

**WÜRTHPHOENIX**  
NetEye

## Release Notes Version 3.2



**ntop**

**Nagios**  
Enterprises  
Partner

**... more than  
software**



## WÜRTHPHOENIX NetEye 3.2 – Release Notes

Overview of the updates and newly introduced functionalities.



### **Nagios**

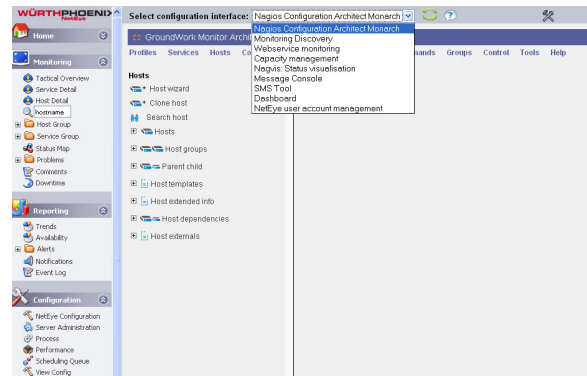
The daemon Nagios® represents the core component of the monitoring solution NetEye. It queries the configured hosts and services and notifies when problems arise within the infrastructure. The latest release of Nagios® 3.2.0 has been integrated into NetEye. This version is

coming not only with a big number of performance improvements, but it brings also additional features like multi-rows acceptance from plug-ins, new recognized macros, flap detection and advanced management of time periods.



### **NetEye Configuration Manager**

The settings for all the NetEye modules can now be entered in a unique centralized pane that allows the access to the main configuration interfaces directly from a single drop down menu.



### **Configuration architect Manager**

Monarch is a Web-based environment integrated into NetEye for the configuration and management of the monitoring environment based on Nagios, coming with

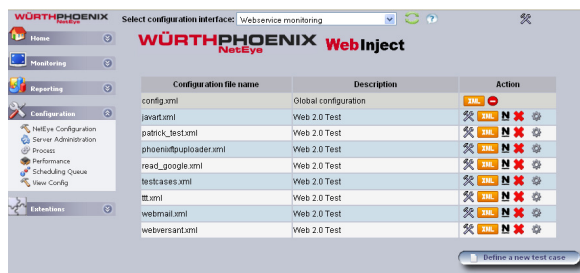
the purpose to support the set-up and maintenance of the own IT infrastructure over the web-based configuration interface. The latest version has been integrated.



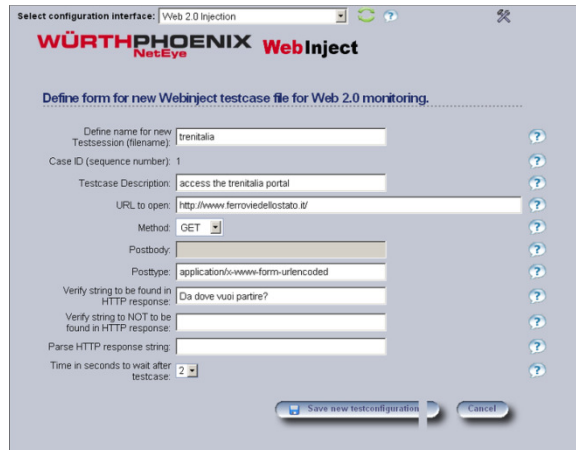
# WebInject

WebInject is a test suite that can operate as an intelligent agent, able to chain together test cases to monitor a web application's functionality through multiple phases: a web interface has been introduced to define new test cases allowing to run and debug trough the various test scenarios. This utility can set up advanced web service checks to move the monitoring of a web site beyond just simply checking the readiness of the web server.

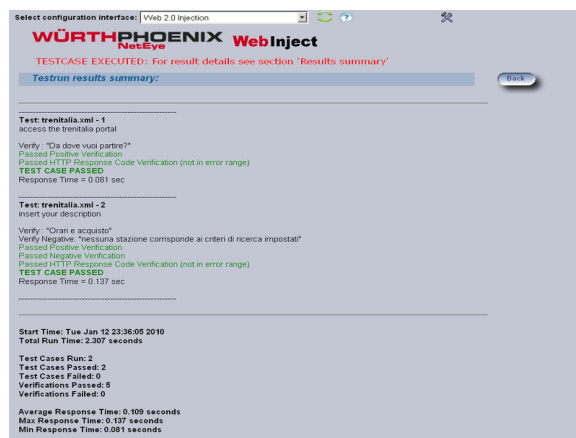
## a. Configuration main pane



## b. Test case definition



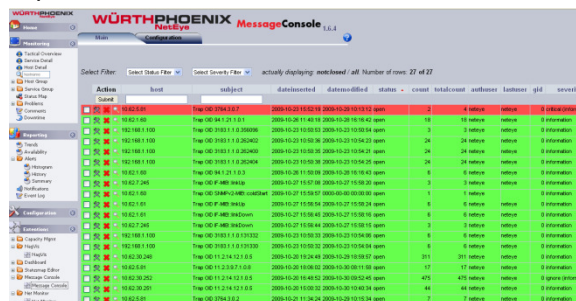
## c. Test Execution results



# Message Console

The Message Console provides a collector of messages and alerts caught by the system, SNMP traps or scheduled alerts to remind for task to perform. The newest version 1.6.4 brings improvements on performance and includes a new configuration settings and SNMP Traps. Additionally, search criteria have been added to filter the content and

expression.





## User Configuration Management

A new user account management has been introduced to add, remove or edit users directly from the NetEye configuration interface. Now also the LDAP is integrated for authentication in this module.

Rem. Passwd	NetEye User account	NetEye Group membership	Monarch Contact	Monarch User
⊖	guest	guests	⊖	⊕
⊖	root	admins	⊖	⊕
⊖	demo	admins guests	⊖	⊖
⊖	jug		⊖	⊖
⊖	neteye		⊖	⊖
⊖	pb00074	guests	⊖	⊖
⊖	syslogadmin	guests	⊕	⊖
⊖	cis_admins	guests	⊕	⊖
⊖	pb00086	admins	⊕	⊕
⊖	pb00011	guests	⊕	⊕
⊖	pb00168	admins	⊕	⊕

In the list are shown the granted privileges: the membership in NetEye groups and the registration status as contact in Monarch and user in Monarch.

Rem. Group	Members
admins	⊖ root ⊖ demo ⊖ pb00086 ⊖ pb00168
guests	⊖ guest ⊖ pb00074 ⊖ demo ⊖ syslogadmin ⊖ cis_admins ⊖ pb00011



## Capacity Management

Integration of Cacti 0.8.7e including the new plug-in architecture:

- UI Improvements on Administration Console
- Improvements on User Administration
  - Add extended LDAP authentication support
  - Added Web Basic authentication
  - Improvement of Polling ( new SPINE poller (binary poller))

- Plug-in architecture
- Performance improvements
- Miscellaneous
  - Allow CSV Export from Graph page
  - Add rra\_path as a global.php config variable



## Integration of Cacti plug-in architecture

The plug-in architecture for Cacti was designed to be both simple in nature and robust enough to allow freedom to do almost anything in Cacti. This architecture comes with the purpose to add tools developed by the community or individually into the capacity management.

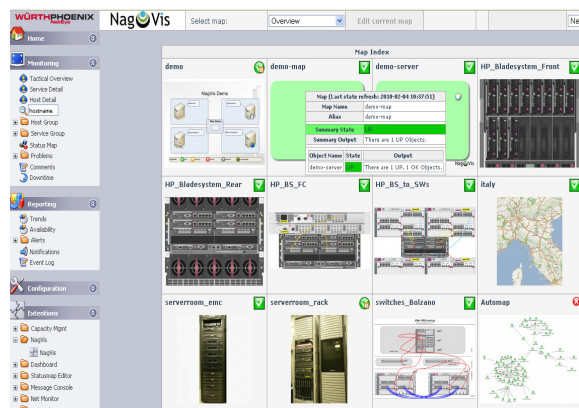
Some of the possible Cacti plug-ins, included into the default release package, will be the weather map and the network traffic analysis tool, integrated into NetEye with the net-flow Sensor (nfSen).



## NagVis

The newest version of NagVis 1.4.5 is mainly a maintenance release with minor bug fixes concerning the installer and automap function. Nevertheless it also includes two really interesting new features. Firstly it is now possible to configure the weight/coverage of the single states and substates. Secondly it has been implemented a backend called mklivestatus, a new data provider which fetches the Nagios state information directly from Nagios core process using live status event broker module. The main advantage of this module is that it provides direct access to the status

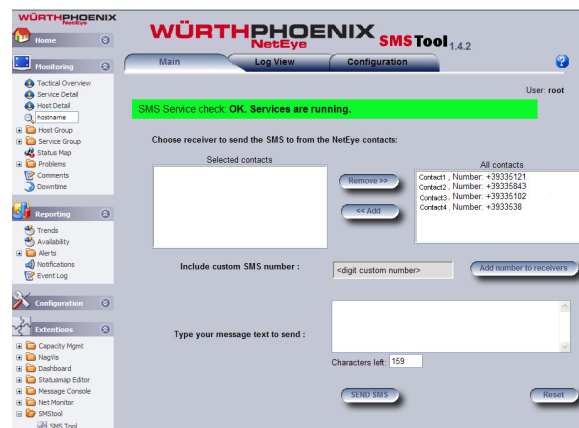
information in the Nagios core without storing any information in a database or file. Therefore, the performances have been significantly improved and ndo2db can now be substituted with the event broker module.





## SMS Tool

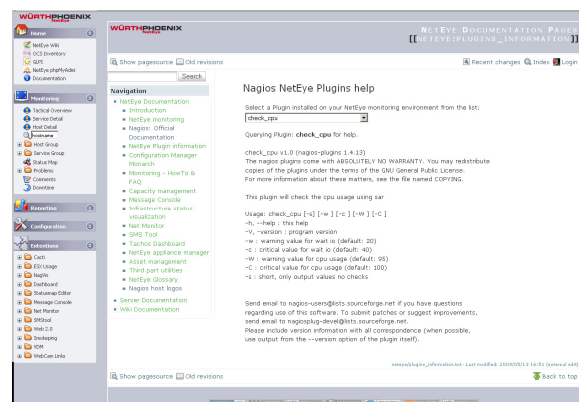
A phonebook utility has been integrated into the SMS Tool, allowing to register not only the standard Nagios phone contacts, but also additional phone numbers that can be used to send SMS directly from the system.



## Documentation

Additional chapters and monitoring scenarios have been integrated into the previously released documentation package.

Furthermore a dynamic search page has been created, to query for help and usage instructions for the installed Nagios plug-ins.



## OCS Inventory and GLPI

GLPI helps you manage and track I.T. equipment, like computers, software, peripherals, and consumables, and their associated maintenance, documentation, and help desk requests, the latest version 0.72 is now available. It can be combined

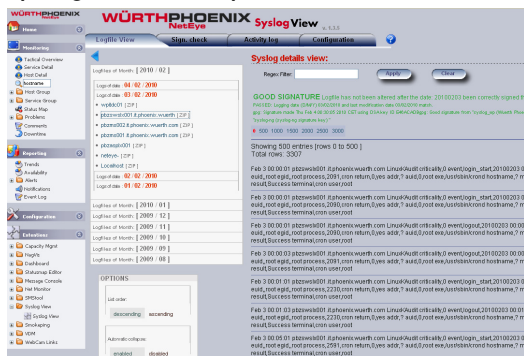
with OCS Inventory to enable auto-discovery, inventory visualization, and application deployment to monitored computers. OCS Inventory 1.0.4 has been integrated including bug fixes and improvements on the Agent's compatibility with the different OS.



# Syslog View

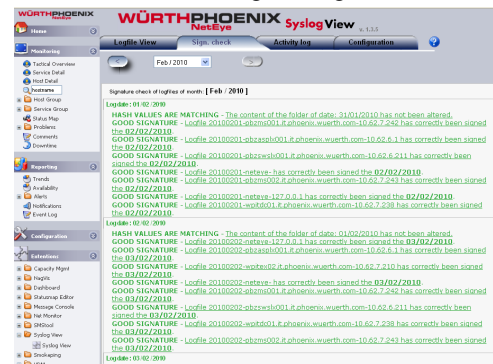
According to the measure of the privacy guarantor "Misura e accorgimenti prescritti ai titolati dei trattamenti con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" a Log Auditing system has been implemented.

- Authentication and access logs are archived in real time including completeness of information: date, time, message logs, user charges, the result of authentication and access client information.
- Verification of system administration accesses is possible through the Syslog View NetEye console

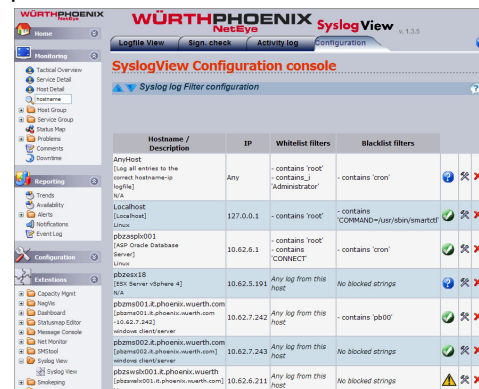


- 6 months data are stored in the central NetEye archive
- Syslog activity log is archived in a dedicated file, containing all the daily operations of the system administrators on the Syslog configuration pane.

- Inalterability of the data is achieved through asymmetric encryption algorithms (PGP implementation) and md5checksum on the storage directory structure. The Logs' integrity can be verified checking the data contained in the digital signature.



- Configuration and management of NetEye Syslog: hosts and filter settings. Only the authorized administrator can access to this pane.





## Safed Agent for Syslog

Newly implemented agent for the registration and the authentication of the access logs in real time including completeness of information: date, time, message logs, user charges, the result of authentication and access client information.

The Safed Agent supports the transmission of messages using the protocols udp and tcp; it is more reliable and the transmission errors

are handled through a persistent cache: even if the client machine is rebooted, the messages are transferred as soon as the agent is started again. Supported platforms: Linux, HP-UX, Solaris and Microsoft Windows.

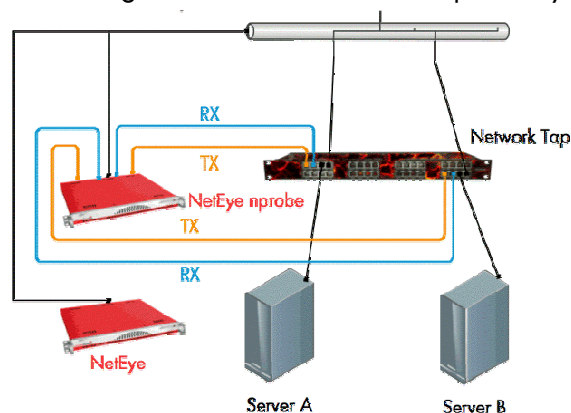
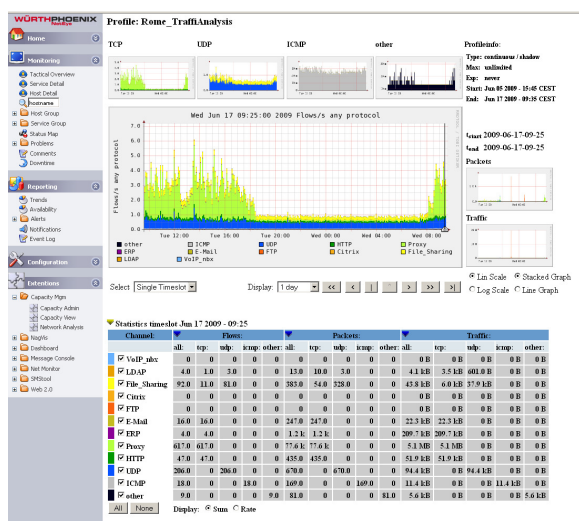
The snare agent for windows now supports also the transmission of messages using the tcp protocol.



## Network Traffic Monitoring

Integration of advanced network analysis, based on net-flow sensor. Netflow/sflow have been integrated in Cacti Graphs to show traffic graphs through protocols (http, citrix, smtp, file share, ...) on WAN. It can be generated a report showing date, protocol, source and target IP address, the Bytes moved, the flows, packets, duration, pps, bps and bpp.

Additionally, nprobe is available to generate detailed NetFlow flows. It collects traffic data and emits NetFlow v5/v9/IPFIX flows towards the specified collector. Every flow, even a very long standing ISO CD image download, has a limited lifetime; this is because the flow collector should periodically receive flow chunks for accounting traffic precisely.







## Voice call notifications

---

In case of anomalies, notifications are sent to preemptively inform the system administrators of possible anomalies (via e-mail, SMS or

pager) . A newly Implemented voice call system is also now available.



## Integrated Tools

---

WÜRTHPHOENIX NetEye integrated the latest versions of various Open Source tools.

Cacti: complete graphic solution for the network

NagVis: Nagios data visualization

ntop: network traffic analyzer

GLPI: Asset Management

WIKI: documentation

OCS Inventory: Inventory

OTRS: Open Source ticket request system

