Kaseya 2

Traverse

Quick Start Guide

Version 7.0

August 1, 2014

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Preface

About this Guide

This guide is a quick installation and overview for the cloud (SaaS) version of **Traverse** monitoring software.

Audience

This guide is intended for **Traverse** cloud administrators.

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.

Contacting Kaseya

- Customer Support - You can contact Kaseya technical support online at:
  - **https://helpdesk.kaseya.com/home** *(https://helpdesk.kaseya.com/home)*
- Community Resources - You can also visit the following community resources for Kaseya **Traverse**:
  - Knowledge base at: http://community.kaseya.com/kb/w/wiki/1206.kaseya-traverse.aspx
  - Forum at: **http://community.kaseya.com/xsp/f/340.aspx** *(http://community.kaseya.com/xsp/f/340.aspx)*

Chapter 1

Installation, Logon and Licensing

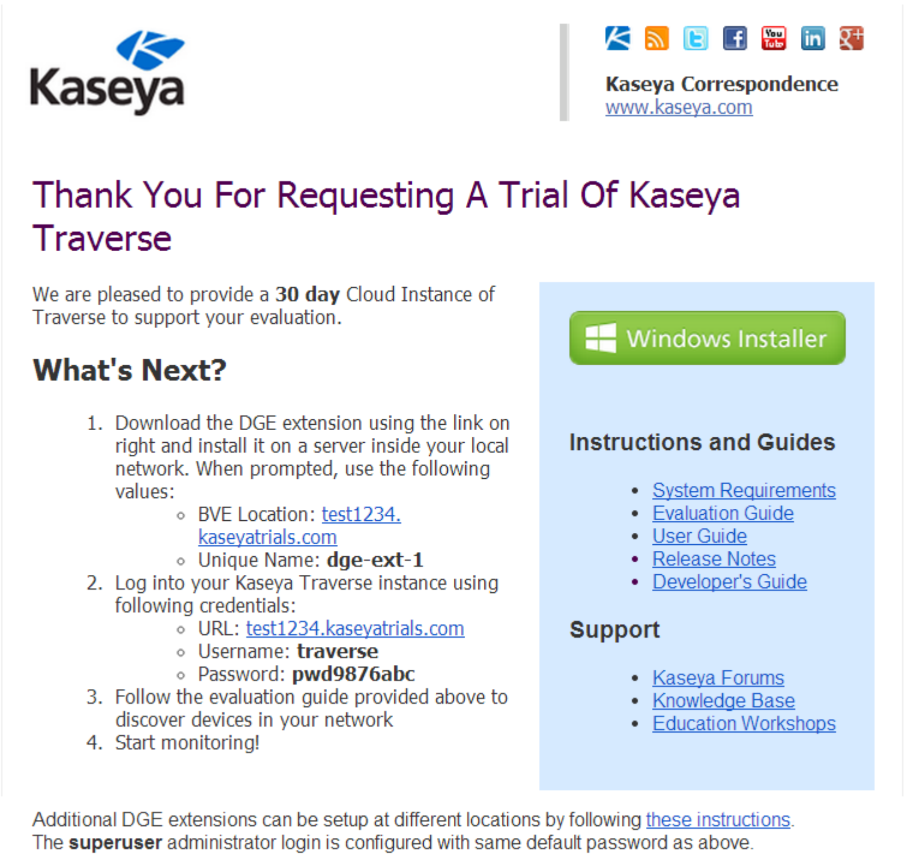
In This Chapter

Getting Started

You can **request either a production or trial subscription to the Kaseya Traverse cloud** *(http://www.kaseya.com/forms/free-trial?prodcode=travsaas)*.

The trial subscription might limit the number of devices that you are allowed to monitor (about 50 devices).

Once your **Traverse** Cloud instance has been created, you will be receive a **Kaseya Traverse** production or trial email similar to the sample image below. The email summarizes 4 simple steps to start monitoring devices on a network.



Kaseya Correspondence
www.kaseya.com

Thank You For Requesting A Trial Of Kaseya Traverse

We are pleased to provide a **30 day** Cloud Instance of Traverse to support your evaluation.

What's Next?

1. Download the DGE extension using the link on right and install it on a server inside your local network. When prompted, use the following values:
   - BVE Location: test1234. kaseyatrials.com
   - Unique Name: **dge-ext-1**
2. Log into your Kaseya Traverse instance using following credentials:
   - URL: test1234.kaseyatrials.com
   - Username: **traverse**
   - Password: **pwd9876abc**
3. Follow the evaluation guide provided above to discover devices in your network
4. Start monitoring!

Windows Installer

Instructions and Guides

- System Requirements
- Evaluation Guide
- User Guide
- Release Notes
- Developer's Guide

Support

- Kaseya Forums
- Knowledge Base
- Education Workshops

Additional DGE extensions can be setup at different locations by following these instructions.
The **superuser** administrator login is configured with same default password as above.

Traverse Module Requirements

Traverse 7.0 requires a *DGE extension* be installed on a network Windows machine, one for each network you intend to monitor. The DGE extension relays collected data to the Traverse cloud website.

> **Note:** Using Netflow requires a larger platform than one without Netflow (**Network Flow Analysis** *(page 31)*).

Without Netflow

- Windows 2003, 2008, 2008 R2, 7, 2012, 2012 R2

- 2 GB RAM
- 10 GB free disk space
- 1 CPU

With Netflow

- Windows 2003, 2008, 2008 R2, 7, 2012, 2012 R2
- 4 GB RAM
- 50 GB disk space
- 2 CPU

Supported Browsers

- Windows
  - Internet Explorer 10 and later
  - FireFox 25 and later
  - Chrome 30 and later
- Apple OS X
  - Safari 6 and later
  - FireFox 25 and later
  - Chrome 30 and later
- In addition, Traverse requires the Adobe Flash Player plugin be installed on your browser.

Disk Space Requirements

- 36 GB free space in a RAID 5 configuration is recommended.
- Additional free space for the `<TRAVERSE_HOME>\logs` directory. Plan for 5 GB of disk space for log files. The default `<TRAVERSE_HOME>` directory is `\Program Files (x86)\Traverse`.

> **Note:** *See* **Installation Prerequisites** *(http://help.kaseya.com/WebHelp/EN/TV/7000000/index.asp#17290.htm).*

Installation Prerequisites

Prior to installing a DGE extension, review the following:

1. Ensure the Windows machine you will install the DGE extension on has access to the internet.
2. Ensure the time on the Windows machine is accurate. Windows includes Internet Time Synchronization software (under **Date & Time**, click the **Internet Time** tab and enable it with default settings). See a detailed explanation below.
3. Identify the administrator password for your Windows servers so that they can be queried using WMI.
4. Identify the username and password with SYSDBA level rights you will use to monitor Oracle databases.
5. Identify, and if necessary, enable the (read-only) SNMP community string (SNMP v1 or v2) or username, password and optionally encryption key (SNMP v3) used by SNMP-capable devices on your network.
6. Update firewall rules and/or access lists (ACL) on routers to allow SNMP queries on the UDP port specified below from the DGE extension 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	DGEx > Cloud	Provisioning Database
(any)	7652	DGEx > Cloud	Provisioning Database
(any)	7653	DGEx > Cloud	Internal Messaging Bus
(any)	9443	DGEx > Cloud	Upstream DGE

Setting the Time on a Non-Domain Server

Since **Traverse** is a distributed platform, it is important to make sure that the time on your DGE extension server is accurate. Windows has a built in time synchronization mechanism to set the time from an internet time server.

> **Note:** For domain machines, time is synchronized from the domain controller.

To set the time on the server running the DGE extension:

- Open Date and Time by clicking the Start button, clicking Control Panel, clicking Clock, Language, and Region, and then clicking **Date and Time**.
- Click the **Internet Time** tab, and then click **Change** settings. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
- Click **Automatically synchronize with an Internet time server**, select a time server, and then click **OK**.

Install the DGE Extension

Identify Your BVE Location and Unique Name

This information is provided by Kaseya and included in **step 1** of the **Kaseya Traverse Evaluation** *(page 2)* email you received. For example:

- BVE Location: `your-unique-site-name.kaseyatrials.com`
- Unique Name: `your-unique-DGE-name`

Download the Installer

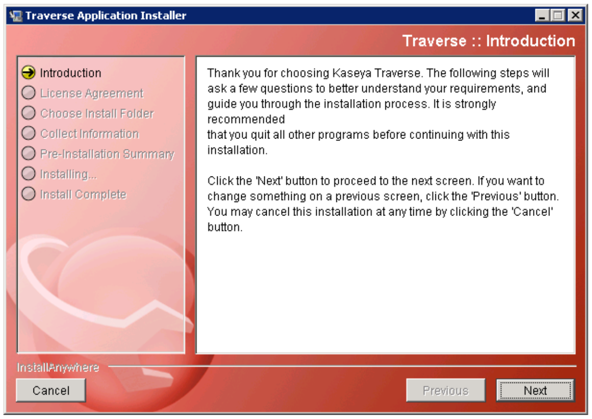
Download the Windows installer for the DGE extension by clicking the **Windows Install** button displayed on the **Kaseya Traverse Evaluation** email.

Run the Installer

Run the installer as a local or domain administrator, not a standard user.

Introduction

Click **Next**.



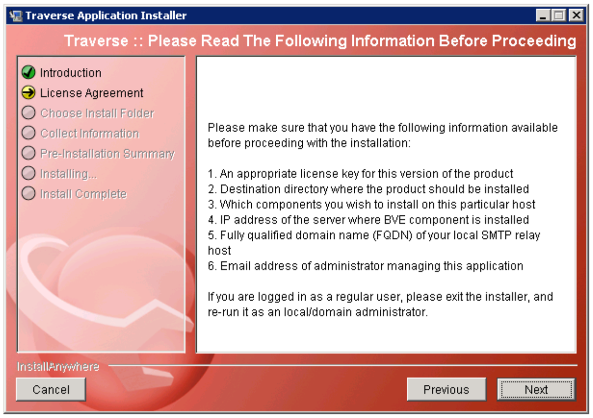
Thank you for choosing Kaseya Traverse. The following steps will ask a few questions to better understand your requirements, and guide you through the installation process. It is strongly recommended
that you quit all other programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button. You may cancel this installation at any time by clicking the 'Cancel' button.

Checklist

Except for running the installer as a local or domain administrator, ignore the instructions on this page.

Click **Next**.



Please make sure that you have the following information available before proceeding with the installation:

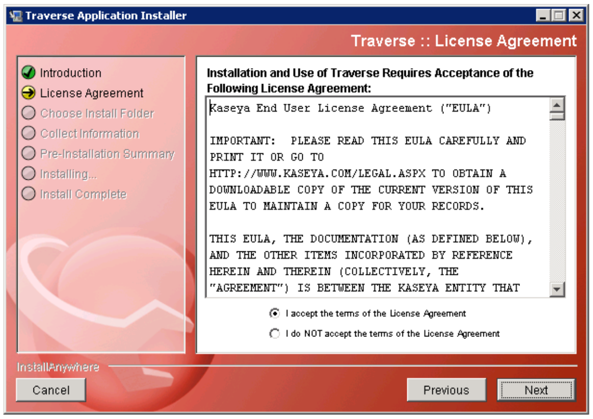
1. An appropriate license key for this version of the product
2. Destination directory where the product should be installed
3. Which components you wish to install on this particular host
4. IP address of the server where BVE component is installed
5. Fully qualified domain name (FQDN) of your local SMTP relay host
6. Email address of administrator managing this application

If you are logged in as a regular user, please exit the installer, and re-run it as an local/domain administrator.

License Agreement

Review the License Agreement, then click the **I accept the terms of the License Agreement** option.

Click **Next**.



Installation and Use of Traverse Requires Acceptance of the Following License Agreement:

```
Kaseya End User License Agreement ("EULA")

IMPORTANT:  PLEASE READ THIS EULA CAREFULLY AND
PRINT IT OR GO TO
HTTP://WWW.KASEYA.COM/LEGAL.ASPX TO OBTAIN A
DOWNLOADABLE COPY OF THE CURRENT VERSION OF THIS
EULA TO MAINTAIN A COPY FOR YOUR RECORDS.

THIS EULA, THE DOCUMENTATION (AS DEFINED BELOW),
AND THE OTHER ITEMS INCORPORATED BY REFERENCE
HEREIN AND THEREIN (COLLECTIVELY, THE
"AGREEMENT") IS BETWEEN THE KASEYA ENTITY THAT
```

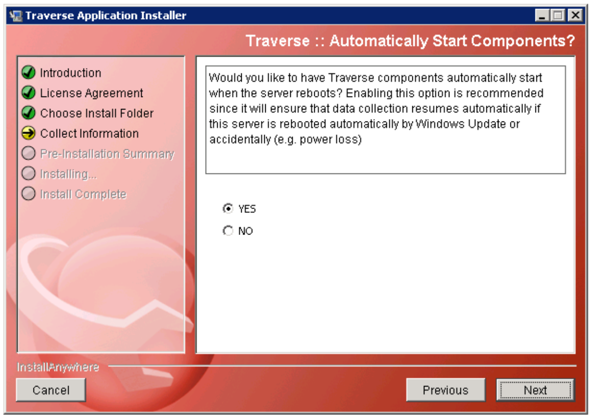
● I accept the terms of the License Agreement

○ I do NOT accept the terms of the License Agreement

Automatically Restart DGE Extension Services After a Reboot

Accepting the default **Yes** option to this prompt is strongly recommended. It ensures all DGE extension services will be restarted if the network Windows machine is rebooted.

Click **Next**.



Traverse :: Automatically Start Components?

Would you like to have Traverse components automatically start when the server reboots? Enabling this option is recommended since it will ensure that data collection resumes automatically if this server is rebooted automatically by Windows Update or accidentally (e.g. power loss)

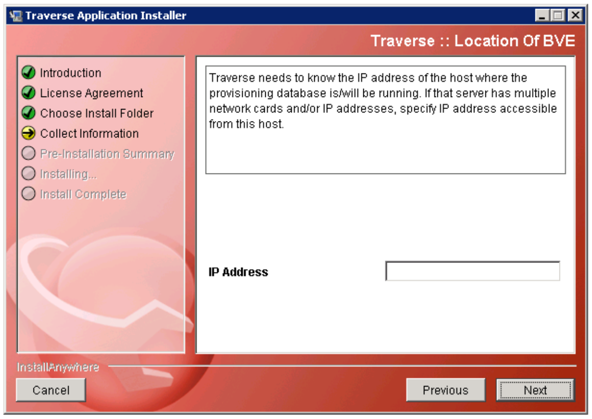
● YES
○ NO

Location BVE

Enter the value for the **BVE Location** you identified in **Install the DGE Extension** *(page 4)* in the **IP Address** field. It should be similar in format to **your-unique-site-name.kaseyatrials.com**.

Note: Do not include an `http://` prefix when you enter this value.

Click **Next**.



Traverse :: Location Of BVE

Traverse needs to know the IP address of the host where the provisioning database is/will be running. If that server has multiple network cards and/or IP addresses, specify IP address accessible from this host.

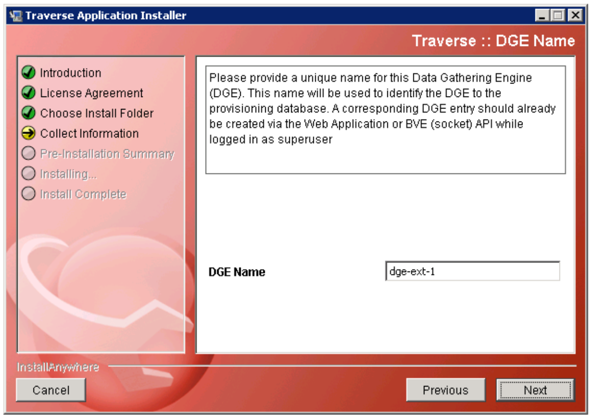
IP Address

DGE Name

Enter the value for the **Unique Name** you identified in **Install the DGE Extension** *(page 4)* above in the **DGE Name** field. It should be similar in format to `your-unique-DGE-name`.

Note: Typically your first DGE extension is called `dge-ext-1`.

Click **Next**.



Traverse Application Installer

Traverse :: DGE Name

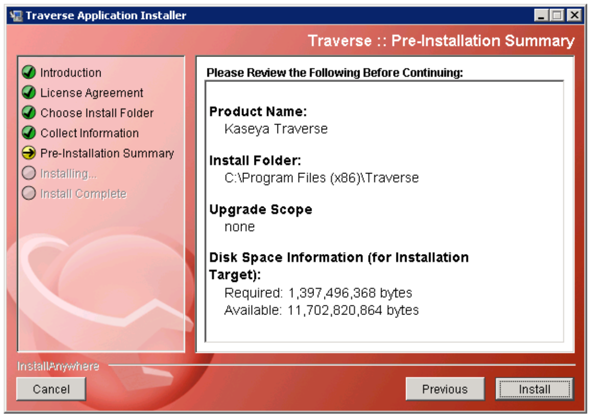
Please provide a unique name for this Data Gathering Engine (DGE). This name will be used to identify the DGE to the provisioning database. A corresponding DGE entry should already be created via the Web Application or BVE (socket) API while logged in as superuser

DGE Name: dge-ext-1

Pre-Installation Summary

Review the following information before beginning the installation.

Click **Install**. It may take a few minutes to complete the install.



Traverse Application Installer

Traverse :: Pre-Installation Summary

Please Review the Following Before Continuing:

Product Name:
Kaseya Traverse

Install Folder:
C:\Program Files (x86)\Traverse

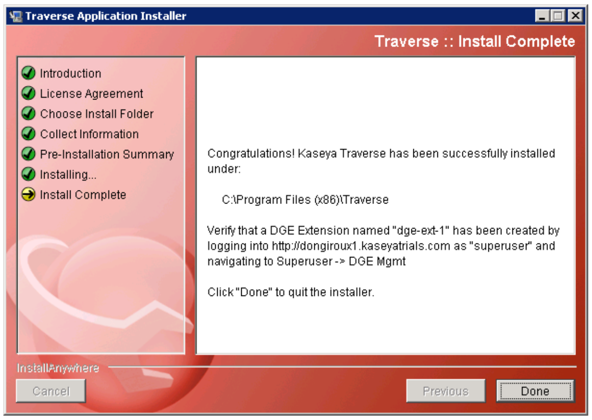
Upgrade Scope
none

Disk Space Information (for Installation Target):
Required: 1,397,496,368 bytes
Available: 11,702,820,864 bytes

Close the Installer

Ensure the text displayed in this box matches the values you were provided in **Install the DGE Extension** *(page 4)*.

> **Note:** The text prompts you to continue by logging on to your unique **Traverse** website, using the username `superuser` and the same assigned password you were provided in the **Kaseya Traverse Evaluation** *(page 2)* email.



Congratulations! Kaseya Traverse has been successfully installed under:

C:\Program Files (x86)\Traverse

Verify that a DGE Extension named "dge-ext-1" has been created by logging into http://dongiroux1.kaseyatrials.com as "superuser" and navigating to Superuser -> DGE Mgmt

Click "Done" to quit the installer.

Traverse Cloud Logon

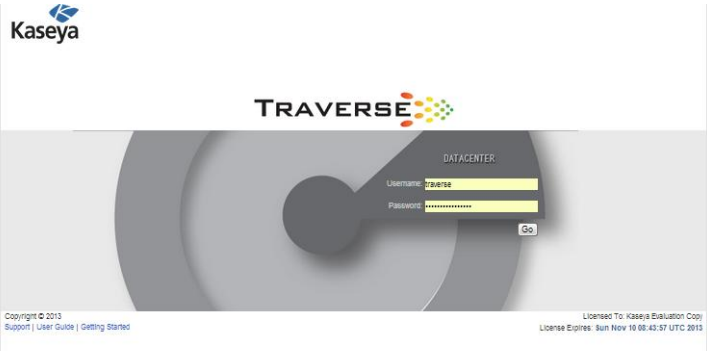
Logon as a Standard User

Identify your **Traverse** Cloud assigned URL, username and password.

This information was included in **step 1** of the **Kaseya Traverse Evaluation** *(page 2)* email you received. For example:

- URL: `your-unique-site-name.kaseyatrials.com`
- Username: `traverse`
- Password: `your-assigned-password`

Use these values to logon to your unique **Traverse** Cloud website as a standard user.



Username: traverse

Password: ••••••••••••••••••

Copyright © 2013

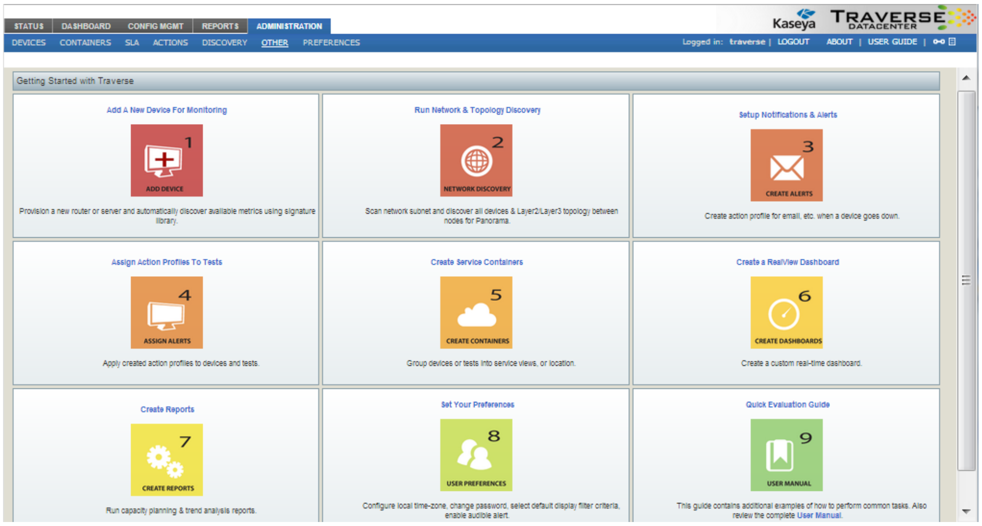
Licensed To: Kaseya Evaluation Copy

License Expires: Sun Nov 10 08:43:57 UTC 2013

Initial Page after Standard User Logon

By default, the first page a standard user sees after logon is the **Getting Started with Traverse** page. You can click any tile to jump immediately to one of these frequently used pages.

You can also navigate to other pages using the menu bar at the top.



Getting Started with Traverse

Add A New Device For Monitoring

Provision a new router or server and automatically discover available metrics using signature library.

Run Network & Topology Discovery

Scan network subnet and discover all devices & Layer2/Layer3 topology between nodes for Panorama.

Setup Notifications & Alerts

Create action profile for email, etc. when a device goes down.

Assign Action Profiles To Tests

Apply created action profiles to devices and tests.

Create Service Containers

Group devices or tests into service views, or location.

Create a RealView Dashboard

Create a custom real-time dashboard.

Create Reports

Run capacity planning & trend analysis reports.

Set Your Preferences

Configure local time-zone, change password, select default display filter criteria, enable audible alert.

Quick Evaluation Guide

This guide contains additional examples of how to perform common tasks. Also review the complete User Manual.

Logon as a Superuser

You can also logon using the administrator-level username `superuser` **and the same assigned password you were provided in the Kaseya Traverse Evaluation** *(page 2)* **email**.

Navigate your browser to the URL you were provided, similar in format to `your-unique-site-name.kaseyatrials.com`

- Username: `superuser`
- Password: `your-assigned-password`

> **Note:** You should only logon as a `superuser` when you need to perform an administrative-level task. Otherwise, logon as a standard user.

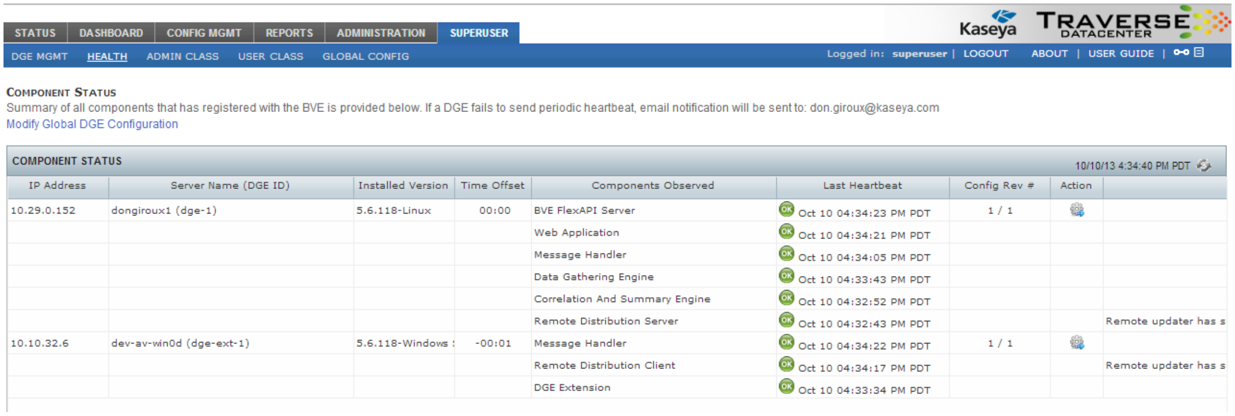
Initial Page after Administrator Logon

> By default, the first page a `superuser` or other administrator sees after logon is the Status > **Departments** page.

Check the Health Status of the DGE Extension

> **Note:** Whenever you install a new DGE extension, you should logon as the `superuser` to verify the connection.

Logon as `superuser`. Navigate to the Superuser > **Health** page. Verify the `IP address` and `Server Name` of the DGE extension you installed. The "heartbeats" for all the components of your DGE extension should display a green OK icon. Logoff when you're done. Re-logon as a standard user to resume normal operations.



COMPONENT STATUS

Summary of all components that has registered with the BVE is provided below. If a DGE fails to send periodic heartbeat, email notification will be sent to: don.giroux@kaseya.com

Modify Global DGE Configuration

COMPONENT STATUS 10/10/13 4:34:40 PM PDT

IP Address	Server Name (DGE ID)	Installed Version	Time Offset	Components Observed	Last Heartbeat	Config Rev #	Action	
10.29.0.152	dongiroux1 (dge-1)	5.6.118-Linux	00:00	BVE FlexAPI Server	OK Oct 10 04:34:23 PM PDT	1 / 1		
				Web Application	OK Oct 10 04:34:21 PM PDT			
				Message Handler	OK Oct 10 04:34:05 PM PDT			
				Data Gathering Engine	OK Oct 10 04:33:43 PM PDT			
				Correlation And Summary Engine	OK Oct 10 04:32:52 PM PDT			
				Remote Distribution Server	OK Oct 10 04:32:43 PM PDT			Remote updater has s
10.10.32.6	dev-av-win0d (dge-ext-1)	5.6.118-Windows :	-00:01	Message Handler	OK Oct 10 04:34:22 PM PDT	1 / 1		
				Remote Distribution Client	OK Oct 10 04:34:17 PM PDT			Remote updater has s
				DGE Extension	OK Oct 10 04:33:34 PM PDT			

A component displays in the status list when the component begins operating. The **Component Status** page includes information about the following:

- IP address of the component
- component name
- the last status update received by the BVE
- the version of the component
- the last action performed on the component

By default, **Traverse** components are configured to send status updates every two minutes. The status changes to a state of "warning" if **Traverse** does not receive an update after more than five minutes. The status changes to "critical" after 10 minutes elapse without **Traverse** receiving an update.

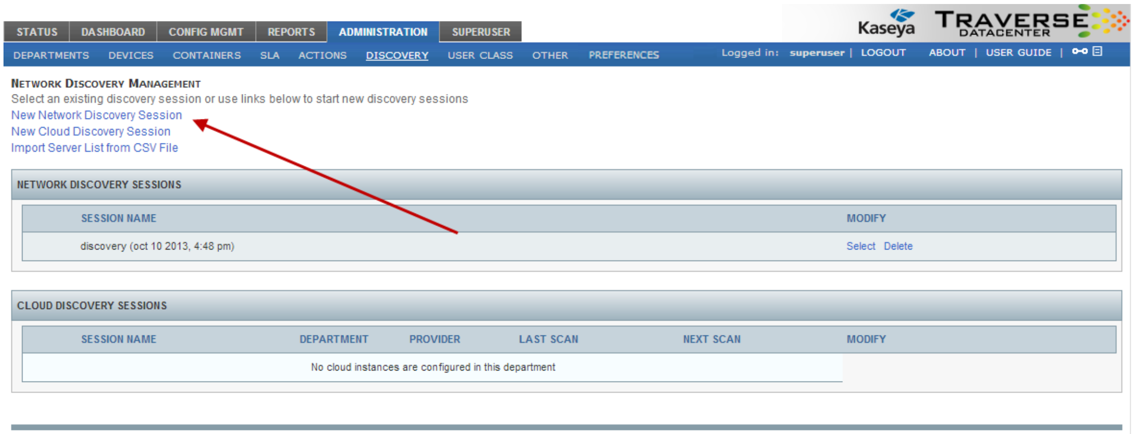
Refresh the **Component Status** page to view the latest **Traverse** component information.

If components are in a "warning" or "critical" state, see **Troubleshooting Traverse** *(http://help.kaseya.com/WebHelp/EN/TV/7000000/index.asp#16912.htm)*.

Run Network Discovery

Traverse can search your network and discover devices. You could add devices manually one at a time, but running network discovery is easier. You should limit the subnets to be included in the discovery to class-C networks instead of class-B or larger.

Start a New Network Discovery Session



NETWORK DISCOVERY MANAGEMENT

Select an existing discovery session or use links below to start new discovery sessions

New Network Discovery Session

New Cloud Discovery Session

Import Server List from CSV File

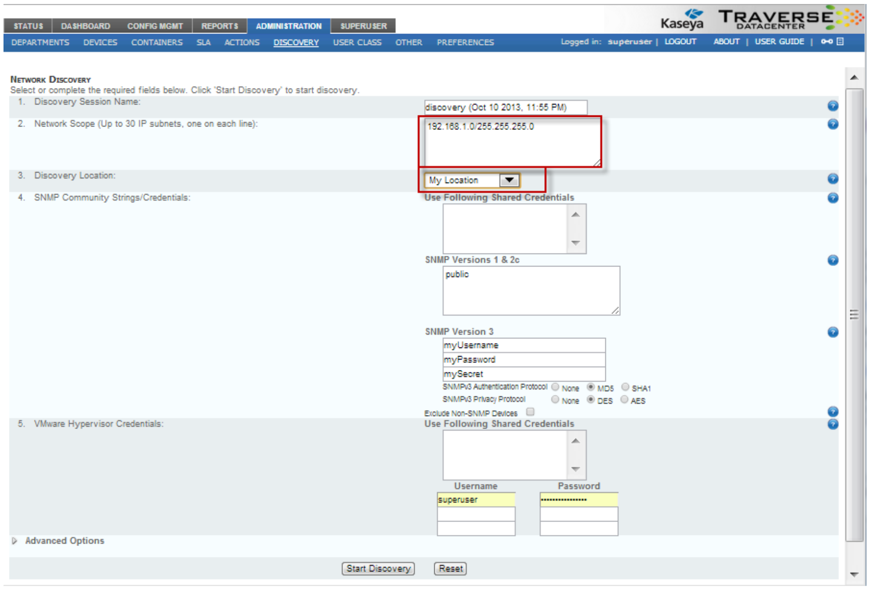
NETWORK DISCOVERY SESSIONS

SESSION NAME	MODIFY
discovery (oct 10 2013, 4:48 pm)	Select Delete

CLOUD DISCOVERY SESSIONS

SESSION NAME	DEPARTMENT	PROVIDER	LAST SCAN	NEXT SCAN	MODIFY
No cloud instances are configured in this department					

1. Logon as `traverse`. Navigate to the Administration > **Discovery** page.
2. Click the **New Network Discovery Session** link.
3. Enter the following values:
   - **Network Scope** - Enter a network subnet starting value followed by the network mask. Example: `192.168.1.0/255.255.255.0`. The DGE extension you installed must have network access to the range of IP addresses you specify.
   - **Discovery Location** - Your DGE extension was assigned a unique location when it was installed. Select it from the drop-down list. Most private networks use the same range of IP addresses. This is how **Traverse** identifies which network you want to run Network Discovery on.
   - **SNMP Community Strings/Credentials** - Optionally enter an SNMP read community name for SNMP-enabled devices on your network. The default community name for SNMP v1 & 2c enabled devices is `public`. Optionally enter a credential for SNMP v3 enabled devices.
   - **VMware Hypervisor Credentials** - Optionally enter a VMware credential to discover additional information about VMware hypervisors.
   - **Advanced Options** - Ignore these advanced features for your first run of network discovery.
4. Click the **Start Discovery** button.



NETWORK DISCOVERY

Select or complete the required fields below. Click 'Start Discovery' to start discovery.

1. Discovery Session Name: discovery (Oct 10 2013, 11:55 PM)
2. Network Scope (Up to 30 IP subnets, one on each line): 192.168.1.0/255.255.255.0
3. Discovery Location: My Location
4. SNMP Community Strings/Credentials: Use Following Shared Credentials

   SNMP Versions 1 & 2c: public

   SNMP Version 3: myUsername, myPassword, mySecret

   SNMPv3 Authentication Protocol ○ None ● MD5 ○ SHA1

   SNMPv3 Privacy Protocol ○ None ● DES ○ AES

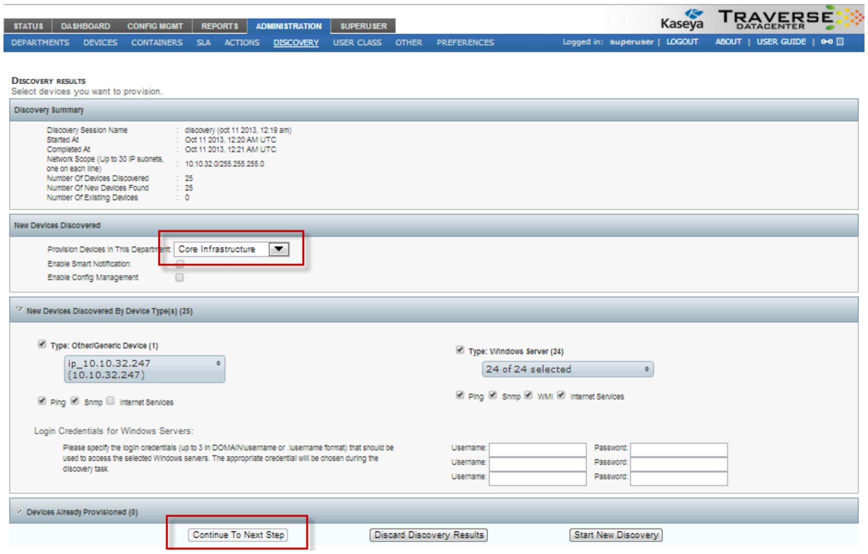
   Exclude Non-SNMP Devices □
5. VMware Hypervisor Credentials: Use Following Shared Credentials

Username	Password
superuser	•••••••••••••••••

▷ Advanced Options

Review Network Discovery Results

1. Review a summary of network **Discovery Results**.
2. Select a **Department**. The default department created for your **Traverse** website is `Core Infrastructure`.
3. Click **Continue to Next Step**.



DISCOVERY RESULTS
Select devices you want to provision.

Discovery Summary

Discovery Session Name	: discovery (oct 11 2013, 12:19 am)
Started At	: Oct 11 2013, 12:20 AM UTC
Completed At	: Oct 11 2013, 12:21 AM UTC
Network Scope (Up to 30 IP subnets, one on each line)	: 10.10.32.0/255.255.255.0
Number Of Devices Discovered	: 25
Number Of New Devices Found	: 25
Number Of Existing Devices	: 0

New Devices Discovered

Provision Devices in This Department: Core Infrastructure
Enable Smart Notification: □
Enable Config Management □

New Devices Discovered By Device Type(s) (25)

☑ Type: Other/Generic Device (1)
ip_10.10.32.247 (10.10.32.247)
☑ Ping ☑ Snmp □ Internet Services

☑ Type: Windows Server (24)
24 of 24 selected
☑ Ping ☑ Snmp ☑ WMI ☑ Internet Services

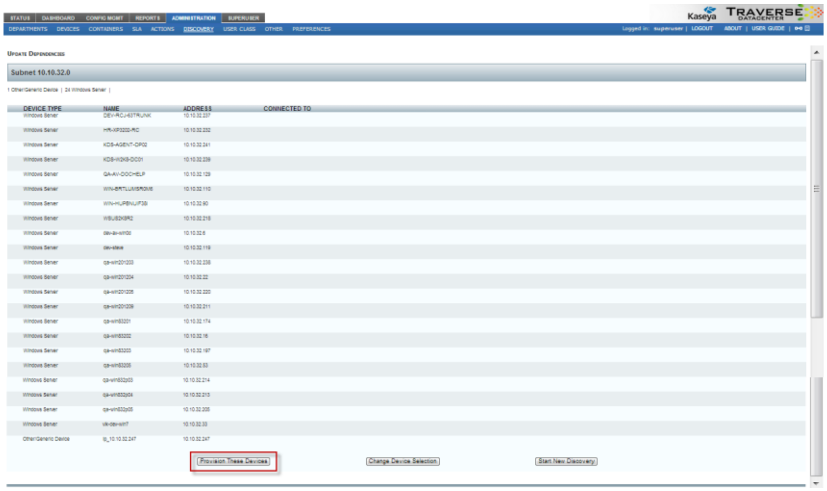
Login Credentials for Windows Servers:
Please specify the login credentials (up to 3 in DOMAIN\username or .\username format) that should be used to access the selected Windows servers. The appropriate credential will be chosen during the discovery task.

Username: Password:
Username: Password:
Username: Password:

Devices Already Provisioned (0)

Assign Standard Monitor Tests to Discovered Devices

1. A list of discovered devices is displayed. Click the **Provision These Devices** button.



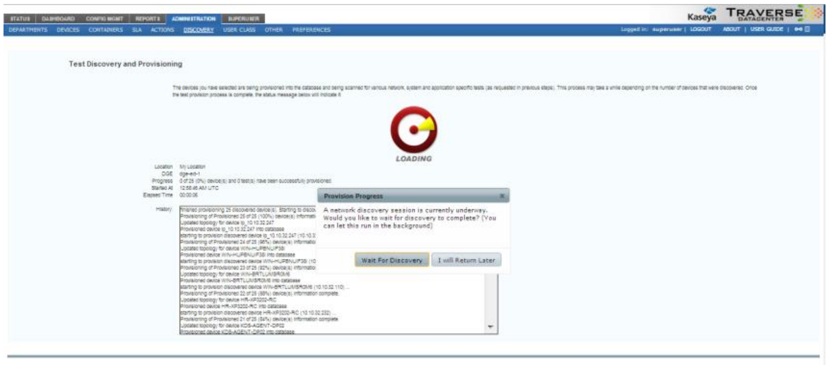
UPDATE DEPENDENCIES

Subnet 10.10.32.0

1 Other/Generic Device | 24 Windows Server |

DEVICE TYPE	NAME	ADDRESS	CONNECTED TO
Windows Server	DEV-RCJ-63TRUNK	10.10.32.237	
Windows Server	HR-XP3202-RC	10.10.32.232	
Windows Server	KDS-AGENT-DP02	10.10.32.241	
Windows Server	KDS-W2K8-DC01	10.10.32.239	
Windows Server	QA-AV-DOCHELP	10.10.32.129	
Windows Server	WIN-BRTLUMSR0M6	10.10.32.110	
Windows Server	WIN-HJPBNUIF38I	10.10.32.90	
Windows Server	WSUS2K8R2	10.10.32.218	
Windows Server	dev-av-win00	10.10.32.6	
Windows Server	dev-steve	10.10.32.119	
Windows Server	qa-win201203	10.10.32.238	
Windows Server	qa-win201204	10.10.32.22	
Windows Server	qa-win201205	10.10.32.220	
Windows Server	qa-win201209	10.10.32.211	
Windows Server	qa-win83201	10.10.32.174	
Windows Server	qa-win83202	10.10.32.16	
Windows Server	qa-win83203	10.10.32.197	
Windows Server	qa-win83205	10.10.32.53	
Windows Server	qa-win832p03	10.10.32.214	
Windows Server	qa-win832p04	10.10.32.213	
Windows Server	qa-win832p05	10.10.32.205	
Windows Server	vik-dev-win7	10.10.32.33	
Other/Generic Device	ip_10.10.32.247	10.10.32.247	

2. Wait for **Traverse** to provision typical monitoring tests for each of your discovered devices.


STATUS | DASHBOARD | CONFIG MGMT | REPORTS | ADMINISTRATION | SUPERUSER
DEPARTMENTS DEVICES CONTAINERS SLA ACTIONS DISCOVERY USER CLASS OTHER PREFERENCES
Logged in: superuser | LOGOUT ABOUT | USER GUIDE
Kaseya TRAVERSE DATACENTER
LOADING

Test Discovery and Provisioning

The devices you have selected are being provisioned into the database and being scanned for various network, system and application specific tests (as requested in previous steps). This process may take a while depending on the number of devices that were discovered. Once the test provision process is complete, the status message below will indicate it.

Location: My Location
DGE: dge-ed-1
Progress: 0 of 25 (0%) device(s) and 0 test(s) have been successfully provisioned.
Started At: 12:58:46 AM UTC
Elapsed Time: 00:00:06

History:

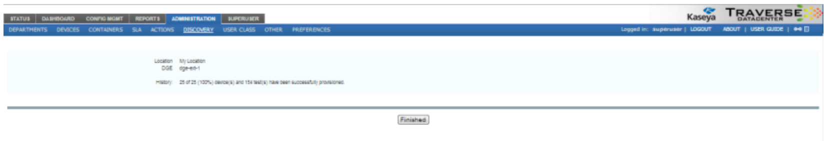
```
Finished provisioning 25 discovered device(s). Starting to disco...
Provisioning of Provisioned 25 of 25 (100%) device(s) informati...
Updated topology for device ip_10.10.32.247
Provisioned device ip_10.10.32.247 into database
starting to provision discovered device ip_10.10.32.247 (10.10.3...
Provisioning of Provisioned 24 of 25 (96%) device(s) informatio...
Updated topology for device WIN-HUPBNUIF38I
Provisioned device WIN-HUPBNUIF38I into database
starting to provision discovered device WIN-HUPBNUIF38I (10...
Provisioning of Provisioned 23 of 25 (92%) device(s) informatio...
Updated topology for device WIN-BRTLUMSR0M6
Provisioned device WIN-BRTLUMSR0M6 into database
starting to provision discovered device WIN-BRTLUMSR0M6 (10.10.32.110) ...
Provisioning of Provisioned 22 of 25 (88%) device(s) information complete.
Updated topology for device HR-XP3202-RC
Provisioned device HR-XP3202-RC into database
starting to provision discovered device HR-XP3202-RC (10.10.32.232) ...
Provisioning of Provisioned 21 of 25 (84%) device(s) information complete.
Updated topology for device KDS-AGENT-DP02
Provisioned device KDS-AGENT-DP02 into database
```

Provision Progress

A network discovery session is currently underway. Would you like to wait for discovery to complete? (You can let this run in the background)

Wait For Discovery | I will Return Later

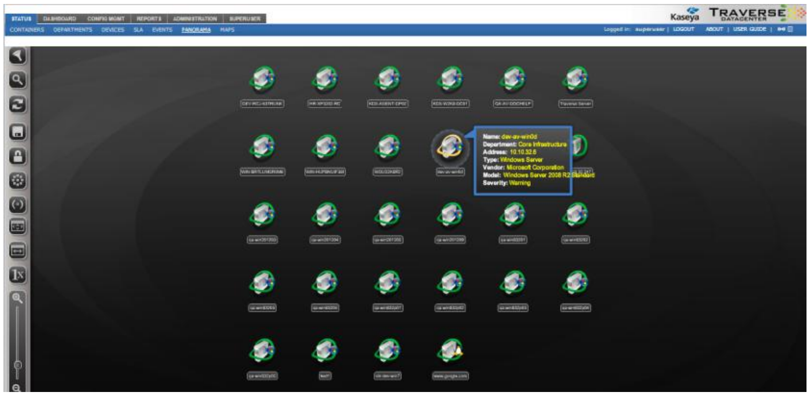
3. Click the **Finished** button to continue.


STATUS | DASHBOARD | CONFIG MGMT | REPORTS | ADMINISTRATION | SUPERUSER
DEPARTMENTS DEVICES CONTAINERS SLA ACTIONS DISCOVERY USER CLASS OTHER PREFERENCES
Logged in: superuser | LOGOUT ABOUT | USER GUIDE
Kaseya TRAVERSE DATACENTER

Location: My Location
DGE: dge-ed-1
History: 25 of 25 (100%) device(s) and 154 test(s) have been successfully provisioned.

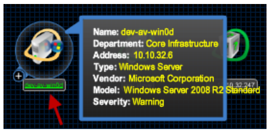
Finished

4. **Traverse** automatically displays the Status > **Panorama** page.
   - Watch **Traverse** construct a topology of monitored devices on your network. This might take a while.
   - Lines are drawn between related nodes on the network. If no lines are shown, your network discovery session did not include the discovery of a router or any other kind of hub, as shown in the image below.
   - Hover the cursor over any node to display a description of the node.


STATUS | DASHBOARD | CONFIG MGMT | REPORTS | ADMINISTRATION | SUPERUSER
CONTAINERS DEPARTMENTS DEVICES SLA EVENTS PANORAMA MAPS
Logged in: superuser | LOGOUT ABOUT | USER GUIDE
Kaseya TRAVERSE DATACENTER

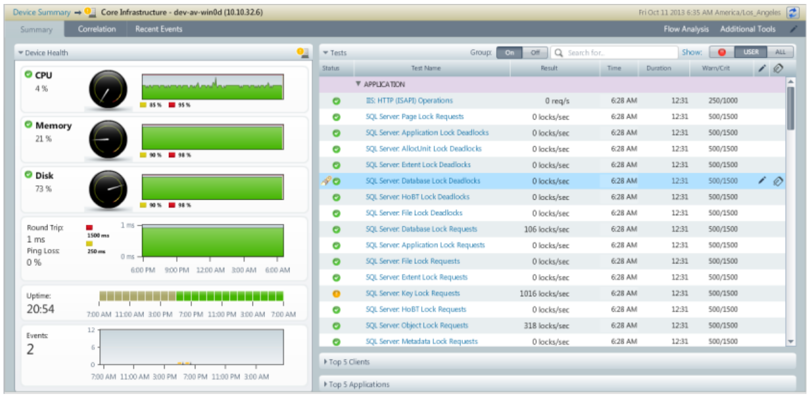
Name: dev-av-win0d
Department: Core Infrastructure
Address: 10.10.32.6
Type: Windows Server
Vendor: Microsoft Corporation
Model: Windows Server 2008 R2 Standard
Severity: Warning

5. Click the **hyperlinked name** of a device to open the **Test Summary** page for that device.



Name: dev-av-win0d
Department: Core Infrastructure
Address: 10.10.32.6
Type: Windows Server
Vendor: Microsoft Corporation
Model: Windows Server 2008 R2 Standard
Severity: Warning

6. The **Device Summary** page displays the status of the device you selected.


Device Summary → Core Infrastructure - dev-av-win0d (10.10.32.6)
Fri Oct 11 2013 6:35 AM America/Los_Angeles
Summary
Correlation
Recent Events
Flow Analysis
Additional Tools
Device Health
Tests
Group: On Off
Search for..
Show: USER ALL
85 % 95 %
90 % 98 %
90 % 98 %
1500 ms
250 ms
1 ms
0 ms
6:00 PM 9:00 PM 12:00 AM 3:00 AM 6:00 AM
7:00 AM 11:00 AM 3:00 PM 7:00 PM 11:00 PM 3:00 AM 7:00 AM
12
6
0
7:00 AM 11:00 AM 3:00 PM 7:00 PM 11:00 PM 3:00 AM
Top 5 Clients
Top 5 Applications

CPU 4 %

Memory 21 %

Disk 73 %

Round Trip: 1 ms

Ping Loss: 0 %

Uptime: 20:54

Events: 2

Status	Test Name	Result	Time	Duration	Warn/Crit
	APPLICATION				
✓	IIS: HTTP (ISAPI) Operations	0 req/s	6:28 AM	12:31	250/1000
✓	SQL Server: Page Lock Requests	0 locks/sec	6:28 AM	12:31	500/1500
✓	SQL Server: Application Lock Deadlocks	0 locks/sec	6:28 AM	12:31	500/1500
✓	SQL Server: AllocUnit Lock Deadlocks	0 locks/sec	6:28 AM	12:31	500/1500
✓	SQL Server: Extent Lock Deadlocks	0 locks/sec	6:28 AM	12:31	500/1500
✓	SQL Server: Database Lock Deadlocks	0 locks/sec	6:28 AM	12:31	500/1500
✓	SQL Server: HoBT Lock Deadlocks	0 locks/sec	6:28 AM	12:31	500/1500
✓	SQL Server: File Lock Deadlocks	0 locks/sec	6:28 AM	12:31	500/1500
✓	SQL Server: Database Lock Requests	106 locks/sec	6:28 AM	12:31	500/1500
✓	SQL Server: Application Lock Requests	0 locks/sec	6:28 AM	12:31	500/1500
✓	SQL Server: File Lock Requests	0 locks/sec	6:28 AM	12:31	500/1500
✓	SQL Server: Extent Lock Requests	0 locks/sec	6:28 AM	12:31	500/1500
!	SQL Server: Key Lock Requests	1016 locks/sec	6:28 AM	12:31	500/1500
✓	SQL Server: HoBT Lock Requests	0 locks/sec	6:28 AM	12:31	500/1500
✓	SQL Server: Object Lock Requests	318 locks/sec	6:28 AM	12:31	500/1500
✓	SQL Server: Metadata Lock Requests	0 locks/sec	6:28 AM	12:31	500/1500

Congratulations! You're monitoring the network!

When your ready, explore additional **Traverse** features using:

- **Basic Configuration** *(page 15)*
- **Advanced Features** *(page 23)*

Chapter 2

Basic Configuration

In This Chapter

Change Your Passwords

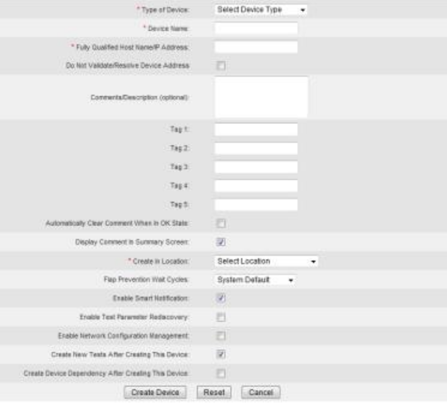
> **Note:** Kaseya strongly urges you to change the passwords you were assigned when your **Traverse** website was created.

1. Navigate to the Administration > **Preferences** page.
2. Change the password for the admin called `superuser`.
3. Change the password for the user called `traverse`.

> **Note:** Unless a feature specifically requires `superuser` access, you should logon as the `traverse` user.

Manually Adding New Devices

Note: You can also add devices automatically, using **Network Discovery** *(page 10)*.



* Type of Device:	Select Device Type ▾
* Device Name:	
* Fully Qualified Host Name/IP Address:	
Do Not Validate/Resolve Device Address:	□
Comments/Description (optional):	
Tag 1:	
Tag 2:	
Tag 3:	
Tag 4:	
Tag 5:	
Automatically Clear Comment When In OK State:	□
Display Comment In Summary Screen:	☑
* Create in Location:	Select Location ▾
Flap Prevention Wait Cycles:	System Default ▾
Enable Smart Notification:	☑
Enable Test Parameter Rediscovery:	□
Enable Network Configuration Management:	□
Create New Tests After Creating This Device:	☑
Create Device Dependency After Creating This Device:	□

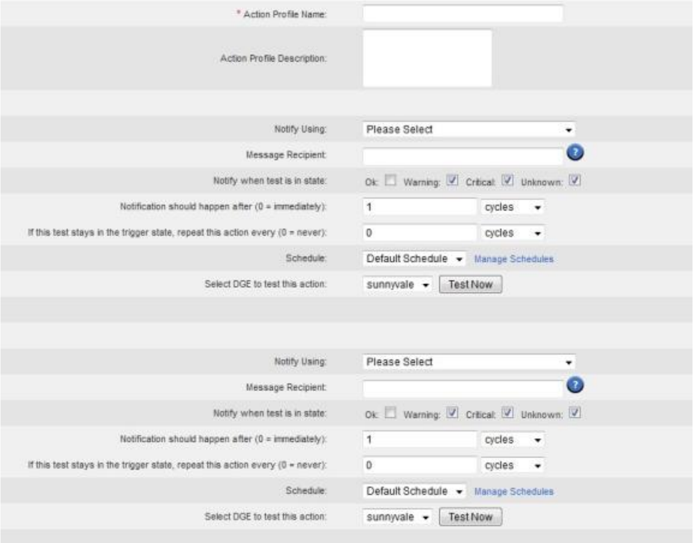
1. Navigate to Administration > Devices > **Create a Device**.
2. Select the device type and provide the device name and IP address or fully qualified host name.
3. The tag fields can be used to give devices arbitrary tags that can be used to search for them later. For example, you might use a tag to 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.

Creating Actions and Schedules

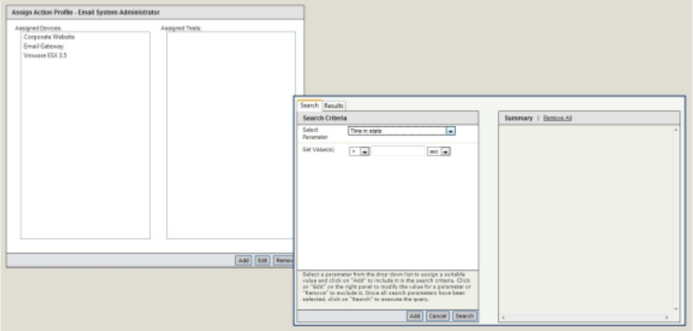
When a test result crosses a threshold, **Traverse** takes action based on rules defined in action profiles. Some possible actions include sending email, sending SNMP traps, opening trouble tickets, or running an external script.

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 Test Now
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 Test Now

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**.



Assign Action Profile - Email System Administrator

Assigned Devices:
Corporate Website
Email Gateway
Vmware ESX 3.5

Assigned Tests:

Search Criteria

Select Parameter: Time in state

Set Value(s): > sec

Select a parameter from the drop-down list to assign a suitable value and click on "Add" to include it in the search criteria. Click on "Edit" on the right panel to modify the value for a parameter or "Remove" to exclude it. Once all search parameters have been selected, click on "Search" to execute the query.

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.

Adjusting Thresholds & Baselining

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 option is under Administration > Devices > **Test Baseline Management**.

Adaptive Thresholds

Traverse also supports dynamic, **Adaptive Thresholds**. This feature 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. Currently you have to enable this on a per test basis. To access this feature for a test:

1. Select a device and display its tests by going to Administration > Devices > **Tests**
2. Then click on the **Modify** button for a test, and select the **Time Based Threshold** checkbox.
3. You can either click on the **Configure** link if you want to set the thresholds manually, or else you can configure the thresholds automatically using the baselining feature by going to Administration > Devices > **Test Baseline Management**.

4. Click on the **Submit** button.

Generating Reports

Traverse has extensive and flexible reporting generated in real time from data collected by your DGE extensions and relayed to your **Traverse** instance in the cloud. 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

There 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**.

Ad Hoc Reports (My Reports)

Users can create ad hoc 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.

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 Reports > Emailed > **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.

Security Model

The **Traverse** security model controls user access to the data generated by customer networks and to **Traverse** user functions that act on that data.

Note: A full description of the security model is described in **Users and Departments** (*http://help.kaseya.com/WebHelp/EN/TV/7000000/index.asp#17371.htm*) in the *Traverse User Guide*.

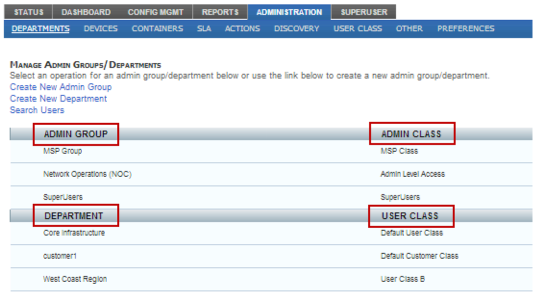
To help quickstart your deployment of **Traverse**, the most common security scenario for MSPs is described below. This configuration will ensure that *all* your MSPs have access *across all* departments. Keep in mind the following guidelines:

- Create a unique **department** for each customer organization. You may need to create more than one department for larger organizations.
- Ensure all the departments you create use the same, single **user class**.
- Define the customers of MSPs as **users** of a selected department. Users of departments only have access to the data in their own department. A department user with the same name as the department is created automatically for you, each time you create a department.
- Define all MSPs as users of the same, single **admin group**. Each admin group can only be assigned to one **admin class**. *Ensure the admin class you select is mapped to the single user class you are using for all your departments.*

Some of the steps below require `superuser` access. Your configuration steps make use of the following pages, in case you have to return to them.

- Superuser > **User Class**
- Superuser > **Admin Class**
- Administration > **Departments**

When you're done, review the Administration > **Departments** page. It's a good way to summarize your security configuration, as shown in the example below:



MANAGE ADMIN GROUPS/ DEPARTMENTS
Select an operation for an admin group/department below or use the link below to create a new admin group/department.
Create New Admin Group
Create New Department
Search Users

ADMIN GROUP	ADMIN CLASS
MSP Group	MSP Class
Network Operations (NOC)	Admin Level Access
SuperUsers	SuperUsers

DEPARTMENT	USER CLASS
Core Infrastructure	Default User Class
customer1	Default Customer Class
West Coast Region	User Class B

Configure an Admin Group and Admins

1. Log in to your **Traverse** website as `superuser`.
2. Navigate to Superuser > **User Class** and click on **Update** for the `Default User Class`.
3. Change the name to be `Default Customer Class` and click **Update User Class**. Alternatively, you can create a new user class instead of renaming the existing one.
4. Navigate to Superuser > **Admin Class** and create a new admin class called `MSP Class`.
5. Now click **User Class Mappings** and then **Assign User Class to Admin Class**. Select the default grid that is presented and click the **Update Privileges** button.
6. Navigate to Administration > **Departments** and click **Create new Admin Group**. Create a new admin group called `MSP Group` belonging to the `MSP Class`.
7. Create new users in the `MSP Group` for each of your staff by going to Administration > **Departments** and clicking on **Create User**.
8. At this point, you have the basic security model setup with all your staff belonging to `MSP Group`.

Configure a Department and User

1. Log into your **Traverse** website as `superuser`.
2. Navigate to Administration > **Departments** and then click **Create New Department**.

3. Give a meaningful name to the department. *A default user will be automatically be created with the same name as the Department name.* You can provide this user logon to the MSP's customer if the customer requests access.
4. Ensure the new department uses the `Default Customer Class` described in step 2 of the previous procedure.
5. You can optionally create a **Read Only** user for this same department. Click **Create User** and add a new user. Using the user's email address as the login is recommended. Make sure you set the user's role to **Read Only** when you do.

> **Creating URL with auto-login:** You can create a URL with an encrypted username and password to do autologin for a single **Traverse** page by using the Auto-Login URL generator at **www.zyrion.com/support/tools/urlgen/** *(http://www.zyrion.com/support/tools/urlgen/)*

Adding Additional DGE Extensions

Installing a DGE extension is required to relay monitoring data from a local network to your **Traverse** website. Use the following procedure for creating *additional* DGE extensions.

> **Note:** Adding **additional** DGE extensions to your **Traverse** Cloud instance requires a different procedure than the one used to install your first DGE extension.

1. Navigate to Superuser > **DGE Mgmt**.
2. Click **Create New DGE Extension**.
3. Provide a unique name like `dgex-customerA`.
4. Give a suitable **Description** to identify the customer.
5. Select the upstream DGE name from the drop down list. This is the **Upstream DGE Name** *(page 2)* you were originally assigned when your **Traverse** website was created. Unless support has created additional upstream DGEs for you, there should only be one upstream DGE you can select.
6. Select the **Upstream DGE Fully Qualified Host Name/IP Address**. This is `your-unique-site-name.kaseyatrials.com` without the `http://` prefix.
7. Click on **Create DGE Extension**.
8. Run the DGE extension installer.
9. Installations steps are **described in detail here** *(page 5)*.
10. When the installer prompts you to enter a **DGE Name**, ensure it matches the **Unique Name** you just specified above for the new DGE extension you are creating.
11. Finish up by confirming the "health" of the new DGE extension, **as described in the installation procedure** *(page 9)*.
12. You are now ready to provision the monitoring of devices for this new network by running **Network Discovery** *(page 10)* or by adding devices and tests manually.

Branding (Logos)

If the provided **Traverse** license permits you to change the logo, you can set the logo and theme and custom URL for each of the customers (and intermediate MSPs) by logging in as `superuser` and going to Administration > **Departments** and selecting **Themes** from the **Modify** column.

Chapter 3

Advanced Features

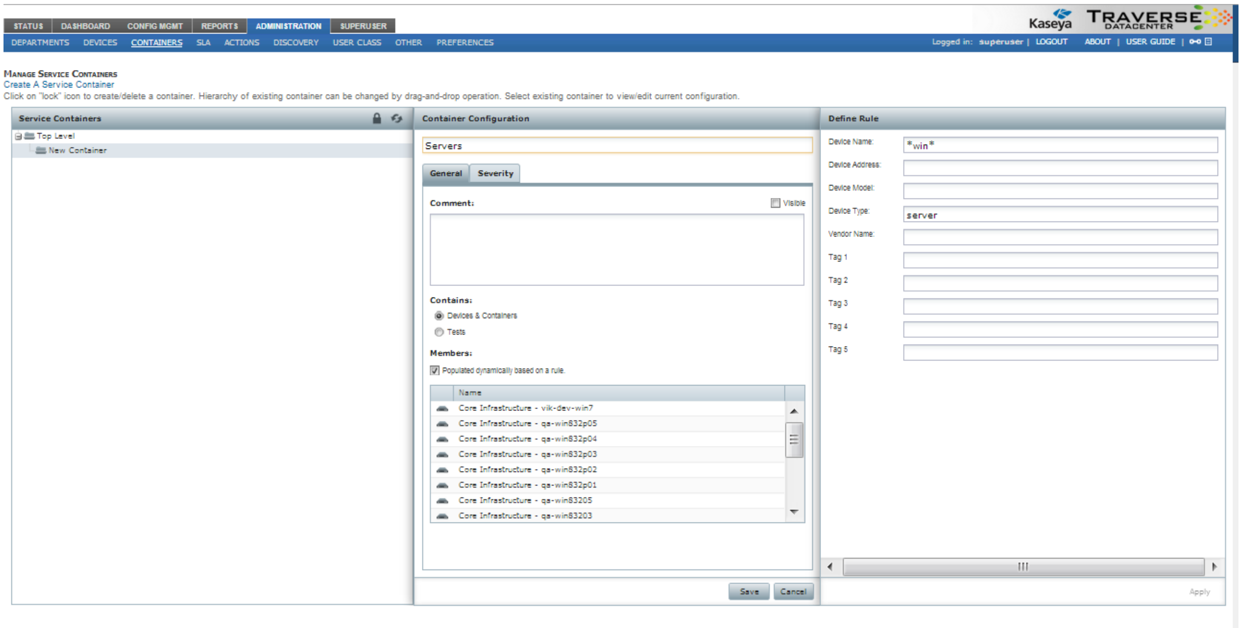
In This Chapter

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 for Devices

1. Navigate to Administration > Containers > **Create a Service Container**. A middle **Container Configuration** panel displays.
2. Enter `Servers` in the field at the top of the **Container Configuration** panel.
3. Select the **Contains: Devices & Containers** option.
4. You can assign devices to a container either by performing a search in the right hand panel and manually selecting the devices to include, or by specifying rules and having the results automatically assigned to the container.
5. For this example, check the **Populated dynamically based on a rule** checkbox. A **Define Rule** panel slides in from the right side of the page. Enter `server` in the **Device Type** field. Click **Apply** to see which devices match this rule. You can add additional rules, such as entering `*win*` in the **Device Name** field to filter the list of devices found even further.
6. Click the **Severity** tab in the middle panel when you are done.



MANAGE SERVICE CONTAINERS
Create A Service Container
Click on "lock" icon to create/delete a container. Hierarchy of existing container can be changed by drag-and-drop operation. Select existing container to view/edit current configuration.

Servers

Comment: □ Visible

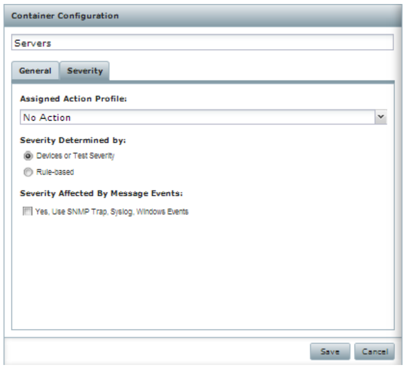
Contains:
● Devices & Containers
○ Tests

Members:
☑ Populated dynamically based on a rule.

Name
Core Infrastructure - vik-dev-win7
Core Infrastructure - qa-win832p05
Core Infrastructure - qa-win832p04
Core Infrastructure - qa-win832p03
Core Infrastructure - qa-win832p02
Core Infrastructure - qa-win832p01
Core Infrastructure - qa-win83205
Core Infrastructure - qa-win83203

Device Name: *win*
Device Address:
Device Model:
Device Type: server
Vendor Name:
Tag 1
Tag 2
Tag 3
Tag 4
Tag 5

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



Container Configuration

Servers

General | Severity

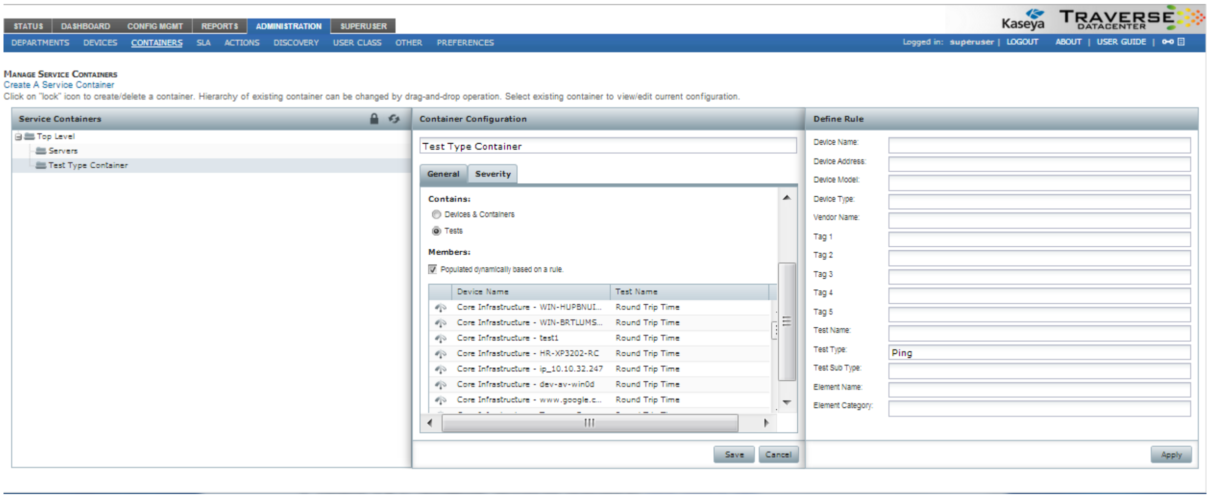
Assigned Action Profile: No Action

Severity Determined by:
● Devices or Test Severity
○ Rule-based

Severity Affected By Message Events:
☐ Yes, Use SNMP Trap, Syslog, Windows Events

Creating a Service Container for Monitoring Tests

1. Navigate to Administration > Containers > **Create a Service Container**.
2. Enter `Test Type Container` in the field at the top of the **Container Configuration** panel.
3. Select the **Contains: Tests** option.
4. You can assign monitoring tests to a container either by performing a search in the right hand panel and manually selecting the test to include, or by specifying rules and having the results automatically assigned to the container.
5. For this example, check the **Populated dynamically based on a rule** checkbox. A **Define Rule** panel slides in from the right side of the page. Enter `Ping` in the **Test Type** field. Click **Apply** to see which devices have tests that match this rule.
6. Click the **Severity** tab in the middle panel.
7. Assign an action profile if desired, decide the criteria for determining the severity status of the container, and then click **Save**.



Manage Service Containers

Create A Service Container

Click on "lock" icon to create/delete a container. Hierarchy of existing container can be changed by drag-and-drop operation. Select existing container to view/edit current configuration.

Service Containers

- Top Level
  - Servers
  - Test Type Container

Container Configuration

Test Type Container

General | Severity

Contains:
○ Devices & Containers
● Tests

Members:
☑ Populated dynamically based on a rule.

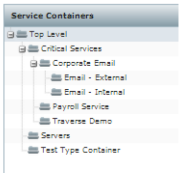
Device Name	Test Name
Core Infrastructure - WIN-HUPBNUI...	Round Trip Time
Core Infrastructure - WIN-BRTLUMS...	Round Trip Time
Core Infrastructure - test1	Round Trip Time
Core Infrastructure - HR-XP3202-RC	Round Trip Time
Core Infrastructure - ip_10.10.32.247	Round Trip Time
Core Infrastructure - dev-av-win0d	Round Trip Time
Core Infrastructure - www.google.c...	Round Trip Time

Define Rule

Device Name:
Device Address:
Device Model:
Device Type:
Vendor Name:
Tag 1
Tag 2
Tag 3
Tag 4
Tag 5
Test Name:
Test Type: Ping
Test Sub Type:
Element Name:
Element Category:

Nesting Service Containers

You can nest service containers to build a logical hierarchy of your environment. For example, you might have critical services for different departments within an organization, all contained within a `Critical Services` container.



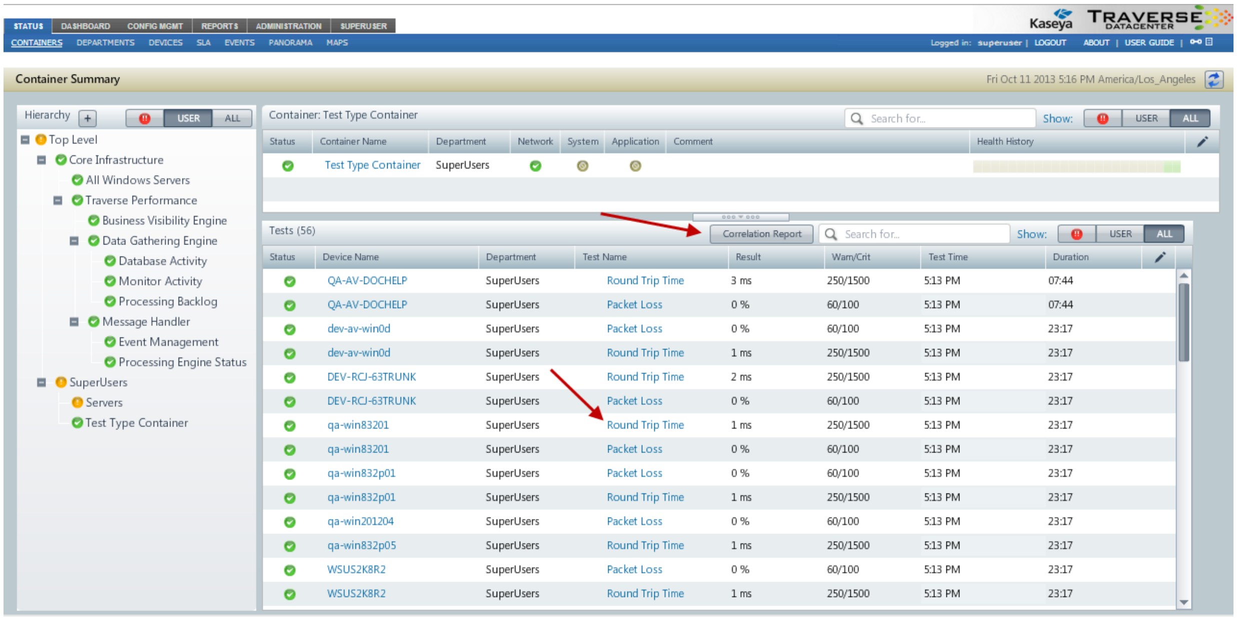
Service Containers

- Top Level
  - Critical Services
    - Corporate Email
      - Email - External
      - Email - Internal
    - Payroll Service
    - Traverse Demo
  - Servers
  - Test Type Container

Examining Service Container Status

1. Navigate to Status > **Containers** to view a status summary for all containers. **Traverse** provides a number of built-in containers ready to use.
2. Click on a container name to list its contents.
3. Drill down into the container hierarchy to reach a test container. Then click the **Correlation Report** button at the top of the page 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.

Note: The ❗ USER ALL options filters the hierarchy of containers in the left hand panel, and items displayed in the right hand panel, *by their state*. Set state filter preferences for the **User** option using the Administration > Preferences > **Only Show Devices In Following State(s) When Filter Is On** settings.



Container Summary

Fri Oct 11 2013 5:16 PM America/Los_Angeles

- Top Level
  - Core Infrastructure
    - All Windows Servers
    - Traverse Performance
      - Business Visibility Engine
      - Data Gathering Engine
        - Database Activity
        - Monitor Activity
        - Processing Backlog
      - Message Handler
        - Event Management
        - Processing Engine Status
  - SuperUsers
    - Servers
    - Test Type Container

Container: Test Type Container

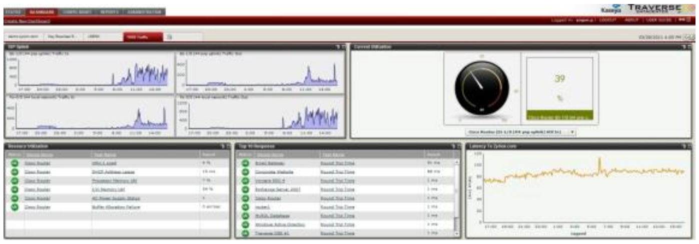
Status	Container Name	Department	Network	System	Application	Comment	Health History
✓	Test Type Container	SuperUsers	✓	●	●		

Tests (56)

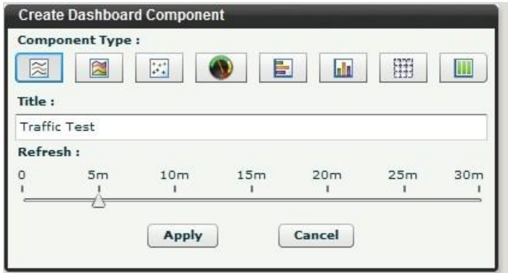
Status	Device Name	Department	Test Name	Result	Warn/Crit	Test Time	Duration
✓	QA-AV-DOCHELP	SuperUsers	Round Trip Time	3 ms	250/1500	5:13 PM	07:44
✓	QA-AV-DOCHELP	SuperUsers	Packet Loss	0 %	60/100	5:13 PM	07:44
✓	dev-av-win0d	SuperUsers	Packet Loss	0 %	60/100	5:13 PM	23:17
✓	dev-av-win0d	SuperUsers	Round Trip Time	1 ms	250/1500	5:13 PM	23:17
✓	DEV-RCJ-63TRUNK	SuperUsers	Round Trip Time	2 ms	250/1500	5:13 PM	23:17
✓	DEV-RCJ-63TRUNK	SuperUsers	Packet Loss	0 %	60/100	5:13 PM	23:17
✓	qa-win83201	SuperUsers	Round Trip Time	1 ms	250/1500	5:13 PM	23:17
✓	qa-win83201	SuperUsers	Packet Loss	0 %	60/100	5:13 PM	23:17
✓	qa-win832p01	SuperUsers	Packet Loss	0 %	60/100	5:13 PM	23:17
✓	qa-win832p01	SuperUsers	Round Trip Time	1 ms	250/1500	5:13 PM	23:17
✓	qa-win201204	SuperUsers	Packet Loss	0 %	60/100	5:13 PM	23:17
✓	qa-win832p05	SuperUsers	Round Trip Time	1 ms	250/1500	5:13 PM	23:17
✓	WSUS2K8R2	SuperUsers	Packet Loss	0 %	60/100	5:13 PM	23:17
✓	WSUS2K8R2	SuperUsers	Round Trip Time	1 ms	250/1500	5:13 PM	23:17

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**.



Create Dashboard Component

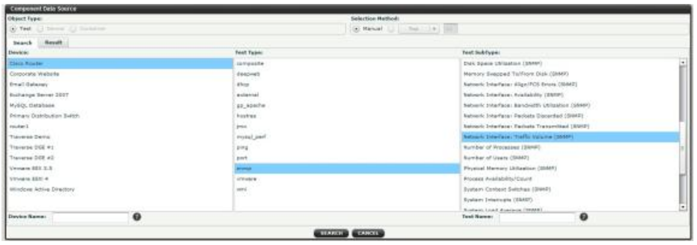
Component Type :

Title :

Traffic Test

Refresh :

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**.



Component Data Source

Object Type: ● Test ○ Device ○ Dashboard

Selection Method: ● Manual

Device: Cisco Router, Corporate Website, Email Gateway, Exchange Server 2007, MySQL Database, Primary Distribution Switch, router1, Traverse Demo, Traverse DGE #1, Traverse DGE #2, Vmware ESX 3.5, VMware ESX 4, Windows Active Directory

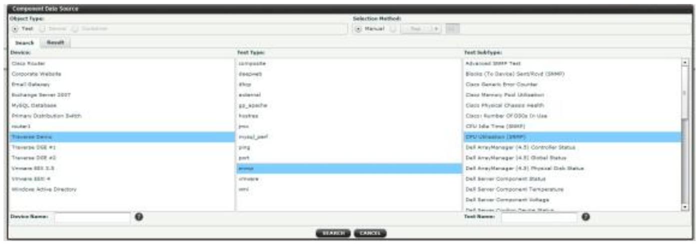
Test Type: composite, deepweb, dhcp, external, gp_apache, hostres, jmx, mysql_perf, ping, port, snmp, vmware, wmi

Test SubType: Disk Space Utilization (SNMP), Memory Swapped To/From Disk (SNMP), Network Interface: Align/FCS Errors (SNMP), Network Interface: Availability (SNMP), Network Interface: Bandwidth Utilization (SNMP), Network Interface: Packets Discarded (SNMP), Network Interface: Packets Transmitted (SNMP), Network Interface: Traffic Volume (SNMP), Number of Processes (SNMP), Number of Users (SNMP), Physical Memory Utilization (SNMP), Process Availability/Count, System Context Switches (SNMP), System Interrupts (SNMP), System Load Average (SNMP)

Device Name:

Test Name:

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**.



Component Data Source

Object Type: ● Test ○ Device ○ Dashboard

Selection Method: ● Manual

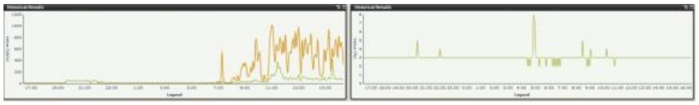
Device: Cisco Router, Corporate Website, Email Gateway, Exchange Server 2007, MySQL Database, Primary Distribution Switch, router1, Traverse Demo, Traverse DGE #1, Traverse DGE #2, Vmware ESX 3.5, VMware ESX 4, Windows Active Directory

Test Type: composite, deepweb, dhcp, external, gp_apache, hostres, jmx, mysql_perf, ping, port, snmp, vmware, wmi

Test SubType: Advanced SNMP Test, Blocks (To Device) Sent/Rcvd (SNMP), Cisco Generic Error Counter, Cisco Memory Pool Utilization, Cisco Physical Chassis Health, Cisco: Number Of DSOs In Use, CPU Idle Time (SNMP), CPU Utilization (SNMP), Dell ArrayManager (4.5) Controller Status, Dell ArrayManager (4.5) Global Status, Dell ArrayManager (4.5) Physical Disk Status, Dell Server Component Status, Dell Server Component Temperature, Dell Server Component Voltage, Dell Server Cooling Device Status

Device Name:

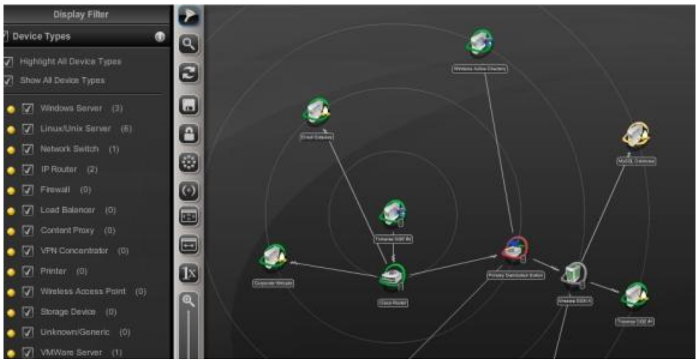
Test Name:



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.



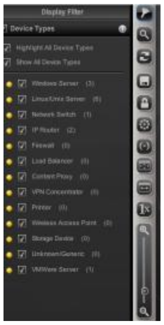
Display Filter

☑ Device Types

☑ Highlight All Device Types
☑ Show All Device Types

● ☑ Windows Server (3)
● ☑ Linux/Unix Server (6)
● ☑ Network Switch (1)
● ☑ IP Router (2)
● ☑ Firewall (0)
● ☑ Load Balancer (0)
● ☑ Content Proxy (0)
● ☑ VPN Concentrator (0)
● ☑ Printer (0)
● ☑ Wireless Access Point (0)
● ☑ Storage Device (0)
● ☑ Unknown/Generic (0)
● ☑ VMWare Server (1)

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.



Display Filter

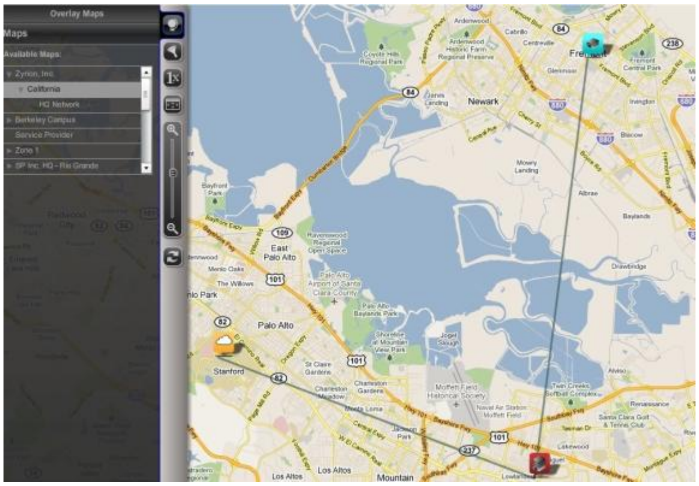
☑ Device Types

☑ Highlight All Device Types
☑ Show All Device Types

● ☑ Windows Server (3)
● ☑ Linux/Unix Server (6)
● ☑ Network Switch (1)
● ☑ IP Router (2)
● ☑ Firewall (0)
● ☑ Load Balancer (0)
● ☑ Content Proxy (0)
● ☑ VPN Concentrator (0)
● ☑ Printer (0)
● ☑ Wireless Access Point (0)
● ☑ Storage Device (0)
● ☑ Unknown/Generic (0)
● ☑ VMWare Server (1)

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.

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

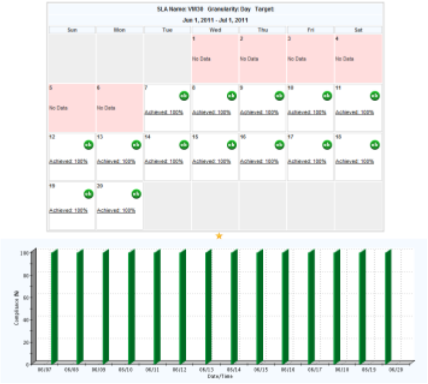


Creating an SLA Measurement

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**.
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.
4. 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**.
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 need, and then click **Apply** to run the search.
6. 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**.
7. 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**.
8. Use the **Add**, **Edit**, and **Remove** buttons to make any further changes to the devices and tests you want to include.
9. Click **Done** to finish creating the SLA measurement.

10. Navigate to Status > **SLA** to view real-time data for your SLA metrics on the SLA Manager dashboard.



Event Manager and Message Handler

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

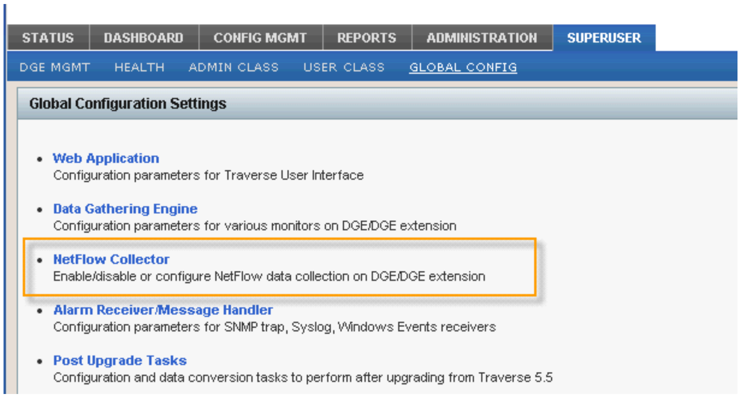
1. Navigate to Status > **Events**.
2. From the **Event Manager** console you can acknowledge, suppress, and delete events. Events can be suppressed until a particular date and time, or until the state changes. The screen refreshes automatically every few minutes (this interval can be changed on the 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 **Event Manager** console and can trigger actions and notifications. For more information on configuring the **Message Handler**, see the **Message Handler for Traps and Logs** *(http://help.kaseya.com/WebHelp/EN/TV/7000000/index.asp#16774.htm)* in the *Traverse User Guide*.

Configuring NetFlow Collectors

Traverse has an integrated NetFlow collector which is pre-installed, but disabled by default.

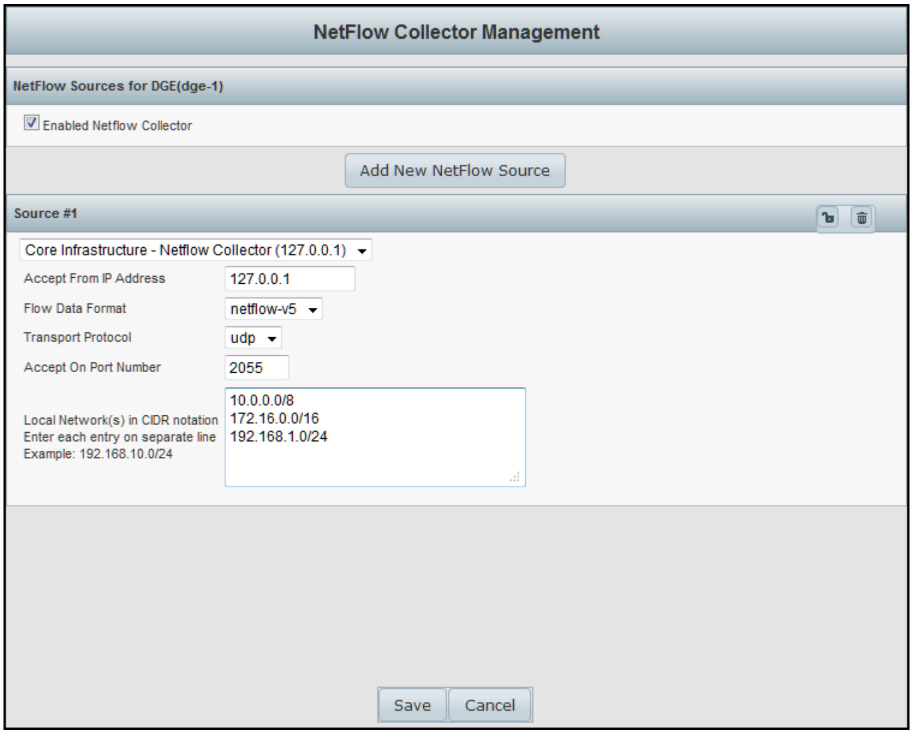
1. Login to **Traverse** as superuser, or an equivalent user.
2. Navigate to the Superuser > Global Config > **Netflow Collector** page.



Global Configuration Settings

- Web Application
  Configuration parameters for Traverse User Interface
- Data Gathering Engine
  Configuration parameters for various monitors on DGE/DGE extension
- NetFlow Collector
  Enable/disable or configure NetFlow data collection on DGE/DGE extension
- Alarm Receiver/Message Handler
  Configuration parameters for SNMP trap, Syslog, Windows Events receivers
- Post Upgrade Tasks
  Configuration and data conversion tasks to perform after upgrading from Traverse 5.5

3. Choose the DGE or DGE extension you wish to add a netflow collector on, and select **Update**.
4. Enable the netflow collector, then choose a device from your list of network devices. Only routers, switches, and firewalls can be used as flow sources. Choose the host to allow flow data from. This allows you to send flow data from the loopback interface, or from a different IP than the one provisioned in **Traverse**). Choose the port, and the protocol that **Traverse** will accept. Additionally, you can specify the network that is "inside" of this device, so that **Traverse** can categorize the data from an internal/external standpoint.



NetFlow Collector Management

NetFlow Sources for DGE(dge-1)

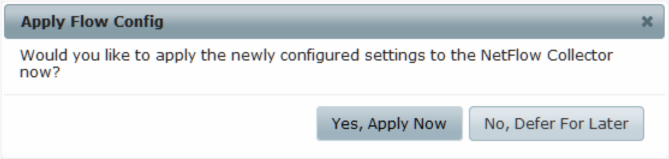
☑ Enabled Netflow Collector

Source #1

Core Infrastructure - Netflow Collector (127.0.0.1)

Accept From IP Address	127.0.0.1
Flow Data Format	netflow-v5
Transport Protocol	udp
Accept On Port Number	2055
Local Network(s) in CIDR notation Enter each entry on separate line Example: 192.168.10.0/24	10.0.0.0/8 172.16.0.0/16 192.168.1.0/24

5. Press the **Save** button when you are done. **Traverse** will respond with the following prompt:



Apply Flow Config

Would you like to apply the newly configured settings to the NetFlow Collector now?

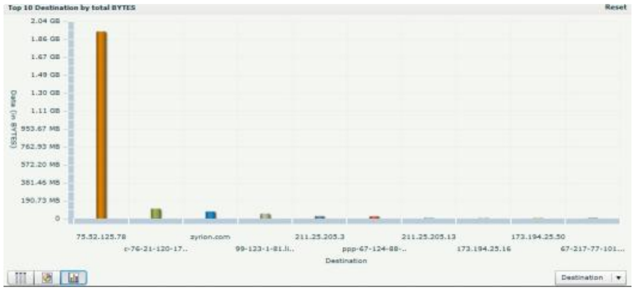
6. Choosing **Yes, Apply Now** will immediately write the new configuration out to the flow collector, and re/start the flow collection subsystem. Choosing **No, Defer For Later** will save your configuration, but not apply it to the DGE extensions nor re/start any flow services.

Using the Network Flow Analysis Console

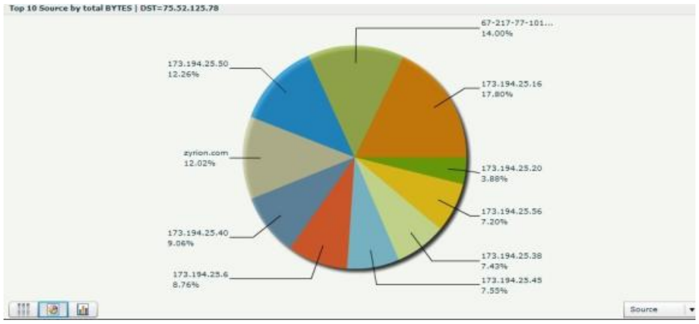
You can access the **Network Flow Analysis** console from a device **Test Summary** page or from a **Test Details** page. Each chart in the network flow analysis console has a title bar that states which device(s) (and optionally, which application) are being examined, as well as their roles.

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 **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.

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.

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 your-unique-site-name.kaseyatrials.com 7661
LOGIN <login_id>/<password>
```

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"
```

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 *Traverse User Guide* for instructions on how to use **Linked Device Template** *(http://help.kaseya.com/WebHelp/EN/TV/7000000/index.asp#17555.htm)* functionality.

Scheduled Maintenance

Scheduled maintenance 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 T*raverse User Guide* for instructions on how to use **Scheduled Maintenance** *(http://help.kaseya.com/WebHelp/EN/TV/7000000/index.asp#17555.htm)* functionality.

Index