopping Home Page

➤ 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.shopping.hp.com** in the URL Address field as the Service Target you want to monitor. Click **OK** and click **Next**.



HTTP - Web Pages Information

Address (URL)

Label:

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

http:// www.shopping.hp.com /

Web Server Port: 80

Encode Special Characters ☑

Pattern Matching Information

Pattern <none>

Pattern Matching Settings <none>

Other

Probe Retries <none>

Wait between Retries <none>

□ POST Data

□ Cookies

○ Load Cookies ○ Save Cookies

Options

Load Images and Frames ☑

Connection Keep-Alive □

No Cache (Proxy) □

Check all Images and Frames □

Override User-Agent Header □ <none>

Override Host Header □ <none>

Web Server Authentication

User: <none>

Password:

Proxy Authentication

User: <none>

Password:

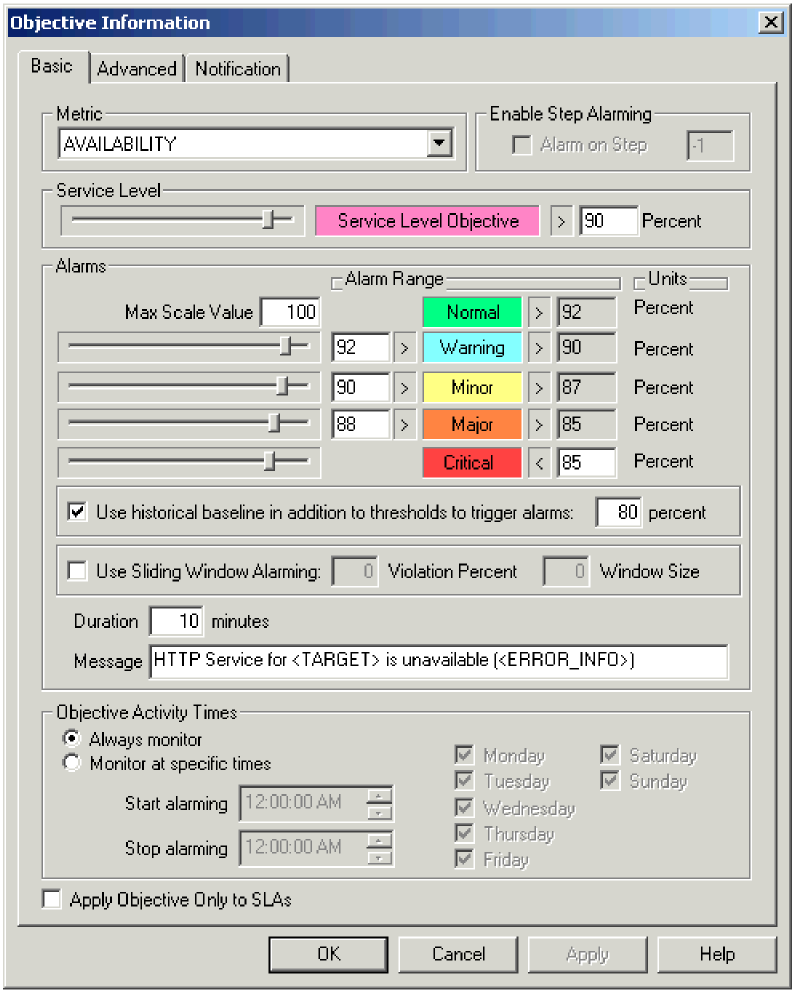
Client Certificate Authentication:

Certificate File Name <none>

Certificate Private Key Password:

Specify file containing data ...
Specify file containing/receiving data...
Help
OK
Cancel

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**.



Metric: AVAILABILITY

Enable Step Alarming: □ Alarm on Step -1

Service Level: Service Level Objective > 90 Percent

Alarms

		Alarm Range			Units
Max Scale Value 100		Normal	>	92	Percent
92	>	Warning	>	90	Percent
90	>	Minor	>	87	Percent
88	>	Major	>	85	Percent
		Critical	<	85	Percent

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

□ Use Sliding Window Alarming: 0 Violation Percent 0 Window Size

Duration 10 minutes

Message HTTP Service for <TARGET> is unavailable (<ERROR_INFO>)

Objective Activity Times

● Always monitor

○ Monitor at specific times

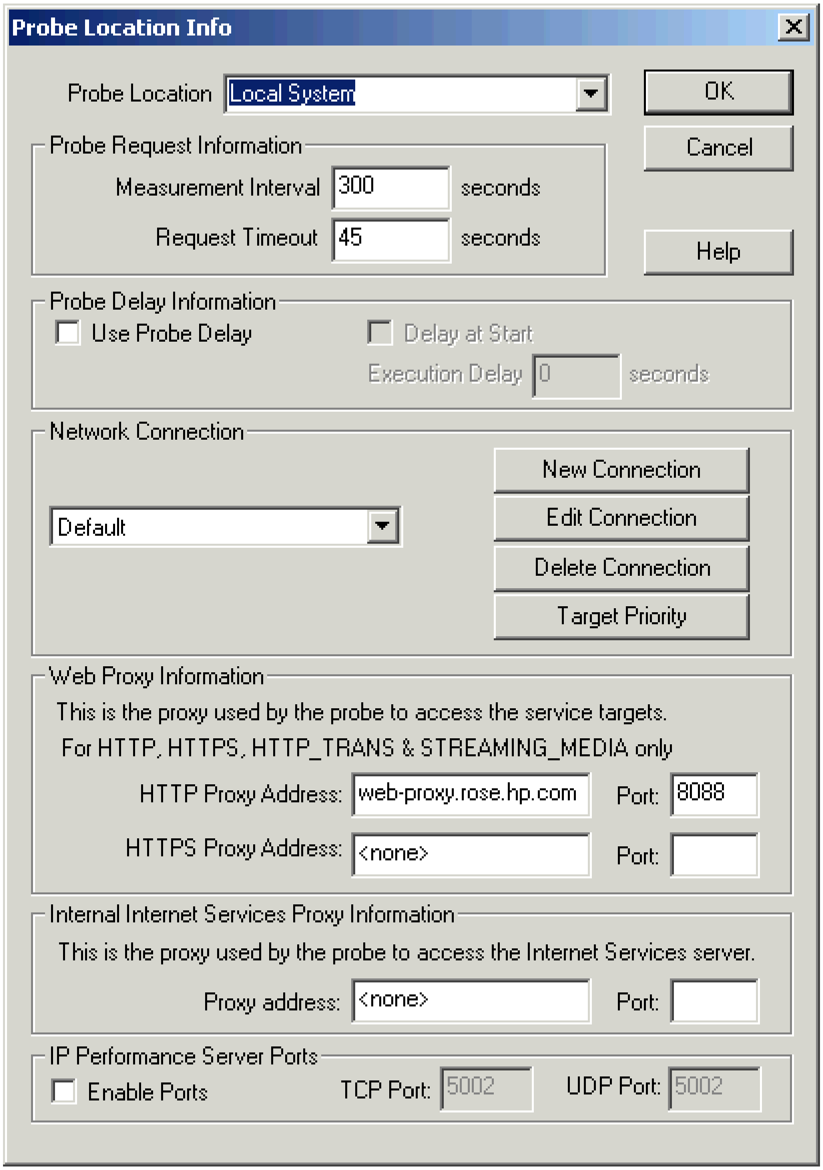
Start alarming 12:00:00 AM

Stop alarming 12:00:00 AM

☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

□ Apply Objective Only to SLAs

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



Probe Location Info

Probe Location: Local System

Probe Request Information

Measurement Interval 300 seconds

Request Timeout 45 seconds

Probe Delay Information

□ Use Probe Delay

□ Delay at Start

Execution Delay 0 seconds

Network Connection

Default

Web Proxy Information

This is the proxy used by the probe to access the service targets.

For HTTP, HTTPS, HTTP_TRANS & STREAMING_MEDIA only

HTTP Proxy Address: web-proxy.rose.hp.com Port: 8088

HTTPS Proxy Address: <none> Port:

Internal Internet Services Proxy Information

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

Proxy address: <none> Port:

IP Performance Server Ports

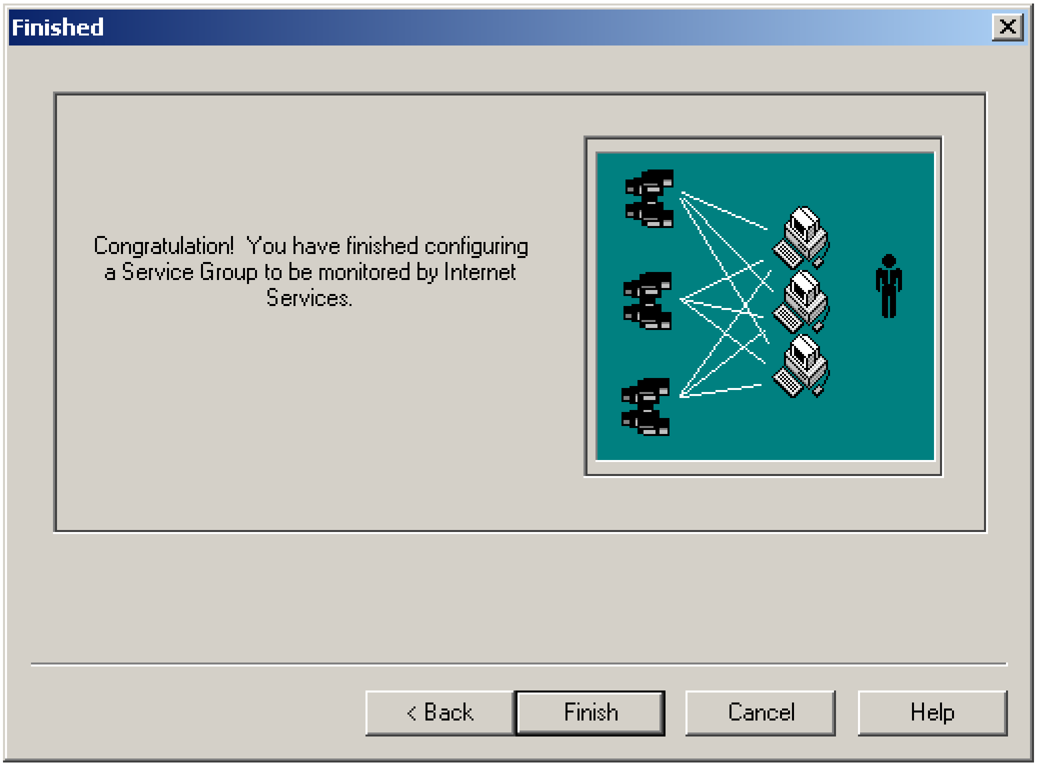
□ Enable Ports TCP Port: 5002 UDP Port: 5002

Accept all of the defaults EXCEPT for Web 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 **Tools > Internet Options > Connections tab > LAN Settings**.

Note that the Probe Location Info 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.



Congratulation! You have finished configuring a Service Group to be monitored by Internet Services.

9 From the Configuration Manager click the **Save Configuration Files** toolbar button or select **File>Save Probe Configuration** 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 prepared for distribution to probe systems.

You can use the Configuration Manager Status window's Remote Probe Update tab to see the distribution status.

10 Take a look at the next few sections to view the configuration information for the probe and to check that the status for the probe is green.

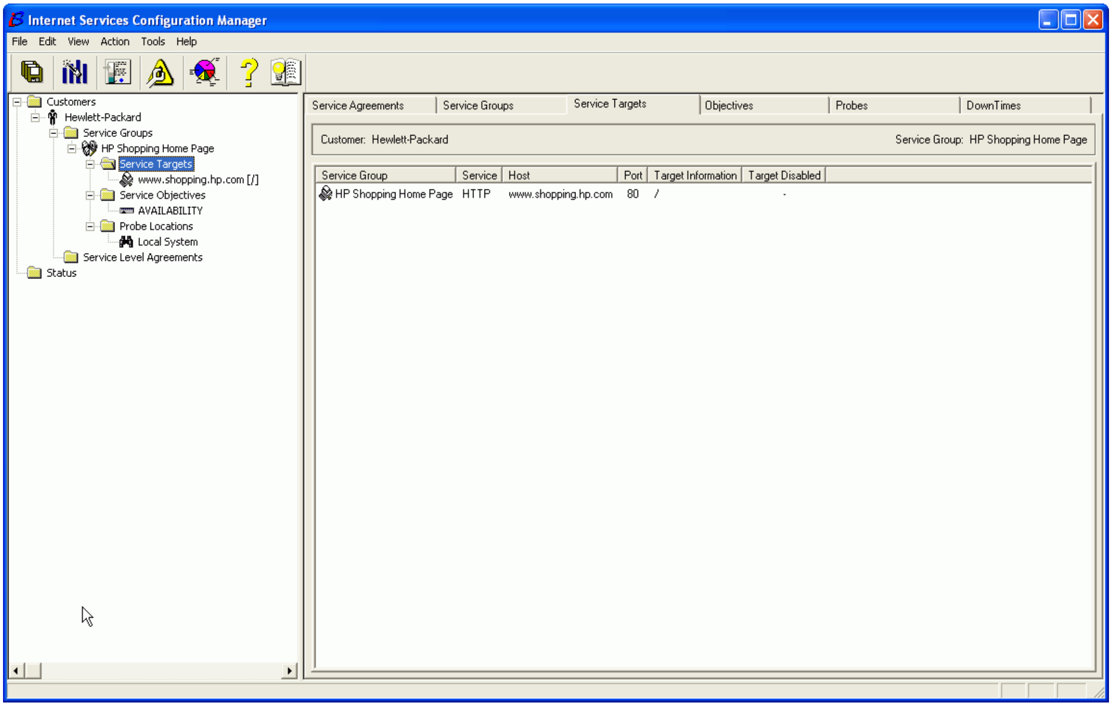
11 Wait a while to give the probe time to collect some data. Then continue on to a Quick Start to Using the Dashboard on page 58 to see how to view the data collected by the probe you configured in this exercise.

View Configuration Information

In the Configuration Manager you can see configuration information for the service target you just created.

Select Customers at the top of the tree in the left pane of the Configuration Manager Main window 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 in the left pane, the **Service Targets** tab is displayed.



Customer: Hewlett-Packard

Service Group: HP Shopping Home Page

Service Group	Service	Host	Port	Target Information	Target Disabled
HP Shopping Home Page	HTTP	www.shopping.hp.com	80	/	-

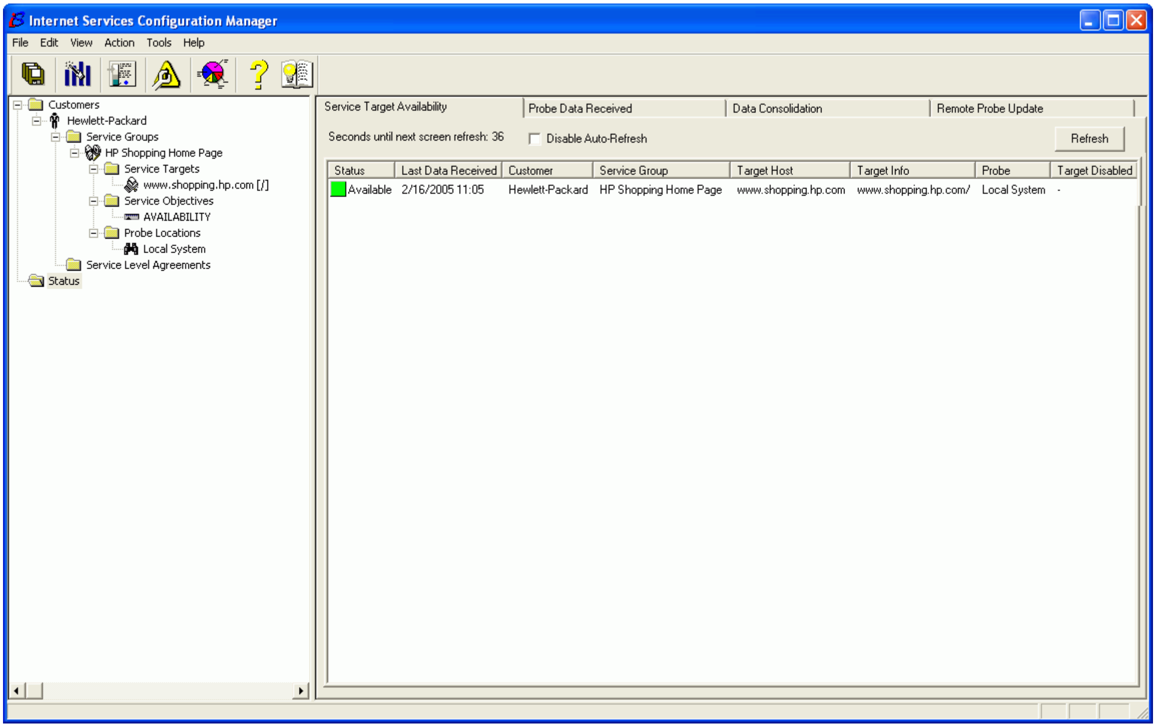
Tabs are as follows:

- Service Agreements
- Service Groups
- Service Targets
- Objectives
- Probes
- DownTimes

Check the Status of Probe Data Collection

In the Configuration Manager left pane, select Status (at the bottom of the tree) to check for success in a probe contacting the service target. If you configured the service target correctly, the icon 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.

Note: You can configure when a target displays as yellow or red by defining how many intervals where the target is unavailable will trigger a change in status to yellow or red. See **File > Configure > Dashboard** to enter values for the Status Page configuration.



- Customers
  - Hewlett-Packard
    - Service Groups
      - HP Shopping Home Page
        - Service Targets
          - www.shopping.hp.com [/]
        - Service Objectives
          - AVAILABILITY
        - Probe Locations
          - Local System
    - Service Level Agreements
- Status

Seconds until next screen refresh: 36 □ Disable Auto-Refresh

Status	Last Data Received	Customer	Service Group	Target Host	Target Info	Probe	Target Disabled
🟩 Available	2/16/2005 11:05	Hewlett-Packard	HP Shopping Home Page	www.shopping.hp.com	www.shopping.hp.com/	Local System	-

The Status page has the following tabs (the content displayed in these tabs is explained in more detail in the following sections):

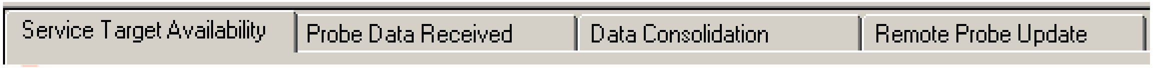
- Service Target Availabiltiy
- Probe Data Received

- Data Consolidation
- Remote Probe Update

Service Target Availability Status Tab

The Status window Service Target Availability display shows the status of the 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 be shown 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.

Right-click a target in the status display to see more detailed data from the **IOPS_TRACE_TABLE** for the target or to open the Dashboard with this target highlighted.



🔴 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.

Probe Data Received Status Tab

The Status window Probe Data Received display 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.

Right-click a target in the status display to see more detailed data from the **IOPS_TRACE_TABLE** for the target or to bring up the Dashboard with this target highlighted.

Data Consolidation Status Tab

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

Remote Probe Update Status Tab

The Status window Remote Probe Update display shows when the remote probe system contacted the server the last time for new configuration information. This status comes from the Distribution Manager (see How the Distribution Manager Works on page 168).

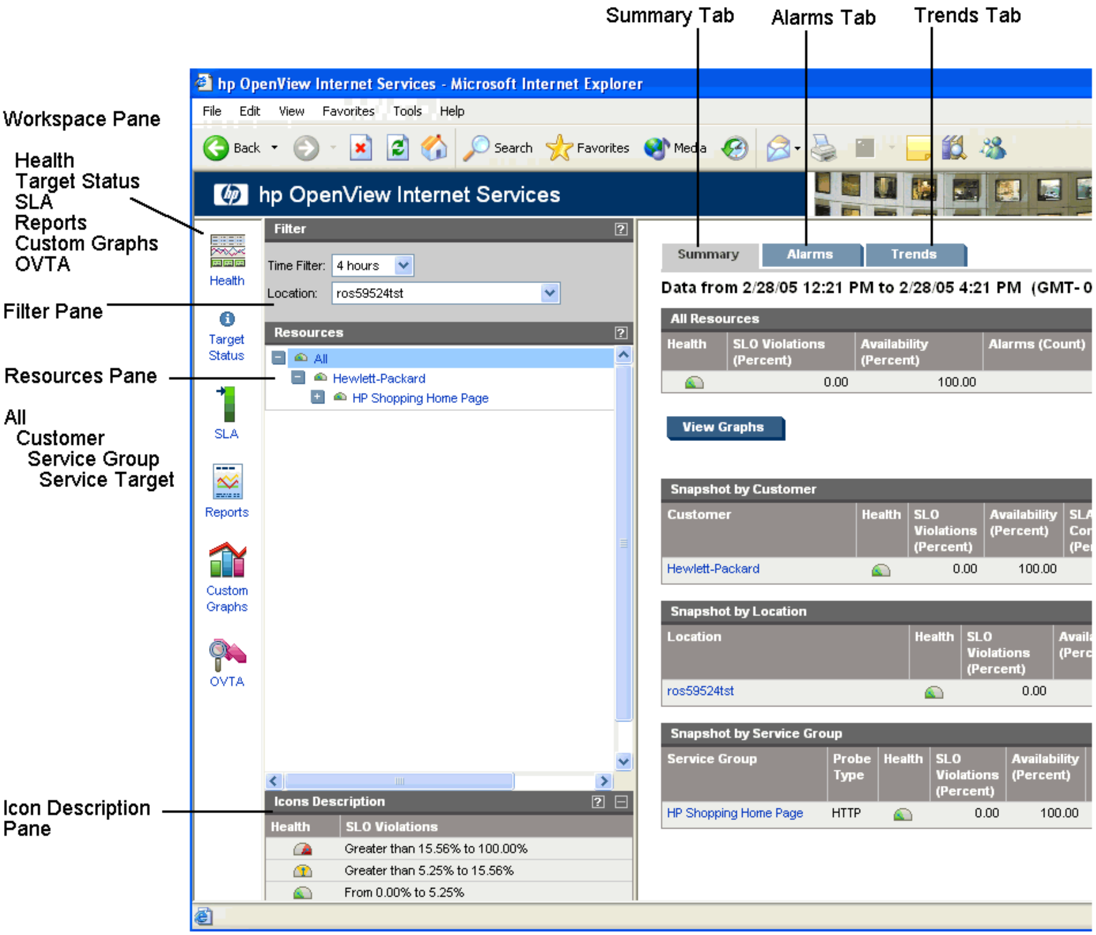
View the Data using the Dashboard

The OVIS Dashboard displays the data collected by the probes. To learn more about the Dashboard:

- Read the description of the main Dashboard window below.
- Complete the Quick Start to Using the Dashboard on page 58 to walk through some of the key Dashboard features.
- Look at More Details on the Dashboard on page 70.

Description of the Main Dashboard Window

In the Dashboard there are a number of different panes displayed.



Time Filter: 4 hours

Location: ros59524tst

Data from 2/28/05 12:21 PM to 2/28/05 4:21 PM (GMT- 0

All Resources

Health	SLO Violations (Percent)	Availability (Percent)	Alarms (Count)
●	0.00	100.00	

Snapshot by Customer

Customer	Health	SLO Violations (Percent)	Availability (Percent)	SLA Cor (Pe
Hewlett-Packard	●	0.00	100.00	

Snapshot by Location

Location	Health	SLO Violations (Percent)	Availa (Perc
ros59524tst	●	0.00	

Snapshot by Service Group

Service Group	Probe Type	Health	SLO Violations (Percent)	Availability (Percent)
HP Shopping Home Page	HTTP	●	0.00	100.00

Health	SLO Violations
●	Greater than 15.56% to 100.00%
●	Greater than 5.25% to 15.56%
●	From 0.00% to 5.25%

The **Workspace pane** is to the far left and allows you to select other functions like custom graphing.

The initial display in the Dashboard is the **Health** view. You can access a different workspace by clicking one of the workspace links shown in the workspace pane of the Dashboard.

- **Health** - the default workspace in the Dashboard. See Health Workspace on page 70.
- **Target Status** - shows status of the data collection for each target, similar to the status display in the Configuration Manager.
- **SLA** - shows whether or not each Service Level Agreement (SLA) is meeting its conformance threshold and drills down to more detail on an SLA. See SLA Workspace on page 81.
- **Reports** - shows reports of summarized data generated automatically each night. See Reports Workspace on page 83.
- **Custom Graphs** - draw additional graphs and create custom graphs based on OVIS data. See Custom Graphs Workspace on page 86.
- **OVTA** - if you have integrated OVIS and OpenView Transaction Analyzer (OVTA), you will see the link to launch the OVTA console. See OVTA Workspace on page 88.

In the main Dashboard window (the Health workspace), the **Resources pane** is the center pane. It shows the service hierarchy of Customer, Service Groups, Service Targets. Use this as a navigation tree to make selections of what data you want to view in the Dashboard. In this pane, you also get a quick view of the health of all services with red, yellow and green health icons. You'll also see the **Filter** pane for selecting the range of data to display and the **Icon Description** pane that gives a brief definition of the icons in the display.

The **Results pane** is the right pane. It displays performance data based on what you selected in the Resources pane. There are three tabs at the top of the Results pane in the Health view, for different kinds of data:

Summary tab - shows information on the health of a resource, such as how many service level objective violations, how many alarms and service availability. Also provides drill down to the detail metrics collected by a probe.

Alarms tab - shows a list of alarms based on the thresholds set.

Trends tab - shows metric baseline graphs.

You can access online help by selecting the **Help** button or clicking the **?** in the corner of some display boxes.

Note that the Health workspace refreshes automatically at 5 minute intervals.

Quick Start to Using the Dashboard

In this example you are going to use the OVIS Dashboard to look at service health for the Web page **www.hpshopping.com**. Steps to configure this service target for the customer Hewlett-Packard were covered in the previous Quick Start exercise (Quick Start for Configuring Internet Services on page 43). More detailed information on the use of the OVIS Dashboard is covered in More Details on the Dashboard on page 70.

1. Open the OVIS Dashboard from the Configuration Manager by first selecting **Start > Programs > HP OpenView > Internet Services > Configuration Manager**. Then select the **Launch Internet Service Dashboard** (pie chart) toolbar button.

   You may see the Dashboard Login screen if restricted views is set, enter User ID and Password, if required.

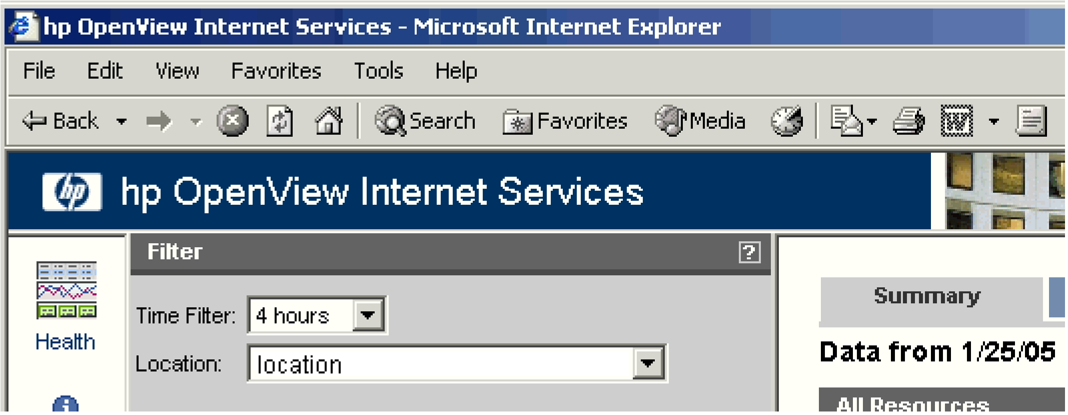
2. In the Dashboard, the initial display is the **Health** workspace.

   Health

   The data displayed is for the time period indicated in the **Filter** pane (see the screen shot below). The default is for the last 4 hours.

   Note that you can select other time periods from the **Time Filter** drop down box. If you select Custom, you can specify the time between two dates.

   Leave this default time setting at 4 hours.



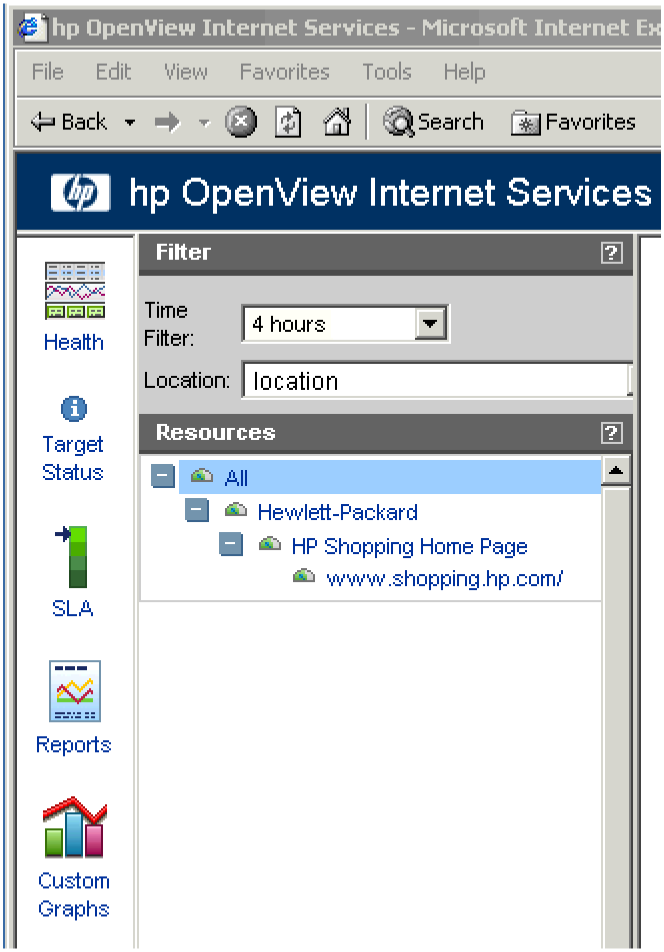
hp OpenView Internet Services - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
hp OpenView Internet Services
Filter
Health
Summary
All Resources

Time Filter: 4 hours

Location: location

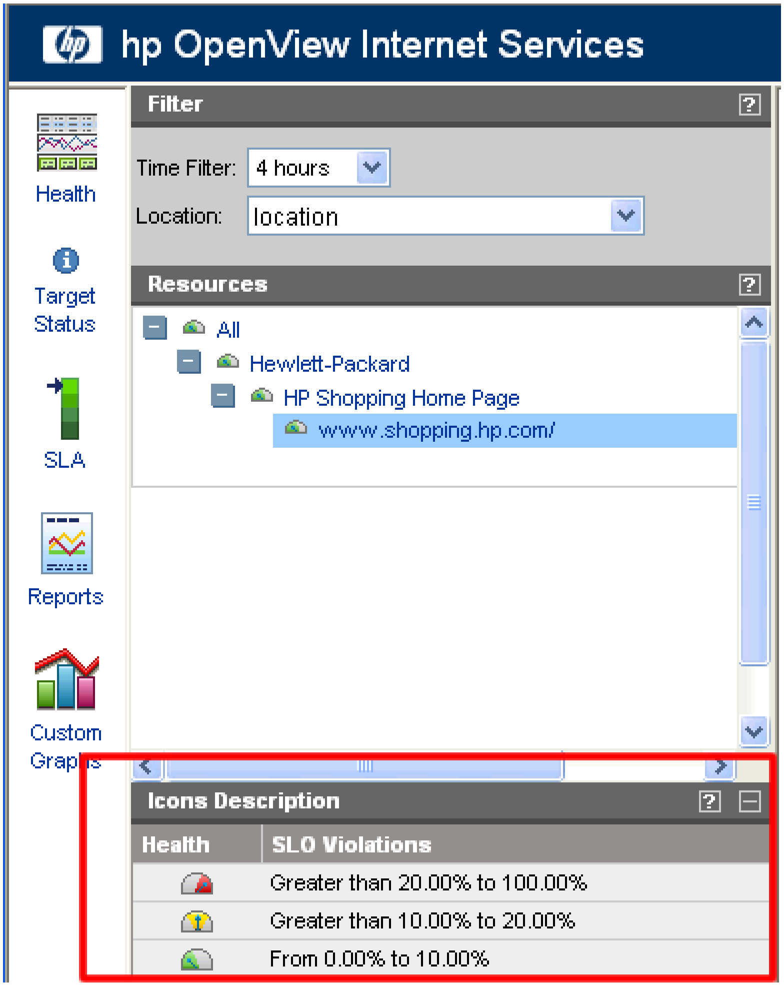
Data from 1/25/05

3 In the Resources Pane, under the first item **All**, find the customer **Hewlett-Packard** that you configured in the previous “Quick Start To Using the OVIS Configuration Manager”. Click on the plus sign (+) for each item to expand the tree and drill down from **Hewlett-Packard** to **HP Shopping Home Page** to **www.shopping.hp.com**. Note that if you have other customers and service targets configured, your display will also show these items.



4 Next to each item in the Resources pane is a red, yellow or green icon indicating the health of the service. The health is based on **Service Level Objective Violations**. The health of the Customer and Service Group is based on the Service Targets associated with that customer and service group. Note that in the example below, one Availability SLO was set up for HP Shopping Home Page service.

The health icons are described in the **Icon Description** pane at the bottom of the display. Values for the service level objective violations thresholds for red, yellow and green can be customized in the OVIS Configuration Manager.



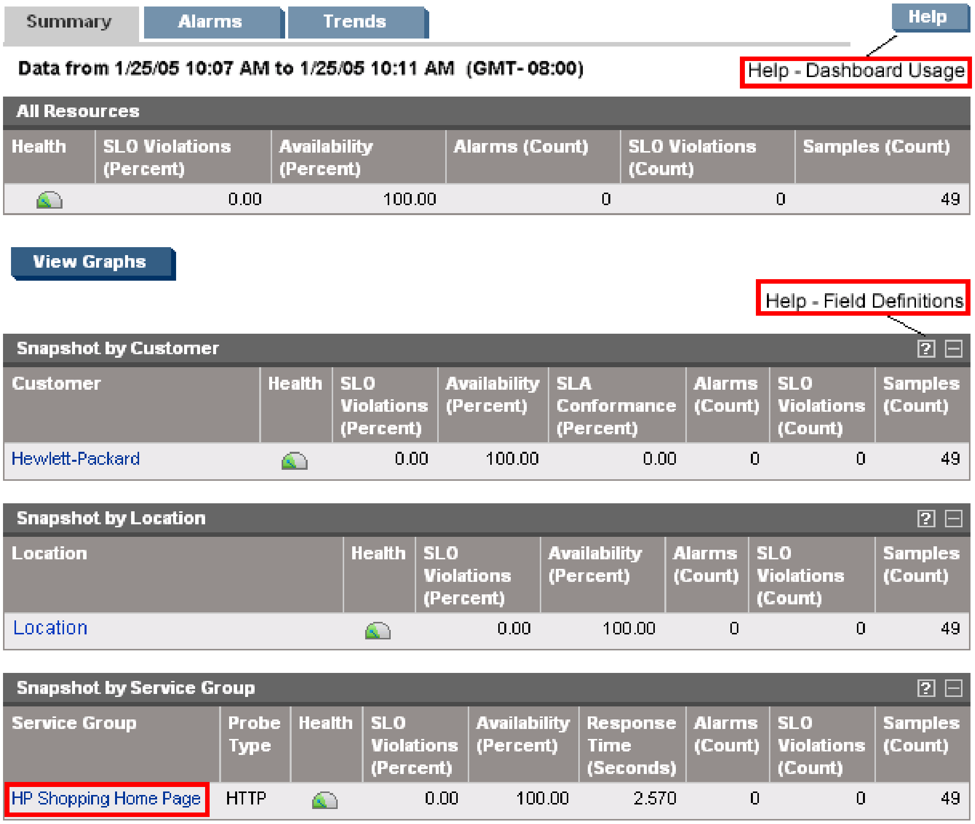
Time Filter: 4 hours

Location: location

Health	SLO Violations
🔴	Greater than 20.00% to 100.00%
🟡	Greater than 10.00% to 20.00%
🟢	From 0.00% to 10.00%

5 In the **Resources** pane, select **All**. In the **Results** pane (on the right-hand side), the **Summary** tab should be selected by default. This displays a snapshot of information for all monitored services. You will see the following tables:

- All Resources
- Snapshot by Customer
- Snapshot by Location
- Snapshot by Service Group



Data from 1/25/05 10:07 AM to 1/25/05 10:11 AM (GMT-08:00)

All Resources

Health	SLO Violations (Percent)	Availability (Percent)	Alarms (Count)	SLO Violations (Count)	Samples (Count)
	0.00	100.00	0	0	49

Snapshot by Customer

Customer	Health	SLO Violations (Percent)	Availability (Percent)	SLA Conformance (Percent)	Alarms (Count)	SLO Violations (Count)	Samples (Count)
Hewlett-Packard		0.00	100.00	0.00	0	0	49

Snapshot by Location

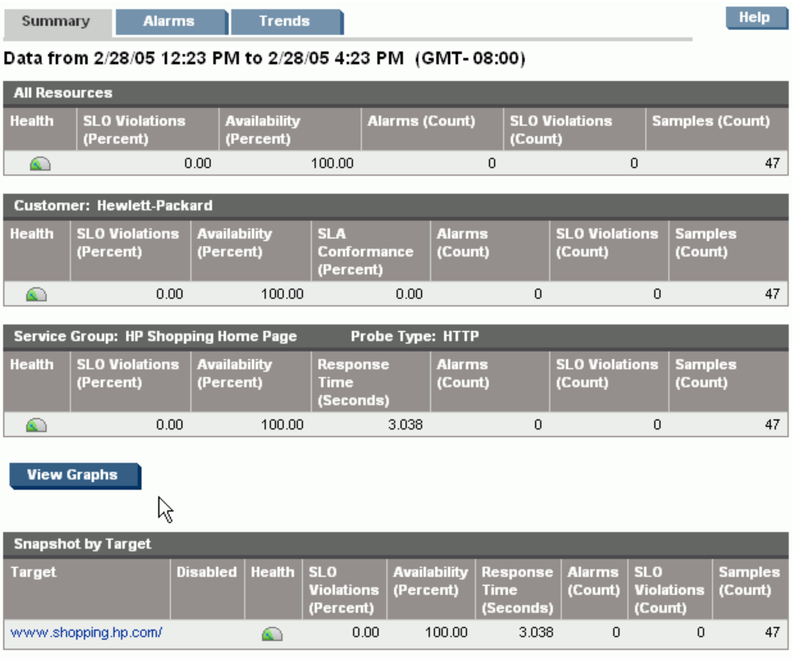
Location	Health	SLO Violations (Percent)	Availability (Percent)	Alarms (Count)	SLO Violations (Count)	Samples (Count)
Location		0.00	100.00	0	0	49

Snapshot by Service Group

Service Group	Probe Type	Health	SLO Violations (Percent)	Availability (Percent)	Response Time (Seconds)	Alarms (Count)	SLO Violations (Count)	Samples (Count)
HP Shopping Home Page	HTTP		0.00	100.00	2.570	0	0	49

Click the **?** button on the table for online help describing each field.

6 You can also make drill down selections in this Results pane; select the **HP Shopping Home Page** Service Group in the Snapshot by Service Group table. Notice that the display in the Results pane changes based on your selection.



Data from 2/28/05 12:23 PM to 2/28/05 4:23 PM (GMT-08:00)

All Resources

Health	SLO Violations (Percent)	Availability (Percent)	Alarms (Count)	SLO Violations (Count)	Samples (Count)
◔	0.00	100.00	0	0	47

Customer: Hewlett-Packard

Health	SLO Violations (Percent)	Availability (Percent)	SLA Conformance (Percent)	Alarms (Count)	SLO Violations (Count)	Samples (Count)
◔	0.00	100.00	0.00	0	0	47

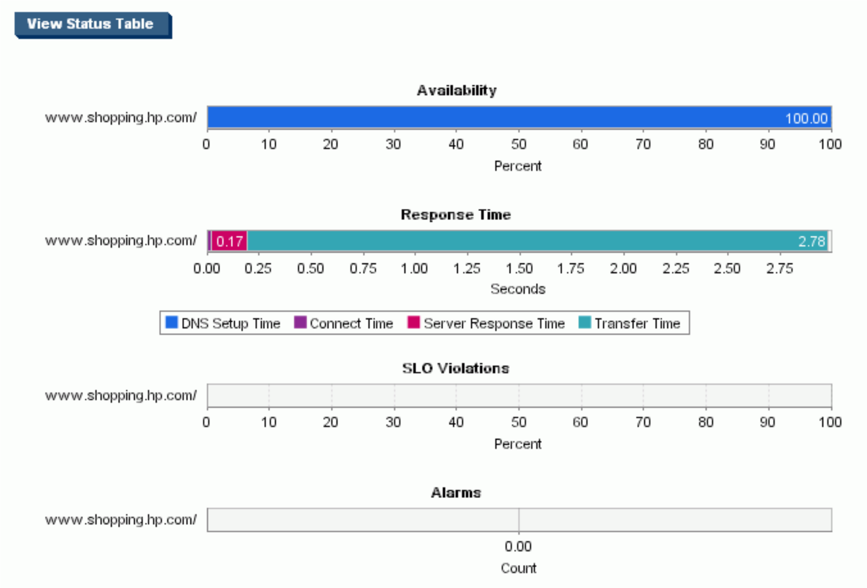
Service Group: HP Shopping Home Page Probe Type: HTTP

Health	SLO Violations (Percent)	Availability (Percent)	Response Time (Seconds)	Alarms (Count)	SLO Violations (Count)	Samples (Count)
◔	0.00	100.00	3.038	0	0	47

Snapshot by Target

Target	Disabled	Health	SLO Violations (Percent)	Availability (Percent)	Response Time (Seconds)	Alarms (Count)	SLO Violations (Count)	Samples (Count)
www.shopping.hp.com/		◔	0.00	100.00	3.038	0	0	47

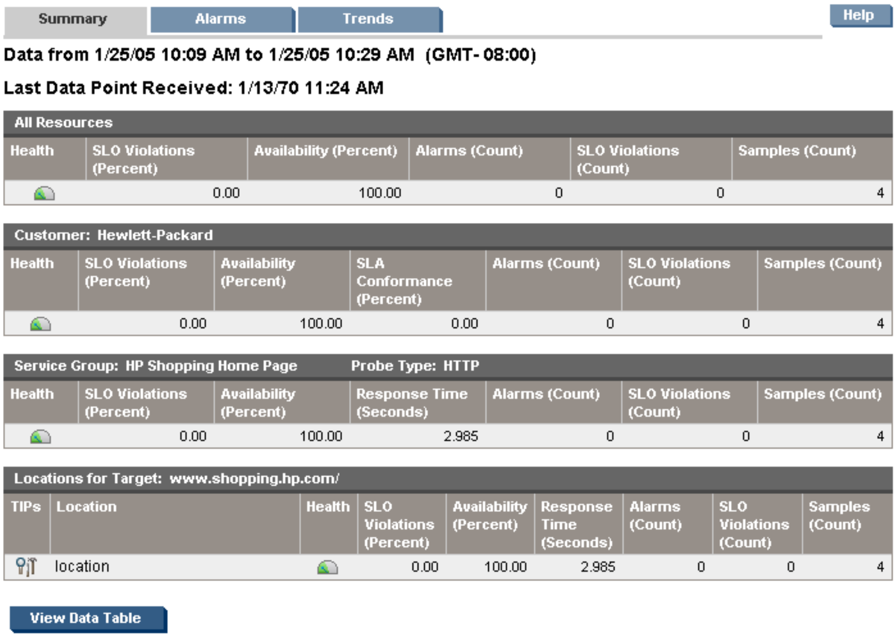
7 Select the **View Graphs** button. A set of bar graphs with summary data for this service group is displayed.



➤ When you select a customer or a service group, graphs are displayed in summary bar chart format. To see the actual metric data collected you have to drill down to the target level, as described in the next two steps.

8 Either in the Resources pane on in the Results pane, select the service target **www.shopping.hp.com** (to make the selection in the Resources pane, select Hewlett-Packard > HP Shopping Home Page > www.shopping.hp.com) and look at the data displayed in the Results pane.

See the example shown below. The data tables show information for the customer, service group and probe system location associated with this target. In the next step you'll look at the graphs displayed below the tables.



Data from 1/25/05 10:09 AM to 1/25/05 10:29 AM (GMT- 08:00)

Last Data Point Received: 1/13/70 11:24 AM

All Resources

Health	SLO Violations (Percent)	Availability (Percent)	Alarms (Count)	SLO Violations (Count)	Samples (Count)
	0.00	100.00	0	0	4

Customer: Hewlett-Packard

Health	SLO Violations (Percent)	Availability (Percent)	SLA Conformance (Percent)	Alarms (Count)	SLO Violations (Count)	Samples (Count)
	0.00	100.00	0.00	0	0	4

Service Group: HP Shopping Home Page Probe Type: HTTP

Health	SLO Violations (Percent)	Availability (Percent)	Response Time (Seconds)	Alarms (Count)	SLO Violations (Count)	Samples (Count)
	0.00	100.00	2.985	0	0	4

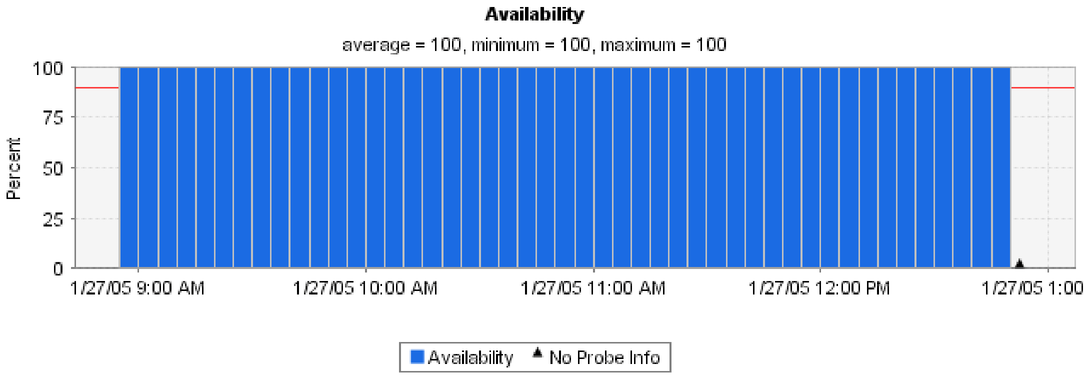
Locations for Target: www.shopping.hp.com/

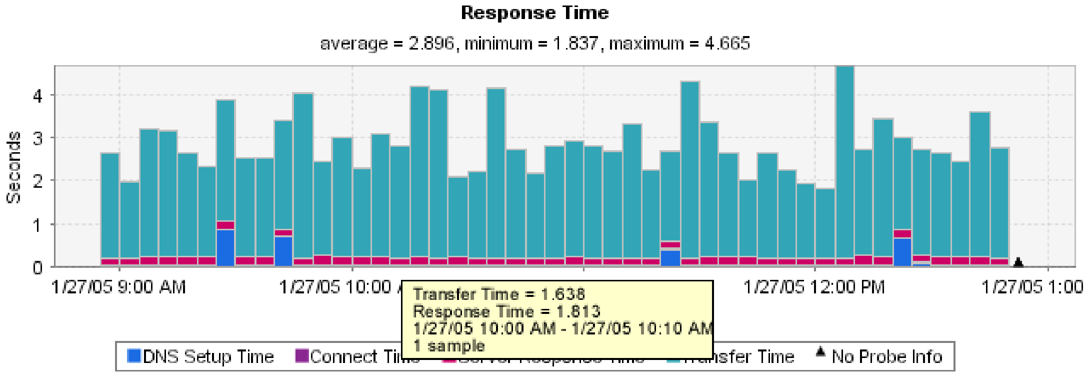
TIPs	Location	Health	SLO Violations (Percent)	Availability (Percent)	Response Time (Seconds)	Alarms (Count)	SLO Violations (Count)	Samples (Count)
	location		0.00	100.00	2.985	0	0	4

9 With the same service target (www.shopping.hp.com) selected, scroll down in the results pane to view the graphs for each metric. The graphs show each data point collected over the time interval. See the example of some of the graphs below.

Note that you can see the service level objective (SLO) defined for the Availability metric as a red line on the Availability graph. If SLOs have been defined for other metrics you will see a red line indicating the SLO on those graphs too. No red line, means no SLO was defined for the metric.

Use your mouse to hover over a bar or point on the graph and a pop up displays the metric's value and the time of the measurement (see the pop up box on the Response Time graph below).



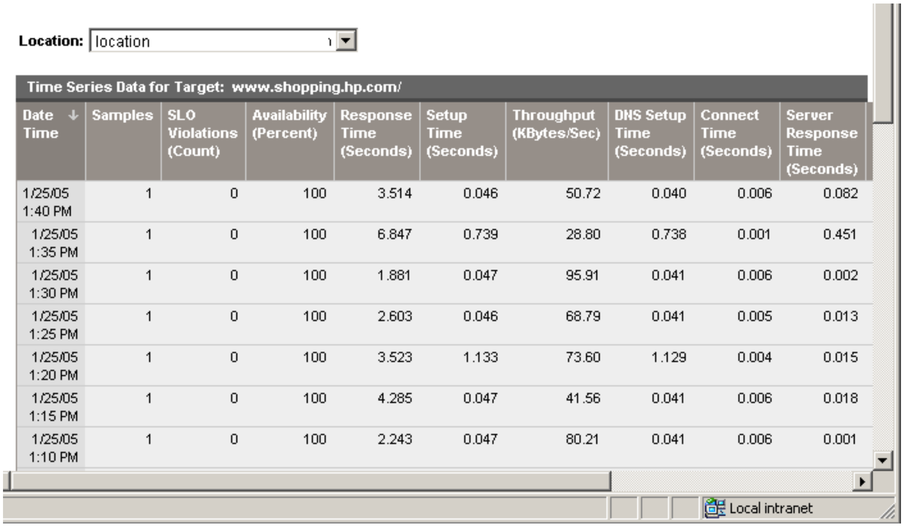


10 With the same service target (www.shopping.hp.com) selected, scroll back up in the results pane and select the **View Data Table** button.

The graphs are replaced by a table showing each five-minute measurement the probe made and all the metrics collected or calculated by the probe. The **View Graphs** and **View Data Table** buttons allow you to toggle back and forth between the display of time series data in tabular and graphical format.

The data is sorted by timestamp but you can sort by any of the columns just by clicking on the column heading. When you select a column, you will see an arrow that indicates if the column is sorted in increasing or decreasing order. Select the arrow next to the column heading to reverse the sorting. Similar sorting is available elsewhere in the Dashboard.

Note that if you had remote probes measuring this target, you could select a different probe location and view the metrics being collected from that location.

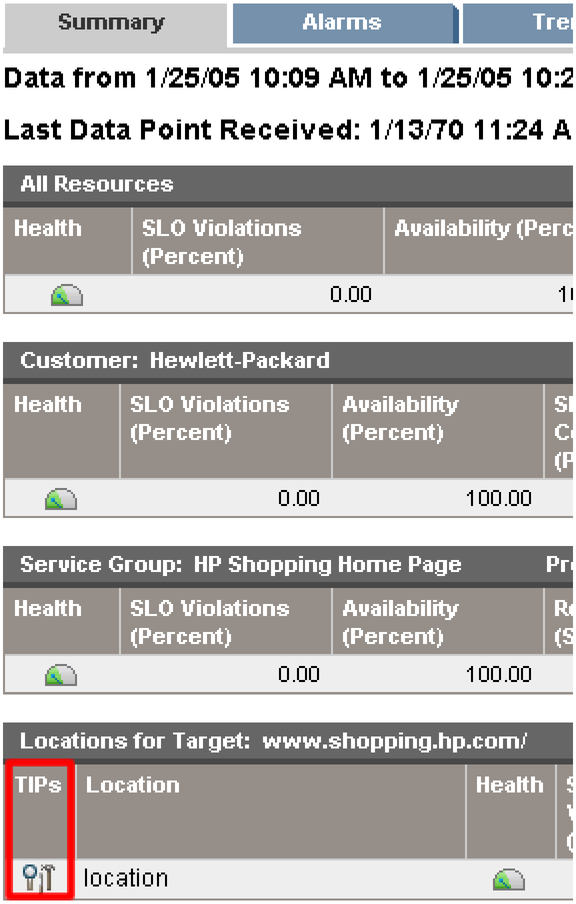


Location: location

Time Series Data for Target: www.shopping.hp.com/

Date ↓ Time	Samples	SLO Violations (Count)	Availability (Percent)	Response Time (Seconds)	Setup Time (Seconds)	Throughput (KBytes/Sec)	DNS Setup Time (Seconds)	Connect Time (Seconds)	Server Response Time (Seconds)
1/25/05 1:40 PM	1	0	100	3.514	0.046	50.72	0.040	0.006	0.082
1/25/05 1:35 PM	1	0	100	6.847	0.739	28.80	0.738	0.001	0.451
1/25/05 1:30 PM	1	0	100	1.881	0.047	95.91	0.041	0.006	0.002
1/25/05 1:25 PM	1	0	100	2.603	0.046	68.79	0.041	0.005	0.013
1/25/05 1:20 PM	1	0	100	3.523	1.133	73.60	1.129	0.004	0.015
1/25/05 1:15 PM	1	0	100	4.285	0.047	41.56	0.041	0.006	0.018
1/25/05 1:10 PM	1	0	100	2.243	0.047	80.21	0.041	0.006	0.001

11 With the same service target (www.shopping.hp.com) selected, scroll back up in the results pane and select the Troubleshooting Insight Packages (TIPs) icon in the first column of the **Locations for Target** table next to the **www.shopping.hp.com** target.



Summary | Alarms | Tre

Data from 1/25/05 10:09 AM to 1/25/05 10:2

Last Data Point Received: 1/13/70 11:24 A

All Resources

Health	SLO Violations (Percent)	Availability (Perc
◔	0.00	1(

Customer: Hewlett-Packard

Health	SLO Violations (Percent)	Availability (Percent)	Sl C (P
◔	0.00	100.00	

Service Group: HP Shopping Home Page Pr

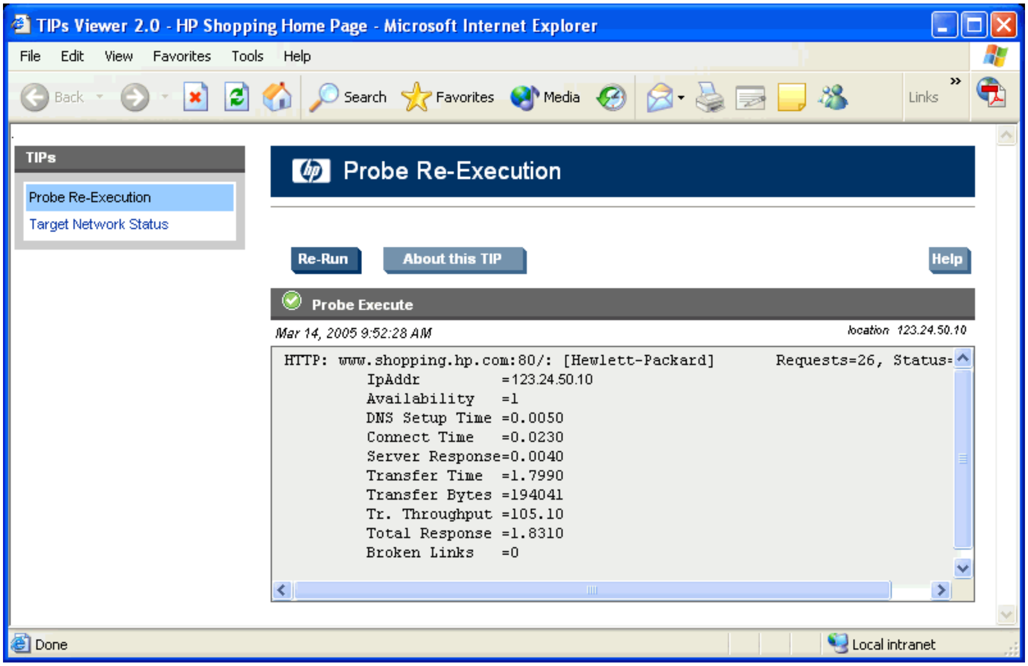
Health	SLO Violations (Percent)	Availability (Percent)	R (S
◔	0.00	100.00	

Locations for Target: www.shopping.hp.com/

TIPs	Location	Health	S V (
	location	◔	

When you select the TIPs icon, the **TIPs Viewer** is displayed and all the TIPs defined for this probe are run automatically on the probe system. The results are displayed in the right pane of the TIPs viewer. Links to the command results for each TIP are displayed in the left pane.

When you first enter the TIPs Viewer, the first TIP is displayed in the right pane. To see the results for another TIP, select another TIP in the list in the left pane of the TIPs Viewer (in the example you can select the Target Network Status command).


TIPs Viewer 2.0 - HP Shopping Home Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media Links
TIPs
Probe Re-Execution
Target Network Status
Probe Re-Execution
Re-Run
About this TIP
Help
Probe Execute
Done
Local intranet

Mar 14, 2005 9:52:28 AM location 123.24.50.10

```
HTTP: www.shopping.hp.com:80/: [Hewlett-Packard]      Requests=26, Status=
          IpAddr          =123.24.50.10
          Availability    =1
          DNS Setup Time  =0.0050
          Connect Time    =0.0230
          Server Response=0.0040
          Transfer Time   =1.7990
          Transfer Bytes  =194041
          Tr. Throughput  =105.10
          Total Response  =1.8310
          Broken Links    =0
```

Select the **Re-Run** button to run the TIP you selected in the left pane again. Select the **About this TIP** button to get detailed information on each TIP and the **Help** button for TIPs Viewer online help.

You can customize TIPs or create your own TIPs using the TIPs Configuration program. See Configuring and Using TIPs on page 155 for more information on customizing TIPs.

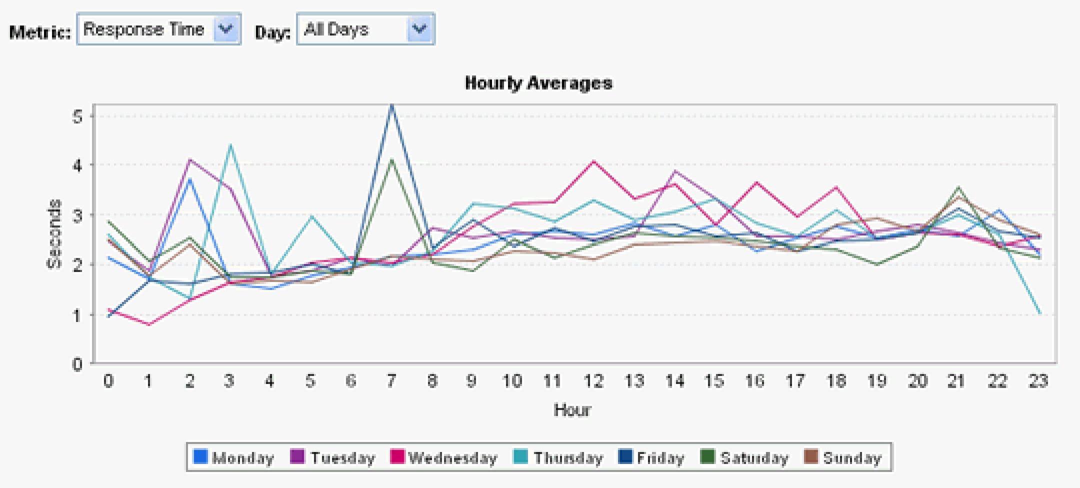
Close the TIPs Viewer by clicking the red button in the top right corner.

12 From the Dashboard, go back to the Resources pane and select **All**. Scroll to the top of the Results pane and select the **Alarms** tab. If any alarms have been generated, they will be listed in this display. (Since the Availability service level objective (SLO) you defined in the previous "Quick Start for the Configuration Manager" will not likely have any SLO violations, there may not be any alarms to display.)

TIPs are available for each Alarm.

➤ Note that in order to have alarms displayed in the Dashboard, you must have configured alarm thresholds to trigger alarms AND you must have configured alarm targets to be sent to the Dashboard in the Configuration Manager File > Configure > Alarm Destinations dialog.

13 Scroll to the top of the Results pane again and select the **Trends** tab to view baseline data based on data for a single metric like Response Time. See an example graph below. Select the **Help** button for a description of each graph.



Metric: Response Time Day: All Days

That gives you a quick view of the Dashboard Health workspace. See the following sections for more information about the Dashboard.

More Details on the Dashboard

Once you complete the “Quick Start to Using the Dashboard” see the following sections for more information on the Dashboard.

Login

Note that there are a number of ways to access the Dashboard.

- From the Configuration Manager, select the **Launch Internet Services Dashboard** (pie chart) toolbar button.
- From the Configuration Manager menu you can select **Action > Run > Internet Service Dashboard** to launch the Dashboard.
- You can also launch the Dashboard in context. From the Configuration Manager Status display, right-click a service target in the Service Target Availability tab or the Probe Data Received tab.
- You can also start the Dashboard data display by typing the following URL into your browser address bar:

  ```
  http://<management server>:8080/OvisDashboard
  ```

  Where <*management server*> is the OVIS management server and *8080* is the port configured for the Dashboard. See Configuring and Changing Ports in OVIS on page 445 for information on changing the port.

Different logins can be configured to give each user access to a different set of data. For example, you may want a customer to only view their data or you may want to assign a number of customers and selected service groups to a particular operator. Use the Configuration Manager to set up restricted views and user profiles to control what data can be viewed by each user. See Dashboard Login using Restricted Views on page 131 for details.

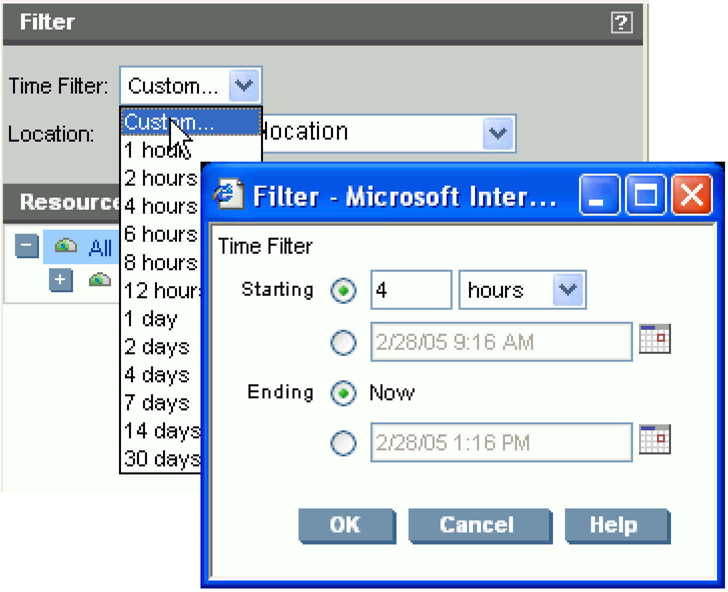
Health Workspace

Use the health workspace to see the health of all services, drill down to detailed data on availability, response time, service level violations and other measurements, see alarms generated by OVIS, see trend and baseline graphs, and access diagnostic tools and commands (Troubleshooting Insight Packages - TIPs) you can run to analyze problems.

Filter Pane

Use filters to determine what time period and what probe location is used to construct the data displayed in the Dashboard.

The **Time** period currently selected is shown in the Filter Pane. If you want to change the time period for the data display, select a predefined time period from the drop down box. Or you can select Custom from the drop down box to enter a particular set of dates.



Time Filter: Custom...

Location: ...location

Time Filter

Starting ● 4 hours

○ 2/28/05 9:16 AM

Ending ● Now

○ 2/28/05 1:16 PM

The probe **Location** currently selected is shown in the Filter Pane. To change to display a different probe location, select a location from the drop down box. Note that for OVTA data, the location includes the servicing systems.

By default you will see data for All customers and all service groups for the time span configured for the Dashboard in the Configuration Manager (**File > Configure > Dashboard**).

Resources Pane

The Resources pane gives a quick view of the health of all services. Health icons are described below. Health is based on the percentage of service level objectives violated for targets. The percentages associated with each icon can be customized in the configuration manager **(File > Configure > Dashboard)**. Health is propagated up through the service hierarchy.

The Resources pane is also used for navigation, allowing you to select an item in the tree view (+ to expand and - to close). Data in the tree view is grouped into the following categories (a service hierarchy):

- All - all targets for all customers
- Customer - a grouping of services and service targets
- Service group - a grouping of similar service targets for a customer
- Service target - a service for a probe to monitor and the location to be probed

Data associated with the item you select is displayed in the right pane.

If you see an item in the Dashboard's Resource pane navigation tree that says "Unknown Target Name", this means that there is no collected data in the database for this target. If there is a host name configured for this target, the host name will be displayed to help you identify the target. If there a re multiple targets in a single service group that do not have data, you will see a sequential index after the name to uniquely identify the target.

Icon Descriptions Pane

The Icon description pane gives a definition of the icons used in the display.

The Resources pane and Summary view in the righthand pane, display icons indicating the health of the services. Health is based on percent of service level objectives violated for targets. See Configuring the Dashboard on page 129 for more information on how health is measured.

Note that if NO service level objectives (SLOs) have been defined, the status icon will be green. If some targets for a customer have no SLOs defined, these targets are not computed into overall health for the service group and customer. This is useful for preproduction and test systems, or other systems deemed as not important to overall health but that you do want probe measurements for. Also if, for example, all the SLOs you set up are based on Response Time, then Availability will have no effect on the Health.

Note that the values for the service level objective violations thresholds for red, yellow and green can be customized in the OVIS Configuration Manager, **File > Configure > Dashboard** dialog.

The Alarms tab displays icons indicating the severity of an alarm condition. See Alarms Tab on page 76.

Summary Tab

Selecting the Summary tab displays status information for your monitored Services.

If “ALL” is selected in the Resources pane (this is the default selection) then in the Summary tab, you will see the following data tables:

- Snapshot by Customer
- Snapshot by Location
- Snapshot by Service Group

You can select a customer, service group, or target in either the Resources pane navigation tree or from a list in one of these tables. The Results pane will then display data for just that selection. This allows you to easily drill down to a particular problem identified by a red or yellow health icon.

Different data is displayed depending on whether you have selected to view the data for All customers, a customer, a service group for a customer, a target or probe location.

So for example, if you select a target, then the tables in the Results pane will show data for the customer, service group and probe location associated with the target.

When you select a customer or service group, you can scroll down the Results pane to see summary graphs. (If graphs are not displayed, select the **View Graphs** button. The **View Graphs** and **View Data Table** buttons allow you to toggle back and forth between the tabular and graphical data display.)

For example, when you select a customer, the summary bar chart graphs displayed are as follows:

- Availability - this graph shows the percent Available for each service group under that customer.
- SLO Violations - this graph shows the percent of SLO violations for each service group under that customer.

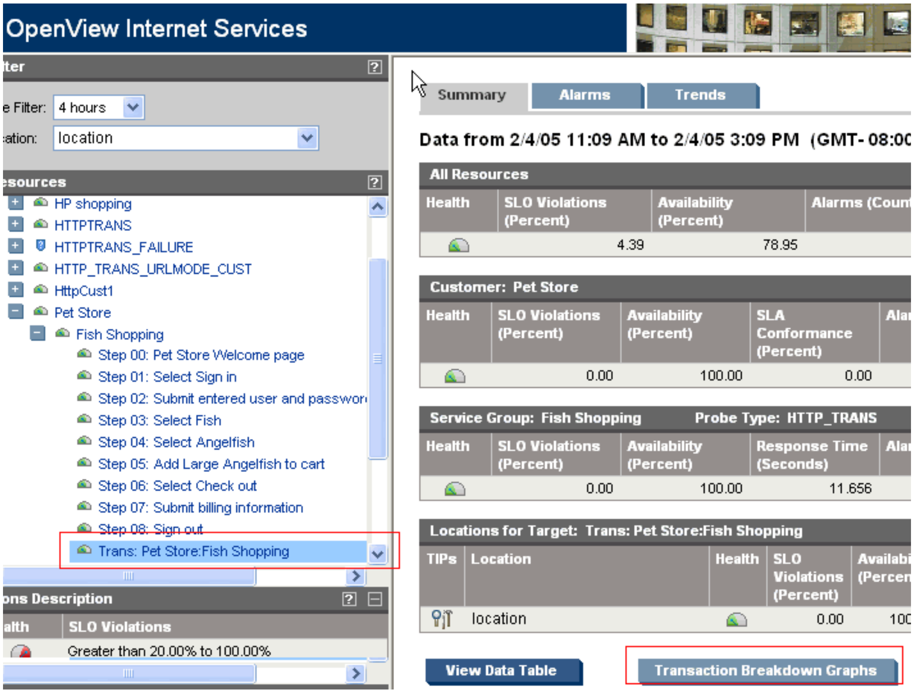
- SLA Conformance - this graph shows the percent of SLA conformance for each service group under that customer.
- Alarms - this graph shows the number of alarms for each service group under that customer.

When you select a service group, the summary bar chart graphs displayed are as follows:

- Availability - this graphs shows the percent Available for each target under that service group.
- Response Time - this graph shows the Response Time components for each target under that service group.
- SLO Violations - this graph shows the percent of SLO violations for each target under that service group.
- Alarms - this graph shows the number of alarms for each target under that service group.

If you select a target, detailed time series data for each metric the probe collects is displayed. The **View Data Tables** and **View Graphs** buttons allow you to toggle back and forth between the display of the time series data in tabular and graphical format. At the target level, the View Data Tables button displays a table listing a timestamp for each measurement the probe made and all the metric data collected or calculated by the probe.

Transaction Breakdown graphs are available when you have a multi-step transaction probe like HTTP_TRANS and you select (drill-down) the target step that represents the overall combined transaction steps. Graphs of each metric are displayed with a breakdown for each step in the transaction. See the example below for a multi-step HTTP_TRANS transaction.



OpenView Internet Services

ter

e Filter: 4 hours

ation: location

esources

- HP shopping
- HTTPTRANS
- HTTPTRANS_FAILURE
- HTTP_TRANS_URLMODE_CUST
- HttpCust1
- Pet Store
  - Fish Shopping
    - Step 00: Pet Store Welcome page
    - Step 01: Select Sign in
    - Step 02: Submit entered user and passwor
    - Step 03: Select Fish
    - Step 04: Select Angelfish
    - Step 05: Add Large Angelfish to cart
    - Step 06: Select Check out
    - Step 07: Submit billing information
    - Step 08: Sign out
    - Trans: Pet Store:Fish Shopping

ons Description

alth	SLO Violations
	Greater than 20.00% to 100.00%

Summary | Alarms | Trends

Data from 2/4/05 11:09 AM to 2/4/05 3:09 PM (GMT-08:0C

All Resources

Health	SLO Violations (Percent)	Availability (Percent)	Alarms (Coun
	4.39	78.95	

Customer: Pet Store

Health	SLO Violations (Percent)	Availability (Percent)	SLA Conformance (Percent)	Ala
	0.00	100.00	0.00	

Service Group: Fish Shopping Probe Type: HTTP_TRANS

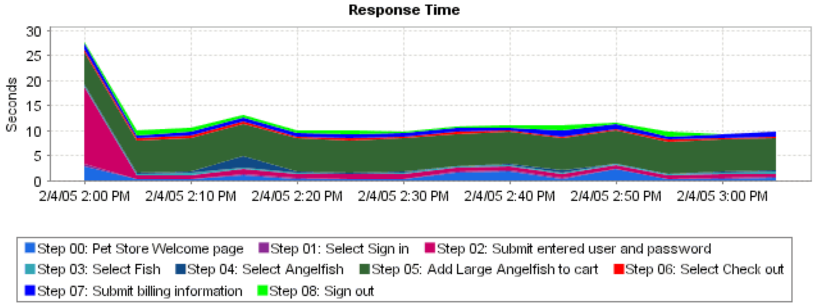
Health	SLO Violations (Percent)	Availability (Percent)	Response Time (Seconds)	Ala
	0.00	100.00	11.656	

Locations for Target: Trans: Pet Store:Fish Shopping

TIPs	Location	Health	SLO Violations (Percent)	Availabi (Percen
	location		0.00	10C

View Data Table

Transaction Breakdown Graphs



TIPs

Once you have drilled down to the target level, Troubleshooting Insight Packages (TIPs) are available to help you further characterize the problem. TIPs are also available for each alarm displayed in the Alarms tab.

When you select the TIPs icon, the TIPs Viewer is displayed and all the TIPs that are defined to help you troubleshoot the problem are run automatically on the probe system. Each TIP executes one or more commands against the service target or alarm in question, to collect relevant information. The results are displayed in a TIPs Viewer.

TIPs includes many out-of-the-box TIPs and troubleshooting commands for all supported OVIS platforms. See the **About this TIP** help for detailed descriptions of the TIPs and commands and the TIPs Viewer help for information on running TIPs. After you finish viewing the TIPs, you can close the TIPs Viewer window and return to the OVIS Dashboard.

The TIPs can be edited or new TIPs and commands created to meet specific troubleshooting objectives. To open the TIPs Configuration program, select **Start > Program > HP OpenView > Tips >TIPs Configuration** on the OVIS management server. See the TIPs Configuration program's online help for more information about how you can edit and create your own TIPs. Also see the What's New Troubleshooting Insight Packages paper available on the CD or installed in `<install dir>\help\iops\c\ovis60-tips.pdf`.

Alarms Tab

Selecting the Alarms tab, displays the alarms for the items selected in the Resources pane navigation view.

Alarms generated in OVIS are displayed in order by timestamp. The detailed information displayed for the alarm varies depending on the item you selected in the navigation pane.

You can sort the alarms by different columns by clicking on the column heading. Then you can click the arrow in the column heading to sort in descending or ascending order.

➤ Also note that in order for alarms to be displayed in the dashboard, the Alarm Targets dialog Database checkbox must be checked (see the Configuration Manager **File > Configure > Alarm Destinations**).

TIPs (Troubleshooting Insight Packages) - Selecting the TIPs icon launches the TIPs Viewer display where you can run troubleshooting commands relevant to the alarm condition to help you diagnose the problem.

Trace (if you have OVTA integration configured) - Selecting the OVTA icon launches the OVTA Console with the Trace tab displayed. The data displayed is in the context of the target transaction's alarm you had selected in OVIS.

Severity - The icons you see displayed in the Severity column relate to the alarm severity. These are different than the Health icons displayed in the Summary tab. You can see, in the Icon Description pane, the definition for Critical, Major, Minor, Warning and Normal alarm severity. These alarm severities correspond to the alarm thresholds configured in the Configuration Manager Objectives dialog.

⊗ CRITICAL

▼ MAJOR

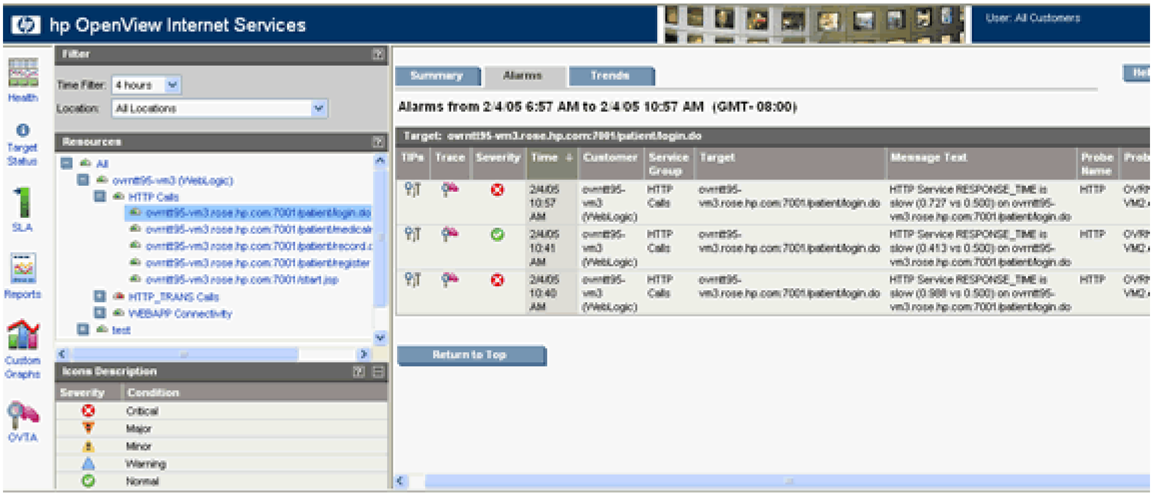
⚠ MINOR

△ WARNING

✓ NORMAL

These severity levels vary by probe based on what has been set up in the OVIS Configuration Manager. For example, you might have set up a Response Time SLO of 5 seconds with an alarm threshold of 10 seconds for a critical severity alarm.

Here is an example of the Alarms display in the Dashboard.



Time Filter: 4 hours

Location: All Locations

Resources:

- All
  - ovrtt95-vm3 (WebLogic)
    - HTTP Calls
      - ovrtt95-vm3.rose.hp.com:7001/patient/login.do
      - ovrtt95-vm3.rose.hp.com:7001/patient/medical
      - ovrtt95-vm3.rose.hp.com:7001/patient/record.
      - ovrtt95-vm3.rose.hp.com:7001/patient/register
      - ovrtt95-vm3.rose.hp.com:7001/start.jsp
    - HTTP_TRANS Calls
    - WEBAPP Connectivity
  - test

Icons Description

Severity	Condition
⊗	Critical
▼	Major
▲	Minor
▲	Warning
✓	Normal

Alarms from 2/4/05 6:57 AM to 2/4/05 10:57 AM (GMT-08:00)

Target: ovrtt95-vm3.rose.hp.com:7001/patient/login.do

TIPs	Trace	Severity	Time	Customer	Service Group	Target	Message Text	Probe Name	Prob
		⊗	2/4/05 10:57 AM	ovrtt95-vm3 (WebLogic)	HTTP Calls	ovrtt95-vm3.rose.hp.com:7001/patient/login.do	HTTP Service RESPONSE_TIME is slow (0.727 vs 0.500) on ovrtt95-vm3.rose.hp.com:7001/patient/login.do	HTTP	OVR VM2
		✓	2/4/05 10:41 AM	ovrtt95-vm3 (WebLogic)	HTTP Calls	ovrtt95-vm3.rose.hp.com:7001/patient/login.do	HTTP Service RESPONSE_TIME is slow (0.413 vs 0.500) on ovrtt95-vm3.rose.hp.com:7001/patient/login.do	HTTP	OVR VM2
		⊗	2/4/05 10:40 AM	ovrtt95-vm3 (WebLogic)	HTTP Calls	ovrtt95-vm3.rose.hp.com:7001/patient/login.do	HTTP Service RESPONSE_TIME is slow (0.988 vs 0.500) on ovrtt95-vm3.rose.hp.com:7001/patient/login.do	HTTP	OVR VM2

Trends Tab

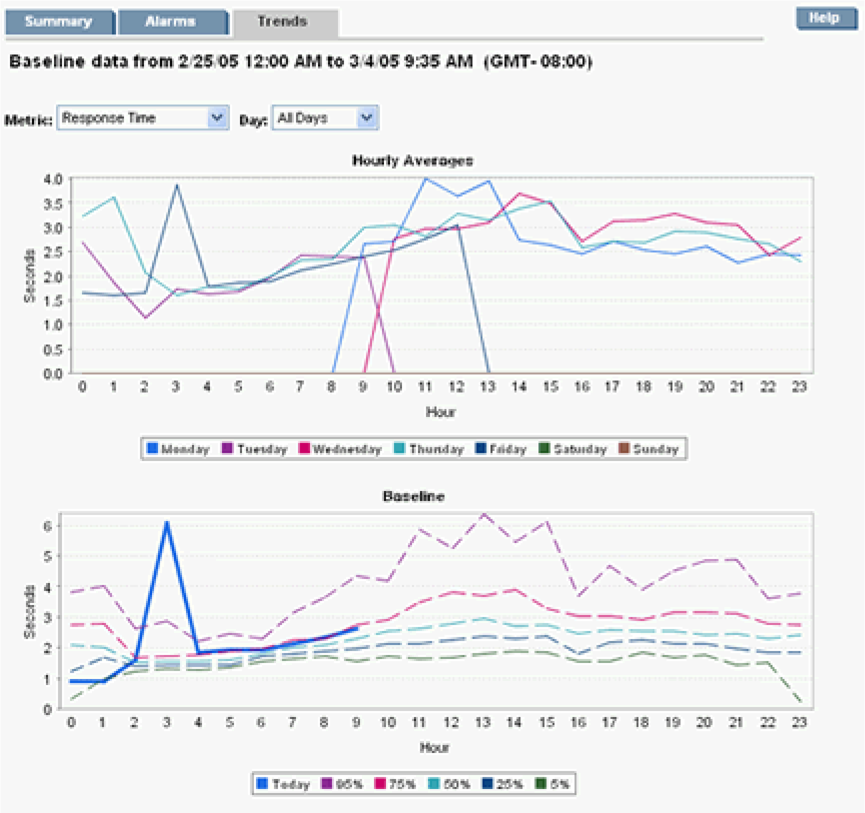
Selecting the Trends tab, displays baseline data for the item selected in the Resources pane navigation view. The baseline graphs are based on data for a single metric for the date range displayed at the top of the page. The date range is based on the amount of data configured in the Configuration Manager **File > Configure > Database Options** dialog for **Probe/Target Level Data**. By default, the database is configured to store 7 days of detail data, but these trend graphs are more meaningful if you have 30 days or more. If you use these graphs, and disk space is not an issue, we recommend you increase the size for Probe/Target Level Data to 30 days.

See the online help for the Trends tab for details. Baseline graphs include:

- Hourly Averages - shows the average values for the metric for each hour of the day.
- Baseline - shows how today's values for the metric compare to typical values for this metric for each hour of the day.
- Density - shows the number of times the metric was a particular value during the date range (for example, Response Time was 2.2 seconds, 38 times during the date range). This gives you a histogram where you can easily see the most common metric value during the date range.

- Cumulative Distribution - shows the percentage of times the metric was a particular value or less (for example, Response Time was 2.2 seconds or less 80% of the time). With this graph you can see the overall quality of service. The larger the area under the curve the better the service was.
- Hourly Statistics - Shows the mean, median, normal, maximum and minimum values for the metric for each hour of the day.

An example of some of the trend graphs follows:



Baseline data from 2/25/05 12:00 AM to 3/4/05 9:35 AM (GMT-08:00)

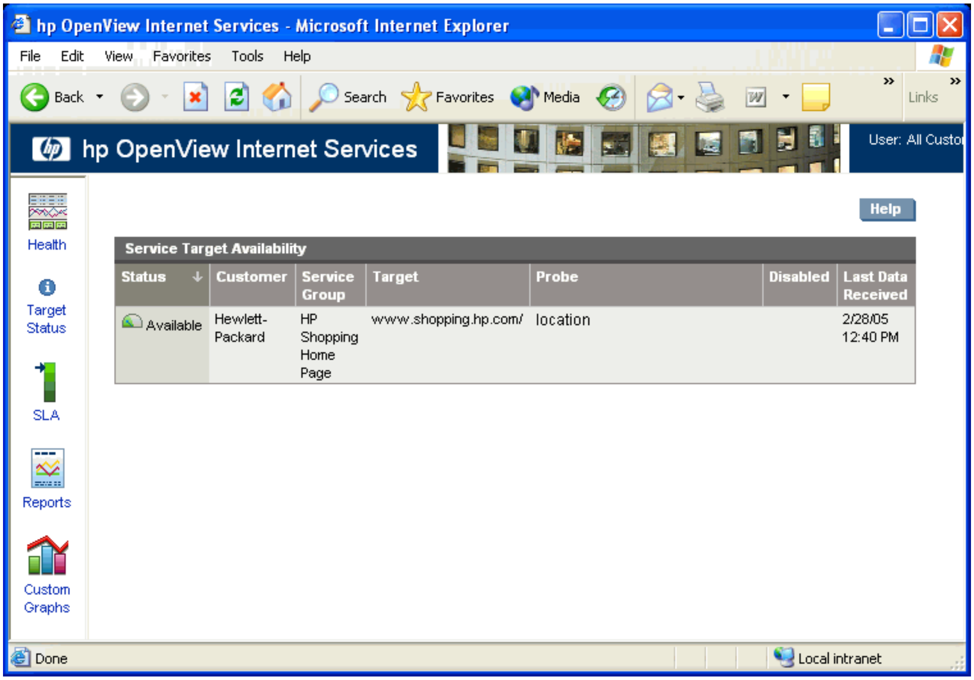
Metric: Response Time

Day: All Days

Target Status Workspace

In the Workspace pane on the left in the Dashboard, select the Target Status workspace link to view the status of service target availability. The service target status display indicates whether or not the probe could connect to the service target. Note that this page does not Auto Refresh. Also if you have a large configuration it may take a while to display this page.

Green indicates Available, Red indicates Unavailable. Error information may also be displayed for Unavailable targets. The last communication error is displayed at the top of the screen. Note that the timestamp of this error is when the given error occurred.



Service Target Availability

Status	Customer	Service Group	Target	Probe	Disabled	Last Data Received
Available	Hewlett-Packard	HP Shopping Home Page	www.shopping.hp.com/	location		2/28/05 12:40 PM

You will see the following icons to indicate the status:

"No Probe Info" There are no measurements for this service target within the expected amount of time.

"Unavailable" The service target was unavailable at the last measurement.

🟥 "Available - Late" The service target was available at the last measurement, but no probe information was received within the number of intervals selected for the 'Red Status' in the **File > Configure > Dashboard** menu (default is 4).

🟨 "Available - Late" The service target was available at the last measurement, but no probe information has been was received within the number of intervals selected for the 'Yellow Status' in the **File > Configure > Dashboard** menu (default is 2).

🟩 "Available" The service target is available.

▨ "Disabled" The service target is disabled.

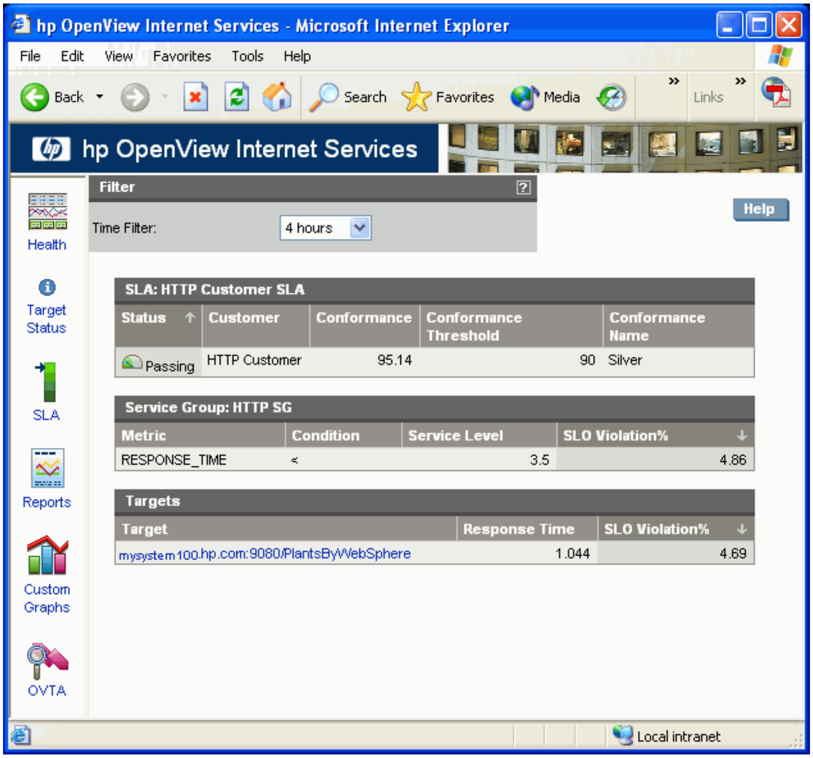
You can configure when a target displays as yellow or red by defining how many intervals where the target is unavailable will trigger a change in status to yellow or red (for example, if unavailable for 2 - 4 intervals show the status as yellow). Use the Configuration Manager to define these values for the Status page by selecting **File > Configure > Dashboard** (see Other Configuration Options on page 96 for more information).

SLA Workspace

In the Workspace pane on the left in the Dashboard, select the SLA workspace link to view Service Level Agreement conformance data.

The **Conformance** value is the percent of time that the objectives (SLOs) that make up the SLA have met their service levels. For example, if you have two SLOs in an SLA, and in 12 intervals, one of them had 1 SLO violation (11 conforming samples) and the other had 5 violations (7 conforming samples), then the SLA conformance would be 75 percent. ((11+7)/24 = .75) The number of samples is determined by the Time Filter selection in the Dashboard. Changing the time filter will change the results of the conformance because a larger or smaller sample will be used in the calculation.

The status of the SLA is determined by the **Conformance Threshold**. If the conformance is greater than or equal to the Conformance Threshold, it will have a Passing status. If the conformance is less than the Conformance Threshold, it will have a Failing status. If no Conformance Threshold is selected for the SLA, the status will always be Passing.



Filter

Time Filter: 4 hours

SLA: HTTP Customer SLA

Status	Customer	Conformance	Conformance Threshold	Conformance Name
Passing	HTTP Customer	95.14	90	Silver

Service Group: HTTP SG

Metric	Condition	Service Level	SLO Violation%
RESPONSE_TIME	<	3.5	4.86

Targets

Target	Response Time	SLO Violation%
mysystem100.hp.com:9080/PlantsByWebSphere	1.044	4.69

To see the SLA conformance for the current month, select "Custom..." in the Time Filter drop down box, and select the beginning of the month for the start time and Now for the end time.

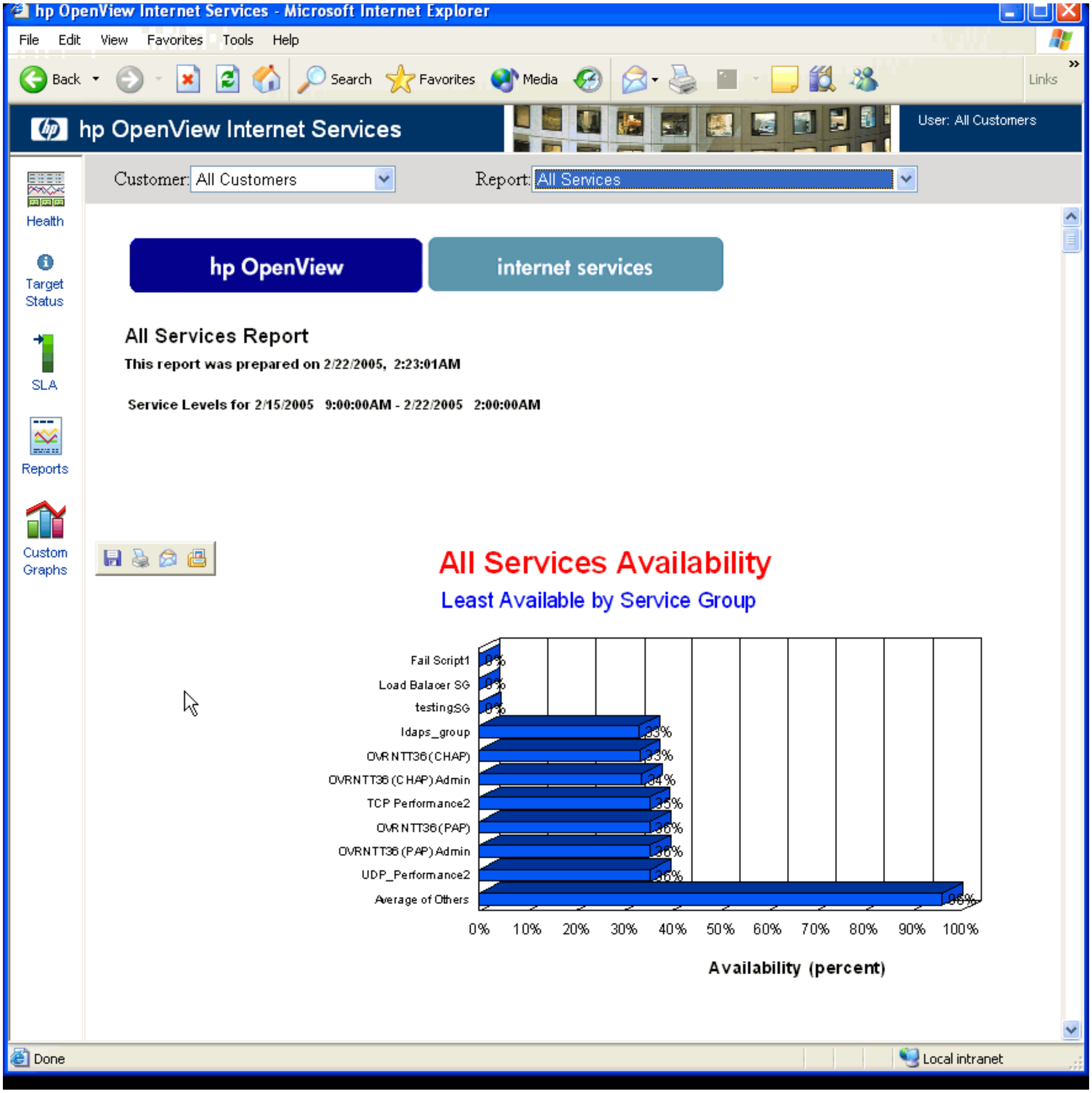
You can drill down to the SLOs within a given SLA. The drill down will show you how much each Service Group is contributing to the SLA. You can also drill down to see the service level violation percentage of a particular metric and the average metric value by target within a Service Group.

Reports Workspace

In the Workspace pane on the left in the Dashboard, select the Reports workspace link to view summary reports. These reports are generated automatically every night and so they will not be available until the day following installation and configuration. The out-of-the-box reports provided with OVIS are as follows.

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

For the first three you can select all service types or a particular service and all customers or a particular customer.



All Services Report

This report was prepared on 2/22/2005, 2:23:01AM

Service Levels for 2/15/2005 9:00:00AM - 2/22/2005 2:00:00AM

See Removing Unused OVTA Reports on page 172 for information on how to remove OVTA report templates if you are not planning to integrate OVIS and OVTA.

OVTA Reports

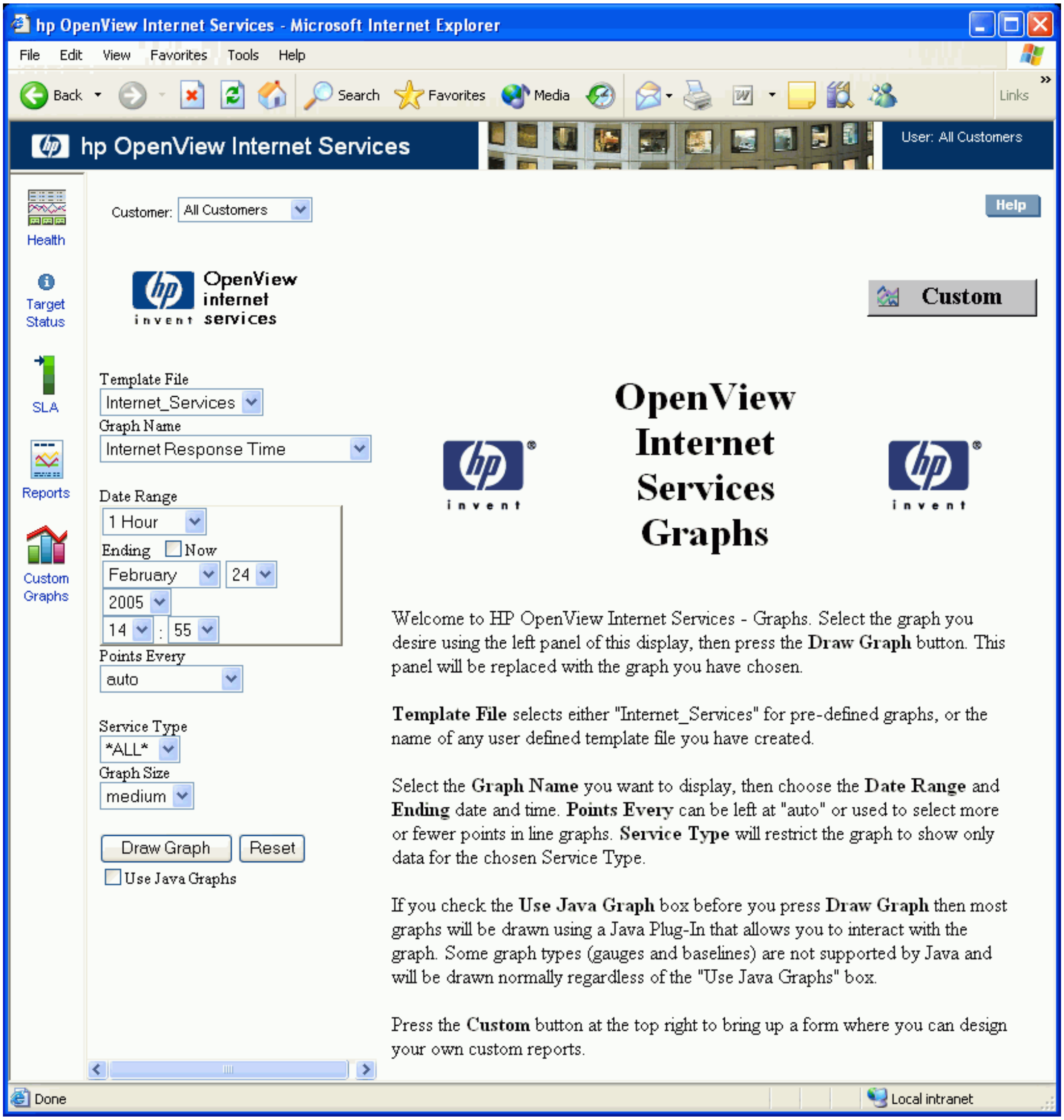
If you have integrated OVIS with OpenView Transaction Analyzer (OVTA) you will see the following reports based on OVTA data imported into OVIS. Refer to the *OVTA User's Guide* for detailed descriptions of each of these reports. See Chapter 5, Integrating with OpenView Products for more information on OVTA integration.

- OVTA Service Group Summary
- OVTA Application Summary of Activity for the Last Day
- OVTA Application Summary of Activity for the Last Week
- OVTA Application Response Time Violations
- OVTA Application Response Time
- OVTA Application Transaction Volume
- OVTA Application Response Time Violations (Consumer Perspective)
- OVTA Application Response Time Violations (Consumer/System Detail)
- OVTA Application - Worst Performing Transactions

See Removing Unused OVIS Reports (Optional) on page 314 for how to remove OVTA report templates if you are only using OVIS for OVTA data.

Custom Graphs Workspace

Use the Custom **Graphs** workspace to draw additional graphs. If you use the custom graphs function, you can create your own graphs based on OVIS data.



hp OpenView Internet Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media Links
hp OpenView Internet Services
User: All Customers
Health
Target Status
SLA
Reports
Custom Graphs
Help
OpenView internet services invent
Custom
OpenView Internet Services Graphs
invent
Done
Local intranet

Customer: All Customers

Template File: Internet_Services

Graph Name: Internet Response Time

Date Range: 1 Hour

Ending □ Now

February 24

2005

14 : 55

Points Every: auto

Service Type: *ALL*

Graph Size: medium

Draw Graph Reset

□ Use Java Graphs

Welcome to HP OpenView Internet Services - Graphs. Select the graph you desire using the left panel of this display, then press the **Draw Graph** button. This panel will be replaced with the graph you have chosen.

Template File selects either "Internet_Services" for pre-defined graphs, or the name of any user defined template file you have created.

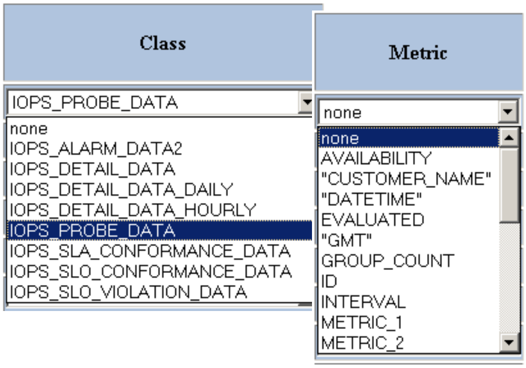
Select the **Graph Name** you want to display, then choose the **Date Range** and **Ending** date and time. **Points Every** can be left at "auto" or used to select more or fewer points in line graphs. **Service Type** will restrict the graph to show only data for the chosen Service Type.

If you check the **Use Java Graph** box before you press **Draw Graph** then most graphs will be drawn using a Java Plug-In that allows you to interact with the graph. Some graph types (gauges and baselines) are not supported by Java and will be drawn normally regardless of the "Use Java Graphs" box.

Press the **Custom** button at the top right to bring up a form where you can design your own custom reports.

Note that within the Graphs display, if you select the **Custom** button and then select the **Help** button, you can see the metrics stored in the various OVIS database tables along with metric descriptions. The example below shows the OVIS data classes you can graph and some of the metrics.

.



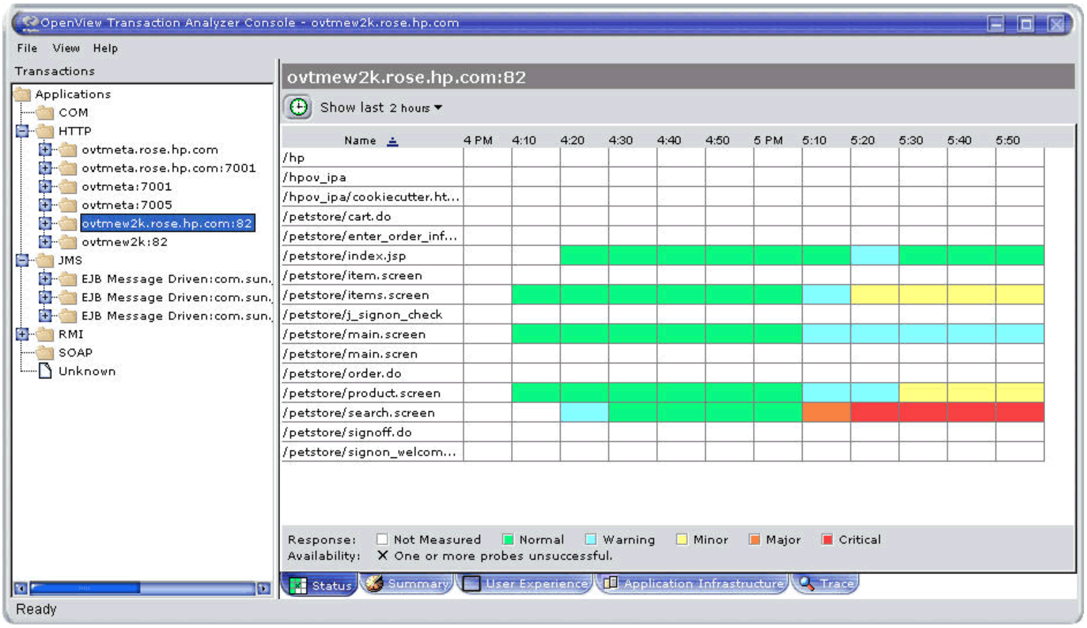
OVTA Workspace

If you have integrated OVIS and OpenView Transaction Analyzer (OVTA) then in the Workspace pane of the OVIS Dashboard, you will see the link to the OVTA Console.

When you select this link, a page is displayed with information about having to have Java Web Start installed in order for the OVTA application to launch. It includes information about how to download it if you don't have it. Select the Launch OVTA Console button to launch the OVTA Console with the Status tab displayed.

Note that you can also launch the OVTA console from a similar icon for each OVTA target's alarms displayed in the Alarms tab. Here it is in the context of the alarm.

See Chapter 5, Integrating with OpenView Products for information about OVTA integration.



OpenView Transaction Analyzer Console - ovtmew2k.rose.hp.com
File
View
Help
Transactions

- Applications
  - COM
  - HTTP
    - ovtmeta.rose.hp.com
    - ovtmeta.rose.hp.com:7001
    - ovtmeta:7001
    - ovtmeta:7005
    - ovtmew2k.rose.hp.com:82
    - ovtmew2k:82
  - JMS
    - EJB Message Driven:com.sun.
    - EJB Message Driven:com.sun.
    - EJB Message Driven:com.sun.
  - RMI
  - SOAP
  - Unknown

ovtmew2k.rose.hp.com:82

Show last 2 hours

Name	4 PM	4:10	4:20	4:30	4:40	4:50	5 PM	5:10	5:20	5:30	5:40	5:50
/hp												
/hpov_ipa												
/hpov_ipa/cookiecutter.ht...												
/petstore/cart.do												
/petstore/enter_order_inf...												
/petstore/index.jsp			🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟩	🟩	🟩
/petstore/item.screen												
/petstore/items.screen		🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟨	🟨	🟨	🟨
/petstore/j_signon_check												
/petstore/main.screen		🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟦	🟦	🟦	🟦
/petstore/main.scren												
/petstore/order.do												
/petstore/product.screen		🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟦	🟨	🟨	🟨
/petstore/search.screen			🟦	🟩	🟩	🟩	🟩	🟧	🟥	🟥	🟥	🟥
/petstore/signoff.do												
/petstore/signon_welcom...												

Response: □ Not Measured 🟩 Normal 🟦 Warning 🟨 Minor 🟧 Major 🟥 Critical
Availability: X One or more probes unsuccessful.

Refer to the *OVTA User's Guide* for more information about the OVTA Console.

Uninstalling Internet Services

To uninstall Internet Services:

1. Stop the Internet Services components listed below. For example, on Windows 2000, select **Start > Settings > Control Panel > Administrative Tools > Component Services**. In the Component Services window, select the **Services** folder. In the service list displayed, right-click on each service to be stopped and select **Stop**.

   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 **Change** to uninstall the HP OpenView Internet Services product.

3. You should also uninstall any OVIS patches via Add/Remove Programs, even those from previous releases.

4. To uninstall remote probes see Installing and Removing Remote Probe Software on page 159.

When the OVIS uninstall script removes OVIS and TIPs, it does not remove the file that contains the defined TIPs in the TIPs Configuration program. The file name and location are as follows:

```
<data_dir>\datafiles\tips\database\SavedTIPsConfig.xml
```

If you reinstall on this same system, you can re-import your TIPs definitions from the `SavedTIPsConfig.xml` file. If you do not want to use these TIPs definitions, delete the `SavedTIPsConfig.xml` file before you reinstall OVIS on the same system.

You can use your TIPs definitions on multiple OVIS systems. See the TIPs Configuration program online help for more information.

3

Configuring Internet Services

Topics covered in this section are as follows:

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) such as availability or response time.
- the **probe location**: where you plan to run the probe (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.

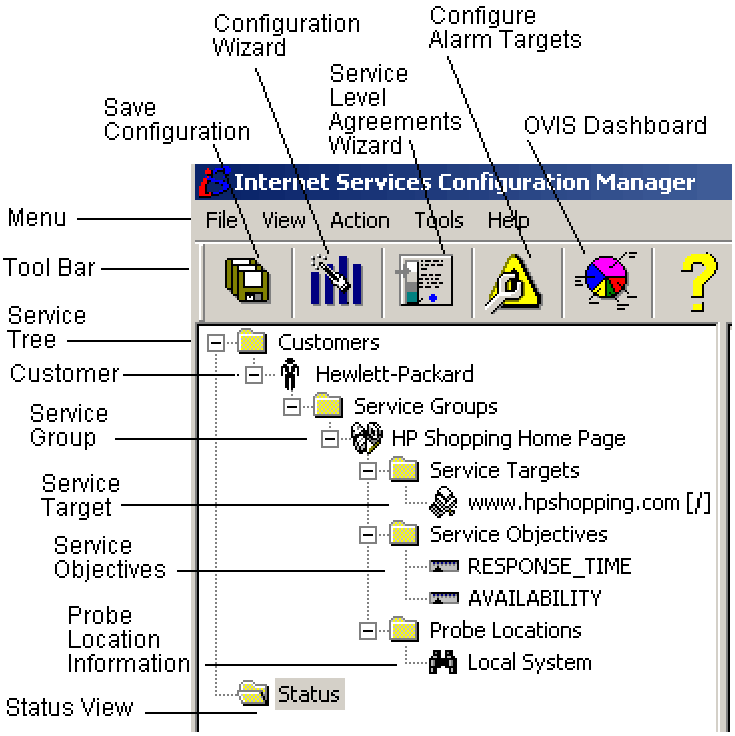
You can configure these services, manually using the **Configuration Manager** (see the sections below). Or you can use the **Configuration Wizard** to step you through setting up services for monitoring by probes.

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 173).

Configuration Manager

You can use the Internet Services Configuration Manager to add, modify and delete services and configure probes for these services. This includes setting up: customers, service groups, service targets, service level objectives, probe locations and service level agreement conformance levels.

To open the Configuration Manager window, select **Start > Programs > HP OpenView > Internet Services > Configuration Manager**.



Multiple users can be logged into the Configuration Manager at the same time. Use the **File > Configure > Multiple User Options** dialog box to set whether you want to turn on locking so that when one user is adding/updating/deleting an item, other users are temporarily locked from making changes. See Other Configuration Options on page 96 for additional requirements for the Multiple User locking feature.

The Configuration Manager has 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.

You can use copy and paste within the Service Tree to add items from one customer/service group/target to another. There is also a rename utility you can run to rename customers or service groups. The `OvisDataRename` program is found in the `<installdir>\bin` directory. After running this utility, the configuration file will be updated to the new Customer or Service Group name and all the data collected in the database will be changed to this new name. Note that a number of messages will be displayed as the rename takes place. Respond to each message in order to continue the rename operation. See the online help for details.

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 configuring probes by defining 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. And you can access the **Online Help** for 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 probe for a service, 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 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.

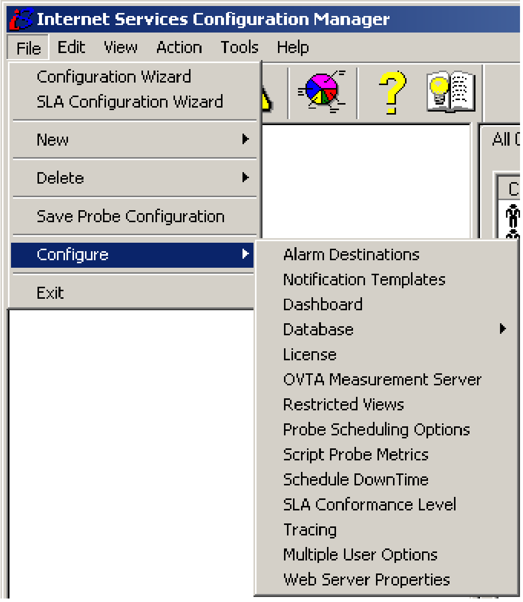
6 Save the configuration changes and exit the Configuration Manager. For remote probes, you also need to be sure the probe software is installed on the remote system. Then probe configuration files are distributed to the remote systems.

See Quick Start for Configuring Internet Services on page 43 for an 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.

➤ In the Configuration Manager Service tree display in the left pane, you can use copy (**Ctrl-C**) and paste(**Ctrl-V**) to add items such as Service Level Objectives. You can also select copy and paste from the **Edit > Copy** and **Edit > Paste - Service Targets** menu selections.

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.

  Also note that in order for alarms to be displayed in the dashboard, the Alarm Targets, Database checkbox must be checked in the Configuration Manager.

- Notification Templates - Create templates for notifications when there is an alarm. Notification can be by email or can be the execution of an external command.

- Dashboard Settings - Configure default setting for the OVIS Dashboard such as what you want the default time span to be for the data display. For the Dashboard health icons you can configure defaults for the minimum and maximum service level violation values and define the percentages where the icon changes from one severity (red, yellow, green color) to another.

Also configure when a target displays status of yellow or red by defining how many intervals where the target is unavailable will trigger a change in status to yellow or red (for example, if unavailable for 2 - 4 intervals show the status as yellow).

- Database - Configure the database login and options for retaining data in the database.
- License - View license data, run the License Wizard to get license keys and import a license you receive in e-mail directly into OVIS.
- 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, and test the connection.
- Restricted Views - Limit access to data in the OVIS Dashboard by customer. Also Profiles can be set up for access to multiple customers or access only to select service groups under a customer, or any combination of these.
- 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).
- Script Probe Metrics - Load a customized script probe SRP file to allow the probe to collect additional metrics you define.
- Schedule DownTime - Configure a new downtime value that can be applied to services.
- SLA Conformance Level - Define service level agreement conformance levels such as Gold = 95%. These levels can be applied to SLAs.
- Tracing - Specify more detailed server or probe tracing for use in troubleshooting. Also specify trace file size for server or probe system.
- Multiple User Options - Specify if you want the Configuration Manager to use locking if multiple users attempt to add/edit/delete/save items in the configuration concurrently. Note that if someone is using a wizard like the configuration wizard, a global lock is used so not much else can be done by any other user. The default is not to use locking, which means that multiple users can be logged into the Configuration Manager and make changes concurrently that may result in changes being overwritten.

It is important to note that for Windows 2000 systems, this locking feature requires Service Pack 4 or later. It does not work with Windows 2000 Service Pack 3.

In addition, this locking feature requires that users running the Configuration Manager or using the batch configuration have the Create Global Objects security privilege set. This is set in the Local Security Policies in the Control Panel as follows: In the Control Panel, go to **Administrative Tools > Local Security Policy**. Then expand **Local Policies > User Rights Assignment** in the left pane. Double-click **Create Global Objects** in the right pane. Add users and groups as needed to this policy. If the Create Global Objects security privilege is not set, and you turn on locking, everything will be locked, so no changes can be made.

If for some reason, you get into a state where things are not getting unlocked, just turn off locking to release all the locks. If this doesn't work, close all instances of the Configuration Manager (`IopsConfig.exe`) and the batch configuration (`IopsLoad.exe`) to release all locks.

- Web Server Properties - Configure communications between server and probe systems and configure ports.

See the online help for more information on these items.

Also in the Configuration Manager you can select the following items from the Tools menu:

- **Tools > Probe Info** to get a report of how many service targets you have set up.
- **Tools > Find Item** to locate a particular item in the Service Hierarchy.
- **Tools > Mass Target Update** to do a mass update of a parameter like password, over a number of service targets.

Running Configuration Manager as a Non-Administrator User

The configuration manager requires local Administrator capability to install a permanent or trial extension license. Running as local Administrator will also provide all the necessary capabilities, permissions, and security to successfully execute.

If you wish to run the configuration manager as a non-Administrator, perform the following steps. Steps 4 through 5 may need to be repeated after any OVIS patch, hot fix, or update is applied since these can apply new files or registry entries that may not have the appropriate permissions.

1 Be sure you have installed any required licensing as Administrator.

2 If you wish to run the Configuration Manager with Multiple User Options turned on (**File > Configure > Multiple User Options)**, grant each user **Create Global Objects** (**Control Panel > Administrative Tools > Local Security Policy > Local Policies > User Rights Assignment**).

3 As Administrator, configure Probe Scheduling Options not to restart the probes after save. To do this, run the Configuration Manager and select **File > Configure > Probe Scheduling Options** to bring up the Schedule-Network Options dialog. Check the box under Local Scheduler specifying **Do Not Restart Probes After Save** and select the **OK** button.

4 Add Modify permission for each user to the following directories as described below:

`C:\Program Files\Common Files\Hewlett-Packard\HPOvLIC`

`<OVIS install directory>`
(By default this is `C:\Program Files\HP OpenView`).

> ➤ If the OVIS data directory is a subdirectory of the OVIS install directory, skip the directory below.

`<OVIS data directory>`
(By default this is `C:\Program Files\HP OpenView\Data`).

Users can be added into a directory's security as follows:

a Execute Windows Explorer, right-click the desired directory and select **Properties**. Select the **Security** tab, then press the **Add** button to bring up the Select User or Groups dialog.

b Select the desired **Look in** group and User name. Click the **Add** button to bring it down into the lower pane, and press **OK**.

c This will bring you back to the Data Properties dialog, where you can click the **Allow** box for Modify. Be sure to have the **Allow inheritable permissions from parent to propagate to this object** box checked, and then click **OK** to assign the permission to that user.

5. Give each user **Read** and **Full Control** permissions to the `HKEY_LOCAL_MACHINE>SOFTWARE>Hewlett-Packard>Internet Services` hive.

   To accomplish this, run `regedt32` from the **Start > Run** window. Expand `HKEY_LOCAL_MACHINE > SOFTWARE > Hewlett-Packard`, then select `Internet Services`. From the regedt32 menu bar select **Security > Permissions...** to bring up the Permissions for Internet Services dialog. Select the desired user, and check the **Allow** box for both Read and Full Control permissions. Then click the **Apply** button.

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

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

Configuring Service Level Objectives and Alarms

When you set up a service group, you can establish an expected service level objective (SLO) for such measurements as availability or response time, for the group.

An SLO defines desired availability or performance levels for a service (based on metrics such as response time). For example: Availability = 95%, or Response Time = 5 seconds. When a probe monitors a particular service target, it collects data on these metrics and the metric values are compared to the SLO. For example, if the probe finds the response time is 10 seconds when the SLO is 5 seconds, an SLO violation is recorded. SLO violations are tracked and displayed in the Dashboard SLO Tab. In addition, alarms can be sent to OVO or NNM based on alarm threshold violations. The rest of this section give more details on SLOs and alarm generation.

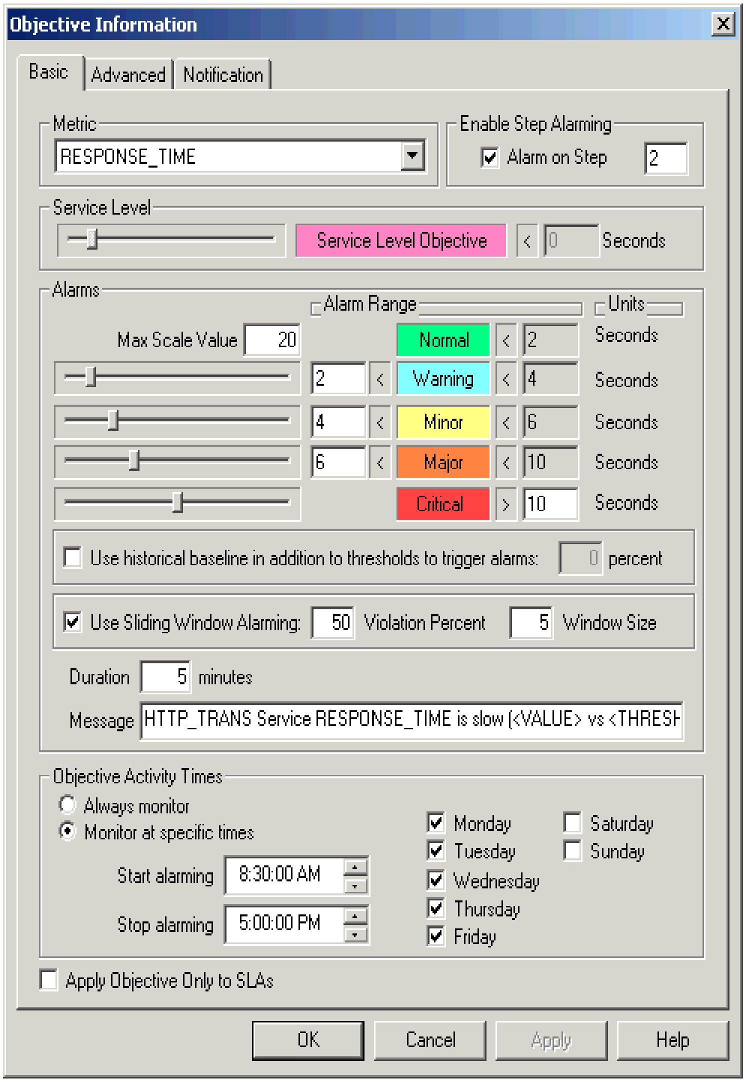
You can also set up Service Level Agreements (SLAs). An SLA is basically a combination of a number of service level objectives (SLOs). You then can set up conformance levels for the SLA, such as Gold = 95% conformance which can be applied by customer. Conformance to an SLA is displayed in the Dashboard SLA tab. See Setting Up Service Level Agreements (SLAs) on page 135.

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 the process of configuring SLOs and alarm thresholds by providing the Objective Information dialog with three tabs:

- **Basic** tab is used to set service level objectives and define basic alarms.
- **Advanced** tab is used to specify alarm expressions (rather than alarms based on a single metric value).
- **Notification** tab is used to set up objective notifications for an alarm.

Setting Up Basic Service Level Objectives and Alarms



Metric: RESPONSE_TIME

Enable Step Alarming: ☑ Alarm on Step 2

Service Level: Service Level Objective < 0 Seconds

Alarms

Max Scale Value 20

Alarm Range					Units
		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: 0 percent

☑ Use Sliding Window Alarming: 50 Violation Percent 5 Window Size

Duration 5 minutes

Message HTTP_TRANS Service RESPONSE_TIME is slow (<VALUE> vs <THRESH

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

□ 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, OpenView Operations for Windows and other event managers that accept SNMP.

In addition, if you want alarms to be displayed in the OVIS Dashboard you must set the **Database (Alarms and NNM Integration)** checkbox in the Configure > Alarm Destinations dialog in the Configuration Manager.

See Send Alarms on page 127 for more information on the Alarm Destinations dialog.

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.

Metric section:

In the Metric section, select the desired metric.

Step Alarming:

Note that you can specify Step Alarming. Check this box if you want to enable alarming on an individual step in a web transaction (HTTP_TRANS Probe), Script probe or Custom Probe. Step alarming only applies to alarms so once you check this box, the SLO fields are grayed out.

Enter the number of the step. The default is -1, which indicates alarms are for the total transaction. To select a step, you can enter any numeric values starting with 0. Steps start at 0. You can only select a single step per set of alarms. To create alarms for several individual steps in a transaction, create a separate alarm definition for each. You can use the same metric in multiple sets of alarm definitions. Step Alarming is for use with Response Time metrics not Availability. This is because Availability is determined for the whole transaction; if any step is unavailable then the transaction is marked as unavailable.

The step number is displayed in the Dashboard drill-down page and in the Status page drill down in the Configuration Manager.

Service Level section:

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. And used in determining Service health. Service level settings are *not* used for generating alarms.

Alarms section:

- **Alarm Range:** 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 mean a warning for response times of 3, 4 and 5 seconds.

➤ 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.

- **Use historical baseline...:** When unchecked, it is not used for alarms. Check this box 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. See How Baselines Work on page 119.

  ➤ Note that this baseline value is only used in determining when alarms are triggered, it is not applied to the Baseline graph in the Dashboard.

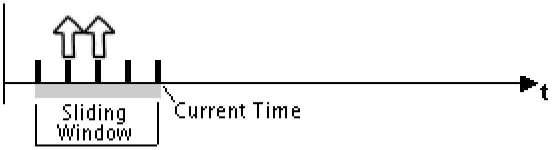
- **Sliding Window Alarming:** Sliding window alarming can be used to reduce false alarms and only alarm if there is a persistent problem within a given time window. Check this box to have an algorithm applied to suppress jittery alarms.

  The sliding window is defined as a specified number of probe measurements. So for example you enter a Window Size of 5 measurement samples. The algorithm will then keep the specified number of samples in memory. As new samples are logged, the window slides forward, always keeping the specified number of measurements in memory. The number of non-normal alarms is compared to the number of samples in the window to calculate a percentage. This percentage is compared against the specified Violation Percent. If the calculated percentage is higher or equal to the Violation Percent, an alarm is triggered.

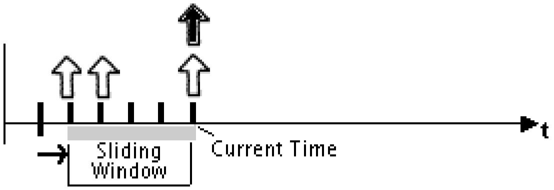
Note that after startup, you have to wait for the number of samples specified in Window Size, before any violation percentage calculation is performed.

For example, if the Window Size is 5, and the first 5 probe measurements resulted in alarm threshold violations, the alarm would be generated at the fifth violation.

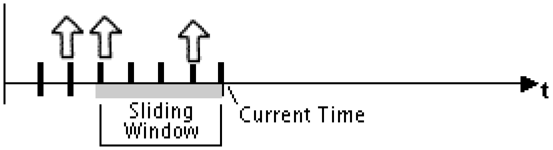
The following graphs illustrate the use of a sliding window alarming. In the examples, 5-minute measurements are shown as vertical black bars. The sliding window is shown as a horizontal gray bar. The Window Size is 5 samples. The current time is shown and the alarm threshold violations are shown as white arrows. Actual alarms are shown as black arrows. The Violation Percent for generating alarms within the sliding window is defined as 50%.



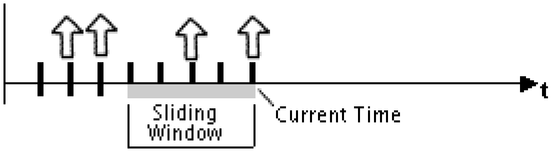
In the figure above, the sliding window contains the last 5 samples. Two violations occur, each marked by a white arrow. The percentage of violations occurring within the window is calculated as the number of non-normal alarms/number of samples in the window (2/5 = 40%). 40% is less than the 50% Violation Percent, so no alarm is triggered.



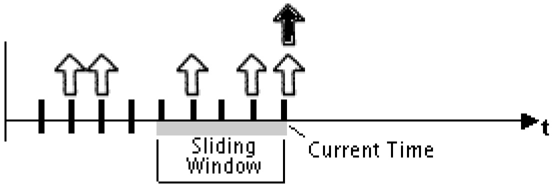
In the figure above, the sliding window has shifted over 5 minutes to include the latest 5 samples. A new violation occurs, shown as a third white arrow. The window now contains three violations. The percentage of violations occurring within the window is 3/5 = 60%. This is above the 50% Violation Percent and therefore an alarm is triggered (shown as a black arrow).



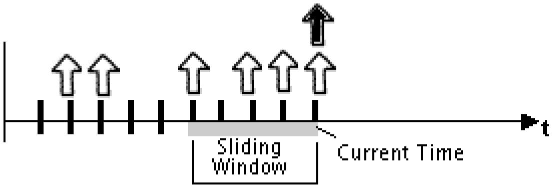
In the figure above, the sliding window has shifted over again and one violation has rolled outside the window. There are now only two violations within the window. The resulting violation percentage is 2/5 = 40%. The alarm state returns to normal and a normal alarm is sent. If you've configured Suppress Normal Alarms in the **File > Configure > Alarm Destinations** dialog box, then no alarm will be sent. See Send Alarms on page 127 for more on the Alarm Destinations.



In the figure above, another alarm threshold violation occurs, but there are only two violations within the window, so no alarm is triggered.

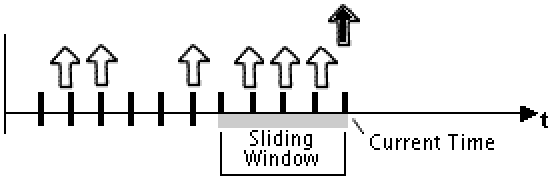


In the figure above, the violation continues. There are now three alarm threshold violations in the window, so an alarm is triggered.



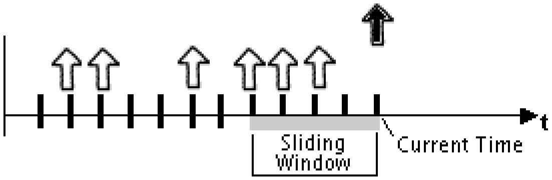
In the figure above, the violation continues. There are now four alarm threshold violations in the window and if “continuous alarming” has been specified, a new alarm is triggered. The value for Continuous Alarming is set in the **File > Configure > Alarm Destinations** dialog box.

The two examples below show that if a lot of alarm threshold violations occur within a window, it will take some time until the alarm state returns to normal because the violations require some cycles before they roll out of the window. So you see that as long as three violations are within the window a new alarm will be triggered at the current time.



In the figure above, the window still contains three violations, so an alarm is triggered (if continuous alarming is specified) even though there is no violation in the current sample.

And in the next interval, shown below, there are still three violations, so an alarm is again triggered. When the sliding window shifts over once more, the alarm state can return to normal.



- **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.

- **Message:** You can enter a textual description of the alarm event and provide information captured from that alarm event that can be sent to NNM or OVO along with the alarm notification. The Message is only used with alarm definitions it does not affect the Service Level Objective in any way. To include data captured from the alarm event into a message, add special key words to your message. See Alarm Message on page 124 for a list of key words for use in alarm messages.

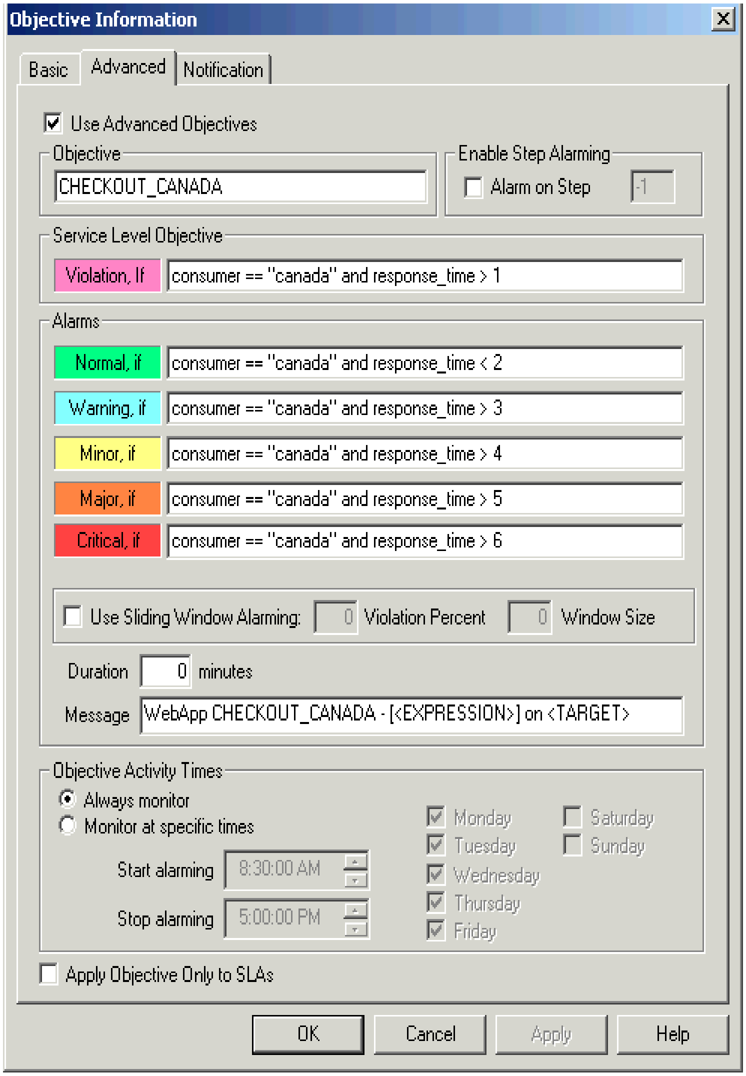
Objective Activity Times section:

You can filter the time periods you would like to alarm by activity time. This is useful to avoid false alarms during times when objectives are not expected to be met, such as during backups.

SLA Objective section:

Check the SLA Objective 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

Setting Up Advanced Service Level Objectives and Alarms



☑ Use Advanced Objectives

Objective: CHECKOUT_CANADA

Enable Step Alarming: □ Alarm on Step -1

Service Level Objective

Violation, If: consumer == "canada" and response_time > 1

Alarms

Normal, if: consumer == "canada" and response_time < 2

Warning, if: consumer == "canada" and response_time > 3

Minor, if: consumer == "canada" and response_time > 4

Major, if: consumer == "canada" and response_time > 5

Critical, if: consumer == "canada" and response_time > 6

□ Use Sliding Window Alarming: 0 Violation Percent 0 Window Size

Duration 0 minutes

Message: WebApp CHECKOUT_CANADA - [<EXPRESSION>] on <TARGET>

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

□ Apply Objective Only to SLAs

Use this dialog to define expressions for service level objectives and alarms. Expressions allow SLO and alarm conditions that combine multiple metrics (multivariable SLO/alarm) for a particular probe. For example, response_time > 100 and transaction_rate > 10000. It is primarily for use with OVTA metrics.

To use expressions, switch to the Advanced Objectives Information tab and check the box for Use Advanced Objectives. Enter a name for the objective you are defining. This label will be shown in the OVO and NNM integration.

Note that for an advanced objective, the metrics that are part of the objective are not colored in the Dashboard drill down display. Also note that for advanced objectives the expression must be written so that it is true if metric values are outside the service level objective. For example, the service level is violated if RESPONSE_TIME > 2. This is different than the basic objective where the logic is reversed. For example, the service level requires that RESPONSE_TIME <= 2.

You would typically use the OVTA application performance metrics in these expressions. The metrics are described in List of Metrics by Probe Type on page 281. You can use any metric in this list except AVAILABILITY. Expressions are only evaluated if the probe is available, therefore it would not make sense to add an AVAILABILITY metric into an expression. Even with a basic Availability objective, if the probe returns unavailable, any other objectives are not evaluated.

The evaluation order for alarm expressions starts with the highest severity: Critical, Major, Minor, Warning. If the evaluation returns true for one of these severities, the alarm is triggered and no further expressions are checked. If the alarm state is non-normal, the Normal expression is checked first. If it evaluates as true, the alarm state transitions to normal and no other expression is checked. If “suppress normal alarms” is not checked a normal alarm message is triggered.

Note that there is no baseline capability for advanced objectives. The alarm sliding window functionality, if defined, is applied after the expression is evaluated. The duration functionality is applied last.

The Message variable <EXPRESSION> can be used to indicate the expression that triggered the alarm (that is it evaluated as true).

All other fields on this dialog are used the same as the Basic Objective dialog.

SLO/Alarm Expression Syntax

Syntax:

```
Variable | Relational-Operator | Constant | Factor
RESPONSE_TIME > 100 AND TRANSACTION_RATE > 10000
```

```
Boolean-Expression ::= Boolean-Term | Boolean-Term OR Boolean-Expression
Boolean-Term ::= Boolean-Negation | Boolean-Negation AND Boolean-Term
Boolean-Negation ::= Boolean-Factor | NOT Boolean-Factor
Boolean-Factor ::= ( Boolean-Expression ) | Variable | Variable Relational-Operator  Constant
Relational-Operator ::= < | > | == | <= | >= | !=
Variable ::= OVIS Metric
Constant ::= Number | String
Number ::= Floating Point Number
String ::= "{character}+"
```

Parameters:

Variable - OVIS metric specific to the probe type. An OVIS metric is either a string or a floating point number.

Relational-Operator - <, >, ==, <=, >=, != (The relational operators ignore case when matching strings, for example, “OVis” is equal to “ovis”.

Constant - Number, String (Number is a floating point number and String is character and enclosed in quotes).

Factor - AND, OR, NOT

Example:

RESPONSE_TIME > 100 AND CONSUMER == “Probe”

RESPONSE_TIME > 100 AND TRANSACTION_RATE > 10000

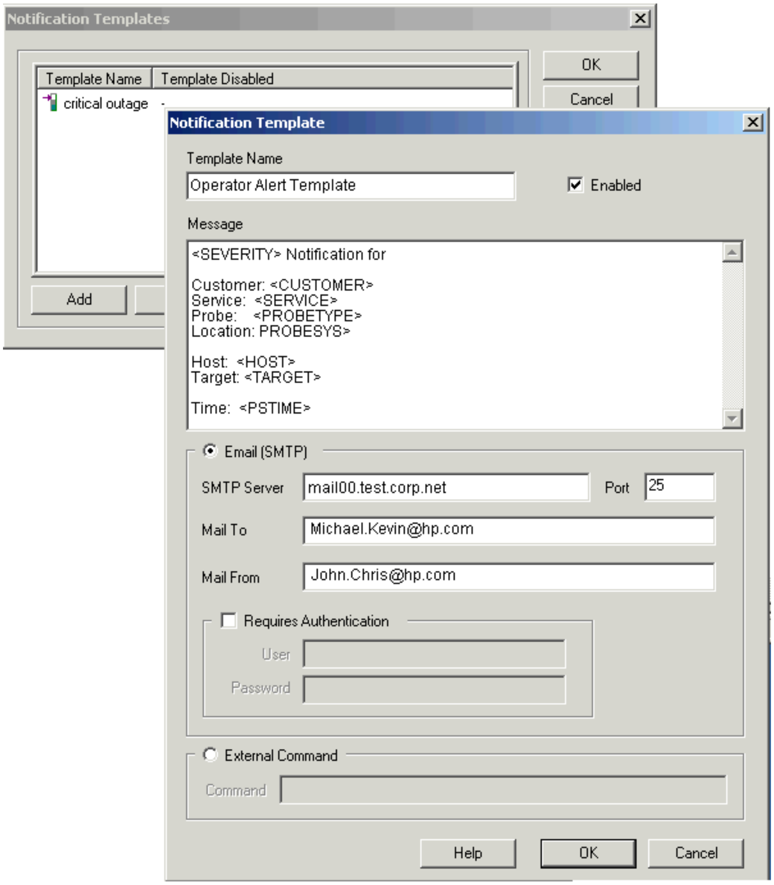
Error Handling:

String and Numbers (floating point) are supported. Comparing terms of invalid types will be noted as an error.

Setting Up Notifications

You can create a template for notifications to be activated when there is an alarm.Then, you use the Objective Information dialog's **Notification tab** to add a notification to an objective alarm (see Add Notification to an Objective Alarm on page 117). You must have some objectives defined in order to add notifications.

Notification can be by email or can be the execution of an external command. In the Configuration Manager, you use the **File > Configure > Notifications** dialog to create notification templates.



Template Name: Operator Alert Template

☑ Enabled

Message:

```
<SEVERITY> Notification for

Customer: <CUSTOMER>
Service:  <SERVICE>
Probe:    <PROBETYPE>
Location: PROBESYS>

Host:  <HOST>
Target: <TARGET>

Time:  <PSTIME>
```

● Email (SMTP)

SMTP Server: mail00.test.corp.net   Port: 25

Mail To: Michael.Kevin@hp.com

Mail From: John.Chris@hp.com

□ Requires Authentication

User:

Password:

○ External Command

Command:

To send an Email (SMTP) notification, you enter information about the email server and the email accounts sending and receiving the email.

Note that if you select Requires Authentication, the User and Password applies to the SMTP Server except in the case of Microsoft Exchange Server. With Exchange, the User and Password is authenticated with the Mail From account.

You can also create the message to be used in the notification. The following keywords can be used in the Message field (they have the same definition as the message field in the Objectives dialog):

<CUSTOMER> The customer name that owns this objective.

<SERVICE> The name of the Service Group to which this objective belongs.

<PROBETYPE> The type of probe measuring the data (HTTP, ICMP, DNS, etc.).

<PROBESYS> The name of the system where the probe was executing.

<HOST> The name of the system that was being measured.

<TARGET> The objective target (URL, hostname, etc.).

<PSTIME> Time (formatted) when a measurement was taken by the probe.

<ERROR_INFO> Probe specific error information returned by the server or protocol and logged by the probe. For example, for HTTP_TRANS probes this may show the step where the failure occurred, the failed pattern or the HTTP status code. See Error Messages and Status Codes on page 387 for additional information.

<VALUE> The value of the metric in this objective at the time of the alarm.

The following keywords are only available in the Notification Template:

<SEVERITY> Severity of the alarm.

<METRICNAME>	Name of the metric (e.g. AVAILABILITY).
<URL>	Drill-down URL to the dashboard.
<MESSAGE>	The formatted alarm message.

If you don’t change anything in the Message field, a default message is provided.

An example of this default message is shown below :

```
Critical Notification for
Customer: Hewlett-Packard
Service:  test http
Probe:    HTTP
Location: mylocation.hp.com
Host:   go.shop
Target: go.shop/
Time:   02/03/05 13:21:28
Metric: AVAILABILITY
Value:  0.000
Error:  [DNS Unable to resolve host (go.shop:80)] [URL] http://
go.shop:80/ [PROXY] (none)
URL:    http://mylocation.hp.com:8080/OvisDashboard/
Controller?action=login&enc=UTF-8&LN0=All&LN1=Hewlett%2dPackard&LN
2=test+http&LN3=go%2eshop/
Message:
HTTP Service for go.shop/ is unavailable ([DNS Unable to resolve
host (go.shop:80)] [URL] http://go.shop:80/ [PROXY] (none) )
Best regards,
  OVIS
```

Note that the message you configure in the notification template only applies when a service level objective alarm is generated. Is it not used for SLA alarms or OVISstatus alarms.

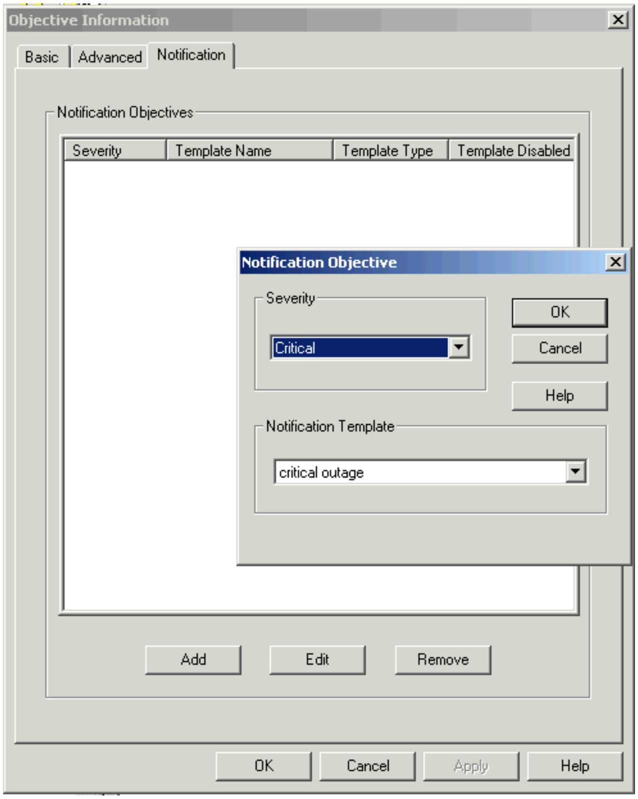
To execute an External Command, the only parameter that gets substituted in the **Command** text field is <CONTENTFILENAME>.

The test script example below is responsible for removing the file after processing:

```
Set fsoObject = CreateObject("Scripting.FileSystemObject")

if Wscript.Arguments.Count <> 1 then

  Wscript.Echo "Filename expected"

  Wscript.Quit 1

end if

Rem Log the contents of the passed file

Set fLog = fsoObject.OpenTextFile("c:\\temp\\notifCmd.log", 8,
true)

Set fContentFile =
fsoObject.OpenTextFile(Wscript.Arguments.Item(0), 1)

sContent = fContentFile.ReadAll

fContentFile.close

fLog.Write sContent

fLog.close

Rem The script is responsible for deleting the passed file

fsoObject.DeleteFile(Wscript.Arguments.Item(0))
```

Add Notification to an Objective Alarm

Then, in order for a notification to be sent, you must add the notification to an objective alarm. First select an objective (metric) to edit, then in the Objective Information dialog select the **Notification** tab. You can select the **Add**, **Edit** or **Remove** buttons to select a notification to add, edit a notification or remove an already configured notification for this objective.



Severity: Critical

Notification Template: critical outage

Notifications for Other Types of Alarms (SLA and OVISstatus)

Notifications can also be sent for two other types of alarms: SLA alarms and OVISstatus alarms. When you configure notifications for an alarm based on an SLO that is part of an SLA, an SLA alarm notification message will also get generated automatically. The SLA alarm notification message is based on information in the SLA instead of the message in the template. For example:

```
SLA Conformance Threshold Violated:  SLA: "SLA Failure"
```

`Customer: "http"; Threshold: 95.00  Conformance: 75.00`. Note that SLAs are evaluated hourly and if an SLA alarm with notifications is triggered, the notification will also be sent at this time.

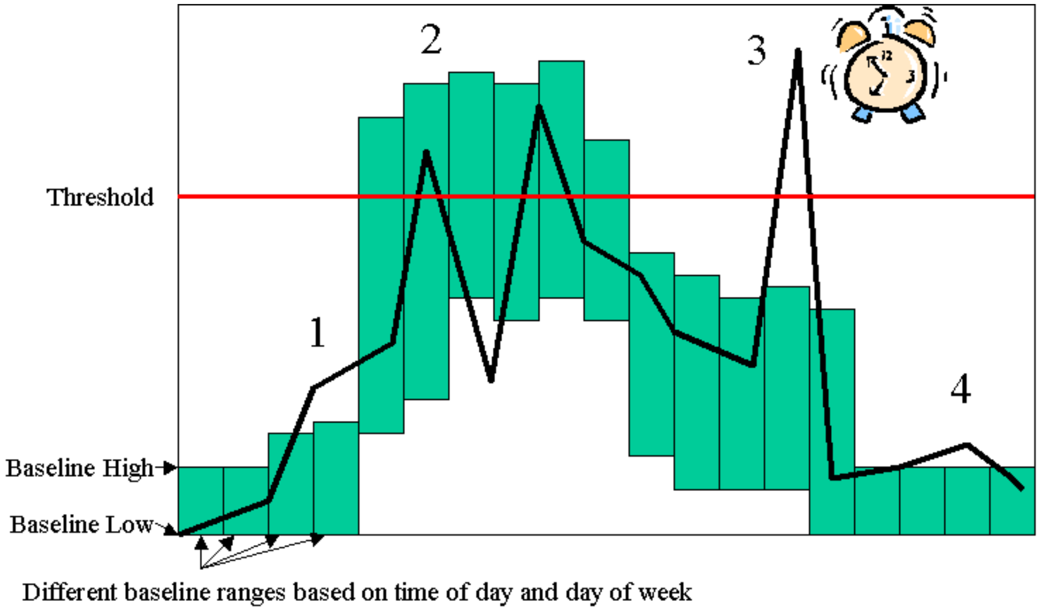
Notifications for OVISstatus alarms are set in the File > Configure > Alarm Destinations dialog. You select a notification template to be used but information from OVISstatus is used in the message instead of the message in the template. For example: `Probe-Server Comm Delay: ovruxd04.test.corp.com (09m:49s)`. Note that OVISstatus runs every 5 minutes and if an OVISstatus alarm with notifications is triggered, the notification will also be sent at this time.

Note that the message you configure in the notification template only applies when a service level objective alarm is generated. Is it not used for SLA alarms or OVISstatus alarms.

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. Note that baselines are available for advanced objectives.

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.



In the example above the alarm threshold for response time is 3 seconds, for a stock trading page. Between 10 AM and 12 PM on Monday the page gets many purchase orders and experiences its peak period (labeled #2 in the diagram above). See the description below for each item labeled 1 - 4 in the example:

1. No alarm event - the response time value is above baseline, but is less than the 3 second threshold.

2. No Alarm event - the response time is above the 3 second threshold, but according to baseline this is normal for between 10 - 12 on a Monday.

3. Alarm event - the response time is greater than the 3 second threshold and is not inside the normal range of the baseline, that is it is no longer a peak time.

4. No Alarm event - response time is above the baseline but less than the threshold.

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
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.

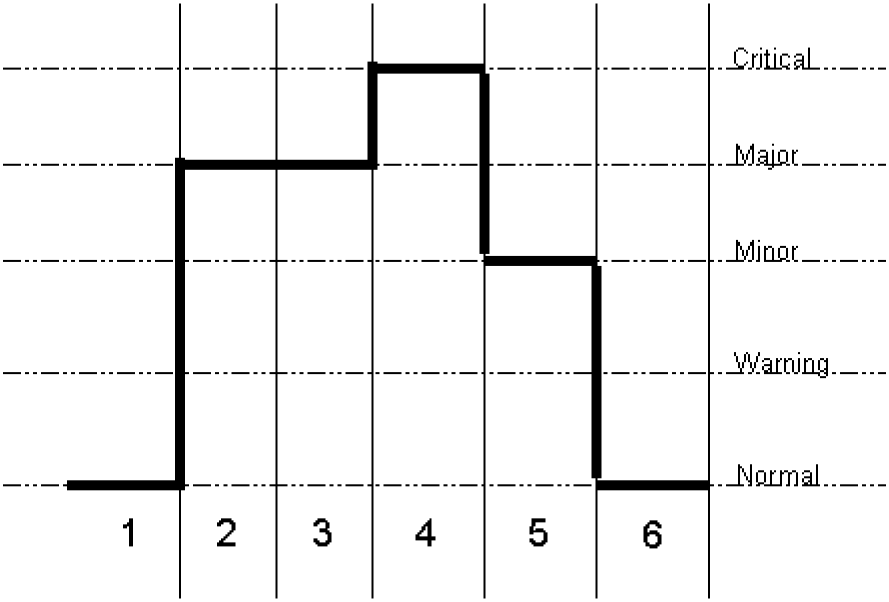
⚠ Caution: When trying to create alarms for test purposes, you should set baselines to off since it may inhibit the alarms you are trying to test.

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 Both Alarm Ranges and 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) 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 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 returns to the NORMAL status and this is the END of the alarm event.

See the example below of the path for an Service Level Objective alarm:



1 NORMAL status (no alarm event sent)

2 MAJOR status (send START event, severity=MAJOR)

3 MAJOR status (send CONTINUE event, severity=MAJOR)

4 CRITICAL status (send START event, severity=CRITICAL)

5 MINOR status (send START event, severity=MINOR)

6 NORMAL status (send END event, severity=NORMAL)

Alarm Message

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

To include data captured from an alarm event 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

Keyword	is replaced with
<ERROR_INFO>	Probe specific error information returned by the server or protocol and logged by the probe. For example, for HTTP_TRANS probes this may show the step where the failure occurred, the failed pattern or the HTTP status code. See Error Messages and Status Codes on page 387 for additional information.
<EXPRESSION>	The alarm expression that triggered the alarm (if this probe supplies it)
<PSTIME>	Time (formatted) when a measurement was taken by the probe.
<PSTS>	Time (number of seconds since 00:00:00 UTC on Jan. 1, 1970) when a measurement was taken by the probe.
<THRESHOLD_SW>	Sliding Window threshold value when a violation occurs.
<RESPONSE_TIME>	The response time metric value (if this probe supplies it)
<AVAILABILITY>	The availability metric value (if this probe supplies it)
<SETUP_TIME>	The setup time metric value (if this probe supplies it)
<THRUPUT>	The throughput metric value (if this probe supplies it)
<THRESHOLD_SW>	Sliding Window threshold value when a violation occurs.
<METRIC1>	Metrics are probe specific. Refer to the List of Metrics by Probe Type in Chapter 4.
<METRIC2>	Metrics are probe specific. Refer to the List of Metrics by Probe Type in Chapter 4.
<METRIC3>	Metrics are probe specific. Refer to the List of Metrics by Probe Type in Chapter 4.
<METRIC4>	Metrics are probe specific. Refer to the List of Metrics by Probe Type in Chapter 4.
<METRIC5>	Metrics are probe specific. Refer to the List of Metrics by Probe Type in Chapter 4.
<METRIC6>	Metrics are probe specific. Refer to the List of Metrics by Probe Type in Chapter 4.

Keyword	**is replaced with**
<METRIC7>	Metrics are probe specific. Refer to the List of Metrics by Probe Type in Chapter 4.
<METRIC8>	Metrics are probe specific. Refer to the List of Metrics by Probe Type 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:

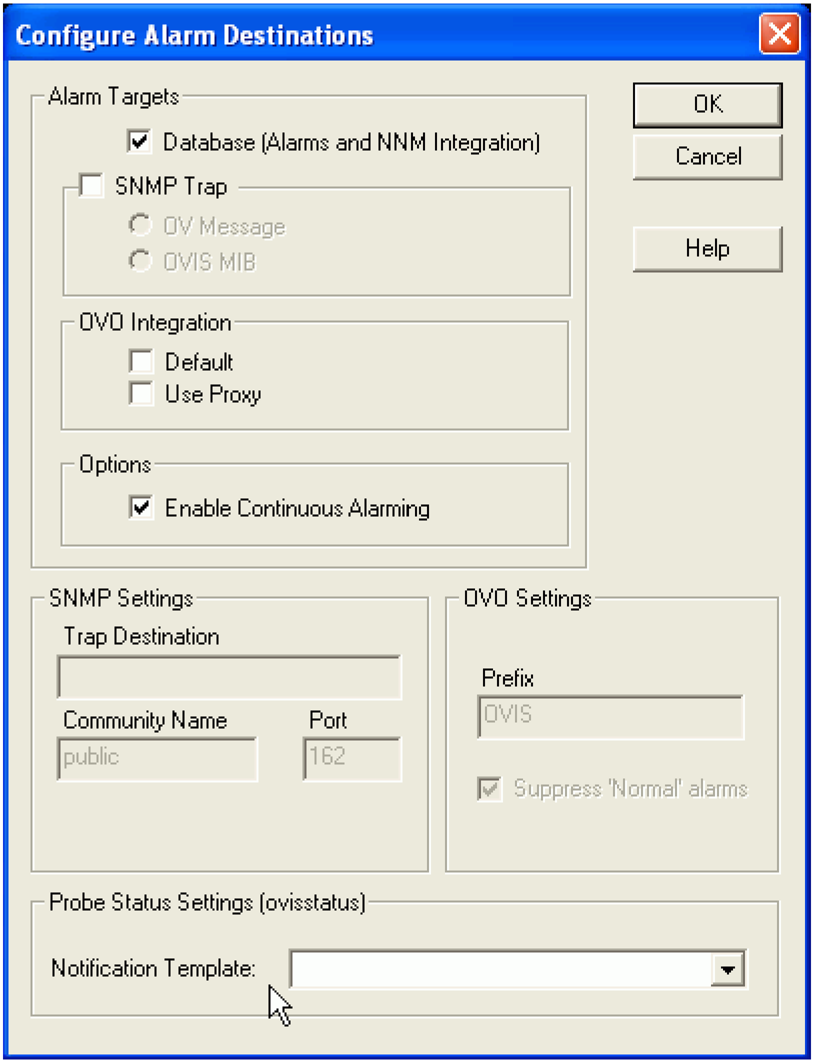
> HTTP response time from **curly.myhouse.com** to **webserver1.yourhouse.com** is 7 seconds (should be < **5.0** or between (**3.2** and **6.5**)

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, OpenView Operations for Windows and other event managers that accept SNMP traps.

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



☑ Database (Alarms and NNM Integration)

□ SNMP Trap

○ OV Message

○ OVIS MIB

□ Default

□ Use Proxy

☑ Enable Continuous Alarming

Trap Destination:

Community Name: public

Port: 162

Prefix: OVIS

☑ Suppress 'Normal' alarms

Notification Template:

➤ Check the **Database (Alarms and NNM Integration)** checkbox if you want alarms to be shown in the OVIS Dashboard.

Also check the **Database (Alarms and NNM Integration)** checkbox to allow one or more NNM agents to pull alarm events from the OVIS database. Network Node Manager does not have to be installed on the OVIS Management Server but must be installed on a system that can access the OVIS Management Server. Special alarm records are written to Internet Services EventDB where they can be retrieved and forwarded to NNM. Internet Services will add icons to system icons in the NNM map to represent the services being monitored. The color of these icons represents the current status of the corresponding service. Note that only services that are configured to be monitored by Internet Services will be populated with service icons.

Check the **SNMP Trap** box to do one of the following:

OV Message - configure OVIS to send each alarm event as a general SNMP (Simple Network Management Protocol Manager) trap. It uses the NNM OV Message trap. Any program registered to receive SNMP traps can then receive this message and process it.

OVIS MIB - Send an SNMP trap defined in the OVIS MIB. The OVIS MIB is located in the `<install dir>\contrib` directory of OVIS and must be uploaded to the SNMP management system.

For **OVO integration**, select either default mode or using a proxy.

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

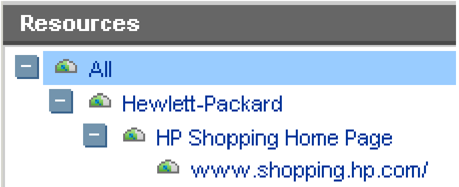
NOTE: When you save changes to any service configuration, IIS is restarted. When IIS is restarted, the last alarm state is saved. This alarm state information is loaded back in at restart so the alarm state is retained.

➤ In addition, the program OVISStatus.exe runs automatically and sends alarms to OVO or NNM if data is not received from the probe system within the expected time + 10 percent, to allow for minor delays. You can assign a notification template to these alarms using the Notification Template field (see Setting Up Notifications on page 113). Notifications can be emails or executing a program.

Configuring the Dashboard

The OVIS Dashboard Health workspace shows a view of the health of the services. Each item (Customer, Service Group, Service Target) has an icon displayed next to it that reflects the health of the service. The thresholds for these icons are customizable in the Configuration Manager (see the following page).

An example of the Dashboard health icons is shown below.



Resources

- All
  - Hewlett-Packard
    - HP Shopping Home Page
      - www.shopping.hp.com/

Status or health is based on percent of service level objectives violated for targets. See Measuring Health Based on SLO Violations on page 130 for details on how health is measured. The icons are defined below:

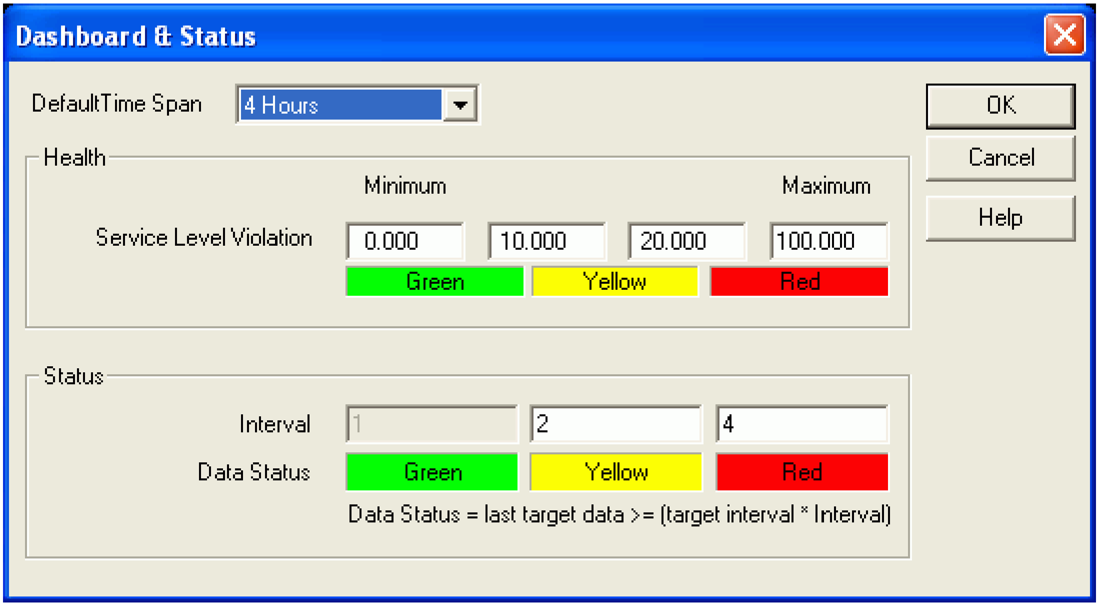
🟥 Red icon indicates that Service Level Violations for the item were by default between 20-100%.

🟨 Yellow icon indicates that the Service Level Violations for the item were by default between 10-20%.

🟩 Green icon indicates that the Service Level Violations for the item were by default between 0-10%.

? The blue icon indicates no probe data received.

Note that the values for the service level objectives violation thresholds for the red, yellow and green health icons can be customized in the OVIS Configuration Manager, **File > Configure > Dashboard** dialog.



DefaultTime Span: 4 Hours

Service Level Violation: 0.000 | 10.000 | 20.000 | 100.000

🟩 Green | 🟨 Yellow | 🟥 Red

Interval: 1 | 2 | 4

Data Status: 🟩 Green | 🟨 Yellow | 🟥 Red

Data Status = last target data >= (target interval * Interval)

This dialog is also used to configure the red, yellow and green thresholds in the Configuration Manager Status display and the Dashboard Target Status workspace.

Measuring Health Based on SLO Violations

Health is propagated up the service hierarchy. The health for the upper level (like customer) is based on the average of the health for the lower levels.

Health = 100% - SLO_VIOLATIONS(%)

SLO_VIOLATIONS(%) = (SLO_VIOLATIONS COUNTS / TOTAL Measurement Samples) X 100

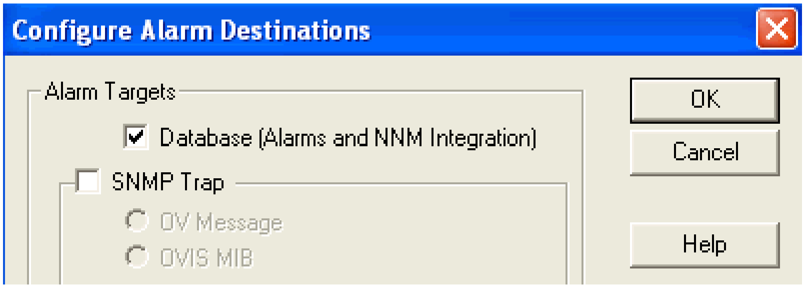
So, the SLO_VIOLATIONS(%) for the upper level is the sum of all SLO violations at the lower level divided by the total counts of the lower level (that is the targets). So if a target has more samples (valid data from the probes), it has more affect on the overall health than the targets with fewer samples (like a new target or a recently diabled one).

Note the following regarding how health is calculated:

- If no service level objectives (SLOs) have been defined, the health icon will be green.
- If some targets for a customer have no SLOs defined, these targets are not computed into overall health for the service group and customer. This is useful for preproduction and test systems, or other systems deemed as not important to overall health but that you do want probe measurements for.
- If, for example, all the SLOs you set up are based on Response Time, then Availability will have no effect on the Health.

Configuring the Dashboard to Display Alarms

Check the **Database (Alarms and NNM Integration)** checkbox in the Configure > Alarm Destinations dialog in the Configuration Manager, if you want alarms to be shown in the OVIS Dashboard.



Configure Alarm Destinations

Alarm Targets

☑ Database (Alarms and NNM Integration)

☐ SNMP Trap

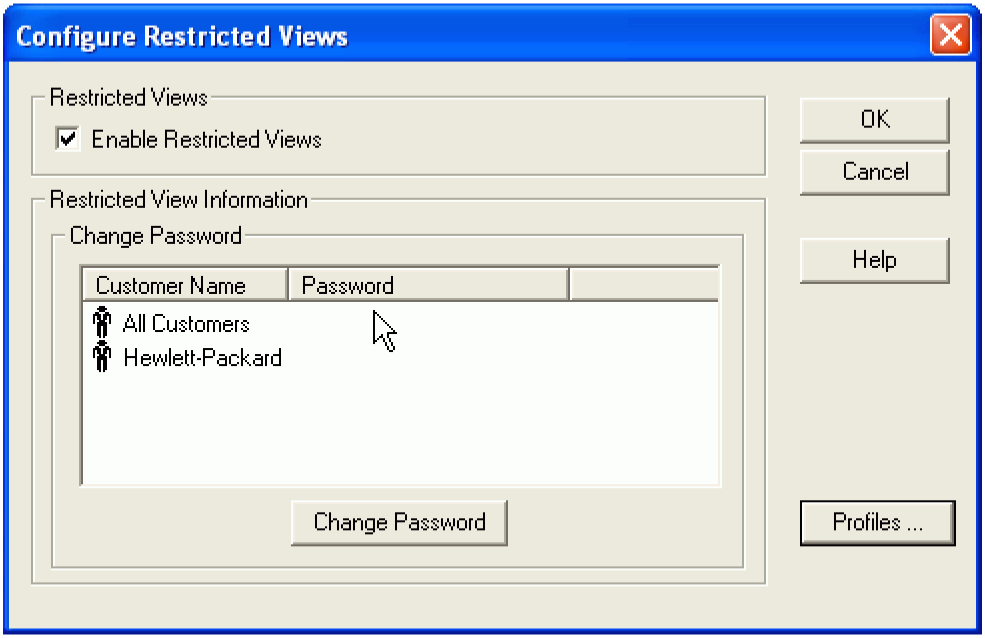
○ OV Message

○ OVIS MIB

Dashboard Login 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 Restricted Views, anyone logging in to the Dashboard must enter a User ID and password to see the Dashboard's main page.



Configure Restricted Views

Restricted Views

☑ Enable Restricted Views

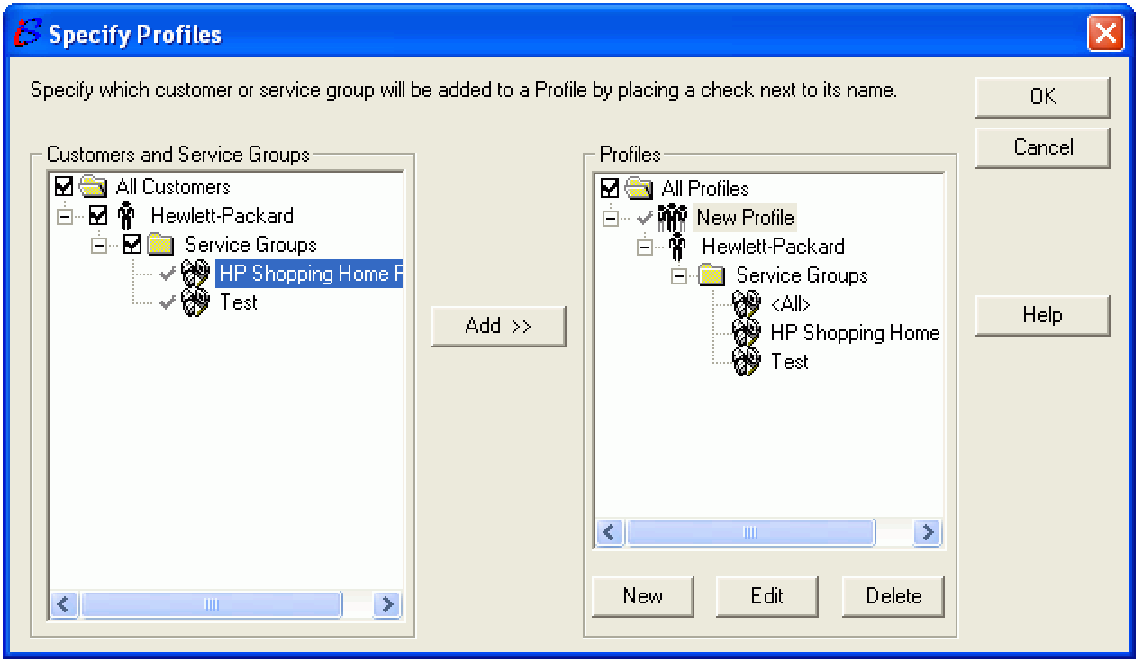
Restricted View Information

Change Password

Customer Name	Password	
All Customers		
Hewlett-Packard		

Note that the User ID and Password can either be a Customer and password or a Profile and password. The Restricted Views feature, limits you to viewing data for a single customer. But Profiles can be set up for access to multiple customers or access only to select service groups under a customer, or any combination of these.

Select the **Profiles** button on the Restricted Views dialog to create a profile. See the screen shot on the next page and refer to online help for the Specify Profiles dialog for details on how to configure Profiles.



Specify which customer or service group will be added to a Profile by placing a check next to its name.

NOTE: If you have a profile with access to only some service groups for a customer, you will NOT be able to access Reports or Custom Graphs in the Dashboard. This is because these components display data by customer and this type of profile doesn't give you access to all the data for that customer. If you have a profile with access to all data for one customer but only some service groups for another customer, you will be able to access Reports and Custom Graphs but will only be able to see data for the one customer where you have access to all service groups.

There is also a superuser/administrator account named **All Customers** that has access to all customers and reports. The superuser account allows anyone using it access to the Dashboard data display that shows data for all customers.

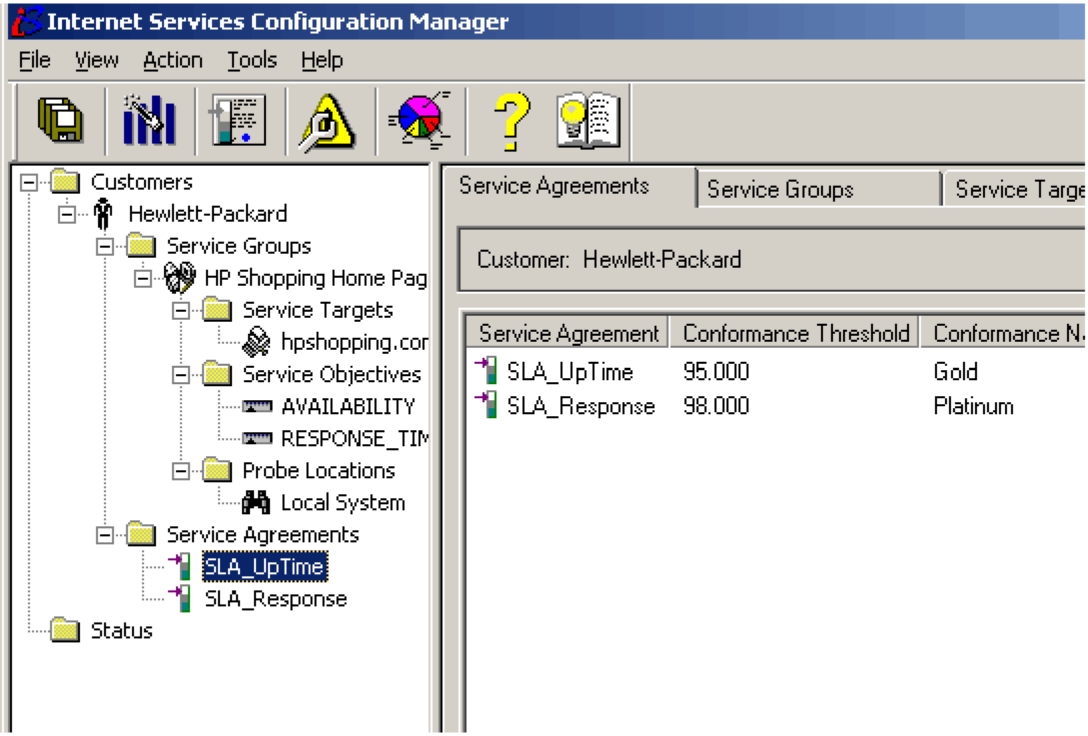
If you have OVIS and OpenView Performance Manager 5.0 (OVPM) installed on the same system and you have restricted view turned on, you will need to sync up the passwords in order for the Custom Graphs display in the OVIS Dashboard to work properly (see Troubleshooting Custom Graphs and Restricted Views on page 367).

➤ The Dashboard is by default accessible from `http://<management server>:8080/OvisDashboard` where <management server> is your OVIS management server and <8080> is your Dashboard port. 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 User ID and password in the Login page that appears.

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 basic idea of an SLA is that you combine a number of service level objectives (SLOs) into a single SLA. Each SLO defines availability or performance (based on metrics such as response time). The combination of SLOs can be a logical expression spanning all service groups that belong to the customer under which the SLA is configured.



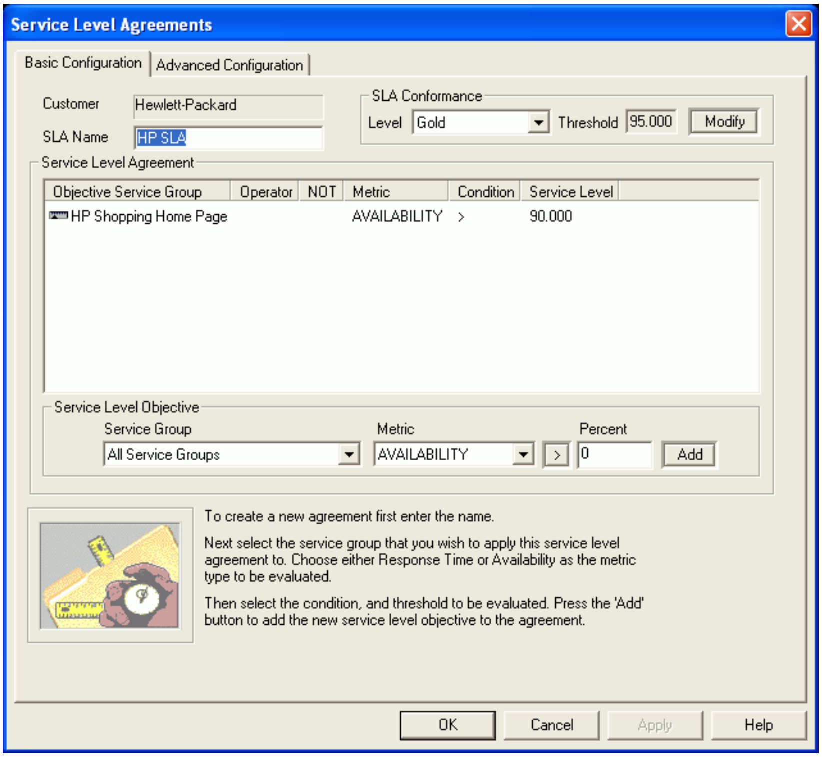
Customer: Hewlett-Packard

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

SLAs are created using either the **SLA Configuration wizard** (accessed from the **File** menu in the Configuration Manager) or by using the SLA Configuration dialog in the Configuration Manager. You set up the SLA for a customer, including the customer's 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 (accessed by right-clicking an SLA and selecting Edit Service Level Agreement) 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. See the online help for details on configuring SLAs.



Customer: Hewlett-Packard

SLA Name: HP SLA

SLA Conformance

Level: Gold   Threshold: 95.000

Service Level Agreement

Objective Service Group	Operator	NOT	Metric	Condition	Service Level
HP Shopping Home Page			AVAILABILITY	>	90.000

Service Level Objective

Service Group: All Service Groups   Metric: AVAILABILITY   >   Percent: 0

To create a new agreement first enter the name.

Next select the service group that you wish to apply this service level agreement to. Choose either Response Time or Availability as the metric type to be evaluated.

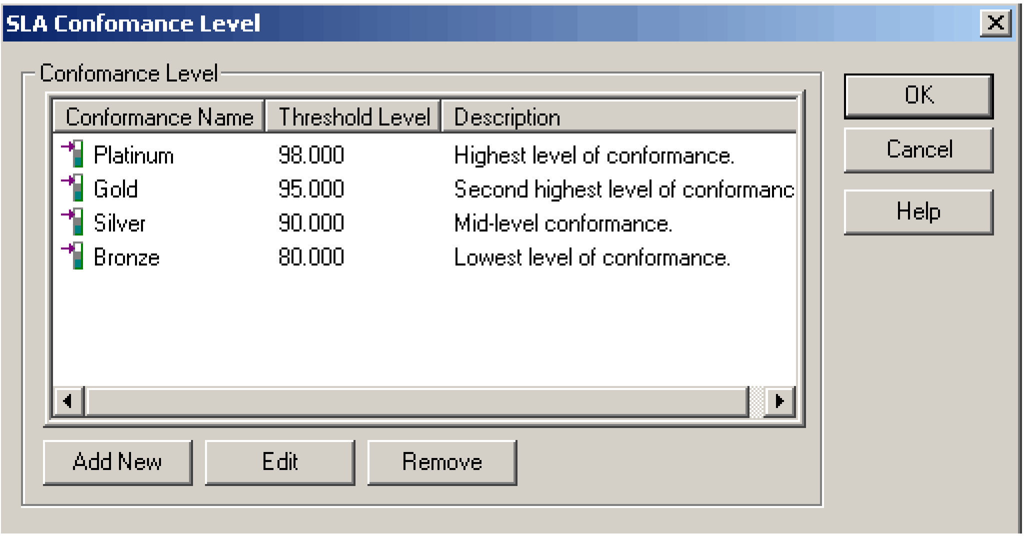
Then select the condition, and threshold to be evaluated. Press the 'Add' button to add the new service level objective to the agreement.

How an SLA is Evaluated

For each SLA, Internet Services evaluates the SLOs in the SLA, 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.

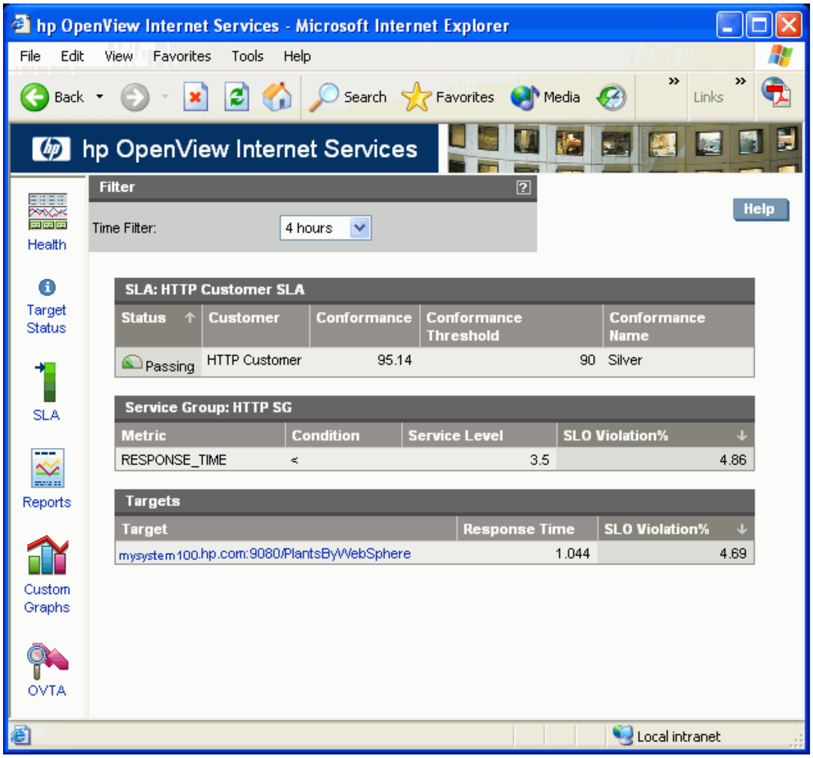
You can also set SLA conformance thresholds in the Configuration Manager **File > Configure > SLA Conformance Level** (for example platinum = 98%, gold = 95%, silver = 90% and bronze = 80%). These are compared with the resulting SLA conformance at each hour. If an SLA does not meet or exceed the SLA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



Conformance Name	Threshold Level	Description
Platinum	98.000	Highest level of conformance.
Gold	95.000	Second highest level of conformanc
Silver	90.000	Mid-level conformance.
Bronze	80.000	Lowest level of conformance.

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.

SLA conformance is reported in the OVIS Dashboard. From the main page select the SLA icon in the Workspace pane. See SLA Workspace on page 81 for more information.


hp OpenView Internet Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Links
hp OpenView Internet Services
Health
Target Status
SLA
Reports
Custom Graphs
OVTA
Help
Local intranet

Filter

Time Filter: 4 hours

SLA: HTTP Customer SLA

Status	Customer	Conformance	Conformance Threshold	Conformance Name
Passing	HTTP Customer	95.14	90	Silver

Service Group: HTTP SG

Metric	Condition	Service Level	SLO Violation%
RESPONSE_TIME	<	3.5	4.86

Targets

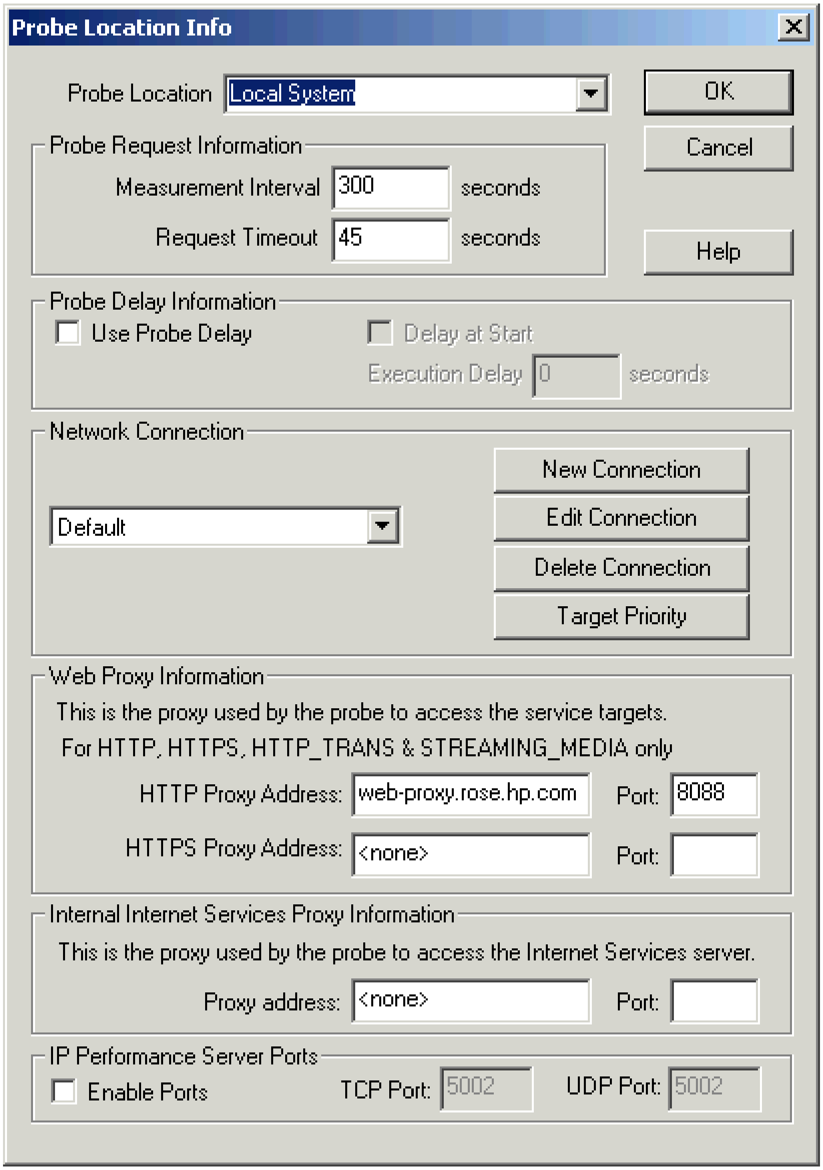
Target	Response Time	SLO Violation%
mysystem100.hp.com:9080/PlantsByWebSphere	1.044	4.69

Probe Location, Timing and Scheduling

The Probe Location dialog is used to configure the following:

- A location where the probes will be running. Note that for OVTA data the location includes the servicing system.
- 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.
- Whether to delay probe execution by the scheduler.
- Proxy information required for the probe to access the service targets or to send data back to the Management Server.
- Ports for use by the TCP Performance or UDP Performance probes.

For more information about setting probe timing and scheduling see Scalability Information on page 478.



Probe Location Info

Probe Location: Local System

Probe Request Information
Measurement Interval: 300 seconds
Request Timeout: 45 seconds

Probe Delay Information
□ Use Probe Delay
□ Delay at Start
Execution Delay: 0 seconds

Network Connection: Default

Web Proxy Information
This is the proxy used by the probe to access the service targets.
For HTTP, HTTPS, HTTP_TRANS & STREAMING_MEDIA only
HTTP Proxy Address: web-proxy.rose.hp.com Port: 8088
HTTPS Proxy Address: <none> Port:

Internal Internet Services Proxy Information
This is the proxy used by the probe to access the Internet Services server.
Proxy address: <none> Port:

IP Performance Server Ports
□ Enable Ports
TCP Port: 5002
UDP Port: 5002

Configure the Type of Network Connection

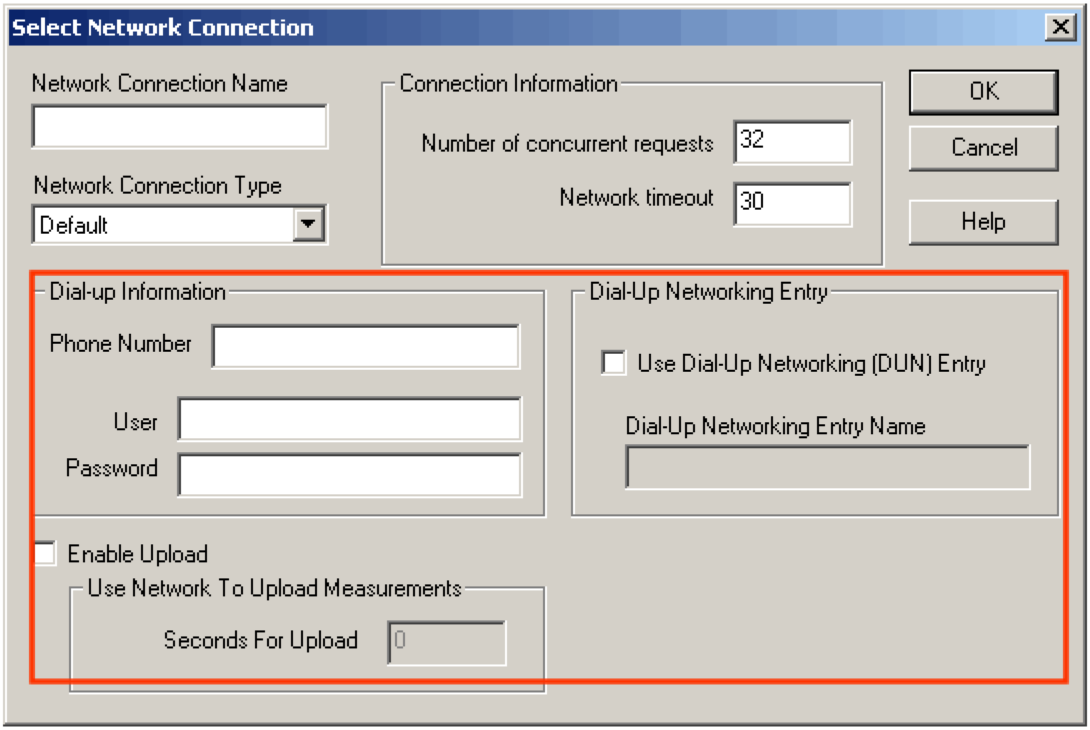
As you step through configuring a probe within the Configuration Manager, you have the option of configuring the probe's network connection. The default configuration has the probe connecting to the target through the LAN. However, you can configure other network connections and define concurrency for 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, or Delete a network connection.

When you select the New Connection button, the Select Network Connection dialog is display. In this dialog you name the connection so that you can see it referenced as a Service Group in the Internet Services data display.

In this dialog, select the **Network Connection Type** (LAN or Dial-Up).

The number of targets probed at the same time is specified in the **Number of Concurrent Requests** field. The **Network Timeout** specifies the number of seconds the network should stay connected. This value applies to all probes that are configured for this network connection. See Probe Timing and Scheduling on page 144 for more details on these fields.



Select Network Connection

Network Connection Name

Network Connection Type: Default

Connection Information

Number of concurrent requests: 32

Network timeout: 30

Dial-up Information

Phone Number

User

Password

Dial-Up Networking Entry

□ Use Dial-Up Networking (DUN) Entry

Dial-Up Networking Entry Name

□ Enable Upload

Use Network To Upload Measurements

Seconds For Upload: 0

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).

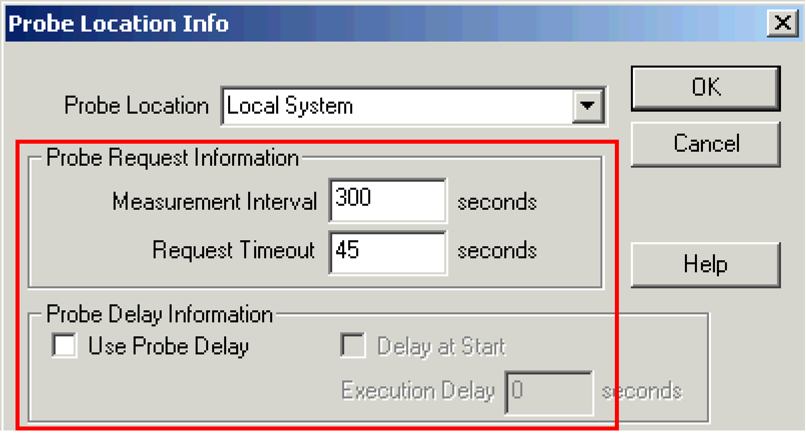
You can run multiple probes over this single Dial-Up connection and login. To do this for other probes under a Customer group, you open the Probe Location window and select the Dial-Up connection you just configured as the network connection.

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.



Probe Location Info

Probe Location: Local System

Probe Request Information

Measurement Interval: 300 seconds

Request Timeout: 45 seconds

Probe Delay Information

□ Use Probe Delay

□ Delay at Start

Execution Delay: 0 seconds

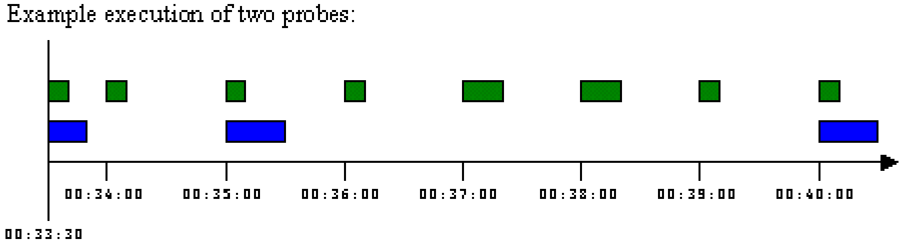
For example, the value 300 tells the scheduler to probe all targets that are contained in this Service Group for this probe location, every 300 seconds (5 minutes). The smallest value that can be specified is 60 seconds.

The time allowed for probing a target is specified in the **Request Timeout** field. The Request Timeout value may vary depending on the probe type. If the Request Timeout is exceeded, the target will be shown as unavailable.

Check the **Use Probe Delay** box if you want to add a delay before each probe runs. Enter the number of seconds delay. By default this is set to 0, so there is no delay. You may enter any number of seconds up to 25% of the minimum measurement interval for the whole probe location. For example if the measurement interval is 300 seconds, 25% of 300=75 seconds as the maximum probe delay value. If you check the box for Delay at Start, this will apply the delay to the first probe run.

The probe tries to do the measurement within the request timeout value specified for the probe. If the probe is unable to get a complete measurement, it determines that the service is unavailable. If the probe does not timeout within the Request Timeout, the scheduler, which launched the probe will terminate the probe according to the following calculation: (request timeout value + probe delay + (request timeout/3)) for example, 20 + 5 + (20/3) = 31 seconds. This ensures that no more than the specified number of probes, as set in the network connection concurrency field (defined when selecting New Connection), runs at the same time. In these exceptional cases no data record is generated by the probe's execution but an error is logged in the error log.

The probe scheduler may delay the execution of a single probe for up to 10 seconds since it may take up to 10 seconds for the scheduler to see whether the probe is ready to run.

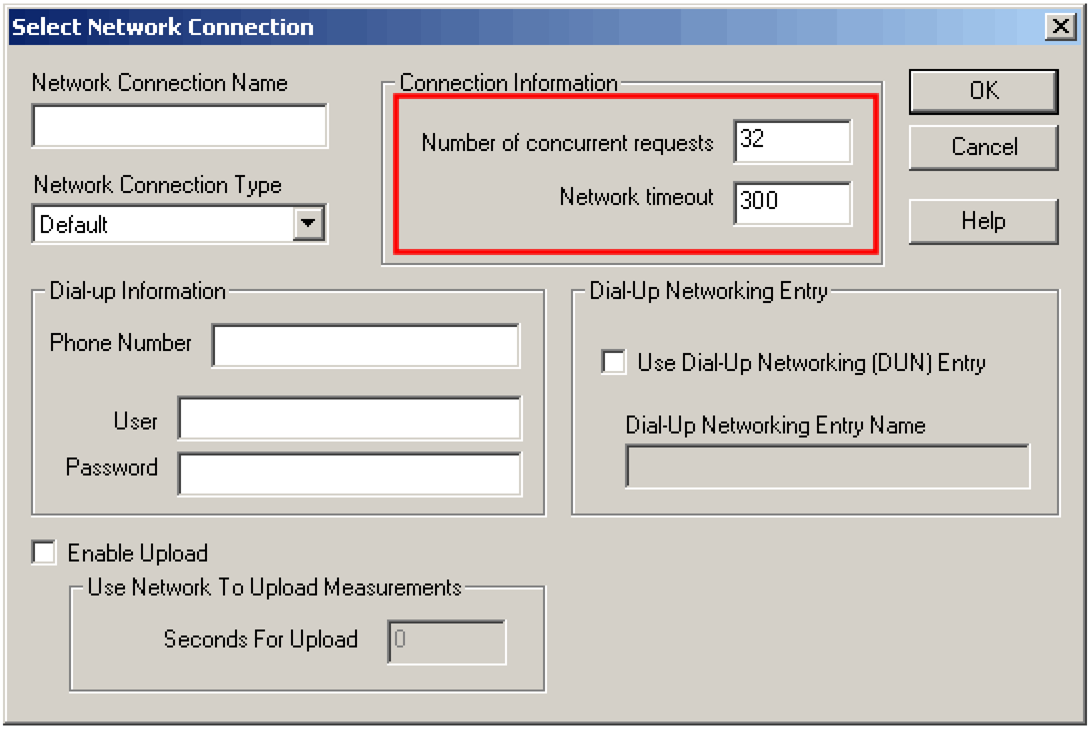


Example Execution of Two Probes: In the above example, there are two probes configured, one shown in the top row and the other shown in the bottom row. The probe in the top row has an interval of 60 seconds and a timeout of 20 seconds, and the probe in the bottom row has an interval of 300 seconds and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

When the scheduler is started, it executes the probes after a 10 second delay. In the above example, the probes are executed at 00:33:30. 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.

In addition, the scheduler may delay the execution of a single 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).



Select Network Connection

Network Connection Name

Network Connection Type: Default

Connection Information

Number of concurrent requests: 32

Network timeout: 300

Dial-up Information

Phone Number

User

Password

Dial-Up Networking Entry

□ Use Dial-Up Networking (DUN) Entry

Dial-Up Networking Entry Name

□ Enable Upload

Use Network To Upload Measurements

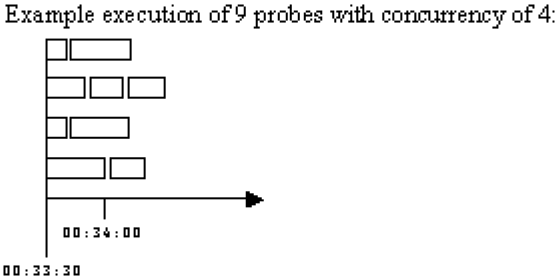
Seconds For Upload: 0

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 478.

➤ HTTP_TRANS probes use more probe system resources than the other probes. This can limit the number of parallel executions for this probe type. A concurrency of between 1-10 (set in the Probe Location dialog box) is best for this probe type. See Scalability Information on page 478 for more details.

Network Timeout specifies the number of seconds the network should stay connected. This value applies to all probes that are configured for this network connection. Note that the network timeout needs to be long enough that all probes using this connection can execute within this time period. The value you should set depends on the number of concurrent probes and the timeout for each of the probes. If the probes run longer than the network timeout, the OVIS scheduler will postpone the probes that haven't run yet. If this happens, the scheduler logs a warning message in error.log.

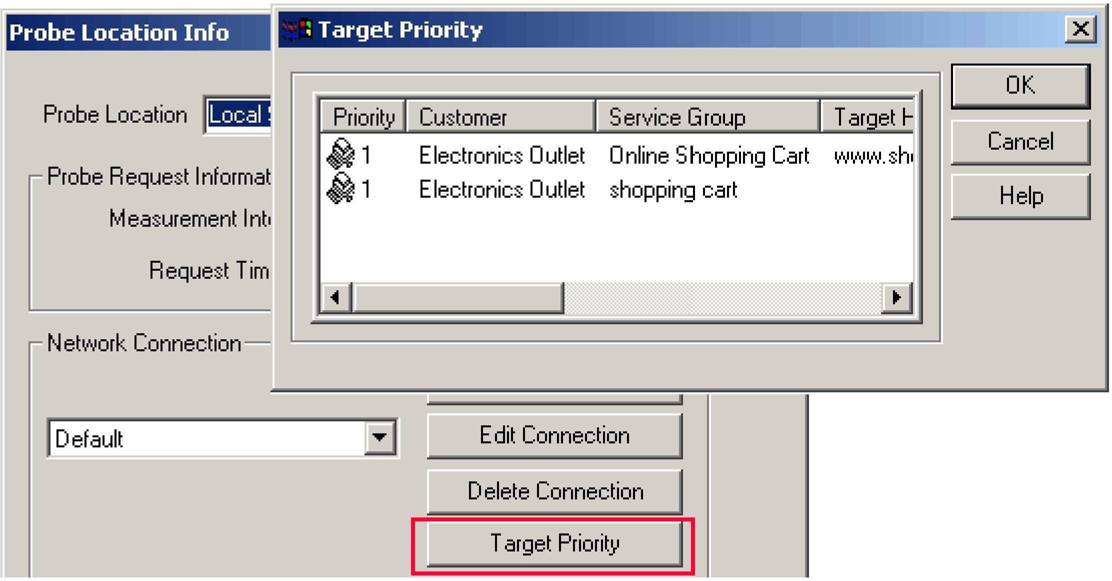
The default network timeout for a Dial-Up connection is set to 300 seconds.



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 HTTP_TRANS 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.



Probe Location Info

Probe Location: Local :

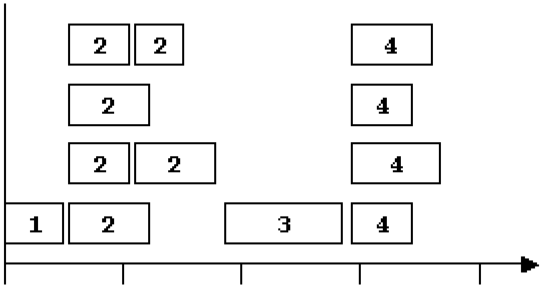
Target Priority

Priority	Customer	Service Group	Target H
1	Electronics Outlet	Online Shopping Cart	www.sh
1	Electronics Outlet	shopping cart	

Network Connection: Default

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.

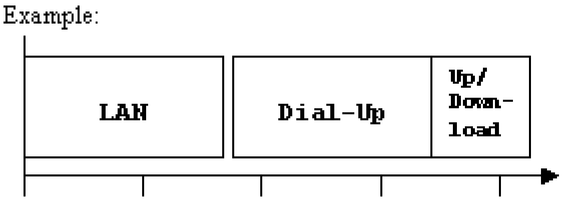
Usually, it is only necessary to have one or two network connections configured.

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.

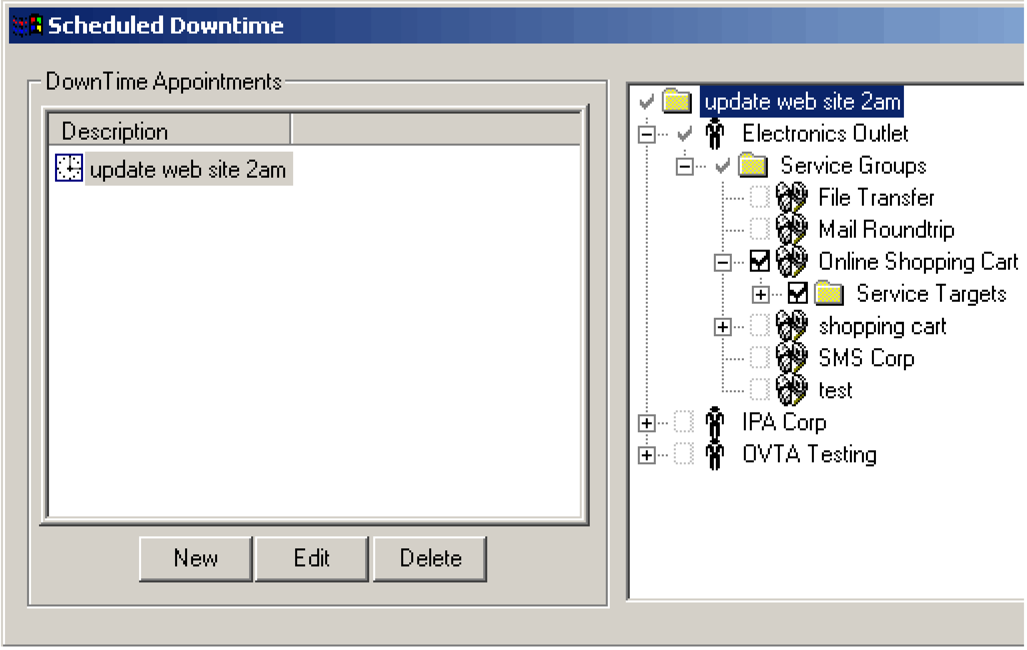
Things to watch out for:

- 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 HTTP_TRANS 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 configure probes to monitor different services. It is helpful, though, to understand how probes work and what you need to consider in accepting or changing the default settings assigned in the Configuration Wizard 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 step 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 available 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.

Configuring and Using TIPs

A number of Troubleshooting Insight Packages (TIPs) are provided out-of-the-box with OVIS. These TIPs can be used to quickly troubleshoot a service or infrastructure problem. In the Dashboard, you can run any of the TIPs that are associated with a particular service target or alarm condition (select the TIPs icon which is displayed when you select a target or an alarm).

When a TIP is run, each TIP command that meets the defined command conditions automatically executes on the probe system to collect troubleshooting information. The command results are displayed in the Dashboard in the TIPs viewer display.

Some of the TIPs and troubleshooting commands provided with OVIS are not set to run automatically because of overhead concerns. To configure these TIPs to run in your environment, to edit existing TIPs and commands, or to define new ones - use the TIPs Configuration program.

The TIPs Configuration program is accessed from **Start > Programs > HP OpenView > Tips > TIPs Configuration**. You can perform the following actions:

- Create troubleshooting Commands with implementations for different operating systems.
- Define Conditions that control when a specific TIP runs.
- Define Conditions that control when a specific Command runs.
- Identify the information that you want to see after a Command is run.
- Specify presentation rules to help you quickly evaluate troubleshooting results.
- Configure TIPs to automatically gather information at the time a problem is reported.

See the TIPs Configuration online help for a getting started example that walks you through the use of the TIPs Configuration program.

Also see the What's New Troubleshooting Insight Packages paper available on the CD or installed in `<install dir>\help\iops\c\ovis60-tips.pdf`.

Examples of How to Use TIPs

There are two ways to trigger a TIP:

1. On demand - For a service target or alarm that meets a TIP condition, you can run that TIP on demand by selecting the TIP icon in the OVIS Dashboard. The results for a TIP that is run on demand are displayed in the Dashboard TIPs Viewer but are not stored.
2. Triggered by Alarm - A TIP that is Triggered by Alarm will run whenever a specified alarm occurs. You can configure any TIP to be Triggered by Alarm in the TIPs Configuration program. Data for a TIP that is Triggered by Alarm is stored in a TIPs database and is available for comparison with an on demand run of the same TIP later. Triggered by Alarm data is stored until the TIP command that generated the data is no longer in the TIP's configuration or until the condition that caused the TIP to execute no longer exists in the data source.

Results from every TIP that runs are displayed in the Dashboard in the TIPs Viewer. Triggered by Alarm TIP data will only display in the context of the alarm that triggered it. When data is gathered at the time an alarm occurs, you will see Triggered by Alarm in the TIPs Viewer above the data.

For each service target, you can define conditions to identify TIPs that will be available to troubleshoot that service target. These TIPs are run on demand.

On Demand TIP Example

An example of an on demand TIP is as follows:

You are monitoring a web server and have configured a Web Transaction Recorder (HTTP_TRANS) probe using the IE mode. In the Dashboard, you see that the associated service target for this probe has a red health icon displayed. You drill down to the service target’s summary page. From this page, you select the TIPs icon. The TIPs Viewer displays. The Monitored Service Status TIP executes. This TIP displays the error log file and the captured error screen from the Web Transaction Recorder probe activity. This information allows you to troubleshoot the current state of the web server and understand how to fix it.

For each alarm, you can define conditions to identify TIPs that will be available to troubleshoot that alarm. These TIPs are run on demand or configured to run when Triggered by Alarm.

Triggered by Alarm TIP Example

An example of a triggered by alarm TIP is as follows:

You are monitoring a critical domain server in the network. You have configured a probe (DNS) to monitor the DNS activity of this server. In the Dashboard, you see that the service target for this probe has a yellow health icon displayed. You drill down to the service target's alarm page. From this page, you select the TIPs icon for a particular alarm. The TIPs Viewer displays. The Target Network Status TIP executes. This TIP displays `nslookup`, `traceroute`, and `ping` command results against the domain server. This information allows you to troubleshoot the current state of the domain server and understand how to fix it.

You realize that if the domain server's availability becomes more critical, you will need to know, at the time that the alarm occurs, what the networking state was. You use the TIPs Configuration program to configure the Target Network Status TIP to be triggered when alarms occur. You save the TIPs configuration. Time passes. You are alerted in the Dashboard that the domain server's service target reports a critical alarm. You drill down to the service target's alarm page and select the TIPs icon for the critical alarm. The TIPs Viewer displays. The Target Network Status TIP executes. This time the TIP displays `nslookup`, `traceroute`, and `ping` command results that were gathered at the time the alarm occurred. In the TIPs Viewer, you can re-execute this TIP to see the current networking state for the domain server. And you can toggle back to the networking state information at the time the alarm occurred. This information allows you to troubleshoot the state of the domain server at the time of an alarm versus the current state.

See the TIPs Configuration program online help for information about changing a TIP definition so that it is triggered by an alarm.

Default TIPs

OVIS provides you with a number of TIPs which execute a command or group of commands. You can create new TIPs and new commands to address the troubleshooting needs in your environment. See the TIPs Configuration online help for a getting started example that walks you through the use of the TIPs Configuration program.

The following TIPs are automatically configured to work in your environment:

- Probe Re-Execution TIP

- Monitored Service Status TIP
- Target Network Status TIP

The following additional OVIS TIPs require some configuration tasks to work in your environment:

- Probe System Network Status TIP
- Probe System Resources TIP
- Probe System Status TIP
- Probe System OpenView Status TIP
- TIPs Runner Status Tip

See the TIPs Viewer online help for details on each of these OVIS TIPs. See the TIPs Configuration program online help for how to configure TIPs to work in your environment.

OVIS provides you with a number of TIPs commands. Each command can be associated with any number of TIPs. You can see the list of OVIS TIPs troubleshooting commands in the TIPs Viewer online help. You'll see the following types of commands:

- OVIS Target Commands (such as Target Ping Command and Target Traceroute Command)
- OVIS Probe Commands (such as Probe CPU Utilization Command and Probe Environment Command)
- OVIS Exchange Probe Commands (These commands require some additional configuration tasks to work in your environment. See the TIPs Configuration program online help for how to configure these commands to work in your environment.)
- OVIS Web Transaction Recorder Probe Commands
- TIPs Runner Commands
- OpenView Software Commands (such as OV Installed Software Command)

Installing and Removing Remote Probe Software

Internet Services runs probes on the local system and 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 OVIS Management Server for consolidation and reporting.

Once you have configured your remote probes and saved the configuration, you need to install the remote probe software onto the remote Windows and UNIX systems. You only need to install the remote probe software when you first install OVIS or when you upgrade to a new version of OVIS. On Windows systems you can either install interactively or in silent mode.

See the TIPs Configuration program's online help for information about how to configure the TIPs runner on remote probe systems.

Remote Windows Systems

Install Remote Probes Interactively on Windows Systems

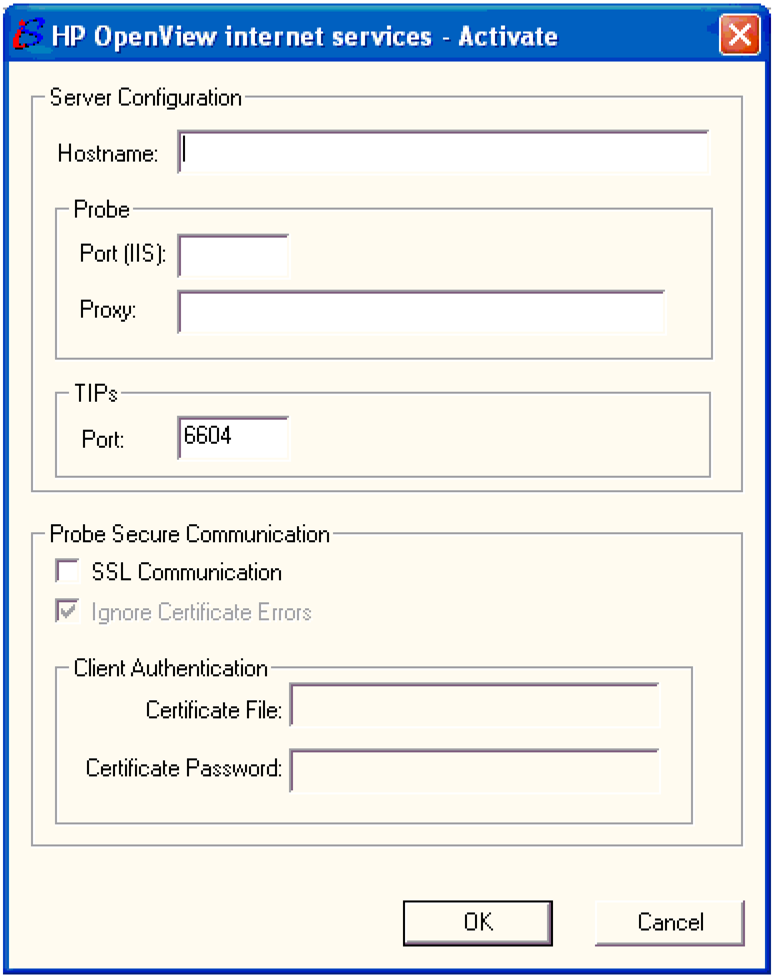
If you already have remote probe software installed on the system, you can upgrade by just installing over the existing probe software using the same steps described below (*the remote probe software upgrade capability is new with OVIS 6.0*).

To interactively install remote probe software 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 161 for silent install instructions.

1. Copy `<install dir>\newconfig\remote_probes_install.exe` file to the Windows remote probe system.
2. Run the program. Dialog boxes may be displayed for you to override the default install drive and the install directory. If there are no other OpenView products on the system including previous versions of the remote probes, you may change the drive and directory.

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 software installation.

3 In the next dialog that displays, enter the hostname of the Internet Services Management Server and other values.


HP OpenView internet services - Activate
Server Configuration
Probe
TIPs
Probe Secure Communication
Client Authentication
OK
Cancel

Hostname:

Port (IIS):

Proxy:

Port: 6604

□ SSL Communication

☑ Ignore Certificate Errors

Certificate File:

Certificate Password:

Hostname. This is the Internet Services Management Server hostname. You are required to enter a value.

Port (IIS). This is 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.

TIPS Port. This an optional entry, only needed if the TIPs (Troubleshooting Insight Packages) port is not 6604. See Changing the TIPs Port on page 451 for more information.

SSL Communication. 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 457 for details.

Certificate File. Enter the file name for the client certificates. The Base64 encoded X.509 formatted certificate must be installed in the `<data dir>\conf\probe` directory with the specified name (**clientcert**). All probe locations share the same certificate file name and password.

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

Note that you can run the `ovisactivate` program at a later time to edit these same entries on the remote probe system.

4 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 remote probe software 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. Use SET [variable=[string]] to edit, and REM to comment out settings.

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_WMF=TRUE
- OVIS_HOST=ManagementServer
- OVIS_PORT=80
- OVIS_PROXY=someproxy:8088
- TIPS_PORT=6604
- 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.

OVIS_WMF=TRUE means that the Windows Media Format program used by the Streaming Media probe can be installed. If you have proxy authentication set up on this system with Username and Password required, the installation of Windows Media Format may cause the silent installation to fail (because it is waiting at a Username and Password prompt). In this case, set OVIS_WMF=FALSE, so that the Windows Media Format (`wmfdist.exe`) installation is not executed. If you plan to run the Streaming Media probe using Windows Media on the system, you will need to install the Windows Media Format after the remote probe installation is complete. Also note that if you are installing on a Windows XP system the value will be set to OVIS_WMF=FALSE and you will need to install the Windows Media Format after installation is complete, if you plan to run the Streaming Media probe. To install, double-click the `wmfdist.exe` file located in the `<install dir>\newconfig` directory.

3 Save your changes.

4 Launch the `remote_probes_install.cmd` file from the Command Prompt window on the remote Windows system.

Change the Install Directory on a Remote Probe Windows Systems

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

1 Uninstall the remote probe software 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.

Remove Remote Probing Completely from Windows Systems

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

1 On the OVIS Management Server, using the Configuration Manager, delete the remote Probe Location from all Service Groups and save the change.

2 Stop the Scheduler service on the remote probe system by entering the following on the command line:

```
ovc -stop ovprobes
```

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 On the OVIS Management Server, using the Configuration Manager, delete the remote Probe Location from all Service Groups and save the change.

2 Copy the script `<install dir>\newconfig\remote_probes_uninstall.vbs` from the Management Server into the `<install dir>\bin` 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.

Remote UNIX Systems

Install Remote Probe Software on UNIX Systems

If you already have remote probe software installed on the system, you can upgrade by just installing over the existing probe software using the same steps described below (the upgrade capability is new with OVIS 6.0).

This section gives you instructions for installing remote probe software 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, SMS, Exchange, ODBC, SYS_BASIC_WMI and the OVTA integration probes are not available for UNIX systems.

Install Internet Services

1 Login to the UNIX system as `root`.

2 Insert the OVIS 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 remote probe installation program is located by typing:

```
cd /cdrom/SETUP/Remote_Probes_Unix/<platform>/
```

4 Type the following (note that Korn shell (ksh) is required for these installation scripts to function properly):

```
sh remote_probes_install.bin
```

Or copy `remote_probes_install.bin` to the UNIX system, make it executable using the `chmod` command (`chmod a+x remote_probes_install.bin`) and execute it. `./remote_probes_install.bin`

5 After successful installation, enter the Internet Services Management Server host name and any other parameter changes in the list that is displayed (select the number of the item to edit).

Hostname. This is the Internet Services Management Server hostname. You are required to enter a value.

IIS 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.

TIPS Port. This an optional entry, only needed if the TIPs (Troubleshooting Insight Packages) port is not 6604. See Changing the TIPs Port on page 451 for more information.

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 457 for details.

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

Certificate File. Enter the file name for the client certificates. The Base64 encoded X.509 formatted certificate must be installed in the `<DataDir>/conf/probe` 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, Save and Exit**. The Scheduler is automatically started. Note that on an install/upgrade you should select 10 to Save and Exit (rather than 11 Exit) even if you are not making any changes; this is required so that TIPs gets configured properly.

Start Internet Services

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

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

   ```
   cd /opt/OV/bin
   ```

2. Start Internet Services by entering:

   ```
   ovc -start ovprobes
   ```

3. Verify that the Scheduler is running by entering:

   ```
   ovc -status
   ```

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

Remove Remote Probing Completely from UNIX Systems

1. On the OVIS Management Server, using the Configuration Manager, delete the remote Probe Location from all Service Groups and save the change.

2 Login as root on the remote UNIX system.

3 Change to the `uninstall` directory by entering:

```
cd /opt/OV/uninstall/RemoteProbes/
```

4 Stop Internet Services (if necessary).

```
ovc -stop ovprobes
```

5 Start the removal script by entering the following:

```
sh uninstall.sh
```

Distributing Configuration Files and Updates

For probes to run correctly on remote systems you must install the remote probe software and have the configuration file and any other script or data files required for particular probes distributed to the remote system.

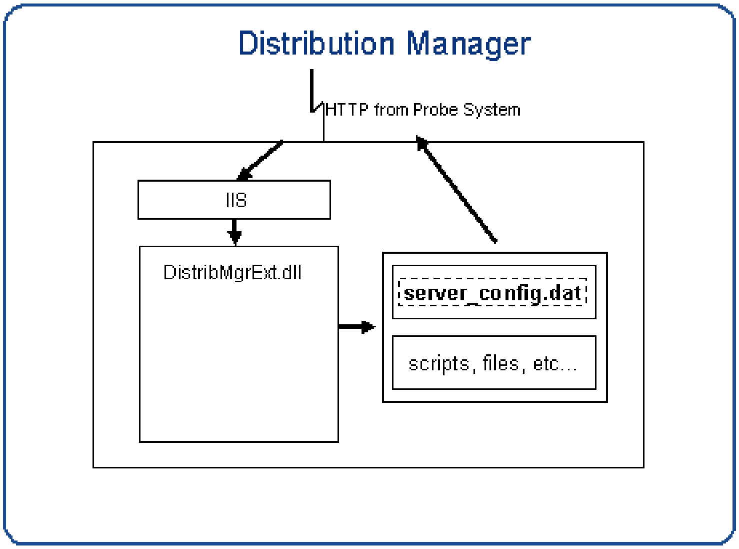
See Installing and Removing Remote Probe Software on page 159 for how to install the remote probe software. You only need to install the remote probe software when you first install OVIS or when you upgrade to a new version of OVIS.

The probe's configuration information is saved when you exit the Configuration Manager. OVIS automatically creates a `config_<system_name>.dat` file and stores this Configuration file in the `<install dir>\newconfig\` directory. The `<system_name>` matches the system name.

After the initial remote probe software installation on a local or remote system, the configuration file will automatically be downloaded for you from the Management Server. This is done via the Distribution Manager which is part of IIS. The Distribution Manager can also be used to distribute scripts or data files required by the probes to the remote and local systems. And it is used to automatically distribute updates of the configuration.

How the Distribution Manager Works

The probe software is designed to check every minute for configuration information from the OVIS Management Server. These requests from the probe systems for configuration updates are taken by the Distribution Manager. The Distribution Manager then distributes the `config_<system_name>.dat` file from the `<install dir>\newconfig\` directory as well as any script or data files you have placed in the appropriate subdirectories under the `<install dir>\newconfig\distrib\` directory.



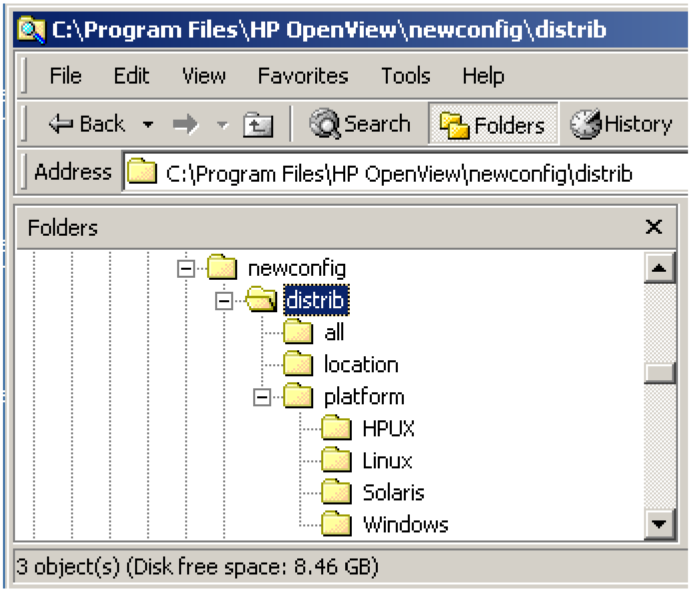
To use the distribution manager to distribute your script and data files, place these files in the appropriate directory on the OVIS Management Server under the `<install dir>\newconfig\distrib\` directory prior to creating the probe. (See the note below for the appropriate subdirectory.) When you save the configuration, the files under `\newconfig\distrib\` are copied to the `<datadir>/bin/instrumentation/probe/scripts/` distributed directory on the probe system (note that Windows uses a \ and UNIX systems use a /). The Distribution Manager does not distribute directories, only files.

When a probe gets a new configuration, the Distribution Manager looks in the following directories for files, so you should place your scripts and data files in these directories according to the systems where you want them distributed:

`newconfig\distrib\all` - You should place files that are valid for all platforms and probe locations in the `all` directory.

`newconfig\distrib\platform\{Windows|HPUX|Linux|Solaris}` - Platform specific files can be placed in the `Windows`, `HPUX`, `Linux` or `Solaris` directories. The probe will only receive files for the operating system under which it is running.

`newconfig\distrib\location\{probe location as defined in the Configuration Manager}` - It is further possible to create a directory under the location directory with the name of the probe location as it is configured in the Configuration Manager (usually the fully qualified hostname). For example, if the probe location is mysystem.mydomain.com, simply create a directory with the same name mysystem.mydomain.com and place the files there for distribution.


C:\Program Files\HP OpenView\newconfig\distrib
File
Edit
View
Favorites
Tools
Help
Back
Search
Folders
History
Address
C:\Program Files\HP OpenView\newconfig\distrib
Folders
newconfig
distrib
all
location
platform
HPUX
Linux
Solaris
Windows
3 object(s) (Disk free space: 8.46 GB)

Please note that these directories are not added, deleted or modified by OVIS! It is your responsibility to make sure that these directory names match what is configured in OVIS. Therefore, it is recommended to place files in the all and platform directory and only use the location directory if absolutely necessary. Further, please note that the Local System is actually the fully qualified domain name of the OVIS Management Server system. For example, if the name of the Management Server is ovis.domain.com, create the directory ovis.domain.com if you want to distribute files only to the Local System.

If you modify the configuration for a probe after the initial remote probe software installation on a local or remote system, the updated configuration files will automatically be downloaded for you from the Management Server via the Distribution Manager. And the changes will take effect without you having to reinstall the remote probe software.

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

In the Configuration Manager, the 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 by the Distribution Manager.

Please note that when the Distribution Manager 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 this case you can create the following file on the remote probe system `<datadir>/conf/probe/nodeid.dat` and enter the remote system's IP Address on the first line. For example: 14.24.157.8. Then restart the Hp Internet Services service `ovc -restart ovprobes.`

Removing Unused OVTA Reports

If you are not importing OVTA data to your OVIS Management Server then you may want to remove the unused OVTA reports (9 reports) that are automatically generated each night. This can shorten the nightly report generation cycle by eliminating empty reports.

The following file is provided to allow you to easily remove these OVTA only reports:

```
<install
dir>\newconfig\packages\remove\repload_IOPS_remove_OVTA_repo
rts.SRP
```

To remove the unused OVTA probe report templates from the nightly processing, run:

```
repload -remove repload_IOPS_remove_OVTA_reports.SRP
```

If OVTA data import is ever used in the future, you can just rerun the repload command above, with this SRP file but without the `-remove` option.

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 196 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.

IOPSLoad Program

The **IOPSLoad** program supports the batch configuration facility. This program can be found in the `<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.
- **disable** disables configured targets based upon -Customer or -Service or -Location or -Targetid values you enter.
- **enable** enables configured targets base upon -Customer or -Service or -Location or -Targetid values you enter.
- **refresh** runs exportiops to create new configuration files and reloads MeasEvent and AlarmEvent but does not restart HP Internet Services. Equivalent to Configuration Manager **File > Configure > Probe Scheduling** setting “Do not restart probes after save”.
- 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 `<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** option 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
IOPSload -disable [-Customer] [-Service] [-Location] [-Targetid]
IOPSload -enable [-Customer] [-Service] [-Location] [-Targetid]
IOPSload -refresh
```

Only one of these parameters should be provided. If none is provided then `-check` is assumed.

IOPSLoad Loading and Removing at the Component Level

The IOPSLoad program is not designed to update individual fields in a component. A component is a CUSTOMER, SERVICE, TARGET, OBJECTIVE, LOCATION, CONFORMANCE_LEVEL, DOWNTIME, or NETWORK. To update a component field you must remove the component and then load it again from an XML file containing the desired change. To remove a component like a CUSTOMER, which may include other components such as SERVICE, TARGET, OBJECTIVE, and LOCATION, you must remove all the included components.

For example, let's say you wanted to change the host name of all configured targets from `name.oldcompany.com` to `name.newcompany.com`. You could first run `IOPSLoad -save config.date.txt`, copy the `config.date.txt` file to `config.date.mod.txt`, then edit `config.date.mod.txt` to change the host names as desired and save it under the same name. Then you could run `IOPSLoad -removeall` to erase the current configuration followed by an `IOPSLoad -load config.date.mod` to load the modified configuration. Note that for this particular example `IOPSLoad -remove config.date.txt` would have produced the same result as the `removeall` option since `config.date.txt` has all components of the current configuration specified.

In order to facilitate automated checking of the success of an `IOPSLoad` function, `IOPSLoad` output can be routed to a disk file by appending `>filename.txt` to the command.

WARNING: Care must be taken to insure the automated processing does not produce duplicate names or invalid data since the editing capabilities of the `IOPSLoad` utility are significantly less than the configuration manager.

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 178 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 the 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 of **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\repload_IOPS.SRP` for details.

<TARGET (...) >

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

Table 1 Probe attributes

PROBE	Attribute	Description
ANYTCP	host= port= pattern= patternConfig=	system name of server TCP/IP port to access pattern to find pattern configuration parameters
DHCP	host= port= clientport= acceptOffer= pattern= patternConfig= chaddr= retries= label=	system name of DHCP server TCP/IP port default=67 client port to use, default port 68 whether to accept offered address pattern to find pattern configuration parameters client hardware address (MAC Address) number of retries name to be used for the target
DIAL	phoneNumber= username= password= phoneEntryName= stayConnected= retry= waittime=	phone number to dial user name password DUN entry file name stay connected (1) after dial or not (0) number of times to retry request time to wait between retries

Table 1 Probe attributes (cont'd)

PROBE	Attribute	Description
DNS	host= port= query= retries= pattern= patternConfig=	system name of Domain Name Server TCP/IP port default=53 system name to be resolved by DNS number of retries pattern to find pattern configuration parameters
Exchange	host= port= username= password= domain= recipient= displayName= emailtype= usernameRT= passwordRT= domainRT= profilenameRT= runtype= checkinterval= mailbox= exchangeServer= mailboxRT= exchangeServerRT= datasize= label=	system name of Exchange Server port default=80 Exchange user name password domain of the user logged on email address to send to name on mailbox to send to 2 types: EX or SMTP (only EX is supported) user to login with for roundtrip password domain of the user logged in for roundtrip name of the roundtrip profile -1, 0, 1,2 (Send/Read, Send, Read, Roundtrip) how often to check the mailbox (Auto) create profile mailbox (Auto) create profile Exchange server (Auto) create Roundtrip profile mailbox (Auto) create Roundtrip Exchange server message size name to be used for the target
FTP	host= port= file= username= password= mode=	system name of FTP Server TCP/IP port default=21 name of file to transfer user name password Automatic, Passive, or Active

Table 1 Probe attributes (cont'd)

PROBE	Attribute	Description
HTTP	host=	system name of Web Server
	port=	TCP/IP port default=80
	urlfile=	reference string for the web page
	username=	user name
	password=	password
	options=	KeepAlive
		nocache
		host=<string>
		availCheck=1
		bind
		sec=1
		agent=<user agent>
		SOAPAction: <soap action>
		post
		version
	pattern=	pattern to find
	patternConfig=	pattern configuration parameters
	embedded=	load images and frames?
	proxyusername=	user name for proxy server
	proxypassword=	password for proxy server
	retry=	number of times to retry request
	waittime=	time to wait between retries
	ua=	override user agent header
	postFile=	post file name
	cookieFile=	file used to save or load cookies
	label=	name to be used for the target

Table 1 Probe attributes (cont'd)

PROBE	Attribute	Description
HTTPS	host=	system name of Secure Web Server
	port=	TCP/IP port default=443
	urlfile=	reference string for the secure web page
	username=	user name
	password=	password
	options=	KeepAlive
		nocache
		host=<string>
		availCheck=1
		bind
		sec=1
		agent=<user agent>
		SOAPAction: <soap action>
		post
		version
	pattern=	pattern to find
	patternConfig=	pattern configuration parameters
	embedded=	whether to load images and frames
	ignore=	ignore flag (0 or 1)
	proxyusername=	user name for proxy server
	proxypassword=	password for proxy server
	clientcertfile=	client certificate file used in authentication
	clientcertpassword=	client certificate password
	retry=	number of times to retry request
	waittime=	time to wait between retries
	ua=	override user agent header
	postFile=	post file name
	secure=	1 for HTTPS
	cookieFile=	file used to save or load cookies
	label=	name to be used for the target
HTTP_TRANS	transFile=	name of transaction file (httptrans.dat)
	embedded=	load images and frames?
	ignore=	ignore flag (0 or 1)
	version=	2 for IE mode, for URL mode do not include version attribute
	retry=	number of times to retry request
	waittime=	time to wait between retries

Table 1 Probe attributes (cont’d)

PROBE	Attribute	Description
ICMP	host=	system or TCP/IP address to be polled
	packetsize=	bytes to be sent
	requests=	number of requests
	label=	name to be used for the target
IMAP4	host=	system name of IMAP4 mail server
	port=	TCP/IP port default=143
	username=	user name for login
	password=	password for login
	label=	name to be used for the target
LDAP	host=	system name of LDAP server
	port=	TCP/IP port default=389
	distinguishedName=	LDAP distinguished name parameter
	filter=	filter
	scope=	LDAP_SCOPE_SUBTREE, LDAP_SCOPE_ONELEVEL, or LDAP_SCOPE_BASE
	pattern=	pattern to find
	patternConfig=	pattern configuration parameters
	enableauth=	enable authentication for LDAP
	authtype=	type of authentication
	username=	username
	password=	password
	domain=	Active Directory/Windows domain name in which the LDAP server resides
	ldaps=	enable LDAP over SSL
	certfile=	path to certificate database
	labe=l	name to be used for the target

Table 1 Probe attributes (cont'd)

PROBE	Attribute	Description
MAILROUNDTRIP	host=	system name of the sending email server
	port=	port for sending server
	rhost=	system name of the receiving (IMAP/POP3) email server
	sprotocol=	protocol used by the sending server
	sender=	email sender name
	datasize=	message size
	rport=	port for receiving server
	rprotocol=	protocol used by the receiving server
	recipient=	email recipient fully qualified address
	rusername=	username for the email account on the receiving server
	rpassword=	password for the email account on the receiving server
	susername=	username for the sending email server
	spassword=	password for the sending email server
	pollinterval=	interval to check receiving server for message receipt.
	ESMTP=	indicates if an ESMTP/SMTP-A server is used
	label=	name to be used for the target
ODBC	host=	ODBC system DSN for the database
	query=	select statement for the database query
	username=	user name to login to the database
	password=	password to login to the database
	pattern=	pattern to be applied to the query
	patternConfig=	pattern configuration parameters
	label=	name to be used for the target
ovtacollector (COMAPP, JMSAPP, RMIAPP, SOAPAPP, WEBAPP)	transactionid=	Guid identifier for the OVTA transaction

Table 1 Probe attributes (cont'd)

PROBE	Attribute	Description
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= label=	system name of POP3 mail server TCP/IP port default=110 user name password name to be used for the target
RADIUS	host= port= username= password= protocol= sharedSecret= NASPort= retries= calledstId= callingstId=	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 phone number called to get to the NAS requesting authentication phone number the call came from to the NAS requesting authentication

Table 1 Probe attributes (cont'd)

PROBE	Attribute	Description
SAP	sapprobetype=	sap probe type
	sapsystemid=	unique 3 character name for the system within the system landscape
	saphostname=	system name for the SAP server
	sapinstance=	SAP instance
	sapclient=	SAP client number
	sapuser=	user name to access the SAP transaction
	sappassword=	password to access the SAP transaction
	sapgwhost=	gateway host
	saphwservice=	gateway service
	saptcode=	SAP transaction code
	sapgrouplogon=	enable group logon
	sapgroup=	name of the group to be used for group logon
Script	script=	location of script or data file
	pattern=	pattern to match in script return value
	patternconfig=	pattern configuration parameters
	chkstat=	check exit code for return value of zero
	ofile=	results file script for output file
	options=	flags for: checkInteractive addInternalParams noLog
	username=	user name for login authentication
	password=	password for login
	multistep=	1 or 0 to use multi-step label.
SMS	phoneno=	target phone number for the service center
	smscno=	number for the SMSC
	query=	the information you want queried
	pattern=	pattern to be applied to the SMS message
	patternConfig=	pattern configuration parameters
	deviceEntry=	the specific SendModem/ReceiveModem pair

Table 1 Probe attributes (cont'd)

PROBE	Attribute	Description
SMTP	host=	system name of SMTP mail server
	port=	TCP/IP port default=25
	recipient=	mail user to whom the mail will be sent
	sender=	mail user that is sending the mail
	dataSize=	number of bytes in the message
	ESmtp=	indicates if you are monitoring ESMTP/SMTP-A servers
	username=	username to authenticate ESMTP/SMTP-A server
	password=	password to authenticate the ESMTP/SMTP-A server
	label=	name to be used for the target

Table 1 Probe attributes (cont’d)

PROBE	Attribute	Description
SOAP	host=	system name of Web Server
	port=	TCP/IP port default=443
	urlfile=	reference string for the secure web page
	username=	user name
	password=	password
	options=	KeepAlive
		nocache
		host=<string>
		availCheck=1
		bind
		sec=1
		agent=<user agent>
		SOAPAction: <soap action>
		post
		version
	pattern=	pattern to find
	patternConfig=	pattern configuration parameters
	embedded=	whether to load images and frames
	ignore=	ignore flag (0 or 1)
	proxyusername=	user name for proxy server
	proxypassword=	password for proxy server
	clientcertfile=	client certificate file used in authentication
	clientcertpassword=	client certificate password
	retry=	number of times to retry request
	waittime=	time to wait between retries
	ua=	override user agent header
	postfile=	post file name
STREAM_MEDIA	host=	system name of server
	port=	Streaming media port default=80
	file=	Media file to be played on server
	protocol=	(HTTP, RTSP) Protocol to be used for playing the media clip
	playtime=	time (in seconds) the clip is to be played
	playtype=	format of media file

Table 1 Probe attributes (cont'd)

PROBE	Attribute	Description
SYS_BASIC_WMI	host= username= password= interface=	name of system you want metrics from valid user login to above system password of above user exact name of network interface (this is best found by running the config mgr wizard to create the probe, filling out the info in the config screen and then hitting "connect". If it successfully connects, it will give you the exact name of the network interface to use for batch configurations.)
TCP - Performance	host= port= label= protocol= packetSize= duration=	system name of the server TCP port default=5002 name to be used for the target TCP or UDP protocol packet size in bytes of the payload duration for the transfer
TFTP	host= port= file= mode= retries=	system name of server TFTP port default=69 file you want to TFTP mode used to download file, Ascii or Octet number of times to retry request
UDP - Performance	host= port= label= protocol= packetSize= duration= packetDelay=	system name of the server TCP port default=5002 name to be used for the target TCP or UDP protocol packet size in bytes of the payload duration for the transfer delay between packets
WAP	host= port= url= pattern= patternConfig= retry= waittime=	system name of WAP server TCP/IP port default=9200 reference string for the Web page pattern to find pattern configuration parameters number of times to retry request time to wait between retries

<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` (...) >

Attributes are shown below:

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
<=	&lt;=	Less Than or Equal to
>=	&gt;=	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. The character positions begin with Monday, then Tuesday, ... and end with Sunday.

If the character position has an X, no alarms will be triggered. If the character position has a different value like M or T or F, alarms can be triggered. A value which allows alarms only Monday, Wednesday and Friday would be "MXWXFXX", a value which allows alarms only on Sunday would be "XXXXXXS".

- 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 below. For the values for METRIC 1 - 8 refer to the List of Metrics by Probe Type in Chapter 4.

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)

Table 3 Symbol Substitutes (cont'd)

Symbol	Substitutes for
<SETUP_TIME>	Setup Time value (if available from the probe)
<THRUPUT>	Throughput value (if available from the probe)
<ERROR_INFO>	Probe specific value (if available from the probe.)
<EXPRESSION>	The alarm expression that triggered the alarm (if this probe supplies it)
<PSTIME>	Time when a measurement was taken by the probe.
<THRESHOLD_SW>	Sliding Window threshold value when a violation occurs.
<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 (...) >

Attributes are listed below:

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(...) >

Attributes are listed below:

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 (...) >

Attributes are listed below:

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 is specified for this network.
- Attribute **service=** specifies the name of the Service Group associated with this Network. Blank if no service group is 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 (...) >

Attributes are listed below:

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;0,1,1011118215,1,0,0;0,1
011118215,0,0,0,0,0,0,0;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 to configure a probe for the service, it is helpful to understand how each service type works.

➤ Refer to List of Metrics by Probe Type on page 281 for a complete list of the metrics collected by the probe for each service 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, Streaming Media probe, SMS probe, SYS_BASIC_WMI probe, Exchange probe, ODBC probe and the service types for data imported from OVTA.

- ANYTCP (Transmission Control Protocol)
- DHCP (Dynamic Host Configuration Protocol)
- DIAL (Dial-Up Networking Service)
- DNS (Domain Name System)
- Exchange (MAPI)
- FTP (File Transfer Protocol)
- HTTP (Hypertext Transfer Protocol)

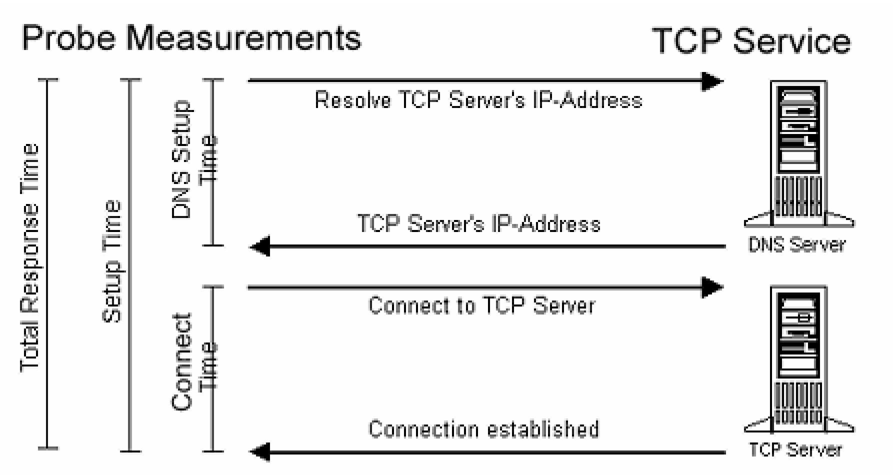
- HTTPS (Hypertext Transfer Protocol Secure)
- HTTP_TRANS (Web Transaction Recorder)
- ICMP (Internet Control Message Protocol—Ping)
- IMAP4 (Internet Message Access Protocol)
- LDAP (Lightweight Directory Access Protocol)
- MAILROUNDTRIP (Mail Round Trip)
- NNTP (Network News Transfer Protocol)
- NTP (Network Time Protocol)
- ODBC (Open Database Connectivity)
- POP3 (Post Office Protocol 3)
- RADIUS (Remote Authentication Dial In User Service)
- SAP Basis
- Script (generic script)
- SMS (Short Message Service)
- SMTP (Simple Mail Transfer Protocol)
- SOAP (Simple Object Access Protocol)
- STREAM_MEDIA (Streaming Media)
- SYS_BASIC_WMI (Basic System Metrics)
- TCP - Performance
- TFTP (Trivial File Transfer Protocol)
- UDP - Performance
- WAP (Wireless Application Protocol)
- Your Own Custom Probes
- Data Imported from OVTA

ANYTCP (Transmission Control Protocol)

The ANYTCP probe measures the time it takes the TCP steps to complete to connect a client to the specified host at the specified port.

See the Configuration Manager online help for details on configuring this probe.

The following diagram shows the steps the probe completes in measuring response time:



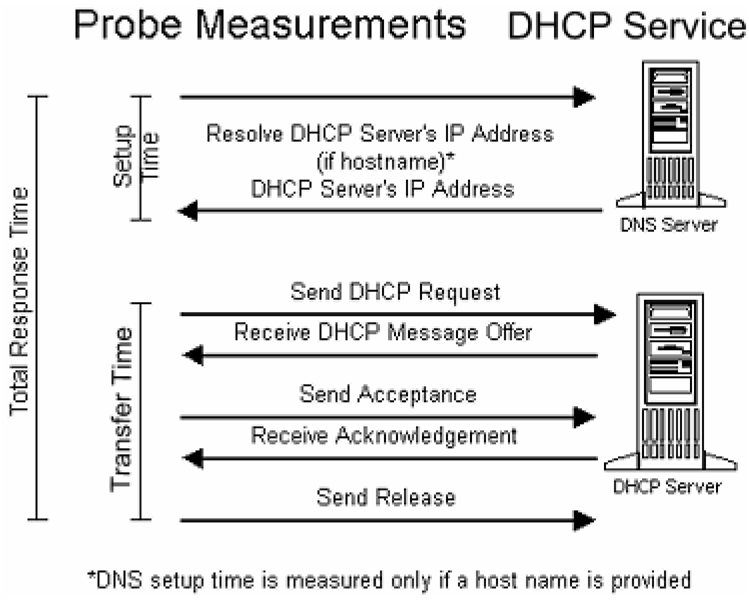
DHCP (Dynamic Host Configuration Protocol)

The DHCP probe measures the time it takes the DHCP server to service an IP address request. It uses the UDP protocol to transact with the DHCP server. 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 served 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 steps the probe completes in measuring response time:



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.

See the Configuration Manager online help for details on configuring this probe.

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 measures the amount of time it takes to dial, handshake, and complete the ppp connection protocol. You may configure the Dial-Up probe to disconnect afterward, or to stay connected so other probes may be run on that network connection.

➤ 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.

Also note that the Dial-Up probe is available on all supported versions of UNIX except SuSE Linux.

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 a new Dial-Up network connection, a Dial-Up service group and target are automatically set up for you. You will see them 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 for the Dial-Up connection. See the Configuration Manager online help for details on configuring this probe.

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 transact with 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 processed the request and returned a valid reply.

You can configure the number and duration of retries to control how often the probe resends the request before the request timeout is reached.

See the Configuration Manager online help for details on configuring this probe.

Exchange (MAPI)

The Microsoft Exchange 2000/2003 Mail Service (MAPI) is monitored via the Exchange probe. **The probe works on the Windows platform only.**

Before configuring the probe, you'll need to set up the prerequisites listed below. If you plan to run the probe on a remote system (as opposed to the OVIS Management Server) you'll need to set these prerequisites up for the remote probe system.

The prerequisites ensure that the probe runs from a user account (domain or local account) with the proper privileges, uses the Exchange profile tied to the specified account, and has access to the mailbox on the Exchange server.

Refer to the following sections on configuring an Exchange probe:

Prerequisites

Exchange Probe Settings

How to Manually Set Up an Exchange Profile

How to Configure the Exchange Probe

How to Test Access to the Exchange Server

Prerequisites

- Determine the system the Exchange probe will be executed from.
- On the system where the Exchange probe will run, make sure that an Exchange Client (such as Microsoft Outlook) has been installed for the desired user.
- Set up the user account (domain or local account) on the probe system, with proper privileges as described below. Note, for Windows NT it is recommended that your client user be trusted by the Exchange servers domain, in a one-way trust relationship.

  Privileges Required: certain privileges are required to be set for the Exchange probe to function properly.

  First the user account must have "Log On Locally" permission on the local computer. This permission is granted by default to all users on workstations and servers, but only to administrators on domain controllers. If the probe is not able to run as the desired user then it will not be able to access the Local Message Store when run from the OVIS Scheduler.

The second privilege that may need to be enabled is SE_TCB_NAME (Act As Part of the Operating System). If the probe does not possess the TCB Name privilege or if this privilege is not enabled, the probe may not function correctly when run from the OVIS Scheduler.

Other user rights may be needed if the user is other than admin or root. See the Configuration Manager online help for the Exchange probe for information on how to set user rights.

- Set up the User Mailbox on the Exchange server to be probed.
- Create an Exchange profile on the probe system or you can have OVIS create a profile for you when probe first runs. See How to Manually Set Up an Exchange Profile on page 211 for an example of the steps you would go through to create a mail profile.

➤ Note that with Outlook XP or Outlook 2002, if you check Auto Create Profile, it will not be able to correctly create the mail profile and the probe will return unavailable. If you look at the Exchange mail profile section for the user, the profile will not have the mailbox configured. This issue is seen primarily when the username and the mailbox alias name are not the same. See http://support.microsoft.com/default.aspx?kbid=329295 for more information on the MAPI problem.

- On the probe system, be sure that for the Exchange Mail service, “Logon network security” is set to NT Password Authentication. See Step 10 of How to Manually Set Up an Exchange Profile on page 211.
- Gather the following Exchange Server and User Account information to be used in configuring the probe in the Configuration Manager. See How to Configure the Exchange Probe on page 213 for an example of the Exchange configuration dialog.
  - — Exchange Server fully qualified name
  - — Exchange mailbox of desired user.
  - — The username, domain, and password for the user.

When the probe runs on the probe system, it first logs in as the user tied to the Exchange mailbox you've set up. If the user the probe logs in as, does not have permission to login locally to the probe system, or is unable to access the Exchange account from the probe system, or requires manual user interaction when connecting to the Exchange mailbox, then the Exchange probe will not function properly. See the test step below.

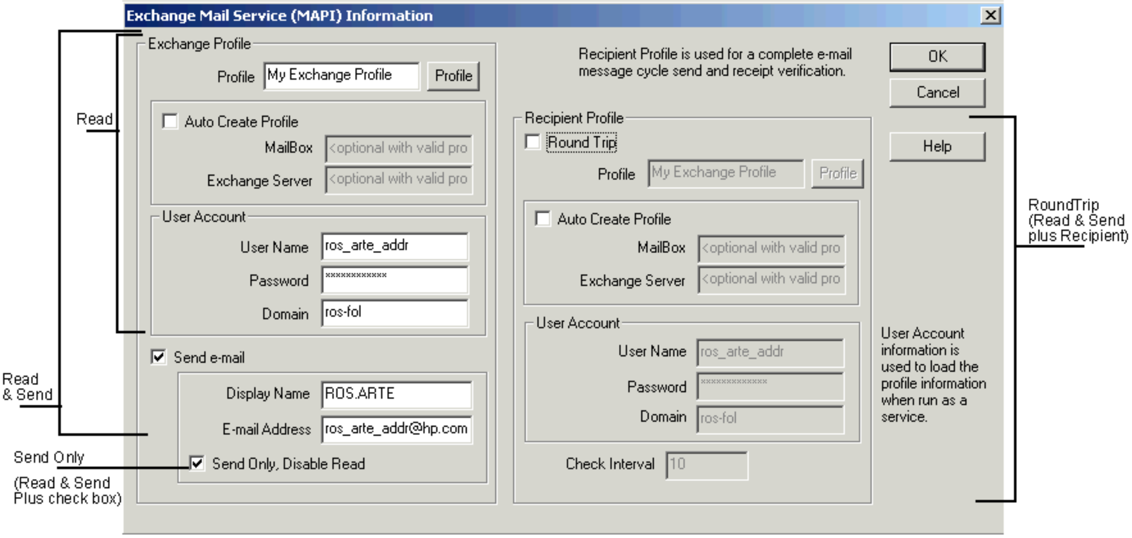
- Test access to the Exchange server from the probe system. See How to Test Access to the Exchange Server on page 215.

Exchange Probe Settings

You can set the Exchange probe up in the following ways:

- Read Only - Just monitor the availability and connection to an Exchange server and read only access to a mailbox. Enter an Exchange profile or have one created for you. Also enter any user account information required to access the Exchange profile.
- Read and Send - Monitor the availability and connection to an Exchange server, read the mailbox as well as send an e-mail. Enter a Display Name (Exchange Mail Service (MAPI) Information) and E-mail Address for sending the e-mail. The probe first looks for the Display Name in the Global Address List to see if an e-mail address is associated with it.
- Send Only - Monitor send only and disable reading the mailbox. Enter the information as described for Read and Send above, but check the box for Send Only, Disable Read.
- Roundtrip - Monitor the availability and connection to an Exchange server, and the roundtrip time to send and receive an e-mail. In addition to the basic Exchange profile and send e-mail information described for Read and Send above, enter a recipient Exchange profile or have one created for you. Also enter any user account information required to load the recipient profile information.

The Exchange dialog used to configure the Exchange probe is shown with an indication of what fields you enter for each of the above probe configurations.



Exchange Mail Service (MAPI) Information

Exchange Profile
Profile: My Exchange Profile [Profile]

☐ Auto Create Profile
MailBox: <optional with valid pro
Exchange Server: <optional with valid pro

User Account
User Name: ros_arte_addr
Password: ************
Domain: ros-fol

☑ Send e-mail
Display Name: ROS.ARTE
E-mail Address: ros_arte_addr@hp.com
☑ Send Only, Disable Read

Recipient Profile is used for a complete e-mail message cycle send and receipt verification.

Recipient Profile
☐ Round Trip
Profile: My Exchange Profile [Profile]

☐ Auto Create Profile
MailBox: <optional with valid pro
Exchange Server: <optional with valid pro

User Account
User Name: ros_arte_addr
Password: *************
Domain: ros-fol

Check Interval: 10

User Account information is used to load the profile information when run as a service.

Read

Read & Send

Send Only (Read & Send Plus check box)

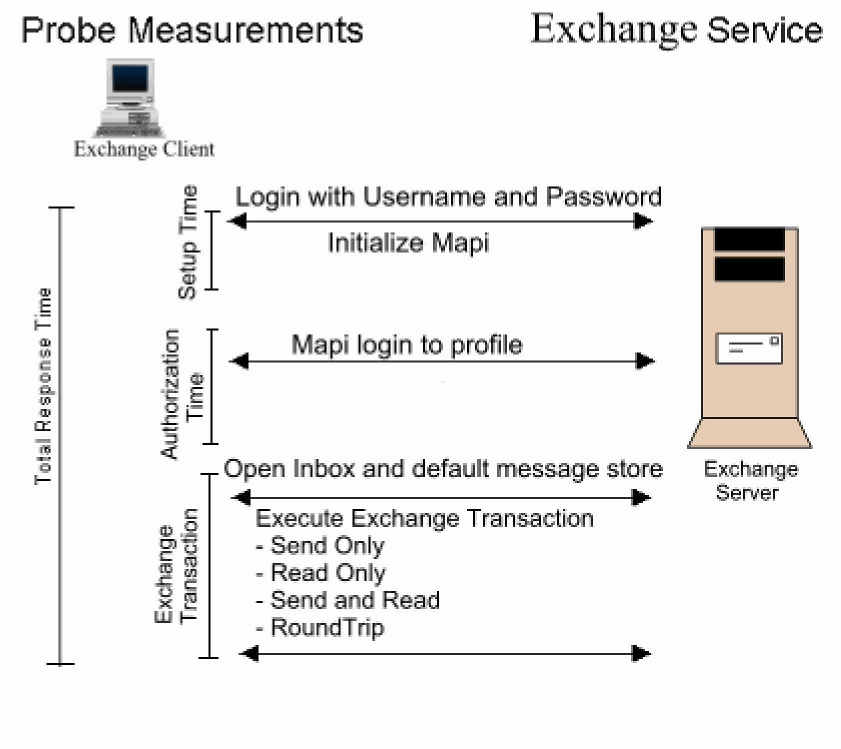
RoundTrip (Read & Send plus Recipient)

If you are not configuring the probe for monitoring the roundtrip message cycle, the probe logs onto the Exchange Server specified under Exchange Profile, downloads the inbox, reads the inbox and deletes any OVIS messages.

If configuring for roundtrip, the probe waits to download and read the inbox until after the e-mail message cycle of sending and receiving the message has completed.

!! The exchange probes should be limited to no more than a few remote probes pointing to the same Exchange server and user/mailbox, so as not to overwhelm the Exchange server and cause it to slow down.

The following diagram shows the steps the Exchange probe completes in measuring response time. (Note that if you choose to auto create a profile it is created during the first active probe run before the MAPI login is done.)



How to Manually Set Up an Exchange Profile

Two options are available when setting up an Exchange profile for use by the Exchange Probe: manually configure a profile or have the probe create an Exchange Mail Profile for you. In each case the Exchange probe requires that the Exchange Mail Profile be available from the user account you specify when configuring the probe, since the Mail Profile is specific to the user.

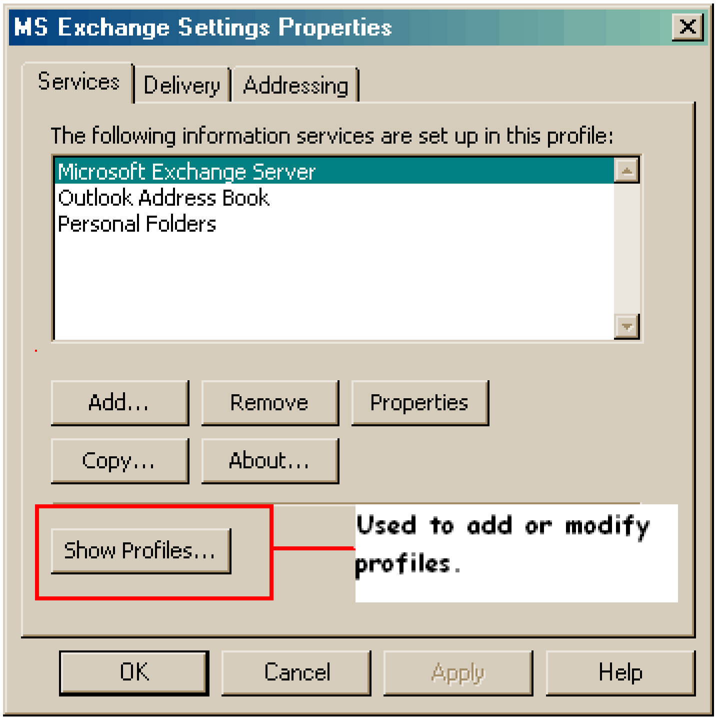
The instructions below are using the Microsoft Outlook Mail Client.

1 Gather information as described in the Prerequisites section above.

2 Login to the system where you plan to run the Exchange probe, as the user that the Exchange Mailbox belongs to.

3 Go to **Start > Settings > Control Panel**, double-click the **Mail** item.

4 In the Properties dialog displayed, select the **Show Profiles...** button.



MS Exchange Settings Properties

The following information services are set up in this profile:

Microsoft Exchange Server
Outlook Address Book
Personal Folders

Used to add or modify profiles.

5 In the Mail dialog displayed select the **Add** button.

6 In the Microsoft Outlook Setup Wizard, select **Microsoft Exchange Server** as the Information Service and click **Next**.

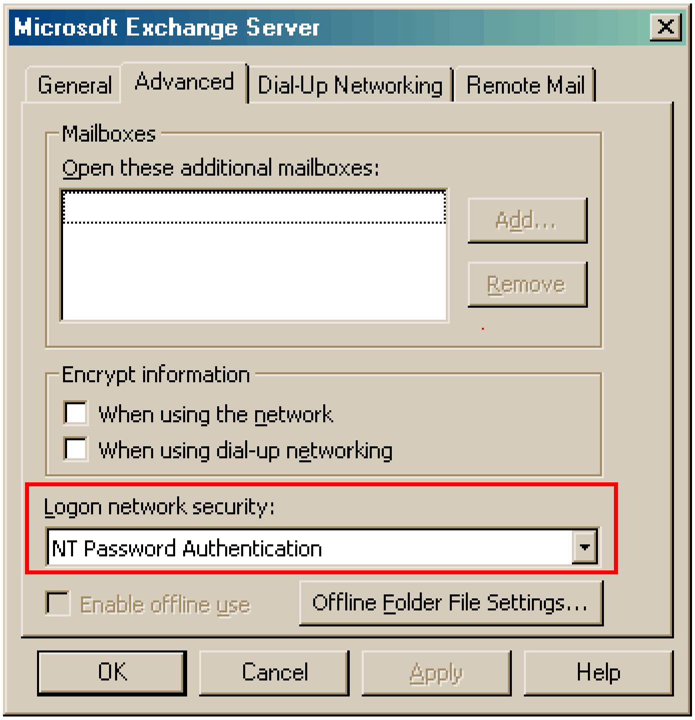
7 Enter the Profile Name that you want to use and click **Next**.

8 Enter the Exchange Server and Mail box to be accessed and click **Next**.

9 Complete the Setup Wizard and click **Finish**.

10 One specific property that is required for the Exchange Probe to work is to have Logon network security set to NT Password Authentication. This is required since the probe will be logging in as the user to access the account. If NT Password Authentication is not set for Logon network security then the probe will not be able to login to the Exchange Server.

To set NT Password Authentication, select **Mail** in the Control Panel as shown in Step 3 above. Double-click on the profile you have set up and the Microsoft Exchange Server dialog shown below is displayed. Select the Advanced tab, and under Logon network security, select NT Password Authentication from the drop down box.



□ When using the network

□ When using dial-up networking

Logon network security: NT Password Authentication

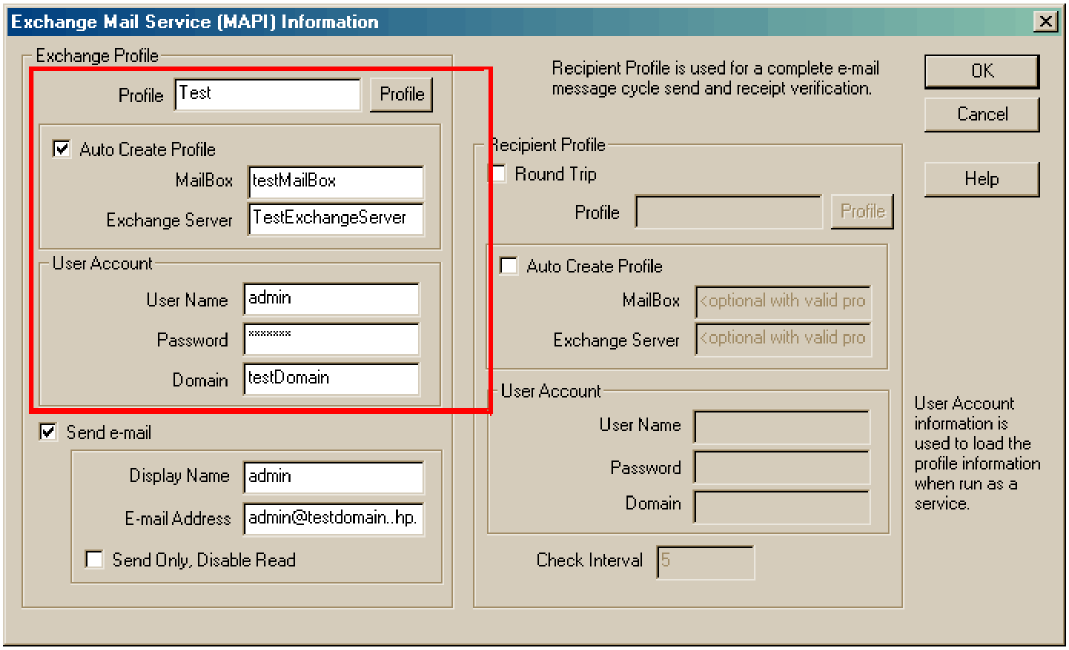
□ Enable offline use

11 When complete, you will have a new Exchange profile for the specified user, with access to the specified mailbox, that you can use in configuring the Exchange probe.

How to Configure the Exchange Probe

1 Be sure you have set up all the prerequisites and gathered the necessary information for configuring the probe.

2 In the OVIS Configuration Manager Exchange Mail Service dialog, enter the information required for the probe to read, read/send, send only, or do round trip measurements. SeeExchange Probe Settings on page 209 for what values in this dialog are required for each of these settings. Also refer to the Configuration Manager online help for details on this dialog.



Exchange Mail Service (MAPI) Information

Exchange Profile

Profile: Test

☑ Auto Create Profile

MailBox: testMailBox

Exchange Server: TestExchangeServer

User Account

User Name: admin

Password: *******

Domain: testDomain

☑ Send e-mail

Display Name: admin

E-mail Address: admin@testdomain..hp.

□ Send Only, Disable Read

Recipient Profile is used for a complete e-mail message cycle send and receipt verification.

Recipient Profile

□ Round Trip

Profile:

□ Auto Create Profile

MailBox: <optional with valid pro

Exchange Server: <optional with valid pro

User Account

User Name:

Password:

Domain:

Check Interval: 5

User Account information is used to load the profile information when run as a service.

3 If you have manually created an Exchange profile, you can enter the profile name and User Account information.

4 If you want OVIS to create a profile for you, select the Auto Create Profile option. Note that on the probe system, the Exchange client, User Account and password must already exist; and the mailbox must already be set up on the Exchange server, for OVIS to create a profile. The first time the probe runs on a probe system, the profile is created for you, using the settings you've configured. This profile is tied to the User Account information you entered.

➤ Note that with Outlook XP or Outlook 2002, if you check Auto Create Profile, it will not be able to correctly create the mail profile and the probe will return unavailable. If you look at the Exchange mail profile section for the user, the profile will not have the mailbox configured. This issue is seen primarily when the username and the mailbox alias name are not the same. See http://support.microsoft.com/default.aspx?kbid=329295 for more information on the MAPI problem.

5 Save the configuration.

How to Test Access to the Exchange Server

It is important to check that the user has the necessary access rights to use the desired Exchange server. To check user rights, we recommend that you complete these steps to simulate the probe:

1 Login locally to the probe system with the user, password, domain.

2 Open an Exchange Mail Client, like Microsoft Outlook, using the specified Profile.

If you are required to manually enter user and password information at this point then the probe will not be able to access the profile.

3 Send an E-mail from that account back to itself and check that it works.

If any of the above steps fail when you manually run them, then the Exchange probe will also fail.

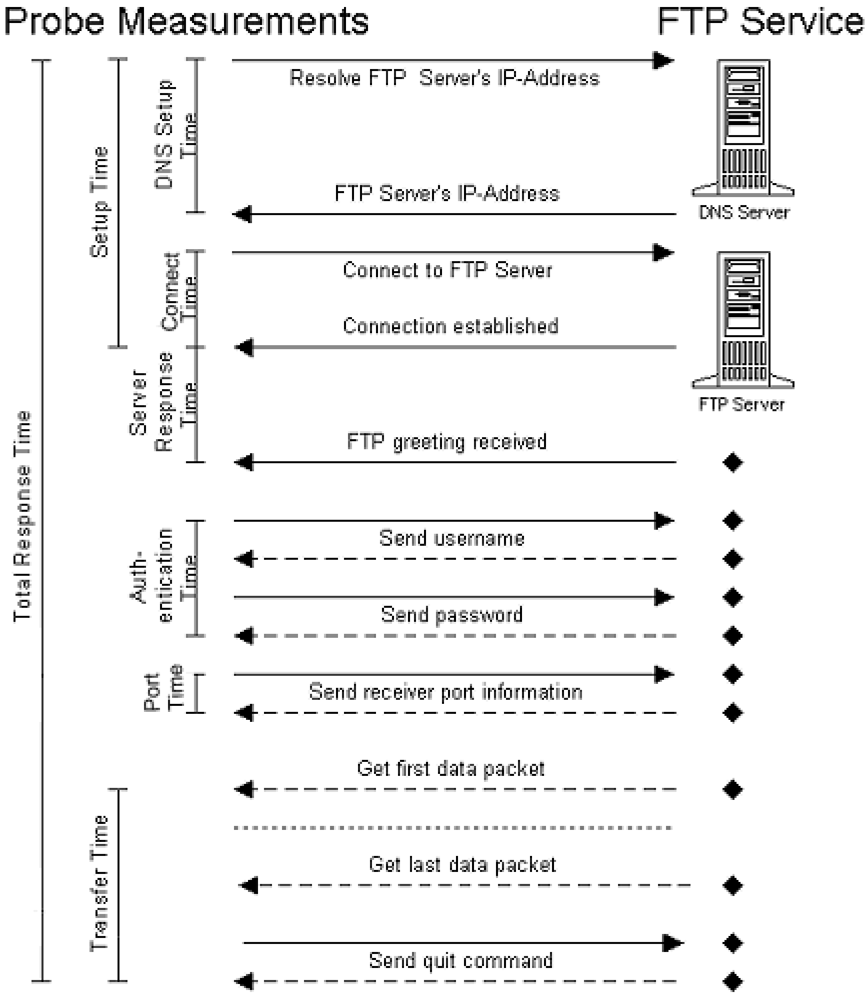
FTP (File Transfer Protocol)

The FTP probe performs a simple file retrieval or directory listing. If authentication is required, it uses 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).

See the Configuration Manager online help for details on configuring this probe.

The following diagram shows the steps the probe completes in measuring response time:

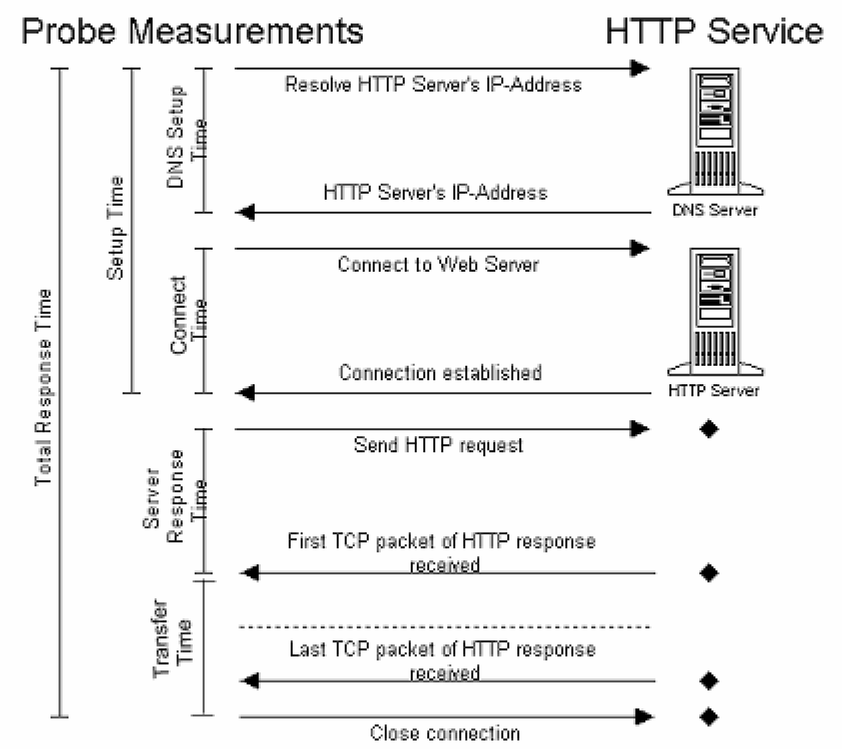


HTTP (Hypertext Transfer Protocol)

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. Note that the HTTP probe on UNIX supports only the Basic authentication method.

You can configure the HTTP probe to use pattern matching to check for successful web page downloads. The probe can be set up to work with proxies. You can set various flags to control how the web page is loaded by the probe and what page elements are considered in determining availability. You can configure the number and duration of retries to control how often the probe resends the request before the request timeout is reached. See the Configuration Manager online help for details on configuring this probe.

The following diagram shows the steps the probe completes in measuring response time:



HTTPS (Hypertext Transfer Protocol Secure)

The HTTPS probe works the same as the HTTP probe (see above) except it uses a secure protocol.

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.

You can specify for the probe to ignore certificates 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 a 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 `<data dir>\conf\probe` 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 `<data dir>\conf\probe` directory.

6 Repeat steps for multiple certificates.

7 Comments may be added above the -----BEGIN CERTIFICATE----- line 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. See Configuring Secure Communication on page 457 for more information on secure communications.

See the Configuration Manager online help for details on configuring this probe.

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.

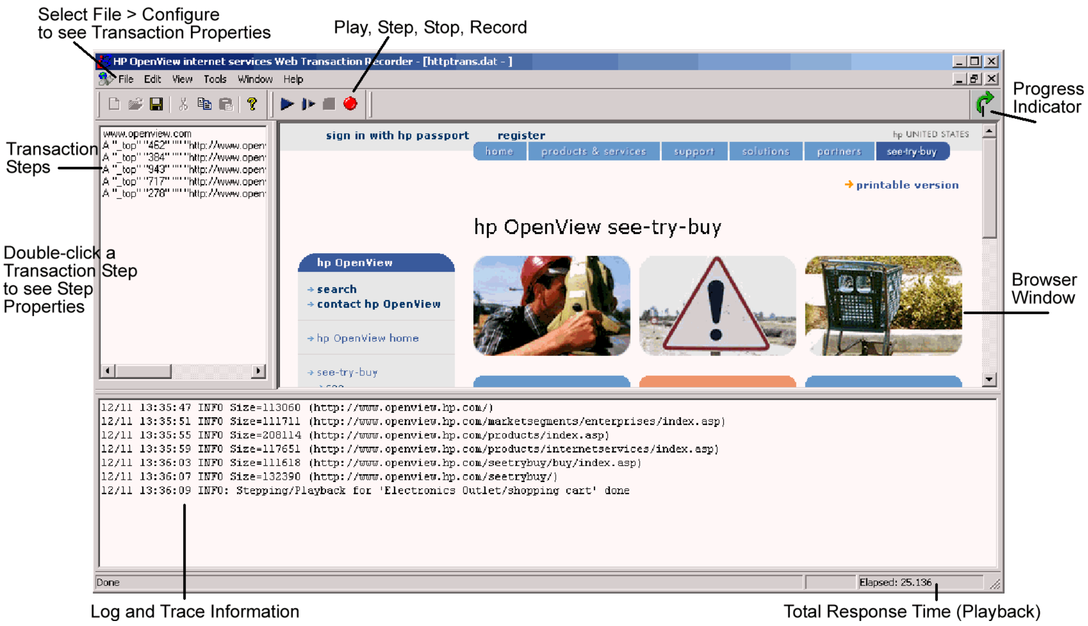
When you create an HTTP_TRANS service target, the Web Transaction Recorder is automatically launched. The Web Transaction Recorder allows you to specify the user actions that you want to track and record them for the probe to play back on a regular basis, simulating typical end-user activity and collecting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

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 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. The maximum number of steps you can record is 100.

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



```
www.openview.com
A "_top" "462" "" "http://www.open
A "_top" "384" "" "http://www.open
A "_top" "943" "" "http://www.open
A "_top" "717" "" "http://www.open
A "_top" "278" "" "http://www.open
```

```
12/11 13:35:47 INFO Size=113060 (http://www.openview.hp.com/)
12/11 13:35:51 INFO Size=111711 (http://www.openview.hp.com/marketsegments/enterprises/index.asp)
12/11 13:35:55 INFO Size=208114 (http://www.openview.hp.com/products/index.asp)
12/11 13:35:59 INFO Size=117651 (http://www.openview.hp.com/products/internetservices/index.asp)
12/11 13:36:03 INFO Size=111618 (http://www.openview.hp.com/seetrybuy/buy/index.asp)
12/11 13:36:07 INFO Size=132390 (http://www.openview.hp.com/seetrybuy/)
12/11 13:36:09 INFO: Stepping/Playback for 'Electronics Outlet/shopping cart' done
```

The basic steps to recording a transaction are as follows (**please see the *OVIS Web Transaction Recorder Guide* for details**):

1 Plan what web pages you want to record. Go through the steps of the web transaction in a browser first to be sure you know the sequence and selections to make for correct recording.

2 In the Web Transaction Recorder use the **Tools > Cache Viewer** to delete cookies before recording your transaction. You can set the Scrub Cookies flag to enable this during playback.

3 Configure global transaction properties in the Web Transaction Recorder **File > Configure > Properties** dialog box. You can specify such things as how the recorder should handle pop-ups and error dialogs, timeout and waittime, error capture, proxy settings and tracing levels.

4 In the main window press the **Record** button to start recording the transaction steps.

5 Enter the starting URL.

After the web page has been completely loaded in the Browser Window in the right pane (indicated when the blue circle in the upper right corner stops turning), you can navigate through the transaction steps in the web page displayed.

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

6 Press **Stop** to end the recording.

7 Playback the recording to test whether all the steps you wanted were included. Check the response time during playback, which is shown in the lower right corner.

8 Make any changes using the options in the Web Transaction Recorder. For example:

- Modify transaction step properties in the **Step Properties** dialog box accessed by right-clicking on a transaction step in the left pane and selecting **Properties**.
- Enter advanced scripting information in the **Advanced Step Properties** dialog box accessed by right-clicking on a transaction step in the left pane and selecting **Properties**, then selecting the **Advanced** tab.

9 Exit the Web Transaction Recorder and press the OK button in the HTTP_TRANS Web Transaction Information dialog.

10 Set up a Probe Location for the probe you created in the Web Transaction Recorder.

11 Set up Service Level Objectives for the probe you created in the Web Transaction Recorder.

Note that you can specify Step Alarming. See Setting Up Basic Service Level Objectives and Alarms on page 102 for details on configuring alarms for an individual step in the HTTP_TRANS probe transaction. The step alarming function is for alarms only and the step thresholds are not used for service level objectives.

You can only select a single step per set of alarms. To create alarms for several individual steps in a transaction, create a separate alarm definition for each. You can use the same metric in multiple sets of alarm definitions.

Step Alarming is for use with Response Time metrics not Availability. This is because Availability is determined for the whole transaction; if any step is unavailable then the transaction is marked as unavailable.

The step number is displayed in the Dashboard drill-down page and in the Status page drill down in the Configuration Manager.

12 Save the probe changes in the Configuration Manager and exit.

HTTP_TRANS probes use more probe system resources than the other probes. This can limit the number of parallel executions for this probe type. A concurrency of between 1-10 (set in the Probe Location dialog box) may be best for this probe type. See Scalability Information on page 478 for more details.

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.

You can configure the number of retries to control how often the probe resends the request before the request timeout is reached. See the Configuration Manager online help for details on configuring this probe.

IMAP4 (Internet Message Access Protocol)

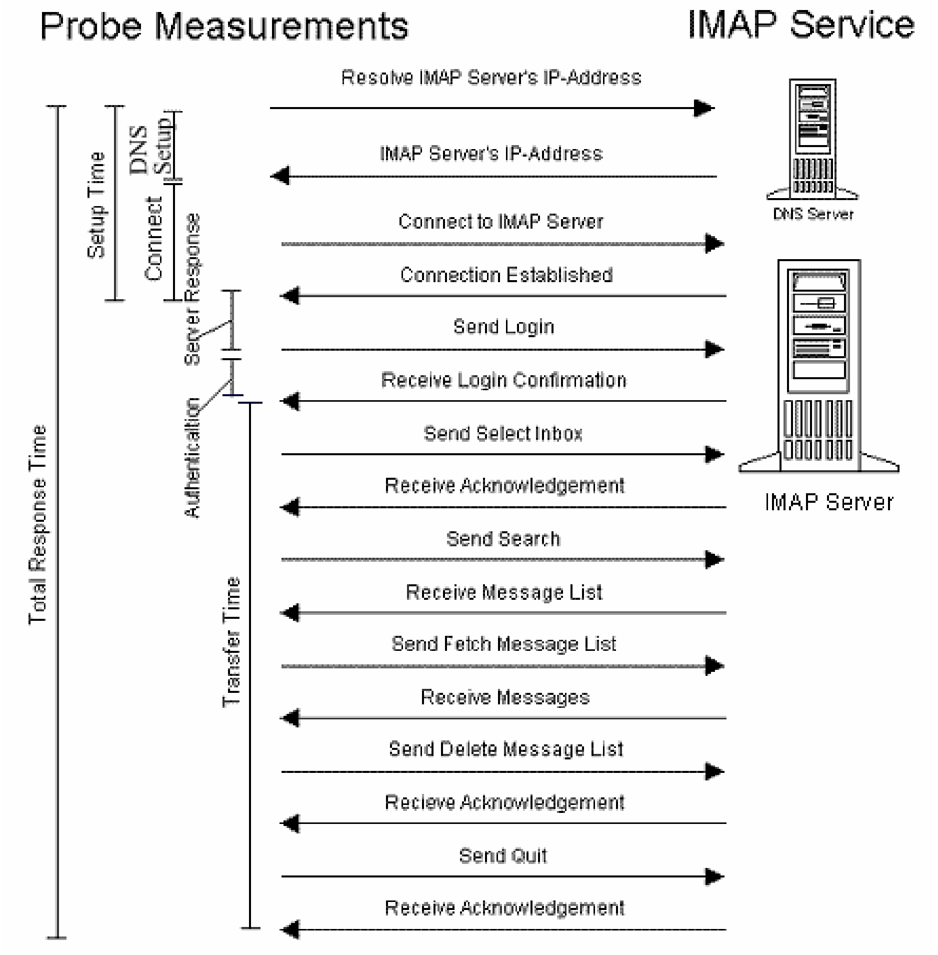
Internet Message Access Protocol (IMAP4) provides a method of accessing electronic mail or bulletin board messages that are kept on a (possibly shared) mail server. IMAP is a TCP based service. IMAP permits a *client* email program to access remote message stores as if they were local. The IMAP client just gets a copy of the e-mail, the e-mail itself stays on the server. 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 probes.

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

Note that there are special considerations for using the IMAP probe to monitor the IMAP4 service as provided by Microsoft Exchange 2000/2003 server. See to the online help on the IMAP4 service target for more information.

The following diagram shows the steps the probe completes in measuring response time:


Probe Measurements
IMAP Service
Resolve IMAP Server's IP-Address
IMAP Server's IP-Address
Connect to IMAP Server
Connection Established
Send Login
Receive Login Confirmation
Send Select Inbox
Receive Acknowledgement
Send Search
Receive Message List
Send Fetch Message List
Receive Messages
Send Delete Message List
Recieve Acknowledgement
Send Quit
Receive Acknowledgement
DNS Server
IMAP Server
Total Response Time
Setup Time
DNS Setup
Connect
Server Response
Authentication
Transfer Time

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. The LDAP probe uses the UDP protocol to transact with the LDAP server.

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.co
m host=ldap.corp.corp.com port=389 scope=LDAP_SCOPE_SUBTREE
```

Note on configuring LDAPS: There are special considerations to configuring this probe to the LDAPS protocol. The LDAP probe currently only supports the Netscape iPlanet/SunOne Directory server 5.X for the LDAPS protocol.

The required SSL certificate for the corresponding LDAPS server must be stored in a cert7.db database file used by Netscape Communicator 4.x. Note that previous and later versions of Netscape communicator use different file formats for the certificate database. Attempting to use a different version of the certificate database will result in database errors.

1. For proper functioning of LDAPS the following libraries of the iPlanet/ SunOne client SDK 5.0 must be copied into the `<install dir>/bin` directory on each system where you plan to run the probe. These libraries are included as part of the iPlanet/SunOne Server product and can also be requested from Sun Microsystems.

   ```
   libnspr4.dll
   libplc4.dll
   libplds4.dll
   LibRfc32.dll
   librfc32u.dll
   nsldap32v50.dll
   nsldappr32v50.dll
   nsldapssl32v50.dll
   nss3.dll
   ssl3.dll
   ```

2 The following certificate database files as created by Netscape Communicator 4.X must be copied into the `<data dir>\conf\probe` directory on the system where you plan to run the probe.

```
cert7.db
key3.db
```

To create the certificate database, follow the instructions below.

1 Point the Netscape 4.x browser to the following URL:

https://ldaps_hostname:ldaps_port/

Where ldaps_hostname is the hostname of the server hosting the LDAPS service.

Ldaps_port is the port number on which the LDAPS service is offered.

2 The browser will prompt to accept a certificate, and will walk you through a series of dialogs, ending in an error message indicating document contains no data. Accept the certificate and close the browser after that.

Note that there are other ways to create the required certificate database, refer to the iPlanet/SunOne server documentation for more information.

3 Verify the LDAPS connection to the server by typing the following URL in the browser

ldaps://ldaps_hostname:ldaps_port/dn=?

where dn=? Is a valid distinguished name. The browser should display the dn entry in it.

4 Finally, copy the `cert7.db` and `key3.db` files from the `\Netscape\Users\UserId` folder into the `\probes` folder.

See the Configuration Manager online help for additional information on configuring this probe.

MAILROUNDTRIP (Mail Round Trip)

The Mail Round Trip mail service is monitored via the 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.

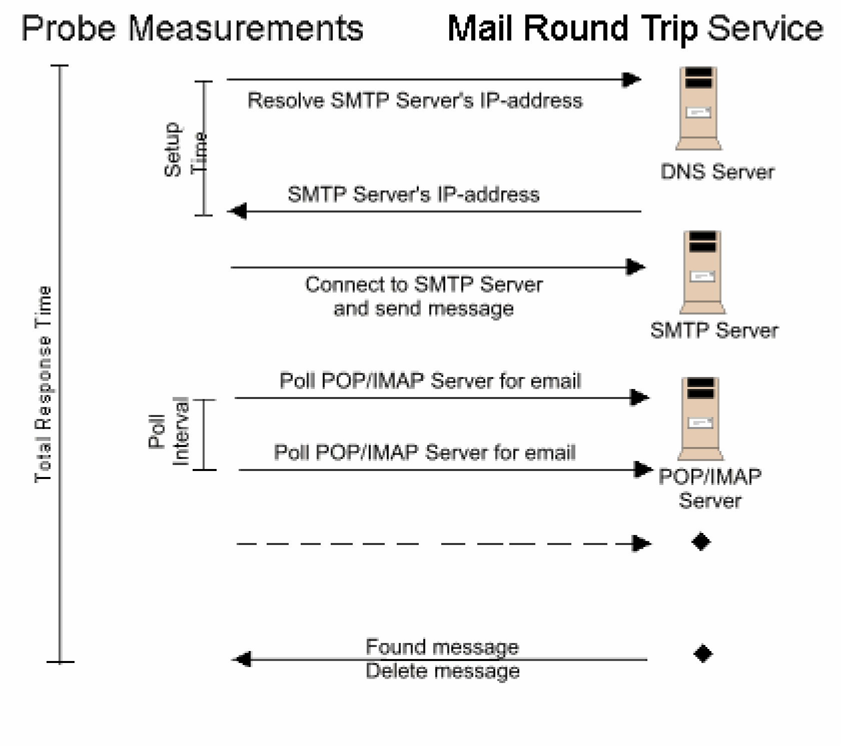
Note there are special considerations for using the Mail Round Trip probe to monitor the mail service as provided by Microsoft Exchange 2000/2003 server. Please refer to the online help for the Mail Round Trip service target for more information.

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.

You can configure the number and duration of retries to control how often the probe resends the request before the request timeout is reached.

See the Configuration Manager online help for details on configuring this probe.

The following diagram shows the steps the probe completes in measuring response time:

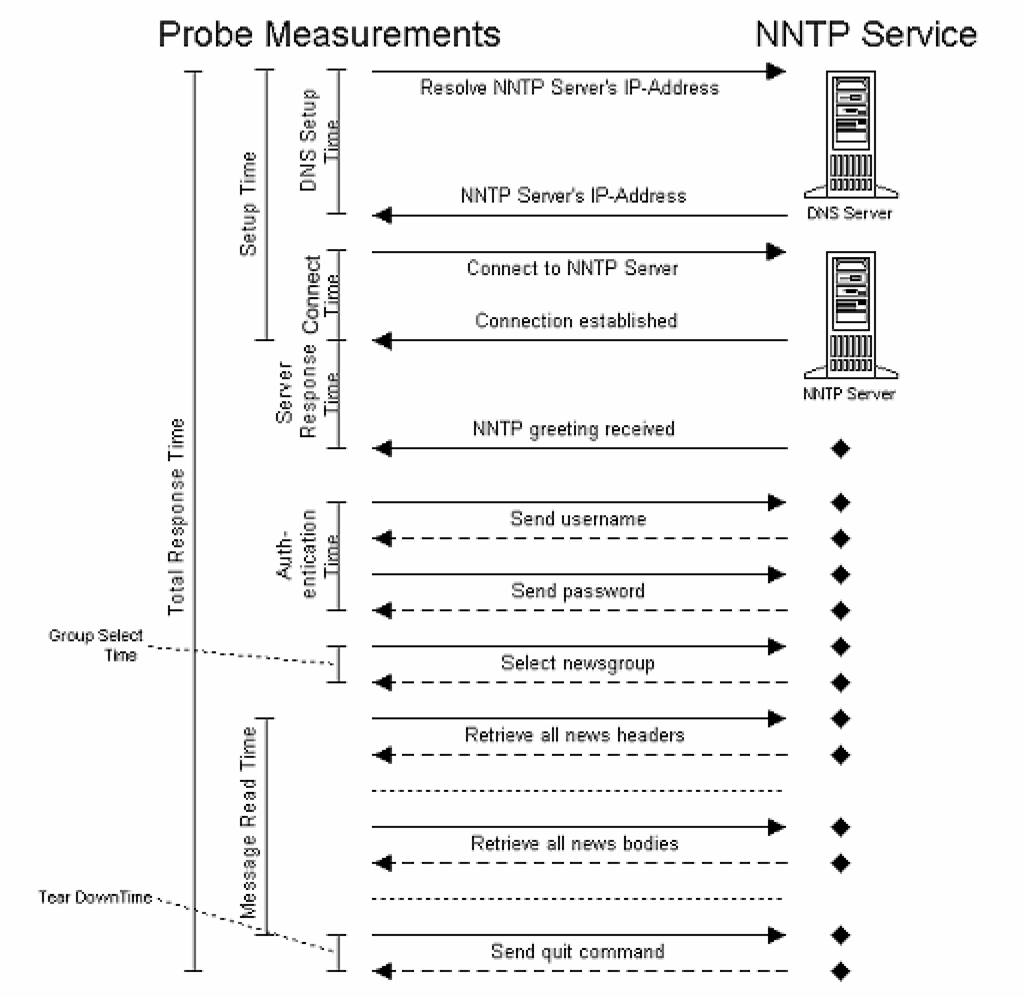


NNTP (Network News Transfer Protocol)

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.

See the Configuration Manager online help for details on configuring this probe.

The following diagram shows the steps the probe completes in measuring response time:

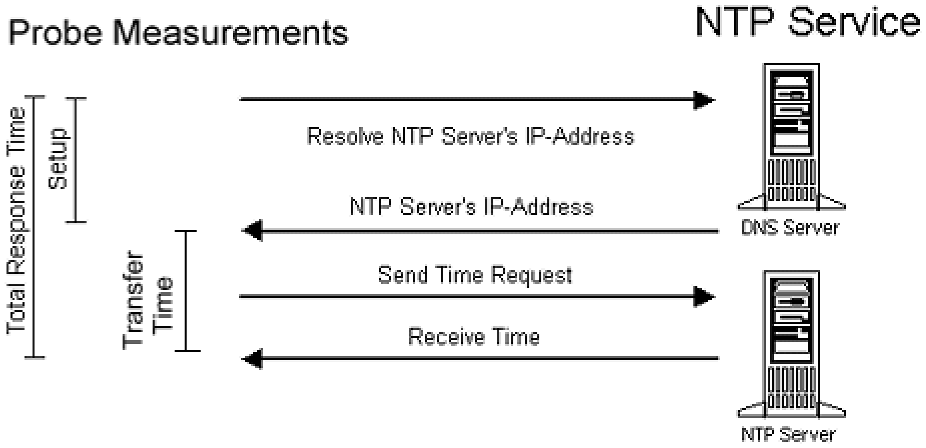


NTP (Network Time Protocol)

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.

See the Configuration Manager online help for details on configuring this probe.

The following diagram shows the steps the probe completes in measuring response time:



ODBC (Open Database Connectivity)

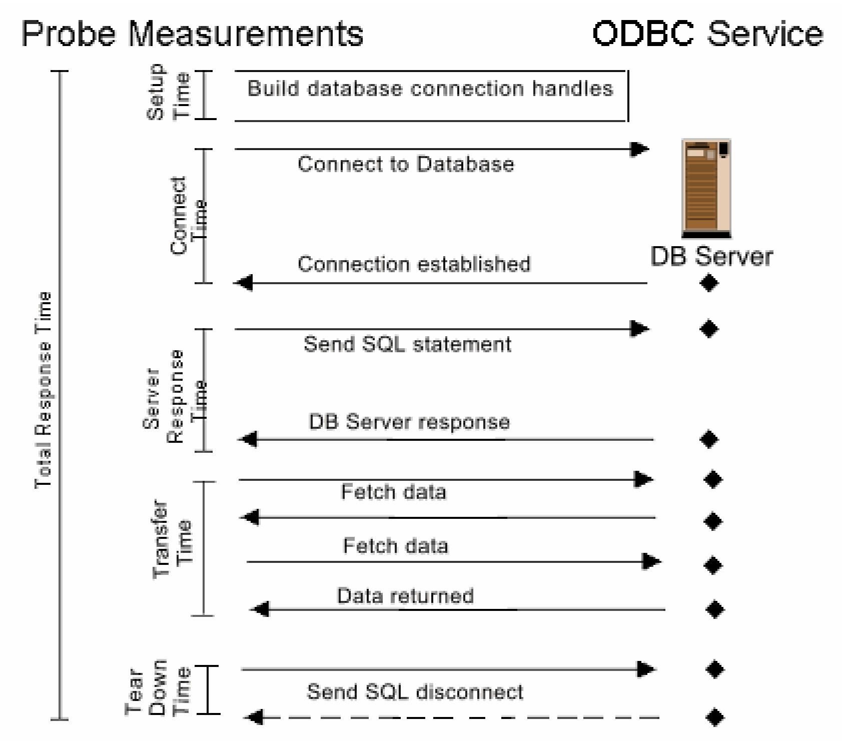
The ODBC (Open Database Connectivity) service is monitored via the ODBC probe. The ODBC probe is a generic database probe that monitors the availability of a database with a user defined SQL select statement. **The probe runs on Windows systems only.**

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 set up to access the SQL Server database. This may also include setting up trust relationships for the account across domains. Also only one account may be used for all ODBC 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. See the Configuration Manager online help for details on configuring this probe.

The following diagram shows the steps the probe completes in measuring response time:



POP3 (Post Office Protocol 3)

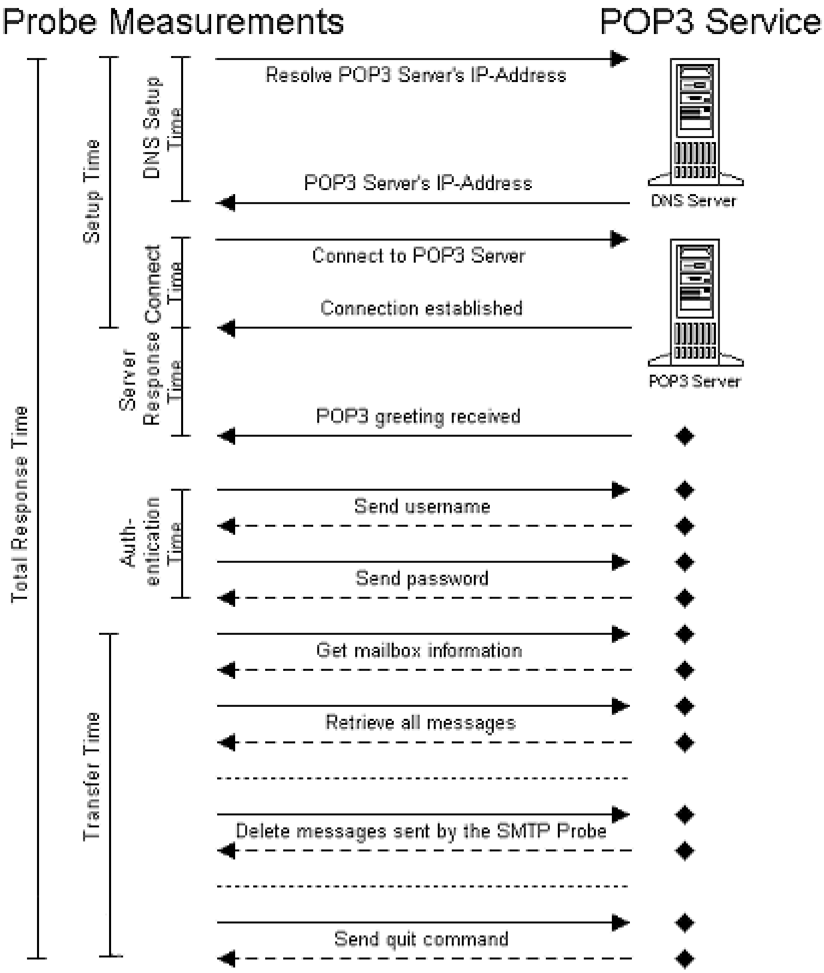
The POP3 probe emulates a user downloading email. After connecting to the POP3 server, the mailbox is authenticated by the specified username and password. On UNIX servers, this is typically the username and password of a local user. On Windows (for example, the Exchange Server), the username must include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

The POP3 probe pulls the e-mail off the server and down to the client (messages are no longer stored on the server). The probe retrieves all mail in the mailbox and scans for the OVIS-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 OVIS-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 2000/2003 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.

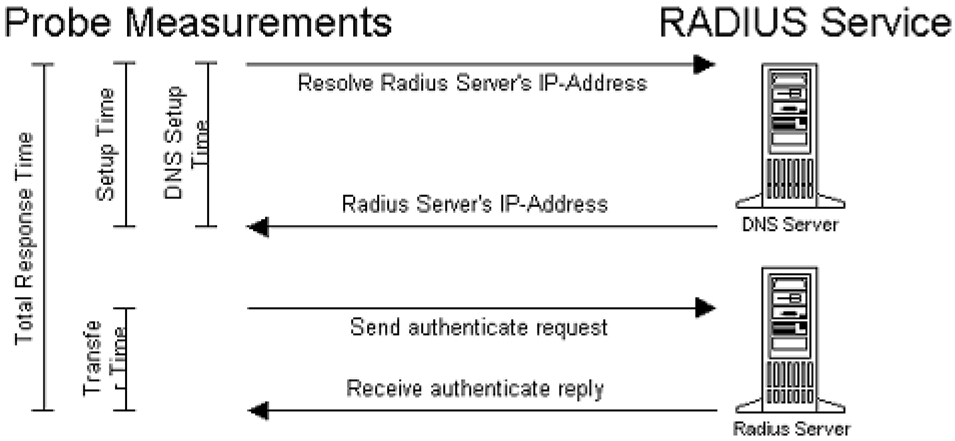
The following diagram shows the steps the probe completes in measuring response time:


Probe Measurements
POP3 Service
Total Response Time
Setup Time
DNS Setup Time
Connect Time
Server Response Time
Auth-entication Time
Transfer Time
Resolve POP3 Server's IP-Address
POP3 Server's IP-Address
DNS Server
Connect to POP3 Server
Connection established
POP3 Server
POP3 greeting received
Send username
Send password
Get mailbox information
Retrieve all messages
Delete messages sent by the SMTP Probe
Send quit command

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. It uses the UDP transport protocol to transact with the RADIUS server.

The following diagram shows the steps the probe completes in measuring response time:



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)

Note that MS CHAP is not supported.

The shared secret, username and password must be specified.

See the Configuration Manager online help for details on configuring this probe.

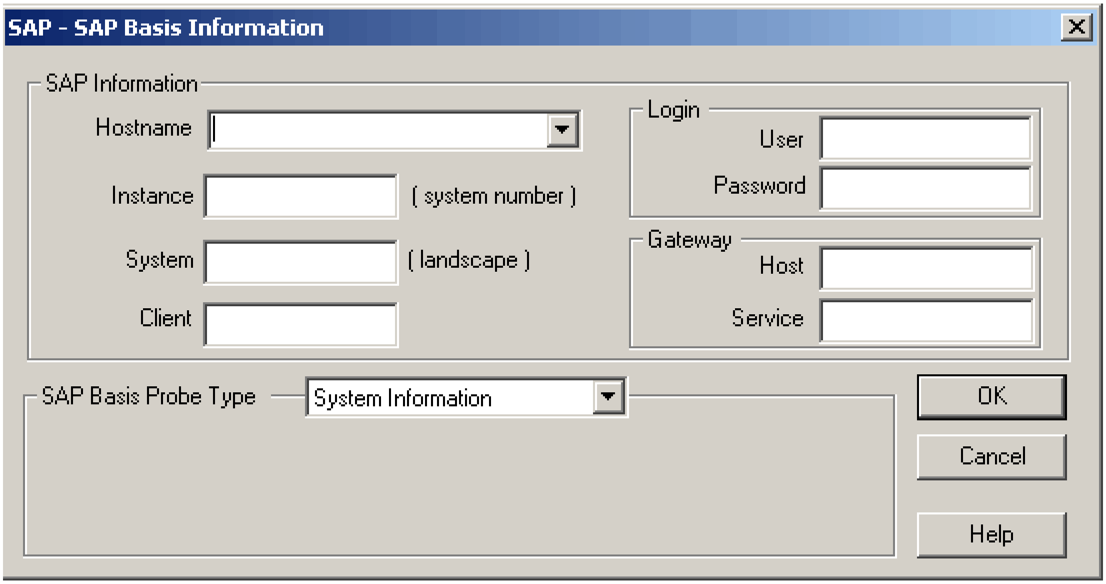
SAP Basis

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:

- **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 whether 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:



SAP Basis Probe Type: System Information

➤ 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 type 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 an RFC connection.

Set up an SAP User

1 Login 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 OpenView Operations SAP Smart Plug-in. If you have already configured this user you may use it. Or you may use a different user name as long as it has these attributes:

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

   Initial Password: any SAP-admissible 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 OpenView Operations SAP Smart Plug-in. 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 this is used with the OpenView Operations SAP Smart Plug-in, 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 that you already created.

5 Login to SAP as the user you created.

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

Configuring the SAP Probe

In configuring the probe, you need to enter the following:

- 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.
- 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.
- 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, transaction data, assigned user master records, charts of accounts and specific customizing parameters.
- If you select the Transaction type of SAP probe described above, then you must 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 follows:

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

MM (Material Management) - MB51, MB59

See the Configuration Manager online help for details on configuring this probe.

Script (generic script)

The Script probe runs a given script and monitors availability and response time. (See Collecting Additional Metrics on page 246 for how to configure a Script probe to collect additional metrics). Using the Script probe, you can monitor a generic application through a script without having to write a custom probe. Scripts may be written in VBScript, Javascript or Perl or run using batch, command and UNIX shells.

Distributing Files

You can either use the absolute path to the scripts or data files or use the Distribution Manager to have the files distributed to remote systems as well as the local system. To use the distribution manager, place your scripts and data files in the appropriate directory on the OVIS Management Server under the `<install dir>\newconfig\distrib\` directory prior to creating the probe. (See the note below for the appropriate subdirectory.) When you save the configuration, the files under `\newconfig\distrib\` are copied to the `<data dir>\bin\instrumentation\probe\scripts` directory on the probe system (note that Windows uses a \ (backslash) and UNIX systems use a / (forward slash)). Note it does not distribute directories, only files.

When a probe gets a new configuration, the distribution manager looks in the following directories for files, so you should place your scripts and data files in these directories according to the systems you want them distributed to:

`newconfig\distrib\all` - You should place files that are valid for all platforms and probe locations in the `all` directory.

`newconfig\distrib\platform\{Windows|HPUX|Linux|Solaris}` - Platform specific files can be placed in the `Windows`, `HPUX`, `Linux` and `Solaris` directories. The probe will only get files for the operating system under which it is running.

newconfig\distrib\location\{probe location as defined in the Configuration Manager} - It is further possible to create a directory under the location directory with the name of the probe location as it is configured in the Configuration Manager (usually the fully qualified hostname). For example, if the probe location is mysystem.mydomain.com, simply create a directory with the same name mysystem.mydomain.com and place the files in there.

Please note that these directories are not added, deleted or modified by OVIS! It is your responsibility to make sure that these directory names match what is configured in OVIS. Therefore, it is recommended to place files in the all and platform directory and only use the location directory if absolutely necessary. Further, please note that the Local System is actually the fully qualified domain name of the OVIS Management Server system. For example, if the name of the Management Server is ovis.domain.com, create the directory ovis.domain.com if you want to distribute files only to the Local System.

Configuring the Script Probe

Configure the Script probe in the Configuration Manager Script Service Target dialog box. Enter in the command to run the script, including the appropriate location and any parameters required. The script files distributed as described above are copied into the <data dir>\bin\instrumentation\probe\scripts directory for all the probe systems where the script probe runs. A script distributed in this manner may use the relative path scripts\<script name> for the appropriate location of the script. For example, when the script test.pl is copied to the <install dir>\newconfig\distrib\all directory, the following relative path may be used to configure the probe:

```
c:\Perl\bin\Perl.exe scripts\test.pl
```

The script you create should handle launching any applications or programs, returning the appropriate value for availability (1 or 0), and handling any error conditions. By default if the script completes it will be marked as available. If the script probe times out, it will be marked unavailable. Availability can also be determined by applying pattern matching or checking the exit code.

The script probe does not manage Child processes associated with a script or application. If the script probe times out and terminates a script or application, any associated child processes with the script or application must be manually terminated.

In configuring the Script probe, you can specify pattern matching to be applied to the output of the script. You can specify if you want the probe to check the script exit code when determining availability. You can specify if you want the probe to check for an interactive session, that is, if a user is logged on before running a script. You can append internal parameters of OVIS to your script and specify if you don't want results logged.

If you want to run the Script probe under a different logon session, you can set up the user and password required for authentication. Note that certain privileges are required for this logon session (see the Configuration Manager online help for information on setting these user rights).

Scripts run by the script probe can be impacted by the environment settings particularly with UNIX/Linux. You should be sure that the script is configured to run in the environment that is defined for the OVIS Scheduler (root .profile). This environment may be different from the environment that the script was created in (your user login .profile). An example of environment variables that may have an impact are locale settings of 'en_US' or 'C'.

If you are using the Script probe to launch application test tool scripts or other scripts that execute a multi-step transaction, you can specify a Results File to launch a second script to parse the output file from the main script or program. See Using a Results File below for details. You can also set the label for multi-step transaction to CustomerName:ServiceGroupName

It is recommended that only one target per service group be used for multi-step transactions. And there is a maximum of 100 steps.

See the Configuration Manager online help for details on configuring this probe.

Using a Results File

For a multi-step transaction, you can have your script send results (like StepResponseTime) to a Results File. Or if your script can write to the screen then you can have the results sent to STDOUT as it runs (without writing to a file). The script probe will capture the output either way. Configure this in the Configuration Manager Script Service dialog as follows:

- In the first case, enter the Results File name in the Results File Script field
- In the second case where your script outputs to the screen, enter the script name itself in the Results File Script field.

Format and Example Results File or Output

The format for the entries in the Results File (or output to the screen) is as follows (see Notes on Results File Output on page 244 for definitions of these entries):

For multi-step scripts:

StepName
StepSetupTime
StepTransferTput
StepMetric_1
StepMetric_2
StepMetric_3
StepMetric_4
StepMetric_5
StepMetric_6
StepMetric_7
StepMetric_8
ErrorInfo
StepTimestamp
StepAvailability
StepResponseTime

For the final metrics (Availability and ResponseTime are required):

Target
SetupTime
TransferTput
Metric_1

Metric_2
Metric_3
Metric_4
Metric_5
Metric_6
Metric_7
Metric_8
ErrorInfo
Timestamp
Availability
ResponseTime

Note that these step metrics and final metrics are case sensitive so you must use the exact capitalization above. Metric_1 - Metric_8 and StepMetric_1 - StepMetric_8 are for additional user-defined metrics your script is collecting. See Collecting Additional Metrics on page 246 for how to set this up.

An example Results File

```
############### win_script3.sh

StepName=Test_00
StepAvailability=1
StepResponseTime=1.51
StepName=Test_01
StepAvailability=1
StepResponseTime=3.51
StepName=Test_02
StepAvailability=1
StepResponseTime=17.563451
StepName=Test_03
StepAvailability=1
StepResponseTime=22.7656542491
Availability=1
ResponseTime=42.16243
#############
```

Notes on Results File Output

See the following notes about the results file output:

- The parameters in the Results File (or output) can be in any order. Except that once the Script probe finds a **complete measurement** either in the step or in the final wrap-up, it will consider the step or measurement done and thus not read any additional output for that step. A complete measurement string for a step consists of StepName, StepResponseTime and StepAvailability or for the final transaction it consists of ResponseTime and Availability.

- Use the **Target** parameter if your script passes in what the target output is.
- Use **SetupTime** if your results include setup time as a component of response time. Use **TrasferTput** if your results include a transfer throughput time measurement.
- If your results include **ErrorInfo**, be sure it is output at the beginning or middle of the results. If it is at the end, after the Script probe finds a complete measurement, the Script probe will include the ErrorInfo as part of the next step.
- Also be sure that your script does not output ErrorInfo if there is no failure.
- In addition, ErrorInfo must be less than 256 characters and StepName must be less than 250 characters. If you exceed this limit the field is either truncated or the script probe fails executing.
- The **Timestamp** and **StepTimestamp** allow you to include an external timestamp. The Timestamp and StepTimestamp format is in epoch time (seconds since 1/1/70). The following VB script can be used to convert date to timestamp format:

```
TimeZoneSec = 28800 ‘PST

DateToEpoch = DateDiff(“s”, “00:00:00 1/1/1970”, Now()) +
TimeZoneSec
```

- For **Availability and ResponseTime**, your script needs to add up the total for the transaction (summary roll-up of all the steps). The Script probe does not do this calculation for you. Also Availability and ResponseTime need to be the last lines in the results output.
- **StepMetric** is used (for example StepMetric_1) if you are collecting metrics for steps. If you want to also report the total measurement for all steps, your script must do the summary roll-up of all the steps into a Metric value (for example Metric_1) specified as a final metric. The Script probe does not do any calculations for you.

Collecting Additional Metrics

Out of the box the script probe collects the following metrics: Availability and Response Time. You can configure the script probe to collect additional metrics based on the scripts you are running.

The process you would go through to begin collecting additional metrics is shown below (more details for these steps follows):

1 Decide what metrics to collect.

2 Make sure your script collects these metrics and outputs the results in the correct format to be picked up by the probe. See Results Script to Output Additional Metrics on page 246 below for details.

3 Decide on the metric labels, units and if there will be separate step metrics that require summarization. The summarization will need to be done by your script to output final metrics since the script probe does not do any calculation.

4 Create a customized SRP file for the script probe. See SRP File for Additional Metrics on page 248 for details.

5 Put the scripts in the proper location to be distributed.

6 Load the SRP file from the Configuration Manager. See Load SRP File on page 256 for details.

7 Configure the script probe. For each script probe SRP file you load, you will see a separate probe type listed in the probe type selection screen. See Configure Probe to Collect Metrics on page 256 for details.

Note that no reports (from the Reports workspace of the Dashboard) will be available for these customized script probes.

Results Script to Output Additional Metrics

For the script probe to collect additional user-defined metrics, you must create a Results Script that outputs the metrics in the correct format. If your script can write to the screen then you can have the metrics results sent to STDOUT or the metrics results can be written to a Results File. For details on the Results file format see Format and Example Results File or Output on page 243.

See the example `.vbs` script below (collects the total disk size, total free space on the disk, and percent available disk space).

Example Script that Collects Additional Metrics

```
strComputer = "."

totalsize = 0.0
totalfree = 0.0
totalAvail= 0.0
probeAvail= 0

Set objWMIService = GetObject("winmgmts:" _
    & "{impersonationLevel=impersonate}!\\" _
    & strComputer & "\root\cimv2")
Set colDisks = objWMIService.ExecQuery _
    ("Select * from Win32_LogicalDisk where DeviceID = 'c:'")
For Each objDisk in colDisks
    freePercent = 0.0
    if( objDisk.Size > 0 ) then
       freePercent = ((objDisk.FreeSpace)/(objDisk.Size))
       totalsize = totalsize + objDisk.Size
       totalfree = totalfree + objDisk.FreeSpace
    end if
Next

Wscript.Echo "Target=Drive(c)"
Wscript.Echo "ResponseTime=0"
Wscript.Echo "Metric_1=" _
   & totalsize

Wscript.Echo "Metric_2=" _
   & totalfree

if( totalsize > 0 ) then
   totalAvail = (totalfree/totalsize) * 100
end if

if( totalAvail > 0 ) then
   probeAvail= 1
end if

Wscript.Echo "Metric_3=" _
   & totalAvail

Wscript.Echo "Availability=" _
   & probeAvail

wscript.Quit(0)
```

Example Results File with Additional Metrics

The example script above would give the following Results output when executed:

```
***-*Example output from script when excuted.
-----------------------------------------
Target=Drive(c)
ResponseTime=0
Metric_1=60003868672
Metric_2=38358384640
Metric_3=63.9265192210839
Availability=1
```

SRP File for Additional Metrics

To get the additional user-defined Script probe metrics to be reported in the Dashboard, you need to add the metrics to a customized script probe SRP file and then load this SRP file into OVIS. (See Load SRP File on page 256.) There is no syntax check on the SRP file when you load it so take care in creating the SRP file. You can use `trace.repload` to see what was loaded if you encounter problems.

Note that after loading the SRP file, changes to probe definitions will not be reflected in the Dashboard until the `ovtomcatA` service is refreshed. To refresh the service, run the following at the command line: `ovc -restart ovtomcatA`.

The SRP file describes the probe, probe parameters, metrics collected and default conditions such as SLOs and alarms. Use the Example Script SRP File below as a guide for how your customized script probe SRP file should be laid out.

You can add or remove metrics from your customized script probe SRP file. If you make changes to the SRP file, remember to reload the SRP file and restart `ovtomcatA` service for changes to take affect. See Load SRP File on page 256.

Note that your script probe SRP file can contain multiple script probe metric definitions. Also note that you can create a script probe SRP file for each script probe you plan to run.

The key item that cannot be changed in the script probe SRP file is the `PROBE: probeScript` value; this is what tells OVIS it is a script probe. Also PARAMETER values in the SRP file cannot be changed.

For example, to add a metric, you would add these lines to the SRP file:

METRIC: DISK_METRIC

LABEL: Disk Free Space

STDMETRIC: M2

UNITS: MBytes

FORMAT: 0.0000

DEFAULT_CONDITION: <

The METRIC value is what is collected. The LABEL is the name that will be displayed in the Dashboard. The STDMETRIC value is M1 - M8. The UNITS value is the metric’s units. Possible UNITS include: Percent, Seconds, Count, KBytes/Sec, Bytes, Number, Status Code, Trans/Sec, FailedTran/Sec, Avg. Bytes, Mbit/s, MB. The DEFAULT_CONDITION is either < or > and identifies whether the SLO should be either greater than the value (as in availability greater than 95%) or less than the value (as in response time less than 5 seconds).

Example Script SRP File

An example script probe SRP file for the Example Script that Collects Additional Metrics is shown below. The script probe name is SCRIPT_DISK.

```
# ##########################################################
# OpenView Internet Services Example script probe SRP file
##########################################################
PACKAGENAME: DiskSpace

PROBENAME:  SCRIPT_DISK
    DESCRIPTION:    SCRIPT_DISK_SPACE - WMI Disk space
    PROBEMETRICLIST:    IOPS_SCRIPT_DISK
    IDENTIFIER:     HOST
    INSTANCEID:     TARGET
    DEFAULT_TARGET:
    DEFAULT_PORT:
    PROBE:          probeScript
    TRANSPORT:
    PARAMETER1:     script
    PARAMETER2:     pattern
    PARAMETER3:     patternConfig
    PARAMETER4:     chkstat
    PARAMETER5:     ofile
    PARAMETER6:     options
    PARAMETER7:     username
    PARAMETER8:     password
    END_PROBENAME:


PROBEMETRICS:   IOPS_SCRIPT_DISK

    METRIC:     AVAILABILITY
    UNITS:  Percent
    DEFAULT_CONDITION:  >
    DEFAULT_SERVICE_LEVEL: 90.000
    DEFAULT_WARNING:    90.000
    DEFAULT_BASELINE:   80.000
    DEFAULT_DURATION:   600
    DEFAULT_MESSAGE:    SCRIPT Service for <TARGET> is unavailable

    METRIC:     RESPONSE_TIME
    UNITS:  Seconds
    DEFAULT_CONDITION:  <
    DEFAULT_SERVICE_LEVEL: 2.000
    DEFAULT_WARNING:    4.000
    DEFAULT_BASELINE:   80.000
    DEFAULT_DURATION:   600
    DEFAULT_MESSAGE:    SCRIPT Service RESPONSE_TIME is slow
(<VALUE> vs <THRESHOLD>) on <TARGET>

    METRIC:     SETUP_TIME
    UNITS:  Seconds
    DEFAULT_CONDITION:  <
    DEFAULT_WARNING:    3.000
    DEFAULT_BASELINE:   80.000
    DEFAULT_DURATION:   600
   DEFAULT_MESSAGE:   Script 'x' is slow  (<VALUE> vs <THRESHOLD>)
on <TARGET>

    METRIC:     TRANSFER_TPUT
    UNITS:  KBytes/Sec
    DEFAULT_CONDITION:  >

    METRIC:     DISK_SIZE
    LABEL: Disk Size
    STDMETRIC:  M1
    UNITS:  MBytes
    FORMAT: 0.000
    DEFAULT_CONDITION:  <

    METRIC:     FREE_SPACE
    LABEL: Free Space
    STDMETRIC:  M2
    UNITS:  MBytes
    FORMAT: 0.000
    DEFAULT_CONDITION:  <

    METRIC:     PERCENT_AVAILABLE
    LABEL: Percent Available
    STDMETRIC:  M3
    UNITS:  Percent
    FORMAT: 0.000
    DEFAULT_CONDITION:  >

    END_PROBEMETRICS:
```

Another Example Script SRP File

Another example script probe SRP file is shown below. Example results files from various conditions are shown following this example.

Note that in this SRP file the parameters FORMAT, COMPOSITE_METRIC and COMPOSITE_ORDER are used. These parameters can only be added manually into the SRP file (are not input from the Configuration Manager). These parameters, like create a stacked bar chart, are set for you on standard metrics, but for user-defined metrics in the Script probe you would need to specify in your customized Script probe SRP file.

FORMAT - Used to set the display format for a metric (e.g., FORMAT: 0.000 will display a number with only 3 digits after the decimal). The value for FORMAT follows the Java formatter convention.

COMPOSITE_METRIC and COMPOSITE_ORDER - Used by the OVIS Dashboard to create a stacked bar chart. The COMPOSITE_METRIC specifies the parent metric (usually response time) and the COMPOSITE_ORDER specifies the position fo the metric within the bar chart.

```
##########################################################
# OV internet services Example SRP File
##########################################################

PROBENAME: TEST_PROBE_ALPHA
    DESCRIPTION:      Test - Test Probe Alpha
    PROBEMETRICLIST:  IOPS_TEST_PROBE_ALPHA
    IDENTIFIER:       URL
    INSTANCEID: URL
    DEFAULT_TARGET:
    DEFAULT_PORT:
    PROBE:       probeScript
    TRANSPORT:
    PARAMETER1:   script
    PARAMETER2:   pattern
    PARAMETER3:   patternConfig
    PARAMETER4:   chkstat
    PARAMETER5:   ofile
    PARAMETER6:   options
    PARAMETER7:   username
    PARAMETER8:   password
    END_PROBENAME:

PROBEMETRICS:     IOPS_TEST_PROBE_ALPHA

    METRIC:     AVAILABILITY
    UNITS:    Percent
    DEFAULT_CONDITION:    >
    DEFAULT_SERVICE_LEVEL: 90.000000
    DEFAULT_WARNING:  90.000000
    DEFAULT_MINOR:    0.000000
    DEFAULT_MAJOR:    0.000000
    DEFAULT_CRITICAL:    0.000000
    DEFAULT_BASELINE:    80.000000
    DEFAULT_DURATION:    600
    DEFAULT_MESSAGE: Test Service for <TARGET> is unavailable

    METRIC:    SETUP_TIME
    UNITS:    Seconds
    DEFAULT_CONDITION:    <
    DEFAULT_SERVICE_LEVEL: 1.000000
    DEFAULT_WARNING:  3.000000
    DEFAULT_MINOR:    0.000000
    DEFAULT_MAJOR:    0.000000
    DEFAULT_CRITICAL:    0.000000
    DEFAULT_BASELINE:    80.000000
    DEFAULT_DURATION:    600
    DEFAULT_MESSAGE: Test Service SETUP_TIME is slow  (<VALUE> vs
<THRESHOLD>) on <TARGET>

    METRIC:    METRIC_1_TIME
    STDMETRIC:    M1
    LABEL:   Transfer Time
    UNITS:   Seconds
    FORMAT:  0.000
    COMPOSITE_METRIC:       RESPONSE_TIME
    COMPOSITE_ORDER:        1
    DEFAULT_CONDITION:     <
    DEFAULT_SERVICE_LEVEL:   1.500
    DEFAULT_WARNING:    2.000
    DEFAULT_BASELINE:      80.000
    DEFAULT_DURATION:      600
    DEFAULT_MESSAGE: Test Service METRIC_1_TIME is slow  (<VALUE>
vs <THRESHOLD>) on <TARGET>

    METRIC:    METRIC_2_TIME
    STDMETRIC:    M2
    LABEL:    Auth Time
    UNITS:    Seconds
    FORMAT:   0.000
    COMPOSITE_METRIC:       RESPONSE_TIME
    COMPOSITE_ORDER:        2
    DEFAULT_CONDITION:     <
    DEFAULT_SERVICE_LEVEL:   1.500
    DEFAULT_WARNING:    2.000
    DEFAULT_BASELINE:     80.000
    DEFAULT_DURATION:     600
    DEFAULT_MESSAGE: Test Service METRIC_2_TIME is slow  (<VALUE>
vs <THRESHOLD>) on <TARGET>

    METRIC:    METRIC_3_TIME
    STDMETRIC:    M3
    LABEL:    Send Time
    UNITS:    Seconds
    FORMAT:   0.000
    COMPOSITE_METRIC:       RESPONSE_TIME
    COMPOSITE_ORDER:        3
    DEFAULT_CONDITION:    <
    DEFAULT_SERVICE_LEVEL:  1.500
    DEFAULT_WARNING:  2.000
    DEFAULT_BASELINE:    80.000
    DEFAULT_DURATION:    600
    DEFAULT_MESSAGE: Test Service METRIC_3_TIME is slow  (<VALUE>
vs <THRESHOLD>) on <TARGET>

    METRIC:     RESPONSE_TIME
    UNITS:     Seconds
    DEFAULT_CONDITION:     <
    DEFAULT_SERVICE_LEVEL: 2.000000
    DEFAULT_WARNING:  0.000000
    DEFAULT_MINOR:    0.000000
    DEFAULT_MAJOR:    0.000000
    DEFAULT_CRITICAL:    0.000000
    DEFAULT_BASELINE:    0.000000
    DEFAULT_DURATION:    600
   DEFAULT_MESSAGE:    Test Service RESPONSE_TIME is slow (<VALUE>
vs <THRESHOLD>) on <TARGET>

    METRIC:    TRANSFER_TPUT
    UNITS:     Bytes/Sec
    DEFAULT_CONDITION:     >
    DEFAULT_SERVICE_LEVEL: 0.000000
    DEFAULT_WARNING:  0.000000
    DEFAULT_MINOR:    0.000000
    DEFAULT_MAJOR:    0.000000
    DEFAULT_CRITICAL:    0.000000
    DEFAULT_BASELINE:    0.000000
    DEFAULT_DURATION:   0
    DEFAULT_MESSAGE:

    END_PROBEMETRICS:
```

The following Results files give example output from a fictious script matching the SRP file shown above. The first example shows results when there is a problem in step 2 and the probe returns availability and response time of 0.

Results Example 1

```
Target=MyServer.test@80_To_HisServer.Test@90

StepSetupTime=0.001

StepTransferTput=123

StepMetric_1=1.5

StepMetric_2=5.5

StepMetric_3=9.5

StepResponseTime=16.501

StepAvailability=1

StepName=Connect To MyServer@80

StepMetric_1=0

StepMetric_2=0

StepMetric_3=0
```

```
StepResponseTime=0

StepAvailability=0

StepName=Connect To HisServer@90

ResponseTime=0

ErrorInfo=System down, error returned is x00005, status 500.
Metric_1=0 Metric_2=0 Metric_3=0 Availability=0
```

Results Example 2

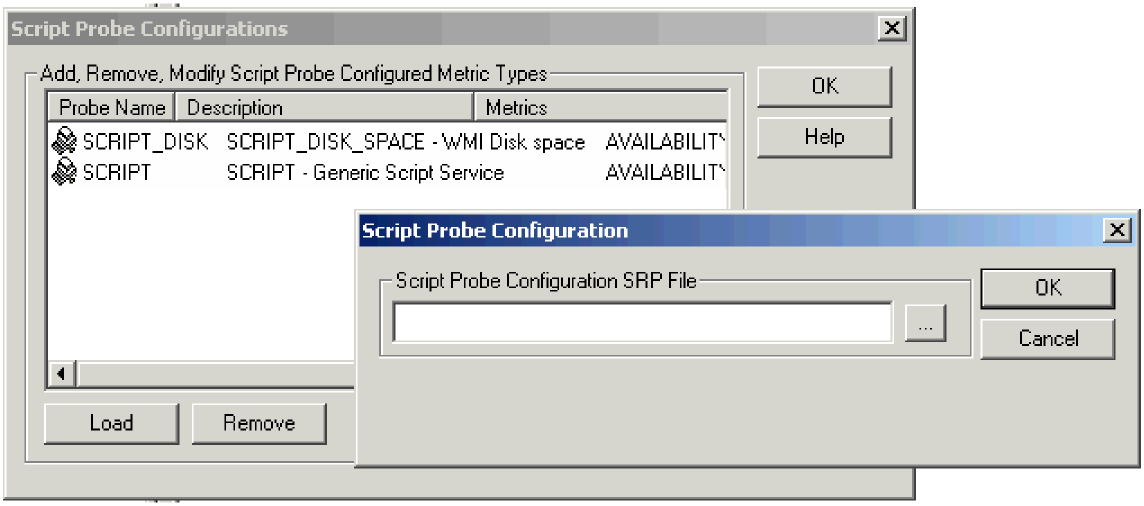
The second example shows results when all steps are available.

```
Target=MyServer.test@80_To_HisServer.Test@90

StepSetupTime=0.001

StepTransferTput=123

StepMetric_1=1.5

StepMetric_2=5.5

StepMetric_3=9.5

StepResponseTime=16.501

StepAvailability=1

StepName=Connect To MyServer@80

StepSetupTime=0.001

StepTransferTput=345

StepMetric_1=1.33

StepMetric_2=2.33

StepMetric_3=3.34

StepResponseTime=7.000

StepAvailability=1

StepName=Connect To HisServer@90

ResponseTime=23.502

Metric_1=2.83

Metric_2=7.83

Metric_3=12.84

Availability=1
```

Load SRP File

Once you have created a script probe SRP file, load the SRP file into OVIS from the Configuration Manager **File > Configure > Script Probe Metrics** dialog. There is no syntax check on the SRP file when you load it. You can use `trace.repload` to see what was loaded if you encounter problems.

➤ After loading the SRP file, changes to probe definitions will not be reflected in the Dashboard until the `ovtomcatA` service is refreshed. To refresh the service, run the following at the command line: `ovc -restart ovtomcatA`.



Script Probe Configurations

Add, Remove, Modify Script Probe Configured Metric Types

Probe Name	Description	Metrics
SCRIPT_DISK	SCRIPT_DISK_SPACE - WMI Disk space	AVAILABILIT
SCRIPT	SCRIPT - Generic Script Service	AVAILABILIT

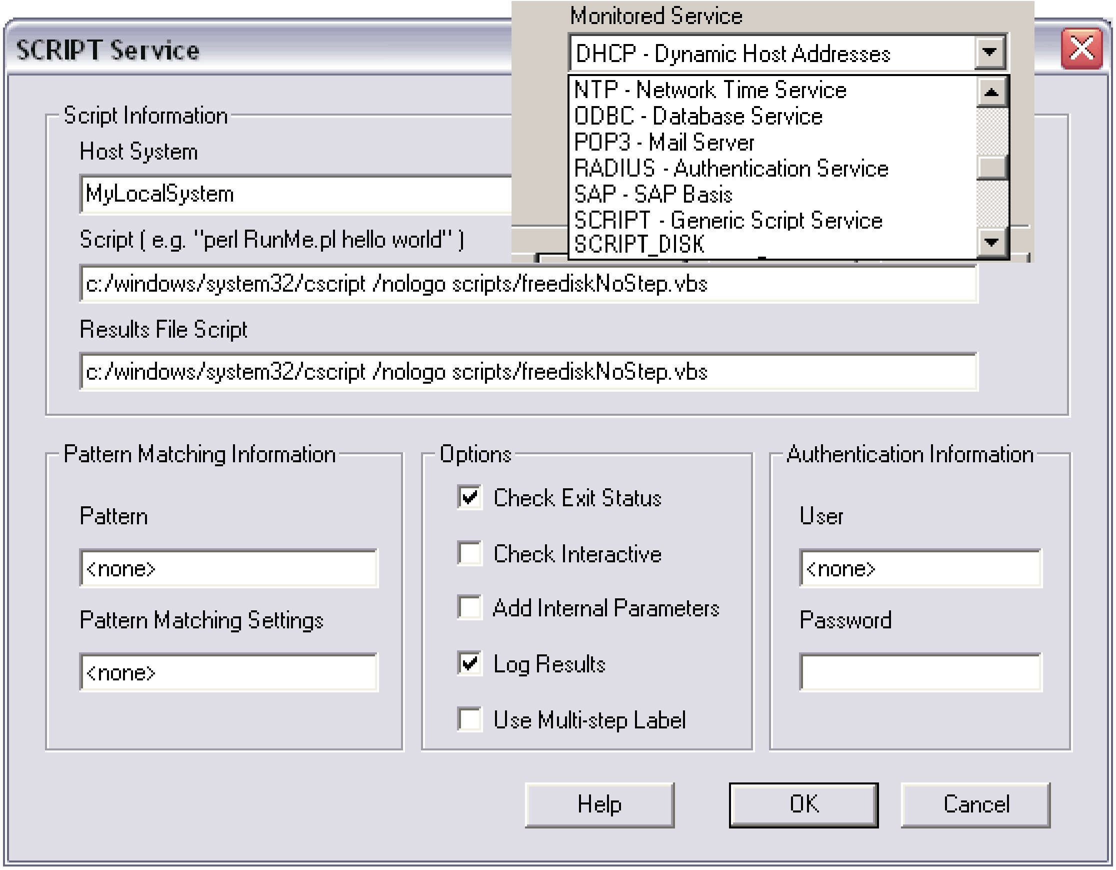
Script Probe Configuration

Script Probe Configuration SRP File

Configure Probe to Collect Metrics

After loading the customized script probe SRP file you created, you can configure a script probe in the Configuration Manager.

The probe type you select will be the probe name you configured in the SRP file. In the example above `PROBENAME: SCRIPT_DISK`. See the following screen shot example.



SCRIPT Service

Monitored Service: DHCP - Dynamic Host Addresses

Script Information

Host System: MyLocalSystem

Script (e.g. "perl RunMe.pl hello world"): c:/windows/system32/cscript /nologo scripts/freediskNoStep.vbs

Results File Script: c:/windows/system32/cscript /nologo scripts/freediskNoStep.vbs

Pattern Matching Information

Pattern: <none>

Pattern Matching Settings: <none>

Options

☑ Check Exit Status

☐ Check Interactive

☐ Add Internal Parameters

☑ Log Results

☐ Use Multi-step Label

Authentication Information

User: <none>

Password:

NTP - Network Time Service
ODBC - Database Service
POP3 - Mail Server
RADIUS - Authentication Service
SAP - SAP Basis
SCRIPT - Generic Script Service
SCRIPT_DISK
Help
OK
Cancel

Another Script Probe Example

The following is a VBScript example to echo “Hello World” to the Console and return an exit code of 0 when finished:

Create the file **helloworld.vbs** and add the code below and save the file to `<install dir>\newconfig\distrib\all` directory on the OVIS Management Server:

```
WScript.Echo "Hello World"

WScript.Quit 0
```

Here's the syntax to run the `helloworld.vbs`:

```
cscript.exe /nologo scripts\helloworld.vbs
```

On the **cmd.exe** shell use the `/c` option to terminate the shell when processing is completed.

```
cmd.exe /c dir c:\winnt\system32
```

More examples:

```
c:\tests\runA.bat
```

```
netstat /a
```

```
ping mysystem
```

Note spaces in the path must be delimited by an escape quote when running the script probe on both Windows and UNIX platforms. For example:

```
"c:\my tests\runB.bat"
```

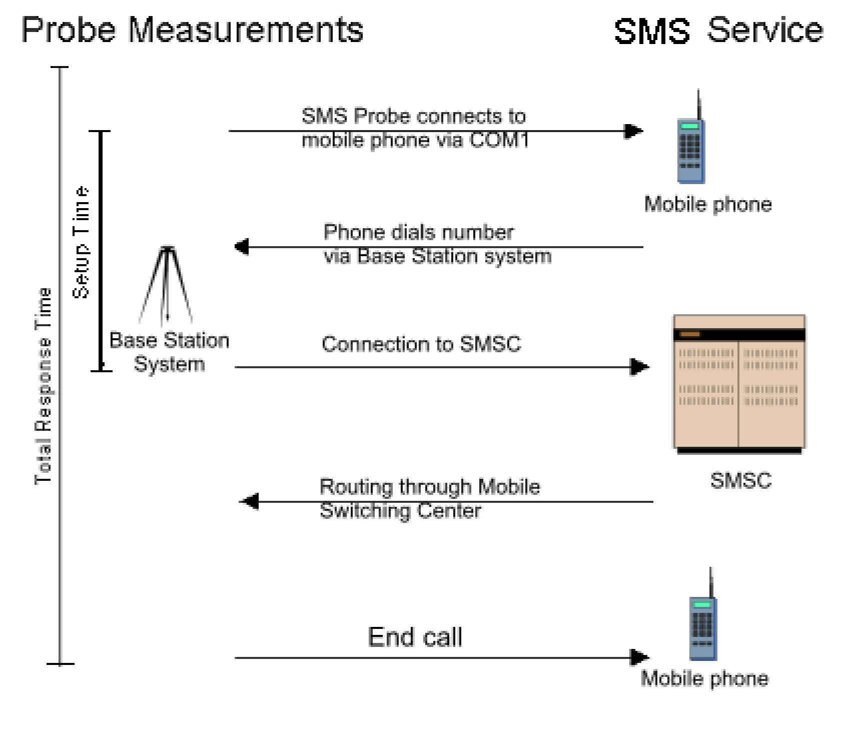
SMS (Short Message Service)

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 probe works on the Windows platform only.**

The phone connects to the PC’s COM port using a data cable. The probe can change the target SMSC of the sending phone automatically, 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 `<data dir>\conf\probe` directory on the Management Server) to set up the configuration for a specific vendor’s phone.

The following diagram shows the steps the probe completes in measuring response time:



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 `<data dir>\conf\probe` directory on the Management Server) 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.

See the Configuration Manager online help for details on configuring this probe.

SMTP (Simple Mail Transfer Protocol)

SMTP (Simple Mail Transfer Protocol) is the primary service used for sending e-mail. It has evolved into ESMTP (Enhanced SMTP). ESMTP is the same as Authenticated SMTP (A-SMTP). The SMTP/ESMTP/A-SMTP 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/ESMTP/SMTP-A 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. The probe pushes the message out to the Internet but doesn't verify that the message was received.

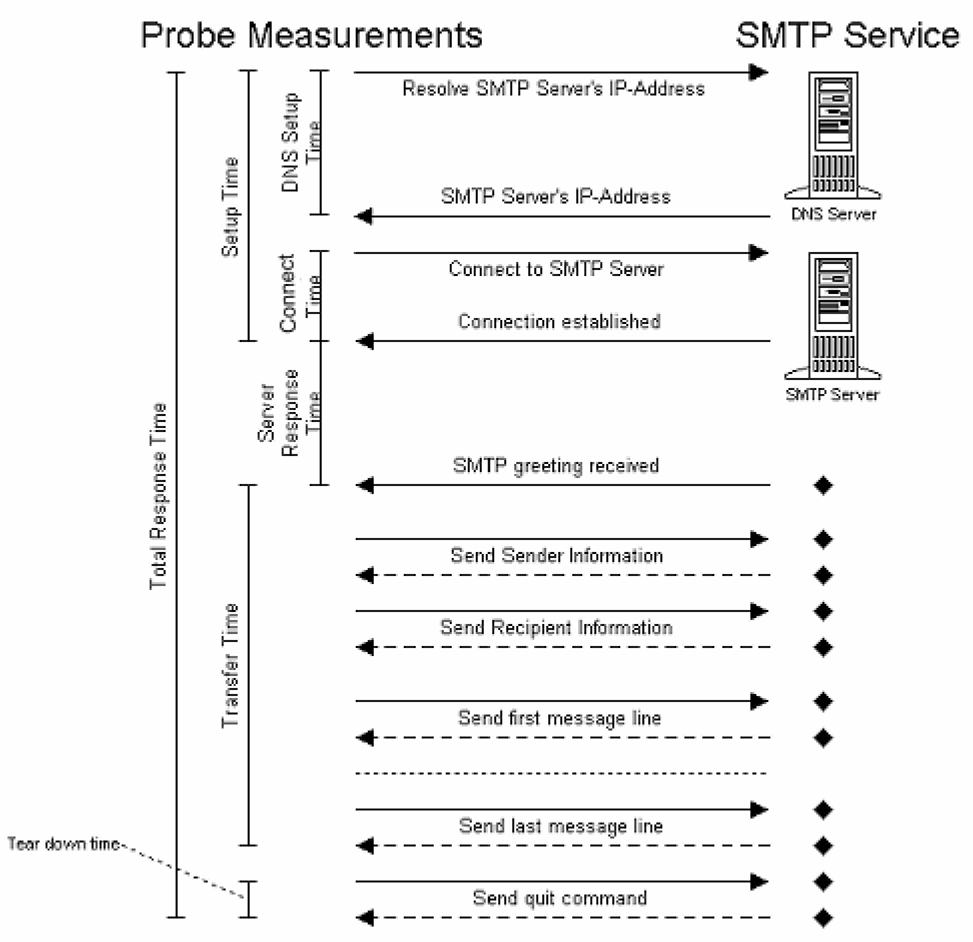
⚠ Make sure to use the POP3 or IMAP4 probe in conjunction with the SMTP probe. The POP3 or IMAP4 probes can delete the messages that are sent by the SMTP probe. Otherwise the recipient's mailbox will be flooded with messages.

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.

The recipient field specifies the email address, which must be resolvable by the SMTP server. Usually, it is in the form <username>@<server>.<domain> (for example: 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, you must enter username and password information to authenticate the mail send request.

The following diagram shows the steps the probe completes in measuring response time:

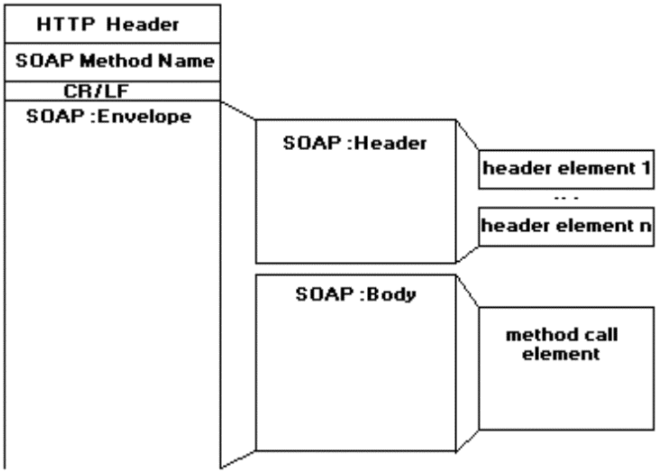


SOAP (Simple Object Access Protocol)

The SOAP probe supports SOAP 1.1 requests. Simple Object Access Protocol (SOAP) provides a simple and lightweight way to exchange structured and typed information in a decentralized, distributed environment using XML. SOAP consists of three parts:

- The SOAP envelope - which defines a framework for expressing what is in a message, who should deal with it and whether it is optional or mandatory.
- The SOAP encoding rules - which defines a mechanism used to exchange instances of application-defined datatypes.
- The SOAP RPC representation - which defines a convention used to represent remote procedure calls and responses.

All SOAP messages are encoded using XML. The SOAP message is an XML document. Within this, the SOAP payload is encapsulated within the mandatory SOAP envelope. The SOAP envelope, in turn, consists of an optional SOAP header and a mandatory SOAP body. The SOAP header is optional but if present must immediately follow the opening envelope (root) XML tag. If it exists, you'll likely find one or more header elements that provide metainformation regarding the method call. The SOAP body contains the serialized method arguments. The remote method name is to be used to name the method call's XML element, and it must immediately follow the SOAP body opening XML tag.



You configure the SOAP probe using the same Configuration Manager dialog as for the HTTP and HTTPS probes, but in addition you enter a **SOAPAction** (for a SOAP 1.1 request). Note that SOAP 1.2 does not use the SOAPAction request header.

And you specify a path for a **POST Data file** containing the data that will be posted to the Web application. The file must be available directly to the probe so be sure the file is on the probe system and the path specified is valid on the remote system. This allows for the posting of your SOAP request. The most likely use is to post form data to a Web application (e.g., CGI, ASP, Java Servlet).

Additionally, a search pattern can be configured which is applied to the XML.

You can either use the absolute path to the POST Data file or use the Distribution Manager to have the data files distributed to remote systems. To use the distribution manager, place your data files in the appropriate directory on the OVIS Management Server under the `<install dir>\newconfig\distrib\` directory, prior to creating the probe. (See the note below for the appropriate subdirectory.) When you save the configuration, the files under `newconfig\distrib\` are copied to the `<data dir>\bin\instrumentation\probe\scripts` directory on the probe system.

When a probe gets a new configuration, the distribution manager looks in the following directories for files, so you should place your data files in these directories according to the systems you want them distributed to:

`newconfig\distrib\all` - You should place files that are valid for all platforms and probe locations in the all directory.

`newconfig\distrib\platform\{Windows|HPUX|Linux|Solaris}` - Platform specific files can be placed in the Windows, HPUX, Linux and Solaris directories. The probe will only get files for the OS under which it is running.

`newconfig\distrib\location\`{probe location as defined in the Configuration Manager} - It is further possible to create a directory under the location directory with the name of the probe location as it is configured in the Configuration Manager (usually the fully qualified hostname). For example, if the probe location is `mysystem.mydomain.com`, simply create a directory with the same name `mysystem.mydomain.com` and place the files in there.

Please note that these directories are not added, deleted or modified by OVIS! It is the user's responsibility to make sure that these directory names match what is configured in OVIS. Therefore, it is recommended to place files in the `all` and `platform` directory and only use the `location` directory if absolutely necessary. Further, please note that the Local System is actually the Fully Qualified Domain Name of the OVIS Management Server system. For example, if the name of the OVIS Management Server is `ovis.domain.com`, create the directory `ovis.domain.com` if you want to distribute files only to the Local System.

See the Configuration Manager online help for details on configuring this probe and for an example SOAP request and response.

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 (version 8 or higher) 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 the Windows platform only.**

The following files types are supported for the Real Server: .rm, .ram, .ra, .rpm, .mp3, .mid, .rmi, .midi, .mpeg, .mpg, .mlv, .mp2, .mpa, wav, .snd, .au, .aif, .asf, .wm, .wma, .wmv, .avi.

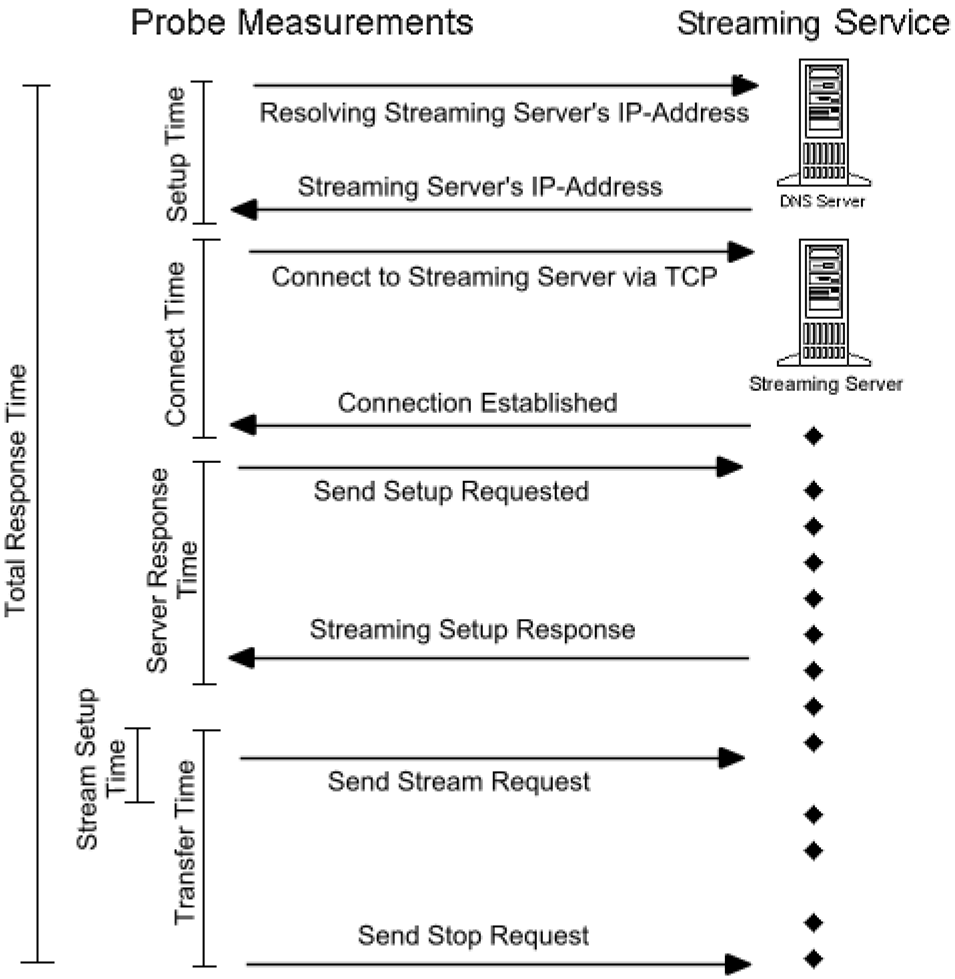
The following files types are supported for the Windows Media Server: .mp3, .mms, .mid, .rmi, .midi, .mpeg, .mpg, .mlv, .mp2, .mpa, .wav, .snd, .au, .aif, .asf, .wm, .wma, .wmv, .avi.

If the probe will run 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.

It is recommended that at least 60 seconds of sampling be performed for a streaming media target. See the Configuration Manager online help for details on configuring this probe and on the value for **Play Time**.

➤ If you plan to run the STREAM-MEDIA probe with Windows Media Player on Windows XP you need to install the `wmfdist.exe` file onto the system after the remote probe installation is complete. The executable is located in the `<install dir>\newconfig` directory and you just double-click it to install.

The following diagram shows the steps the probe completes in measuring response time:



SYS_BASIC_WMI (Basic System Metrics)

The SYS_BASIC_WMI probe collects basic Windows system metrics for the four main resource groups (CPU, Memory, Disk and Network) of a computer system running Windows. In addition, it provides a basic system availability check as well.

To configure this probe you enter the Server, which is the target system to collect the system metrics from and the Username and Password. This is the username and password of the Windows account that has access to WMI.

Please make sure that this user has access to WMI on the system specified in the above server field. Use the WMI Control to configure WMI security.

Note, if a local user is used, make sure to fully qualify the username (<hostname>\<username> or <domain>\<username>).

If metrics should be collected from the same system where the probe runs, username and password doesn't need to be specified. If they are specified, an error (0x80041064) will be returned.

You also select the network interface to be used for the network utilization metric. Currently, only one network interface is supported. Note, the virtual loopback interface (127.0.0.1) will show up in the list as well.

The metrics are collected through WMI and are as follows:

CPU: The CPU metrics consist of Total CPU Utilization across all processors and overall Processor Queue Length. Continuously high values for this metric over long periods of time paired with high processor queue length can indicate a processor bottleneck. Please note that it is normal for the utilization metric to spike when new programs are executed or programs perform CPU intensive tasks. The processor queue length usually has normal values higher than 2. For multiprocessor systems, the queue length can usually double (for example, for a system with 2 processors the queue can start at 4). Other components such as number of disks or network interface cards can increase the normal processor queue length as well.

Memory: The memory metrics consist of Available Mbytes (amount of physical memory available to processes running on the computer) and Pages Per Second of hard page failures (rate at which pages are read from or written to disk to resolve hard page faults).

Depending on the workload of the server, it should have sufficient physical memory available. (Otherwise, the system will start swapping memory pages in and out which degrades application performance). A low amount of available physical memory with a pages per second rate of >20 can indicate a memory bottleneck.

Disk: The disk metrics consist of % Disk Time (percentage of elapsed time that all disk drives were busy servicing read or write requests) and the Average Queue Length (average number of both read and write requests that were queued for all disks). Usually, percent disk time should be less than 50% and average queue length less than 4.

Note: These metrics might need to be enabled by executing `diskperf -y` on the target system.

Network: The network Utilization metric shows how much the selected interface is utilized. If a high value (that is, more than 40%) persists over a period of time, it may indicate a network bottleneck.

Availability: Since the metrics are collected remotely through WMI, the Availability metric, checks whether the system could contact the remote WMI agent or not. This provides a simple "system is up" check. Note that incorrect security permissions and or firewall settings can indicate that the system is down although it is still reachable via ping (ICMP).

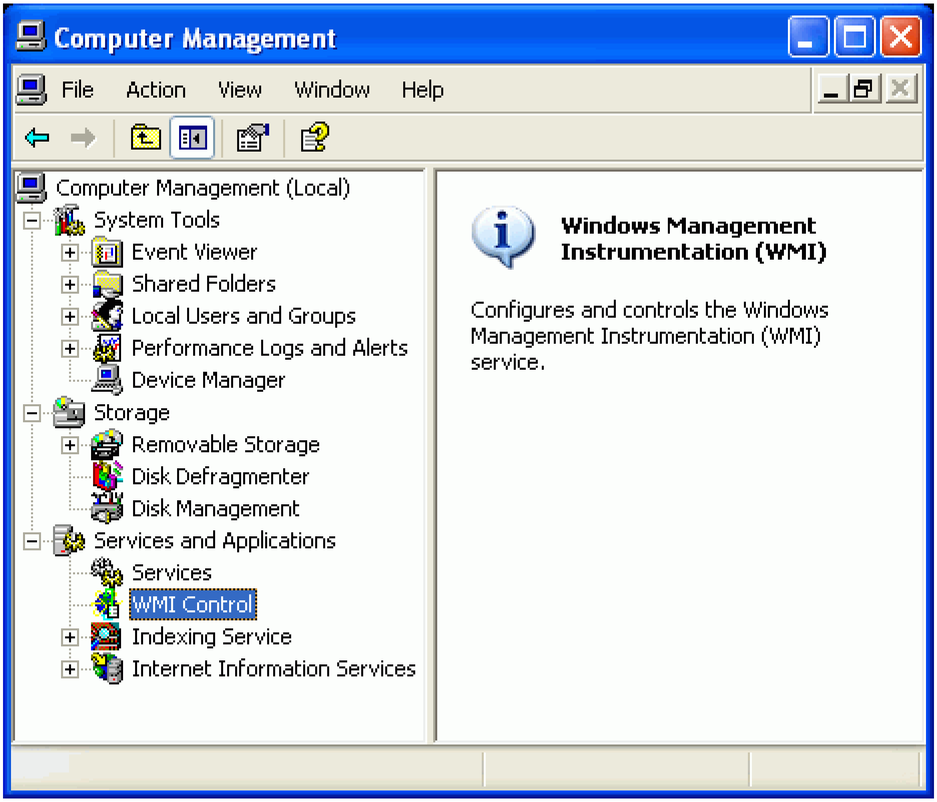
Please note that none of the metrics should be looked at in isolation - only taking all metrics in the above four resource groups into consideration will indicate or help troubleshooting a resource problem.

Measurements are taken by the SYS_BASIC_WMI probe once each interval. For some measurements an average is taken of the previous and current measurements. For example, if the default interval of 5 minutes is used, the Total CPU Utilization would be the average over 10 minutes. Therefore, it will take up to twice the interval before a metric value is available.

If the underlying counters of the metric wrap or if there is a reboot of the remote probe system, the metric cannot be calculated. In this case, a Missing Data icon will appear in the Dashboard bar chart for this interval.

In order to access the WMI on the target system, a Windows username and password credentials are needed. If the user is not part of the administrators group (local and/or domain), the user must be granted access to WMI as shown on the following pages.

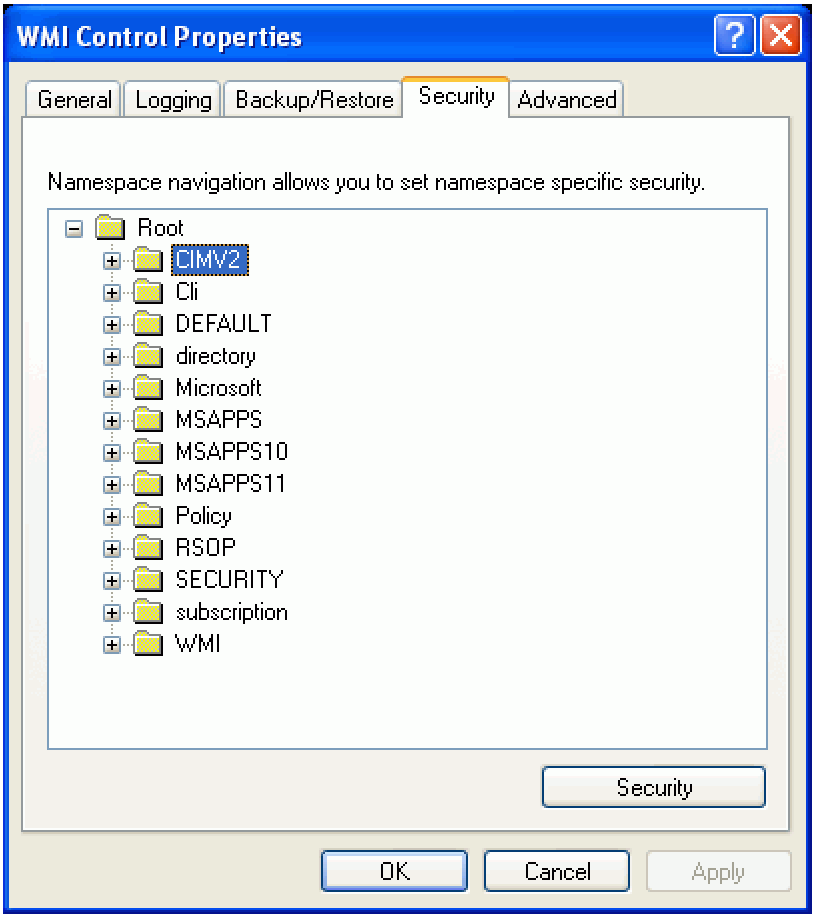
1 On the target system, right click on My Computer and select the **Manage** option. Select the **WMI Control** menu in the list:



Windows Management Instrumentation (WMI)

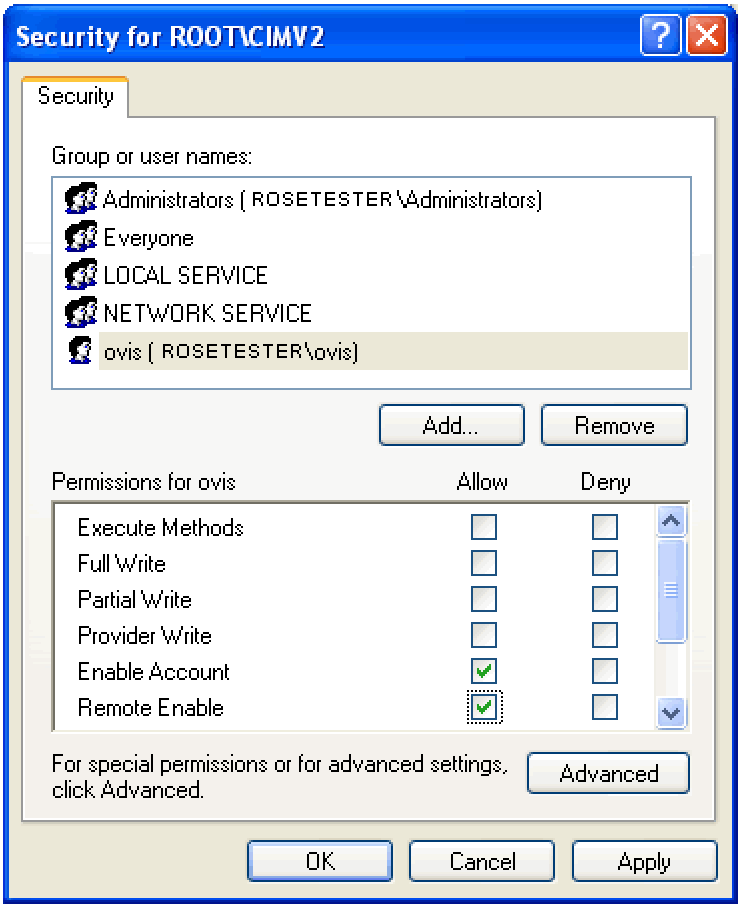
Configures and controls the Windows Management Instrumentation (WMI) service.

2 Right-click WMI Control. Select **Properties** and in the WMI Control Properties dialog box select the **Security** tab. Select **Root > CIMV2** namespace as show below. Then click the **Security** button.



Namespace navigation allows you to set namespace specific security.

3 In the Security dialog box, add the user you want to use to allow WMI access to this system. Use the **Add** button if the user doesn't appear in the list. Select the user and check the **Remote Enabled** checkbox if not checked already as shown below. Click **Apply** to save the settings.



Security for ROOT\CIMV2

Group or user names:

- Administrators (ROSETESTER\Administrators)
- Everyone
- LOCAL SERVICE
- NETWORK SERVICE
- ovis (ROSETESTER\ovis)

Permissions for ovis	Allow	Deny
Execute Methods	□	□
Full Write	□	□
Partial Write	□	□
Provider Write	□	□
Enable Account	☑	□
Remote Enable	☑	□

For special permissions or for advanced settings, click Advanced.

Note: It is not possible to use the guest account.

Note: A firewall between the probe system and the target might not allow WMI DCOM traffic. For more information search **msdn.microsoft.com** for "WMI Connecting Through Windows Firewall".

See the Configuration Manager online help for details on configuring this probe.

TCP - Performance

The TCP - Performance probe measures network bandwidth between the probe and a server.

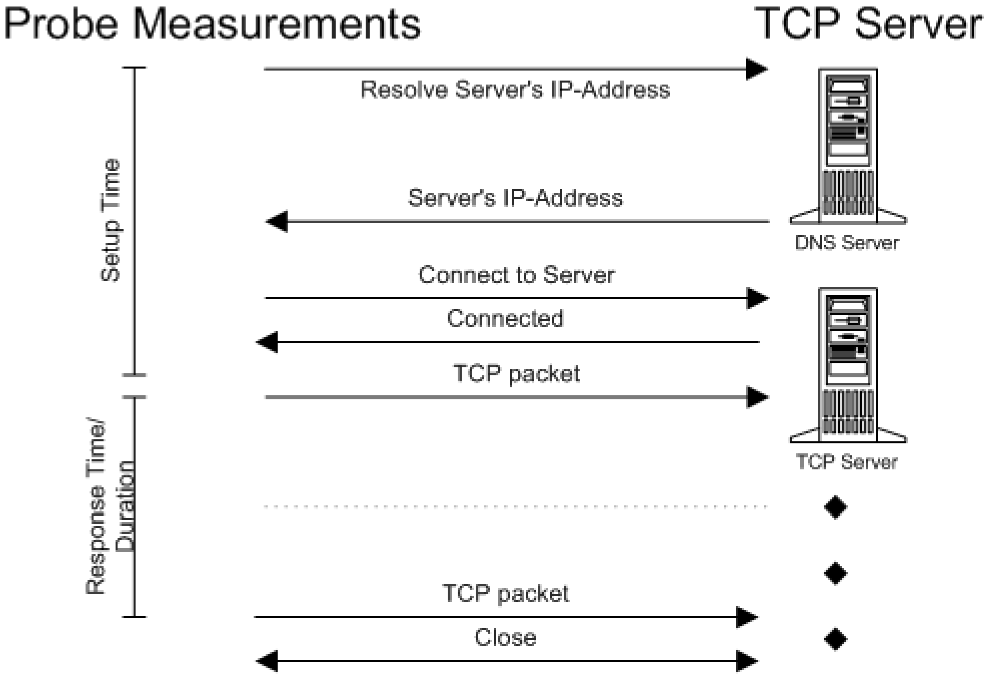
The server is part of the remote probe package and is disabled by default. In order to run the probe, a remote probe package must be installed on the target system. An existing remote probe system can be used as well. The server is part of the OVIS Scheduler process and can be enabled and disabled by setting the **IP Performance Server Ports**, **Enable Ports** checkbox in the Probe Location dialog box in the Configuration Manager.

The reported bandwidth is dependent on available system resources (CPU, memory and network I/O) on probe and target server system. If the system already has a high load, the measurements will be impacted by that load. Therefore it is recommended to not run the performance probes (TCP and UDP) in parallel with other probes in order to ensure correct measurements. Set **Target Priority** in the Probe Location dialog box in the Configuration Manager to run the performance probe without other probes running in parallel.

Note: the TCP Performance server cannot handle more than 32 connections at the same time.

See the Configuration Manager online help for details on configuring this probe.

The following diagram shows the steps the probe completes in measuring response time:



After resolving the IP-address of the server and connecting to the server, the probe sends TCP packets of the specified size for the specified duration. The probe tries to send the TCP packets as fast as possible to the server. Since the probe does not receive any data from the server, the reported bandwidth is for sending data.

Please note that the duration does not include connection establishment and connection tear-down (close).

The Bandwidth metric is reported in Mbit/s according to the SI norm where 1 Mbit/s means 106 = 1,000,000 bit/s which is more prevalent in the telecommunication industry for measuring bit rates. However, the Throughput metric is reported in KB/s where 1 KB = 1024 bytes.

TFTP (Trivial File Transfer Protocol)

The Trivial File Transfer Protocol (TFTP) probe performs a simple file retrieval. TFTP is a simple form of the file transfer protocol FTP. Unlike FTP, there is no authentication involved - the probe directly requests the download of the specified file. The TFTP probe also determines if the service is available and collects other information about this service as it executes.

To sample this service you should set up a test file with a constant size to guarantee correct measurements.

See the Configuration Manager online help for details on configuring this probe.

UDP - Performance

The UDP - Performance probe measures network bandwidth and jitter between the probe and a server.

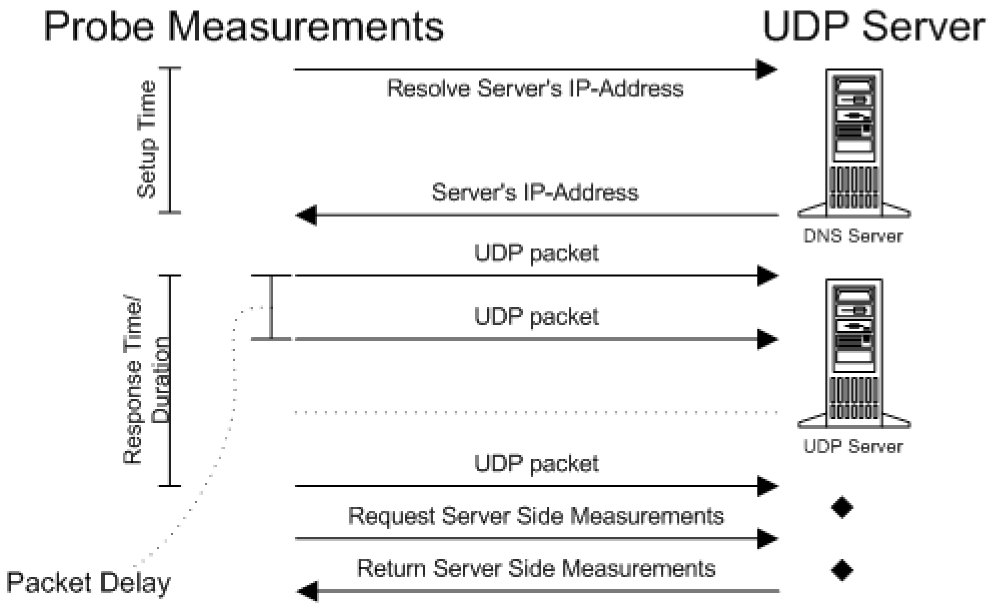
The server is part of the remote probe package and is disabled by default. In order to run the probe a remote probe package must be installed on the target system. An existing remote probe system can be used as well. The server is part of the OVIS Scheduler process and can be enabled and disabled by setting the **IP Performance Server Ports**, **Enable Ports** checkbox in the Probe Location Info dialog box in the Configuration manager.

The reported bandwidth and jitter is dependent on available system resources (CPU, memory and network I/O) on probe and target server system. If the system already has a high load, the measurements will be impacted by that load. Therefore it is recommended to not run the performance probes (TCP and UDP) in parallel with other probes in order to ensure correct measurements. Set **Target Priority** in the Probe Location dialog box in the Configuration Manager to run the performance probe without other probes running in parallel.

Note: the UDP Performance server cannot handle more than 32 connections at the same time.

See the Configuration Manager online help for details on configuring this probe.

The following diagram shows the steps the probe completes in measuring response time:



After resolving the IP-address of the server, the probe sends UDP packets of the specified packet size. The probe tries to evenly space sending the packets according to the specified packet delay. For example, if a packet takes 1ms to send and the packet delay is 20ms, the probe will wait 19ms before sending the next packet. After all the packets have been sent for the specified duration, the probe requests server side measurements from the server. Since retrieving the measurements takes some time and is not part of the duration, please set the timeout parameter for this probe to three times the duration.

The Bandwidth metric is reported in Mbit/s according to the SI norm where 1 Mbit/s means 106 = 1,000,000 bit/s which is more prevalent in the telecommunication industry for measuring bit rates. However, the Throughput metric is reported in KB/s where 1 KB = 1024 bytes.

WAP (Wireless Application Protocol)

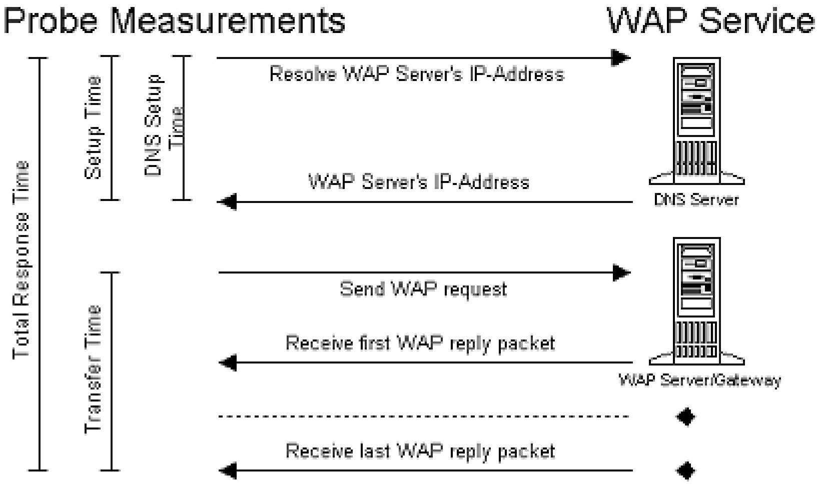
The WAP (Wireless Application Protocol) probe measures the total response time of an emulated WAP request. After the hostname or IP address is resolved, a WAP request for a document is sent to the WAP Server or WAP Gateway. Once the WAP server receives the request, it locates the requested document and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

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

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.

See the Configuration Manager online help for details on configuring this probe.

The following diagram shows the steps the probe completes in measuring response time:



Your Own Custom Probes

You can create your own custom probes using either of the following:

- Custom Probes SDK
- Probe Builder

➤ The Custom Probes SDK and Probe Builder are only supported with the English language version of Internet Services at this time.

The Custom Probe SDK 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 OVIS Management Server. The SDK requires C/C++ coding skills. The APIs primarily provide functionality for command line parsing, time measurement, probe tracing, error logging and data logging to the OVIS Management Server.

Refer to the *Internet Services Custom Probes API Guide* (CustomProbes.pdf) for more information on the Custom Probes SDK. The Custom Probe SDK is located in the `<install dir>\Sdk` directory on the OVIS Management Server. Examples are also located in this directory.

The Probe Builder is a toolkit that uses Jscript in a script development environment to provide an easier way to build, test, and deploy custom probes. It is for Windows only.

The Probe Builder can be downloaded from the hp developer resource central web site under the hp OpenView unified developer toolset.

http://devresource.hp.com/drc/unifieddev/probe.jsp

‼ Warning: Support for developing probes with the Internet Services custom probe SDK and Probe Builder is **NOT** available through standard support channels. Technical support for Internet Services custom probe SDK and Probe Builder 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.

Data Imported from OVTA

The following OVIS service types, are used to import transaction data from OpenView Transaction Analyzer (OVTA) into OVIS. These service types are defined as follows:

WEBAPP - For importing OVTA transaction data from Web based applications using the HTTP protocol to access web content.

SOAPAPP - For importing OVTA transaction data from Web service oriented applications using the SOAP protocol to communicate with other Web services. The SOAP protocol is typically implemented over HTTP.

RMIAPP - For importing OVTA transaction data from J2EE applications using the Java Remote Method invocation to access other application components. Remote EJB invocations are implemented over RMI.

JMSAPP - For importing OVTA transaction data from J2EE applications using the Java Messaging Service to communicate with other application components.

COMAPP - For importing OVTA transaction data from applications using the Component Object Model to communicate with other application components.

Transaction data collected by OVTA and imported into OVIS is displayed in the OVIS Dashboard. Furthermore, if you define service level objectives, alarm thresholds and service level agreements for OVTA data, OVIS will forward OVTA alarms to OVO and NNM.

Refer to Integrating with OpenView Transaction Analyzer on page 300 for more information on these service types and the metrics collected for each.

List of Metrics by Probe Type

You can look at the following file for a list of metrics by probe type:

```
<install directory>\newconfig\packages\repload_IOPS.SRP
```

Note that “OVTA Applications” in the list below shows the metrics for these service types: COMAPP, JMSAPP, RMIAPP, SOAPAPP, WEBAPP.

Also note that the Metric Identifier is shown to identify Metric 1 - Metric 8 for each probe type. This information can be used in configuring alarm messages. See Alarm Message on page 124.

➤ The metric name as displayed in the Dashboard is shown first, the metric name in parentheses is the name as seen in the Configuration Manager.

ANYTCP

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

Response Time (*RESPONSE_TIME)* - Total response time for the TCP service. (DNS Setup Time + Connect Time).

Setup Time (*SETUP_TIME)* - Time to resolve address and establish the connection

Throughput (*TRANSFER_TPUT)*- Transfer bytes/Transfer Time in kbytes/sec.

DNS Setup Time *(DNS_SETUP_TIME)* - *Metric 1* - Time to resolve hostname through DNS.

Connect Time *(CONNECT_TIME)* - *Metric 2* - Time to perform connect to resolved IP address.

DHCP

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

Response Time (*RESPONSE_TIME)* - Total response time for the DHCP service. (Setup Time + Transfer Time).

Setup Time (*SETUP_TIME)* - Time to resolve address and establish the connection if host is specified.

Throughput (*TRANSFER_TPUT)* - Transfer bytes/Transfer Time in kbytes/sec.

Offer Time (*OFFER_TIME) - Metric 1* - Time to first offer from server.

Lease Time (*LEASE_TIME) - Metric 2* - Time to lease offered IP address.

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

Bytes Transferred (*TRANS_BYTES) - Metric 6* - The number of bytes transferred.

DIAL

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

Response Time (*RESPONSE_TIME)* - Time taken to establish PPP connection.

RAS Connect Status (*RAS_CONNECT_STATUS) - Metric 1* - Error returned by RAS Dial. Will be 0 for successful connection.

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

Total Connection Time (*TOTAL_CONNECTION_TIME) - Metric 3* - Total time connected.

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

DNS

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

Response Time (*RESPONSE_TIME)* - Execution time of the query to a hostname/IP address.

Resolved *(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.

Exchange

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

Setup Time (*SETUP_TIME)* - Time to log in to the Exchange Server and resolve the name.

Response Time (*RESPONSE_TIME)* - Total response time of the Exchange service. Setup Time + time to read all messages and mark the OVIS ones for delete.

Authentication Time *(AUTH_TIME) - Metric 4* - Time to authenticate the user.

Transfer Time *(TRANSFER_TIME) - Metric 5* - Overall time to receive data.

Send Time *(SEND_TIME) - Metric 6* - Time to send message.

FTP

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

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

Setup Time (*SETUP_TIME)* - Time to resolve address and establish the connection.

Throughput (*TRANSFER_TPUT)* - Transfer bytes/Transfer Time in kbytes/sec.

DNS Setup Time (*DNS_SETUP_TIME) - Metric 1* - Time to resolve hostname through DNS.

Connect Time (*CONNECT_TIME) - Metric 2* - Time to perform connect to FTP server.

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

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

Port Time *(PORT_TIME) - Metric 5* - Time to send the client connection ports to the FTP server.

Transfer Time (*TRANSFER_TIME) - Metric 6* - Overall time to receive data on the data connection.

Bytes Transferred (*DATA_TRANS_BYTES) - Metric 7* - The number of bytes transferred.

HTTP/HTTPS

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

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

Setup Time (*SETUP_TIME)* - Time to resolve address and establish the connection.

Throughput (*TRANSFER_TPUT)* - Transfer bytes/(Transfer Time + Server Response Time) in kbytes/sec.

DNS Setup Time (*DNS_SETUP_TIME) - Metric 1* - Time to resolve hostname through DNS.

Connect Time (*CONNECT_TIME) - Metric 2* - Time to connect to HTTP/S server or proxy.

Server Response Time (*SERVER_RESP_TIME) - Metric 3* - Time it takes to send HTTP/S Get request and receive first response packet.

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

Bytes Transferred (*TRANS_BYTES) - Metric 5* - The number of bytes transferred.

HTTP Status *(HTTP_STATUS) - Metric 6* - HTTP/S status code.

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

Broken Links *(BROKEN_LINKS) - Metric 8* - Number of embedded objects that couldn't be downloaded (e.g., URL not found).

HTTP_TRANS

URL/Navigation Point Mode

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

Response Time (*RESPONSE_TIME) -*
Step: Total response time for the web page access (DNS Setup Time + Connect Time + Server Response Time + Transfer Time).
Transaction: Total response time for all steps.

Setup Time (*SETUP_TIME) -*
Step: Time to resolve address and establish the connection.
Transaction: Total setup time for all steps.

Throughput (*TRANSFER_TPUT) -*
Step: Transfer bytes/(Transfer Time + Server Response Time) in kbytes/sec.
Transaction: Total transfer throughput for the transaction.

DNS Setup Time *(DNS_SETUP_TIME) - Metric 1 -*
Step: Time to resolve hostname through DNS.
Transaction: Total DNS setup time for all steps.

Connect Time *(CONNECT_TIME) - Metric 2 -*
Step: Time to connect to HTTP/S server or proxy.
Transaction: Total connect time for all steps.

Server Response Time *(SERVER_RESP_TIME) - Metric 3 -*
Step: Time it takes to send HTTP Get request and receive first response packet.
Transaction: Total server response time for all steps.

Transfer Time (*TRANSFER_TIME) - Metric 4 -*
Step: Time it took to send request and receive all reply packets.
Transaction: Total transfer time for all steps.

Bytes Transferred (*TRANSFER_BYTES) - Metric 5 -*
Step: The number of bytes transferred.
Transaction: Total transfer bytes for all steps.

HTTP Status *(HTTP_STATUS) - Metric 6 -*
Step: HTTP status code.
Transaction: HTTP status code of the last step.

Requests *(REQUESTS) - Metric 7 -*
Step: Number of HTTP requests. For example, if the page was redirected or embedded objects are downloaded.
Transaction: Total requests for all steps.

Broken Links *(BROKEN_LINKS)* - Metric 8 -
Step: Number of embedded objects that couldn't be downloaded (e.g., URL not found).
Transaction: Total broken links for all steps.

HTTP_TRANS

IE Mode

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

Response Time (*RESPONSE_TIME) -*
Step: Setup Time + Server Response Time + Transfer Time.
Transaction: Total response time for all steps.

Setup Time (*SETUP_TIME) -*
Step: Time it takes from executing a step and starting the download of the document.
Transaction: Total setup time for all steps.

Throughput (*TRANSFER_TPUT) -*
Step: Transfer bytes/Response Time in kbytes/sec.
Transaction: Total transfer throughput for the transaction.

DNS Setup Time *(DNS_SETUP_TIME) - Metric 1 -* Not Available.

Connect Time *(CONNECT_TIME) - Metric 2 -* Not Available.

Server Response Time *(SERVER_RESP_TIME) - Metric 3 -*
Step: Time it takes from starting to download the document and first time the download progress changes (IE progress indicator).
Transaction: Total server response time for all steps.

Transfer Time (*TRANSFER_TIME) - Metric 4 -*
Step: Time it takes from first progress change to completion of the step.
Transaction: Total transfer time for all steps.

Bytes Transferred (*TRANSFER_BYTES) - Metric 5 -*
Step: The number of bytes for all images, frames and javascript includes contained in the page. Note, this does not correspond with the actual number of bytes downloaded in case the images/javascript includes are cached (client or server side).
Transaction: Total transfer bytes for all steps.

HTTP Status *(HTTP_STATUS) - Metric 6 -*
Step: HTTP status code, IE WININET error code or -1 (if first connection timed out).
Transaction: HTTP status code of last step.

Requests *(REQUESTS) - Metric 7 -*
Step: Number of documents (includes redirects and frames but not other embedded objects).
Transaction: Total number of complete documents for all steps.

Broken Links *(BROKEN_LINKS) - Metric 8 -* Not Available.

ICMP

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

Response Time (*RESPONSE_TIME)* - Response time is the average roundtrip time for all ICMP packets.

Throughput (*TRANSFER_TPUT)* - Transfer bytes/Transfer Time in kbytes/sec.

Min Response *(MIN_RESPONSE) - Metric 1* - Minimum roundtrip time of all ICMP packets.

Max Response *(MAX_RESPONSE) - Metric 2* - Maximum roundtrip time of all ICMP packets.

Packet Loss *(PACKET_LOSS) - Metric 3* - Number of packets lost.

IMAP4

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

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

Setup Time (*SETUP_TIME)* - Time to resolve address and establish the connection

Throughput (*TRANSFER_TPUT)* - Transfer bytes/Transfer Time in kbytes/sec.

DNS Setup Time *(DNS_SETUP_TIME) - Metric 1* - Time to resolve hostname through DNS.

Connect Time *(CONNECT_TIME) - Metric 2* - Time to connect to IMAP server.

Server Response Time *(SERVER_RESP_TIME) - Metric 3* - Time for IMAP server to respond.

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

Transfer Time (*TRANSFER_TIME) - Metric 5* - Overall time it took for the data transfer only.

Bytes Transferred (*DATA_TRANS_BYTES) - Metric 6* - The number of bytes transferred.

LDAP

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

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

Throughput (*TRANSFER_TPUT)* - Transfer bytes/Transfer Time in kbytes/sec.

DNS Setup Time *(DNS_SETUP_TIME) - Metric 1* - Time to resolve hostname through DNS.

Number of Entries *(NUM_ENTRIES) - Metric 2* - Number of returned entries.

Connect Time *(CONNECT_TIME) - Metric 3* - Time to connect to LDAP server.

Transfer Time (*TRANSFER_TIME) - Metric 4* - Overall time it took for the data transfer only.

Bytes Transferred (*TRANS_BYTES) - Metric 5* - The number of bytes transferred.

MAILROUNDTRIP

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

Setup Time (*SETUP_TIME)* - Time to resolve address and establish the connection.

Response Time (*RESPONSE_TIME)* - Total response time for the SMTP mail send + the POP/IMAP receive.

Throughput (*TRANSFER_TPUT)* - Transfer bytes/Transfer Time in kbytes/sec.

NNTP

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

Response Time (*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 (*SETUP_TIME)* - Time to resolve address and establish the connection.

Throughput (*TRANSFER_TPUT)* - Transfer bytes/Transfer Time in kbytes/sec.

DNS Setup Time *(DNS_SETUP_TIME) - Metric 1* - Time to resolve hostname through DNS.

Connect Time *(CONNECT_TIME) - Metric 2* - Time to connect to NNTP server.

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

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

GROUP Cmd Time *(GROUP_TIME) - Metric 5* - Time to select newsgroup and get request overview of last 100 articles.

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

Tear Down Time *(TEAR_DOWN_TIME) - Metric 7* - Overall time to send the QUIT request and receive the response.

Bytes Transferred (*DATA_TRANS_BYTES) - Metric 8* - The number of bytes transferred.

NTP

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

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

Setup Time (*SETUP_TIME)* - Time to resolve address and establish the connection.

Throughput (*TRANSFER_TPUT)* - Transfer bytes/Transfer Time in kbytes/sec.

Bytes Transferred (*DATA_TRANS_BYTES) - Metric 5* - The number of bytes transferred.

Transfer Time (*TRANSFER_TIME) - Metric 6* - Overall time it took for the data transfer only.

ODBC

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

Response Time (*RESPONSE_TIME)* - Total response time for the ODBC service.

Setup Time (*SETUP_TIME)* - Time to setup database connection handles.

Throughput (*TRANSFER_TPUT)* - Transfer bytes/Transfer Time in kbytes/sec.

Connect Time *(CONNECT_TIME) - Metric 1* - Time to connect to database.

Server Response Time *(SERVER_RESP_TIME) - Metric 2* - Time to respond to the SQL statement.

Transfer Time (*TRANSFER_TIME) - Metric 3* - Overall time it took for the data transfer.

Bytes Transferred (*TRANS_BYTES) - Metric 4* - The number of bytes transferred.

OVTA Application (COMAPP, JMSAPP, RMIAPP, SOAPAPP, WEBAPP)

Availability (*AVAILABILITY) - WEBAPP and SOAPAPP service type only.* The ratio of availability probe requests that failed, to the total attempts during the last interval.

Response Time (*RESPONSE_TIME)* - The average response time of the successfully completed transactions during the interval.

Transaction Rate *(TRANSACTION_RATE) - Metric 1* - Total number of completed transactions per second over the last interval.

Response Time Violation Count *(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 *(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 *(TRANSACTION_SIZE) - Metric 4* - WEBAPP service type only. The average size of the successfully completed transactions. The size varies depending on the type of application and the type of transaction.

For transactions measured in the browser using an OVTA Browser Client Monitor, the size of these transactions is the size of the downloaded page plus all embedded content and images.For transactions measured at the Web or Application server using an OVTA Web Server Monitor, the size of these transactions is the size of the downloaded page as reported in the Content-Length HTTP header. This is the size of the page itself and does not include embedded images. Moreover, some web-based applications will not set the Content-Length field; therefore, this metric will be 0 for transactions in these types of applications.

Failed Transaction Rate *(FAILED_TRANSACTION_RATE) - Metric 5* - Total number of failed transactions per second over the last interval.

POP3

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

Response Time (*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 (*SETUP_TIME) -* Time to resolve address and establish the connection.

Throughput (*TRANSFER_TPUT) -* Transfer bytes/Transfer Time in kbytes/sec.

DNS Setup Time *(DNS_SETUP_TIME) - Metric 1* - Time to resolve hostname through DNS.

Connect Time *(CONNECT_TIME) - Metric 2* - Time to connect to POP3 server.

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

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

Transfer Time (*TRANSFER_TIME) - Metric 5* - Overall time to read all messages in the mailbox and delete the IOPS test messages.

Bytes Transferred (*DATA_TRANS_BYTES) - Metric 6* - The number of bytes transferred.

RADIUS

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

Setup Time (*SETUP_TIME)* - Time to resolve address and make connection.

Throughput (*TRANSFER_TPUT)* - Transfer bytes/Transfer Time in kbytes/sec.

Transfer Time (*TRANSFER_TIME) - Metric 4* - Overall time it took for the data transfer only.

Bytes Transferred (*TRANS_BYTES) - Metric 5* - The number of bytes transferred.

SAP

Availability (*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 (*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 (*SETUP_TIME)* - Time to get a successful connection with the RFC server.

Script

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

Response Time (*RESPONSE_TIME)* - Total time running the script. Or the total response time imported from the Result File script.

SMS

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

Response Time (*RESPONSE_TIME)* - Total response time for the SMS service.

Setup Time *(SETUP_TIME)* - Time to establish connection.

Throughput *(TRANSFER_TPUT)* - Transfer bytes/Transfer Time in kbytes/sec.

SMTP

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

Response Time (*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 (*SETUP_TIME)* - Time to resolve address and establish the connection.

Throughput (*TRANSFER_TPUT)* - Transfer bytes/Transfer Time in kbytes/sec.

DNS Setup Time (*DNS_SETUP_TIME) - Metric 1* - Time to resolve hostname through DNS.

Connect Time *(CONNECT_TIME) - Metric 2* - Time to connect to SMTP server.

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

Transfer Time (*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.

Bytes Transferred (*TRANS_BYTES) - Metric 5* - The number of bytes transferred.

Tear Down Time *(TEAR_DOWN_TIME) - Metric 6* - Overall time to send the QUIT request and receive the response.

SOAP

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

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

Setup Time (*SETUP_TIME)* - Time to resolve address and establish the connection.

Throughput (*TRANSFER_TPUT)* - Transfer bytes/Transfer Time in kbytes/sec.

DNS Setup Time *(DNS_SETUP_TIME) - Metric 1 -* Time to resolve hostname through DNS.

Connect Time *(CONNECT_TIME) - Metric 2 -* Time to connect to SOAP server or proxy.

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

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

Bytes Transferred (*TRANS_BYTES) - Metric 5 -* The number of bytes transferred.

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

STREAM_MEDIA

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

Response Time (*RESPONSE_TIME)* - Total response time for the Streaming Media service (Setup Time + Connect Time + Server Response Time + Transfer Time).

Setup Time (*SETUP_TIME)* - Time to resolve address.

Throughput (*TRANSFER_TPUT)* - The average bandwidth used in data transfer in Kbytes/sec.

Connect Time *(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 Response Time *(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 (*TRANSFER_TIME) - Metric 3 -* The time it takes to transfer the data.

Packets Received *(PACKETS_RECEIVED) - Metric 4* - Total number of packets received.

Packet Loss *(PACKET_LOSS) - Metric 5* - The percentage of packets lost.

Latency *(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 *(CONGESTION) - Metric 7* - The percentage of time spent in buffering data vs. the total time for playing the streams. This excludes the initial buffering time.

Stream Setup Time *(STREAM_SETUP_TIME) - Metric 8* - The initial buffering time, before the stream actually starts playing on the client.

SYS_BASIC_WMI

Availability *(AVAILABILITY)* - Indicates whether metrics could be successfully retrieved from WMI on the target system.

CPU:

Total CPU Utilization *(TOTAL_CPU_UTL) - Metric 1* - Total CPU Utilization over the specified interval

Processor Queue Length *(PROCESSOR_QUEUE_LENGTH) - Metric 2* - Total processor queue length.

Memory:

Available Mbytes *(AVAILABLE_MBYTES) - Metric 3* - Physical MB available.

Pages Per Second (Hard Page Faults) *(MEM_PAGES_PER_SEC) - Metric 4* - Rate at which pages are read from or written to disk to resolve hard page faults.

Disk:

% Disk Time *(PERCENT_DISK_TIME) - Metric 5* - Percentage of elapsed time that all disk drives were busy servicing read or write requests

Average Queue Length *(DISK_AVG_QUEUE_LENGTH) - Metric 6* - Average number of both read and write requests that were queued for all disks.

Network:

Utilization *(NET_UTIL) - Metric 7* - Utilization of specified interface card.

TCP- Performance

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

Bandwidth (SI Norm) *(SI_BANDWIDTH) Metric 1* - Bandwidth in Mbit/s (1 Mbit/s means 10^6 = 1,000,000 bit/s, measured as sent bits divided by actual duration.

Throughput *(TRANSFER_TPUT)* - Throughput in Kbytes/s, measured as sent bytes divided by actual duration.

Megabytes sent *(MB_SENT) Metric 2* - Megabytes sent.

Response Time *(RESPONSE_TIME)* - This is close to the specified duration.

Setup Time *(SETUP_ TIME)* - Time it takes for DNS resolution and connecting to the server.

TFTP

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

Response Time *(RESPONSE_TIME)* - Total response time for the TFTP service. (Setup Time + Transfer Time).

Setup Time *(SETUP_ TIME)* - Time to resolve the TFTP address.

Throughput *(TRANSFER_TPUT)* - Transfer bytes/Transfer Time in kbytes/sec.

Transfer Time *(FILE_TRANSFER_TIME) - Metric 1* - Transfer bytes/ Transfer Time in Kbytes/sec.

Bytes Transferred *(TRANSFER_BYTES) - Metric 2* - The total number of bytes transferred in the transaction.

UDP- Performance

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

Bandwidth (SI Norm) *(SI_BANDWIDTH) Metric 1* - Bandwidth in Mbit/s (1 Mbit/s means 10^6 = 1,000,000 bit/s, measured as sent bits divided by actual duration.

Jitter *(JITTER) Metric 4* - Jitter (variance in packets sent and received) in milliseconds (ms) according to RFC 1889, Real Time Protocol (RTP).

Throughput *(TRANSFER_TPUT)* - Throughput in Kbytes/s, measured as sent bytes divided by actual duration.

% Packets Lost *(PCT_PACKET_LOST) Metric 5* - Packets lost in transmission calculated as number of packets received divided by number of packets sent.

Megabytes sent *(MB_SENT) Metric 2* - Megabytes sent by the probe.

Megabytes received *(MB_RECEIVED) Metric 3* - Megabytes received by the server.

Packets out of order *(PACKET_OUT_OF_ORDER) Metric 6* - Number of packets that haven't been received in the same order as they were sent.

Response Time *(RESPONSE_TIME)* - This is close to the specified duration.

Setup Time *(SETUP_ TIME)* - Time it takes for DNS resolution.

WAP

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

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

Throughput (*TRANSFER_TPUT) -* Transfer bytes/Transfer Time in kbytes/sec.

DNS Setup Time *(DNS_SETUP_TIME) - Metric 1 -* Time to resolve hostname through DNS.

Transfer Time (*TRANSFER_TIME) - Metric 4 -* Overall time it took for the data transfer only.

Bytes Transferred *(TRANS_BYTES) - Metric 5 -* The number of bytes transferred.

5

Integrating with OpenView Products

You can integrate Internet Services (OVIS) with OpenView Transaction Analyzer (OVTA), OpenView Operations for UNIX (OVO for UNIX), 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.

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

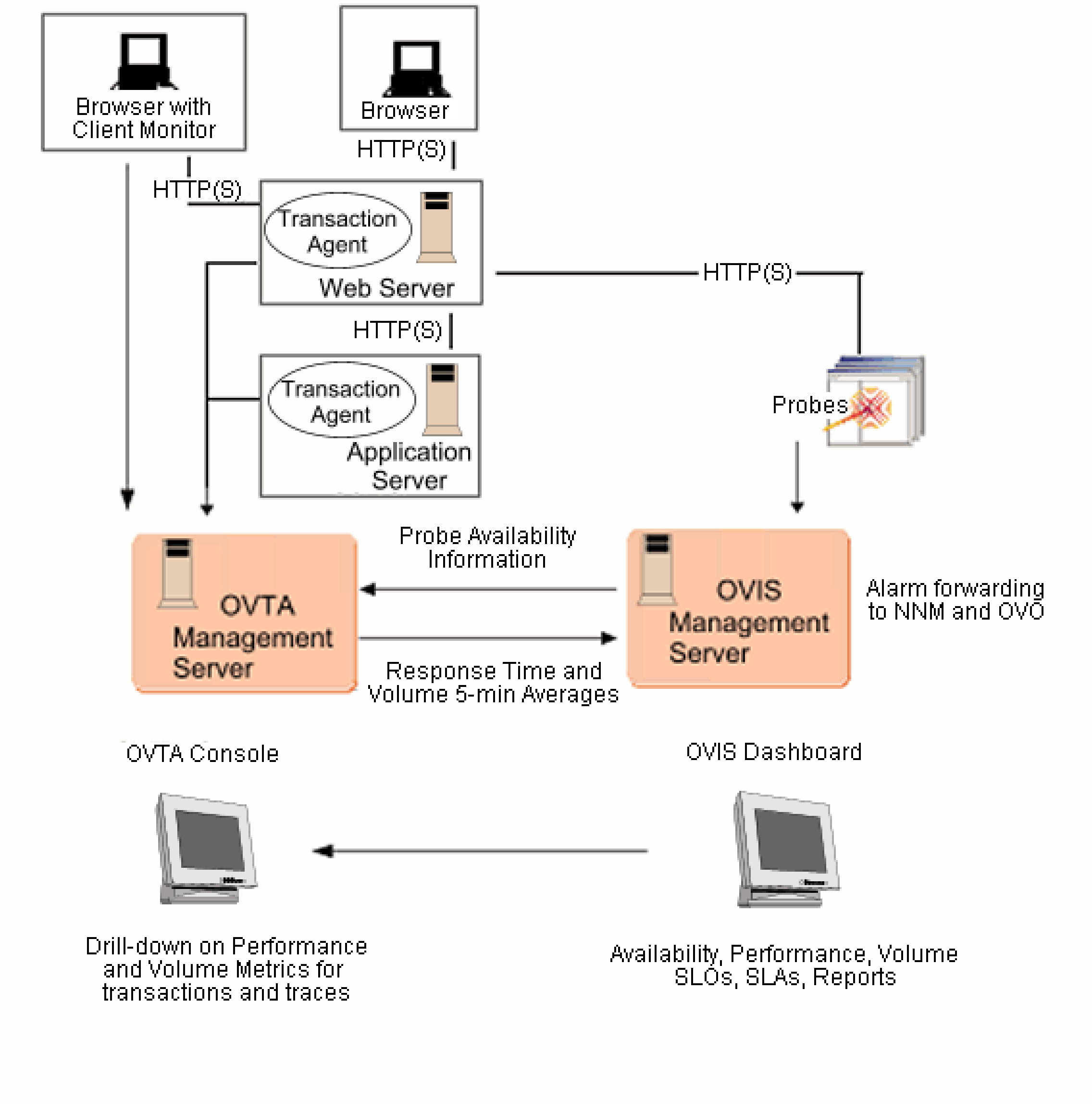
OVIS includes several service types (COMAPP, JMSAPP, RMIAPP, SOAPAPP, WEBAPP) that map to different types of applications monitored in OpenView Transaction Analyzer (OVTA). This OVTA transaction performance data is imported into OVIS and summarized at reporting intervals (currently set at five minutes). OVTA measures and analyzes transaction volume and transaction response times for applications monitored in OVTA. 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: http://ovweb.external.hp.com/lpe/doc_serv/.

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


Browser with
Client Monitor
Browser
HTTP(S)
HTTP(S)
Transaction Agent
Web Server
HTTP(S)
HTTP(S)
Transaction Agent
Application Server
Probes
Probe Availability Information
OVTA Management Server
OVIS Management Server
Alarm forwarding to NNM and OVO
Response Time and Volume 5-min Averages
OVTA Console
OVIS Dashboard
Drill-down on Performance and Volume Metrics for transactions and traces
Availability, Performance, Volume SLOs, SLAs, Reports

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 306 for details on how to perform each step 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 one of the following service types as the Monitored Service when setting up the service group:

   WEBAPP
   SOAPAPP
   RMIAPP
   JMSAPP
   COMAPP

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 OVTA based 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 OVTA icon in the Workspace pane.
6. In the OVIS Dashboard, in the Health workspace's Alarms tab, you can click on the OVTA icon in the Trace column of an alarm to launch the OVTA Console which provides transaction sub-component detail.
7. After the nightly reports are generated in OVIS, you can use the Reports link in the OVIS Dashboard workspace pane 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.

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 (WEBAPP, SOAPAPP only).

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 - The average size of the successfully completed transactions. The size varies depending on the type of application and the type of transaction:

> WEBAPP: For transactions measured in the browser using an OVTA Browser Client Monitor, the size of these transactions is the size of the downloaded page plus all embedded content and images.For transactions measured at the Web or Application server using an OVTA Web Server Monitor, the size of these transactions is the size of the downloaded page as reported in the Content-Length HTTP header. This is the size of the page itself and does not include embedded images. Moreover, some web-based applications will not set the Content-Length field; therefore, this metric will be 0 for transactions in these types of applications.
>
> COMAPP, RMIAPP, SOAPAPP, JMSAPP: The TRANSACTION_SIZE metric is not available and will always be 0.

FAILED_TRANSACTION_RATE - Metric 5 - Total number of failed transactions per second over 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 useful for alarms, service level agreements or reporting.

When adding service level objectives (SLO), 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 315 for examples.

The OVIS probe location contains the OVTA requesting node information. This allows an operator to use the OVIS Dashboard 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

You must install and have OVIS and OVTA configured but 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. Also see the *OVTA Performance and Scaling Guide* for sizing recommendations.

⚠ Also note that if OVIS and OVTA servers are on different systems, the clocks of the two systems need to be synchronized within five minutes.

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

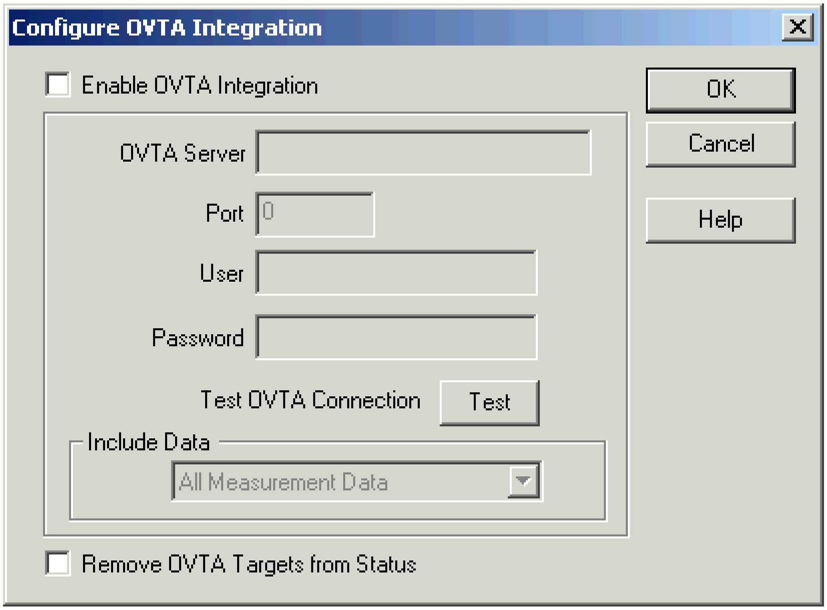
The steps to integrate OVIS and OVTA are as follows.

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. You can select the test button to test the connection to the OVTA Server.

You can also select the data you want the OVTA servlet to collect. By default it collects all measurement data available. You can select probe measurement data. This data from OVIS probes could be gathered by the OVTA client receptor or it could be collected from OVIS probes (HTTP probes) you have configured to monitor an OVTA instrumented server or transaction. You can select OVTA measurement data. This is the measurement data imported into OVIS based on the service targets configured.

If you have a large number of OVTA targets this may slow the display of the Target Status worksapce page in the OVIS Dashboard and the Status page in the Configuration Manager. Check the box Remove OVTA Targets from Status, to keep the OVTA targets from being displayed in OVIS status pages.



Configure OVTA Integration

☐ Enable OVTA Integration

OVTA Server

Port 0

User

Password

Test OVTA Connection

Include Data: All Measurement Data

☐ Remove OVTA Targets from Status

Task 2: Configure the OVTA 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 one of the following service types from the drop down list as the Monitored Service. These service types generally correspond to the type of middle ware and the underlying protocol used to communicate between remote application components.

WEBAPP - A Web based application using the HTTP protocol to access web content.

SOAPAPP - A Web service oriented application using the SOAP protocol to communicate with other Web services. The SOAP protocol is typically implemented over HTTP.

RMIAPP - A J2EE application using the Java Remote Method invocation to access other application components. Remote EJB invocations are implemented over RMI.

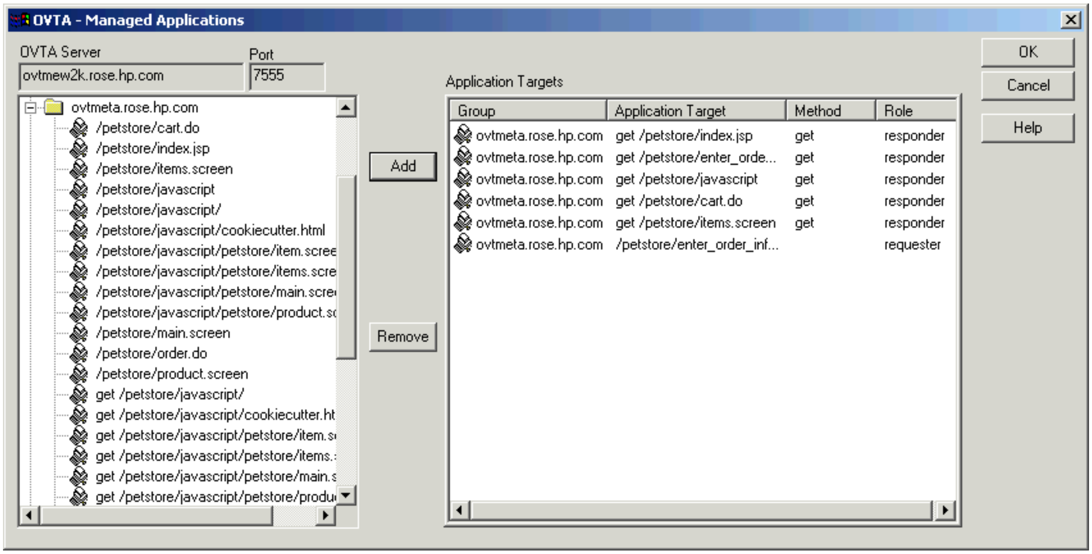
JMSAPP - A J2EE application using the Java Messaging Service to communicate with other application components.

COMAPP - An application using the Component Object Model to communicate with other application components.

Refer to the *OVTA User's Guide* for more information on these service types.

A Service Group is added 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 - Managed Applications dialog is displayed (an example for the WEBAPP service target is shown below). This dialog allows you to select from the currently discovered transactions from the OVTA server for the service type you've configured. It may take some time for all the data to display.



OVTA Server: ovtmew2k.rose.hp.com

Port: 7555

ovtmeta.rose.hp.com
- /petstore/cart.do
- /petstore/index.jsp
- /petstore/items.screen
- /petstore/javascript
- /petstore/javascript/
- /petstore/javascript/cookiecutter.html
- /petstore/javascript/petstore/item.scree
- /petstore/javascript/petstore/items.scre
- /petstore/javascript/petstore/main.scre
- /petstore/javascript/petstore/product.sc
- /petstore/main.screen
- /petstore/order.do
- /petstore/product.screen
- get /petstore/javascript/
- get /petstore/javascript/cookiecutter.ht
- get /petstore/javascript/petstore/item.s
- get /petstore/javascript/petstore/items.:
- get /petstore/javascript/petstore/main.s
- get /petstore/javascript/petstore/produ

Application Targets

Group	Application Target	Method	Role
ovtmeta.rose.hp.com	get /petstore/index.jsp	get	responder
ovtmeta.rose.hp.com	get /petstore/enter_orde...	get	responder
ovtmeta.rose.hp.com	get /petstore/javascript	get	responder
ovtmeta.rose.hp.com	get /petstore/cart.do	get	responder
ovtmeta.rose.hp.com	get /petstore/items.screen	get	responder
ovtmeta.rose.hp.com	/petstore/enter_order_inf...		requester

For the WEBAPP service type, transactions 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 for the WEBAPP service type:

```
/estore/control/category

/estore/control/product

get /petstore/cart.do

get /petstore/main.screen
```

Note that 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.

Note that other OVTA Application service types such as RMI, JMS, SOAP and COM have transaction names prefixed with Requester or Responder. Requester is a transaction making a request, responder is a server responding to a request.

Service groups can be used to logically group related transactions (e.g. shopping cart). Or you can group transactions measured by the OVTA client monitors separate from those on the servers. This would give you an end user perspective and the server perspective. Refer to the *OVTA User's Guide* for more information.

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. Use the OVTA Console launch in the Dashboard Workspace pane 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 SLOs (Service Level Objectives) SLAs (Service Level Agreements made up of several SLOs) 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.

Also note that in order for alarms to be displayed in the OVIS Dashboard, the Alarm Targets **Database (Alarms and NNM Integration)** checkbox must be checked in the Configuration Manager (**File > Configure > Alarm Destinations**).

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 315 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.

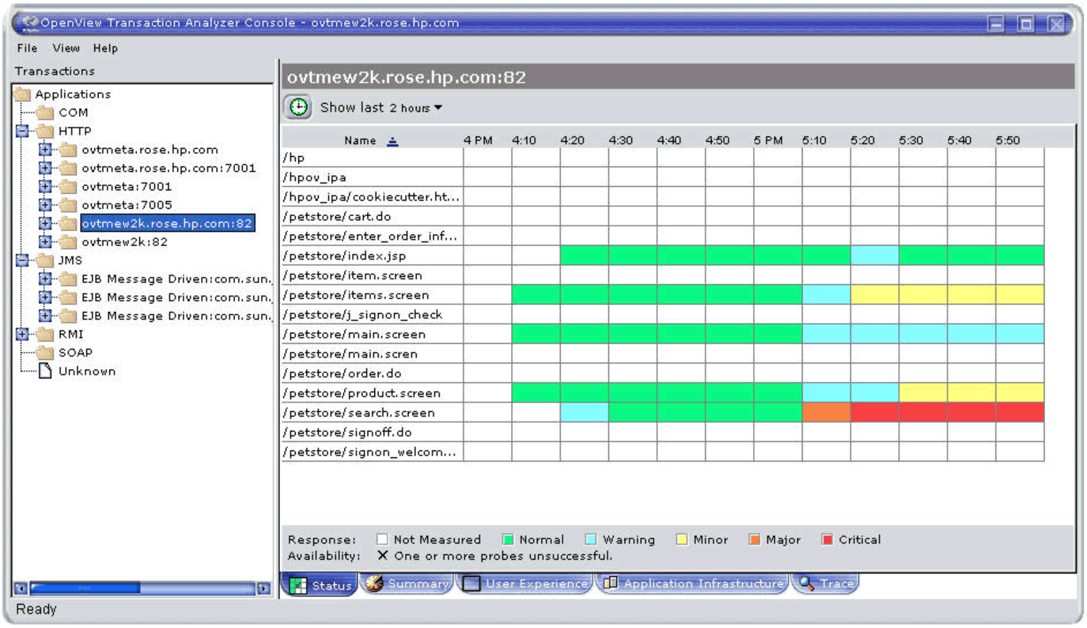
After saving the configuration, wait 10 - 15 minutes for the data to be collected. Then check the status of the new OVTA based service targets imported from OVTA. In the OVIS Configuration Manager select **Status** in the left pane. The service targets will show status of green if the OVTA transaction 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 accessed, 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 OVTA Transactions

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

When you select this link, a page is displayed with information about having to have Java Web Start installed in order for the OVTA application to launch. Select the **Launch OVTA Console** button to launch the OVTA Console with the Status tab displayed.

The OVTA Console is shown below:



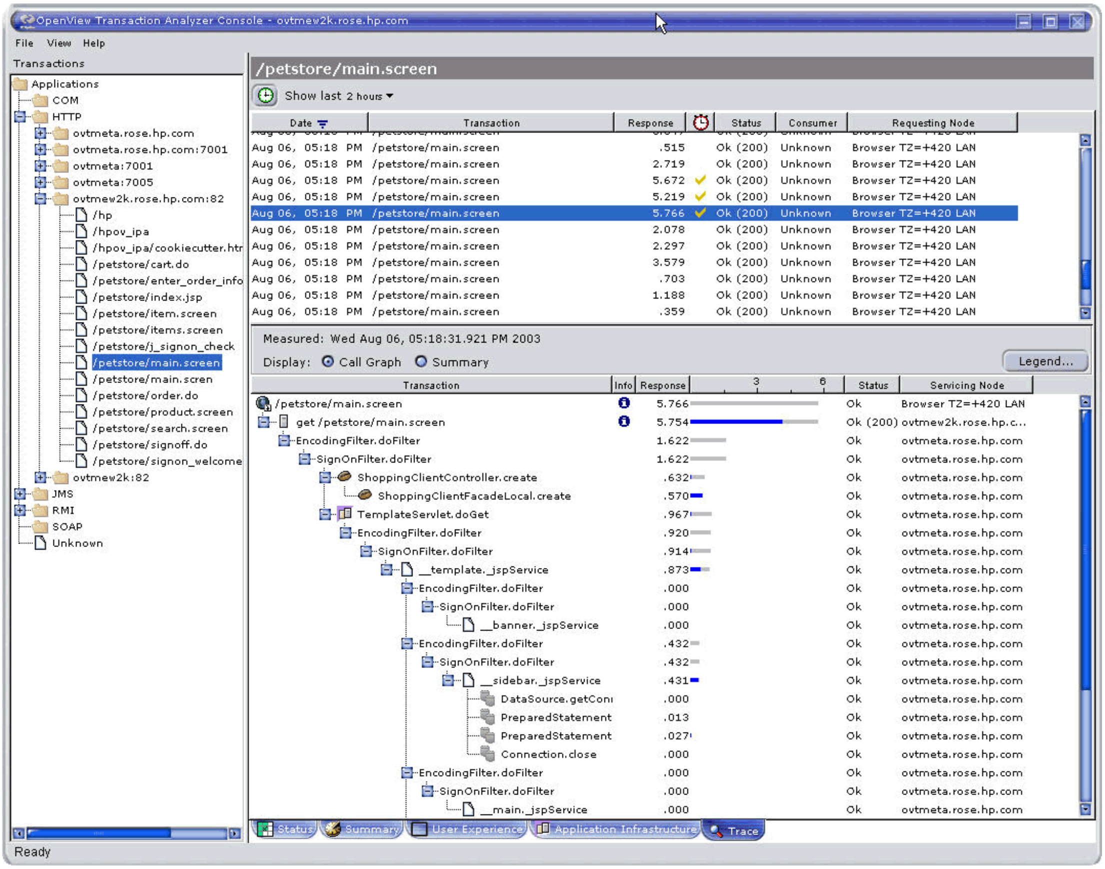
Name	4 PM	4:10	4:20	4:30	4:40	4:50	5 PM	5:10	5:20	5:30	5:40	5:50
/hp												
/hpov_ipa												
/hpov_ipa/cookiecutter.ht...												
/petstore/cart.do												
/petstore/enter_order_inf...												
/petstore/index.jsp			🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟩	🟩	🟩
/petstore/item.screen												
/petstore/items.screen		🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟨	🟨	🟨	🟨
/petstore/j_signon_check												
/petstore/main.screen		🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟦	🟦	🟦	🟦
/petstore/main.scren												
/petstore/order.do												
/petstore/product.screen		🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟦	🟨	🟨	🟨
/petstore/search.screen			🟦	🟩	🟩	🟩	🟩	🟧	🟥	🟥	🟥	🟥
/petstore/signoff.do												
/petstore/signon_welcom...												

Response: □ Not Measured 🟩 Normal 🟦 Warning 🟨 Minor 🟧 Major 🟥 Critical
Availability: ✕ One or more probes unsuccessful.

Task 6: Use the Trace function in the OVIS Dashboard

Clicking on the OVTA icon in the Trace column of the OVIS Dashboard Health workspace Alarms tab launches the OVTA Console in context, automatically selecting the corresponding transaction and showing the trace view for this transaction.

See the OVTA Console Trace example shown below:


OpenView Transaction Analyzer Console - ovtmew2k.rose.hp.com
File
View
Help
Legend...
Status
Summary
User Experience
Application Infrastructure
Trace
Ready

Transactions

- Applications
  - COM
  - HTTP
    - ovtmeta.rose.hp.com
    - ovtmeta.rose.hp.com:7001
    - ovtmeta:7001
    - ovtmeta:7005
    - ovtmew2k.rose.hp.com:82
      - /hp
      - /hpov_ipa
      - /hpov_ipa/cookiecutter.htr
      - /petstore/cart.do
      - /petstore/enter_order_info
      - /petstore/index.jsp
      - /petstore/item.screen
      - /petstore/items.screen
      - /petstore/j_signon_check
      - /petstore/main.screen
      - /petstore/main.scren
      - /petstore/order.do
      - /petstore/product.screen
      - /petstore/search.screen
      - /petstore/signoff.do
      - /petstore/signon_welcome
    - ovtmew2k:82
  - JMS
  - RMI
  - SOAP
  - Unknown

/petstore/main.screen

Show last 2 hours

Date	Transaction	Response	⏱	Status	Consumer	Requesting Node
Aug 06, 05:18 PM	/petstore/main.screen	.515		Ok (200)	Unknown	Browser TZ=+420 LAN
Aug 06, 05:18 PM	/petstore/main.screen	2.719		Ok (200)	Unknown	Browser TZ=+420 LAN
Aug 06, 05:18 PM	/petstore/main.screen	5.672	✓	Ok (200)	Unknown	Browser TZ=+420 LAN
Aug 06, 05:18 PM	/petstore/main.screen	5.219	✓	Ok (200)	Unknown	Browser TZ=+420 LAN
Aug 06, 05:18 PM	/petstore/main.screen	5.766	✓	Ok (200)	Unknown	Browser TZ=+420 LAN
Aug 06, 05:18 PM	/petstore/main.screen	2.078		Ok (200)	Unknown	Browser TZ=+420 LAN
Aug 06, 05:18 PM	/petstore/main.screen	2.297		Ok (200)	Unknown	Browser TZ=+420 LAN
Aug 06, 05:18 PM	/petstore/main.screen	3.579		Ok (200)	Unknown	Browser TZ=+420 LAN
Aug 06, 05:18 PM	/petstore/main.screen	.703		Ok (200)	Unknown	Browser TZ=+420 LAN
Aug 06, 05:18 PM	/petstore/main.screen	1.188		Ok (200)	Unknown	Browser TZ=+420 LAN
Aug 06, 05:18 PM	/petstore/main.screen	.359		Ok (200)	Unknown	Browser TZ=+420 LAN

Measured: Wed Aug 06, 05:18:31.921 PM 2003

Display: ● Call Graph ○ Summary

Transaction	Info	Response	3 6	Status	Servicing Node
/petstore/main.screen	ℹ	5.766		Ok	Browser TZ=+420 LAN
get /petstore/main.screen	ℹ	5.754		Ok (200)	ovtmew2k.rose.hp.c...
EncodingFilter.doFilter		1.622		Ok	ovtmeta.rose.hp.com
SignOnFilter.doFilter		1.622		Ok	ovtmeta.rose.hp.com
ShoppingClientController.create		.632		Ok	ovtmeta.rose.hp.com
ShoppingClientFacadeLocal.create		.570		Ok	ovtmeta.rose.hp.com
TemplateServlet.doGet		.967		Ok	ovtmeta.rose.hp.com
EncodingFilter.doFilter		.920		Ok	ovtmeta.rose.hp.com
SignOnFilter.doFilter		.914		Ok	ovtmeta.rose.hp.com
__template._jspService		.873		Ok	ovtmeta.rose.hp.com
EncodingFilter.doFilter		.000		Ok	ovtmeta.rose.hp.com
SignOnFilter.doFilter		.000		Ok	ovtmeta.rose.hp.com
__banner._jspService		.000		Ok	ovtmeta.rose.hp.com
EncodingFilter.doFilter		.432		Ok	ovtmeta.rose.hp.com
SignOnFilter.doFilter		.432		Ok	ovtmeta.rose.hp.com
__sidebar._jspService		.431		Ok	ovtmeta.rose.hp.com
DataSource.getConı		.000		Ok	ovtmeta.rose.hp.com
PreparedStatement		.013		Ok	ovtmeta.rose.hp.com
PreparedStatement		.027		Ok	ovtmeta.rose.hp.com
Connection.close		.000		Ok	ovtmeta.rose.hp.com
EncodingFilter.doFilter		.000		Ok	ovtmeta.rose.hp.com
SignOnFilter.doFilter		.000		Ok	ovtmeta.rose.hp.com
__main._jspService		.000		Ok	ovtmeta.rose.hp.com

Also note that although OVIS save up to 30 days of trace data, OVTA may not have this much data, it depends on how you have set up OVTA. And if you select a transaction that has been deleted from the OVTA database you will get an error saying transaction definition not found.

Task 7: OVTA Reports

Reports with OVTA specific data are available in the OVIS Dashboard Reports workspace. See the *OVTA User's Guide* for details on these reports.

- OVTA Service Group Summary

- OVTA Application Summary of Activity for the Last Day
- OVTA Application Summary of Activity for the Last Week
- OVTA Application Response Time Violations
- OVTA Application Response Time
- OVTA Application Transaction Volume
- OVTA Application Response Time Violations (Consumer Perspective)
- OVTA Application Response Time Violations (Consumer/System Detail)
- OVTA Application - Worst Performing Transactions

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.

Removing Unused OVIS Reports (Optional)

If your OVIS Management Server is dedicated to importing OVTA data only then you may want to remove the unused OVIS reports (over 30 reports) that are automatically generated each night. This can shorten the nightly report generation cycle time by eliminating empty reports.

The following file is provided to allow you to easily remove these OVIS only reports:

```
<install dir>\newconfig\packages\remove\repload_IOPS_remove_OVIS_reports.SRP
```

To remove the unused OVIS probe report templates from the nightly processing, run:

```
repload -remove repload_IOPS_remove_OVIS_reports.SRP
```

If OVIS probes are ever used in the future, you can just rerun the repload command above with this SRP file but without the `-remove` option.

Example SLOs and SLAs

Availability

While possible, there is really no need to configure availability SLO/SLAs for the imported 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).

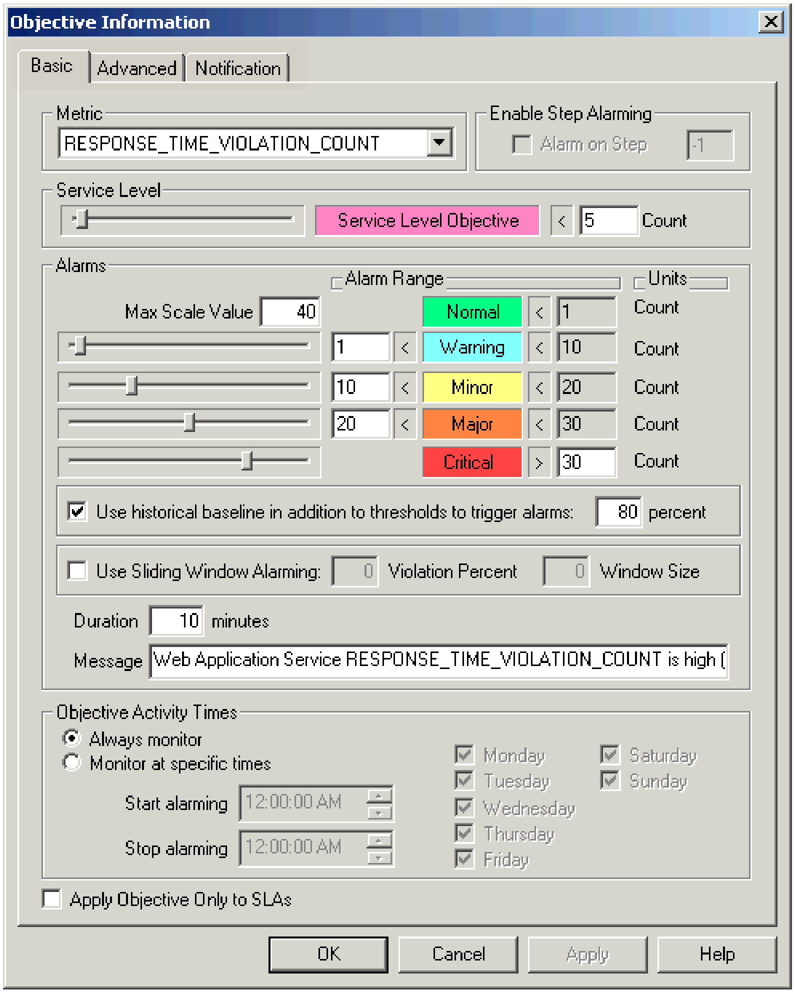
The response time violation threshold for OVTA transactions cannot be configured in the OVIS Configuration Manager. Use the OVTA Configuration Editor to set the thresholds on the transactions of interest. The RESPONSE_TIME_VIOLATION_COUNT and RESPONSE_TIME_VIOLATION_PERCENTAGE metrics are measured in the OVTA Transaction Agent against these configured thresholds. Refer to the *OVTA Users Guide* for additional information.

The transaction types selected in the WEBAPP 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.

The following examples are shown using the WEBAPP service type

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.



Metric: RESPONSE_TIME_VIOLATION_COUNT

Enable Step Alarming: □ Alarm on Step -1

Service Level: Service Level Objective < 5 Count

Alarms

Max Scale Value 40

	Alarm Range			Units
	Normal	<	1	Count
1 <	Warning	<	10	Count
10 <	Minor	<	20	Count
20 <	Major	<	30	Count
	Critical	>	30	Count

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

□ Use Sliding Window Alarming: 0 Violation Percent 0 Window Size

Duration 10 minutes

Message: Web Application Service RESPONSE_TIME_VIOLATION_COUNT is high (

Objective Activity Times

● Always monitor

○ Monitor at specific times

Start alarming 12:00:00 AM

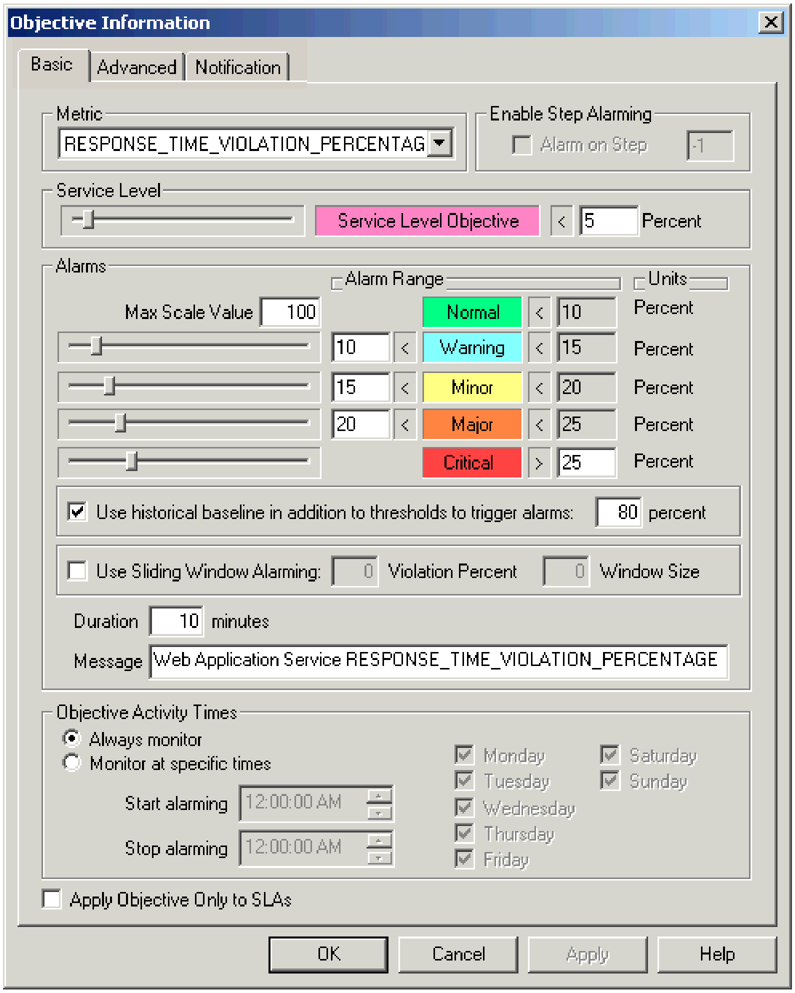
Stop alarming 12:00:00 AM

☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

□ Apply Objective Only to SLAs

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.



Metric: RESPONSE_TIME_VIOLATION_PERCENTAG

Enable Step Alarming: □ Alarm on Step -1

Service Level: Service Level Objective < 5 Percent

Alarms

Max Scale Value 100

		Alarm Range			Units
		Normal	<	10	Percent
10	<	Warning	<	15	Percent
15	<	Minor	<	20	Percent
20	<	Major	<	25	Percent
		Critical	>	25	Percent

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

□ Use Sliding Window Alarming: 0 Violation Percent 0 Window Size

Duration 10 minutes

Message Web Application Service RESPONSE_TIME_VIOLATION_PERCENTAGE

Objective Activity Times

● Always monitor

○ Monitor at specific times

Start alarming 12:00:00 AM

Stop alarming 12:00:00 AM

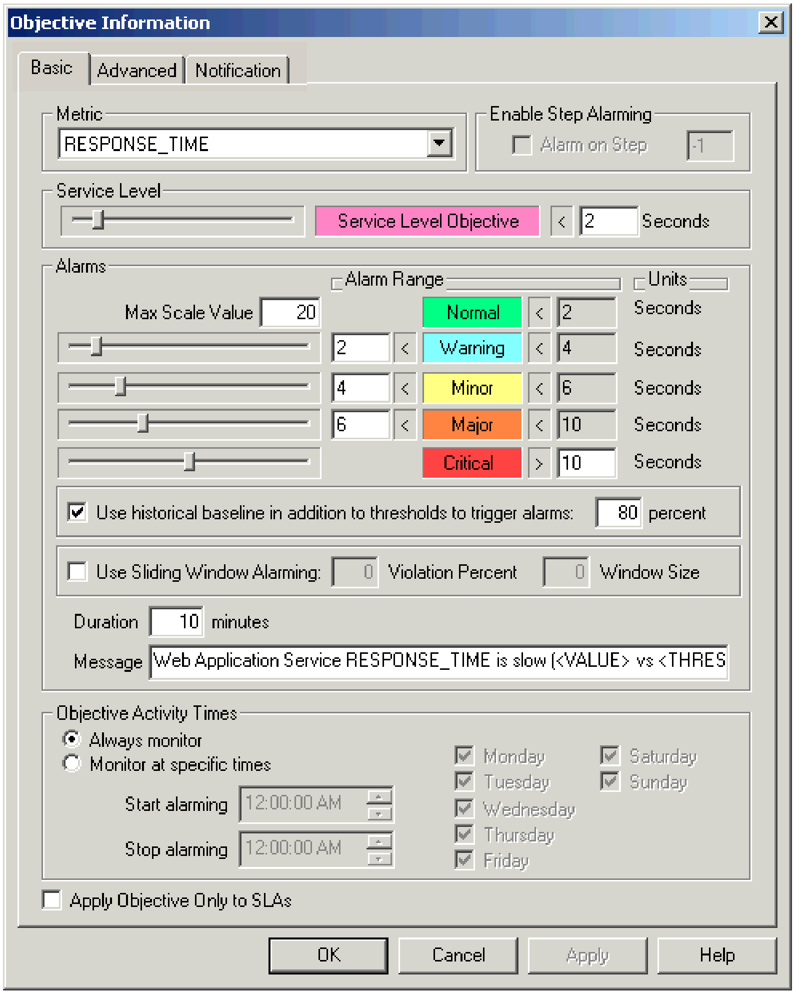
☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

□ Apply Objective Only to SLAs

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: RESPONSE_TIME

Enable Step Alarming: ☐ Alarm on Step -1

Service Level: Service Level Objective < 2 Seconds

Alarms

Max Scale Value 20

Alarm Range				Units
	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

☐ Use Sliding Window Alarming: 0 Violation Percent 0 Window Size

Duration 10 minutes

Message Web Application Service RESPONSE_TIME is slow (<VALUE> vs <THRES

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

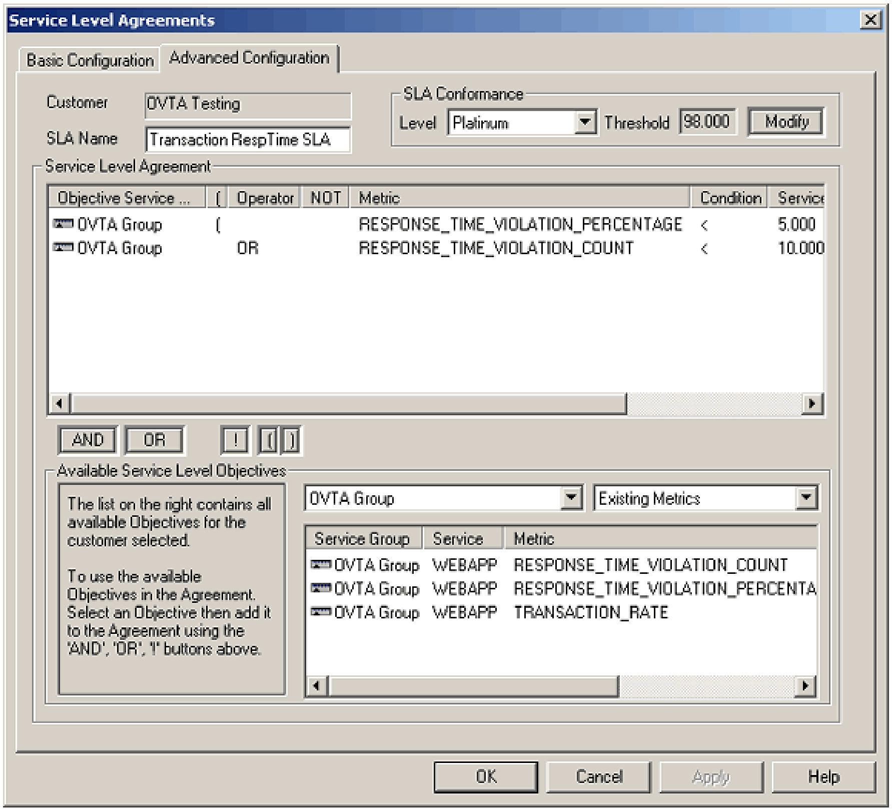
☐ Apply Objective Only to SLAs

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).



Customer: OVTA Testing

SLA Name: Transaction RespTime SLA

SLA Conformance — Level: Platinum — Threshold: 98.000

Service Level Agreement

Objective Service ...	(	Operator	NOT	Metric	Condition	Servic
OVTA Group	(			RESPONSE_TIME_VIOLATION_PERCENTAGE	<	5.000
OVTA Group		OR		RESPONSE_TIME_VIOLATION_COUNT	<	10.000

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

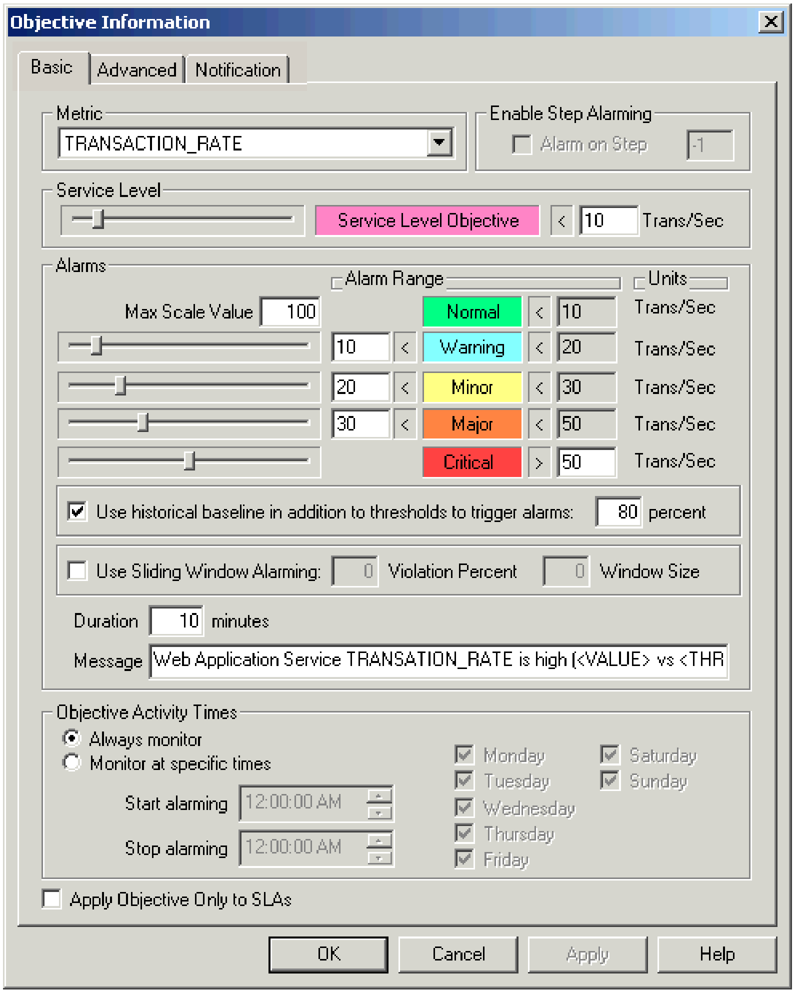
Volume

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.



Metric: TRANSACTION_RATE

Enable Step Alarming: □ Alarm on Step -1

Service Level: Service Level Objective < 10 Trans/Sec

Alarms

Max Scale Value 100

		Alarm Range			Units
		Normal	<	10	Trans/Sec
10	<	Warning	<	20	Trans/Sec
20	<	Minor	<	30	Trans/Sec
30	<	Major	<	50	Trans/Sec
		Critical	>	50	Trans/Sec

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

□ Use Sliding Window Alarming: 0 Violation Percent 0 Window Size

Duration 10 minutes

Message Web Application Service TRANSATION_RATE is high (<VALUE> vs <THR

Objective Activity Times

● Always monitor

○ Monitor at specific times

Start alarming 12:00:00 AM

Stop alarming 12:00:00 AM

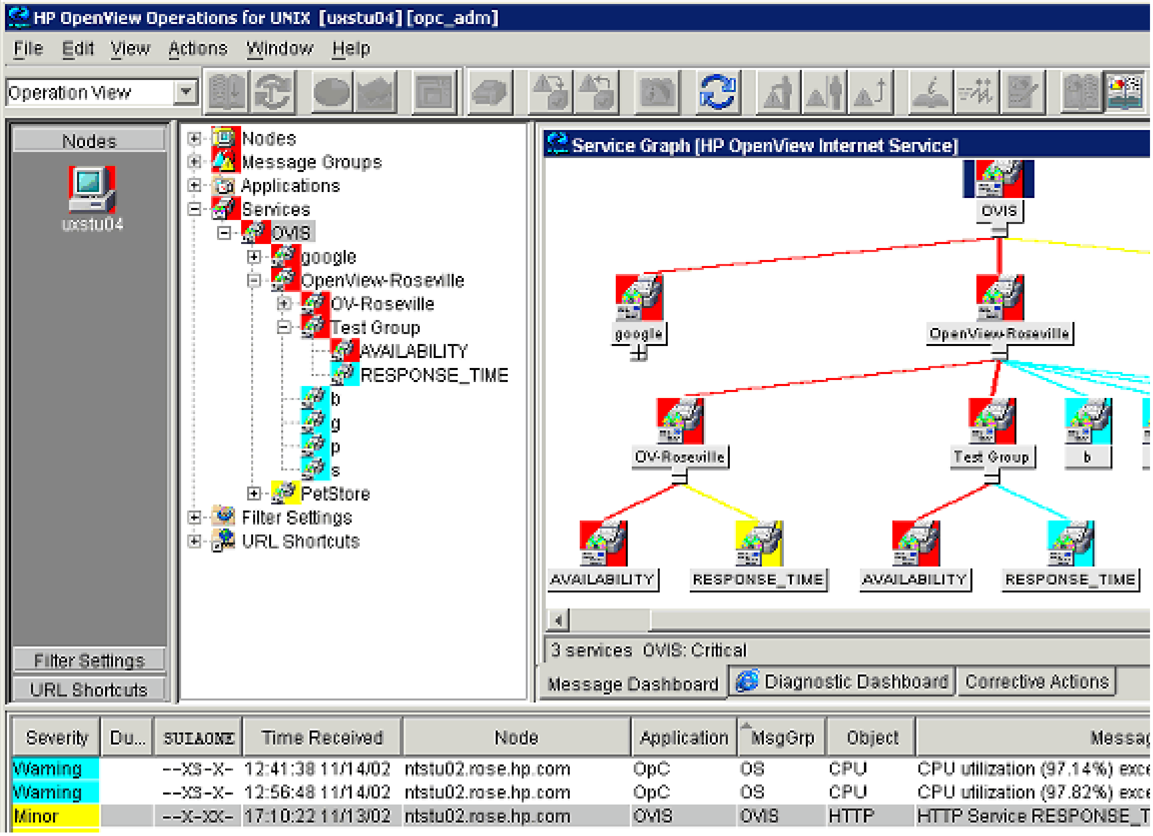
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday

□ Apply Objective Only to SLAs

Integrating with OpenView Operations for UNIX

To integrate OVIS with OpenView Operations for UNIX (OVO), you must install the OVIS integration package for OVO for UNIX (on the OVIS CD) onto the OVO for UNIX management server. Then, from the OVO Console, you can distribute the Internet Services templates to the OVIS 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 template (OVIS Alarms (3)) provides state based correlation of failure alarms (critical, minor, major, warning and normal alarms). This means an old alarm is automatically acknowledged and put in the history browser thus reflecting the current state of the objective. The Continuous Alarming option should be enabled for the state based correlation.
- You can configure an OVO action to launch the OVIS Dashboard in context based on customer. Note that if you have restricted views set up in OVIS, the Dashboard launch will take you to a login screen and then to the main Dashboard rather than to a detail view based on customer.
- The integration package is installable on Japanese systems running Japanese OVO for UNIX (6 and 7). Note that templates are not yet localized.



Severity	Du...	SUIAONE	Time Received	Node	Application	MsgGrp	Object	Messag
Warning		--XS-X-	12:41:38 11/14/02	ntstu02.rose.hp.com	OpC	OS	CPU	CPU utilization (97.14%) exce
Warning		--XS-X-	12:56:48 11/14/02	ntstu02.rose.hp.com	OpC	OS	CPU	CPU utilization (97.82%) exce
Minor		--X-XX-	17:10:22 11/13/02	ntstu02.rose.hp.com	OVIS	OVIS	HTTP	HTTP Service RESPONSE_T

Requirements

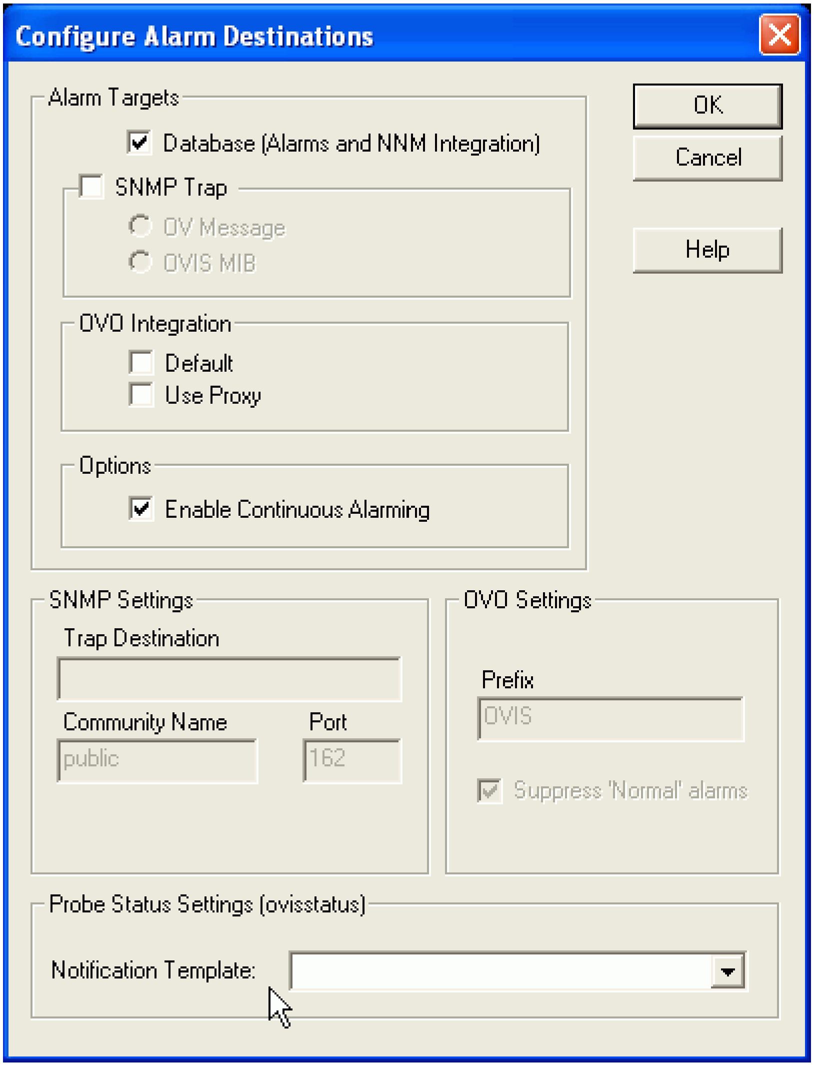
- Refer to the Internet Services release notes for OVO UNIX version requirements.
- Mozilla 1.7 or higher is required on the OVO management server for displaying the Internet Services Dashboard web display. The browser is launched with the **ovweb** command. Please refer to the **ovweb** man-page for correct setup.
- In order to display the Internet Services Dashboard in the OVO Java GUI correctly on Windows systems, the Web browser option under **Edit > Preferences** must be set to ActiveX Internet Explorer control.

- An OVO agent must be installed and running on the OVIS management server for the Internet Services dashboard integration, forwarding alarm messages to OVO, 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, the OVO agent and OVIS must be installed into C: drive unless you have installed the latest OVO NT agent patch.
- A checkbox selection must be made within the Internet Services Configuration Manager Alarm Destinations dialog to forward alarms 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. After selecting the alarm destination settings, be sure to select **Save Probe Configuration Files** before exiting the Configuration Manager.

- **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



Alarm Targets

☑ Database (Alarms and NNM Integration)

☐ SNMP Trap

○ OV Message

○ OVIS MIB

OVO Integration

☐ Default

☐ Use Proxy

Options

☑ Enable Continuous Alarming

SNMP Settings

Trap Destination:

Community Name: public

Port: 162

OVO Settings

Prefix: OVIS

☑ Suppress 'Normal' alarms

Probe Status Settings (ovisstatus)

Notification Template:

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) or OVIS Alarms (3) 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 go through the following steps to delete the existing templates.

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

Un-assign all Internet Services OVO templates from the OVIS Management Server and all OVIS probe systems as follows:

1. From within the OVO **Message Source Template** window:

   a. Double-click on Internet Services in the Template Groups list in the left pane.

b Select each entry in the right pane and click the **Delete from All** button for each of the following groups:

OVIS Probe NT
OVIS Probe Unix
OVIS Server
OVIS Server (2)
OVIS Server (3)
OVIS ITO Mgmt Server

c In the left pane select Internet Services again and click the **Delete from All** button.

d In the right pane select each item containing “OVIS” and click the **Delete from All** button, this includes the following:

Message OVIS Alarms
Message OVIS Alarms (2)
Message OVIS Alarms (3)
Logfile OVIS Errors (Probe)
Logfile OVIS Error (Probe-Unix)
Logfile OVIS Errors (Server-OVIS)
Logfile OVIS Errors (Server-Reporter)
Monitor OVIS_SM_InetInfo
Monitor OVIS_SM_Sched
Monitor OVIS_SM_Sched_UX
Schedule OVIS Service Sync

e Then go to the OVO Message Group Bank window and delete the OVIS and OVIS_Errors group if still present

f Deinstall the integration package: swremove HPVPIS-SP.

➤ A deletion of a group will only delete the group and NOT the group members; it is important that you complete all the above steps to delete all the group members.

Task 2: Install the Integration Package

If you are upgrading from a previous version, be sure to complete Task 1 above first to delete any existing OVIS/OVO integration templates, then you can install the new integration package.

1. Follow the OVO Integration installation instructions provided with the OVIS installation CD (**readme.txt** or the install document provided in hardcopy with your OVIS CD).
2. In the OVIS Configuration Manager select the **Save Probe Configuration Files** toolbar button.
3. 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 (**`Actions > Node > Add`**). You add nodes using the Node Bank window. If this window is not already open, use the Window pull-down menu from any current windows and select the Node Bank window.

   Enter the name of your node in the “Hostname” field and press **Tab**. When the window updates, check to be sure it has the following configuration:

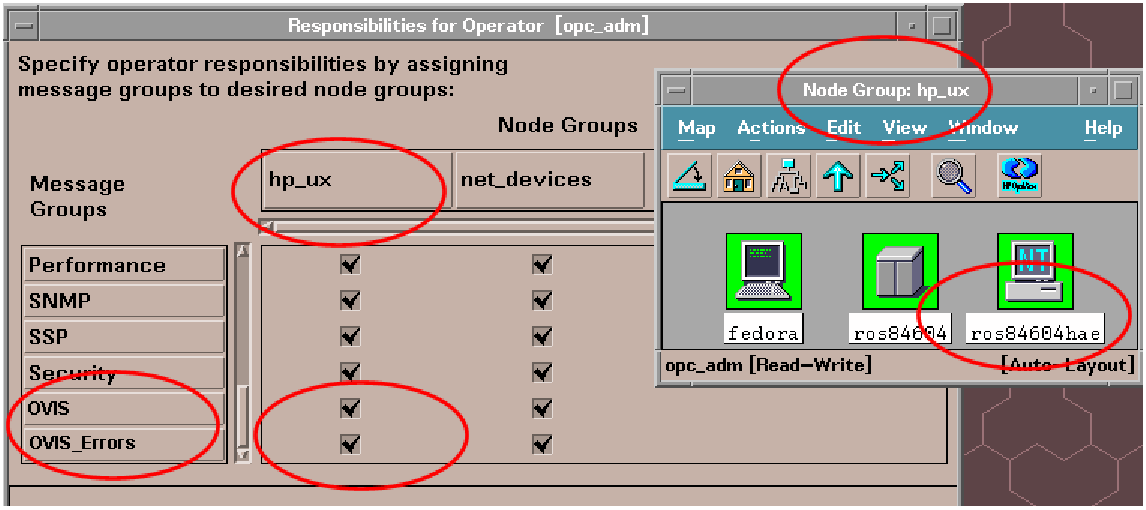
   Net Type - IP Network Intel x86/PX Windows NT/2000

   Type of managed node - Controlled
3. Install an OVO agent on the Internet Services management 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. Restart the OVIS sever.

4 The following steps are to 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 (see the note below for when you do not need to install the OVO agent on these nodes).

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 probe-installed systems (nodes) to an OVO node group (**Window > Node Group Bank**). First be sure there is a Node Group created and then drag and drop your OVIS nodes from the Node Bank window into the new node group.



Specify operator responsibilities by assigning message groups to desired node groups:

Message Groups	hp_ux	net_devices
Performance	☑	☑
SNMP	☑	☑
SSP	☑	☑
Security	☑	☑
OVIS	☑	☑
OVIS_Errors	☑	☑

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**. Then select the appropriate operator (for example, opc_adm) and

right-click and select **Modify**. From the Modify User window select the **Responsibilities** button to assign the OVIS and OVIS Error message groups. Select **Close** in this window and **OK** in the Modify User window.

7 Go to the Node Bank window

> ➤ 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`. Note that on Windows the path must be enclosed in quotes if it has any spaces.

a In the Node Bank window, highlight your OVIS Server node and then select **Actions > Agents > Assign Templates**.

b In the Define Configuration window select the **Add** button, this brings up the Add Configuration window.

c In the Add Configuration window, select the **Open Template Window** button, this brings up the Message Source Templates window.

d Highlight the Internet Services template group in the left pane and then select **Group OVIS Probe NT** and either **Group OVIS Server, OVIS Server (2) or OVIS Server (3)** (see the note below for how to choose which one).

> ➤ Note that there are three template groups: OVIS Server, OVIS Server (2) and OVIS Server (3). Only one of these needs to be assigned. Typically you would use the OVIS Server (3) template group if you wish a state based correlation or OVIS Server (2) if you wish to use good/bad message correlation. The OVIS Server template group does not provide correlation. The OVIS Server (3) 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 you are using OVIS Server (2) or OVIS Server (3) Template groups.

e Go back to the Add Configuration window and select the **Get Template Selections** button and then select **OK**.

f In the Define Configuration window, select **OK**.

g Close the Message Source Template window.

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

➤ On Windows systems, 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`. Note that on Windows the path must be enclosed in quotes if it has any spaces.

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

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

2 Assign the **OVIS ITO Mgmt Server** template group to the OVO Management Server.

3 In the **OVIS ITO Mgmt Server** template group, select the **OVIS Service Sync** scheduled action template and add the Internet Services server name to the command line. (Include the fully qualified hostname of the Internet Services server; for example, `/opt/OV/OVIS/bin/vpispull.sh jester.dev.hp.com`. This script synchronizes the Internet Services customer/service group/objective hierarchy to Service Navigator every 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.)

Task 5: Complete the Integration

1 Now you need to deploy the templates (and optionally, the schedule for the Service Navigator integration) to your OVO Agent running on the OVIS Server.

a First select your OVIS Server node from the node bank and use the menu option **Actions > Agents > Install/Update SW & Config** from the menu.

b. In the **Install/Update Software and Configuration window**, be sure to de-select Agent Software under Components but select all other options (Templates, Actions, Monitors, Commands) including Force Update.

c. Press **OK**. If the distribution was successful, you receive appropriate messages in the OVO message browser.

2. Be sure you have set up Alarm Destinations for **OVO Integration** in the OVIS Configuration Manager and have checked either of the following. If you make any changes to the settings, be sure to select **Save Probe Configuration Files** before exiting the Configuration Manager.

   Default - See Configuration Options on page 324 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 6: 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
```

OVIS Message Forwarding to OVO

OVIS uses the following set of OVO attributes (opcmsg) when passing alarm messages.

```
opcmsg [-help] [-id] [severity=normal|warning|minor|major|critical]
          application=<application> object=<object> msg_text=<text>
          [msg_grp=<message group>] [node=<node>] [service_id=<svcid>]
         [-option <var>=<value>}
```

Table 4 opcmsg Attributes for Message Forwarding

OVO attribute (opcmsg)	OVIS value
object	target host:probe system:target info
msg_grp	OVIS_<probe name>
node	OVIS server FQDN (or if proxy was configured in the GUI, target node FQDN)
msg_txt	message text
application	OVIS
severity	OVIS severity

option variables	host=<target host>
	ps=<probe system>
	target=<target info>
	vpis=<OVIS server FQDN>
	customer=<customer>
	customerURLE=<customer>
	serviceGroup=<service group>
	serviceGroupURLE=<service group>
	probeDesc=<probe desc>
	probeDescURLE=<probe desc>
	probeType=<probe name>
	probeTypeURLE=<probe name>
	metric=<metric>
	ipAddr=<ip addr of target if available>
	psts=<timestamp in UTC when measurement was taken>

➤ In addition, the program OVISStatus.exe runs automatically and sends alarms to OVO or NNM if data is not received from the probe system within the expected time + 10 percent, to allow for minor delays.

Integrating with Network Node Manager

Integrating Internet Services with NNM allows NNM to receive configuration and event information from the Internet Services database, adding 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.

➤ In addition, the program OVISStatus.exe runs automatically and sends alarms to OVO or NNM if data is not received from the probe system within the expected time + 10 percent, to allow for minor delays.

The first task for initiating the Internet Services integration is to install the Internet Services NNM integration 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 important information on NNM version and patch requirements.
- You may not use terminal services when installing the Internet Service NNM integration software on Windows.

- Refer to the OVIS-NNM Integration release notes that come with the integration package. After installation these release notes can be found under `/opt/OV/www/htdocs/C/ReleaseNotes/ovisnnm_releasenotes.html` on UNIX systems and on Windows systems these release notes can be launched after the installation finishes.
- 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).
- Internet Explorer (version 6.0 or greater) and Mozilla 1.7 are supported browsers on the management server for the Internet Services Dashboard integration

➤ Before you install OVIS's 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 OVIS-NNM Integration installation instructions provided with the OVIS CD (readme.txt or in the printed install document).** Installation differs depending on whether you are integrating with NNM on Windows, Sun Solaris, or HP-UX.

Refer to the OVIS-NNM Integration release notes that come with the integration package. After installation these release notes can be found under `/opt/OV/www/htdocs/C/ReleaseNotes/ovisnnm_releasenotes.html` on UNIX systems and on Windows systems these release notes can be launched after the installation finishes.

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 and provide the OVIS Dashboard port number. The OVIS Management Server name and OVIS Dashboard port can be changed after the installation by modifying the following file on your NNM system: `<install dir>/conf/ovis.conf`.

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).

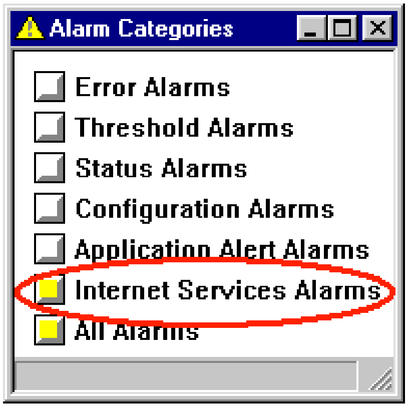
Features in NNM after Integration with Internet Services

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.
- **Dashboard** - launch the Internet Services dashboard.

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:

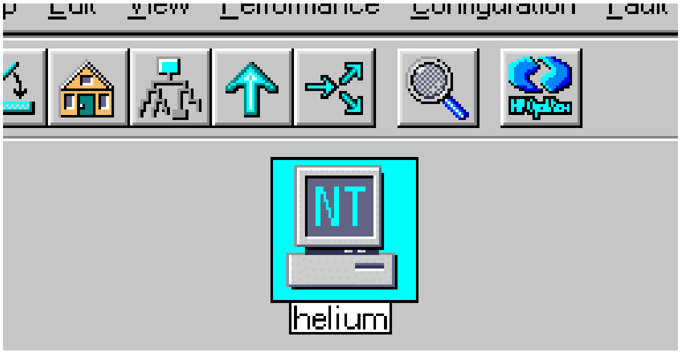
- **Customer(s)** served by the node.
- **Services monitored** - customers have child submaps that contain symbols representing the services monitored for them.
- **Service objective alarms** - services also have child submaps that display the service objective alarms for the monitored service.

An illustration later in this chapter shows new symbols.

About Configuration Events

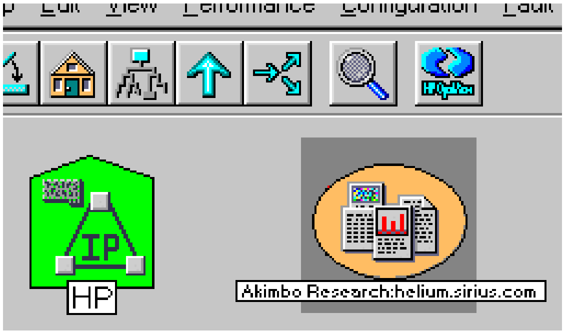
A Internet Services configuration change is an event that results in a change to the NNM display. In this way, NNM is updated to reflect the new Internet Services information. For example, configuration events could cause the following behaviors in NNM:

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.

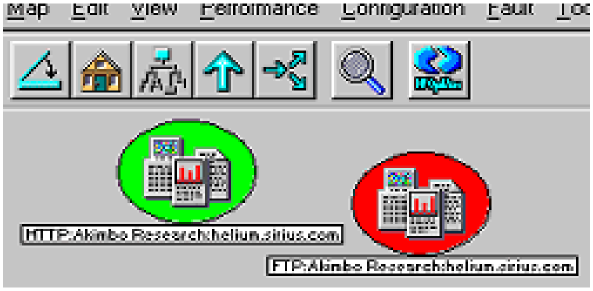


2 Creates a symbol representing the customer as a child of the target node. The name of the symbol is "`customer_name:node_name`". For example, suppose you have a node named "`helium.sirius.com`" which provides a service for a customer named "`Akimbo Research`". NNM creates a new

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`".


Map
Edit
View
Performance
Configuration
Fault
HTTP:Akimbo Research:helium.sirius.com
FTP: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

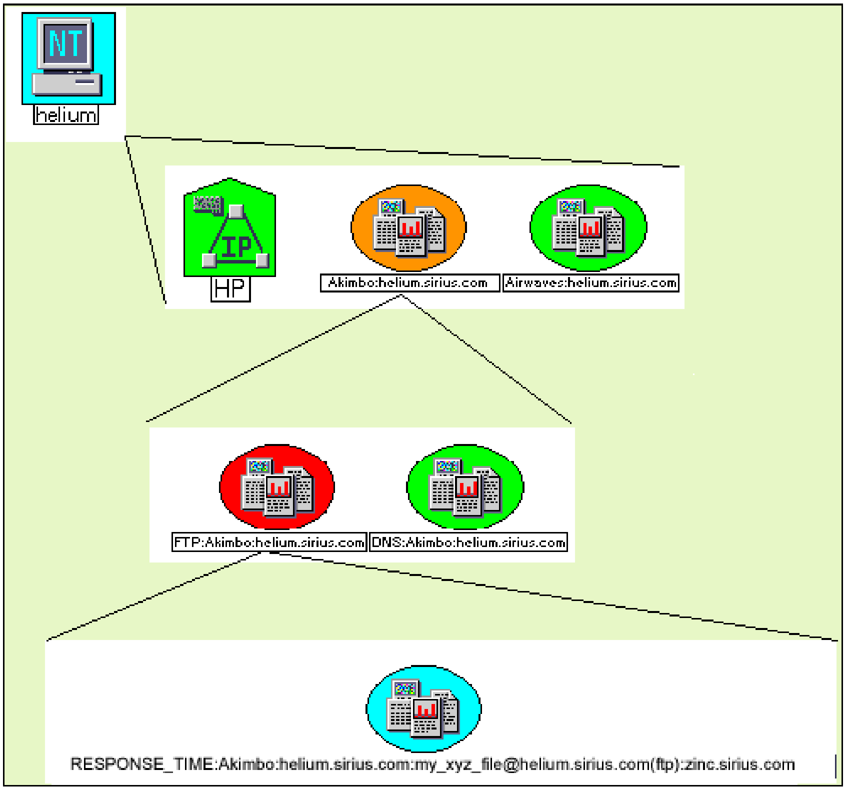
The name of the service objective symbol would then be:

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.


NT
helium
IP
HP
Akimbo:helium.sirius.com
Airwaves:helium.sirius.com
FTP:Akimbo:helium.sirius.com
DNS:Akimbo:helium.sirius.com
RESPONSE_TIME:Akimbo:helium.sirius.com:my_xyz_file@helium.sirius.com(ftp):zinc.sirius.com

Simple Troubleshooting for NNM Integration

Re-Set Data with ovisclean.ovpl

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 OVIS station. The script also causes a rebuild of all Internet Services symbols within NNM maps.

Handling NNM and OVIS Port Conflicts

If you find there are port conflicts between NNM and OVIS when they are installed on the same system, you can change the OVIS Dashboard ports (Tomcat) as follows on the OVIS Management Server (the port numbers shown below are only examples):

```
cd <installdir>\bin

ovc -stop ovtomcatA

cscript /nologo OvTomcatCtl.vbs -setshutdownport 9005

cscript /nologo OvTomcatCtl.vbs -sethttpport 9080

cscript /nologo OvTomcatCtl.vbs -setjk2port 9007

ovc -start ovtomcatA
```

Note, the above port numbers are only examples. You can use `nestat -an` to see which ports are taken.

Note, after changing the ports, you need to set the http port that you chose above in the OVIS Configuration Manager **File > Configure > Web Server Properties**. Enter the port number in the Tomcat - Dashboard (Web Server) Port field.

Cleanup after Uninstalling NNM-OVIS Integration

After uninstalling the NNM integration (`/opt/OV/bin/remove.ovisnnm`), the Internet Services alarm category needs to be removed.

1 Start `ovw` and select **Options > Event Configuration**.

2 In the Enterprise Identification, select **OpenView**. Select all events starting with **OVIS_**. Select **Edit > Delete > Events**.

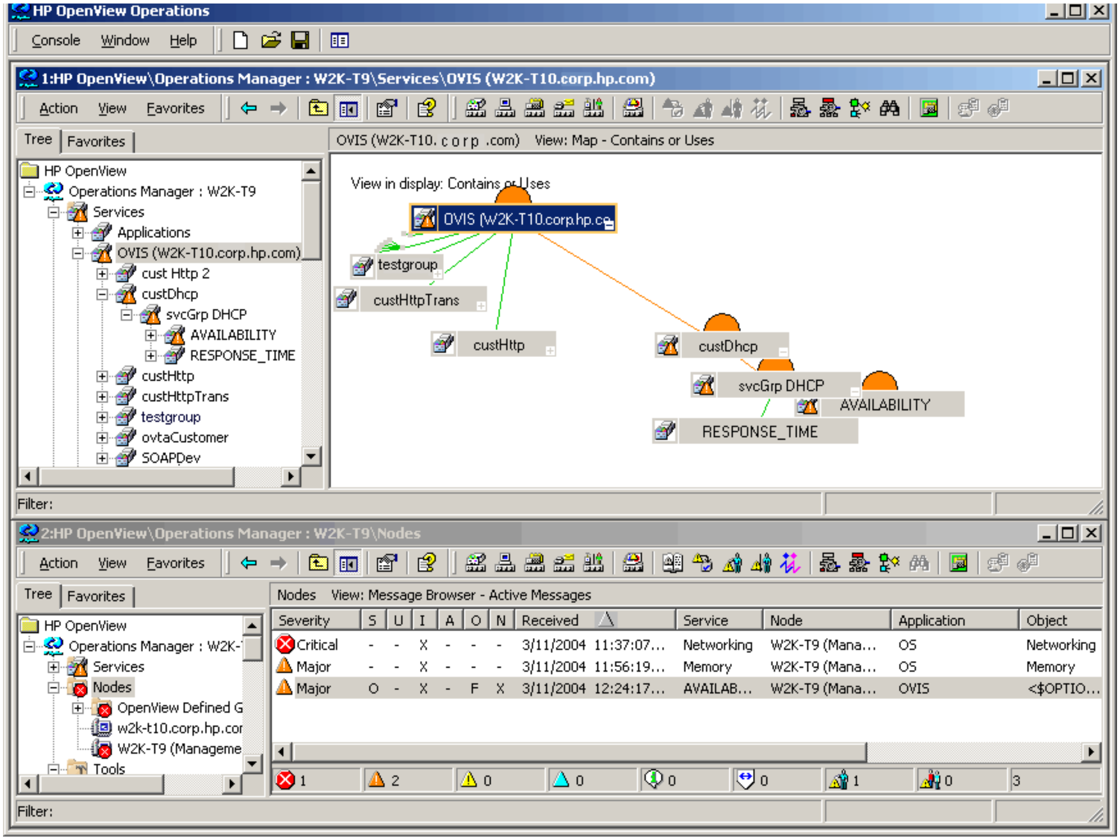
3 To remove the category, select **Edit > Configure > Alarm Categories**. Select **Internet Services Alarms**, press **Delete**.

Integrating with OpenView Operations for Windows

OVIS integration with OpenView Operations for Windows (OVO for Windows) results in the following:

- OVIS customer/service groups are added to the OVO for Windows services tree and displayed in the service map view. OVIS metrics with service level objectives (SLOs) for a service group are shown in the service map view.
- OVIS service level alarms are forwarded as alarm messages to OVO for Windows for display in the Console message browser. The messages are related to corresponding services.
- You can run Operator Initiated commands for these OVIS generated alarms which launch the OVIS Dashboard display.
- For a selected service you can select Launch Tool to launch the OVIS Dashboard in context for a specific customer, service group or metric.

See the example that follows of the OVO for Windows Console after integration with OVIS.



Severity	S	U	I	A	O	N	Received	Service	Node	Application	Object
Critical	-	-	X	-	-	-	3/11/2004 11:37:07...	Networking	W2K-T9 (Mana...	OS	Networking
Major	-	-	X	-	-	-	3/11/2004 11:56:19...	Memory	W2K-T9 (Mana...	OS	Memory
Major	O	-	X	-	F	X	3/11/2004 12:24:17...	AVAILAB...	W2K-T9 (Mana...	OVIS	<$OPTIO...

Requirements

OVO for Windows and OVIS can be integrated when they are on the same or on different systems. If they are on different systems, an OVO agent must be installed on the OVIS Management Server system. The OVO for Windows integration for OVIS 6 requires the OVOW Agent version 7.27 or higher on the OVIS Management Server (patch OVOW_00059).

Prior to integration, you must be sure OVIS service targets, objectives and alarm thresholds have been configured in OVIS and that graphs are being generated in the OVIS Dashboard.

Note that if you have restricted views set in the OVIS Dashboard the Dashboard launch from the OVO Console will take you to a login screen and then to the main Dashboard rather than to a detail view based on the context of the item selected in OVO.

Installing OVIS and a clustered OVO for Windows server (7.5 or higher) on the same system is not supported.

Installation Steps

On the OVO for Windows Server, use the OVIS installation CD (if the installation program does not automatically start, run `\Autorun\setup.exe` from your CD drive) and select **Operations for Windows Integration**.

Install the OVIS Operations for Windows Integrationsoftware. You will be prompted to enter the OVIS Management Server hostname.

If the OVIS/OVOW Integration is to be installed on a clustered OVOW system, additional steps have to be performed (for more information see the OVO online help topic: “Managing cluster-aware applications”). The additional steps are to sure that the scheduled task that updates the service map is only executed on the active OVOW server. See Steps for a Clustered OVOW System on page 347.

During installation of the OVO for Windows integration component, files are installed onto the OVO for Windows Server in the following directory: `%OVINSTALLDIR%\bin\OvIS`.

Configuration Steps

1 In the OVO for Windows Console, add the Internet Services Management 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 Adding the OVIS Management Server as an OVO for Windows node initiates auto-discovery which includes the deployment of an OVO agent to the OVIS Management Server, if it is on a different system than OVO. If for some reason this does not happen, you will need to install the OVO agent on the OVIS Management Server.

With OVO 7.x, the OVO agent and OVIS must be installed into the C: drive unless you have installed the latest OVO Agent Windows patch (see the OVO documentation).

3 Reboot the OVIS server after the agent is deployed.

Steps for a Clustered OVOW System

If the OVIS/OVOW Integration is to be installed on a clustered OVOW system, additional steps have to be performed.

1 Install the OVIS/OVOW Integration on all OVOW management server cluster nodes and follow the configuration steps above.

2 Modify the file `OvOWSelfManagement.apm.xml` in the `%OvOWShareInstallDir%\instrumentation\Windows Server 2003\5.2\VP_SM` directory and add the following line under `<Application>`

```
<Template>OvisUpdateServices</Template>
```

The file should look similar to the following:

```
<?xml version="1.0"?>

<APMApplicationConfiguration xmlns="http://www.hp.com/OV/opcapm/
cluster">

     <Application>

           <Name>OvOWSelfManagement</Name>

           <Template>OvSvcDiscServerLog</Template>

           <Template>VP_SM-Server_EventLogEntries</Template>

           <Template>VP_SM-Server_SyncAgentServices</Template>

           <Template>VP_SM_OVOWServices</Template>

           <Template>VP_SM-WMI-Restart</Template>

           <Template>VP_SM_DeleteNodesFromReporterDB</Template>

           <Template>VP_SM-Cluster Consistency Check</Template>

           <Template>OvisUpdateServices</Template>

     </Application>

</APMApplicationConfiguration>
```

3 Redeploy the instrumentation (category VP_SM) to each cluster node.

4 Re-start the agents on each cluster node:

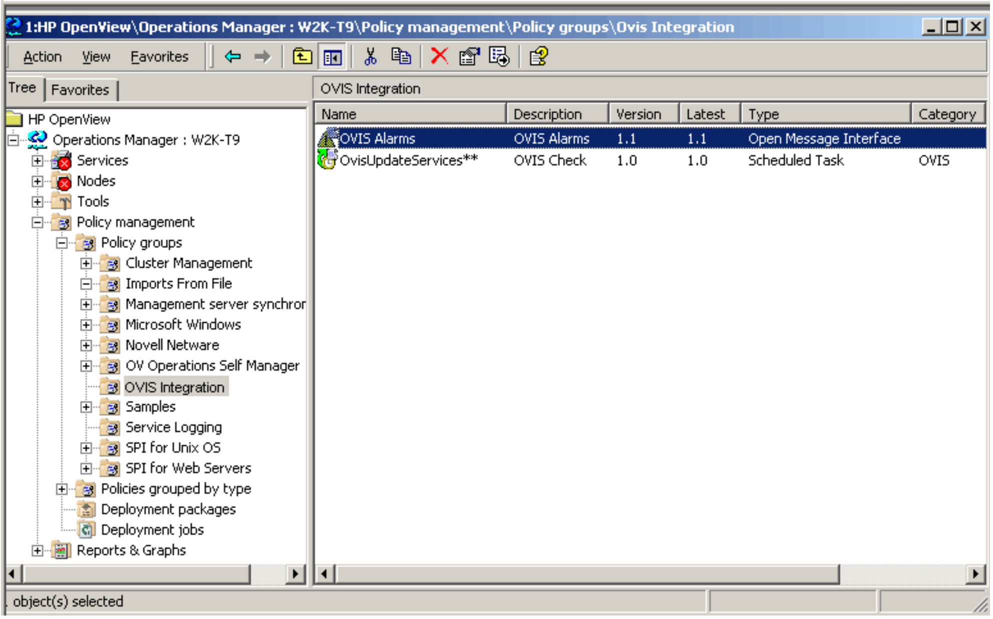
```
opcagt -kill
opcagt -start
```

Steps to Deploy OVIS Policies

Once the OVIS OVO for Windows Integration component has been installed you need to deploy two OVIS policies.

1 If you plan to choose **OVO Integration—Use Proxy** as the alarm-forwarding mode in OVIS, add all Internet Services service target systems to the Nodes folder in OVO for Windows.

2 The `OvisUpdateServices` Scheduled Task policy is located in the OVIS Integration policy group. Locate this folder in the left pane of the OVO for Windows Console by selecting **HP OpenView > Operations Manager > Policy Management > Policy Groups >OVIS Integration**. See the screen shot below.



1:HP OpenView\Operations Manager : W2K-T9\Policy management\Policy groups\Ovis Integration

OVIS Integration

Name	Description	Version	Latest	Type	Category
OVIS Alarms	OVIS Alarms	1.1	1.1	Open Message Interface	
OvisUpdateServices**	OVIS Check	1.0	1.0	Scheduled Task	OVIS

object(s) selected

3 In the right pane, select the `OvisUpdateServices` policy and right-click to select **All Tasks > Deploy on**.

4 In the Deploy Policies On dialog box, select the check box in the Nodes tree for the **OVO for Windows Management Server** (use the default for other check boxes) and click **OK** to deploy the policy.

5 The `OVIS Alarms` policy is an opcmsg Interface policy type which is located in the OVIS Integration policy group. This policy is also located in the same folder: **HP OpenView > Operations Manager > Policy Management > Policy Groups > OVIS Integration**.

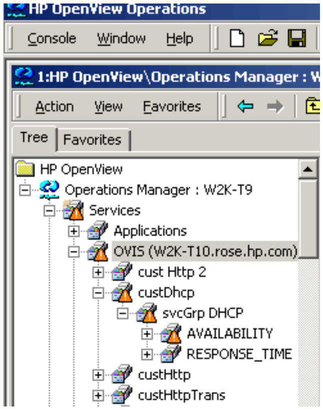
6 In the right pane, select the `OVIS Alarms` policy and right-click to select **All Tasks > Deploy on**.

7 In the Deploy Policies On dialog box, select the check box in the Nodes tree for the **OVIS Management Server** (use the default for other check boxes) and click **OK** to deploy the policy.

8 After a few minutes, you should see the OVIS services added to the OVO for Windows Services tree. You will see a hierarchy in the OVIS services:

OVIS Management Server Node
  Customer
    Service Group (click the + sign in the map to see the metrics)
      SLOs monitored for service targets in the service group

If Service Level Agreements are defined, they are at the Customer level.

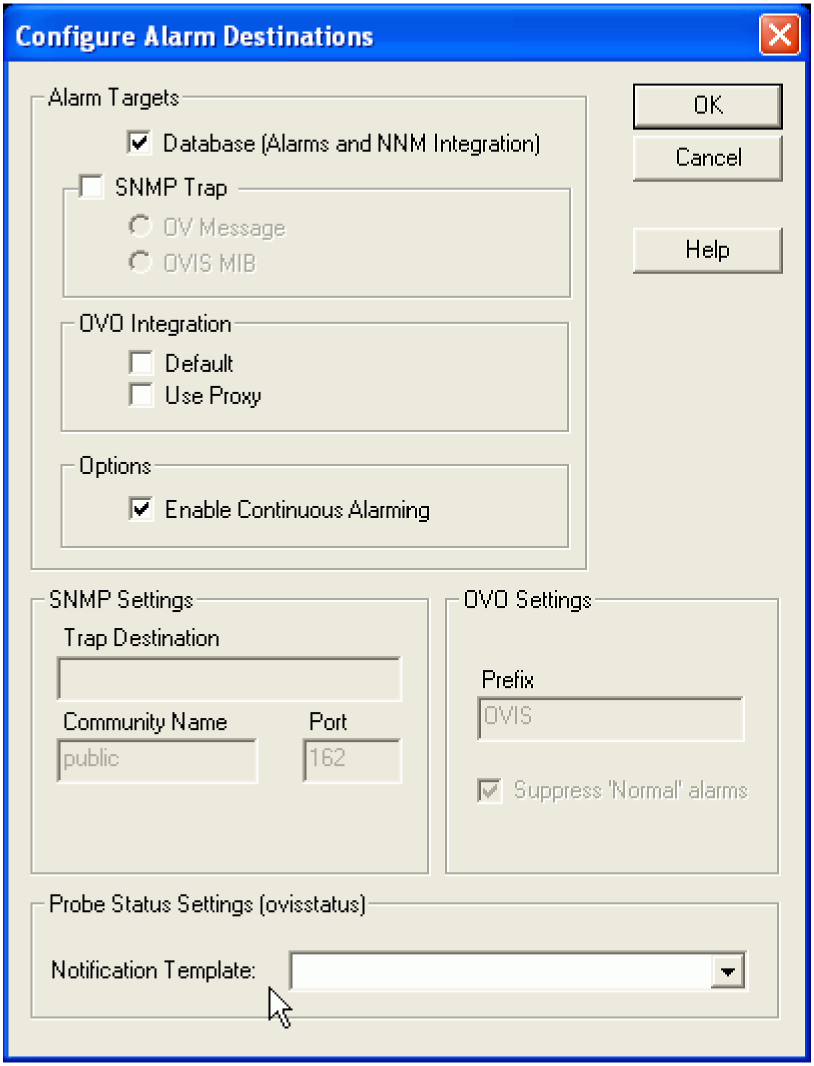


9 Configure OVIS Alarms to be sent to OVO for Windows, using the OVIS Configuration Manager **File > Configure > Alarm Destinations** dialog box, choose between two options for forwarding OVIS data to OVO for Windows. Be sure to **Save** the configuration after you set the alarm destination.

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 monitored Internet Services service target node. This configuration requires that you add the Internet Services Management Server and the Internet Services service targets system to the Node folder in OVO for Windows. You also need to deploy an OVO agent to the OVIS Management Server system (the OVO agent is not required on OVIS target systems).



Configure Alarm Destinations

Alarm Targets

☑ Database (Alarms and NNM Integration)

□ SNMP Trap

○ OV Message

○ OVIS MIB

OVO Integration

□ Default

□ Use Proxy

Options

☑ Enable Continuous Alarming

SNMP Settings

Trap Destination:

Community Name: public

Port: 162

OVO Settings

Prefix: OVIS

☑ Suppress 'Normal' alarms

Probe Status Settings (ovisstatus)

Notification Template:

The OVIS Alarms policy provides state based correlation of failure alarms (critical, minor, major, warning and normal alarms) in OVO for Windows.

In the Configure Alarm Destinations dialog box (shown above) you can check the **Enable Continuous Alarming** box and disable the **Suppress Normal Alarm** box. With these settings, when an alarm condition continues, an OVIS alarm is generated interval after interval until the condition returns to normal and an alarm state change to normal is sent. Then in OVO for Windows, the first alarm message is kept in the message browser and subsequent similar messages are correlated with the first message and cause the date on the message to be updated.

10 Alarm messages should now be forwarded to OVO for Windows. They will be displayed in the OVO for Windows Message Browser - Active Messages view. The status of sub-services with service alarms will also be propagated up the Service tree, so each item changes its color depending on the severity of the alarm.

➤ In addition, the program OVISStatus.exe runs automatically and sends alarms to OVO or NNM if data is not received from the probe system within the expected time + 10 percent, to allow for minor delays.

OVIS Message Forwarding to OVO

OVIS uses the following set of OVO attributes (opcmsg) when passing alarm messages.

```
opcmsg [-help] [-id] [severity=normal|warning|minor|major|critical]
          application=<application> object=<object> msg_text=<text>
          [msg_grp=<message group>] [node=<node>] [service_id=<svcid>]
         [-option <var>=<value>}
```

Table 5 opcmsg Attributes for Message Forwarding

OVO attribute (opcmsg)	OVIS value
object	target host:probe system:target info
msg_grp	OVIS_<probe name>
node	OVIS server FQDN (or if proxy was configured in the GUI, target node FQDN)
msg_txt	message text

Table 5 opcmsg Attributes for Message Forwarding

OVO attribute (opcmsg)	OVIS value
application	OVIS
severity	OVIS severity

option variables	host=<target host>
	ps=<probe system>
	target=<target info>
	vpis=<OVIS server FQDN>
	customer=<customer>
	customerURLE=<customer>
	serviceGroup=<service group>
	serviceGroupURLE=<service group>
	probeDesc=<probe desc>
	probeDescURLE=<probe desc>
	probeType=<probe name>
	probeTypeURLE=<probe name>
	metric=<metric>
	ipAddr=<ip addr of target if available>
	psts=<timestamp in UTC when measurement was taken>

To make sure that messages are forwarded as expected from the Internet Services Management Server, open a Command Prompt window on the OVIS server and enter the following command. You should see a corresponding message in the OVO message browser.

```
opcmsg a=OVIS o=OVIS_Test msg_text="Test"
```

Note that this is just a simple test and not all the necessary options are included, so that, for example, operator initiated actions aren't enabled.

Usage Tips

The following are some ways you can use the integration with OVIS from within the OVO for Windows Console.

- For each OVIS customer, service group and metric shown in the OVO for Windows service view map, you can right-click and select **All Tasks > Launch Tool**. This will launch the OVIS Dashboard in the context of the item selected. The Dashboard displays detailed performance data and graphs as well as reports of summarized performance data. The Dashboard context for each item you can select in the OVO for Windows service view is shown below:

OVIS server - Dashboard Health workspace Summary page for all customers.

Customer - Dashboard Health workspace Summary page for the customer.

Service Group - Dashboard Health workspace Summary page details for the service group.

Metric - Note that only those metrics that are configured as SLOs in OVIS are displayed. Dashboard Health workspace Summary page details for the service group.

SLA - Dashboard SLA workspace.

Alarms - Dashboard Health workspace Summary page details for the Service Group that generated the alarm, Normal alarms launch Dashboard Health workspace main page.

- For each OVIS alarm shown in the OVO for Windows Message Browser - Active Messages view, you can right-click and select **Commands > Start > Operator Initiated** to launch the OVIS Dashboard.
- If you get OVIS messages in the browser which are "unmatched" then this may be a sign that the message was generated by another opcmsg policy. Make sure that you have deployed the OVIS Alarms policy to the OVIS Management Server. Then check that other opcmsg policies deployed to the OVIS Management Server don’t create unmatched messages but suppress OVIS messages. If an opcmsg policy is creating a problem you may need to uninstall it from the OVIS Management Server.
- The OVIS integration creates a number of tools which are used to launch the OVIS Dashboard from within OVO for Windows. These tools are located in the folder **HP OpenView > Operations Manager > Tools > OVIS Tools**.
- The OVIS server hostname is input during the installation of the integration component. If you want to change this after installation it is read from the file `%OVINSTALLDIR%\bin\OvIS\oviscnfg.ini` on the OVO server. You can change this file as follows:

```
[CONFIG]
ovishost=your.ovis.host.fqdn.com
```

```
trace=False
```

The trace flag turns on log file tracing. The log file `OvisUpdateServices.log` is located in the `%OVINSTALLDIR%\Data\log` directory on the OVO system.

- Changes (including adding or removing customers, service groups or SLOs) you make and save in the OVIS Configuration Manager are automatically reflected in the OVO Services tree after a timing delay of about five minutes.
- The utility `forceupdate.cmd` is provided in the integration component you install. You can run this utility, from a command prompt, to manually force the OVIS update in the OVO Services tree. Use the `-t` option with this utility to turn on tracing and write to the `OvisUpdateServices.log` trace file. The `-t` option is similar to the `trace=` option described above. Use the `-r` option with this utility to force the manual removal of OVIS from the Services tree. You would only use `-r` when you want to get rid of OVIS in the tree. The tree will be repopulated at the next scheduled update or you can run `forceupdate`.

6

Troubleshooting Information

This chapter gives you basic troubleshooting information including the following:

- Troubleshooting Probe Status
- Troubleshooting the Dashboard
- Troubleshooting Custom Graphs and Restricted Views
- Troubleshooting Installation
- TIPs Troubleshooting
- OVIS Tracing and Logging Files
- Error Messages and Status Codes
- Troubleshooting Alarms
- Troubleshooting by Probe
- Troubleshooting the OVIS to OVTA Integration
- Multiple Users in the Configuration Manager
- Probe Scheduling Considerations
- Troubleshooting Tools

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

Troubleshooting Probe Status

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.

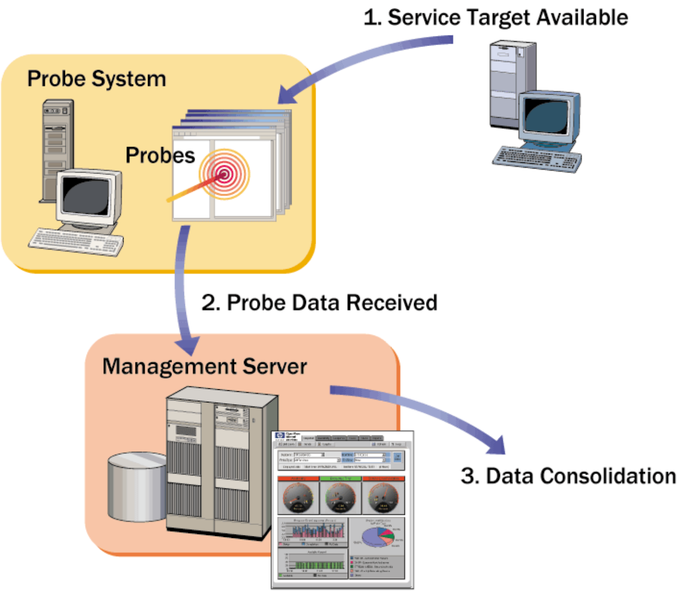
If you are not receiving data regarding a service target you have configured, any one of three areas or the connections between these areas could be the cause.

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. See Target Status Unavailable on page 359.
- **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 there is a name resolution problem, or a problem in the communication between the probe and the OVIS management server. See No Probe Information on page 360.

Target Status Unavailable

When a target is unavailable, there are a number of possible causes, as shown below. Also see Troubleshooting by Probe on page 420.

- **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 362
- **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 362

- **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 363
- **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 either a name resolution problem or a problem in the communication between the probe and the OVIS management server. Here are some possible causes and actions to take:

- **The OVIS Management Server has a name resolution problem and creates a config.dat file that points back to itself with an invalid name.** If this happens, the probe systems pick up the config.dat file and can not send data back to the Management Server, resulting in a No Probe Info condition on the server.

  One resolution is to correct the name in the config.dat file and manually distribute this to the probe systems.
- **The probe system cannot properly resolve the OVIS Management Server name in the config.dat file even though it is correct.** If this is the case, data will not get to the Management Server unless the name resolution problem is corrected. In both of the above cases the number of queue files on the probe system will increase as measurement data is stored, waiting to be sent to the Management Server.
- **The Web Server on the OVIS system is not running and operational:** See Possible Cause: Local Web server connection failed on page 361.

- **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 457 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 `<datadir>\datafiles\probe\queue` directory, 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 `<datdir>\datafiles\probe\queue` directory, this means that the probe service (HP Internet Services) is probably running fine, but there is a name resolution problem or the OVIS management server is not accepting the measurement data. First check that the host name in the `config.dat` file can be properly resolved from the probe system. If that checks out, then, 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 360 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 360 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.

Troubleshooting the Dashboard

Problem: Out of Memory Errors or Dashboard aborts.

Resolution: If the application server running the OVIS Dashboard (Tomcat server) is hit repeatedly with unique requests, such as those from the HTTP_TRANS probe (IE mode), it may run out of memory and either abort or return out of memory errors to browsers. Each unique session has resources associated with it and Tomcat will hold these resources open for up to two hours after the last request has been made, even if it has already expired the session.

If your OVIS Dashboard servlet is having this problem during normal use, the memory can be increased by entering the following at the command line:

```
<install dir>\nonOV\tomcat\a\bin>tomcat5w //ES//OvTomcata
```

Select the Java tab and then you can increase the “Initial Memory Pool” and the “Maximum memory pool” fields to 256MB each or values that suit your specific needs.

Problem: You do not see alarms, as expected, in the Dashboard.

Resolution: Check the following: in order for alarms to be displayed in the dashboard, the Configuration Manager **File > Configure > Alarm Destinations**, **Database (Alarms and NNM Integration)** checkbox must be checked.

Problem: You get an error “The Page Can Not Be Displayed”.

Resolution: Check that the Tomcat service is started. Bring up the Services dialog from the control panel and search for “HP OpenView Tomcat(A) Servlet Container Service” and start it if it is stopped.

Problem: You get an error “This graph cannot be displayed for this metric”.

Explanation: In the Baseline and Hourly Statistics graphs in the Trends tab of the Dashboard Health workspace, certain metrics like Availability and SLO Violations will show the message “This graph cannot be displayed for this metric”. This is because the value for these metrics is always a zero or a one, so there is not enough variability in the data to calculate the percentiles.

Problem: You see “Unknown Target Name”.

Explanation: If you see an item in the Dashboard’s Resources navigation tree or Target Status page that says “Unknown Target Name”, this means that there is no collected data in the database for this target. If there is a host name configured for this target, the host name will be displayed to help you identify the target. If there are multiple targets in a single service group that do not have data, you will see a sequential index after the name to uniquely identify the target.

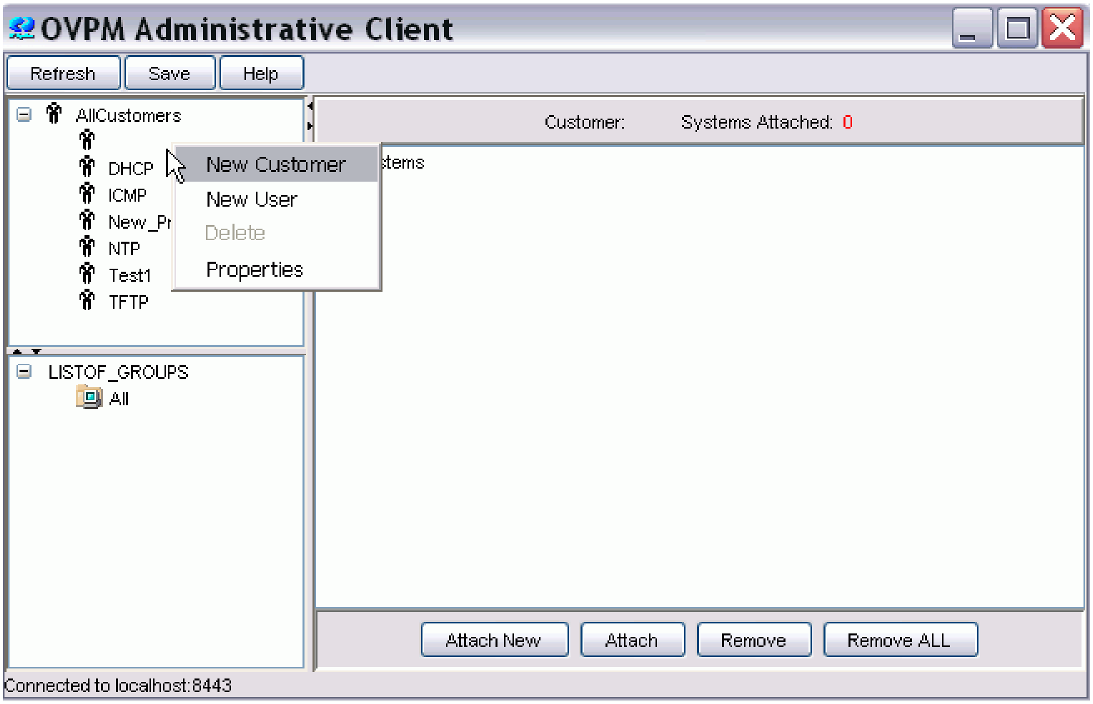
Troubleshooting Custom Graphs and Restricted Views

If you have OVIS and OpenView Performance Manager 5.0 (OVPM) installed on the same system and you have restricted view turned on, you will need to sync up the passwords in order for the Custom Graphs display in the OVIS Dashboard to work properly. You may see the following error in the OVIS Dashboard Custom Graphs window:

```
Invalid password supplied for the admin customer (err18)
No data source was specified. Please select a system or other data
source (err203)
```

After you've set up restricted views (or profiles) in OVIS, then you will need to use the OVPM Administrator GUI to sync up the passwords.

Select **Start > Programs > HP OpenView > Performance Manager > Performance Manager Administration**. See the screen below.



To sync passwords you will need to add the OVIS customers (and passwords) set up for restricted views to OVPM using the OVPM Administration program. Right-click in the Customer list box and select New Customer. Enter Customer and password (same as in OVIS) and then select the **Save** button.

Then you can log into the OVIS Dashboard with this customer/password and will be able to draw custom graphs for the selected customer.

If you’ve set up profiles in OVIS, you add the profiles as described above in OVPM and enter profile in the customer name and add the password for the profile. The in the Dashboard custom graphs you will be able to draw graphs for any customer under that profile.

To sync up the OVIS All Customers login, use the OVPM Administration program and select the blank customer in the Customer list box. Right-click and select Properties. Set the password (same as All Customers in OVIS). Then you can log into the OVIS Dashboard with All Customers and will be able to draw custom graphs for all customers.

Note that if you make changes to OVIS restricted views (customer/password or profiles) you will need to go back and change it in OVPM.

Troubleshooting Installation

The following provides some troubleshooting help for installation problems.

Problem: Install Error 1923

Resolution: This may be caused by an open Services applet. Close the Services applet to resolve the error.

TIPs Troubleshooting

Troubleshooting information for the TIPs component is found in the TIPs Configuration program online help.

The following TIPs troubleshooting sections are included here for your convenience:

- Check TIPs Log Files
- TIPs Viewer Troubleshooting

Check TIPs Log Files

A variety of log files provide useful information for troubleshooting TIPs. Log files are generated on the OVIS management server system and on the systems where TIPs Runners are installed. See OVIS Tracing and Logging Files on page 376 for information on OVIS log files.

The location for the TIPs log files is:

- Windows: `<data_dir>\log\*`
- UNIX: `/var/opt/OV/log/*`

For log files ending with `"_0_<0-9>.log"`, if two processes attempt to log a message into a log file with the same name at the same time, one process writes to `FileName_0_<0-9>.log`, and the other writes to `FileName_1_<0-9>.log`. When a log file reaches maximum size, the number, `<0-9>`, is increased.

Table 6 TIPs Log Files :

Log File	Contents	Location
OvTIPsConfig_0_<0-9>.log	TIPs Configuration program log information.	Server System
OvTIPsCreateDB_0_<0-9>.log	TIPs database creation script log information. The creation script is called as part of installation.	Server System
OvTIPsDataExchange_0_<0-9>.log	TIPs import and export batch scripts log information. The import is called as part of the installation. The export is called as part of the uninstall. NOTE: Import and export actions from the TIPs Configuration program are logged in the TIPs Configuration program log file.	Server System
OvTIPsRunner.log.txt	TIPs Runner log information.	Server System and Remote TIPs Runner Systems
OvTIPsServer_0_<0-9>.log	TIPs Server log information and Triggered by Alarm cleanup log information.	Server System

TIPs Viewer Troubleshooting

This section gives you some basic troubleshooting information for errors you may encounter when you run TIPs.

TIPs Command Timing Issues

When you see an error message in the Dashboard TIPs Viewer stating that a command did not run in the time specified, try the following actions:

- In the TIPs Viewer, click the **Re-Run** button for that TIP. The command timeout may be due to heavy system activity when multiple TIPs run simultaneously. Running a TIP individually often solves the problem.
- Check the TIPs Server log file for errors relating to command execution not succeeding. See Check TIPs Log Files on page 369 and “Fixing Command Timing Issues” below for more information.
- Restart the TIPs Runner. The TIPs Runner should have a status of running. Even if it has a status of running, it may need to be restarted. To cover the case where it may be stopped or where it may need a restart, just use the restart command as described below.

To restart the TIPs Runner, complete the following steps:

1. Go to the system where the TIPs Runner is installed.
2. Restart the TIPs Runner by executing this command in a command window:

   on Windows: `<install dir>\bin\ovc -restart ovtiprn`

   on UNIX: `/opt/OV/bin/ovc -restart ovtiprn`

Fixing Command Timing Issues

There are times when a TIPs command takes longer to execute than is expected. In this case, there are two messages in the TIPs Server log file:

```
Command <command name> with ID <identifier> did not complete
within <number> milliseconds.
```

```
Command <command name> with ID <identifier> that resulted in a
command time out message (received after <number> milliseconds),
has now completed (received after <number> milliseconds).
```

The second message may not immediately follow the first message. Match the <*command name*> and <*identifier*> to determine if the messages you find refer to the same command.

For this situation, click the **Re-Run** button in the Dashboard TIPs Viewer for the TIP that has a timed out command. Running only one TIP means a smaller set of commands will be processed, and they are less likely to timeout.

If a command consistently times out, you can change the command's timeout value. See the TIPs Configuration program online help for more information on configuring Commands.

Clicking the Stop Button in the TIPs Viewer Browser

If you click the browser's **Stop** button while the Dashboard TIPs Viewer waits for TIPs execution results, the progress indicator continues to display, but the TIPs results will not be displayed.

When this occurs, the TIPs Server log file contains an error stating that the TIPs results cannot display due to a client abort exception.

To recover from this action, close the TIPs Viewer window and launch it again.

HTTP_TRANS Probe Configuration for TIPs

Problem: You have executed the Monitored Service Status TIP for an HTTP_TRANS probe and see the error listed below in the TIPs Viewer:

```
Specified directory does not exist
```

Resolution: You need to be sure the **Capture Window on Error** option is checked in the Web Transaction Recorder **File > Configure > Properties** dialog box. The HTTP_TRANS probe does not produce an error log or error screen image that the TIP is trying to retrieve, until this option is checked.

Problem: You have executed the Probe Re-Execution TIP for an HTTP_TRANS probe and see the error listed below in the TIPs Viewer:

```
No results returned for command
```

Resolution: You'll see this message when running the HTTP_TRANS IE mode remote probe on Windows 2000 because this probe does not produce any output on Windows 2000 systems. Running the HTTP_TRANS IE mode probe (probehttptrans2) with the -print option will not produce results on Windows 2000 because that platform does not support the ability to write to a console from a Windows GUI application.

TIPs Authentication Issues

Problem: You have added one of the HP supplied Expect or WMIC Commands to a new or existing TIP. When the TIP runs, you see one of the errors listed below in the TIPs Viewer.

```
Error: User authorization is not configured for system
myserver.hp.com
```

```
Node - myserver.hp.com ERROR: Code = 0x80041003 Description
= Access denied Facility = WMI
```

Probable Solution: Add an entry to the TIPs Authentication Data Manager for the system (in the example message above it is myserver.hp.com). See the TIPs Configuration program's online help for more information on adding authentication records.

Problem: You have added one of the HP supplied WMIC Commands to a new or existing TIP as well as added the /user and /password options to the command for user access. When the TIP runs, you see the error listed below in the TIPs Viewer.

```
Invalid UserID.
```

Probable Solution: Add an entry to the TIPs Authentication Data Manager for the Windows TIPs Runner machine. See the TIPs Configuration program's online help for more information on adding authentication records.

Target System's Operating System Issues

Problem: You have added one of the HP supplied WMIC Commands to a new or existing TIP. When the TIP runs from a Windows TIPs Runner machine to a Unix remote target machine, you see one of the errors listed below in the TIPs Viewer.

```
Node - myunixserver.hp.com ERROR: Code = 0x800706ba
Description = The RPC server is unavailable. Facility =
Win32
```

```
WARNING: Could not obtain host information from machine:
[myunixserver.hp.com]. Some commands may not be
available.The RPC server is unavailable.The network path was
not found.
```

Probable Solution: The operating system categories for the TIPs Runner and remote target machines are mixed. See the TIPs Configuration program's online help on target system's operating system considerations for more information.

Problem: You have added one of the HP supplied Expect Commands to a new or existing TIP. When the TIP runs from a Unix TIPs Runner machine to a Windows remote target machine, you see the errors listed below in the TIPs Viewer.

```
Error: Cannot connect to system mywindowsserver.hp.com
```

Probable Solution: The operating system categories for the TIPs Runner and remote target machines are mixed. See the TIPs Configuration program's online help on target system's operating system considerations for more information.

TIPs Runner Routing

Problem: You have added the HP supplied Target TCP Connections Command to a new or existing TIP. When the TIP runs from a Windows TIPs Runner machine to a Windows remote target machine, you see the error listed below in the TIPs Viewer

```
The Routing and Remote Access Service is not currently
running on mywindowsserver.hp.com. Please use 'net start
remoteaccess' on the machine to start the service.
```

Probable Solution: Enable and start the routing service for the TIPs Runner machine. See the TIPs Configuration program's online help on routing command requirement on Windows Systems for more information.

WMIC TIPs Commands

Problem: You have added one of the HP supplied WMIC Commands to a new or existing TIP as well as added the /user and /password options to the command for user access. When the TIP runs, you see the error listed below in the TIPs Viewer.

```
Node - mymgmtserver.hp.com ERROR: Code = 0x80041064
Description = User credentials cannot be used for local
connections Facility = WMI
```

Probable Solution: The /user and /password WMIC options are not required for execution of this command on the local TIPs Runner machine. See the TIPs Configuration program’s online help on WMIC command considerations for more information.

Problem: You have added one of the HP supplied WMIC Commands to a new or existing TIP. When the TIP runs, you see the error listed below in the TIPs Viewer.

```
Node - myserver.hp.com ERROR: Code = 0x800706ba Description
= The RPC server is unavailable. Facility = Win32. Please
wait while WMIC is being installed.
```

Probable Solution: WMIC is not enabled on the TIPs Runner machine. WMIC is enabled when the first WMIC command executes. In this case, the TIP Command caused WMIC to be enabled so no other action is necessary.

OVIS Tracing and Logging Files

OVIS provides tracing and logging files for use in troubleshooting. 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 in these files.

See Check TIPs Log Files on page 369 for information on TIPs status and log files.

There are two types of OVIS trace files:

- Probe error and trace files
- OVIS Management Server status and trace files

The probe error and trace files are found in the following locations:

Table 7 Probe Error and Trace Files

Type	Location	Comment
Error/Status Information	`<datadir>/log/probe/error.log`	Probe and Scheduler errors.
Trace/DebugInformation	`<datadir>/log/probe/trace.log`	Probe and Scheduler trace messages.
	HP OpenView Tracing (for more information see below)	Trace messages of the receptor for the UDP_PERF and TCP_PERF probes are logged to the HP OpenView tracing component. TIPs trace messages are logged to the HP OpenView tracing component.

Management Server status and trace information is found in the following locations:

Table 8 Management Server Status and Trace Files

Type	Location	Comment

Error/Status Information	`<install dir>\data\`
	`status.iops`
	`status.reporter`
	`status.PM`
		OVIS status & errors
		Reporter status & errors
		OVPM status & errors

	HP OpenView Tracing (for more information see below)	OVIS and Reporter status/ error messages are logged to the HP OpenView tracing component in addition to the above log files.
Trace/Debug Information	`<install dir>\data\ trace.<program name>`	Component specific trace information (e.g. trace.measEvent2), except Dashboard and TIPs.
	HP OpenView Tracing (for more information see below)	OVIS and Reporter trace/ debug information is logged to the HP OpenView tracing component in addition to the above log files. TIPs trace messages are logged to the HP OpenView tracing component.
	`<install dir>\nonOV\tomcat\a\logs`	Tomcat related log file (e.g., startup issues, exceptions etc.).
	`<install dir>\data\log\OvisDashboard*`	OVIS Dashboard related log and trace files.
	`<install dir>\data\log\OvTIPs*`	TIPs related log and trace files.
	`<install dir>\data\log\System.txt`	Overall OpenView error messages for install.

Using the HP Openview Tracing Component

The HP OpenView Tracing component provides a consistent trace view across all OpenView products. For more information please refer to the "HP OpenView Tracing - Concepts and User's Guide" on the Management Server in:

```
<InstallDir>\help\iops\c\ov_tracing.pdf
```

The OpenView Tracing tools are located under `<InstallDir>\support`.

To use the OpenView Tracing component, you must first enable the trace GUI to access the system (Unix or Windows). Use `ovtrcadm -a <hostname>`, where <*hostname*> is the name of the system that is going to view the traces. Execute the `ovtrcadm` command on the system that should be traced. Note, even if you are using the local system for tracing and viewing, you need to issue `ovtrcadm -a localhost`.

To view the traces, use the `ovtrcgui` application on Windows and follow the instructions in the Wizard.

Description of Status Files

The OVIS Management Server trace files are named **trace.<programname>**. For example, the trace file for the OVIS module which receives the probe data via the web server is 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.

A brief description of some of the OVIS status files is shown below:

Status File	Description
status.iops	Main status
status.PM	Graphing component custom graphs status
status.Reporter	Reporting component status

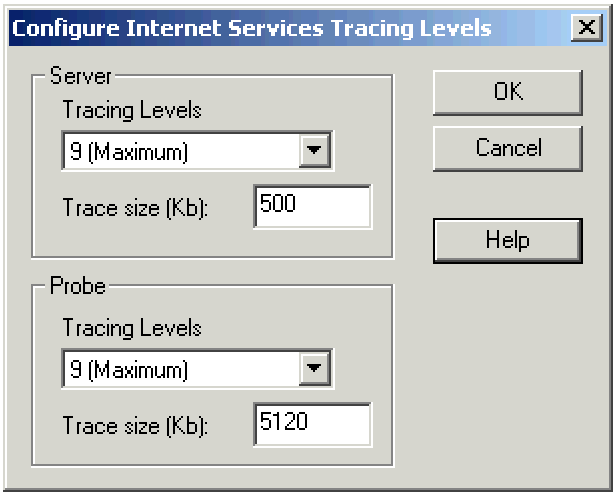
Status File	Description
trace.measEvent2	trace for measEvent2.dll - measEvent2.dll generates alarms via the alarm engine, receives measurements (via queue files) and writes the data to IopsTraceTable
trace.DllVersion	trace for Reporter dlls
trace.iopscollector	trace for iopscollector - iopscollector moves data from IopsTraceTable to the Reporter database
trace.IOpsConfig	trace for the Configuration Manager
trace.iopsmaint	trace for the data maintenance - iopsmaint summarizes the data in hourly and daily weighted averages
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 - RepMaint nightly removes data from the Reporter database if it is older than what is defined for retain days
trace.ExportIOps	trace for the ExportIOps program - ExportIOps moves configuration information from the Reporter database to the config.dat files
trace.IOPSSQLUtils	contains the SQL commands executed by the renamedata utility.

Status File	Description
trace.IOpsLoad	trace for the IOpsLoad program - IOpsLoad moves configuration information to and from Reporter database and config.xml
trace.Scheduler	trace for the Scheduler program - Scheduler provides information for running all these programs
trace.webrecorder	trace for the Web Transaction Recorder

See Error Messages and Status Codes on page 387 for a description of each IOPS error message and see HTTP Status Codes on page 403 and SSL Error Codes on page 405 for descriptions of individual status or error codes that may be contained within the IOPS error message.

How to Get Debug Trace Output for a Specific Probe

The best approach for gathering debug trace output for a specific probe is to turn on tracing using the Internet Services Configuration Manager, under **File > Configure > Tracing**.



Configure Internet Services Tracing Levels

Server

Tracing Levels: 9 (Maximum)

Trace size (Kb): 500

Probe

Tracing Levels: 9 (Maximum)

Trace size (Kb): 5120

To do probe troubleshooting set tracing to 9, save the configuration, the modified configuration files (the [TRACE] option is added to the `config.dat` file) 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.

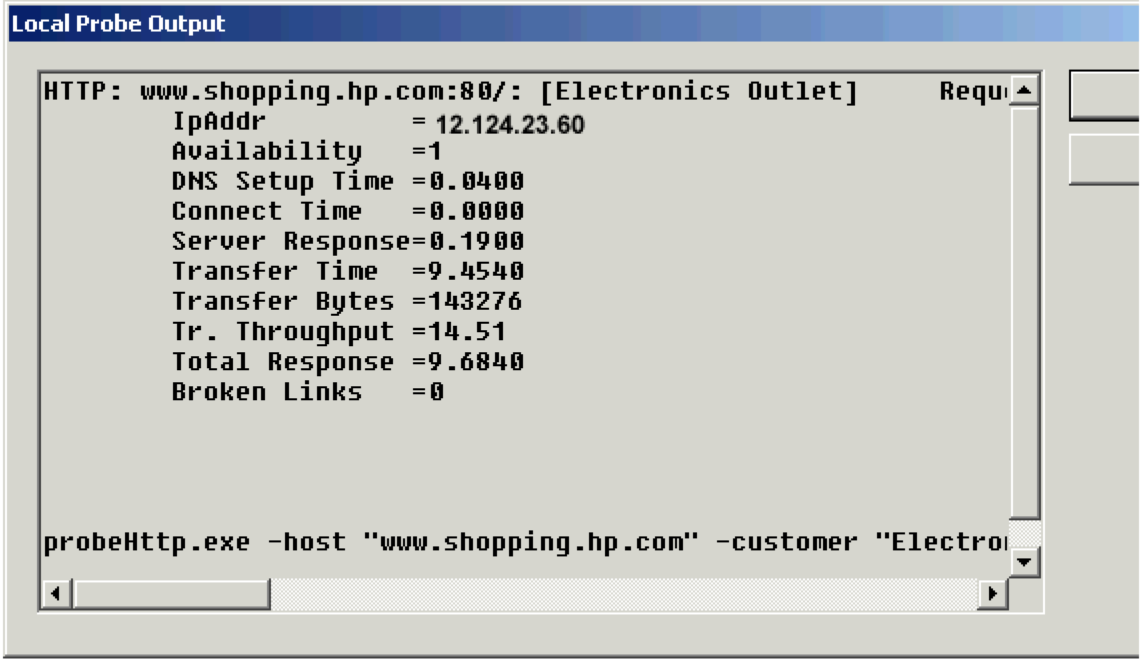
In the resulting probe trace files (`trace.log` and `error.log` in the directory `<datadir>\log\probe` search for ERROR or WARNING statements and examine the text following these for help in resolving the error. See Error Messages and Status Codes on page 387.

If you want to get debug trace output for a particular probe, you can run the probe executable from the command prompt and look at the trace file for just that probe executing. An example of how to do this on a Windows system is shown below.

1 First find the actual command for the probe to execute.

   In the Configuration Manager, right-click on the service target of the probe you want to debug and select **Test on Management Server**.

In the Local Probe Output dialog, copy the probe command line at the bottom of the dialog box (you may have to scroll down to see the command line).



```
HTTP: www.shopping.hp.com:80/: [Electronics Outlet]     Requ
        IpAddr          = 12.124.23.60
        Availability    =1
        DNS Setup Time  =0.0400
        Connect Time    =0.0000
        Server Response=0.1900
        Transfer Time   =9.4540
        Transfer Bytes  =143276
        Tr. Throughput  =14.51
        Total Response  =9.6840
        Broken Links    =0



probeHttp.exe -host "www.shopping.hp.com" -customer "Electro
```

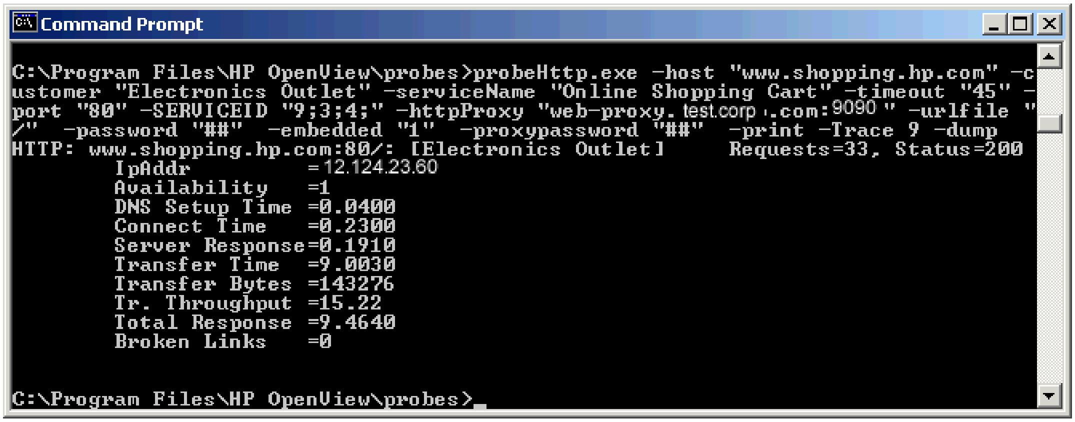
2 Then, on the probe system, stop the HP Internet Services service (net stop “HP Internet Services” or use the control panel to stop the service.

3 Rename any existing `error.log` and `trace.log` files, so the command line execution will create a new set.

4 Then open a command prompt window and go to the `<install dir>\bin` directory.

5 Paste in the command line you copied from the Local Probe Output dialog box. Before you press **Return**, be sure to add in the **-print** and **-dump** options

.



```
C:\Program Files\HP OpenView\probes>probeHttp.exe -host "www.shopping.hp.com" -c
ustomer "Electronics Outlet" -serviceName "Online Shopping Cart" -timeout "45" -
port "80" -SERVICEID "9;3;4;" -httpProxy "web-proxy. test.corp .com:9090 " -urlfile "
/"  -password "##"  -embedded "1"  -proxypassword "##"  -print -Trace 9 -dump
HTTP: www.shopping.hp.com:80/: [Electronics Outlet]     Requests=33, Status=200
        IpAddr          =12.124.23.60
        Availability    =1
        DNS Setup Time =0.0400
        Connect Time    =0.2300
        Server Response=0.1910
        Transfer Time   =9.0030
        Transfer Bytes =143276
        Tr. Throughput =15.22
        Total Response =9.4640
        Broken Links    =0

C:\Program Files\HP OpenView\probes>_
```

6 The resulting files can be used in debugging:

— `<datadir>\datafiles\probe\policies\config.dat`

— `<datadir>\tmp\probe\<dump file>`
The dump file which will be in the format targetname.x.servicetype. An example file for HTTP would be `www.shopping.hp.com.0.HTTP`. This file contains the protocol dump.

From the `<datadir>\log\probe\` directory

— `error.log`

— `trace.log`

7 You should copy these files to another location before restarting HP Internet Services service, so that the `error.log` and `trace.log` files contain only the desired command line test.

An example of these debug output files for a simple HTTP probe is shown below.

The command line execution for the probe from the command prompt:

```
probeHttp.exe -host "shopping.hp.com" -customer "HTTP_Test" -serviceName
"Test_HTTP" -timeout "45" -port "80" -SERVICEID "35;49;30;" -httpProxy
"web-proxy.test.corp.hp.com:9090" -httpsProxy
"web-proxy.test.corp.hp.com:9090" -urlfile "/"  -password "##" -embedded "1"
-proxypassword "##"
-print -dump -trace 9
```

```
HTTP: shopping.hp.com:80/: [HTTP_Test]       Requests=6, Status=200
        IpAddr          =12.124.23.60
        Availability    =1
        DNS Setup Time =0.0160
        Connect Time    =0.0310
        Server Response=0.1410
        Transfer Time  =0.4060
        Transfer Bytes =79788
        Tr. Throughput =142.45
        Total Response =0.5940
        Broken Links    =0
```

The dump file output :

(For example the file name would be `<targetname>.x.<servicetype>` or www.shopping.hp.com.0.HTTP).

```
filename (depends on the configuration):
GET http://shopping.hp.com/ HTTP/1.0
Host: shopping.hp.com
User-Agent: Mozilla/4.0 (WinNT; I; OVIS)
Accept: */*

HTTP/1.0 200 OK
Connection: close
Date: Wed, 22 Oct 2003 16:22:37 GMT
Server: HP-UX_Apache-based_Web_Server/2.0.47 (Unix) DAV/2 mod_ssl/2.0.47
OpenSSL/0.9.6i
Last-Modified: Sun, 25 Aug 2002 22:12:19 GMT
ETag: "306b-aa-907fd6c0"
Accept-Ranges: bytes
Content-Length: 170
Vary: Accept-Encoding,User-Agent
Content-Type: text/html; charset=ISO-8859-1

<html>
<head>
<meta http-equiv="refresh" content="0;URL=http://www.shopping.hp.com/cgi-bin/
hpdirect/shopping/scripts/home/start_home.jsp">
…
GET http://www.shopping.hp.com/cgi-bin/hpdirect/shopping/scripts/home/
start_home.jsp HTTP/1.0
Host: www.shopping.hp.com
User-Agent: Mozilla/4.0 (WinNT; I; OVIS)
Accept: */*
```

```
HTTP/1.0 200 OK
Connection: close
Date: Wed, 22 Oct 2003 16:22:37 GMT
Server: HP-UX_Apache-based_Web_Server/2.0.47 (Unix) DAV/2 mod_ssl/2.0.47
OpenSSL/0.9.6i
Set-Cookie:
hpshopping=1&session_info=%25VM)PXsPg.YT$$$i%5bk$DDHgXmASXJ%25VMlgNNsLP.YTmmm
mGqqRWW%3eW%3cRaAGww%3eWb%3cR%3cmmmmu%2bDD$iPX$ix%2bkiHHkiXiaGtDR&cart_id=102
463255&user_type=0&bivisitor=0&cart_empty=1&time=1066839757940;expires=Monday
, 30-Dec-06 22:00:00 GMT;path=/
P3P: CP="CAO DSP COR CURa ADMa DEVa TAIa PSAa PSDa CONi OUR DELa BUS PHY ONL
UNI PUR COM NAV INT STA"
Vary: Accept-Encoding,User-Agent
Content-Type: text/html; charset=ISO-8859-1

<script language="JavaScript">
```

The resulting trace (probe runs on a Windows host) file with annotation shown in bold as ^^^:

```
Trace init - HTTP or HTTPS Probe
Probe Type was not a parameter or the value was empty, using HTTP value by
default
HTTP: retry=0 of 0, max timeout=45, run timeout=45, wait time=0
^^^ Shows retry/wait time information. Here, no retry was specified.
TCP: Scheduling: 'shopping.hp.com'
Connecting: (web-proxy) 12.124.23.60 @ 9090
^^^ Before socket connect() call. This line shows the hostname, the IP-address
and port that is used in connect()
HandleProtocol(shopping.hp.com): state=0
^^^ State of state machine (state 0 is after connect() succeeded)
Request: url='http://shopping.hp.com/'
Request: 'GET http://shopping.hp.com/ HTTP/1.0
Host: shopping.hp.com
User-Agent: Mozilla/4.0 (WinNT; I; OVIS)
Accept: */*'
^^^ HTTP Request that is about to be sent over the connection
Send[shopping.hp.com]: sb=204 (cnt=204)
Send[shopping.hp.com]: done
^^^ Send was successful, 204 bytes sent
Receive[shopping.hp.com]: num_recv=1 br=528
^^^ First data block from the server (recv() returned 528 bytes)
HTML: Meta refresh timer=0
^^^ Each packet is forwarded to the HTML parser. Here it detected a <META
refresh attribute>.
Receive[shopping.hp.com]: num_recv=2 br=0
^^^ Trying to recv() next block indicates that connection was closed by the
server (br = 0)
```

```
Close
^^^ Close our side of the connection (socket close)
Receive[shopping.hp.com]: connection closed
^^^ The header also indicated a "connection: close"
received: 200 (bytes=528)
^^^ The probe received a total of 528 bytes and the status of the reply was
200
Cookies received :
^^^ No cookies were part of the reply
Close
Close
Connecting: (web-proxy) 12.124.23.60 @ 9090
HandleProtocol(www.shopping.hp.com): state=0
Request: url='http://www.shopping.hp.com/cgi-bin/hpdirect/shopping/scripts/
home/start_home.jsp'
^^^ Redirect (from <META refresh> tag)
Request: 'GET http://www.shopping.hp.com/cgi-bin/hpdirect/shopping/scripts/
home/start_home.jsp HTTP/1.0
Host: www.shopping.hp.com
User-Agent: Mozilla/4.0 (WinNT; I; OVIS)
Accept: */*'
Send[www.shopping.hp.com]: sb=343 (cnt=343)
Send[www.shopping.hp.com]: done
Receive[www.shopping.hp.com]: num_recv=1 br=1072
Receive[www.shopping.hp.com]: num_recv=2 br=1072
Receive[www.shopping.hp.com]: num_recv=3 br=1460
...
Receive[www.shopping.hp.com]: num_recv=36 br=0
^^^ 36 receives; server closed the connection
Close
Receive[www.shopping.hp.com]: connection closed
received: 200 (bytes=72452)
Cookies received : Set-Cookie:
hpshopping=1&session_info=%25VM)PXsPg.YT$$$i%5bk$DDHgXmASXJ%25VMlgNNsLP.YTmmm
mGqqRWW%3eW%3cRaAGww%3eWb%3cR%3cmmmmu%2bDD$iPX$ix%2bkiHHkiXiaGtDR&cart_id=102
463255&user_type=0&bivisitor=0&cart_empty=1&time=1066839757940;expires=Monday
, 30-Dec-06 22:00:00 GMT;path=/
^^^ Server returned some persistent cookies (expires=Monday,30-Dec-06
22:00:00 GMT)
Close
Connecting: (web-proxy) 12.124.23.60 @ 9090
HandleProtocol(hpshopping.speedera.net): state=0
Request: url='http://hpshopping.speedera.net/www.shopping.hp.com/shopping/
images/icons/icon_mpss_23x23.gif'
Request: 'GET http://hpshopping.speedera.net/www.shopping.hp.com/shopping/
images/icons/icon_mpss_23x23.gif HTTP/1.0
Host: hpshopping.speedera.net
User-Agent: Mozilla/4.0 (WinNT; I; OVIS)
Accept: */*'
```

Error Messages and Status Codes

IOPS error messages are logged to the `error.log` files regardless of the trace level you have set.

Note that some of the IOPS error messages reference individual HTTP status codes or SSL error codes. A table of HTTP status codes and a table of SSL error codes is provided following the IOPS ERROR message tables.

Two tables of IOPS error message are shown below. The first table shows IOPS error messages for the HTTP_TRANS probe. The second table shows IOPS error messages for all other probes.

An example of a portion of the `error.log` file for the HTTP_TRANS probe IE Mode is shown below:

```
2004-02-03 08:05:14 ERROR probeHttpTrans2(3296)
[CIETransController.cpp:626]: IOPS 0-20018: Pattern not found in
step #0 for 'ie2/ie2 SG' (Status=0x800c0005(The server or proxy was
not found)).
```

Table 9 IOPS Error Messages for HTTP_TRANS Probe IE Mode

IOPS 0-x Errors	Description
IOPS 0-20001	Unable to load transaction file.
IOPS 0-20002	Customer/Service Name '<customer>/<service group>' not found in <transaction file>.
IOPS 0-20003	Unable to save transactions to '<file>'.
IOPS 0-20004	Unable to load transaction from '<file>'.
IOPS 0-20005	Unable to set timer for replay.
IOPS 0-20008	No transaction recorded or loaded.
IOPS 0-20009	Unable to save playback file '<name>'.
IOPS 0-20010	Unable to execute '<program>'.
IOPS 0-20011	Resolution for '<URL>' failed! Recording will be stopped.
IOPS 0-20014	Unable to delete step.

Table 9 IOPS Error Messages for HTTP_TRANS Probe IE Mode

IOPS 0-x Errors	Description
IOPS 0-20015	Unable to locate pattern.
IOPS 0-20016	Transaction for '<customer>'/'<service group>' timed out.
IOPS 0-20017	Unable to find step '<number>'.
IOPS 0-20018	Pattern not found in step #<number> for '<customer>'/ '<service group>' (Status=<http status code>).
IOPS 0-20019	Unable to execute '<program>'.
IOPS 0-20020	Unable to determine event message.
IOPS 0-20021	Unable to resolve step '<number>' ('<customer>'/'<service group>').
IOPS 0-20022	Unable to find closest match for '<URL>'@<index number>.
IOPS 0-20023	Unable to find frame '<name>'.
IOPS 0-20024	Unknown FORM input element '<name>'.
IOPS 0-20025	Unable to set proxy (<error message>).
IOPS 0-20039	Recording Warning.
IOPS 0-20042	The passwords do not match. Please try again.
IOPS 0-20043	The proxy passwords do not match. Please try again.
IOPS 0-20046	Pattern failed: '<pattern>'.
IOPS 0-20047	Status: <http status code>.
IOPS 0-20048	Window captured to '<path to file>'.
IOPS 0-20049	[Timeout].
IOPS 0-20050	Retry #<number>.
IOPS 0-20051	Script availability check failed in step #<number> for '<customer>'/'<service group>'.

Table 9 IOPS Error Messages for HTTP_TRANS Probe IE Mode

IOPS 0-x Errors	Description
IOPS 0-20052	Script failed: '<name>'.
IOPS 0-20053	Status: <http status code from IE mode>.
IOPS 0-20054	Url could not be parsed.
IOPS 0-20055	No session was established.
IOPS 0-20056	Cannot connect.
IOPS 0-20057	The server or proxy was not found.
IOPS 0-20058	The actual object was not found - e.g. http: 404.
IOPS 0-20059	Connection was established but data can not be retrieved.
IOPS 0-20060	Generic download failure - connection broke.
IOPS 0-20061	To access this object need authentication e.g. http: 401.
IOPS 0-20062	The object is not available of the required type, http: 403 no object.
IOPS 0-20063	The internet connection timed out.
IOPS 0-20064	The request was invalid.
IOPS 0-20065	Protocol is not known and no plugable protocol is registered.
IOPS 0-20066	[Probe Timeout after <number> second(s)].
IOPS 0-20067	[<http status code><http status text>] [URL] <current URL>.
IOPS 0-20068	[Script Check Failed on '<script name>'].
IOPS 0-20069	[Pattern Check Failed on '<pattern>'].
IOPS 0-20070	[[<http status code from IE mode><http status text from IE Mode>] [URL] <current URL>.
IOPS 0-20071	Bad request.

Table 9 IOPS Error Messages for HTTP_TRANS Probe IE Mode

IOPS 0-x Errors	Description
IOPS 0-20072	Unauthorized.
IOPS 0-20073	Payment Required.
IOPS 0-20074	Forbidden.
IOPS 0-20075	Not Found.
IOPS 0-20076	Method Not Allowed.
IOPS 0-20077	Not Acceptable.
IOPS 0-20078	Proxy Authentication Required
IOPS 0-20079	Request Timeout.
IOPS 0-20080	Conflict.
IOPS 0-20081	Gone.
IOPS 0-20082	Length Required.
IOPS 0-20083	Precondition Failed.
IOPS 0-20084	Request Entity Too Large.
IOPS 0-20085	Request-URI Too Long.
IOPS 0-20086	Unsupported Media Type.
IOPS 0-20087	Requested Range Not Satisfiable.
IOPS 0-20088	Expectation Failed.
IOPS 0-20089	Internal Server Error.
IOPS 0-20090	Not Implemented.
IOPS 0-20091	Bad Gateway.
IOPS 0-20092	Service Unavailable.
IOPS 0-20093	Gateway Timeout.

Table 9 IOPS Error Messages for HTTP_TRANS Probe IE Mode

IOPS 0-x Errors	Description
IOPS 0-20094	HTTP Version Not Supported.
IOPS 0-20095	[Proxy] %s
IOPS 0-20096	Error Unknown.
IOPS 0-20097	[Proxy] (none).
IOPS 0-20098	[URL] %s.
IOPS 0-20099	[URL] (unknown).

Note that error numbers IOPS 0-20071 to IOPS 0-20094 are HTTP errors (HTTP error codes 400-417 and 500-505).

The next table show IOPS ERROR messages for all other probes. An example of a portion of the error.log file for an HTTP probe is shown below:

```
2004-02-04 14:50:04 ERROR probeHttp(1636) [CHttpService.cpp:2637]: IOPS
1-112: ERRORINFO: [1 Broken Link(s)] [403 Access Forbidden] http://
ros84007tst3.test.tst.com:80/reports/mypage.htm [URL]
http://ros84007tst3.test.tst.com:80/reports/mypage.htm [PROXY] (none)
Customer='HP' Service Group='MY PAGE' Target='
ros84007tst3.test.tst.com:80/reports/mypage.htm'
```

Table 10 IOPS Error Messages for all Other Probes

IOPS 1-x Errors	Description
IOPS 1-1	Unable to open file '<file name>'.
IOPS 1-2	Unable to write to file '<file name>'.
IOPS 1-3	Unable to read from file '<file name>'.
IOPS 1-4	Unable to allocate memory.
IOPS 1-5	Unable to create file '<file name>'.
IOPS 1-6	Function <name> returned error.
IOPS 1-7	Unable to access '<item>'.
IOPS 1-8	Unable to get file size of '<item>'.
IOPS 1-9	Unable to execute process '<name>'.
IOPS 1-10	Unable to create a thread.
IOPS 1-11	Socket error <number> in '<item>'.
IOPS 1-12	Required property '<item>' not found in section [<name>].
IOPS 1-13	WinInet API--Error <number> in Function '<name>'. Host='<hostname>'.
IOPS 1-14	<name> protocol error: Unexpected response from server '<server>': '<buffer>'.
IOPS 1-15	Connection to '<host>' timed out.

Table 10 IOPS Error Messages for all Other Probes

IOPS 1-x Errors	Description
IOPS 1-16	Unable to resolve IP-address for '<host>'.
IOPS 1-17	RAS or TAPI Failure: <number> in Function '<name>'.
IOPS 1-18	LDAP failure: Error <number> in Function '<name>'.
IOPS 1-19	HTTP failure: Redirection to non-HTTP protocol from < protocol type > to <protocol type> not supported.
IOPS 1-20	Error loading transaction file ‘<name>'.
IOPS 1-21	Transaction file is required.
IOPS 1-22	Schema in URL '<name>' is not known.
IOPS 1-23	Error resolving navigation point '<step>' (type: '<step type>').
IOPS 1-24	Transaction '<customer>:<service group>' timed out.
IOPS 1-25	Too many HTTP/HTTPS redirects (infinite loop?).
IOPS 1-26	Unable to resolve name server.
IOPS 1-27	ICMP: Unable to do ioctlsocket (wsa=<error number>).
IOPS 1-30	Certificate chain bad (usually subject/issuer mismatch).
IOPS 1-31	Certificate has expired.
IOPS 1-32	Unknown and unprovided root certificate.
IOPS 1-33	Unknown Certificate chain validation error <number>.
IOPS 1-34	Trusted Root Certificate count = <total count>.
IOPS 1-35	Certificate validation Failed.
IOPS 1-36	Certificate Name could not be validated.
IOPS 1-37	InitSSLContext() Failed.
IOPS 1-38	SSLHandshake() Failed with error < ssl error number >.

Table 10 IOPS Error Messages for all Other Probes

IOPS 1-x Errors	Description
IOPS 1-39	InitSSLCryptoEngineModules() Failed with error <ssl error number>.
IOPS 1-40	SSLInitialize() Failed with error < ssl error number >.
IOPS 1-41	SSL ConfigureContextForRandom() Failed with error < ssl error number >.
IOPS 1-42	SSLSetCheckCertificateChainFunc() Failed with error < ssl error number >.
IOPS 1-43	SSLSetProtocolSide() Failed with error < ssl error number >.
IOPS 1-44	SSLSetProtocolVersion() Failed with error < ssl error number >.
IOPS 1-45	SSLLoadTrustedCertificateFile() Failed with error < ssl error number >.
IOPS 1-46	SSL ConfigureContextForDB() Failed with error < ssl error number >.
IOPS 1-47	SSLDuplicateChildContext() Failed with error < ssl error number >.
IOPS 1-48	SSLSetIOSemantics() Failed with error < ssl error number >.
IOPS 1-49	SSLSetPeerID() Failed with error < ssl error number >.
IOPS 1-50	SSLGetNegotiatedCipher() Failed with error < ssl error number >.
IOPS 1-51	SSLGetCiphersuiteInfo() Failed with error < ssl error number >.
IOPS 1-52	Loading Client Certificate Failed with error <ssl error number>.

Table 10 IOPS Error Messages for all Other Probes

IOPS 1-x Errors	Description
IOPS 1-53	Loading Client Certificate Failed with error <ssl error number>, verify password on private key.
IOPS 1-54	Loading Client Certificate Failed with error <ssl error number>, verify client certificate file exists in the probes directory.
IOPS 1-55	Unable to create directory '<name>'.
IOPS 1-56	Pattern not found in step #<number> for '<customer>'/ '<service group>' (Status=<http status number>).
IOPS 1-57	Pattern not found for '<customer>'/'<service group>' (Status=<http status code>).
IOPS 1-58	Pattern not found for '<customer>'/'<service group>'.
IOPS 1-59	Pattern failed: '<pattern>'.
IOPS 1-60	Status: <http status code>.
IOPS 1-61	MeasureAll() Failed.
IOPS 1-62	Metric Logging Failed.
IOPS 1-63	SQL ERROR Message = SQLSTATE: <type> Native error: <number> Message: <SQL error message>.
IOPS 1-64	SQLAllocHandle() Environment Setup Failed.
IOPS 1-65	SQLAllocHandle() Connection to Datasource Failed.
IOPS 1-66	SQLConnect() Failed.
IOPS 1-67	SQLAllocHandle() Execute Failed.
IOPS 1-68	SQLExecDirect() Failed.
IOPS 1-69	SQLColAttributes() Failed.
IOPS 1-70	SQLFetch() Failed.
IOPS 1-71	SQLGetData() Failed.

Table 10 IOPS Error Messages for all Other Probes

IOPS 1-x Errors	Description
IOPS 1-72	[Timeout].
IOPS 1-73	User login failed for user '<name>'.
IOPS 1-74	Impersonate logged on user failed.
IOPS 1-75	Create Pipe failed.
IOPS 1-76	Create process failed.
IOPS 1-77	Get password failed.
IOPS 1-78	Change directory failed.
IOPS 1-79	Create fork failed.
IOPS 1-80	Create exec failed.
IOPS 1-81	Unable to set pipe to non blocking.
IOPS 1-82	Web page contains <number> broken image links for '<customer>'/'<service group>'.
IOPS 1-83	Pattern '<pattern>' not found.
IOPS 1-84	Exit code status failed for script. Exit code check returned <number>.
IOPS 1-85	Exit code status failed for Results file script. Exit code check returned <number>.
IOPS 1-86	File '<name>' not found.
IOPS 1-87	File '<name>' access denied.
IOPS 1-88	Unable to impersonate user, error returned - <impersonate user error>
IOPS 1-89	Unable to logon to mapi profile <name>.
IOPS 1-90	Unable to get mapi session.
IOPS 1-91	Exchange server returned error '<type>', '<component>'.

Table 10 IOPS Error Messages for all Other Probes

IOPS 1-x Errors	Description
IOPS 1-92	Exchange server (open inbox) returned error '<type>', '<component>'.
IOPS 1-93	Exchange server (list messages) returned error '<type>', '<component>'.
IOPS 1-94	Exchange server (Read New Message) returned error '<type>', '<component>'.
IOPS 1-95	Exchange server (open delete item folder) returned error '<type>', '<component>'.
IOPS 1-96	MAPIAllocateBuffer failed.
IOPS 1-97	MAPI - Open Address book failed.
IOPS 1-98	MAPI - GetProps from outbox folder object failed.
IOPS 1-99	MAPI - Message Store has no valid PR_IPM_OUTBOX_ENTRYID.
IOPS 1-100	MAPI - Open Entry of Outbox failed.
IOPS 1-101	MAPI - Folder object type of OpenEntry on lpFolder != MAPI_FOLDER.
IOPS 1-102	MAPI - CreateMessage failed.
IOPS 1-103	MAPI - SetProps failed.
IOPS 1-104	MAPI - Create custom address book entry failed.
IOPS 1-105	MAPI - CreateMessage failed.
IOPS 1-106	MAPI - Failed to SetProp on the custom message, will not send e-mail.
IOPS 1-107	MAPI - ModifyRecipients failed.
IOPS 1-108	Failed to create profile, mapi probe service will not run.
IOPS 1-109	Script step error info = <error message>.

Table 10 IOPS Error Messages for all Other Probes

IOPS 1-x Errors	Description
IOPS 1-110	Script format incorrect on Step <number>.
IOPS 1-111	[<number> Broken Link(s)] <URL>.
IOPS 1-112	ERRORINFO: <error message> Customer='<name>' Service Group='<name>' Target='<name>'.
IOPS 1-113	Unable to load Trusted Certificate file <name>.
IOPS 1-114	Unable to load Client Certificate file <name>.
IOPS 1-115	Client Certificate Failed. Verify password on private key.
IOPS 1-116	The Root Certificate is not trusted.
IOPS 1-117	One of the certificates in the chain is expired.
IOPS 1-118	File <name> is not formatted properly, or is missing a certificate or private key.
IOPS 1-119	Certificate Name could not be validated with (<host name>).
IOPS 1-120	SSLDuplicateContext() Failed with error <number>.
IOPS 1-121	Certificate name (<certificate>) does not match server name (<server>).
IOPS 1-122	Unable to create socket for <host name>.
IOPS 1-123	Socket host connection failed for <host name>.
IOPS 1-124	[DNS Unable to resolve host (<error message>)].
IOPS 1-125	[TCP Internal - Check log files] <error message>.
IOPS 1-126	[<number> Broken Link(s)] <http error message>.
IOPS 1-127	[SSL Error] <ssl error message>.
IOPS 1-128	[SSL Internal - Check log files].
IOPS 1-129	[SSL Timeout after <number> second(s). Check log files].

Table 10 IOPS Error Messages for all Other Probes

IOPS 1-x Errors	Description
IOPS 1-130	[Probe Timeout after <number> second(s) at <error message>].
IOPS 1-131	[Pattern Check Failed on '<pattern>'].
IOPS 1-132	[<http error message>].
IOPS 1-135	[PROXY] <proxy server>:<proxy port>.
IOPS 1-136	[PROXY] (none).
IOPS 1-137	[URL] <host:port/…>.
IOPS 1-138	[Probe Timeout after <number> second(s)].
IOPS 1-139	[Error Unknown].
IOPS 1-140	[URL] http://<host:port/…>.
IOPS 1-141	[URL] https://<host:port/…>.
IOPS 1-142	Unhandled Global Exception on '<name>'.
IOPS 1-143	HPPT/S Unhandled Exception: Customer='<customer>' Service Group='<service group>' Host='<host>' URL='<URL string>' Port='<port>' Proxy='<proxy>' Timeout='<number>'.
IOPS 1-144	HPPT_TRANS Unhandled Exception: Customer='<customer>' Service Group='<service group>' Proxy='<proxy>' Timeout='<number>'.
IOPS 1-145	Packet size must be greater than '<number>' and smaller than 65536.
IOPS 1-146	Select failed (error=<error number>).
IOPS 1-147	Timeout while trying to connect to '<name>'.
IOPS 1-148	UDP: Unable to retrieve results from server.

Table 10 IOPS Error Messages for all Other Probes

IOPS 1-x Errors	Description
IOPS 1-149	ssl_CreateConnectionContext() failed with error <ssl error number>.
IOPS 1-150	sslrad_CreateSessionDB() failed with error <ssl error number>.
IOPS 1-151	ssl_SetCipherSuites() failed with error <ssl error number>.
IOPS 1-152	ssl_CreateGlobalContext() failed with error <ssl error number>.
IOPS 1-153	ssl_SetPRNG() failed with error <ssl error number>.
IOPS 1-154	ssl_SetProtocol() failed with error <ssl error number>.
IOPS 1-155	ssl_Handshake() failed with error <ssl error number>.
IOPS 1-156	ssl_SetCheckCertificateChainFunc() failed with error <ssl error number>.
IOPS 1-157	ssl_AddTrustedCACertificates() failed wtih error <ssl error number>.
IOPS 1-158	InitSSLMasterContext() failed with error <ssl error number>.
IOPS 1-159	ssl_SetIOSemantics() failed with error <ssl error number>.
IOPS 1-160	ssl_GetNegotiatedCipher() Failed with error <ssl error number>.
IOPS 1-161	ssl_SetIOFuncs() Failed with error <ssl error number>.
IOPS 1-162	InitSSLCryptoEngineModules() Failed with error <ssl error number>.
IOPS 1-163	ssl_SetClientAuthModes() Failed with error <ssl error number>.
IOPS 1-164	ssl_Read() Failed with error <ssl error number>.

Table 10 IOPS Error Messages for all Other Probes

IOPS 1-x Errors	Description
IOPS 1-165	ssl_Write() Failed with error <ssl error number>.
IOPS 1-166	HTTPS Service timed out during ssl_Handshake().
IOPS 1-167	One of the certificates in the chain is expired in the Trusted Certificate file '<cert filename>'.
IOPS 1-168	Certificate Name (<cert name>) could not be validated with Server Name (<server name>).
IOPS 1-169	Certificate validation failed during the SSL Handshake.
IOPS 1-170	Extracting certificate name with ssl_ExtractCertificateNameItem() Failed with error <ssl error number>.
IOPS 1-171	Certificates not found in ssl_CheckCertificateChainCallback().
IOPS 1-172	Certificate public key is of an unsupported type in ssl_CheckCertificateChainCallback(). Error = <ssl error number>.
IOPS 1-173	Certificate corrupted in ssl_CheckCertificateChainCallback(). Error = <ssl error number>.
IOPS 1-174	Unsupported certificate signature algorithm in ssl_CheckCertificateChainCallback(). Error = <ssl error number>.
IOPS 1-175	Certificate parsing error in ssl_CheckCertificateChainCallback(). Error = <ssl error number>.
IOPS 1-176	Certificate chain not trusted in ssl_CheckCertificateChainCallback(). Error = <ssl error number>.

Table 10 IOPS Error Messages for all Other Probes

IOPS 1-x Errors	Description
IOPS 1-177	Invalid PEM encoded certificate in ssl_CheckCertificateChainCallback(). Error = <ssl error number>.
IOPS 1-178	Certificate has no serial number in ssl_CheckCertificateChainCallback(). Error = <ssl error number>.
IOPS 1-179	ssl_CheckCertificateChainCallback() Failed with certificate error <ssl error number>.
IOPS 1-180	Certificate check failed with the warning: <string> in ssl_CheckCertificateChainCallback().
IOPS 1-181	ssl_GetNegotiatedProtocolVersion() Failed with error <ssl error number>.
IOPS 1-182	WMI authentication failed with error <ssl error number>.
IOPS 1-183	WMI connect failed with error <ssl error number>.
IOPS 1-184	WMI metric retrieval failed with error <ssl error number>.
IOPS 1-185	WMI counter rolled or system rebooted. No queue file will be created this interval.

HTTP Status Codes

The table below shows HTTP 1.1 status codes. The description shown in the table is from www.w3.org documentation. For HTTP, HTTPS and HTTP_TRANS probes, returned HTTP status codes of 200 - 299 indicate the probe is available.

Table 11 HTTP 1.1 Status Codes

HTTP 1.1 Status Code	Description
Informational - 1xx	
100	Continue
101	Switching Protocols
Successful - 2xx	
200	OK
201	Created
202	Accepted
203	Non-Authoritative Information
204	No Content
205	Reset Content
206	Partial Content
Redirection - 3xx	
300	Multiple Choices
301	Moved Permanently
302	Found
303	See Other
304	Not Modified
305	Use Proxy

Table 11 HTTP 1.1 Status Codes

HTTP 1.1 Status Code	Description
307	Temporary Redirect
Client Errors - 4xx	
400	Bad Request
401	Unauthorized
402	Payment Required
403	Forbidden
404	Not Found
405	Method Not Allowed
406	Not Acceptable
407	Proxy Authentication Required
408	Request Timeout
409	Conflict
410	Gone
411	Length Required
412	Precondition Failed
413	Request Entity too Large
414	Request-URI Too Long
415	Unsupported Media Type
416	Requested Range Not Satisfiable
417	Expectation Failed
Server Errors - 5xx	
500	Internal Server Error
501	Not Implemented

Table 11 HTTP 1.1 Status Codes

HTTP 1.1 Status Code	Description
502	Bad Gateway
503	Service Unavailable
504	Gateway Timeout
505	HTTP Version Not supported

SSL Error Codes

SSL Error Codes (may be logged by HTTPS or HTTP_TRANS probes) are shown in the table below. The description is, in part, derived from the Certicom API documentation.

Table 12 SSL Error Codes

Error Number	SSL Error Codes	Description
0x150	CERT_SERVER_NAME_MISMATCH	Certificate name and server name do not match.
0x151	NO_CERTIFICATES_FOUND	No certificates found during certificate validation.
0x152	CERT_WARNING_FOUND	Certificate warning found during certificate validation.
0x00000000	CIC_ERR_NONE	Success.
0x80010000	CIC_ERR_INTERNAL	An error occurred while extracting the certificate validity date.
0x81010001	CIC_ERR_NO_PTR	NULL pointer was passed.
0x81010002	CIC_ERR_ILLEGAL_PARAM	Parameter is invalid.
0x81010004	CIC_ERR_SMALL_BUFFER	Buffer is too small.
0x81010005	CIC_ERR_WOULD_BLOCK	I/O is blocking.

Table 12 SSL Error Codes

Error Number	SSL Error Codes	Description
0x81010006	CIC_ERR_TIMEOUT	Error Timeout.
0x81010007	CIC_ERR_BAD_LENGTH	Length is invalid.
0x81010008	CIC_ERR_NOT_FOUND	Error or record not found.
0x81010009	CIC_ERR_BAD_CTX	Invalid context.
0x8101000A	CIC_ERR_BAD_INDEX	Invalid index.
0x8101000B	CIC_ERR_RANDOM	Invalid random number.
0x8101000C	CIC_ERR_MEM_UNDERRUN	SSL memory error.
0x8101000D	CIC_ERR_MEM_OVERRUN	SSL memory error.
0x8101000E	CIC_ERR_MEM_WAS_FREED	SSL memory error.
0x8101000F	CIC_ERR_MEM_NOT_OURS	SSL memory error.
0x81090001	CIC_ERR_CERT_UNSUPPORTED_PUBKEY_TYPE	The public key inside the certificate is of unsupported type.
0x81090002	CIC_ERR_CERT_CORRUPTED	The certificate is corrupted.
0x81090003	CIC_ERR_CERT_UNSUPPORTED_SIG_ALG	Signature algorithm used to sign the certificate was not previously registered or is unsupported.
0x81090004	CIC_ERR_CERT_NOT_PARSED	Certificate was not initialized properly.
0x81090005	CIC_ERR_CERT_NO_TRUSTED_ISSUER	No trusted issuer was found when trying to verify certificate.
0x81090006	CIC_ERR_CERT_ILLEGAL_ALLOCATION_TYPE	Allocation type is unknown, or not suitable for selected options.
0x81090007	CIC_ERR_CERT_BAD_PEM	The delimiters of Base64 encoded certificate are invalid.
0x81090008	CIC_ERR_CERT_NO_SN	This certificate has no serial number.

Table 12 SSL Error Codes

Error Number	SSL Error Codes	Description
0x810A0001	CIC_ERR_SSL_INCOMPLETE_IDENTITY	Certificate list does not contain both private key and certificate.
0x810A0002	CIC_ERR_SSL_BAD_SIDE	The protocol side of this mode is different from that selected with a previous mode.
0x810A0003	CIC_ERR_SSL_OVERFLOW	An incoming record exceeds the size of the read or write buffer.
0x810A0004	CIC_ERR_SSL_UNEXPECTED_MSG	Unexpected message was received.
0x810A0005	CIC_ERR_SSL_BAD_MAC	Verification of SSL record message failed.
0x810A0006	CIC_ERR_SSL_DECRYPT_FAILED	SSL record decryption failed.
0x810A0007	CIC_ERR_SSL_UNKNOWN_RECORD	Unknown record type.
0x810A0008	CIC_ERR_SSL_NEGOTIATION	SSL negotiation error.
0x810A0009	CIC_ERR_SSL_IO	I/O error from callbacks.
0x810A000A	CIC_ERR_SSL_FATAL_ALERT	Fatal alert was received or sent.
0x810A000B	CIC_ERR_SSL_PROTOCOL	General protocol error. May be caused by incorrectly formatted messages.
0x810A000C	CIC_ERR_SSL_RESUMABLE_SESSION	Peer is trying to resume a session with different session parameters.
0x810A000D	CIC_ERR_SSL_BAD_FINISHED_MESSAGE	The finished message received during SSL handshake was invalid.
0x810A000E	CIC_ERR_SSL_CONNECTION_CLOSED_GRACEFUL	The SSL connection was closed gracefully.

Table 12 SSL Error Codes

Error Number	SSL Error Codes	Description
0x810A000F	CIC_ERR_SSL_CONNECTION_CLOSED	The SSL connection was closed.
0x810A0010	CIC_ERR_SSL_BAD_MAX_FRAGMENT_LENGTH_EXTENSION	The value for the max_fragment_length extension is unknown.
0x810A0011	CIC_ERR_SSL_BAD_CERTIFICATE	General catch all error for bad certificates.
0x810A0012	CIC_ERR_SSL_ALERT_CB_FAILURE	Application alert callback returned an error.
0x810A0013	CIC_ERR_SSL_SESSION_NOT_FOUND	Session was not found in session database.
0x810A0014	CIC_ERR_SSL_NOT_SUPPORTED	Renegotiation with SSL2 is not supported.
0x810A0015	CIC_ERR_SSL_BAD_MESSAGE_LENGTH	Message received from peer has incorrect length.
0x810A0016	CIC_ERR_SSL_NO_SUPPORTED_CIPHER_SUITES	There is no local identity for the ciphersuite, no RSA export keys for an RSA export ciphersuite, or the protocol being negotiated doesn't support the ciphersuite.
0x810A0017	CIC_ERR_SSL_NO_MATCHING_CIPHER_SUITES	Both ends of the handshake cannot agree on a cipher suite.
0x810A0018	CIC_ERR_SSL_TLS_EXTENSION_MISMATCH	Both ends of the handshake cannot agree on a TLS extension.
0x810A0019	CIC_ERR_SSL_BAD_PROTOCOL_VERSION	Server sent ServerHello with protocol version which cannot be negotiated.

Table 12 SSL Error Codes

Error Number	SSL Error Codes	Description
0x810A001A	CIC_ERR_SSL_BAD_EXPORT_KEY_LENGTH	Server sent ServerKeyExchange message with an export key which does not meet the export restrictions.
0x810A001B	CIC_ERR_SSL_BAD_DHPARAM_KEY_LENGTH	Server sent ServerKeyExchange message with DH params which do not meet the export restrictions.
0x810A001C	CIC_ERR_SSL_BAD_PREMASTER_SECRET_VERSION	The premaster secret must contain the same version number as the ClientHello to detect version rollback attacks. The vesion sent by the client was incorrect.
0x810A001D	CIC_ERR_SSL_BAD_PREMASTER_SECRET_LENGTH	The pre-master-secret sent by the peer has an incorrect length.
0x810A001E	CIC_ERR_SSL_NO_CERTIFICATE	The other side sent Certificate message containing no certificates.
0x810A001F	CIC_ERR_SSL_NO_MATCHING_CERTIFICATES	The other side sent Certificate message containing certificate(s) not signed by trusted Cetificate Authority.
0x810A0020	CIC_ERR_SSL_CERTIFICATE_VALIDATE_FAILED	The other side sent a certificate which was not been validated and the user's certificate callback returned error on this certificate.
0x810A0021	CIC_ERR_SSL_CERT_CHECK_CALLBACK	The certificate(s) passed into the certificate callback were rejected by the callback but no external error was inputted to the callback.
0x810A0022	CIC_ERR_SSL_NULL_CB	A NULL callback pointer was passed as an argument or the context is configured with a NULL callback.

Table 12 SSL Error Codes

Error Number	SSL Error Codes	Description
0x810A0023	CIC_ERR_SSL_BAD_CERTIFICATE_REQUEST	The certificate request message was not formatted correctly.
0x810A0024	CIC_ERR_SSL_ENTROPY_COLLECTION	The internal entropy collection failed to generate enough seeding data.
0x810A0025	CIC_ERR_SSL_BAD_CLEAR_KEY_LEN	The CLEAR-KEY-LENGTH in a SSL2 ClientMasterKey message is invalid.
0x810A0026	CIC_ERR_SSL_BAD_ENCRYPTED_KEY_LEN	The ENCRYPTED-KEY-LENGTH in a SSL2 ClientMasterKey message is invalid.
0x810A0027	CIC_ERR_SSL_BAD_KEY_ARG_LEN	The KEY-ARG-LENGTH in a SSL2 ClientMasterKey message is invalid.
0x810A0028	CIC_ERR_SSL_BAD_SECRET_KEY_LEN	The length of SECRET-KEY-DATA from a SSL2 ClientMasterKey message in invalid.
0x810A0029	CIC_ERR_SSL_BAD_PKCS1_PADDING	Decrypted plain text for not padded properly when it was encrypted.
0x810A002A	CIC_ERR_SSL_FAIL_SERVER_VERIFY	Failed to verify SSL2 SERVER-VERIFY message.
0x810A002B	CIC_ERR_SSL_READ_BUFFER_NOT_EMPTY	The read record buffer is not empty and cannot be released.
0x810A002C	CIC_ERR_SSL_WRITE_BUFFER_NOT_EMPTY	The write record buffer is not empty and cannot be released.
0x810A002D	CIC_ERR_SSL_BUFFERS_NOT_EMPTY	Both read and write record buffers are not empty and cannot be released.
0x810A002E	CIC_ERR_SSL_UNSUPPORTED_CLIENT_AUTH_MODE	The client authentication mode(s) enabled cannot be used within the selected cipher suite.

Table 12 SSL Error Codes

Error Number	SSL Error Codes	Description
0x810A002F	CIC_ERR_SSL_BAD_CONTEXT	The global context is incorrectly configured or invalid.
0x810A0030	CIC_ERR_SSL_HANDSHAKE_REQUIRED	Handshake must be completed first.
0x810A0031	CIC_ERR_SSL_HANDSHAKE_REQUESTED	A renegotiated handshake has been requested by connection's peer. Handshake is optional.
0x810A0032	CIC_ERR_SSL_RENEGOTIATION_REFUSED	A renegotiated handshake has been refused by connection's peer.
0x810A0033	CIC_ERR_SSL_HANDSHAKE_ALREADY_COMPLETED	Handshake is already completed.
0x810A0034	CIC_ERR_SSL_RENEGOTIATION_ALREADY_REQUESTED	Renegotiation has already been requested.
0x810A0035	CIC_ERR_SSL_READ_REQUIRED	Renegotiation with the peer has not started yet. There is application data which must be read before handshake can proceed.
0x810A0036	CIC_ERR_SSL_UNSUPPORTED_PUBKEY_TYPE	The public key type is unsupported.
0x810A0037	CIC_ERR_SSL_BAD_RECORD_LENGTH	The length of an incoming record exceeds the maximum length specified in the protocol specification.
0x810A0038	CIC_ERR_SSL_NEEDS_CIPHER_OR_CLIENTAUTH	Before installing a private key, a ciphersuite or client authentication suite using the same key exchange algorithm (RSA vs ECC) must be installed first.

Table 12 SSL Error Codes

Error Number	SSL Error Codes	Description
0x810A0039	CIC_ERR_SSL_INVALID_PFX	The PFX is invalid for this operation, containing either no certificates and no private key, or multiple private keys.
0x810A003A	CIC_ERR_PKCS12_MISSING_ALG	The PFX uses algorithm (s) which have not been supported through the suites parameter.
0x810A003B	CIC_ERR_SSL_NEEDS_PRNG	The PRNG suite has not yet been installed.
0x810A003C	CIC_ERR_SSL_CERT_CHAIN_WARNINGS	There are warnings associated with the certificate chain validation.
0x810A003D	CIC_ERR_SSL_WARN_TRUSTED_EXPIRED	One or more trusted certificates in the certificate list have expired.
0x810A003E	CIC_ERR_SSL_PROTOCOL_VERSION_INVALID	The protocol version being used is not valid.
0x810A003F	CIC_ERR_SSL_PROTOCOL_NOT_INSTALLED	The protocol version being used was not installed.
0xF001	CIC_ERR_MEMORY	Error allocating memory.

Troubleshooting Alarms

If you are not seeing alarms displayed in the Dashboard, you can check to be sure you have configured alarm thresholds in the Objectives Information dialog box of the Configuration Manager.

Then you can check to see if alarms are being generated by setting the trace level to 9 and checking the contents of the trace.measEvent2 file. The trace shows when an alarm was generated.

Also note that in order for alarms to be displayed in the dashboard, the Configuration Manager **File > Configure > Alarm Destinations**, **Database (Alarms and NNM Integration)** checkbox must be checked.

Alarm Forwarding

Alarm forwarding can best be verified by setting the trace level to 9 and checking the contents of the `trace.measEvent2` file. The trace shows when an alarm was generated and to which destination it was sent.

When alarms are forwarded to NNM, they are stored in the IOPS_ALARM_DATA table. The contents of this table can be displayed with the IE 5.0 browser. Just specify the URL `http://<measurement_server's_hostname>/HPOV_IOPS/isapi/alarmEvent.dll?GetEvent`.

This will format the contents of the IOPS_ALARM_DATA table as XML.

When alarms are sent to OVO, a message like the following will be logged to `trace.measEvent2`:

```
2000/10/17 07:25:19 (5): Alarm to ITO: OVIS Trans:
portico.hp.com:xxx.corp.hp.com:Trans:
HPWeb:PorticoNameLookup OVIS_HTTP_TRANS xxx.corp.hp.com
(ovis="xxx.corp.hp.com" customer="HPWeb"
serviceGroup="PorticoNameLookup" probeDesc="HTTP_TRANS - Web
Transactions" probeType="HTTP_TRANS" metric="RESPONSE_TIME")
```

OVIS will set the following OVO attributes:

ITO attribute (opcmsg)	OVIS value
Object	target host:probe system:target info
msg_grp	OVIS_<probe name>
Node	OVIS server FQDN (or, can be configured in the GUI: ipAddr)
msg_txt	message text
application	OVIS
severity	OVIS severity

Option variables	ovis=<OVIS server FQDN>
	customer=<customer>
	seviceGroup=<service group>
	probeDesc=<probeDesc>
	probeName=<probe name>
	metric=<metric>

For example, to emulate an alarm with the above trace message, the opcmsg message call would have the following parameters:

```
opcmsg a=OVIS o="portico.hp.com:xxx.corp.hp.com:Trans:
HPWeb:PorticoNameLookup" msg_grp=OVIS_HTTP_TRANS
node=xxx.corp.hp.com msg_text="Test"
```

Check if Message was sent to the OVO Server

In the `trace.measEvent2` file, you should see what is sent to OVO. For example:

```
2002/02/11 14:28:21 (5): Alarm to ITO (ret=0): OVIS
sev=Critical obj=127.0.0.1:xxx.corp.hp.com:81@127.0.0.1
grp=OVIS_ANYTCP node= (ovis="xxx.corp.hp.com"
customer="Test" serviceGroup="T1" probeDesc="TCP - TCP Port
Service" probeType="ANYTCP" metric="AVAILABILITY"
ipAddr="127.xx.0.1")
```

Note the `ret=0` indicates that the message was put in the OVO queue.

So first check the `trace.measEvent2` file to see whether there are any `Alarm to ITO` messages and what the return code is. If there are no messages, then check in the Configuration Manager **File > Configure > Alarm Destinations** dialog box, that **OVO Default** is enabled. To get continuous alarms, check the **Continuous** box (this is a good idea for testing, otherwise you only get another alarm once the alarm condition clears).

Continuous Alarming Checkbox

In the Configuration Manager **File > Configure > Alarm Destinations** dialog box you can check the **Continuous** box to specify that alarms should be sent continuously when a service level violation occurs. If not checked, alarms are only sent when an alarm state changes.

If this box is not checked you may not be seeing the alarms you think you should, because you will only see alarms when the alarm state changes and not if it stays the same. So if you have a critical alarm and the alarm condition continues in that state for multiple durations, you will not get a new alarm; you will only get a new alarm when it changes to some state other than critical.

Baselining Setting

In the Configuration Manager, when you set up Service Objectives for a service group, you can check the box **Use historical baseline in addition to thresholds to trigger alarms** in the Objective Information dialog to select baselining. Uncheck the box to turn off baselines.

This setting can cause you not to see alarms you think you should see. Try turning it off and see if you get the alarms you think you should. For a more detailed description of this feature see How Baselines Work on page 119.

Suppress Normal Alarms Checkbox

In the Configuration Manager **File > Configure > Alarm Destinations** dialog box you can set Suppress Normal Alarms. By default this box is checked.

Uncheck this box if you want END ALARM events sent to OVO when an alarm condition ends. For OVO, the default is to not send an END ALARM event. Setting Suppress Normal Alarms enables you to take advantage of the OVO for UNIX 6.0 and later state based browser (automatic good/bad message correlation) function and similar functionality in OVO for Windows or less automated event correlation in earlier versions of ITO.

Late Alarms

You may see late alarms if the IP Address in the Default Web Site Properties in IIS is set to a specific IP address.

IP Address should be set to "All Unassigned" (this is necessary to support localhost access of the webserver and OVIS internally uses localhost access).

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:).

OVISStatus

The program `OVISStatus.exe` runs automatically and sends alarms to OVO or NNM if data is not received from the probe system within the expected time + 10 percent, to allow for minor delays.

`OVISStatus` computes the expected time for data to arrive from a probe system by finding the shortest interval for any enabled (i.e., not disabled) and up (i.e., not scheduled down) target being probed from that system, and adding 10% to it. For example, if the shortest probe interval for active targets on a probe system is 60 seconds, then `OVISStatus` will add 10% to that and look for data from that probe location in the last 66 seconds as long as one target is enabled and up.

For customers with full Reporter installed on the OVIS Management Server, the Reporter GUI will show `OVISStatus.exe` with parameters "`-alarm2 -probesystem -waitintervalp 10`" running every 5 minutes. The `-alarm2` default setting causes `OVISStatus` to follow the Continuous Alarm settings along with the settings configured in the OVIS Configuration Manager **File > Configure > Alarm Destinations** dialog.

There are two cases where you may want to reset the default `OVISStatus` parameters. If an additional 10% is not enough time to allow for minor delays, that percentage `(-waitintervalp)` can be increased. Also if you have probe systems that routinely send probe data from 2 nics or more from one system, `OVISStatus` can sometimes not return the correct status. To correct this problem, you can change the default settings for `OVISStatus` to remove `-probsystem` and use the internal probe station identifier. The new parameters would then be `OVISStatus -alarm2 -waitintervalp 10`. OVIS does not support changing any other parameter, and highly recommends you change these parameters with caution.

`OVISStatus` assumes that the target status (i.e., enabled or disabled, up or scheduled down) in the database is consistent with the remote probe configuration.

There is normally some time delay between an OVIS operator changing a configuration, saving it, and it being automatically distributed to the remote probe system.

When there is at least one target up on a remote probe system, this is not a problem. But consider the situation where the configuration manager operator disables all targets on a remote probe system, saves the configuration, which is then distributed automatically to that remote probe system.

Then every time `OVISStatus` runs it sees that there are no active targets on this system, and so does not issue an alarm. Everything is working as expected so far.

One hour later the operator enables all the targets on that system, and forgets to save the configuration. The next time `OVISStatus` runs, it sees from that database that the probe systems on that remote probe location are enabled, and looks for data in the last measurement interval plus 10%. It sees that there has been no data for over an hour, and alarms to indicate there is no probe data from that location when there should have been.

Even if the operator had saved the configuration immediately, `OVISStatus` could have still run before the configuration file was picked up by the remote probe system and probe data collected and transmitted back to the measurement server.

So there is always a timing window, and `OVISStatus` is most vulnerable to that timing window when all targets on a probe location have been down (disabled or scheduled down) and then the operator takes action to bring one or more of them back up.

To minimize this effect with scheduled down time, `OVISStatus` has been coded to consider a target down if it were scheduled down either currently or five minutes previously. This allows an extra buffer to scheduled down time targets. But there is no such buffer with disabled targets. Because of this, it is recommended that you use a scheduled down time definition which is 24 hours per days, 7 days per week to effectively "disable" targets if you are going to occasionally bring all targets on a probe location down for an indeterminate period of time.

Troubleshooting by Probe

How you Run a Probe Affects the Results

There are several ways to run a probe and depending on how you run the probe you may get different results: the probe could be successful or unsuccessful and/or the metrics could be different.

- Configure the probe and let the OVIS Scheduler run the probe on the probe system.
- Select **Test on Management Server** to test the probe from the Configuration Manager.
- Run the probe from the command line.

There are other probes that can be run in additional ways such as the HTTP_TRANS probe can be run from inside the Web Transaction Recorder (playback mode).

One of the major differences in how you run these probes is the user who is actually running the probe.

If the probe is run by the Scheduler, the probe is run as the **Local System account** (as seen in the HP Internet Services Properties window), unless you have changed the HP Internet Services service to run as some other user.

If the probe is run from the command line or by selecting Test on Management Server in the Configuration Manager, then the probe is run as whatever user you are logged on as. This can cause the probe to either be successful or unsuccessful depending on what permissions the log on user has. This can be especially evident in the Script, Exchange, HTTP_TRANS and custom probes.

Also running any of the probes from the Scheduler vs. command line/Test on Management Server can result in slightly different metric values. When the Scheduler runs the probes it may be running more then one probe at a time, depending on what the concurrency is set to. As a result there may be more demands on the resources of the system when the Scheduler runs the probe then when you run a single probe from the command line/Test on Management Server. One example of this would be the response time, which could be higher when run by the Scheduler than when run by the command line/Test on Management Server.

Troubleshooting the Exchange and Script Probes

Problem: If the Exchange probe or Script probe has problems with Service Targets being unavailable on Windows probe systems, it may be that the Windows environment on that system has not been initialized.

Solution: Login to the Windows probe system as the user you've configured for the probe. This will initialize the Windows environment, setting up a Windows user profile.

Troubleshooting the HTTP_TRANS Probe

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

Running the HTTP_TRANS IE mode probe (probehttptrans2) with the -print option will not produce results on Windows 2000 because that platform does not support the ability to write to a console from a Windows GUI application. This means that the **Test on Management Server** function in the Configuration Manager will not return results for the IE mode HTTP_TRANS probe on Windows 2000 (it does work on Windows 2003 and Windows XP or higher). It also means that the Probe Re-Execution TIP for this probe on Windows 2000 will give the message "No results returned for command".

Troubleshooting the SOAP Probe

A successful request will return an HTTP response code of 200. The body element of the SOAP response will contain the Response element values for a valid request

A faulty request will return an HTTP response code of 500 Internal Server Error. A SOAP server will return an error condition by including a <soap:Fault> element inside the <soap:Body> element of the SOAP response. The Fault element must contain a faultcode and faultstring element.

If you set probe tracing level to 9 then you can see the response code and error condition information. See the example below for a sample of a faulty request:

```
HTTP/1.0 500 Internal Server Error.
Connection: close
```

```
Server: Microsoft-IIS/5.0
Date: Fri, 14 Nov 2003 01:49:43 GMT
Cache-Control: private
Content-Type: text/xml; charset=utf-8
Content-Length: 597

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/
envelope/"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <soap:Fault>
      <faultcode>soap:Client</faultcode>
      <faultstring>Server was unable to read request. --&gt;
There is an error in XML document (7, 54). --&gt; The
's0:getPopulationX' start tag on line '6' does not match the end
tag of 's0:getPopulation'. Line 8, position 9.</faultstring>
      <detail />
    </soap:Fault>
  </soap:Body>
</soap:Envelope>
```

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 SYS_BASIC_WMI probe

If the SYS_BASIC_WMI probe is getting an error 80041010, either when connecting to get network interface information or during the actual probe execution, you will need to instruct WMI to rediscover the performance libraries on the system. To do this, enter the following commands in a DOS window on the target system:

```
wmiadap /c

wmiadap /f

wmiadap /r
```

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 Pattern Matching

Encoded HTML Characters

Certain HTML characters are encoded (for example & is &amp; and “ is &quot;). When setting up a pattern to match you should be sure to check the HTML source (right-click in the html document and select View Source) to see whether the string that is displayed in the browser contains any encoded characters. If encoded characters are part of the string you need to adjust the pattern accordingly.

For example in HTML, the string cats&dogs could be encoded as cats&amp;dogs. Therefore, entering +“cats & dogs” as the pattern for matching will not work for this case.

If you have the string “See Spot & Fluffy Run!”, and you put in the pattern matching as +““See Spot & Fluffy Run!”” it will not match, because the & is encoded as &amp; and the quotes are encoded as &quot; in the HTML source.

But if the string is broken up and the special characters are removed, it will match: +“See” +“Spot” +“Fluffy” +“Run”

Using the Minus Sign to not Match Patterns

You can use the minus sign (-) to tell the Web Transaction Recorder to not match a page that contains a certain word. For example, if you want to know when a page is unavailable, you can configure it to not match if the message The page cannot be found is returned. In order to use the - sign, you must make sure that there are no spaces between the - sign and the words to not match. So in the above example you would type in the pattern matching as -”The page cannot be found”

If you are looking for just a single word you could type in the pattern as -cannot. If you put a space between the - sign and the word, then it will be treated like a +.

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 Troubleshooting 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 Troubleshooting 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 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: OVIS is running on the same server as OVTA, but there is no probe data in the OVTA Console.

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, enable tracing in OVIS following the instructions in OVIS Tracing and Logging Files on page 376. Then check the `trace.measEvent2` trace file.

Multiple Users in the Configuration Manager

When you have multiple users logged into the Configuration Manager you can set the **File > Configure > Multiple User Options** to **Locking for concurrent changes**. Locking occurs when one user tries to add/update/delete an item when someone else already is accessing that item or a parent to that item that could potentially modify the same item. If this occurs, a dialog will display, letting you know that you can't add/update/delete the item because it is in use by someone else. Locking also applies to trying to save the configuration when someone else is saving. Note that if someone is using a wizard like the configuration wizard, a global lock is used so not much else can be done by any other user, and you can't open the configuration wizards while anyone else is modifying something. See Other Configuration Options on page 96 for details on Multiple User Options.

The default is not to use locking, which means that multiple users can be logged into the Configuration Manager and make changes concurrently that may result in changes being overwritten.

If you are trying to modify something that is currently locked, you should try again later or coordinate your changes with the user who is holding onto the lock. (The user ID will be displayed in the locking message). If this is not possible, you can turn off locking in the Multiple User Options dialog, which will release all of the locks. Note that the changes you made could potentially be overwritten by the user who had the lock, if he clicks OK in a dialog that does not contain your changes.

If you are locked out of the Multiple User Options dialog, you can release all of the locks by closing all instances of the Configuration Manager (`IopsConfig.exe`) and the batch configuration (`IopsLoad.exe`).

If this does not work, you can turn off locking in the registry. In the following key on the OVIS Management Server system `HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\Internet Services\CurrentVersion` change the `ConfigMgrShare` value to 2. To turn it back on, change the `ConfigMgrShare` value back to 1.

Probe Scheduling Considerations

Measurement Interval: Defines how often you want the probe to initiate the measurement for the service target. The default is 5 minutes (300 seconds). If this is left at the default of 300 seconds then the probe will execute every 5 minutes. This value is per network connection definition, so you could have different Measurement Intervals for different network definitions. The only thing to watch here is to be sure all the probes that are assigned to this network can complete within the interval allotted.

Request Timeout: This is the amount of time a particular probe is allowed to execute and return a measurement. If the probe cannot complete in this time, then the probe will be considered unavailable. So you want to make sure that this value is large enough for the probe to complete. Choose a larger value to be sure the probe is not stopped by the Scheduler. Then if the probe times out, it is likely a true problem accessing the target. Making this number large, has no effect on the measurements of the probe, nor will it hold up other probes. For example it you set it to 200 and the probe actually finishes in 20 seconds, then OVIS will move on to the next probe, it will not sit there for 200 seconds waiting.

Network Timeout: This is the time allotted for all the probes on this network. When this time limit is reached, any probes still running on this network, will be terminated. So you want to make sure that this value is large enough to accommodate all the probes assigned to this network.

Concurrency: This defines how many probes to run at a time on a network connection. If you have 20 probes assigned to this network and the concurrency is set to 4, then 4 will run at a time, until all are finished. This is a useful setting if you are running the HTTP_TRANS probe. Since this probe is resource intensive, it is better to configure it with a lower concurrency setting. This will ensure that the probe does not have to compete for resources, which can have the effect of taking longer to run than a user would actually experience. See the *OVIS Web Transaction Recorder Guide* for more on concurrency and probe resource use. Note the largest setting for concurrency is 256 and the default is 32.

See Probe Location, Timing and Scheduling on page 139 and Scalability Information on page 478 for more details on probe timing and resource usage.

Troubleshooting Tools

Perfstat

This script can be used to monitor the status of HP OpenView's performance tools. Its most common application is to find out the versions of HP OpenView software installed on the system. The most common options are -v, -a and -z.

Usage: perfstat [options]

Option	Function
-?	List all perfstat options.
-a	Display ALL performance information.
-c	Show system configuration information.
-d	Check datacomm services.
-e	Search for warnings and errors from performance tool status files.
-f	List of performance tool status files.
-l	List version of all library files used by performance tools.
-L	List extended version of all library files used by performance tools.
-p [remote Windows system name]	Process list.
-r	List performance tool registry data.
-s [remote Windows system name]	Display status of performance related services.
-S [remote Windows system name]	Display extended status of performance related services.
-t	Display last few lines of performance tool status files.

Option	Function
-v	List version information for performance tools.
-V	List extended version information for performance tools.
-w	Wait for user input at the end of program (keep window open).
-z	Zip performance status, registry data, and files.

OVIS URL Extensions

Test if Probe System can Post to OVIS Server

To see if a probe system can post to the OVIS Server run the following command:

```
http://<Ovis_Server>/HPOV_IOPS/isapi/measEvent2.dll?Refresh
```

It should return a **blank page** if successful, otherwise it will return an http error code.

List of Systems Where Probes are Distributed

To see the node ids that the OVIS Management Server is aware of, load the URL:

```
http://<Ovis_Server>/hpov_iops/isapi/
distribmgrext.dll?GetStatus
```

This will return a list of systems where probes are distributed; this includes the local probes on the OVIS Management Server and remote probes on other systems. If `GetStatus` does not work, then the distribution manager will not be able to send the configuration (`config.dat` and related files) to that system.

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
- Changing System Name
- Security
- Configuring and Changing Ports in OVIS
- TIPs Communications
- Firewalls: Returning Data Through the Firewall
- Configuring Communications Between Probe Systems and the Server
- Custom Reports
- Supported Databases
- Database Adjustment
- Database Backup
- Starting Over
- Recovering TIPs Databases
- 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:

- ANYTCP
- DHCP
- Dial-Up Networking
- DNS
- Exchange
- FTP
- HTTP
- HTTPS
- Web Transaction Recorder (HTTP_TRANS)
- E-mail (IMAP4, POP3, Mail Roundtrip, SMTP)
- ICMP (ping)
- LDAP
- NNTP (Newsgroups)
- NTP
- ODBC
- Radius
- SAP

- Script
- SMS
- SOAP
- Streaming media
- SYS_BASIC_WMI
- TCP Performance
- TFTP
- UDP Performance
- WAP
- Custom Probes

On the probe system, the OVIS 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 by the probe system using HTTP or HTTPS protocol.

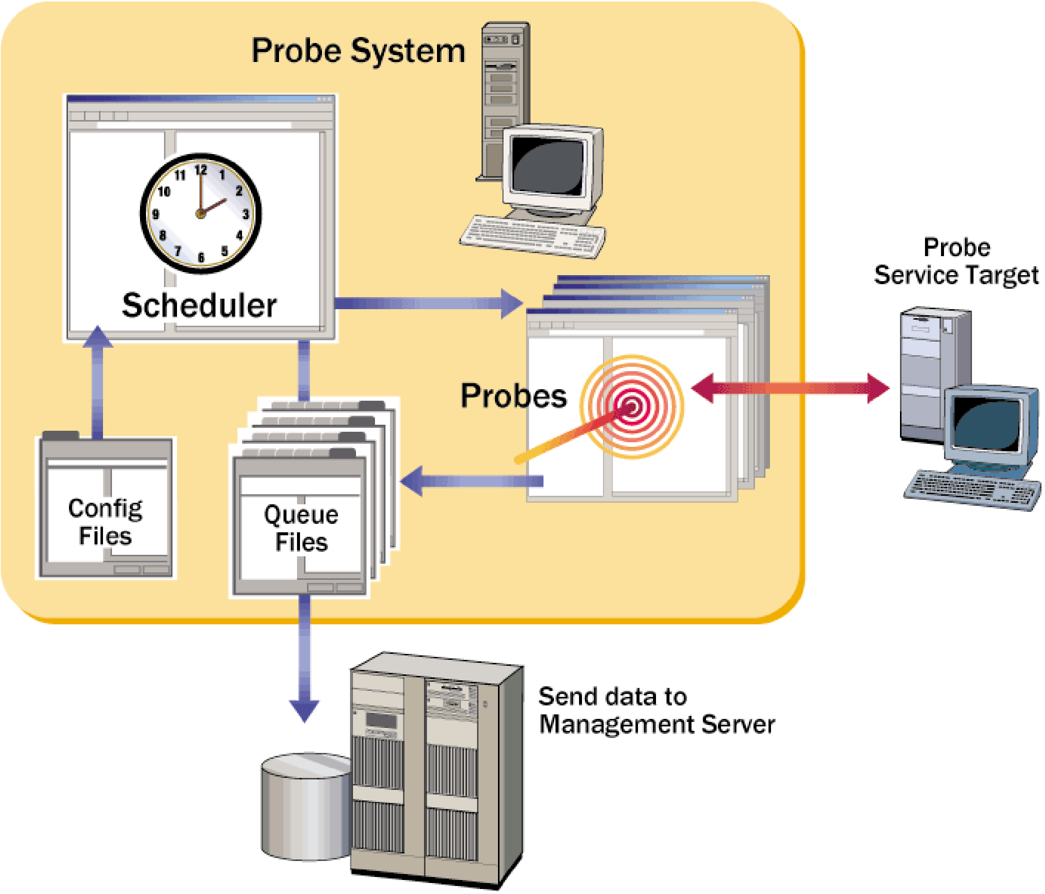


Figure 5 Data Diagram for the Probe Systems

Management Server

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

Periodically iopscollector runs and moves data from the IopsTraceTable to the Reporter database tables IOPS_DETAIL_DATA and IOPS_PROBE_DATA_CACHE.

Then iopsmaint aggregates data from the two tables above into hourly and daily weighted averages as follows:

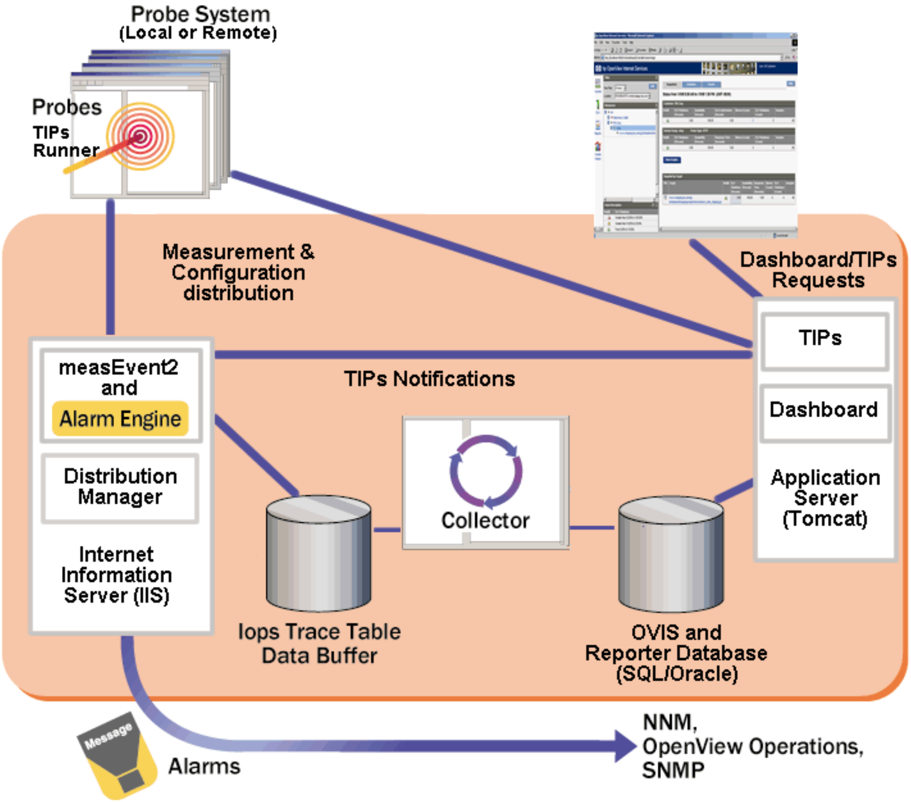
> IOPS_DETAIL_DATA for 5 minute probe/target level data, is aggregated into hourly and daily weighted averages for targets and stored in the following tables:
>
>> IOPS_DETAIL_DATA_HOURLY for hourly probe/target level data
>>
>> IOPS_DETAIL_DATA_DAILY for daily probe/target level data
>
> IOPS_PROBE_DATA_CACHE for 5 minute service group level data, is aggregated into hourly and daily weighted averages for service groups and stored in the following tables:
>
>> 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.

For information on the metrics in each of these data tables, select the **Graphs** button on the Snapshot page of the OVIS Dashboard. Then in the Graphs page, select the **Custom Graphs** button and then the **Help** button. The help topic provides links to data tables with the metric descriptions.

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.

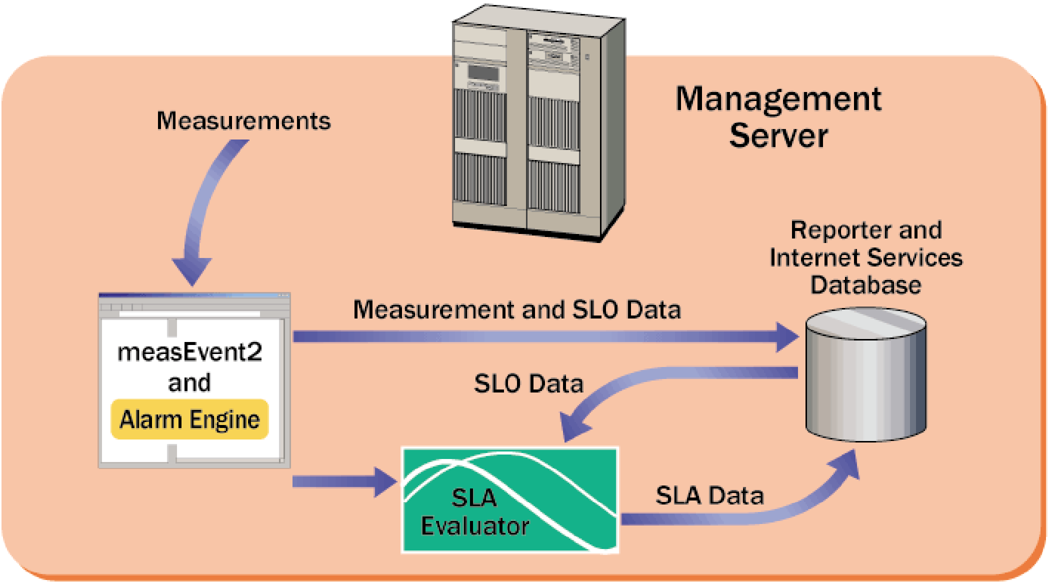


Figure 7 Data Diagram for Service Level Agreements

TIPs Components

Five components of the Troubleshooting Insight Packages (TIPs) are listed below to help you understand how TIPs works:

The *TIPs Server* is a web application in the Tomcat web server on the OVIS management server. When an alarm is detected in OVIS or you want information about a service target, TIPs submits a request for troubleshooting data, either automatically or on demand. The TIPs Action Processor on the TIPs server uses a dedicated port to forward requests for information to the TIPs Runners.

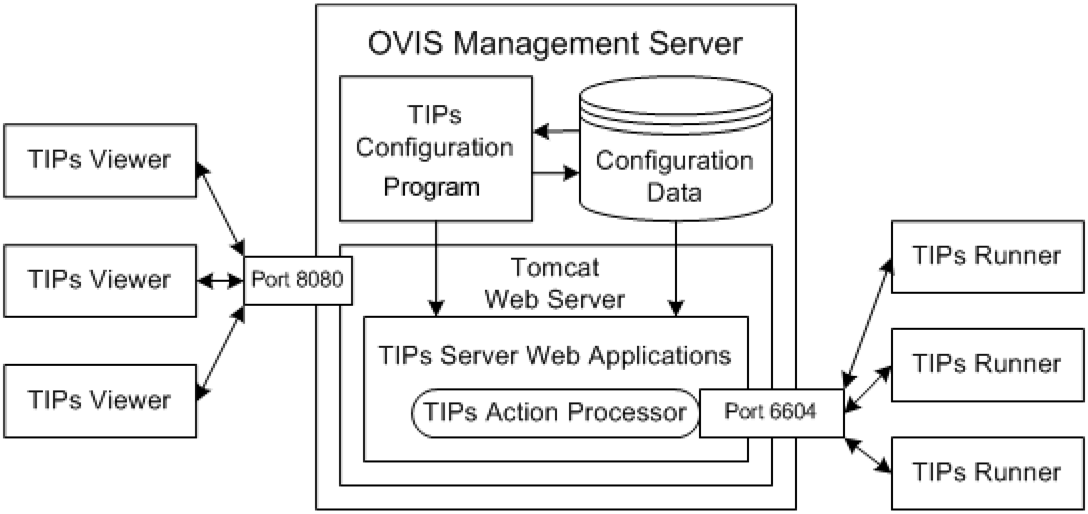
The *TIPs Configuration program* is installed on the OVIS management server. Administrators can use it to modify existing TIPs and commands and define new TIPs and commands.

TIPs Configuration Data is stored in a TIPs database on the server system.

A *TIPs Runner* resides on the OVIS management server and on each remote system where a probe package is installed. TIPs Runners execute troubleshooting commands and return results to the TIPs server.

TIPs Viewers are web clients that present the troubleshooting information you need to quickly resolve problems with your internet services. TIPs Viewers launch from the OVIS Dashboard.

Figure 8 Data Diagram for TIPs



A TIP is configured to run a command or set of commands when defined conditions are met. You can define conditions to control if a whole TIP runs. You can also define conditions to control if each command in a TIP runs. If a TIP runs, only the commands that pass the conditions assigned specifically to each one will run.

A local TIPs Runner is installed on the OVIS Management Server when OVIS is installed. Each remote TIPs Runner is installed and configured when you install the remote probe software. The TIPs Server sends requests for information to the TIPs Runner located on the probe system that monitors the service target or alarm in question.

See the TIPs Configuration program online help for more information about TIPs.

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>
```

```
iopsload -save config.sysname.xml
```

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

From a command prompt window, enter:

```
ovc -stop ovprobes
```

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.

Changing System Name

OVIS does not support changing the hostname or IP address on the Management Server.

If you need to change the system name or IP address on the OVIS Management Server, it is recommended that you install your OVIS Management Server on another system and run `ovisactivate` on every remote probe system to change to point to the new Management Server location.

If you want to change a remote probe system to send data to a different OVIS Management Server, run `ovisactivate` and enter the new host name in the dialog displayed.

If you change the system name of a probe system, then you need to update the probe location in the Configuration Manager for that probe, and save the configuration. The updated configuration will then be downloaded by the probe.

Security

Configuring Proxy/Port Settings

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

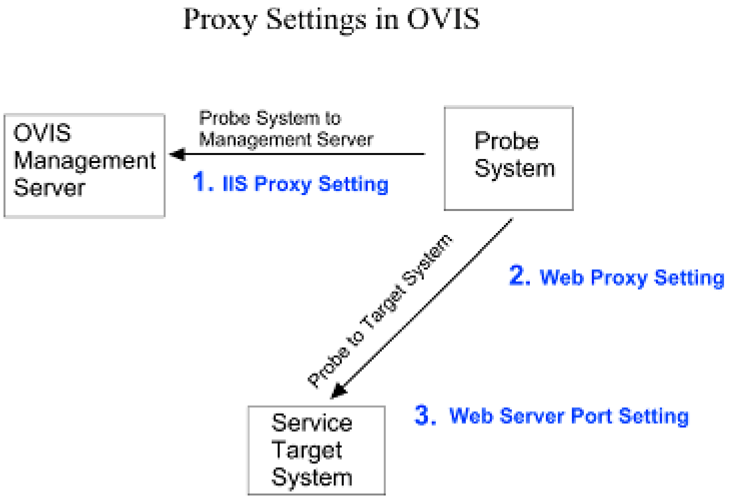
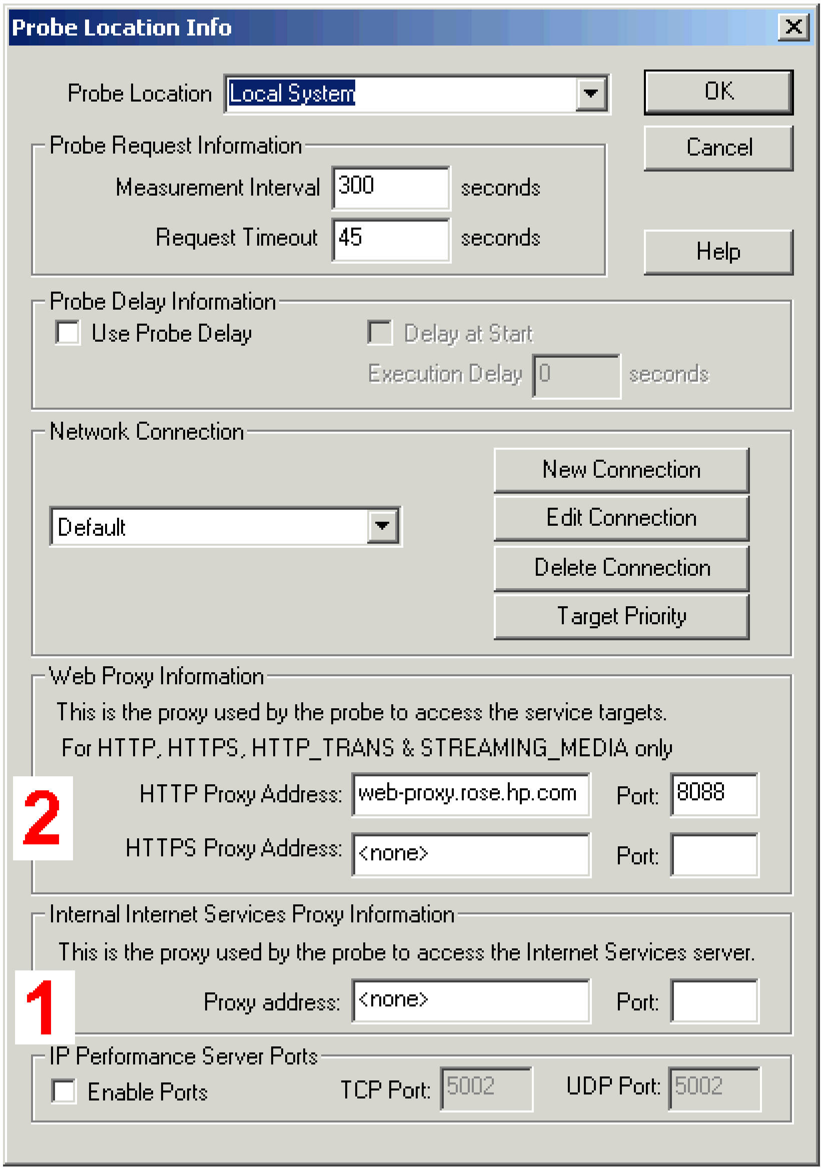


Figure 9 Proxy and Port Settings in Internet Services

The diagram shows the following:

1. You could have a proxy server 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 remote probe system can send and receive data from the OVIS Management Server.
2. You could have a proxy server 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.



Probe Location Info

Probe Location: Local System

Probe Request Information

Measurement Interval: 300 seconds

Request Timeout: 45 seconds

Probe Delay Information

□ Use Probe Delay

□ Delay at Start

Execution Delay: 0 seconds

Network Connection

Default

Web Proxy Information

This is the proxy used by the probe to access the service targets.

For HTTP, HTTPS, HTTP_TRANS & STREAMING_MEDIA only

HTTP Proxy Address: web-proxy.rose.hp.com Port: 8088

HTTPS Proxy Address: <none> Port:

Internal Internet Services Proxy Information

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

Proxy address: <none> Port:

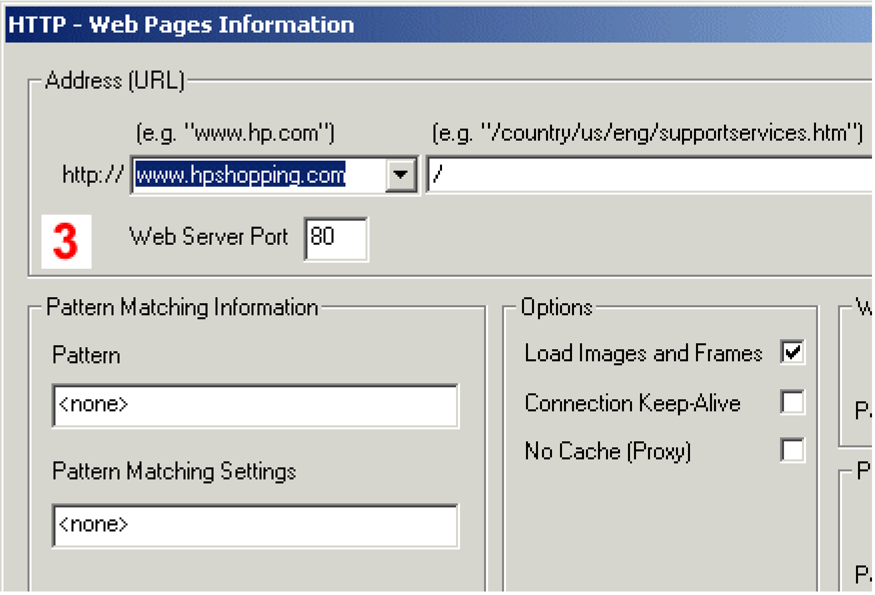
IP Performance Server Ports

□ Enable Ports

TCP Port: 5002

UDP Port: 5002

3 You can specify the port for an HTTP probe target system. It may have a different port than the default port 80 and you can specify this in the Configuration Manager HTTP -Web Pages Information dialog box.



HTTP - Web Pages Information

Address (URL)

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

http:// www.hpshopping.com /

3 Web Server Port 80

Pattern Matching Information

Pattern

<none>

Pattern Matching Settings

<none>

Options

Load Images and Frames ☑

Connection Keep-Alive □

No Cache (Proxy) □

How Internet Services Handles Security

Working with MS Internet Information Server (IIS), OVIS probes for data and stores the values it retrieves in a database. For OVIS to work with IIS in this way, the OVIS 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.

Configuring and Changing Ports in OVIS

The OVIS Management Server has multiple components that listen on TCP ports. If you use a firewall, these ports must be open for communication.

- Microsoft Internet Information Servers (IIS), handling probe to server communication and integration with other OpenView products
  - — Default port 80 (443 if SSL is enabled)
- Tomcat, handling the OVIS Dashboard and communication between the TIPs server and TIPs Viewer
  - — Default ports 8005 (Shutdown), 8009 (JK2) and 8080 (HTTP)
- TIPs port, for handling communication between the TIPs Server and TIPs Runners
  - — Default port 6604

The OVIS installation will prompt you to enter new ports for Tomcat if some of these default ports are already taken. Use `netstat -an` to see what ports are taken.

Changing the IIS Port or the Tomcat Ports

Special care should be taken in modifying the port numbers for an existing configuration with prior existing remote probes deployed. You should only select port numbers that exist or that you will be able to use for the OVIS Management Server. Changing the server port to a port that the OVIS server will not be able to communicate on will cause the remote probe systems to be unable to communicate or send measurements back to the OVIS Management Server.

IIS Port Change

The IIS port can be changed in the Microsoft Internet Information Services (IIS) administration utility (**Control Panel > Administration Tools > Internet Information Services**). After changing the IIS port, the change also needs to be reflected in the Configuration Manager, see the Example of Changing the IIS Port on page 448.

Tomcat Port Changes

Coexistence issues resulting in port conflicts can occur with other OpenView products such as NNM, OVPM or Reporter on the same system as the OVIS Management Server. To resolve these issues you can change the Tomcat (Dashboard) ports. Use `OvTomcatCtl.vbs` script to change the Tomcat ports after installation (note that the ports used below are just an example):

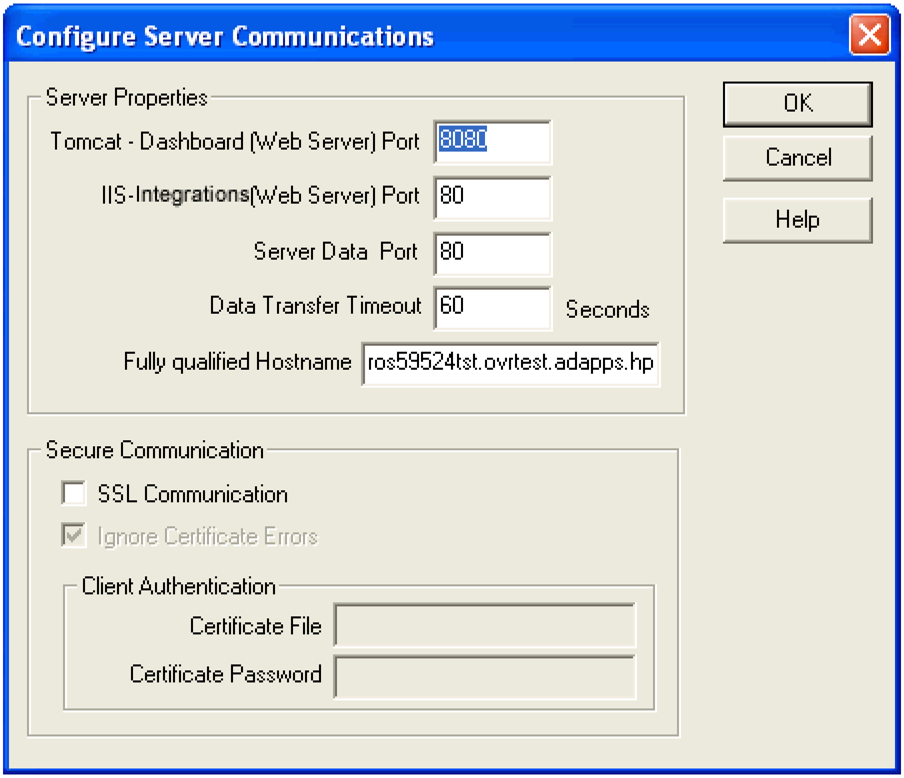
```
cd <installdir>\bin

ovc -stop ovtomcatA

cscript /nologo OvTomcatCtl.vbs -setshutdownport 9005

cscript /nologo OvTomcatCtl.vbs -sethttpport 9080

cscript /nologo OvTomcatCtl.vbs -setjk2port 9007

ovc -start ovtomcatA
```

To see what is currently configured for Tomcat, execute:

```
cscript /nologo OvTomcatCtl.vbs -getconf
```

Configure IIS and Tomcat Port Changes in Configuration Manager

After making changes to IIS and/or Tomcat ports, some of the ports must also be re-configured in the OVIS Configuration Manager (**File > Configure > Web Server Properties**).



Configure Server Communications

Server Properties

Tomcat - Dashboard (Web Server) Port: 8080

IIS-Integrations(Web Server) Port: 80

Server Data Port: 80

Data Transfer Timeout: 60 Seconds

Fully qualified Hostname: ros59524tst.ovrtest.adapps.hp

Secure Communication

☐ SSL Communication

☑ Ignore Certificate Errors

Client Authentication

Certificate File:

Certificate Password:

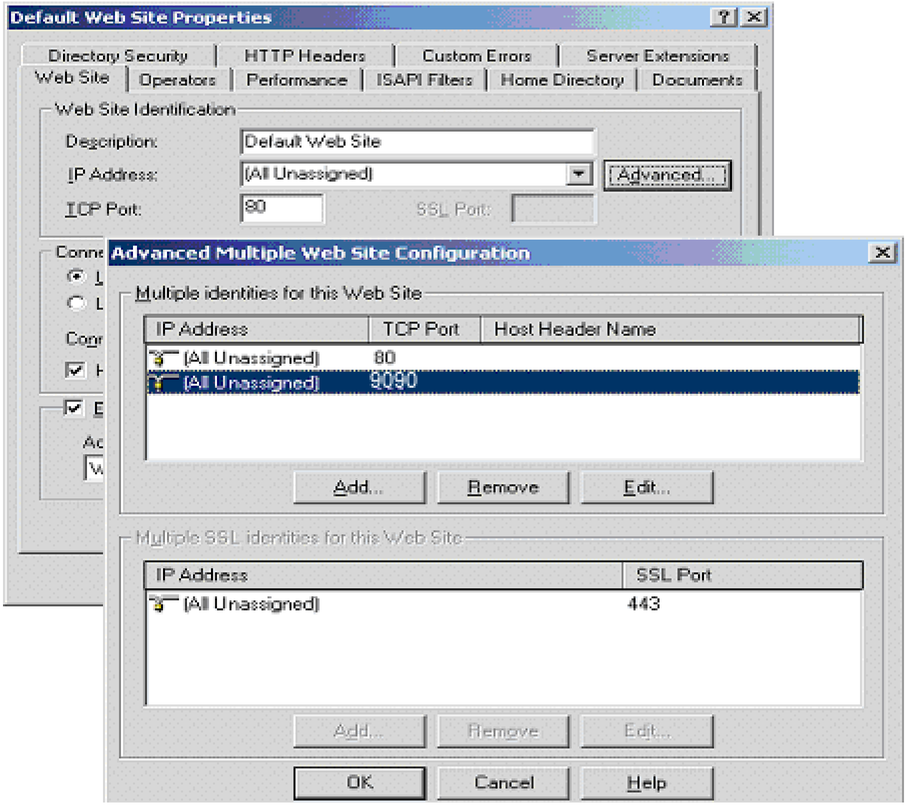
The Tomcat - Dashboard (Web Server) Port must correspond to the Tomcat HTTP port.

The IIS - Integrations (Web Server) port and Server Data Port must correspond to the ports where IIS is running.

Example of Changing the IIS Port

An example of the steps for changing the IIS port are shown below (the order in which you do these steps is very important):

1 Using IIS, go to the Default Web Site Properties dialog and select the **Advanced** button. Add the new server port you want to use instead of the current default. BE SURE NOT TO DELETE THE OLD/EXISTING DEFAULT PORT (in the example below you see both Port 80 and Port 9090). Save the change.



Description: Default Web Site

IP Address: (All Unassigned)

TCP Port: 80

SSL Port:

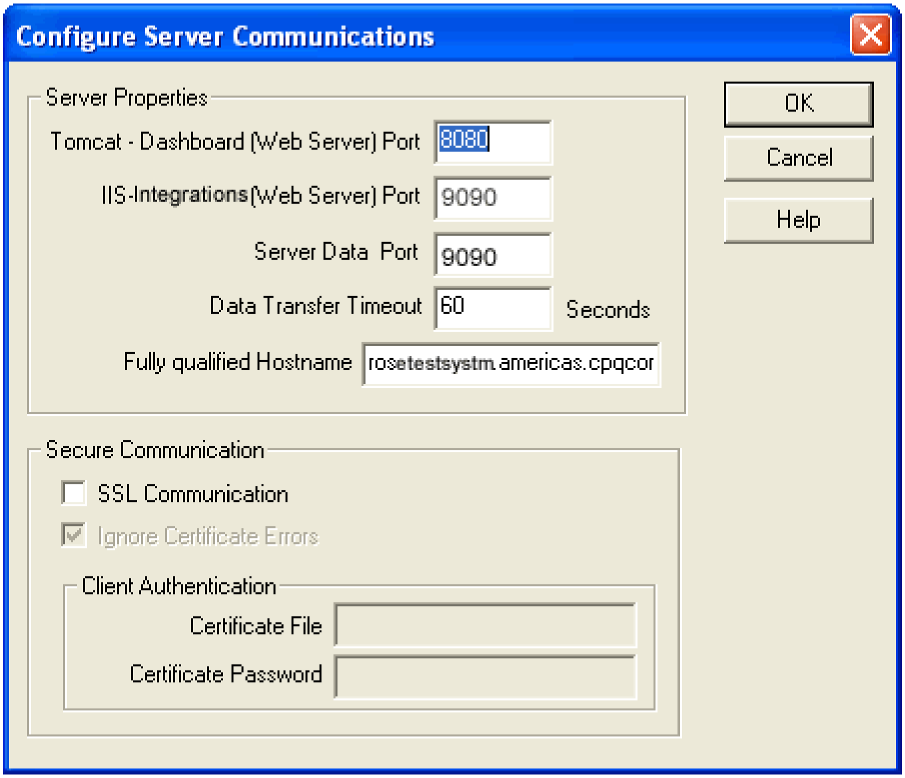
Multiple identities for this Web Site

IP Address	TCP Port	Host Header Name
(All Unassigned)	80	
(All Unassigned)	9090	

Multiple SSL identities for this Web Site

IP Address	SSL Port
(All Unassigned)	443

2 Change the Server Data port using the OVIS Configuration Manager **File > Configure > Web Server Properties** dialog box. See the online help for the **File > Configure > Web Server Properties** dialog for details.



Configure Server Communications

Server Properties

Tomcat - Dashboard (Web Server) Port 8080

IIS-Integrations (Web Server) Port 9090

Server Data Port 9090

Data Transfer Timeout 60 Seconds

Fully qualified Hostname rosetestsystm.americas.cpqcor

Secure Communication

□ SSL Communication

☑ Ignore Certificate Errors

Client Authentication

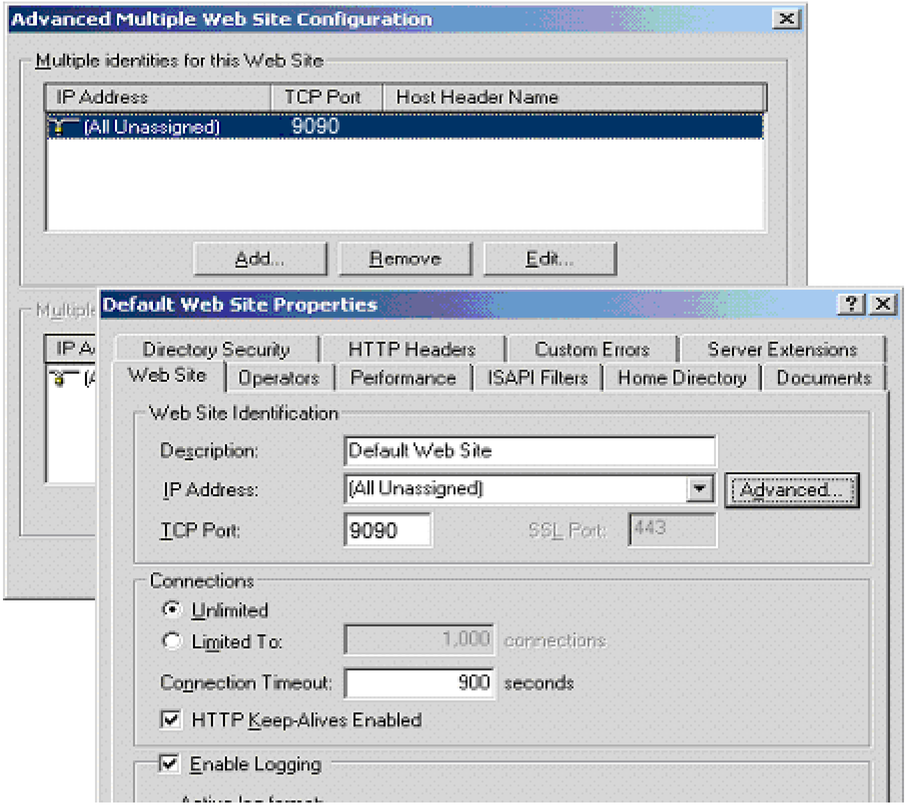
Certificate File

Certificate Password

3 Save and wait for the updated configuration to be deployed to local and remote probe systems. Use the Configuration Manager Status display to be sure all probe systems received the update (all systems are green).

4 Then be sure any remote probe systems are configured to use the new port number.

5 On the OVIS Management Server, return to the IIS Default Web Site Properties dialog box and select the **Advanced** button. Remove the old port if it is no longer needed. Press the **OK** button. Then in the Default Web Site Properties dialog box, set the TCP port to the new port you added above. Save the changes. IIS requires a restart of the service once you make the change.



IP Address	TCP Port	Host Header Name
(All Unassigned)	9090	

Description: Default Web Site

IP Address: (All Unassigned)

TCP Port: 9090 SSL Port: 443

● Unlimited

○ Limited To: 1,000 connections

Connection Timeout: 900 seconds

☑ HTTP Keep-Alives Enabled

☑ Enable Logging

Changing the TIPs Port

In addition to changing the IIS and OVIS Tomcat ports, you can change the port number that the TIPs Server and TIPs Runners use to communicate. The default port is 6604.

See the TIPs Configuration program online help for more information.

To view the current default TIPs Runner port, execute this command in a command window on the TIPs Runner system:

```
Windows: <install_dir>\bin\ovtiprn -retrieve port
```

```
UNIX: /opt/OV/bin/ovtiprn -retrieve port
```

Note that if you change the port number for a TIPs sever system, you must also change the port number for all the TIPs Runner systems that are registered with that TIPs server.

To change the port number for the TIPs Server and the local TIPs Runner:

1 On the TIPs Server system, stop the TIPs Server by executing this command in a command window:

```
<install_dir>\bin\ovc -stop ovtomcatA
```

2 On the TIPs Server system, stop the TIPs Runner by executing this command in a command window:

```
<install_dir>\bin\ovc -stop ovtiprn
```

3 On the TIPs Server system, change the TIPs Server port number by executing this command in a command window:

```
<install_dir>\bin\OvTIPsServer.bat -port <port number>
```

4 On the TIPs Server system, change the TIPs Runner port number by executing this command in a command window:

```
<install_dir>\bin\ovtiprn -replace <host name> <port
number>
```

➤ The *<host name>* for this command is the name of the TIPs Server system where the TIPs Runner is installed.

5 On the TIPs Server system, start the TIPs Server by executing this command in a command window:

```
<install_dir>\bin\ovc -start ovtomcatA
```

6 On the TIPs Server system, start the TIPs Runner by executing this command in a command window:

```
<install_dir>\bin\ovc -start ovtiprn
```

To change the port number for each remote TIPs Runner:

1 On *each* remote TIPs Runner system, stop the TIPs Runner by executing this command in a command window:

Windows:

```
<install_dir>\bin\ovc -stop ovtiprn
```

UNIX:

```
/opt/OV/bin/ovc -stop ovtiprn
```

2 On *each* remote TIPs Runner system, change the TIPs Runner port number by executing this command in a command window:

Windows:

```
<install_dir>\bin\ovtiprn -replace <host name> <port
number>
```

UNIX:

```
/opt/OV/bin/ovtiprn -replace <host name> <port number>
```

➤ The <*host name*> for this command is the name of the TIPs Server system where the TIPs Runner is registered.

3 On *each* remote TIPs Runner system, start the TIPs Runner by executing this command in a command window:

Windows:

```
<install_dir>\bin\ovc -start ovtiprn
```

UNIX:

```
/opt/OV/bin/ovc -start ovtiprn
```

TIPs Communications

The TIPs Server communicates with multiple TIPs Runners and TIPs Viewers.

- Communication between the TIPs Server and TIPs Runners serves the purpose of gathering troubleshooting information.
- Communication between the TIPs Server and TIPs Viewers serves the purpose of displaying the requested troubleshooting information.

TIPs Runners

A local TIPs Runner is automatically installed with the local OVIS probe when OVIS is installed. During the installation, configuration settings are automatically applied.

A remote TIPs Runner is installed with each remote OVIS probe when you use the OVIS remote probe installation package. Remote TIPs Runners are configured with the OVIS probe.

There are TIPs Runner parameters that you may want to change. See the TIPs Configuration program online help for information on configuring TIPs Runners.

TIPs Secure Communications

The TIPs Server communicates with local and remote probe systems and TIPs Runners. The default communication is standard HTTP protocol. TIPs communication is more secure when you use SSL certificate based communication.

If you choose to use secure communication, the TIPs Server and all the TIPs Runners communicating with that TIPs Server must run in secure mode.

See the TIPs Configuration program online help for how to enable secure communication between the TIPs Server and TIPs Runners.

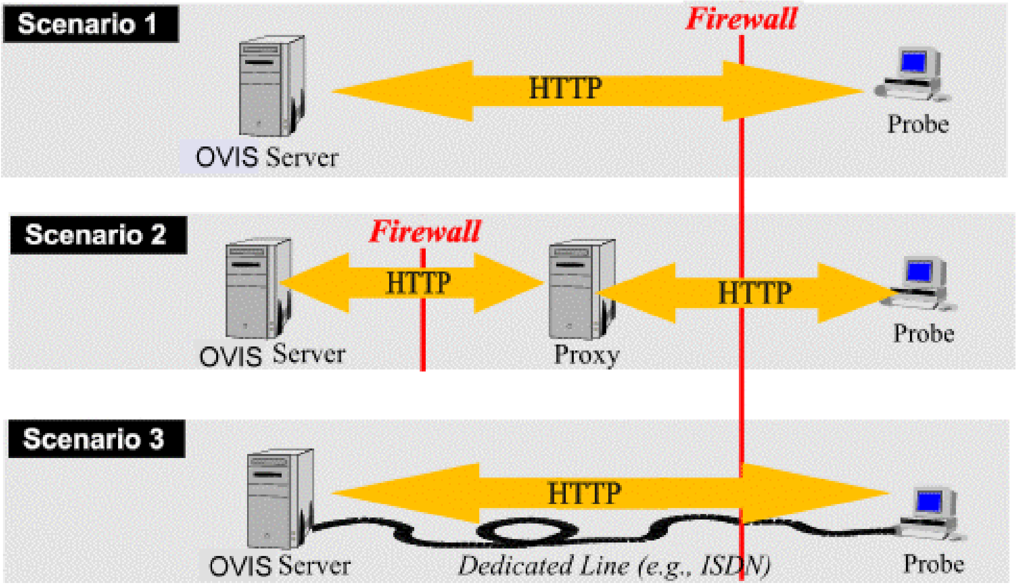
Firewalls: Returning Data Through the Firewall

Internet Services probes use standard HTTP protocol to send measurements to the OVIS Management Server. Probes send HTTP POST requests, using port 80 on the OVIS Management 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 OVIS Management 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 Management 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 on page 432 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, the OpenView integrations web server port, 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.

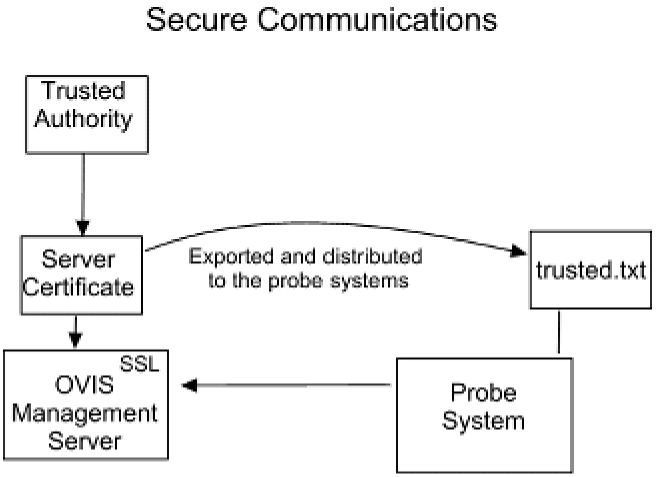
➤ The TIPs Server communicates with local and remote probe systems and TIPs Runners. The default communication is standard HTTP protocol. TIPs communication is more secure when you use SSL certificate based communication.

If you choose to use secure communication, the TIPs Server and all the TIPs Runners communicating with that TIPs Server must run in secure mode.

See the TIPs Configuration program online help for information on Enabling Secure Communication in TIPs (the process is different than in the following section for OVIS).

Configuring Secure Communication

OVIS 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).

   ```
   ovc -stop ovprobes
   ```

2. Set up the OVIS Management Server as a secure web server (see Microsoft Internet Information Services (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 the pending request and install the 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 for the OVIS Management Server 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 `<datadir>\conf\probe` directory (create it if it is not present).

6. In the OVIS 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 OVIS services on each probe location (local and remote).
   ```
   ovc -start ovprobes
   ```
9. In the OVIS 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):
   ```
   ovc -stop ovprobes
   ```
2. Create client certificate and be sure it is Base64 encoded X.509 format. Then be sure it is installed in the `<datadir>\conf\probe` 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 OVIS 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 the correct location (`<datadir>\conf\probe\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 OVIS Configuration Manager, **File > Configure > Web Server Properties** dialog enter the certificate file name 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 OVIS services on each probe location (local and remote).
```
ovc -start ovprobes
```

8 In the OVIS 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.

Exporting Certificates

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 as described below.

1 Run the command `openssl.exe pkcs12 -in <filename.pfx> -out <somename.txt>` from a command prompt.

2 After that, enter the **Import Password**. This is the password that goes with the certificate.

3 Next enter a **PEM pass phrase**, and then verify it. This password can be anything you want it to be, but remember this password, because you will need it when you configure your HTTPS probe and SSL Server communication.

4 After you verify the PEM password, you should now see a text file with the name you specified in the `openssl` command. The last step is to copy the `.txt` file to the `<data dir>\conf\probe` directory. It must be there in order for the probe to work.

5 Everything should be all set now, and the last thing to do is configure the HTTPS probe and SSL Server communication. In the bottom right of the HTTPS Service Target configuration dialog box in the OVIS Configuration Manager, where it asks for **Certificate File Name**, this is the text file you moved to the `<data dir>\conf\probe` directory (remember, this file must be in the `<data dir>\conf\probe` directory in order for this to work). And then where it asks for the **Certificate Private Key Password**, this is the PEM password you entered after issuing the `openssl.exe` command.

Upgrades from OVIS 4.5, 5.0, 5.20 to OVIS 6.0

When upgrading from OVIS version 4.5, 5.0, 5.20 to OVIS 6.0, you must move any configured `trusted.txt` or `ClienCert` files in the `<install dir>\probes` directory to the new certificate location `<data dir>\conf\probe`.

Custom Reports

If you want to create custom reports for your custom probes, you need to use Crystal Decisions Crystal Reports version 10.0 or higher (www.crystaldecisions.com) and the hp OpenView Reporter product version A.03.60 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 OVIS. 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:

   ```
   REPORT = IOPS_<probe name>
   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 workspace of the OVIS Dashboard.

Supported Databases

OVIS and OpenView 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 Microsoft 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 *OVIS Reporter Database Configuration Guide* also has information on database performance.

The default database for OVIS is 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 9.2 for Solaris or HP-UX
- SQL Server 2000

The database can be either local or remote. MSDE database is on the same system as the OVIS Management Server. SQL Server can be on the same system as the OVIS Management Server or it can be on a remote Windows system. Oracle will be on a remote UNIX system.

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 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. You can later use instructions in the *OVIS Reporter Database Configuration Guide* provided with OVIS to configure an Oracle 8.1.7, 9.2 or SQL Server 2000 database instead.

WARNING: Migration of data from your old database to the new database is not supported for Internet Services. And if 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 Adjustment

The `<install dir>\bin\ovisdbclean` tool aides in adjusting the database to remove data records. For example, if it wasn't possible to use the Scheduled Downtime feature, this tool can be used to delete some data out of the database so that it will appear like a scheduled downtime.

Please note that due to the various aggregation mechanisms, the `ovisdbclean` tool works best if a daily summarization hasn't happened yet. The daily summarization is scheduled at 2 am every night.

Also please note that the `ovisdbclean` tool will only show and delete records with less than 100% availability. If a record in the selected time range is 100% available, the application will not be able to delete this record.

In the `ovisdbclean` tool, you can select either a time range or a customer, probe location, service group or service target and a specific time range. Once you've clicked on Query and verified the data records listed are the ones you want deleted (be sure to check each tab), you can check the box **Mark for Deletion** (be sure to check the Mark for Deletion box for each tab where you want data deleted). If records you don't want deleted are listed in the query, try selecting a narrower time range.

The `ovisdbclean` tool removes data (where availability is NOT 100%) from the major data tables that contain measurements (IOPS_DETAIL_DATA, IOPS_DETAIL_DATA_HOURLY, IOPS_DETAIL_DATA_DAILY, IOPS_PROBE_DATA_CACHE, IOPS_PROBE_DATA_HOURLY, IOPS_PROBE_DATA_DAILY), alarm information (IOPS_ALARM_DATA2) and SLO/SLA data (IOPS_SLA_CONFORMANCE_DATA and IOPS_SLO_CONFORMANCE_DATA).

It is highly recommended to verify the data before starting the deletion. Once deleted, it is very difficult to bring back the data. An audit trail with the deleted data is written to `<Data Dir>/Data/Datafiles/ovisdbclean`. The directory contains subdirectories with the date and time when the data was deleted.

Once a table is marked for deletion (or update) the following happens:

Delete: The record is deleted from the database.

Update: If the time range doesn't fall on the full hour/day, the record is updated by setting the group count to the availability count. This is done since some of the data points have already been summarized. For example, if the time range is set to 9:30 to 11:30, the application will update hourly records 9:00 and 11:00 and delete the 10:00 record. The update for 9:00 and 11:00 will set the count field to the availability field which in effect sets the whole hour to 100% availability. Because of this, it is recommended to set the time range to full hours.

Please refer to the online help for the `ovisdbclean` tool for details on usage.

Database Backup

We recommend that you backup the Reporter database used by OVIS.

1. First stop the following services:
   - Reporter Service
   - HP Internet Services Service
   - World Wide Web Publishing Service
2. Then backup the database according to your usual procedures.

Some suggested procedures are provided below for MSDE.

For the default database

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

Option #1, for MSDE using SQL Client tools:
If SQL 2000 Client Tools are installed, use SQL Enterprise Manager to back up you MSDE database.

Option #2, for MSDE without 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 OVIS use MSDE as the default database.

Restarting other products running the reporting services

THIS PROCEDURE RESTARTS OTHER PRODUCTS RUNNING THE REPORTING SERVICES. IF YOU HAVE REPORTER 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. This command will also save the `httptrans.dat` file as well.

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` and `Newiops.exe` programs 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 **Start > 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 Login 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 **Start > Settings > Control Panel > Services** and restart Internet Services components:

- a Reporter Service
- b HP Internet Services
- c World Wide Web Publishing Service

Recovering TIPs Databases

If your TIPs data is corrupted, you can recover the TIPs database if you have created backup files. See the TIPs Configuration program online help for how to create backup files. The steps to recover data from backup files is also included here, in case you cannot access the online help.

➤ The TIPs and Commands that are provided by HP can be recovered at any time by importing the TIPs definitions file that contains those TIPs and Commands. See the TIPs Configuration program online help for how to import and export TIPs definitions.

If you choose to recover data from your most recent backup files, remember that the data you recover will be the same as it was at the time when you did the backup.

Your TIPs database may be corrupted if you see the following behavior:

- You observe database errors in the TIPs Viewer.
- You observe database errors in the TIPs Server log.
- The TIPs Configuration program cannot start.

Verify the TIPs Databases

Verify the following three TIPs databases:

- TIPs Definitions Database
- TIPs Triggered by Alarm Database
- TIPs Authentication and TIPs Runner Registration Database

To verify the TIPs definitions database, complete the following steps:

1 On the TIPs Server system, dump the TIPs definitions database by executing this command in a command window:

Windows:

```
<install_dir>\contrib\OvTIPsDumpDB TIP
```

2 Review the output. If the database is not corrupted, you will see a list of configured TIPs. If the database is corrupted, you will see an exception or error message.

To verify the TIPs Triggered by Alarm database, complete the following steps:

1 On the TIPs Server system, dump the TIPs Triggered by Alarm database by executing this command in a command window:

Windows:

```
<install_dir>\contrib\OvTIPsDumpPregather
```

2 Review the output. If the database is not corrupted, you will see a list of saved Triggered by Alarm results. If the database is corrupted, you will see an exception or error message.

To verify the TIPs authorization and TIPs Runner registration database, complete the following steps:

1 On the TIPs Server system, dump the TIPs authorization and TIPs Runner registration database by executing this command in a command window:

Windows:

```
<install_dir>\contrib\OvTIPsDumpSrvltDB TIPRunner
```

2 Review the output. If the database is not corrupted, you will see a list of registered TIPs Runners. If the database is corrupted, you will see an exception or error message.

Recover the TIPs Databases

When you reinitialize the TIPs database, you lose all Triggered by Alarm data, TIPs definitions, TIPs Runner registrations, and authorization information. You can recover this information if you have created backup files.

To Reinitialize the Database:

1 In a command window, execute this command to stop the local TIPs Runner:

```
<install_dir>\bin\ovc -stop ovtiprn
```

2 In a command window, execute this command to stop the TIPs Server:

```
<install_dir>\bin\ovc -stop ovtomcatA
```

3 Delete all the files in this directory:

```
<data_dir>\datafiles\tips\database
```

4 In a command window, execute this command to recreate the databases:

```
<install_dir>\bin\OvTIPsCreateDB
```

5 If you are going to recover data, skip this step and go to the appropriate data recovery topic below.

If you are not going to recover any data, in a command window, execute this command to restart the TIPs Server:

```
<install_dir>\bin\ovc -start ovtomcatA
```

6 If you are going to recover data, skip this step and go to the appropriate data recovery topic below.

If you are not going to recover any data, in a command window, execute this command to restart the local TIPs Runner:

```
<install_dir>\bin\ovc -start ovtiprn
```

⚠ The TIPs Server and local TIPs Runner must be stopped if you want to recover data.

You can recover the following data with your backup data files: TIPs definitions, Triggered by Alarm data, TIPs Runner registrations, and authentication information.

To Recover Your Most Recent Backup Data Files

1 *Optional*. From your system backup files, retrieve the following files to recreate your TIPs definitions database:

```
TIPs.btx
```

```
TIPs.btd
```

Place these files in the following directory:

```
<data_dir>\datafiles\tips\database
```

2 *Optional*. From your system backup files, retrieve the following files to recreate your Triggered by Alarm database:

```
Pregather.btx
```

```
Pregather.btd
```

Place these files in the following directory:

```
<data_dir>\datafiles\tips\database
```

3. *Optional*. From your system backup files, retrieve the following files to recreate your authorization and TIPs Runner registration database:

```
TIPsAuth.btx
```

```
TIPsAuth.btd
```

Place these files in the following directory:

```
<data_dir>\datafiles\tips\database
```

4. In a command window, execute this command to restart the TIPs Server:

```
<install_dir>\bin\ovc -start ovtomcatA
```

5. In a command window, execute this command to restart the local TIPs Runner:

```
<install_dir>\bin\ovc -start ovtiprn
```

⚠ The TIPs Server and local TIPs Runner must be stopped if you want to recover data.

To Recover Your TIPs Definitions by Importing Your XML File

1. Import your exported TIPs definitions file. See the Configuration program online help for information on importing and exporting TIPs definitions.
2. In a command window, execute this command to restart the TIPs Server:

```
<install_dir>\bin\ovc -restart ovtomcatA
```

3. In a command window, execute this command to restart the local TIPs Runner:

```
<install_dir>\bin\ovc -restart ovtiprn
```

Scalability Information

OVIS performance and scalability can be examined in the following areas:

- Probe Systems
  - What hardware resources are required?
  - How many targets can be executed per probe system?
  - How many different probe systems are required?
  - Are dedicated probe systems needed or can machines in use for other tasks be used as probe systems?
  - Do different probe types have different probe system resource requirements?
- Network Bandwidth
  - How much data is transferred between the probe systems and the probe target?
  - How much data is transferred between the probe systems and the Management Server per target?
  - What probe system configuration settings govern the amount of data transferred?
- Management Server System
  - What hardware resources are required?
  - What is the optimum database configuration?
  - Data processing, storage, and collection
    - How many probe systems / targets can be processed by a single Management Server?
    - What settings impact data processing throughput at the Management Server?
  - Database sizing and access
    - What configuration settings govern the size of the database?
    - How much data can be stored in the database before dashboard responsiveness is noticeably impacted?

  - How much data can be stored in the database before report generation and database maintenance/summarization times are noticeably impacted?

Probe System

An OVIS probe system performs the following tasks:

- Schedules probes for execution
- Executes probes based on scheduling policy
- Forwards the probe results to the OVIS Management Server

In addition to the size and available processing capacity on the probe system, the following factors and configurable settings determine the maximum number probe targets that a single probe system can accommodate:

- Service targets configured per probe system.
- Service target availability - unavailable service targets cause probes to timeout, slowing the succession of sequentially executed probes.
- Probe interval - shorter intervals reduce the time window in which sequentially executed probes can complete.
- Probe timeout - longer timeouts can slow the succession of sequentially executed probes.
- Probe delay - if delays are specified between probe executions, fewer probes can be executed within a single measurement interval.
- Local or remote probe system location - probes accessing targets over slow network connections will take longer, be more likely to timeout, and can therefore slow the succession of sequentially executed probes.
- Concurrent requests - by default up to 32 probes can be executed in parallel. A higher concurrency can enable more probes to execute within a single probing interval; however, a high number of parallel probe executions can likewise result in high system resource consumption on the probe system.

Calculating the Number of Probes Systems Required

The following formula provides a starting point for determining the number of probe systems required:

```
Probe Systems =
((targets / concurrency) * (timeout + delay)) / interval
```

Concurrency = the number of targets allowed to run concurrently

Timeout = the target timeout value in seconds

Delay = the Probe Delay value in seconds if configured in the Probe Location dialog. Default is not set so the value is zero by default.

Interval = the polling interval in seconds

This formula assumes a worst-case probe execution time where all probes timeout. The result of this formula can be rounded up to the next integer value to arrive at a starting point for determining the number of required probe systems.

Examples

In the following environment, it would take 1 probe system to run 100 targets in a five minute interval with a 20 second per target timeout. Note the resultant value of 0.21 is rounded up to 1 probe system required.

```
targets          = 100
concurrency      = 32
timeout          = 20  (seconds)
delay            = 0   (seconds)
interval         = 300 (seconds)
Probe Systems    = (100 / 32) * (20 + 0) / 300
                 = .21
                 = 1 probe system
```

In the next example, the formula is used a little differently to find out how targets can be executed on a single probe system given the other probe configuration settings.

```
probe systems    = 1
concurrency      = 32
timeout          = 20  (seconds)
delay            = 0   (seconds)
interval         = 300 (seconds)
1 Probe System   = (targets / 32) * (20 + 0) / 300
```

```
                = (targets / 8) * 5 / 300
   5 targets   = 8 * 300
     targets   = 480
```

Calculating the Number of Targets Each Probe System Can Execute

The formula in the prior section provides a starting point in that it assumes all probes will execute for the total timeout duration. More importantly, these formulas do not consider the system resource consumption requirements needed by the probes themselves when executing. The resource requirements on the probe system are impacted by the following settings:

- Probe Type - the HTTP_TRANS probes are more resource intensive than the other probe types, especially when there are a large number of steps per transaction sequence. This is because the steps are executed one after the other with little or no think time delays between steps. When many such transactions are executed in parallel, CPU utilization can be high. Moreover, each probe execution requires a process needing approximately 3-20 Mbytes of memory (the IE mode requiring more than the non-IE mode).

  ➤ Non-IE mode can use more CPU time because the probe does not delay (no think time) between each step. A large number of steps can result in CPU spikes, especially when the target steps return results quickly. Memory usage for non-IE mode probes is approximately 3-5 K of resident memory per transaction. IE mode uses less CPU time for the probe itself because the IE mode probe pauses for 1.5 seconds between each step. 1.5 seconds is the default waittime setting (1500 milliseconds) and is configurable. IE mode can, however, use more CPU time when the rendered page contains many client-side browser controls and logic that executes in the browser itself (such controls would not actually execute in the non-IE mode probe). Memory usage for non-IE mode probes is approximately 10-15 K of resident memory per transaction and can vary depending on the type of content rendered in the downloaded page.

  If a probe system is dedicated for OVIS probes, attention needs to be given to the number of parallel executions. If the number saturates system and memory resources such that the probes themselves are starved, the probes will timeout and fail to execute to completion. If HTTP_TRANS probes are executed on a probe system that is also used for other computing tasks and applications, equal attention needs to be given to the number of parallel executions to ensure the additional resource usage of the probes do not negatively impact these other computing functions.

In general, the default concurrency value of 32 is high for HTTP_TRANS probes having more than 5 steps in each sequence. In such environments with many HTTP_TRANS targets, a concurrency value of ten or less is more appropriate. When in doubt, monitor the probe system with performance tools to assess the impact of the probes and whether or not the probes are able to complete in the allotted intervals.

- Concurrency and Number of Targets - all probe types run as processes and use system resources so there is a limit to the number of probe targets that can be executed per interval and in parallel. The probe system can be monitored with performance tools to assess the impact of the probes and whether or not the probes are able to complete in the allotted intervals.
- Interval and delay - If a probe system is executing a large number of targets, longer probe intervals with longer delays between probe executions can also lessen the demand for resource requirements on these systems. You can also use concurrency and priority for this.
- If probes spend a significant amount of time waiting for responses from the target, the overall cycle time can be decreased significantly by increasing the concurrency. Conversely, short probe wait times from fast/ responsive targets increase processing requirements on the probe system with a high concurrency value.

It is difficult to publish hard figures for the number of targets per probe system and the number of probe systems required. In addition to the above configuration variables, the right values are dependent on the overall size and processing power of the probe system as well as spare capacity available on these systems when they are hosting other applications.

If probe location is not important in terms of the physical location of the probe system, avoid using the Management Server as a "local probe" system unless it is a small OVIS deployment with excess Management Server capacity. In most cases where probe location is not important, it is still best to use a remote probe system separate from the OVIS Management Server to prevent probe activities from competing with Management Server functions for available resources.

Network Bandwidth

Probe System to Target

The formula for computing the number of bytes transferred per second between any given probe system and probe target systems is straightforward:

```
Bytes Transferred Per Second =
(targets per interval * bytes transferred per target) /
interval secs
```

The sum of this result for all probe systems provides the total bytes transferred per second in the OVIS managed environment each interval.

The bytes transferred per target will vary depending on the probe type and the specific target. In general, the HTTP, HTTP_TRANS, SOAP, FTP, NNTP, STREAM_MEDIA, EXCHANGE, SMTP, and POP3 probe types transfer the largest payload per probe execution. During configuration of these probes, the size of the target should be fairly well understood. In an HTTP probe, for example, the size of the target in the returned page can be determined by accumulating the size of the downloaded page plus all embedded images and content. Likewise, the size of probed FTP files and email messages should be well understood.

Note that with the HTTP_TRANS probe type, a single target consists of multiple steps and each step results in a downloaded page.

Probe System to Management Server

The probe measurement results sent to the OVIS Management Server are more comparable in size across all probe types. In general, each probe target execution results in a measurement record sent to the OVIS Management Server that is approximately 500-1200 bytes in size (600 bytes is a typical average size). Multiply the number of targets hit per interval across all probe systems by this value to estimate the amount of data sent to the OVIS Management Server each probing interval.

The following variable length fields in the measurement record have the biggest impact on the overall size:

- customer name
- service group name
- target

- error info

Note that with the HTTP_TRANS probe type, there is also a step URL field for each step in the transaction. Moreover, a separate set of measurements is sent for each step within a single HTTP_TRANS target execution.

Management Server System

Sizing the management server for scalability depends on the number of customers, service groups, targets and remote probe systems. The number of probe targets, systems, and probe configuration settings determine how many probe measurements will be sent to the OVIS Management Server each interval. The total number of measurements sent must be able to be processed by the OVIS Management Server in a timely manner while allowing for other Management Server data collection and access functions to likewise complete in their allotted time constraints. When processing individual probe measurements, threshold and alarm conditions are also applied; therefore, the number and type of threshold conditions impacts the processing throughput. All of these variables as well as the number of customers and service groups determine how much data will be stored in the OVIS Management Server database. The amount of data stored has a direct impact on data collection and access operations such as using the Dashboard and generating the nightly reports.

In general, it is always recommended to size the OVIS Management Server with the fastest hardware resources available and make sure the system has adequate memory. A production capable database such as SQL Server or Oracle should be used. If the database resides on a different server, ensure a fast network connection and excess network capacity between the OVIS Management Server and database server.

If OVIS is used with a smaller number of targets and in a small environment, the OVIS Management Server system can be shared with other applications and activities. However, a dedicated system is recommended for medium to large-scale OVIS deployments.

Probe Measurement Processing Throughput

In the prior sections, formulas and guidelines were given to help determine the total number of probe measurement records sent from all probe systems to the OVIS Management Server for each five-minute interval. The total number of records for all probe targets and systems in five minutes divided by 300 (the number of seconds in five minutes) gives the approximate probe measurement record arrival rate per second at the OVIS Management Server.

On a mid-sized Windows platform (that is 2 GHtz single processor, 1+ GByte of memory), the OVIS Management Server can process approximately 150 records per second. This processing involves parsing the incoming results, applying the configured threshold and alarm conditions, generating alarms when necessary, and logging the records to the database. This maximum rate will be less in environments having more, and more complex, threshold and alarm conditions triggered based on the Service Level Objective (SLO) configuration settings.

If the number of projected measurement records per second greatly exceeds this rate, the number of probes and/or probing frequency must be reduced or spread across multiple OVIS Management Server installations. One indicator of an OVIS Management Server nearing the limit of probe measurement record processing is to monitor the IIS inetinfo process CPU utilization using system performance monitoring software. If inetinfo CPU utilization is consistently 50% or greater over a five-minute interval, this is a good indication that the measurement record arrival rate is too high.

If the record arrival rate is borderline and the processing functions are still able to keep up, there is a good chance that when logged in the historical database tables over time, these voluminous records will negatively impact database access operations such as generating reports and queries needed to populate the various Dashboard displays. The ensuing sections provide more information about the size of the historical database tables and the impact on data access operations. In addition, database summarization and maintenance operations must be able to complete in a timely manner. If the OVIS Management Server record processing load consumes all available system processing capacity, these operations will not be able to complete in their allotted time.

Database Sizing

There are many factors that contribute to the size of variable length records and the growth of the historical database tables for each logged record. For example, the Customer, Service Group, Host, and Probe Location names along with target information are dynamically allocated based on their varying lengths. Also, the size of an error message needs to be considered if a probe fails. Probes with multi-step transactions use additional records for each step. Furthermore, each database type also has its own overhead to manage tables, indexes, and records.

The database growth example below is an estimate based on one Customer and Service Group with a single step HTTP target probed on a five-minute interval. This estimate does not take into account SLOs and/or SLAs configured and alarms generated from SLO violations. The results of this estimate provide guidance to determine how much storage space is needed for the number of targets probed per day and the total storage space needed for a target with the default values for "retain days".

Note that this sizing estimate is in addition to any storage requirements for installing and operating the database itself. It is also recommended you use the HP OpenView Database Smart Plug-In to monitor and manage the growth of your database over time.

OVIS Data Storage Tables

For an OVIS target there are six tables used for data storage. Three tables are used for Target Detail data and three are used for Service Group data.

Target Detail Data Tables

- IOPS_DETAIL_DATA (5-minute target data), Default Retain Days = 7
- IOPS_DETAIL_DATA_HOURLY (Summarized hourly target data), Default Retain Days = 30
- IOPS_DETAIL_DATA_DAILY (Summarized daily target data), Default Retain Days = 365

For the Target Detail data tables, the maximum record size is approximately 1200 bytes. On average, a typical HTTP target may use one half of the total record size (600 bytes).

The example shown in the table below uses a record size of 600 bytes to calculate the size in bytes/day for each of the Target Detail data tables:

Table 13 Example: Calculating Data Storage Size for Target Detail Tables

Type of Data	Calculation of Data Storage per day	Bytes/day
IOPS_DETAIL_DATA (5 min. target data)	600 bytes/record * 12 records/hr * 24 hrs/day =	172800 bytes/day
IOPS_DETAIL_DATA _HOURLY	600 bytes/record * 1 record/hour * 24 hrs/day =	14400 bytes/day
IOPS_DETAIL_DATA _DAILY	600 bytes/record * 1 record/24 hr * 24 hrs/day=	600 bytes/day
	Target Detail Data Tables Total =	187800 bytes/day (183Kb/day)

Service Group data tables:

- IOPS_PROBE_DATA_CACHE (5-minute Service Group data), Default Retain Days = 7
- IOPS_PROBE_DATA (Summarized hourly Service Group data), Default Retain Days = 30
- IOPS_PROBE_DATA_DAILY (Summarized daily Service Group data), Default Retain Days = 365

The maximum record size is approximately 350 bytes for Service Group data. On average, a typical HTTP target may use one half of the total record size (175 bytes).

The example shown in the table below uses a record size of 175 bytes to calculate the size in bytes/day for each of the Service Group data tables:

Table 14 Example: Calculating Data Storage Size for Service Group Tables

Type of Data	Calculation of Data Storage per day	Bytes/day
IOPS_PROBE_DATA _CACHE (5 min service group data)	175 bytes/record * 12 records/hr * 24 hrs/day =	50400 bytes/day
IOPS_PROBE_DATA (summarized hourly)	175 bytes/record * 1 record/hour * 24 hrs/day =	4200 bytes/day
IOPS_PROBE_DATA _DAILY	175 bytes/record * 1 record/24 hr * 24 hrs/day=	175 bytes/day
	Service Group Data Tables Total =	54775 bytes/day (~54Kbytes/day)

Total Target Data Storage Space per Day

One HTTP target using one half the total record size for the six OVIS storage tables will use approximately 237 Kbytes of data storage space per day (Target Detail data = 183 KB + Service Group data = 54KB).

Calculating Total Data Storage Space per Target

Now we'll consider the storage for one HTTP target based on the calculations above and the default Retain Days value set for each table.

Table 15 Example: Calculating Data Storage Size per Target

Data Table	Retain Days	Data Storage Calculation	Space Required
IOPS_DETAIL_DATA	7	172800 bytes/day * 7 days=	1209600 bytes (~1181 Kbytes)
IOPS_DETAIL_DATA_HOURLY	30	1440 bytes/day * 30 days =	432000 bytes (~422 kbytes)
IOPS_DETAIL_DATA_DAILY	365	600 bytes/day * 365 days =	219000 bytes (~214 Kbytes)

Table 15 Example: Calculating Data Storage Size per Target

Data Table	Retain Days	Data Storage Calculation	Space Required
IOPS_PROBE_DATA_CACHE	7	50400 bytes/day * 7 days =	352800 bytes (~354 Kbytes)
IOPS_PROBE_DATA	30	4200 bytes/day * 30 days =	126000 bytes (~123 Kbytes)
IOPS_PROBE_DATA_DAILY	365	175 bytes/day * 365 days =	63875 bytes (~62 Kbytes)
		Total Database Space =	~2356 Kbytes or 2.3 Megabytes

The total database storage space needed over one year for one HTTP target probed at a 5-minute interval based on the calculations and retain days shown above (for example daily data is retained for 365 days by default) is approximately 2,356 Kbytes or 2.3 Megabytes. With this model, you can use the following formula to calculate the database space per year required for the number of targets:

```
Total data storage for all targets =
2.3 MB * number of targets
```

If the projected database size exceeds the available capacity, the following configurable items can be tuned to reduce the amount of data stored:

- Reduce the number of probe locations
- Probe less frequently (longer probe intervals)
- Limit the number of steps in multi-step HTTP_TRANS targets
- Reduce the number of customer/service group combinations
- Reduce the data retention period to keep less data

Data Access Performance

The amount of data stored affects the responsiveness of the OVIS Dashboard, the time it takes to generate the nightly reports, and the time it takes the periodic database maintenance and summarization operations to complete. Even if database storage capacity is available to store very large tables (that is, 10 million plus records), query performance for these access operations will degrade at these table sizes to a point where the Dashboard responsiveness is unacceptable and the database maintenance and summarization functions cannot keep up with new arriving data.

Dashboard Responsiveness

The responsiveness of the Dashboard will also vary based on the amount of data requested (not just by the amount of data in the database). Requests for all customers will take considerably longer than requests for a single customer. Lastly, the selected time interval has a direct impact on Dashboard responsiveness.

While it would be expected that requests for long time-intervals with coarse groupings, such as all customer, would take longer, a general responsiveness goal for smaller groupings of data with an interval of 4 hours or less would be no longer than 30-60 seconds. This is a more typical Dashboard use case for Dashboard monitoring where responsiveness is more important.

If the Dashboard responsiveness is not acceptable, the following are some options to reduce response times:

- Request less data - finer customer/service groups, shorter intervals.
- Limit the availability of the dashboard to a smaller subset of authorized users. If too many different web clients run the Dashboard, the responsiveness of each request will degrade.
- Avoid leaving idle Dashboard displays loaded in the browser. The Dashboard Health workspace has an auto-refresh feature - if the dashboard data is not being used but remains open, the OVIS Management Server continues to run queries against the database to service the periodic refresh requests.
- Regularly monitor system and network performance on the OVIS Management Server and database server to ensure sufficient hardware resources are available.
- Reduce the amount of data in the database by configuring smaller retention cycles (retain days) and following the other guidelines in the prior section.
- Maintain the database for optimum performance:
  - Keep indexes optimized by regularly rebuilding/compacting them.

- Run query analyzer functions, such as Oracle Analyze, regularly, especially as the database grows in size.
- Ensure adequate table sizes.
- Ensure adequate memory - maximize the database buffer cache and pool sizes based on available memory.

One can observe heavy Dashboard processing requests on the OVIS Management Server using system performance monitoring tools to identify the Dashboard request generator process named `RepIops`.

Database Maintenance and Summarization

Hourly database maintenance occurs on five-minute intervals while daily maintenance occurs hourly. The OVIS `IopsCollector` process performs trace data summarization every five minutes while the `IopsMaint` process handles the other maintenance and summarization functions on a five-minute and hourly basis. `Repmaint` process runs nightly and removes data from the Reporter database if it is older than what is defined in retain days value.

In a normal operating environment where there is excess processing capacity and the database size is not excessively large, these processes should run to completion in a relatively short time (less than minute). It they are observed through the use of performance monitoring tools to run for much longer periods of time that encroaches on their scheduling interval, they are not keeping up with the rate of new arriving data.

In this situation, the following are some options to reduce database summarization and maintenance times:

- Regularly monitor system and network performance on the OVIS Management Server and database server to ensure sufficient hardware resources are available.
- Reduce the amount of data in the database by configuring smaller retention cycles (retain days) and following the other guidelines in the prior section.
- Maintain the database for optimum performance:
    - Keep indexes optimized by regularly rebuilding/compacting them.
    - Run query analyzer functions, such as Oracle Analyze, regularly, especially as the database grows in size.
    - Ensure adequate table sizes.

— Ensure adequate memory - maximize the database buffer cache and pool sizes based on available memory.

Report Generation

By default, the nightly report generation cycle begins at 3am. The size of the database and available OVIS Management Server processing capacity has the most impact on the report generation times. Report generation is CPU intensive - the goal is to run the nightly reports during off-hours when CPU resources are readily available.

The goal here is obvious - the report generation cycle should complete before the next morning when the other Management Server activities increase corresponding to the peak times of the business day. If the CPU intensive report generation cycle runs well into the morning, reports will not be available, but as important, the report generation processing will impact the other activities needed to process the peak-time loads.

In this situation, the following are some options to reduce the report generation cycle time:

- Remove unnecessary report packages for probe types that are not used. See Removing Unused OVTA Reports on page 172.
- Use the scheduled downtime feature to disable probes during off-hours for probes that do not require 24x7 monitoring. This prevents unnecessary probe processing by the OVIS Management Server during off-hours when resources need to be maximized for report generation tasks.
- Regularly monitor system and network performance on the OVIS Management Server and database server to ensure sufficient hardware resources are available.
- Reduce the amount of data in the database by configuring smaller retention cycles (retain days) and following the other guidelines in the prior section.
- Maintain the database for optimum performance:
  - — Keep indexes optimized by regularly rebuilding/compacting them.
  - — Run query analyzer functions, such as Oracle Analyze, regularly, especially as the database grows in size.
  - — Ensure adequate table sizes.
  - — Ensure adequate memory - maximize the database buffer cache and pool sizes based on available memory.

One can observe when the report generation cycle completes by inspecting the log file `status.reporter`. System performance monitoring tools can also be used to identify the report generation process named `RepCrys`.

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 16 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 17 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 18 NTFS permissions explicitly for the "SYSTEM" account

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

Table 19 Registry Settings

Path	Edit/ Replace ACL	Permissions	Comments
Path = HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\Reporter	Edit	Read (RX)	
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 20 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)

On Windows 2003 Internet Services also sets IWAM and the NETWORK_SERVICE user as follows:

IWAM, full control on:

Program Files\HP OpenView\data\datafiles\IopsTraceTable.mdb

Program Files\HP OpenView\data\tmp\probe

NETWORK_SERVICE, full control on:

Program Files\HP OpenView\data

Program Files\HP OpenView\data\*.*

Program Files\HP OpenView\data\datafiles\IopsTraceTable.mdb

index