WÜRTHPHOENIX
NetEye

New features and highlights

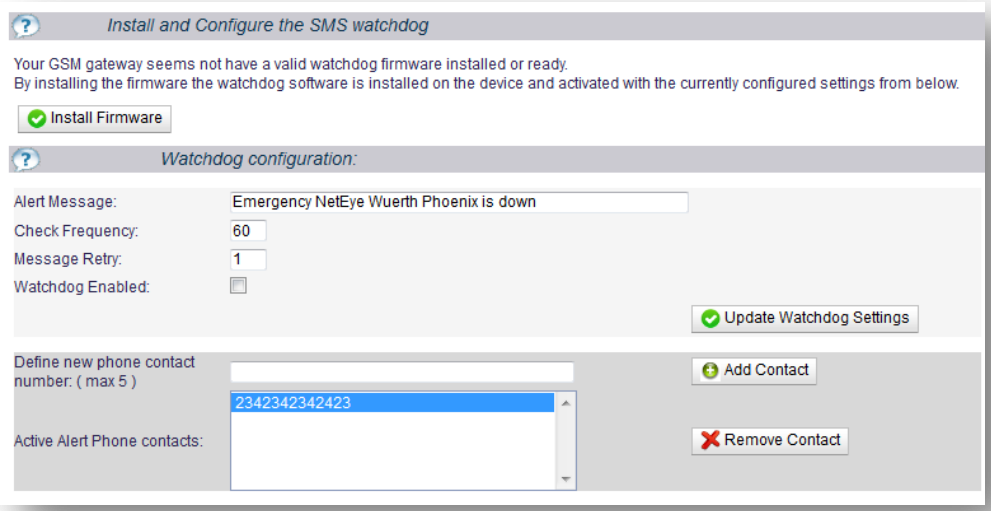
April 2012

System Monitoring

NetEye availability monitoring by the SMS Watchdog

With the newly introduced SMS Watchdog the status of NetEye is constantly monitored. To guarantee the availability of NetEye the mechanism cannot be installed on the NetEye appliance itself, for this reason it is placed on the SMS Gateway.

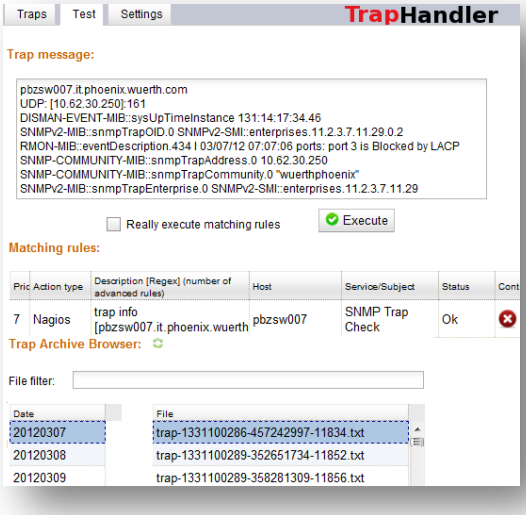
To check the status of NetEye, the SMS Watchdog receives keep alive signals. In case no signals are retrieved in a predefined time period, a SMS emergency notification alert is sent.



Enhancements and improved features with the latest NagVis

The latest version of NagVis 1.6 has been integrated into NetEye. Among the main innovations there are the new Permission Management, an improved Front End to easily configure the maps and higher compatibility with the latest versions of the browsers such as Internet Explorer, Firefox, Safari and Chrome.

New testing engine to easily identify the rule used for the Traps



The SNMP trap handler frontend, a module developed in NetEye, provides a user-friendly way to configure the actions that should be taken when SNMP traps are received. It allows to specify matching-rules to identify the SNMP traps and extract and interpret the information contained. The collected data can then be used to inform the message console host or the Nagios Service Check Acceptor (NSCA) about those events.
Among thousands of traps it is often complicated to identify wich rule is applied. With the new testing engine it is possible to execute existing trap or manually inserting a trap to undestand exactly which rule will be adopted.

New monitoring templates for a easier and quicker NetEye configuration

To facilitate the NetEye monitoring configuration new templates have been added for the following systems/OS/hardware offerings:

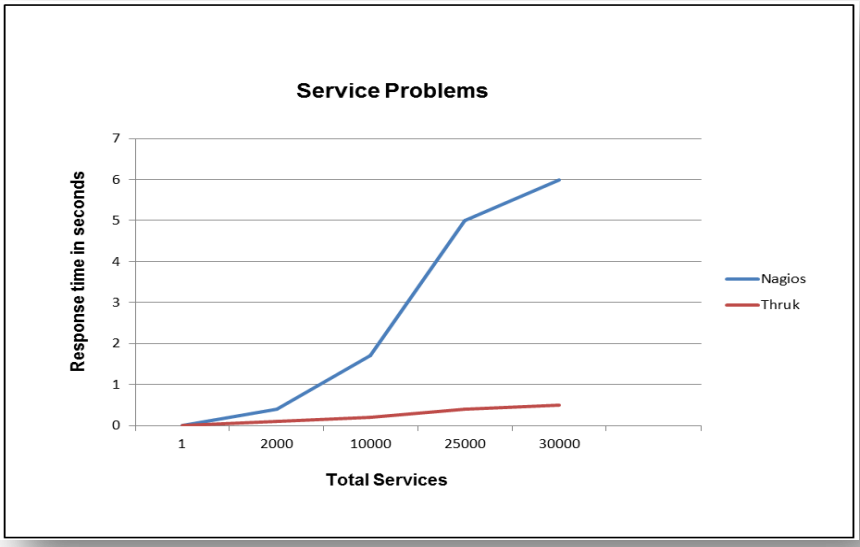
- Exchange
- SharePoint
- MSSQL
- Oracle

- Windows
- Linux
- AIX
- HPUX
- Sun Solaris
- AS400

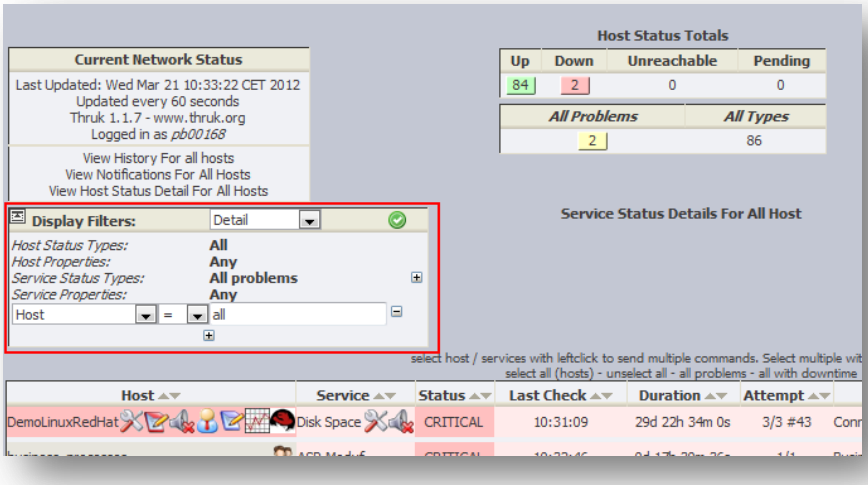
- IBM
- HP
- Dell
- Fujitsu

Improved performances with Thruk

The new Thruk UI for the Nagios Core is designed to assure a quick response time to access the event logs, problems, tactical overview and process information. Thruk allows better performance thanks to multiple backends and no delay between core and UI.



Other features of the Thruk UI are the extended logfile, the customizable paging, the multiple themes and the export of data in excel format.



Network Traffic Monitoring

Who is using your network?

Who is generating heavier traffic? How to prevent undesired network usage?

NetEye, with the ntop and NFSEN technologies, provides the needed information to answer to these questions. The network traffic is collected and displayed on locations, specific protocols or by deepening the level of details the source and destination IP address.

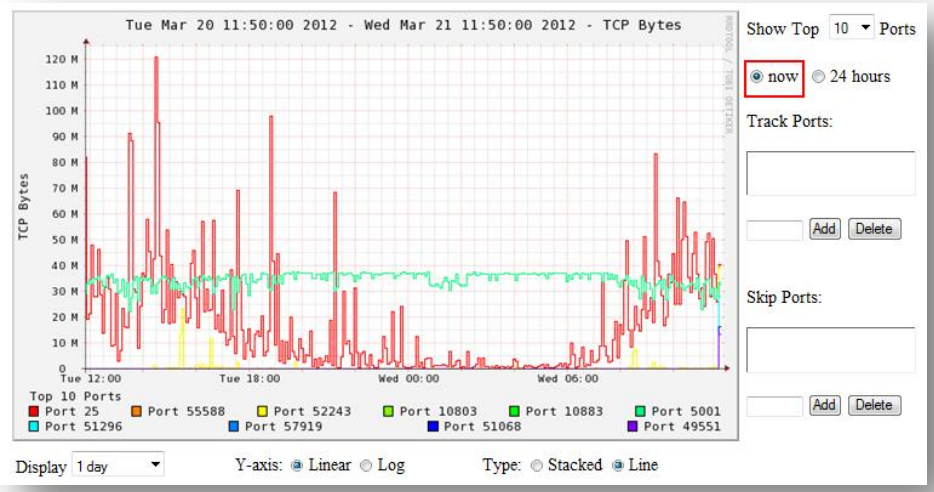
What advantages can you expect?

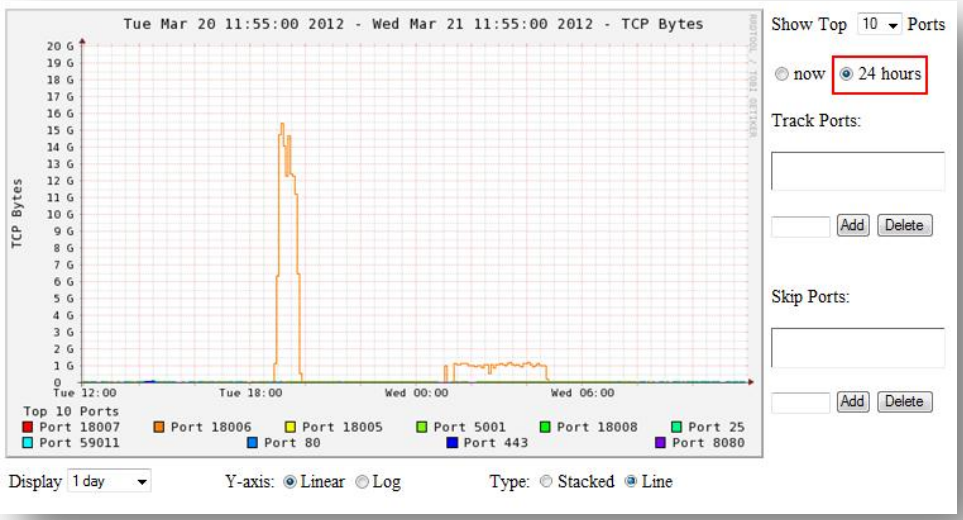
Slowness on business critical applications in case of network congestions can be avoided thanks to the possibility to receive notifications by configured checks on network flows.

The network communication flows analysis allows to detect anomalous network traffic, to identify the origin and to discover if the network services are improperly used by users or applications such as “virus”, “calling home”, bug etc.

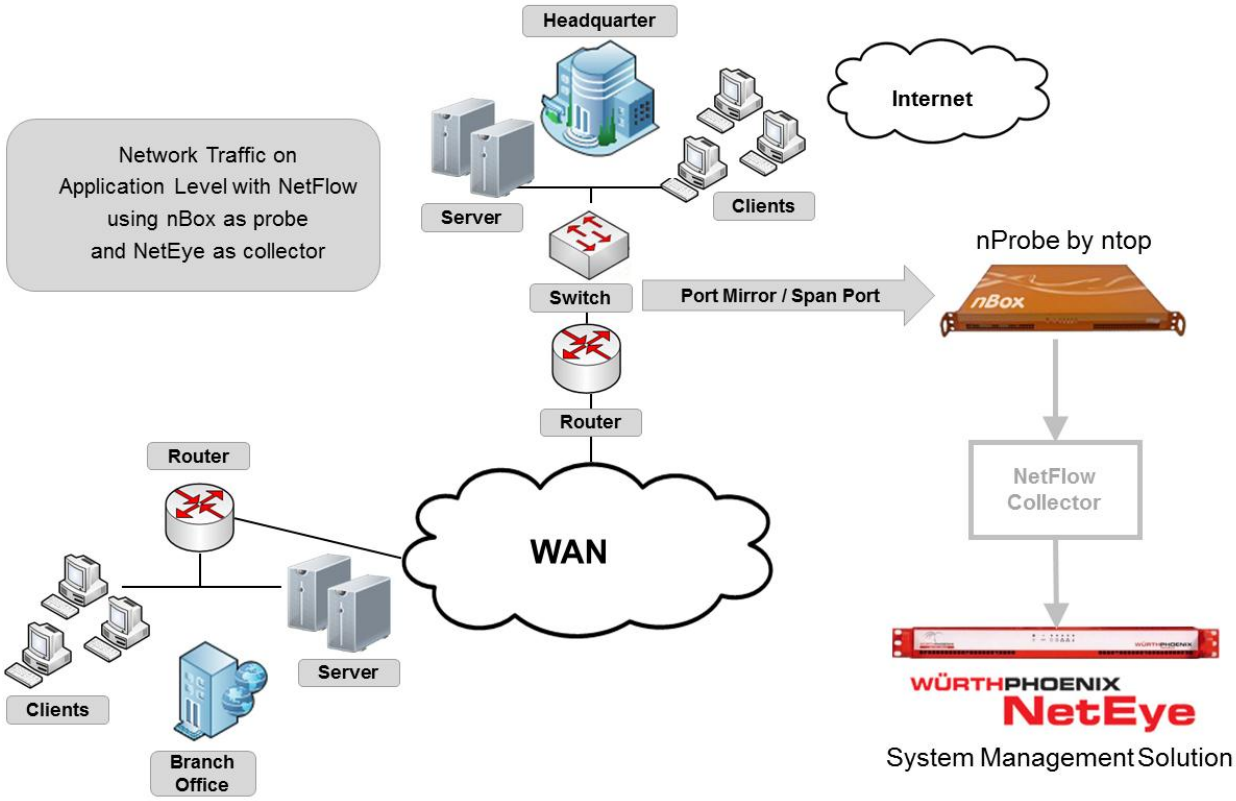
In case of a shared network among different branch offices, data are retrieved to identify the real network usage based on each location. With the information provided by this feature, the cost of the telecommunication services can be rationally divided attributing the costs for the connection to each branch office based on the real network usage.

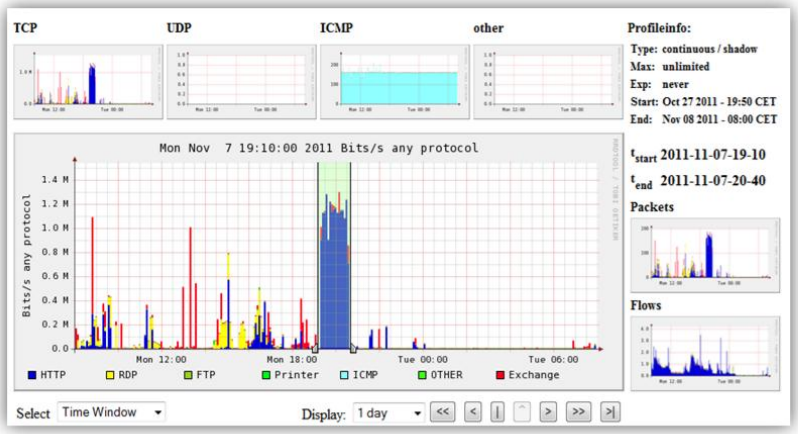
To easily identify which port is using more network, the port tracker plugin generates graphs per port on TCP or UDP network traffic. The graphs can display the ports that have generated most traffic in the last time frame specified by the variable “Now” or in the past “24 hours”.





Below an overview of a possible deployed architecture to get the network traffic on NetEye.



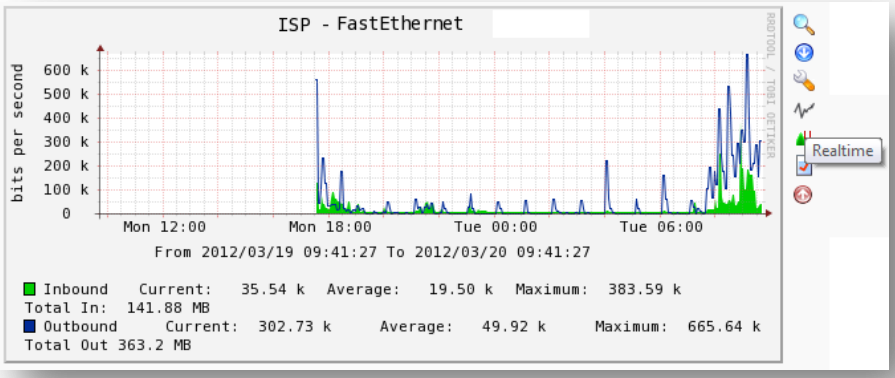


Top 10 flows ordered by bytes:

Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Flags	Tos	Packets	Bytes	Flows
2011-11-07 19:19:52.856	4670.430	TCP	10.62.1.91:33964	->	10.67.10.2:443	.APRSF	0	444663	624.2 M	152
2011-11-07 19:19:53.063	4670.242	TCP	10.67.10.2:443	->	10.62.1.91:34330	.AP.SF	0	45513	19.1 M	152
2011-11-07 19:19:52.869	4670.418	TCP	10.67.10.2:443	->	10.62.1.91:33964	.AP.SF	0	222389	11.6 M	152
2011-11-07 20:12:38.499	30.188	TCP	10.62.1.66:49741	->	10.67.10.2:25	.AP.SF	0	4252	6.3 M	2
2011-11-07 20:34:49.174	23.697	TCP	10.62.1.66:50425	->	10.67.10.2:25	.AP.SF	0	3466	5.2 M	2
2011-11-07 19:19:53.972	13.393	TCP	10.62.1.66:48113	->	10.67.10.2:25	.AP.SF	0	2485	3.7 M	2
2011-11-07 19:19:53.042	4670.263	TCP	10.62.1.91:34330	->	10.67.10.2:443	.APRSF	0	44739	2.4 M	152
2011-11-07 19:52:53.356	8.910	TCP	10.62.1.66:49148	->	10.67.10.2:25	.AP.SF	0	1312	1.9 M	2
2011-11-07 19:58:37.980	4.359	TCP	10.62.1.66:49323	->	10.67.10.2:25	.AP.SF	0	626	893300	2
2011-11-07 19:53:49.626	1439.270	TCP	10.62.1.91:58125	->	10.67.10.2:443	.AP.S.	0	966	620088	36

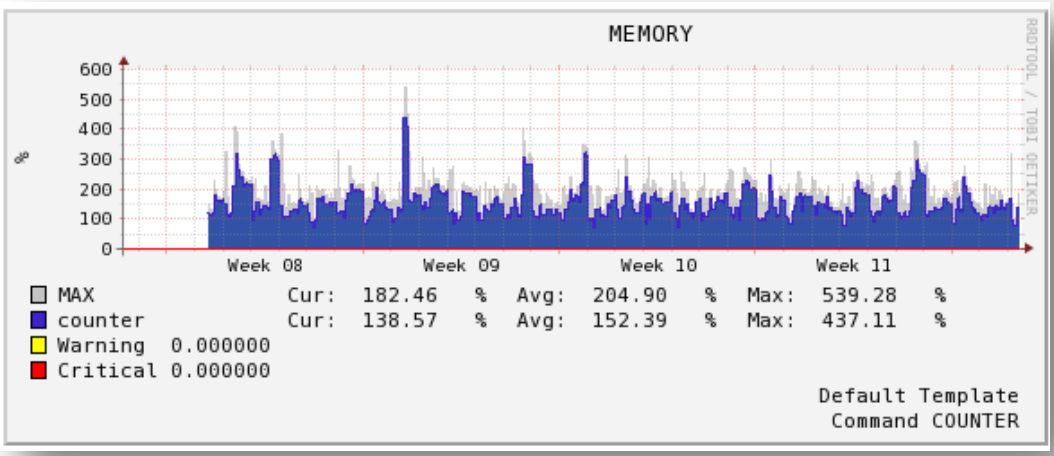
Cacti Upgrade

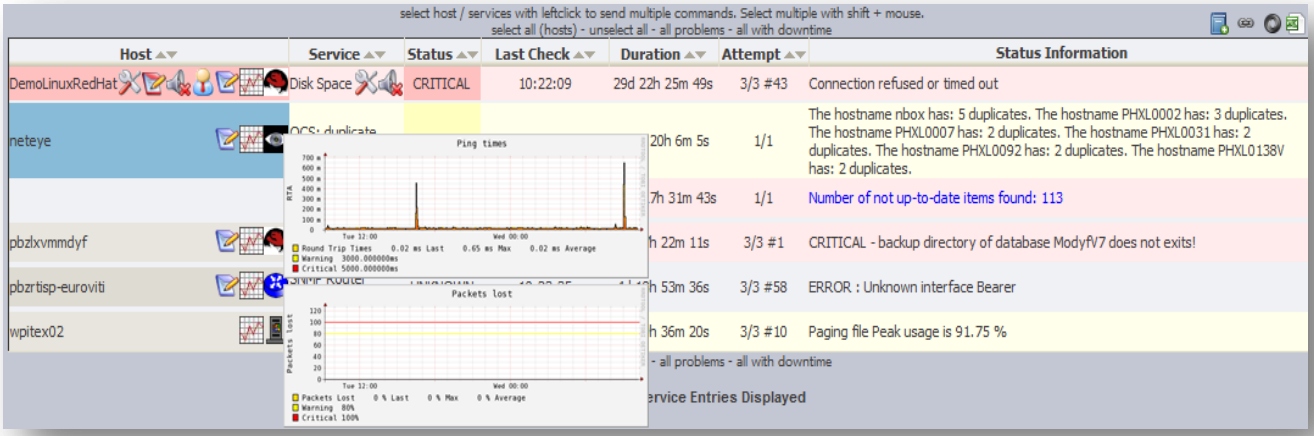
Cacti has been upgraded to the version 0.8.7i. The new features of this version are represented by the possibility to use real time plugin and to create threshold from templates.



New highlights for the PNP graphs

Maximum values and not only the average information are now displayed on the PNP graphs to easily visualize the peaks. PNP graphs can be generated based on customizable time periods and data can be exported in PDF format. Furthermore the mouse over popup shows the graph previews of services, hosts and problems.





Automatic Network Discovery with the integration of NeDi

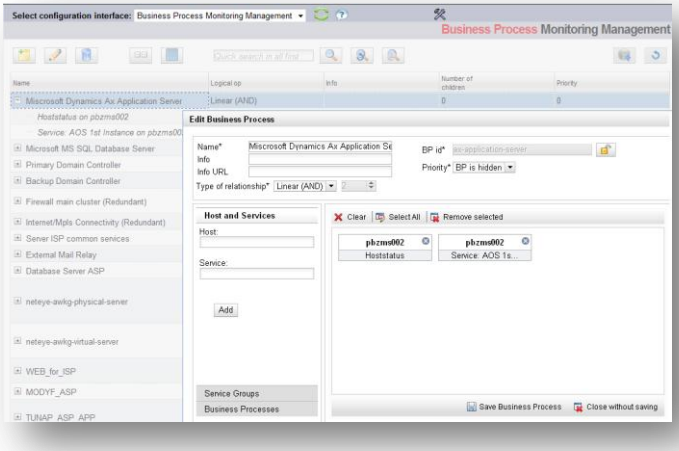
Can you imagine how quick it would be to manage your IT infrastructure, if your network, servers, and computers were automatically tracked?

With the integration of NeDi into NetEye it is possible to discover your network on a regular basis. NeDi allows you to locate and track all connected devices, monitor traffic or broadcasts, send emails or SMS when certain events occur and backup the configuration of your switches and routers. It even lets you observe the printer supplies. The idea is to keep everything simple, you do not need any more to locate a hacked node somewhere on the network. Thanks to the Open Source nature of NeDi, virtually any device can be supported and new (web-)tools can be easily added, with the appropriate PHP knowledge.

Business Monitoring

New business processes monitoring configuration module

A new business processes configuration section has been designed to facilitate the setting of the business processes. Create, modify, delete processes or setting the dependencies of the IT services with the infrastructure components can be easily performed on the configuration module. The business process monitoring is used to obtain a higher abstraction level to define IT Services. In this way it is possible to simulate the business impact that a server anomaly will have on the service level, generating accurate reports on the availability of the business processes (often needed for the Service Level Agreements).



Performance Monitoring

End user experience in the Cloud era

During the daily business operations till now very limited data have been collected to analyze the real end user experience. The Real User Monitoring can represent the right solution to satisfy these needs, measuring the end user experience, providing data on availability, response time and reliability of the IT services (i.e. eShop, CMS, ERP, Mail, …)

This approach aims to maintain an elevated level of productivity and to identify the values able to verify the conformity with the Service Level Agreements. Higher business processes efficiency, for instance, can be guaranteed by avoiding slowness or unavailability of ERP systems, that can cause blockage on the order or invoice processes representing economical loss for the companies. With the Real User Monitoring the IT department can define exactly when and which service is not functioning correctly. This concept with the introduction of the Cloud services is playing a significant role for the IT monitoring, that is moving from the traditional control of systems and hardware to the analysis of the real experience from the user perspective.

In the new era of the Cloud computing the Real User Monitoring is becoming fundamental. The infrastructures, services and platforms are not any more in-house but delocalized to different Cloud providers. For this reason the monitoring of the end user experience is needful to identify if the cause of possible anomalies is related to the network, applications or Cloud. Every supplier, in fact, tries to protect its own Cloud, even if the probability of having malfunctioning is anyway present. The effects can be elevated, hundreds of users or a single employee can be inoperative for certain period of times. When there are situations that lead to significant losses in business, it should be immediately clear where to look for the cause. Inside the company? Or is it the supplier's fault? The network or the application? Which software? And how to demonstrate that the anomaly is depending on the Cloud provider? The complexity of the contractual agreements, that for the Cloud services is starting only now, and the increasing number of providers may enforce this effect. Almost no companies will chose only one provider, but as it happens for the hardware, that are purchased from different vendors, it will be also for the Cloud.

NetEye helps to control the services and Cloud Computing providing two different approaches for the Real User Monitoring:

- Active monitoring to check the availability and reliability through intelligent robot systems that emulate the users interactions. The solutions integrated and proposed to fulfill these requirements are WebInject and Selenium HQ

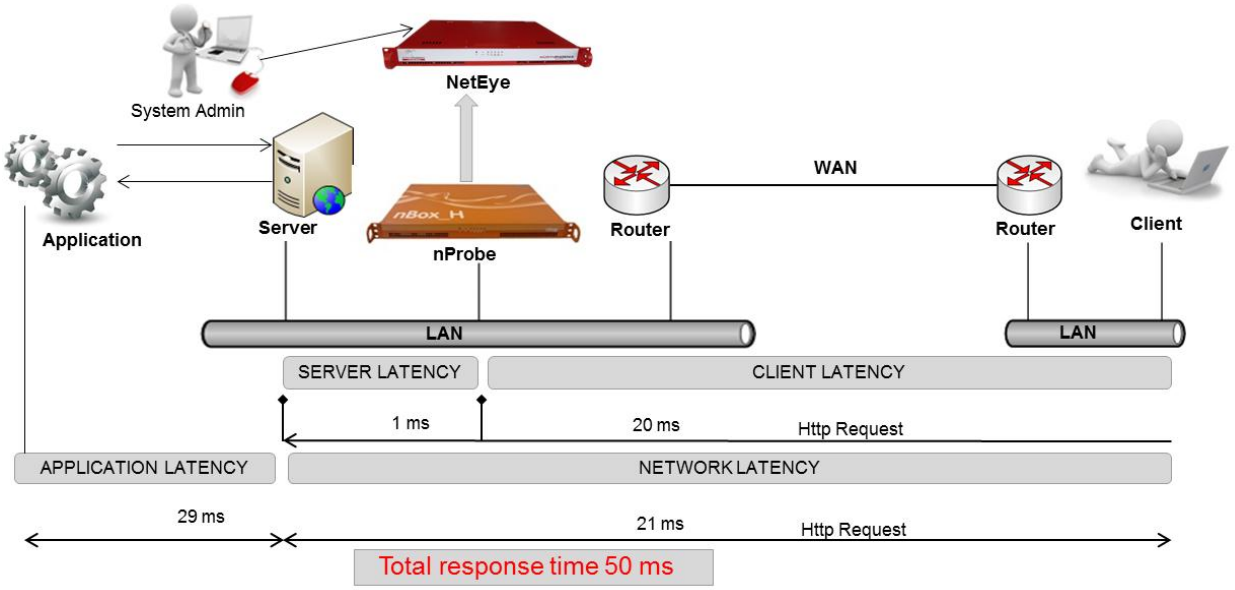
- Passive monitoring to identify the response time collecting the HTTP(S) traffic without any effect on the applications (no trace, no debug, no performance impact). The solution implemented by Würth Phoenix is the Application Latency Monitoring

Control the end user experience with a passive Real User Monitoring

The possibility to trace the response time of each application based on locations and users facilitates to understand if the cause of a possible anomaly is related to the network or application.

The Real User Monitoring reveals the network and application latency of HTTP requests. A probe situated between the clients and servers identifies the HTTP requests and traces the timestamps. The acquired information from the probe are periodically send to NetEye and data aggregation is performed to improve search engine efficiency.

Checks are executed periodically to discover slowness comparing the actual status of the latencies with the expected baseline values. In case of deviation from the recorded baseline performance, system alerts are generated.



Latencies indicators

…aggregated by locations

Netgroup/Application/Subnet/Client	Requests	App Latency	Server Latency	Client Latency	Bytes	Status
Bolzano	8862	0.437	21.762	4.100	67,2M	
Roma	3640	0.510	0.255	18.153	97,3M	
UNMATCHED	3308	0.509	0.252	18.762	92,6M	
Facebook	124	1.122	0.341	14.775	2,7M	
Skype	18	0.029	0.150	10.013	63,5k	
NetEye Updates	3	0.000	0.245	8.853	5,5k	
Google	187	0.169	0.267	10.548	1,8M	
VLAN 1 LAN	124	1.122	0.341	14.775	2,7M	
10.62.11.153	18	2.871	0.212	22.531	1,3M	
10.62.11.20	23	3.413	0.595	10.391	1,2M	
10.62.11.75	83	0.107	0.298	14.308	174,9k	

Application
LAN
User IP

…aggregated by clients

Client/Subnet/Netgroup/Application	Requests	App Latency	Server Latency	Client Latency	Bytes	Status
10.62.11.157	736	0.384	0.154	36.973	27,2M	CRITIC
10.62.11.21	1	0.001	0.568	75.453	537,9b	CRITIC
10.62.37.166	12	0.033	3.362	156.045	182,0k	CRITIC
10.62.37.172	44	0.078	3.886	41.718	466,1k	CRITIC
10.62.37.175	50	0.056	14.952	255.339	379,9k	CRITIC
10.62.37.25	54	0.031	4.202	55.469	303,3k	CRITIC
10.62.37.53	30	0.055	8.162	44.943	389,5k	CRITIC
10.62.38.50	50	0.035	4.586	273.501	407,9k	CRITIC
10.62.4.23	80	0.239	104.869	0.213	127,5k	CRITIC
10.62.4.30	98	0.099	108.672	0.199	148,2k	CRITIC

…aggregated by applications

Netgroup/Application/Subnet/Client	Requests	App Latency	Server Latency	Bytes	Status
Dropbox	10	55.710	88.424	8.4k	CRITICAL
Facebook	143	10.639	57.389	1.0M	CRITICAL
CIS	178	0.657	51.700	1.2M	CRITICAL
Scar App	222	0.030	4.380	2.5M	WARNING
UNMATCHED	3790	0.276	20.065	90.1M	OK
Repubblica	21	0.023	5.162	183.6k	OK
Main Web	7	0.172	0.102	65.0k	OK
Trendmicro Update	37	0.050	4.882	1.5M	OK
Fime App	75	0.005	0.321	128.1k	OK
Skype	1	0.041	18.320	1.0k	OK
NetEye Updates	43	0.000	0.422	83.2k	OK

Drill down to URL details

Details Of Latencies

URL	From	Requests	App Latency	Server Latency	Client Latency	Bytes
http://www.repubblica.it/socia	Repubblica Bolzano	2	0.019	5.178	0.097	NaN
http://www.repubblica.it/image	Repubblica Bolzano	1	0.013	6.402	0.076	NaN
http://www.repubblica.it/socia	Repubblica Bolzano	1	0.012	6.402	0.076	NaN
http://www.repubblica.it/img_	Repubblica Bolzano	1	0.012	6.402	0.076	NaN
http://www.repubblica.it/socia	Repubblica Bolzano	1	0.010	3.954	0.117	NaN
http://www.repubblica.it/image	Repubblica Bolzano	1	0.010	3.954	0.117	NaN
http://www.repubblica.it/static	Repubblica Bolzano	1	0.009	4.007	0.122	NaN
http://www.repubblica.it/static	Repubblica Bolzano	1	0.009	4.121	0.026	NaN
http://www.repubblica.it/rss/h	http://www.repubblica.it/rss/homepage/rss2.0.xml			3.954	0.117	NaN

Security Monitoring

New UI for the Syslog module

The Syslog module designed for Log Auditing purpose, has been completely restructured using a new more intuitive UI.

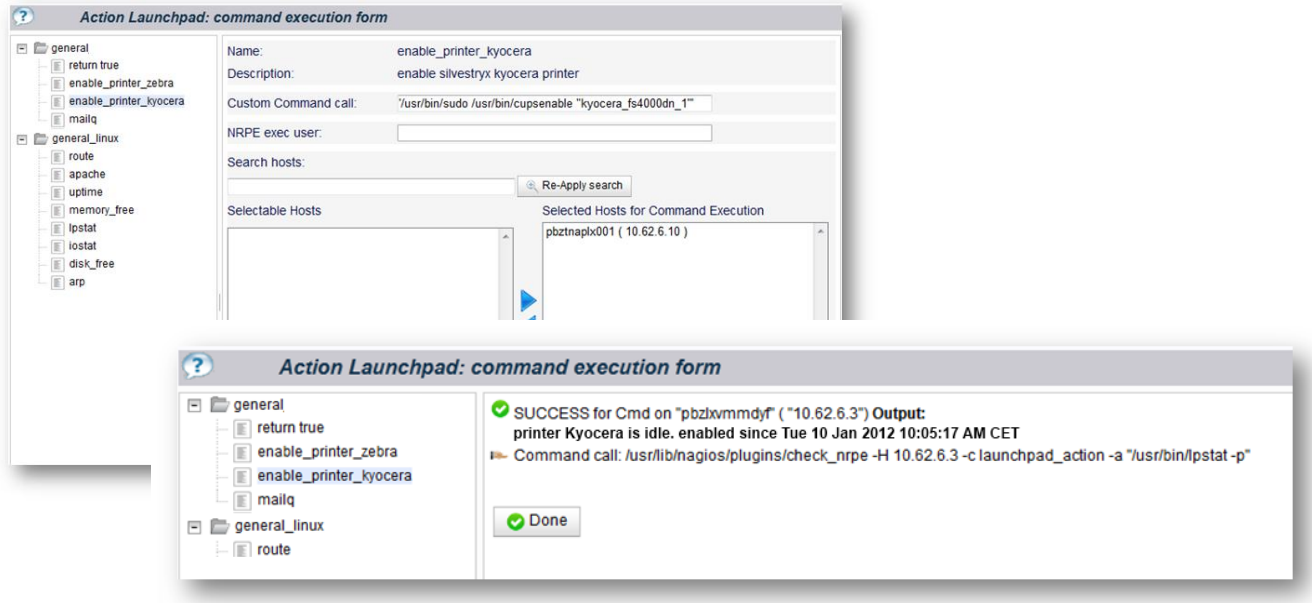
Furthermore, the integration of the Syslog with Nagios has been implemented. If a host is created in the Syslog module, automatically the related check is also generated in Nagios.

Service Desk Management

Simple as a click: Action Launchpad for the Service Desk operators

The first level support often does not have the specific technical knowledge on the systems to solve problems without escalating.

With the Action Launchpad the Service Desk operators can execute predefined commands directly from NetEye, instead of launching them with administrator permissions on productive systems. The risk of executing wrong commands in this way is reduced, most of all the response time of the support team to solve user requests can be significantly quicker. Administrators can delegate the execution of predefined commands or scheduled jobs, even if they are complex, in a save and simple way to service desk operators.



Inventory and Asset Management

New ticketing and license management features with GLPI 0.8

With the integration in NetEye of the version 0.8 of GLPI significant improvements have been performed.

The ticketing management has been enhanced introducing SLA on tickets, links between tickets, usage of solution templates, survey for closed tickets and finally the configuration of observatory actor type for several users on groups of tickets.

Other new features that have been introduced are represented by the license management and by the possibility to add comments on network ports.

Improvements on plugin architecture with the new version 2.0 of OCS Inventory

The plugin architecture in OCS 2.0 has been improved, incompatibility issues have been solved and the agent can be launched by simply clicking on the app icon.

In the new version of OCS 2.0 the usage of useragent.pm module allows to control the agents and solve versions incompatibility between OCS agents and OCS server. Furthermore the datafiler.pm module adds the capability to filter data from the Hardware section (data filtered won't be stored into the database).

Other important enhancements have been performed also on the Agents, improving the compatibility with different OS:

- The Windows AGENT 2.0 is now Full Unicode compatible, supporting Windows Vista / Seven et 2008 / 2008 R2 (NT6 and +). The Agent can detect 64 bits for OS and software.
- The Agents for Unix, Linux and OSX have been unified into one unique Agent, adding improvements on the inventory for Linux, BSD, Solaris, HPUX or Mac OSX.

NetEye Web App

NetEye becomes mobile

The simplicity of the touch technology unified with the potentiality of the web characterizes the new NetEye Web App.

The Web App is compatible with the most common smartphones and tablets (iPhone/iPad, Android Phones and Tablets, Windows Mobile Phones).

The NetEye Web App allows to view the information as the status of host, services and business processes, to navigate through NagVis, Google Maps, performance graphs, to check the documentation in WIKI, or at last but not least to use the Action Launchpad.

- Click here to watch the video showing these features

Help Desk and IT Service Management

New release of OTRS 3.1

One highlight of the new release of OTRS 3.1 is the generic interface, a flexible framework that allows the connection and integration of OTRS with third party applications via web services. Involving connectors, such as the OTRS Solution Manager-Connector or the Ticket-Connector process data, can be synchronized with SAP Solution Manager or other systems.

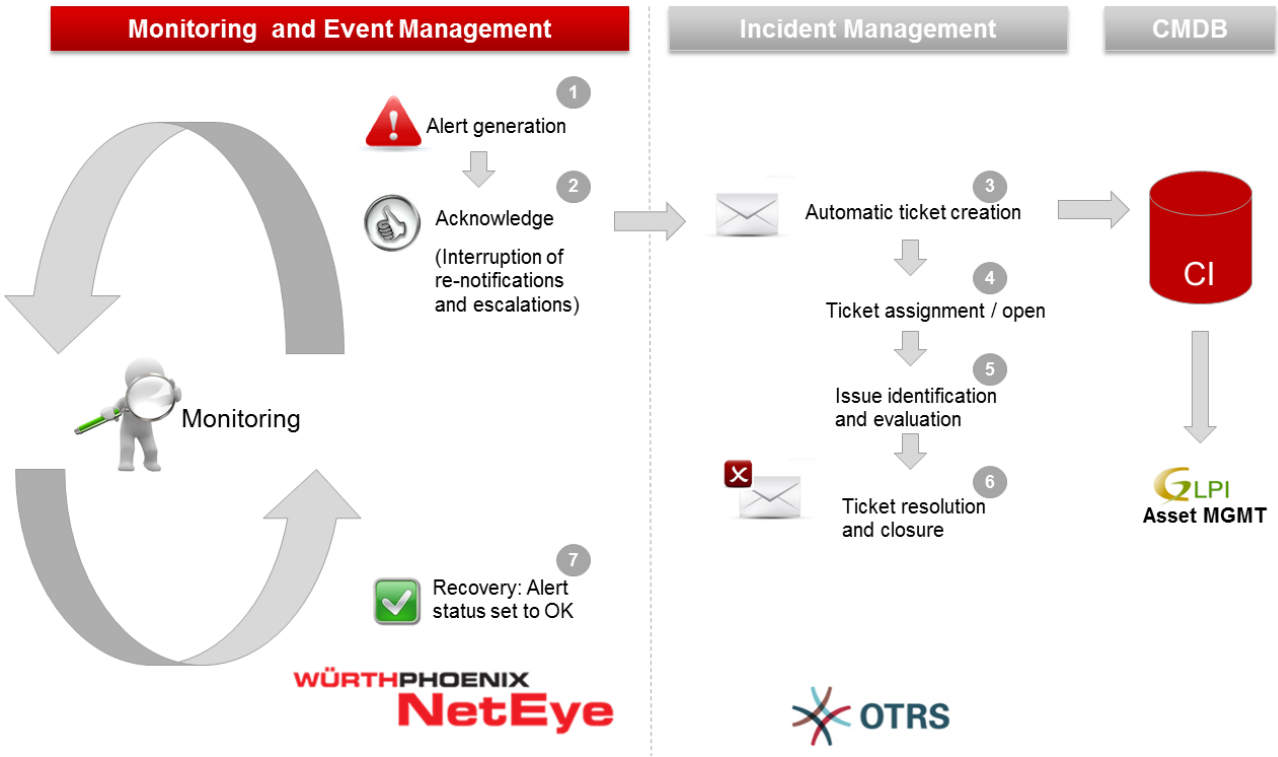
Another highlight are Dynamic Fields, a feature that enables users to create custom forms in OTRS and replaces the inflexible structure of FreeText and FreeTime fields.

How OTRS is interacting with NetEye?

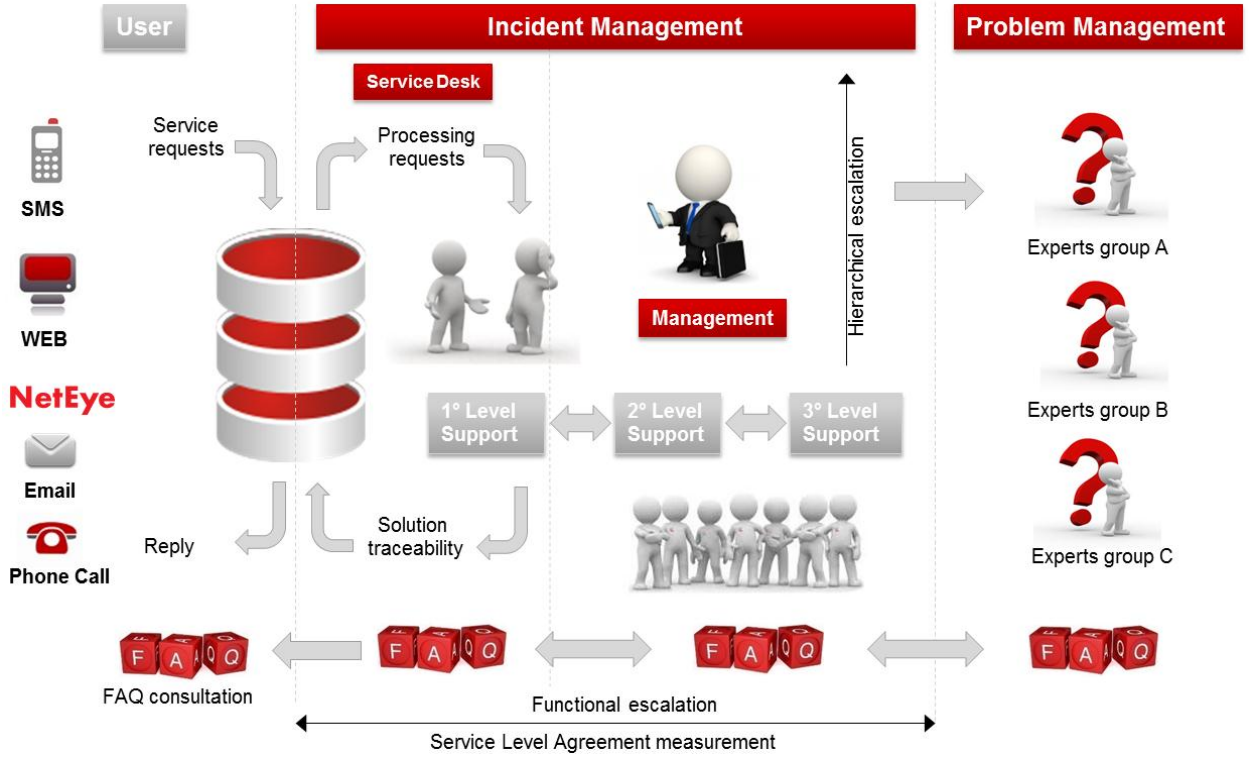
The interaction between NetEye and OTRS helps to manage the Incident life cycle in IT organizations.

In case of anomalies, alerts are generated in the monitoring system and the corresponding ticket for the problem will be automatically created in OTRS. The ticket will be handled and managed in the ticketing system.

In the meantime NetEye will continue to perform the monitoring activities, when the anomaly will be solved by a recovery action the Alert will be set to “OK”.



The below ITIL aligned workflows can be supported by the adoption of OTRS.



Do you need additional information?
Just contact our Product Manager Georg Kostner

Würth Phoenix S.r.l.
Via Kravogl, 4
39100 Bolzano - Italy

Phone: +39 0471 56 41 11
Fax: +39 0471 56 41 22

E-mail: georg.kostner@wuerth-phoenix.com
Website: http://www.wuerth-phoenix.com/neteye
Blog: http://www.neteye-blog.it/