

The Heart of the Data Center

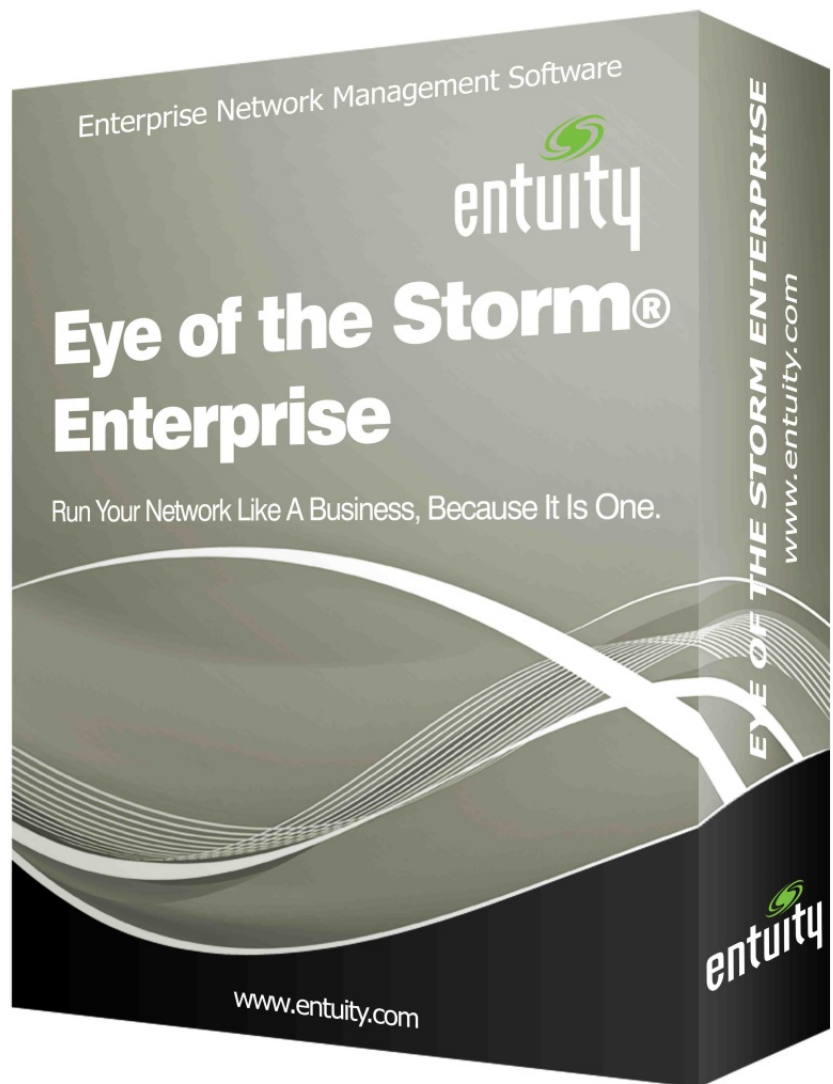
Dr. Götz Gütlich

With EYE of the Storm 2011 Enterprise, Entuity offers a network management solution for data centers which monitors network components using SNMP and similar technologies, analyzes data transfers within the network, and provides administrators visibility to applications, SLAs, and virtual infrastructures. IAIT closely examined the product, paying particular attention to newly added features of this software solution.

Entuity's EYE of the Storm 2011 is a very powerful network monitoring solution, featuring multiple components and tools for analyzing network traffic and application performance. In the product's current version, the manufacturer pays special attention to integrating virtual environments and flow analysis. The product also includes a Web based mapping function, enabling administrators to see the network status at a glance. Another interesting feature is the Live Status overview, which at any given time provides IT staff with information on key components. Finally, leveraging Cisco's IP Service Level Assurance technology, EYE's IP SLA feature lets IT managers monitor performance of data streams from a central location.

The Test

For our test, we installed a Windows version of the software on a Windows 2008 R2 computer (the solution also runs under Linux or Solaris). We monitored routers and switches by Cisco and Lancom, WLAN Access Points by Netgear, as well as servers and workstations under FreeBSD, Redhat Enterprise Linux, Solaris, Windows XP, Windows 7, Windows Server 2003, and Windows Server 2008 R2. After connecting the systems slated



for monitoring, we used the Web based mapping function to create a graphic overview of our network.

Then we used the Live Status feature for quick access to the status information of key network components. Finally, we connected

an ESXi server by VMware to our network and installed a virtual machine under Windows 2008 R2 to test the integration of virtual environments in Entuity EYE. We also took a close look at the integrated flow analysis and the IP SLA implementation of the product.

Installation

Before installing the management solution, the manufacturer recommends the following important points. EYE 2011 should run on a dedicated machine and should not be installed alongside other resource intensive software. Furthermore, administrators should deactivate any services on the EYE machine that could negatively impact performance and availability, such as Windows Update. In order to ensure good performance of the solution, it is of utmost importance that the anti-vi-

serted the DVD into the target system and called up the installation routine from a user account with administrator privileges. A Wizard popped up with a welcome screen and the licensing information. The Wizard requested a target path to install EYE. This triggered setup.

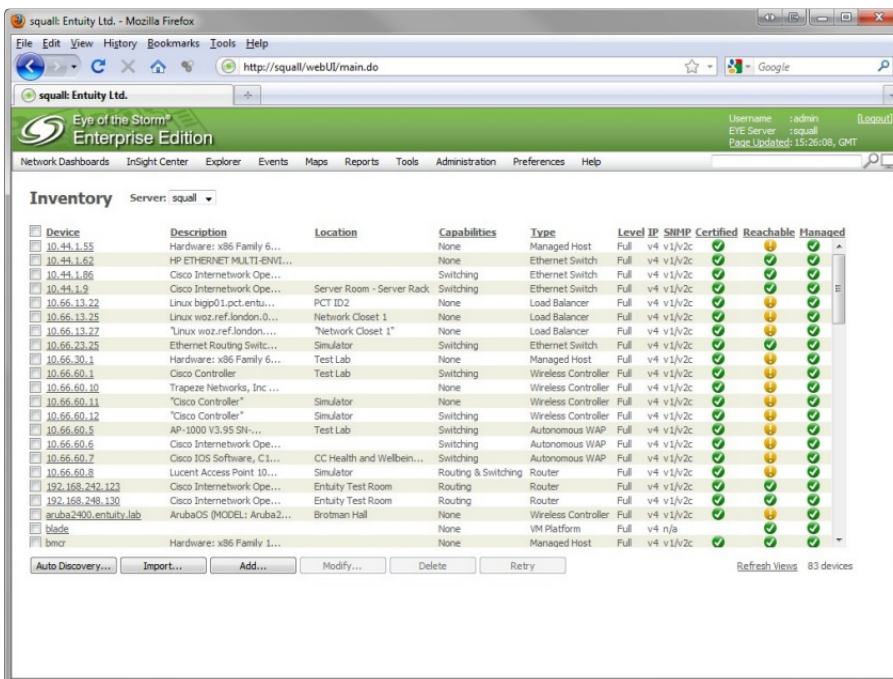
After installation, the Wizard listed an identifier code that uniquely identifies the hardware and is used to create the license file. Since EYE is bundled with a 30-day trial license, for our test it

manufacturer. The system prompts the database, database backup files, and log files. Entuity EYE uses MySQL as its database.

Next, the administrator should select the license file and indicate in which mode EYE should run. There are three different options: Standard (provides elemental management without the integrated NetFlow Analyzer), All in One (includes both elemental management and the integrated NetFlow Analyzer) or Dedicated Flow Collector (which only collects flow information). For our test we chose the All in One server option. Then we decided which modules to activate, which allowed us to add additional functions to EYE.

At this point EYE offers a wide range of different features which can be licensed separately, if desired. The number of available modules is too numerous to list in this review, which is why we will name only the most important. These include: Cisco IP SLA, Cisco SSL Service, Blade Center, VPN Gateway, QoS Module, Wireless Controller, Power over Ethernet, Integration for Fluke NetFlow Tracker, Load Balancer Support, VMware ESX Server, Netcontinuum Firewall, IPv6, MPLS, and High Availability.

Some modules need to be configured individually, which is accomplished by the Configuration Wizard in the next step. Next, staff can select a SMTP server to automatically send alerts or reports and can activate SSL for communication between EYE and the client browsers. IT managers also have the option of changing the root password for the



The Inventory page of Entuity EYE, providing an overview of the devices that it manages and their status.

rus software on that particular machine does not scan EYE's database records. Furthermore, the EYE machine needs a static IP address and the EYE application needs to be allowed to communicate through the firewall. Also, the solution should have SNMP and ICMP access to the network. Regarding hardware requirements, Entuity notes that to monitor 450 machines, a minimum of a 2.8 GHz CPU with four cores, 4 GByte RAM, and a 75 GByte hard drive are necessary. To install the software, we simply in-

was sufficient to email this identifier to the manufacturer and to work with the 30-day trial version (whose functionality was not limited) until the permanent license arrived.

In order to run the software after initial set-up, a configuration step is necessary. Located within the Install directory of the Entuity EYE installation, the configure.exe file launches a Configuration Wizard which raised the MaxUserPort registry value to 65534 as recommended by the

application. Finally, the Wizard prompts for port numbers to use for communication between the various EYE components. In our test we kept all the default settings. The Wizard displayed a summary of all the steps and concluded the software configuration.

cannot access the system by using default login data.

When accessing the running system via the Web interface, the first logical step is to add any network components to be monitored. To communicate with range of individual devices, the solution

the devices running in our environment, so we could immediately integrate them with our EYE installation. This was also because in our network we had already configured all SNMP-enabled devices in accordance with the requirements. As such, we did not have to make any changes on the client side.

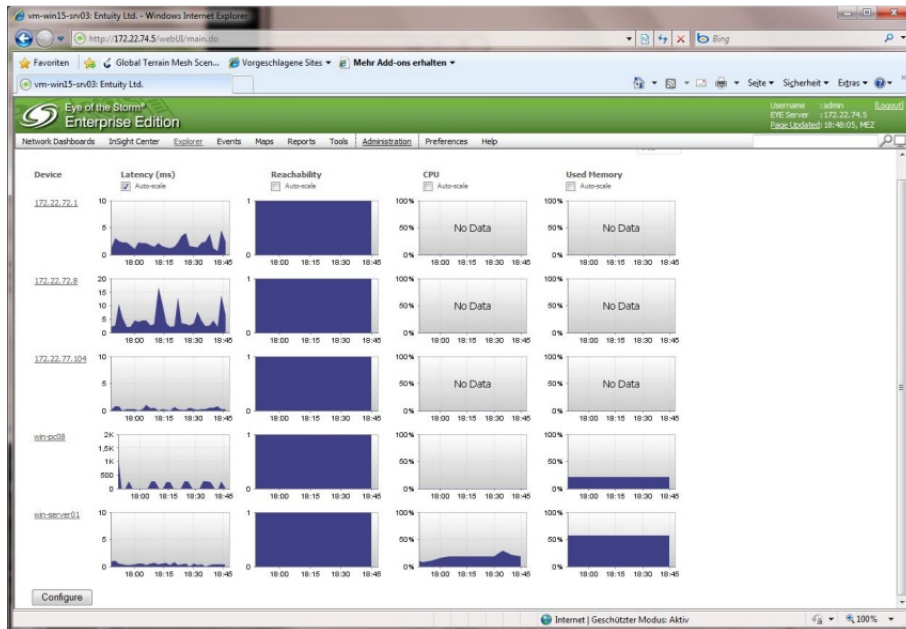
In this context, it is important to note the management levels that EYE provides for the administration of network components. Entuity's software can distinguish between Full Management (All Interfaces), Full Management (Management Interfaces Only), Full Management (No Interfaces), Basic Management, and Ping Only.

With the exception of Basic Management, every level should be self-explanatory. In Basic Management, EYE collects only basic system information and the IP address table via SNMP.

Functions of the Browser Interfaces

After adding monitored equipment to our installation, we completed first an overview of the range of functionality available through the Web interface of EYE 2011. The software features a menu bar at the top of the window from which every available function can be launched.

The first menu provides access to Network Dashboards. These include a Status Summary, which is sorted according to views, and which includes devices, device types (ESX servers, Ping Only device, managed host, etc.), the EYE server, and Worst Events (per device). Also, there are various other dashboards such as Service Summary, Flow Summa-



The Device Metrics overview provides IT managers with a simple Dashboard page that displays information on the network and key components.

Starting the Solution

After configuring the solution with the Configuration Wizard, we started EYE by using the command "startEYE" located within the "bin" directory. The command "checkEYE" in the same directory validates proper execution of EYE services while the system is running. Once all the services are up, users access the EYE solution through a Web interface whose default address is `http://{name of the EYE server}`.

The default administrative credentials supplied with the product are "admin" and "admin." After logging in for the first time, administrators should change the standard password at "Administration / Account Management / Admin / Change Password" to ensure that unauthorized persons

on uses various technologies such as SNMP polling, SNMP traps, syslog events, Ping, and TCP probing. In practice, the Autodiscovery function should be run first which scans networks or IP ranges and then displays a list of devices found during the search.

IT staff then have the option of selecting any or all devices on this list and then adding them as "Managed Devices" within EYE. The Autodiscovery command is located in the configuration interface under "Administration / Inventory / Autodiscovery". Before launching this function, the network addresses to scan along with relevant data such as the SNMP Community String needs to be specified. In our test the search function immediately recognized all

ry, Top-N Summary, and Device Metrics.

Examining the Status Summary in more detail is a good way to get to know the most important functions of the system. Users have the option of accessing individual device entries by means of the Explorer function to discover all existing devices and related interfaces. After drilling down to an individual device in the tree structure on the left side of the window, the work area to the right shows an information page listing current events pertaining to each device along with a range of data such as storage load, CPU load, latency, and IP discards depending on the component.

The work area in EYE also offers details on device ports, plus a Flow Summary to keep users up to speed about data flow on the various devices. (We will discuss the integrated Flow Collector below). Finally, additional information on the CPU model, management levels, IP address, et al, is provided.

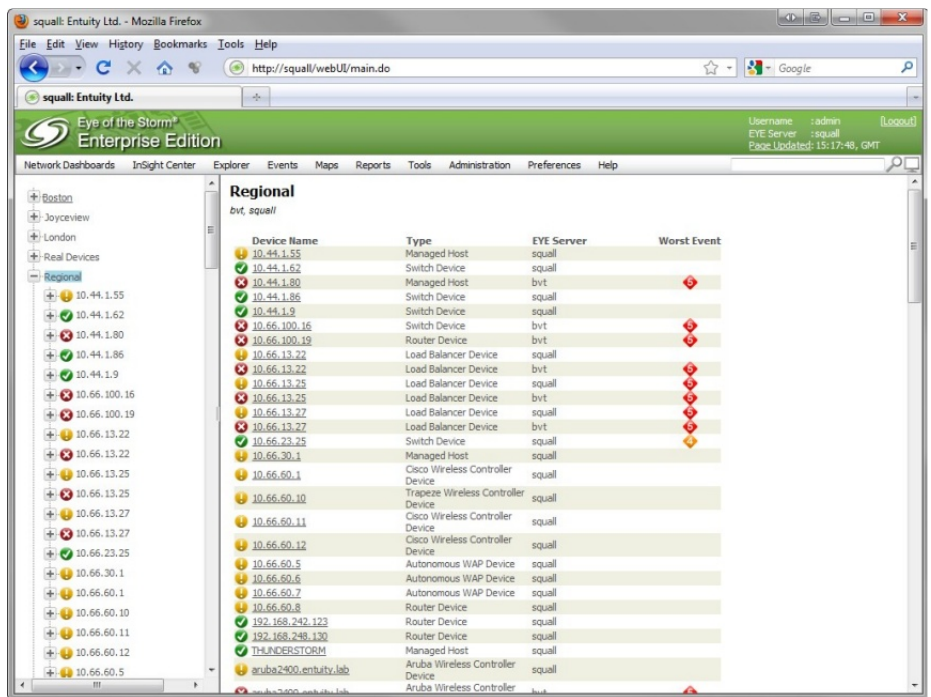
In the upper right hand corner of the information page users have access to a number of different icons linking to other pages. This includes a dedicated page with flow information, which can be turned off or on to collect data flow for the device in question. Receiving information on the data packet rate and the flow packet version of the flows being collected, administrators can see which interfaces sent flow information.

In addition to the flow overview, Explorer provides additional subpages with details on the devices. The first subpage deals with devi-

ce resources utilization and includes as an example an overview of the CPU load. The application page is more interesting, with users having the option of defining certain applications for EYE to monitor, such as mail, DNS, or Web services. The application page also provides an overview of any defined applications, including information on application type, port, IP address, latency values, and status changes.

of the available ports on each individual device. Selecting one of these ports provides a detailed overview in Explorer – similar to the device information just described, except that this provides data on that particular interface instead of listing device information.

This port overview provides an information page with details on events, interface load, dropped



Explorer View provides gives administrators the option of drill downs on individual device components.

Our test determined that application monitoring with EYE can be configured quite easily. Monitoring began immediately after configuration. The third subpage enables users to view and change thresholds for ATM traffic, device operation (temperature, memory usage, etc.), IP SLAs, MPLS, load balancing, processors, etc. Thresholds set here are used to automate events for notification. EYE also provides a page with detailed information on location, model, version, watt usage, size of virtual memory, etc. One of the most important pages of the Explorer function includes a list

packets and any error rates (both inbound and outbound). The relevant data is visualized in the form of a speedometer or in a traditional chart graphic. The info page also contains an overview of data flow being collected with the top five applications, the top five talkers, the top five listeners, and the top five quality-of-service classes (QoS) in a graphic display. Furthermore, a list of general information such as device description, speed, MAC address, and type (such as Ethernet) is provided. Similar to the device overview, port-related Explorer pages feature subpages

availability, load, or information for multiple branch offices regarding WAN connectivity, dial-up, or load balancing. Additional information offered by the InSight Center includes faults, rejected packs, latency, and SLA Quality, plus user-defined views providing links to reports for customers (when EYE is deployed with service providers). For the concept of the InSight Center – collating data from a variety of sources to answer specific questi-

ping function. This feature lets you create overview maps for your network, which can be linked to charts or maps, clearly visualizing which devices are located where.

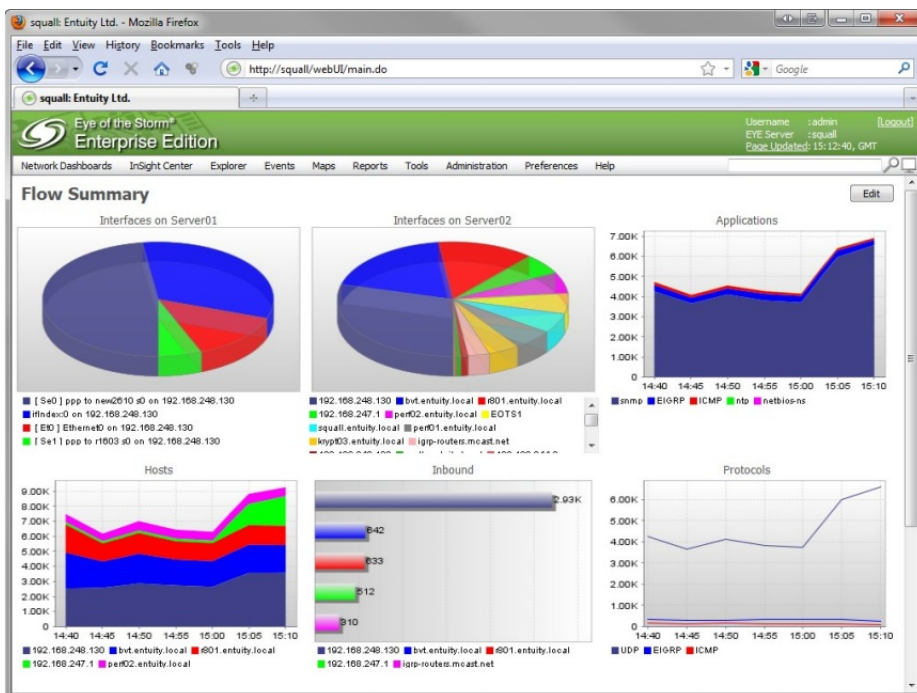
If desired, it is also possible to export these maps in a Visio format. This mapping functionality runs in the browser, so you can simply drag and drop charted devices into the map. But the real highlight of this map functionali-

immediately able to work with it. For running systems the solution provides data for every device selected or for a certain number of hops. All entries can be grouped, say, to add individual devices into a cloud or similar structure. We found the mapping tool to be very useful for quickly collecting information. We particularly appreciated the fact that all mapping functions are immediately available in the browser and that no additional programs are necessary to run the maps. IT staff can also use the map to carry out additional tasks, such as changing threshold definitions or launching trace routes.

Entuity also provides functionality called a Live Status page for applications in which the mapping functionality might be insufficient for monitoring devices. This window can be moved around within the browser and is always in the foreground. It provides IT staff with details on the status of the ten most important devices, applications, and ports. All they need to do is add that particular device to Live Status by right-clicking on its icon in the map or by adding it to Explorer view. This displays the device status in the window, along with respective events, etc. This function, too, made a most favorable impression on us.

Let us now take a closer look at reports integrated in the Web interface. Entuity provides a number of different reports, grouped into categories for the sake of clarity.

These categories include Activity, Administrative (with reports on EYE Server Health and SNMP Polling), Availability, Branch Office Perspective, Con-



Flow Summary provides administrators with a good overview of data traffic in their network.

ons more precisely we consider to be very successful.

Clicking on the Explorer menu option gives IT managers drill down functionality for individual devices and device ports, as already discussed in the Status Overview. As its name implies, the Events option displays events, such as network outages which might have occurred.

Mapping Function and Live Status

One of the highlights of the new version of Entuity EYE is its map-

ping function. This feature lets you create overview maps for your network, which can be linked to charts or maps, clearly visualizing which devices are located where. If desired, it is also possible to export these maps in a Visio format. This mapping functionality runs in the browser, so you can simply drag and drop charted devices into the map. But the real highlight of this map functionali-

ty is that EYE always shows the current status and severity of events on the device icons. For instance, faulty devices are red, components on which there is limited information or their status cannot be absolutely determined are grey, while devices running smoothly are displayed in green. This gives managers a first-rate overview of any problems within the network and where they are located.

nectivity and Routing, Green Reports (with the Server Activity List), Inventory Reports, Service Reports and User Defined Reports. All of these reports can be automatically generated according to user-defined schedules and can be emailed. We had no problems working with these reports during our test.

of keeping an eye on the “health” of the EYE server, database, and similar components. Furthermore, there is the option of adding user accounts and groups with certain access privileges. This affords IT staff with the option of granting certain users access to reports, flow inspection, mapping functionality, etc. Multi Server

IT managers can use Preferences to determine the intervals between Auto Refresh events and to define the homepage for the Web interface to display after Login, etc. The browser also includes a help function with links for documentation and support. By the way, documentation is very detailed and should provide answers to practically any question that might pop up.

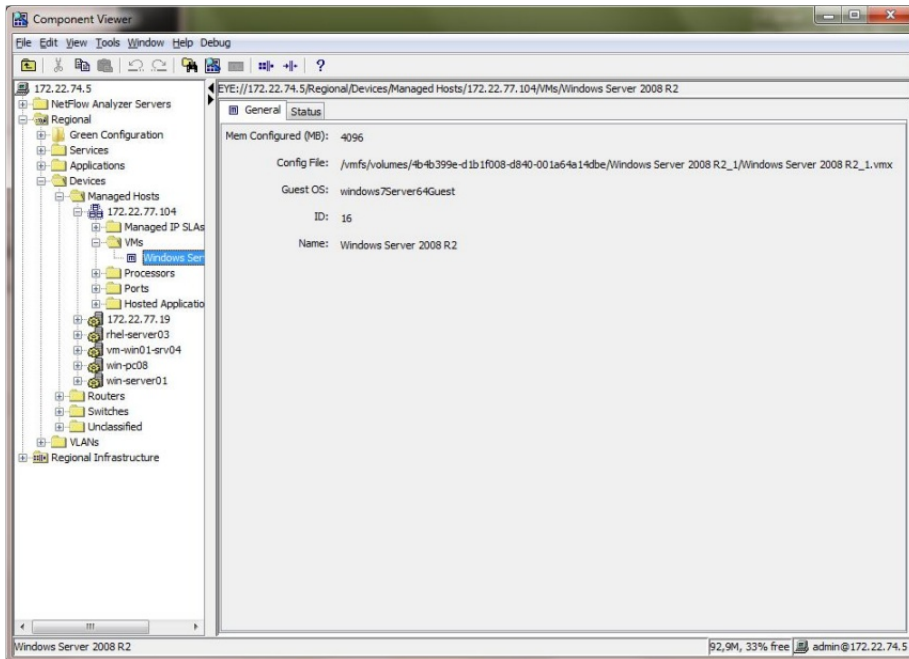
Component Viewer

In addition to the Web interface, Component Viewer is the second significant feature of EYE 2011. This Java application can be launched either directly via the Tools menu of the configuration tool or via Explorer view in the browser.

After launching Component Viewer, in the left hand corner administrators see a window displaying a tree with the EYE server and the managed devices. In our test, at this point we had already launched the VMware ESXi server and linked it to EYE. As expected, the virtual environment was displayed as a node within the tree structure.

The virtual machines (VMs) running on the server are in this ESX node, which enables staff to immediately see which VMs are running on which virtualization platform. Integration is seamless and made a favorable impression. By the way, in addition to VMware, EYE also supports virtual environments by Oracle.

Component Viewer’s menu bar also offers staff a number of commands to add other EYE servers, define thresholds, configure filters to display certain objects, and to carry out similar tasks. There is also an Admin Console for displaying login duration and



EYE 2011 seamlessly links virtual environments in the Device Tree.

A quick rundown on the last points of the browser interface: Component Viewer on the “Tools” menu calls up a Java based tool providing administrators additional functionality for network management. We will discuss Component Viewer in more detail below.

The Tools menu also offers a Search function, which looks for devices and ports. The Flow Analysis menu item enables access to a configuration page to generate flow graphics and interactively links Entuity’s integrated Net-Flow analysis solution, as discussed above.

The Administration menu provides all the necessary functionality for the administration of EYE. Authorized staff have the option

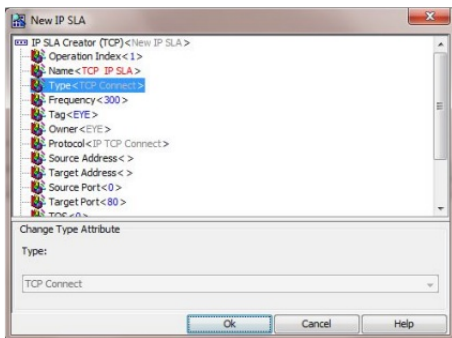
Admin provides authorized staff with the option of defining remote EYE servers in environments with several EYE servers, while Data Export can be used for exporting data sets and jobs.

Inventory adds devices to the EYE database. In addition to the Auto Discovery function already mentioned, EYE allows authorized users to manually add components and to import devices from a list.

Finally, the Administration menu includes configuration options for events (such as their life span) and the Flow Collector (with Application Port Mappings). In our test this functionality seemed to be self-explanatory and should not pose administrators with any major problems.

to send users messages. Furthermore, there is an Annotation Manager to manage comments, such as components.

Right-clicking the EYE server allows authorized users to create an MIB file and to do diagnoses with Ping and Telnet. It is also possible to directly access these commands via an icon bar for important reoccurring tasks, such as editing filters (for objects and events) or for searching for cer-



IP SLAs are easy to configure.

tain components. Users who right-click on a view (such as the standard group Regional) can create a branch office or can define services and reports.

On the right hand side of the window users have a workspace containing entries about devices, applications, and VLANs. This view can easily be limited by filters, as discussed.

The tree below provides various entries for the Green Configuration (with Shutdown Policy Groups, including their address ranges), along with services (connectivity, availability, and SLA components), applications (including all the applications monitored on the systems, also sorted by service names), and devices.

IP SLAs

Before discussing the device entries, let us mention the IP SLA

function, which is also one of the updated features of EYE 2011. This function enables authorized staff to link network information obtained from Cisco network devices on latency, response times, jitter, etc. into the EYE system in real time. Simply right-click the desired network component in Component Viewer and launch the command “Create New IP SLA Creator.”

This enables IT staff to determine the type for the IP SLA Creator (HTTP, Jitter, VoIP, etc.), define source and target addresses, and determine similar settings. These IP SLA entries are located in the workspace of the respective devices under “Managed IP SLAs” and can be processed at that point. The IP SLAs in our test were very well configured and well structured. Experienced network administrators should have no problems with it.

Let us now take a closer look at the device entries in Component Viewer. The Managed Hosts tree lists and provides descriptions of CPUs administered, routers, switches, and VM environments. To manage CPUs, administrators can use tools such as Ping, Traceroute, and Telnet, and can display the CPUs’ Reachability Status (including Response Time). They can access the computers in question via the browser to address any issues.

The workspace provides additional data on the computer systems using diagnostic tools such as Ping and Telnet, and also offers comprehensive information on RAM, a system description, etc. Administrators are also provided with a list of the ports on each device. Usage overviews are provided, as well as information on

the link status of routers and switches. Threshold limits and speeds can be set as well. Furthermore, there are overviews of port availability and port status.

As described above, Component Viewer enables access to the defined IP SLAs according to their service types and volume information regarding virtual and physical memory. Information on hosted applications, processors, chassis data, latency, etc. is provided as well. Regarding hypervisors (that is, virtual environments), the information provided in the workspace looks different because the system also provides additional details regarding server memory, the VMs, etc.

Summary

Across the board, our impression of Entuity EYE 2011 Enterprise was extremely positive. This tool provides a wide range of useful functions for monitoring SNMP-enabled servers and network components, for analyzing data transfer in the network, and for enforcing SLAs. We were particularly impressed with the mapping function, in combination with Live Status. The solution also links virtual infrastructures in exemplary fashion.

Regarding the product’s handling, it is easy to install and will not pose any particular problems for administrators with some system and network experience. Last but not least, we were delighted by the detailed and well written documentation, which will let users quickly get a grip on any issues which might crop up. The bottom line: we highly recommend the deployment of EYE of the Storm in data centers or similar environments within enterprises.