

EVALUATION GUIDE
TRAVERSE 5.5



zyrion
Business Service Assurance

© 2011 Zyrion, Inc. (www.zyrion.com) All rights reserved. Zyrion, Traverse and the Zyrion logo are registered trademarks of Zyrion, Inc. and/or its affiliates in the United States and/or other countries. All other registered and unregistered trademarks herein are the sole property of their respective owners. Zyrion, Inc. reserves the right, at its sole discretion, to make changes at any time in its technical information and specifications, and service and support programs.

About Traverse

Traverse is a breakthrough IT Infrastructure Monitoring and Service Management solution for mission-critical, distributed, and complex environments for Enterprises and Managed Services Providers (MSPs). Traverse delivers real-time, correlated, end-to-end, service-oriented views of the performance of the entire IT infrastructure - physical, virtual and cloud. Traverse's massively-scalable, patented solution architecture supports tens of thousands of distributed end-points, and processes millions of metrics. The software's innovative Service Container technology supports creation of purpose-specific, logical management views of business services and the underlying Cloud and IT infrastructure. Traverse is fully-aligned with ITIL and provides an open, extensible API and plug-in framework for integration with the enterprise ecosystem.

Customer Support

You can reach Zyrion technical support online:

<http://www.zyrion.com/support>

Telephone:

In the US: 877-7-ZYRION (877-799-7644)

Outside the US: +1 408-524-7426

Email:

support@zyrion.com

User Forum

To join our customer-driven user group connecting the worldwide community of Zyrion users, visit the online forum:

<http://community.zyrion.com/>

Contacting Zyrion

CONFIDENTIALITY NOTICE

This document contains information that is the property of Zyrion Incorporated. No part of this document may be reproduced or transmitted, in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without the expressed written permission of Zyrion.

Contents

<i>About Traverse</i>	2
<i>Contacting Zyrion</i>	2
<i>CONFIDENTIALITY NOTICE</i>	2
1. OVERVIEW AND INSTALLATION	5
1.1. ABOUT THIS GUIDE	5
1.2. TRAVERSE ARCHITECTURE	5
1.3. SYSTEM OPERATION.....	5
1.4. TRAVERSE INSTALLATION	6
<i>Installation Checklist</i>	6
<i>Supported Platforms</i>	7
<i>Minimum Hardware Requirements</i>	7
<i>Installing Traverse</i>	7
2. BASIC CONFIGURATION	9
2.1. FIRST-TIME STARTUP	9
2.2. LOGGING INTO THE TRAVERSE WEB APPLICATION	9
2.3. MANUALLY ADDING NEW DEVICES.....	10
2.4. RUNNING NETWORK DISCOVERY	11
2.5. CREATING ACTIONS AND SCHEDULES	11
2.6. ADJUSTING THRESHOLDS	14
2.7. GENERATING REPORTS	14
<i>Advanced</i>	14
<i>Custom</i>	15
<i>SLA</i>	15
<i>My Reports</i>	15
<i>Ad Hoc Reports (My Reports)</i>	15
<i>Scheduling Automatic Reports</i>	15
3. ADVANCED FEATURES	16
3.1. SERVICE MONITORING & CONTAINERS.....	16

<i>Creating a Service Container that Contains Devices</i>	16
<i>Creating a Service Container that Contains Tests (Virtual Device)</i>	17
<i>Nesting Service Containers</i>	18
<i>Examining Service Container Status</i>	19
3.2. CUSTOMIZABLE DASHBOARDS.....	19
3.3. PANORAMA TOPOLOGY & MAPS DISPLAY	21
3.4. CREATING AN SLA MEASUREMENT.....	24
3.5. EVENT MANAGER AND MESSAGE HANDLER	25
3.6. FEDERATED SECURITY MODEL.....	25
3.7. CONFIGURING NETWORK FLOW ANALYSIS	26
<i>Enabling the Traverse Integrated NetFlow Collector</i>	26
<i>Enabling NetFlow on a Cisco Router (or switch running IOS)</i>	27
<i>Using the Network Flow Analysis Console</i>	27
3.8. EXTENSIBLE AND OPEN APIS	29
<i>BVE Flex API</i>	29
<i>Plugin Monitors & Plugin Actions</i>	30
3.9. OTHER ADVANCED FEATURES	30
<i>Linked Device Templates</i>	30
<i>Scheduled Maintenance</i>	31

1. Overview and Installation

1.1. About This Guide

This guide is intended for users who are evaluating Zyrion Traverse. It provides a quick overview of installing the software in your environment, and all of its key features.

Managed Service Providers (MSPs) should also review the "MSP User Guide" available from Zyrion's support web site.

1.2. Traverse Architecture

The Traverse system comprises the following three components:

Business Visibility Engine (BVE): An embedded object-oriented database that stores all configuration information, including metadata related to user authentication, devices, tests, thresholds for test results, action profiles and other key information. The BVE FlexAPI, which allows access to the BVE for provisioning and results, also operates on this server.

BVE WebApp: Provides the Web-based user interface into Traverse. It correlates the data from multiple DGEs, and allows end users to look at the real-time status of their devices, add new devices and actions, and execute reports, using a simple Web browser. It manages the distributed databases and distributed processing while generating the real-time reports and graphs. You can have more than one BVE Web application for load sharing.

Data Gathering Engines (DGE): Performs the actual polling of data, receives SNMP traps, generates alarms based on thresholds, and does the aggregation of data in real time. DGEs should be located as close as possible to the devices being monitored to reduce wide area network traffic. The DGEs can be geographically dispersed or you can have multiple DGEs in the same location to distribute the load across different physical servers. When you have multiple DGEs in the same location, the system automatically provisions new devices onto the DGE with a lower number of devices.

In a large environment, Zyrion recommends that each component reside on its own physical host server, but for a small trial with up to 500 devices, you can install all components on a single host.

1.3. System Operation

Each component of Traverse operates independently to provide a high level of scalability and fault tolerance. When you start a DGE, it connects to the BVE and downloads the entire configuration associated with its unique name, including tests, thresholds and actions.

After this process completes, the DGE performs tests, generates events when thresholds are crossed, and triggers the corresponding notifications. The data collected by each DGE is stored in a local SQL database on the DGE itself.

When a user logs into the Web application, the system searches the configuration database for the list of devices that the user has permission to view. The Web application then connects directly to the distributed DGEs and gets the real-time status of the services or devices. When the user needs a report, the Web application fetches the data using parallel queries from the distributed DGEs and generates the reports in real time.

1.4. Traverse Installation

Installation Checklist

Prior to installing Traverse, you will need the following:

1. A dedicated hardware platform to install the Traverse software (see specifications in the Supported Platforms section below).
2. All network devices that are part of the evaluation footprint must be configured with a (read-only) SNMP community string (SNMP v1 or v2) or username, password and optionally encryption key (SNMP v3).
3. Firewall rules and/or access lists (ACL) on routers should be updated to allow SNMP queries on the UDP port specified below from the BVE/DGEs against the servers/routers/switches to be monitored by Traverse. If the servers are going to be installed at different physical locations, ensure that firewall rules or router access-lists have been updated to allow bi-directional communication between various Traverse components:

Source Port	Destination Port	Direction	Description
(any)	7651	DGE -> BVE	Provisioning Database
(any)	7652	DGE -> BVE	Provisioning Database
(any)	7653	DGE -> BVE	Internal Messaging Bus
(any)	7663	BVE -> DGE	Distributed Performance Database

4. The administrator password for your Windows servers so that they can be queried using WMI.
5. For monitoring Oracle databases, provide username and password with SYSDBA level rights.

Supported Platforms

Windows:

- Windows Server 2008, R2 (32/64-bit)
- Windows XP Professional w/Service Pack 3
- Windows 2003 Standard Edition
- Windows 2003 Enterprise Edition (32/64-bit)

Linux / Unix

- RedHat Enterprise Linux 4/5/6 (32/64-bit)
- CentOS 4/5/6 (32/64-bit)
- SuSE Enterprise Linux 10 (64-bit)
- Solaris 9 and 10 on UltraSparc platforms

Minimum Hardware Requirements

- 2GHz+ CPU on x86 platform (Windows and UNIX versions)
- 1.5GHz+ UltraSPARC III CPU on Sun Sparc platform (Solaris version)
- 4GB RAM (2GB if running DGE only)
- 18GB free disk space (SCSI or fast IDE)

NOTE: It is not recommended to install Traverse on a laptop, since laptop disk drives are generally not fast enough.

Installing Traverse

- Download the latest version of the Traverse software from the Zyrion website at www.zyrion.com.
- Make sure you are not running any other Web server on TCP port 80 on the Traverse host.
- Make sure the Traverse host has a static IP address.
- Make sure the Traverse host has access to an email relay for sending notifications.
- Execute the installation file.

a. Windows: Double-click **traverse-x.y.z-windows.exe**, and then follow the instructions.

b. UNIX: You should be logged in as root.

Extract the installation package as follows (you must use GNU tar on Solaris):

```
gunzip -c traverse-x.y.z-platform.tar.gz | tar xpf -
```

Change to the directory containing the extracted files, execute the install script, and then follow the instructions:

```
cd traverse-x.y  
./install.sh
```

- If you are installing Traverse on Windows, you **must** reboot after the installation.

2. Basic Configuration

2.1. First-time Startup

1. Start Traverse and verify that all of the components started and are operating correctly.

Windows:

```
Start > Programs > Zyrion Traverse > Start Zyrion Traverse
```

The Traverse Service Controller reports the status of all the components.

UNIX:

```
cd /usr/local/traverse/etc
./traverse.init start
./traverse.init status
```

2. If some components do not start, check for the following common start-up problems:
 - Expired license key (send email to eval@zyrion.com to get a new key)
 - Another Web server using TCP port 80
 - Failure to reboot after Windows installation

You can also look for errors in the `logs/error.log` file in the Traverse directory.

NOTE: After identifying and fixing any problems related to component start-up, restart Traverse.

2.2. Logging into the Traverse Web Application

1. Use your web browser to connect to `http://your_host/` where `your_host` is the fully qualified host name or IP address of the server that the Traverse Web application is running on.



2. Log in using the default end-user name *zyrion* with password *zyrion*.
3. Set your time zone and other user preferences by navigating to Administration > Preferences.

2.3. Manually Adding New Devices

1. Navigate to Administration > Devices > Create a Device.

* Type of Device:	Select Device Type
* Device Name:	<input type="text"/>
* Fully Qualified Host Name/IP Address:	<input type="text"/>
Do Not Validate/Resolve Device Address	<input type="checkbox"/>
Comments/Description (optional):	<input type="text"/>
Tag 1:	<input type="text"/>
Tag 2:	<input type="text"/>
Tag 3:	<input type="text"/>
Tag 4:	<input type="text"/>
Tag 5:	<input type="text"/>
Automatically Clear Comment When In OK State:	<input type="checkbox"/>
Display Comment In Summary Screen:	<input checked="" type="checkbox"/>
* Create In Location:	Select Location
Flap Prevention Wait Cycles:	System Default
Enable Smart Notification:	<input checked="" type="checkbox"/>
Enable Test Parameter Rediscovery:	<input type="checkbox"/>
Enable Network Configuration Management:	<input type="checkbox"/>
Create New Tests After Creating This Device:	<input checked="" type="checkbox"/>
Create Device Dependency After Creating This Device:	<input type="checkbox"/>
<input type="button" value="Create Device"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>	

2. Select the device type and provide the device name and IP address or fully qualified host name.
3. The tag fields can be used to give devices arbitrary tags that can be used to search for them later. For example, you might use a tag to record the location of the device (HQ or CHICAGO), or the function of the device (ROUTER or SWITCH). Add a device with a value for Tag 1 of "ROUTER" for use later in this evaluation.
4. Leave the "Create New Tests After Creating This Device" box checked and click **Create Device**.
5. To create tests for the new device, first select the type of tests. You can use built-in or user-defined Application Profiles (which auto-discover a filtered list of tests) or user-defined Monitoring Profiles (which define a specific list of tests), or you can manually choose which monitors and tests to add, in which case Traverse automatically discovers all monitors and tests for the device.
6. If you want to use SNMP (Simple Network Management Protocol) or WMI (Windows Management Instrumentation) monitors, you must enter the SNMP community string and port number or WMI domain username and password.
7. Once the device is added, it appears on the Administration > Devices page. Click **Tests** under the Modify column to manage all tests for that device. Then, click the icon under the Modify column next to a test to update the test parameters, such as the polling interval and the values for warning and critical thresholds.
8. Navigate to Status > Devices to view a status summary for all devices. From here click on a device name to drill down and see the status of the tests for that device, and then click on a test name to see details and graphs of short- and long- term history.

2.4. Running Network Discovery

You can also have Traverse search your network to automatically discover any devices, or just specific types of devices. You should also limit the subnets to be included in the discovery to class-C networks instead of class-B or larger.

1. Navigate to Administration > Other > Device Discovery & Import > New Network Discovery Session.
2. Enter the IP and netmask for each subnet you want to discover devices in. If you want to discover SNMP devices, enter the SNMP community string(s). If you check the "Discover physical connectivity (topology) between devices" box, Traverse will automatically map the relationships between devices.
3. Once discovery is complete, select and confirm the devices you want to provision, and then discover and select tests.

For information about displaying the discovered network topology, see *Panorama Topology Display* later in this document.

2.5. Creating Actions and Schedules

When a test result crosses a threshold, Traverse takes action based on rules defined in Action Profiles. Some possible actions include sending email, sending SNMP traps, opening trouble tickets, or running an external script.

1. Navigate to Administration > Actions > Create an Action Profile.
2. Create an action profile with two levels of escalation. In this example, email is sent immediately to the admin when a test goes into warning, critical, or unknown state, and to the manager after a test is critical for 15 minutes during peak hours.

* Action Profile Name:

Action Profile Description:

Notify Using: Please Select

Message Recipient:

Notify when test is in state: Ok: Warning: Critical: Unknown:

Notification should happen after (0 = immediately): 1 cycles

If this test stays in the trigger state, repeat this action every (0 = never): 0 cycles

Schedule: Default Schedule [Manage Schedules](#)

Select DGE to test this action: sunnyvale

Notify Using: Please Select

Message Recipient:

Notify when test is in state: Ok: Warning: Critical: Unknown:

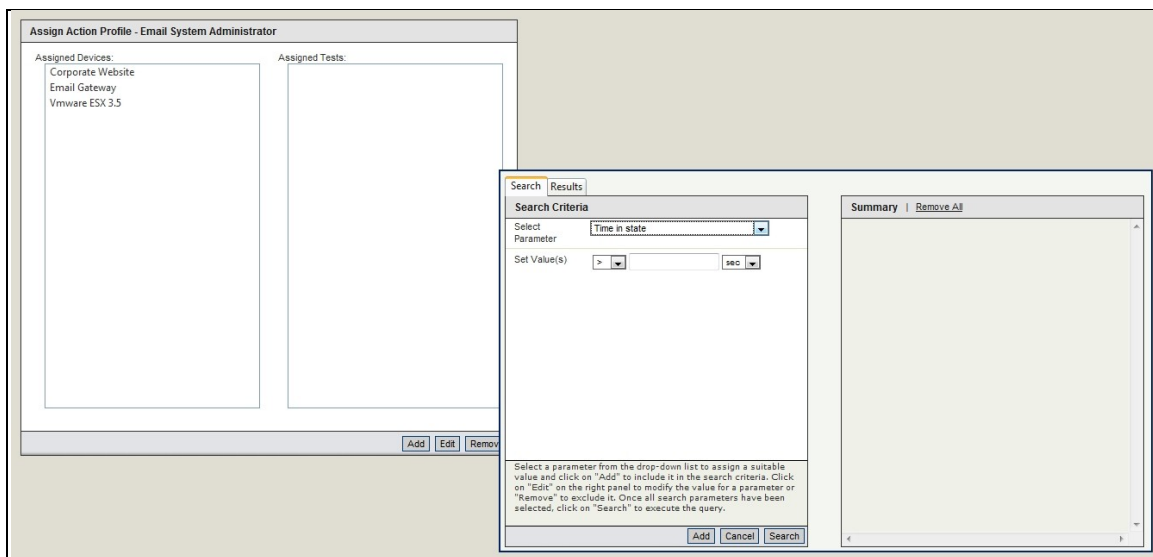
Notification should happen after (0 = immediately): 1 cycles

If this test stays in the trigger state, repeat this action every (0 = never): 0 cycles

Schedule: Default Schedule [Manage Schedules](#)

Select DGE to test this action: sunnyvale

3. Click **Create Action Profile** to create the profile.
4. To assign this profile to tests, click **Assign to Tests** in the row where the new action profile now appears on the Manage Action Profiles page, and then click **Add**.
5. Choose a parameter you want to search with, then a value, and then click **Add** to use this as a search criterion. Add as many other search criteria as you like, and then click **Search**.



6. In the Results pane, select the devices whose tests you want to use the action profile, and then click **Assign Action Profile**.
7. The Assign Action Profile page now lists all of the devices with tests to which this action profile is assigned, and if you click on a device, you can see the specific tests on that device that are using the profile.

By default, tests and actions run all the time, but you can control when they run by creating and assigning Schedules to them. For instance, you might want some tests and actions to run only during business hours.

1. Navigate to Administration > Other > Custom Schedules > Create a Schedule.
2. Enter "business hours" in the Schedule Name field, uncheck all the boxes for days and times that fall outside of business hours, and then click **Create Schedule**.
3. To assign this schedule to a device, click **Select Devices For Schedule** in the row where the new schedule appears, and then click **Add**.
4. Choose a parameter you want to search with, then a value, and then click **Add** to use this as a search criterion. Add as many other search criteria as you like, and then click **Search**.
5. In the Results pane, select the device you want to add, and then click **Assign Schedule**. The new schedule is assigned to all tests for that device.

You can also assign a schedule to specific tests through device administration.

1. Navigate to Administration > Devices and click Tests in the row for the device whose tests you want to schedule.
2. Click the Modify icon in the row for the test you want to schedule, and then use the drop-down Schedule menu to assign a schedule.

You can assign the new business hours schedule to the actions in your Action Profiles as well.

1. Navigate to Administration > Actions and click **Update** in the row for the Action Profile you created.
2. For each action, use the drop-down Schedule menu to assign a schedule.

2.6. Adjusting Thresholds

Traverse comes with pre-defined thresholds for most metrics, but these warning & critical thresholds might be too low for your environment and require adjustments. If you have a small number of devices, and if you are seeing some devices in warning or critical state for long periods of time, you should click on the devices and increase the thresholds as needed.

1. Click on *Status > Tests* from the main menu
2. Click once on the test name which is in red or yellow state to select that row. Note the current result, and then click on the "edit" icon on the top right menu.
3. On the *Update Test* page, change the warning threshold to be a little higher than the current value for the test that you noted earlier and a matching critical threshold (slightly higher than warning).
4. Click on the **Submit** button.
5. Repeat these steps for the remaining tests which are in warning or critical state.

If you have a large number of devices, you can use the "baselining" feature in Traverse to automatically adjust the thresholds based on the historical data collected (this is described in the Traverse User Guide). This option is under *Administration > Devices > Test Baseline Management*.

Traverse also supports dynamic, Adaptive Thresholds, the functionality for which is described in more detail in the User Guide. This allows setting alarm thresholds that match varying patterns of use or load in the IT infrastructure. For example, if nightly back-up jobs increase the utilization levels of a server during the evening hours, then you can set higher threshold levels for this time period so that unnecessary alarms are not generated.

2.7. Generating Reports

Traverse has extensive and flexible reporting generated in real time from data collected by the DGEs and then processed by the BVE reporting engine. Navigate to Reports to access the different report capabilities. Traverse reports are organized and accessible in four areas, each one serving a specific purpose.

Advanced

These are a set of pre-defined reports that allows users to view and analyze different "types" of performance data for a user-specified set of devices or containers (and some additional context depending on the report itself). These reports are designed to allow users to quickly perform specific types of operational analysis of the IT infrastructure, and answer some commonly asked questions for specific tests, devices and containers.

Custom

These reports allow users to conduct system-wide or broader analysis of events, thresholds, capacity, future-trending and availability. Users have greater flexibility in selecting the report parameters, and can choose to run more granular reports for specific test, devices and containers if desired.

SLA

These reports are designed for the purpose of historical and deeper analysis of the SLA metrics and measurements configured and monitored in Traverse.

My Reports

Users can create and 'save off' specific report queries for the first three types of reports, and retrieve and run these in the future. Traverse allows adding individual components from the various pre-defined reports into the same composite, user-specific report. The reporting framework is very flexible and allows completely arbitrary user-defined statistics generated on an as needed basis.

Ad Hoc Reports (My Reports)

You can create and save your own Ad Hoc reports that combine components from different reports and make them easy to access.

1. Run a report, and then click on the icon next to a component title to bring up the Add To My Reports dialog.
2. Name your Ad Hoc report in the Create A New Report field, and then click **Submit**.
3. Your saved report now shows up when you navigate to Reports > My Reports, where you can click the name of the report to run it.

Scheduling Automatic Reports

You can also schedule any saved report (saved query parameters or ad hoc reports) to execute automatically and email the results to a list of recipients.

1. Navigate to Administration > Other > Scheduled Reports For Email Delivery > Create A Scheduled Report.
2. Name your scheduled report in the Scheduled Report Name field, use the drop-down Generate Using Saved Query menu to select a saved report, and then enter the recipient(s) and define the schedule.

3. Advanced Features

3.1. Service Monitoring & Containers

Service containers allow you to group tests and devices to create logical, business-oriented views of your network in addition to your hardware-oriented views. A service container can hold virtual devices (special types of containers that hold only tests), real devices, or other service containers.

Creating a Service Container that Contains Devices

1. Navigate to Administration > Containers > Create a Service Container.
2. In this example, you are creating a service container named Routers. Fill in the Service Container name, and then click **Next**.
3. Select **Devices & Containers** in the Container Will Include field.
4. You can assign devices to a container either by performing a search and manually selecting the devices to include, or by specifying rules and having the results automatically assigned to the container.

For this example, select **Automatically Based On Specified Rule** in the For Device Containers, Assign Devices field. Choose Tag 1 in the selection_criteria drop-down menu, type "ROUTER" in the text field, click **Test This Rule** to see which devices will match the rule, and then click **Next Step**.

The screenshot shows a configuration form for creating a service container. The 'Service Container Name' is 'TEST-YP'. The 'Container Will Include' section has 'Devices & Containers' selected. The 'For Device Containers, Assign Devices' section has 'Automatically Based On Specified Rule' selected. A rule is defined with 'Device Type' as 'Tag 1' and the rule text as '* ROUTER'. The 'Test This Rule' button has been clicked, and the 'Rule Results' area displays 'No device found matching the current rule selection'. At the bottom, there are 'Next Step', 'Reset', and 'Cancel' buttons.

5. Assign an action profile if desired, decide the criteria for determining the severity status of the container, and then click **Create Container**.

Creating a Service Container that Contains Tests (Virtual Device)

1. Navigate to Administration > Containers > Create a Service Container.
2. In this example, you are creating a service container named All ICMP Tests. Fill in the Service Container name, and then click **Next**.
3. Select **Tests (Virtual Device)** in the Container Will Include field.

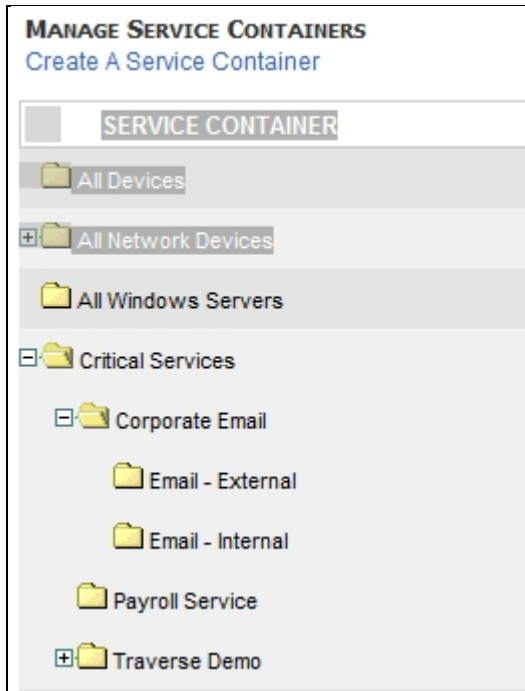
4. You must manually select tests for a virtual device container. Click **Add** in the Selected Device box, and then build a filter that matches the devices or tests you want to find; choose a parameter you want to search with, then a value, and then click **Add** to use this as a search criterion. Add as many other search criteria as you like, and then click **Search**. In this example, you are adding all ICMP Ping type tests.

- In the Results pane, select the devices whose tests you want to add, and then click **Add**. The Create a Service Container page now lists all of the devices with tests to be added to the new container, and if you click on a device, you can see the specific tests on that device that are included.

- Click Next Step, assign an action profile if desired, decide the criteria for determining the severity status of the container, and then click Create Container.

Nesting Service Containers

You can nest service containers to build a logical hierarchy of your environment. For example, you might have Routers, Switches, and Firewalls containers, all contained within a Network Devices container.



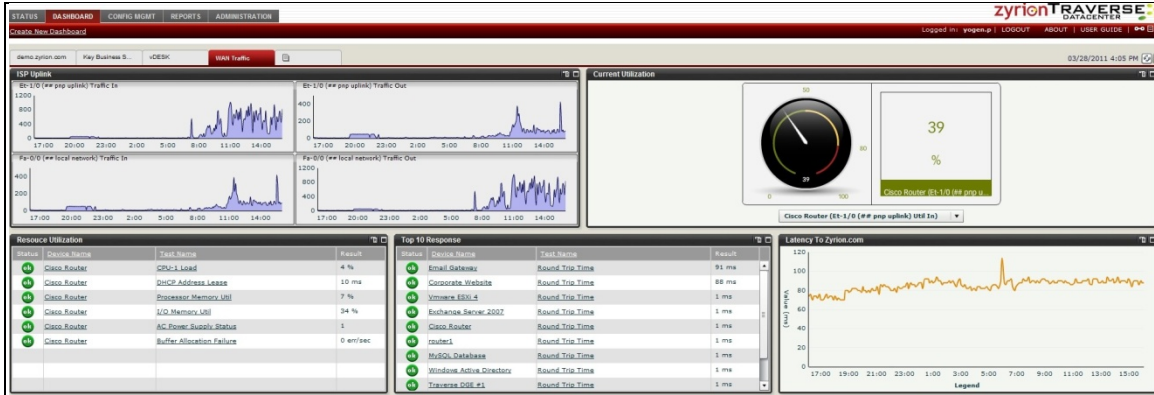
Examining Service Container Status

1. Navigate to Status > Containers to view a status summary for all containers.
2. Click on a container name to list its contents.
3. Drill down into the container hierarchy to reach a test container, and then click on the Run Reports menu to generate reports of Recent Events and Correlation.
4. Click on a test name to see its status page and access Long-Term History, Trend Analysis, and Raw Data reports.

Name	Network	System	Application
Primary Distribution Switch	!!	!!	!!
MySQL Database	!!	!!	!!
VMware ESX 3.5	!!	!!	!!
VMware ESX 4	??	??	??
router1	!!	!!	!!
Corporate Website	!!	!!	!!
Email Gateway	!!	!!	!!

3.2. Customizable Dashboards

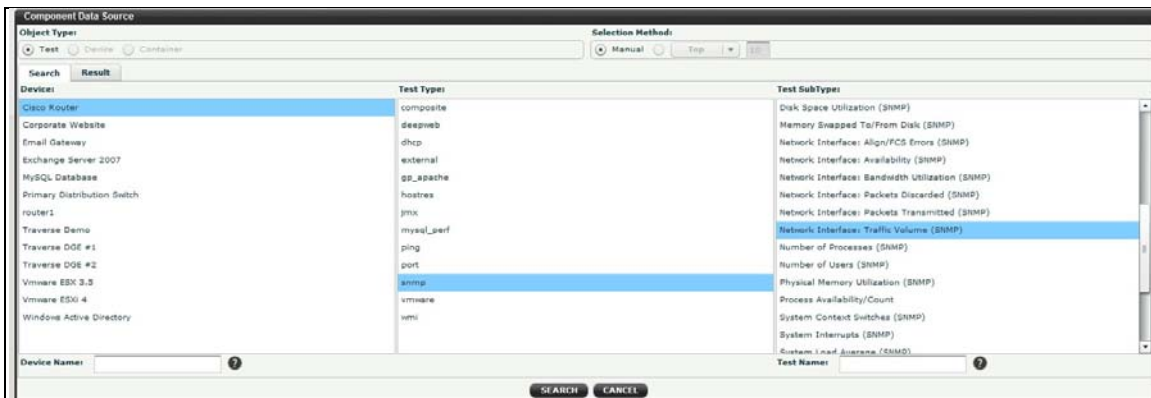
The customizable RealView dashboard feature lets you create custom dashboards to view the performance of services and infrastructure. You can create multiple dashboards, each containing dashboard components related to a particular area of service you want to monitor.



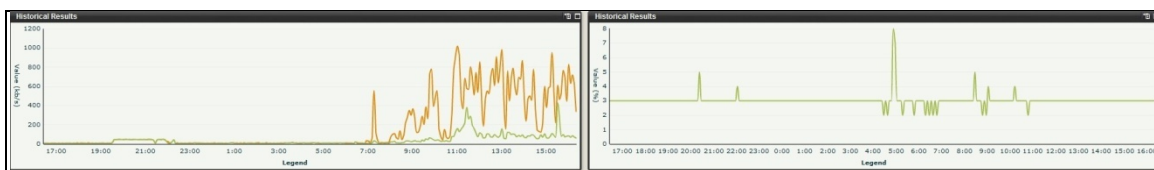
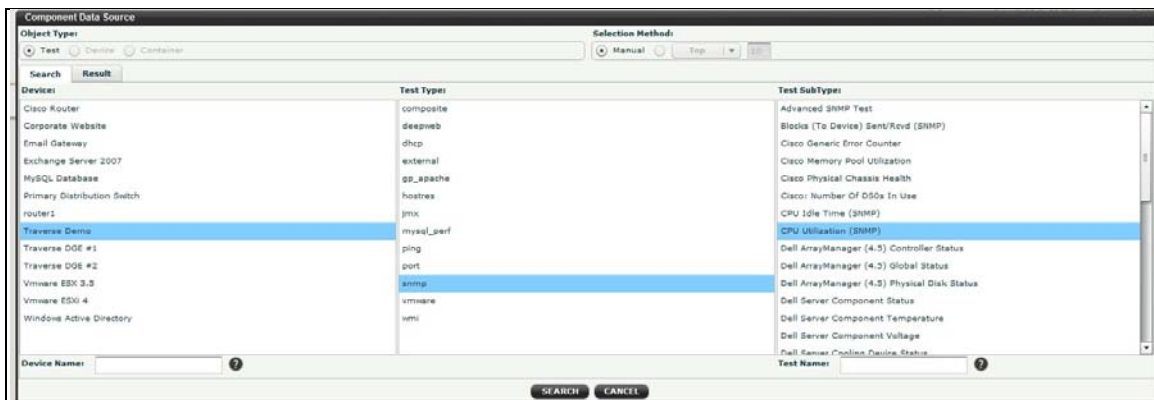
1. Navigate to Dashboard > Create New Dashboard.
2. Enter a name for your dashboard and choose whether you want it to be visible to other users or private, and then click **OK**.
3. Click **Create New Chart/Table** in your new empty dashboard to open the Create Dashboard Component dialog.
4. In this example, you are creating a line chart component for traffic tests. Select the line chart component type icon, fill in the Title field, select the refresh interval, and then click **Apply**.



5. Now specify the data source for the component. Select the devices and test types, and then click Search to find the matching tests. Select the tests you want the component to use by dragging and dropping them from the Matching Tests list to the Selected Tests list, and then click **Apply**.



6. Now add a gauge component for a CPU utilization test. Click the '+' Add Dashboard Component icon in the upper right corner of the dashboard, select the gauge component type icon, fill in the Title field, select the refresh interval, and then click Apply.
7. Now specify the data source for the component. Select a device, and then click Search to find the matching tests. Drag and drop the CPU load tests to the Selected Tests list, and then click **Apply**.



3.3. Panorama Topology & Maps Display

The Panorama feature offers an interactive graphical representation of the devices in your network that are being monitored, including the status of the devices and the dependency relationships between them. Panorama offers three different topology layouts, flexible display

filters, pan and zoom functionality, the ability to configure and save custom views, and the ability to add or remove device dependencies.

1. Navigate to Status > Panorama.
2. Click on the **Display Filter** icon on the top left hand corner to view various filtering and layout options.



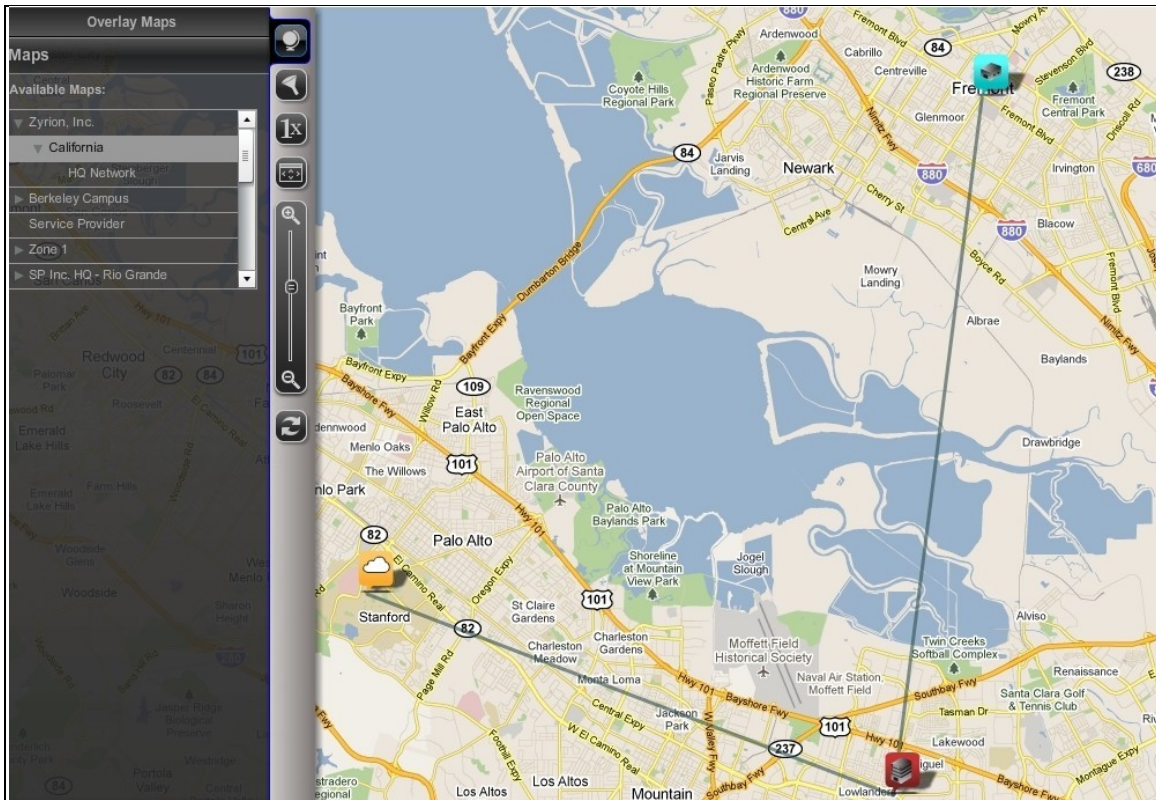
3. Choose between hierarchical (the default), circular, or grid layout options.
4. In edit mode, you can move the position of the nodes on the canvas. You can also add or remove device dependencies. When you click on a device node, a plus sign appears on the icon; click this plus sign and drag to another device to create a new parent/child dependency relationship. When you click on the line connecting two devices, a red X icon appears; click this X to remove the device dependency.
5. You can filter the devices shown in the topology view by type or status. By default, the Filter By Device Type & Status frame opens with the Device Types pane expanded. If you click on the Status bar, the Status pane expands instead. You can also click on the highlight option for each device or state, and device nodes of that type or state will appear highlighted in the topology view.



6. You can choose to collapse nodes based on depth in the hierarchy or threshold number of child nodes. If you select the Leaf Nodes Only check box, only the leaf nodes will be collapsed.

7. After customizing the topology view, you can save it as a custom layout.

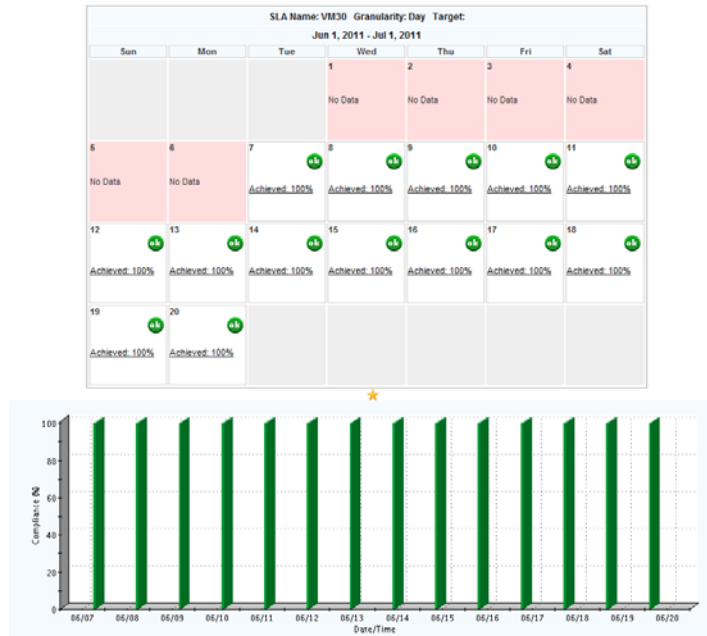
You can Navigate to Status >Maps to view network on a geographical overlay.



3.4. Creating an SLA Measurement

The SLA Manager lets you track compliance against user-defined Service Level Agreement metrics for Containers, Devices and Tests. These SLA metrics are calculated and displayed on a real-time dashboard that displays the amount of time that the metric is within the SLA threshold and also displays how close the metric is to violating the SLA requirement.

1. Navigate to Administration > SLA in the Traverse Web application.
2. On the Configure SLA Manager page, click **Create an SLA Measurement**.
3. Fill out the fields in the Create an SLA Measurement form:
 - SLA Measurement Name
 - Comments/Description: An optional field that lets you provide some additional descriptive information that will appear in the SLA Manager list of SLA measurements.
 - Calculation Period
 - Calculation Frequency
 - Threshold: The percentage of the Calculation Period that the metric must be in the OK state.
 - Schedule: Used to specify business hours and weekdays for calculation of the SLA period.
 - ✓ Select whether the SLA is being created for a Container, Device or Test
 - ✓ If you selected Container or Device, then via the drop-down list, select the specific Container or Device for which the SLA is being created, and then click **Submit**.
 - ✓ If you selected Test, then click **Submit** to go to the page for selecting the underlying device tests for this SLA metric, and then click **Add**.
 - ✓ Choose a parameter you want to search with, then a value, and then click **Add** to use this as a search criterion. Add as many other search criteria as you need, and then click **Apply** to run the search.
 - ✓ In the Search Results pane, select the tests that you want to be a part of the SLA metric for each device, and then click **Assign to SLA Measurement**.
 - ✓ You can now click on the devices you've added in the Assigned Devices list, and the tests you selected will appear under Assigned Tests. Use the Add, Edit, and Remove buttons to make any further changes to the devices and tests you want to include.
4. Click **Done** to finish creating the SLA measurement.
5. Navigate to Status > SLA to view real-time data for your SLA metrics on the SLA Manager dashboard.



3.5. Event Manager and Message Handler

The Traverse Event Manager Console displays messages (traps, logs, windows events) forwarded from the Message Handler, as well as threshold violations.

- Navigate to Status > Events.
- From the Event Manager Console you can acknowledge, suppress, and delete events. Events can be suppressed until a particular date and time, or until the state changes. The screen refreshes automatically every few minutes (this interval can be changed on the Administration > Preferences page).

The Message Handler is a distributed component of Traverse which accepts syslogs, SNMP traps, Windows events or any other text messages and then searches for specified patterns in these messages. When a pattern match is found, the message string is transformed and a severity assigned to it, and then it is forwarded to the DGE. The processed messages from the Message Handler are displayed on the Traverse Event Manager Console and can trigger actions & notifications setup on the DGE.

For more information on configuring the Message Handler, see the *Traverse User Guide*.

3.6. Federated Security Model

Traverse has a multi-tier user model, which allows you to create accounts for different departments such that users in one department cannot see the devices in another department. You can also create administrator accounts for users who need to view multiple departments across the enterprise. For more information, see the *Traverse User Guide*.

3.7. Configuring Network Flow Analysis

Traverse integrates with network flow and packet level data collection tools to provide a seamless drilldown from system and device level monitoring to troubleshooting and analysis using flow and packet data. This data provides details about the network traffic between hosts, enabling quick identification of impacted services, trouble areas, and problem sources.

Enabling the Traverse Integrated NetFlow Collector

Traverse has an integrated NetFlow collector that is pre-installed with the DGE, but disabled by default.

1. On UNIX, execute the following command as root:

```
touch /usr/local/traverse/plugin/monitors/flow.enable
```

On Windows, open a command window and execute the following commands:

```
sc config tvFlowQD start= auto
sc config tvSiLK start= auto
```

NOTE: The space after "start=" is required.

2. Edit <TRAVERSE_HOME>/apps/silk/data/sensor.conf and locate the following line:
internal -i pblock 192.168.10.0/24

Update the network segment (192.168.10.0/24) to match your local IP subnet in n.n.n.n/mask format.

For more information about the options in this configuration file, see <http://tools.netsa.cert.org/silk/sensor.conf.html>.

3. On UNIX, start the NetFlow collector by executing the following command as root:

```
<TRAVERSE_HOME>/etc/traverse.init start
```

On Windows, start the NetFlow collector by navigating to Start > Programs > Zyrion Traverse > Traverse Service Controller and clicking **Start All** to start the NetFlow collector components.

Enabling NetFlow on a Cisco Router (or switch running IOS)

The network flow analysis feature in Traverse relies on collecting network flow data exported by a router or switch, so you need to enable your network equipment to export flow records. Network flow records are exported from the routers to the default TCP port of 9996.

1. Telnet or SSH into the router and enter enable mode.

2. Enable Cisco Express Forwarding:

```
router(config)# ip cef
```

3. Enable NetFlow on all physical interfaces that will take part in routing traffic between devices of interest:

```
router(config)# interface <interface>
```

```
router(config-if)# ip route-cache flow
```

NOTE: Routers may by default export flow data only for traffic entering the router, so make sure you enable NetFlow on all interfaces for accurate analysis of traffic both into and out of the router.

4. Enable export of NetFlow records:

```
router(config)# ip flow-export version 5
router(config)# ip flow-export destination
<dge_address> 2055
router(config)# ip flow-export source FastEthernet0
router(config)# ip flow-cache timeout active 1
router(config)# ip flow-cache timeout inactive 15
```

NOTE: The 'ip flow-export source' can be any interface that stays active; a stable or Loopback interface is preferred.

5. Save the configuration:

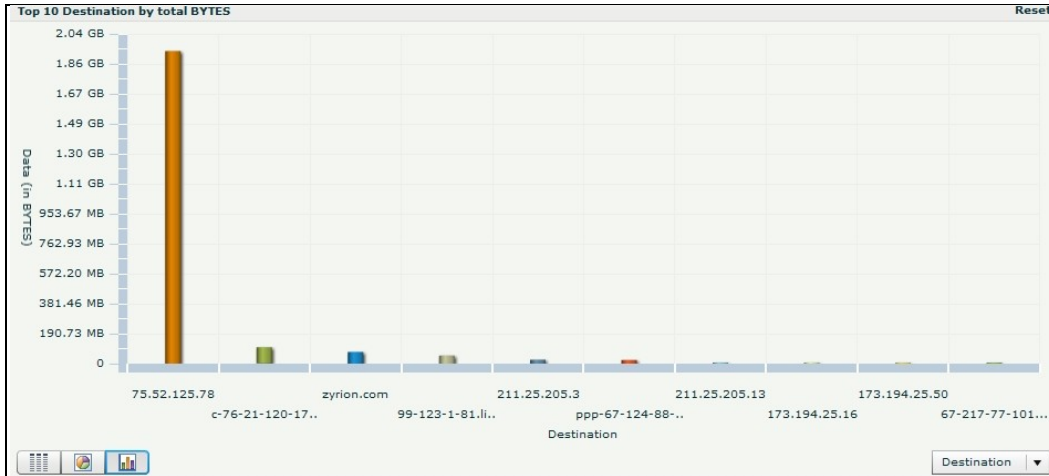
```
router(config)# end
router# write mem
```

Using the Network Flow Analysis Console

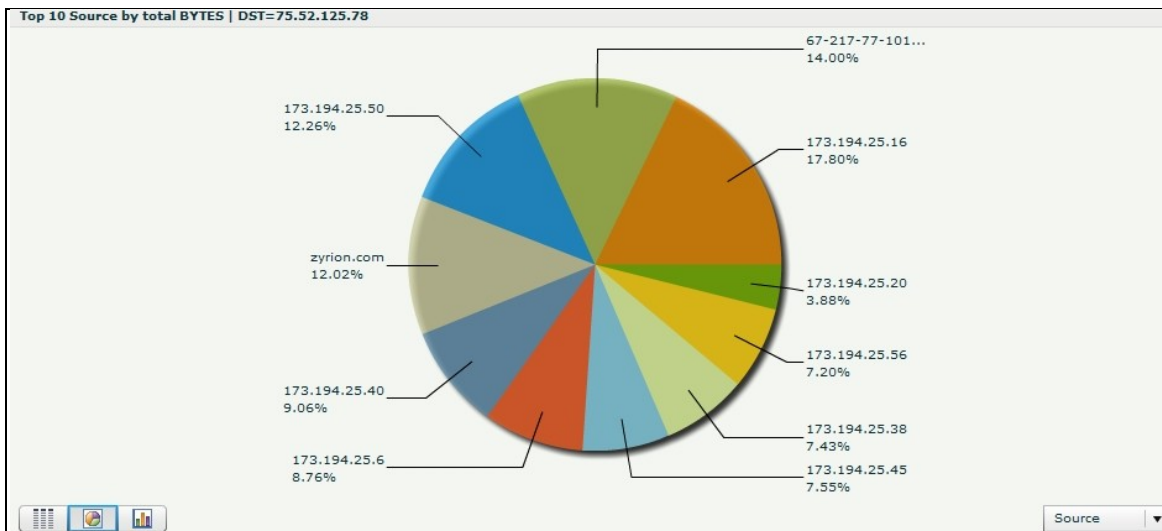
You can access the Network Flow Analysis console from the Traverse Web application from a device Test Summary page or from a Test Details page. Each chart in the network flow analysis console has a title bar that states which device(s) (and optionally, which application) are being examined, as well as their roles.

1. Navigate to Status > Devices and click on a device name.

2. On the Test Summary page, open the Run Reports drop-down menu and click on Flow Analysis.
3. By default, network flow data for the past 24 hours is analyzed to determine the top 10 destinations communicating with the selected device (source), and the results are presented in bar chart format.



4. Click on the results for an IP address on the Destination chart to display the top 10 applications for that destination of that source alongside in pie chart format.



5. Click on the results for an application on the Applications chart to display historical data for network traffic for that application for the selected destination-source pair.
6. Normally data is displayed for a single source or destination device, but you can click on Reset in the upper right corner of the first chart in the network flow analysis console to expand the scope of data to the entire network, providing a network-wide view of the top-N sources, destinations, or applications.
7. Click through as described above to get detailed device data.
8. Each network flow analysis chart can be displayed as a table, a pie chart, or a bar chart. Click on the corresponding button in the lower left corner of the chart to change how the data is displayed.
9. You can change the network flow analysis workflow by looking at a device first from any of the three different roles: source, destination, or application. Choose the role from the drop-down menu in the lower right corner of the chart.
10. Use the options in the menu bar at the top of the network flow analysis console to customize the data shown:
 - The Protocol drop-down menu lets you choose whether to show just tcp or udp traffic, or all traffic.
 - You can specify the Start Time and End Time to see network flow data for a particular time period.
 - The Metric drop-down menu lets you choose whether to show data in bytes or packets.
 - The Top field lets you choose how many clients or servers to show.

NOTE: You must click Apply to show the new data after making any changes to these options.

3.8. Extensible and Open APIs

Traverse has very powerful APIs which allow access to all components of the software. Users familiar with Perl or C can start using the API very quickly due to its familiar commands and interface. These APIs allow you to configure connections to other legacy products or custom applications.

BVE Flex API

You can use the BVE API to perform bulk changes to tests or devices. The BVE API can be accessed via a direct telnet connection or through the perl API. Any Traverse end user can log in

to the API and will get access to the same privileges and devices as when logging in via the Web interface.

1. To log in, ensure that the BVE API is running on the Traverse host. Then, from a Windows command prompt, UNIX shell, or alternate telnet client, telnet to port 7661 and enter the following command:

```
telnet localhost 7661
```

```
LOGIN <login_id>/<password>
```

2. The basic commands are list, add, delete, and suspend, which can be applied to contexts such as device, test, and user. The general syntax is "context.command <parameters>", as in the following examples.

List all devices:

```
device.list "deviceName=*"
```

List all tests for a device:

```
test.list "deviceName=xyz", "testName=*"
```

Set the warning threshold for all line utilization tests to 80% (you can also set this threshold using the Web application):

```
test.update "testName=Line Utilization", "deviceName=*", warningThreshold="80"
```

Plugin Monitors & Plugin Actions

The plugin monitor functionality in Traverse allows creating new monitors in Java or any other programming language such as C, perl, shell, etc. The system treats such plugin monitors as an integrated component of Traverse and provides a similar multi-threaded framework as it uses internally for its own monitors.

Plugin Actions allow you to run any custom script when a threshold is crossed or a new event is generated.

For more information, see the *“Traverse Developers Guide & API Reference”*.

3.9. Other Advanced Features

Linked Device Templates

A Linked Device Template contains a group of Tests that can then be applied to multiple devices so that each associated device is provisioned with the same tests. The Linked Device Template can also include an Action Profile and a Custom Schedule as well. Creating a Linked Device Template, allows you to configure tests for a master device and then apply that template across

multiple associated devices. What's important to note is that when the template for the master device is updated, you have the option to push the updated template to all the devices associated with the given Linked Device Template. See the User Guide for instructions on how to use Linked Device Template functionality.

Scheduled Maintenance

Scheduled Maintenance functionality allows defining in advance any number of time periods for automatically suspending devices at the start of the time-period, and then automatically resuming the devices at the end of the time-period. This functionality is in addition to the functionality that allows users to manually (on-demand) suspend/resume devices. Both the scheduled and the manual functionality allow you to temporarily turn off all the tests for one or more devices and turn them on again. This is useful for the purpose of performing maintenance tasks on the devices, where you do not want to receive alerts while the device is offline. Once a device is suspended, the polling and data collection for all the tests on the device is suspended and thus any associated actions to the tests will not generate notifications. Furthermore, when a device is suspended (e.g. for maintenance), this time is not included in the total downtime reports since it is considered a planned outage. See the User Guide for instructions on how to use Scheduled Maintenance functionality.