

# NetEye Release Notes 2015 – Version 3.6



*This document provides an overview of the new features and enhancements released on WÜRTHPHOENIX NetEye version 3.6.*

## Effective Log Auditing, meaningful reports and better integration of the single modules

The new version NetEye 3.6 provides some substantial improvements, to respond to specific customer needs, as well as to satisfy the continuously growing requirements in the complex world of IT monitoring.

Major investments were made in the fields of reporting and SLA measurement. Thanks to a unified data structure, the merge of de-centrally collected data in a single reporting database is now possible.

Through continuous developments, based on results of yearly customer surveys, user groups feedback and trends in the open source community, NetEye reached the state of a unified monitoring solution, which is able to respond to customer requirements also in an enterprise environment.

## 1. Data Becomes Information: Log Analysis and Event Correlation with the new Log Management Module

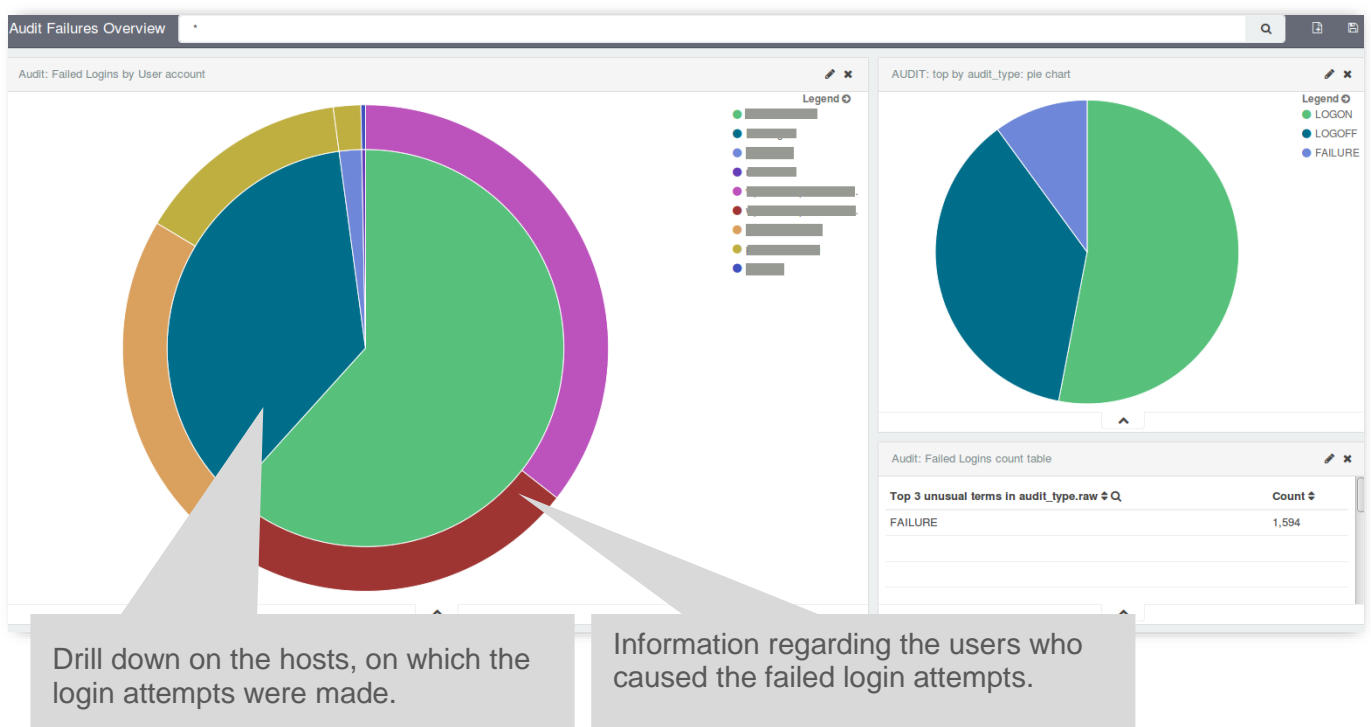
Nowadays, Security Auditing becomes more and more important for companies of different dimensions. On the one hand, a well-structured Log Management is indispensable for the fulfillment of **legal guidelines**, on the other hand, it supplies relevant information regarding the actual state of security of the company.

The Log Management of NetEye 3.6 allows to extract **meaningful information** from the collected logs. To do so, the contents of the collected log files are indexed, classified and structurally saved for further analysis. In this way, efficient requests on data volumes of any size become possible, to examine their contents in a context. Consequently, the definition of extensive queries on complex expression of substantial statements on the collected data is possible.

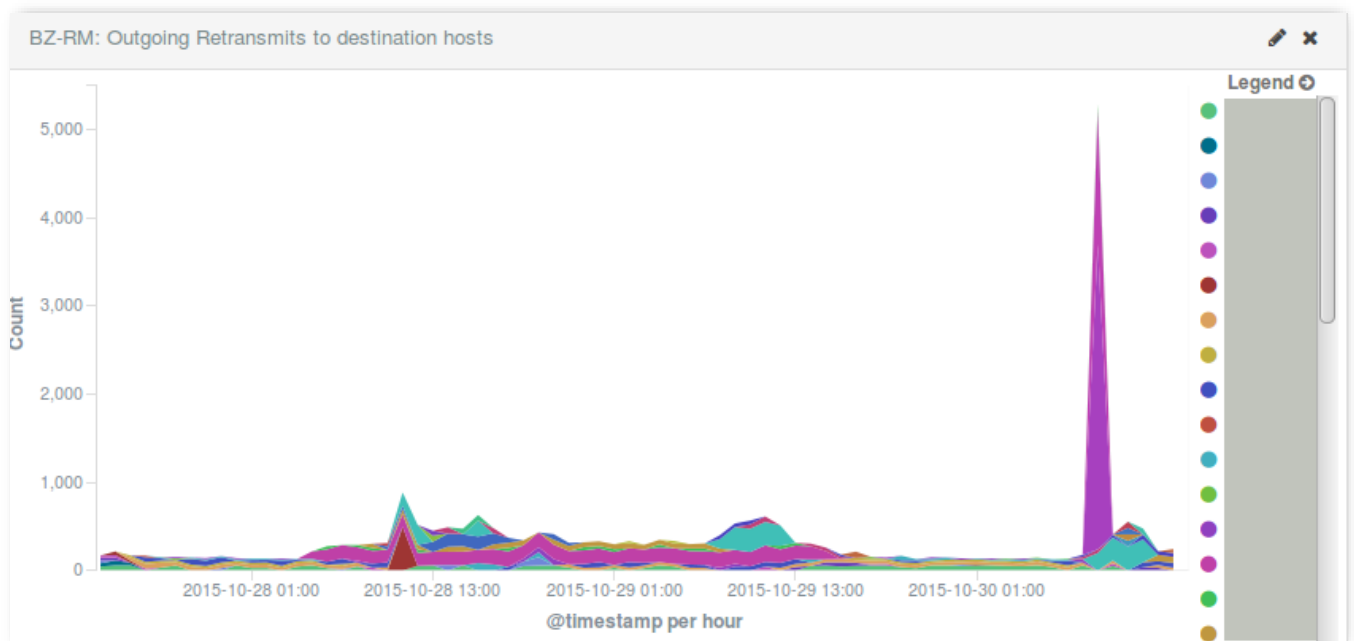
The extended Log Management of NetEye 3.6 is able to recall all collected data, such as system errors or authentication and event logs, to filter, aggregate, and graphically display them. This representation allows to immediately recognize connections, trends, anomalies and security vulnerabilities.

With this method it is possible to implement a **security auditing strategy**, providing metrics like the number of failed logins.

Another representation allows to breakdown on the **user accounts** which caused the failed logins.



Moreover, **undesirable network activities** can be deduced from identified anomalies (peaks). Problems on data transmission can be detected through the representation of undelivered data packages.



The above-mentioned examples should provide a first impression on the different application possibilities of the extended Log Management module in NetEye 3.6.

The reorganization of initially chaotic data masses becomes possible through the integration of the Elastic Stack (consisting of Elasticsearch, Logstash and Kibana), which allows the individual definition of alarms, no matter how big the data amount is.

*N.B.: Through the integration of Kibana 4, Internet Explorer 9 is not further supported.*

## 2. More Precise Reporting: Event Correction to Better Monitor SLAs

To guarantee a high quality level for business critical IT services, the strict supervision of defined Service Level Agreements (SLAs) is unavoidable.

With NetEye 3.6 new possibilities for the management of availability data are provided. The logged monitoring events, which are required to evaluate the compliance with predefined SLAs, are examined on their accuracy and can now also be adjusted. It is now possible to adapt data to the effective perception of the service receiver. Downtimes can be adjusted and completed with additional, relevant information. This is for example useful if a disruption was not caused by the service provider and therefore should have no impact on the SLA report. Moreover, downtimes within appointed maintenance windows can be marked and afterwards excluded from the SLA report. Therefore, the subsequent correction of monitoring events helps to ensure the exactness of the reporting regarding compliance with SLAs.

This functionality is ensured also in case of automatic report dispatching, where it can be decided if the event correction should be applied or not.

### **3. Better Integration: Data Exchange among Modules**

A smooth interaction among different modules and therefore the exchange of data within NetEye, is especially important for the reliable management of company assets.

Through the latest enhancements, data recorded by the network discovery can be completely transferred to the asset management. All devices can now be linked to the corresponding maintenance and support contracts in the asset management. Additionally to the network devices themselves, also their single components and their state of utilization can be displayed within the asset management.

Data collected by the network discovery, as well as data stored in the asset management can be used for the definition of monitoring checks.

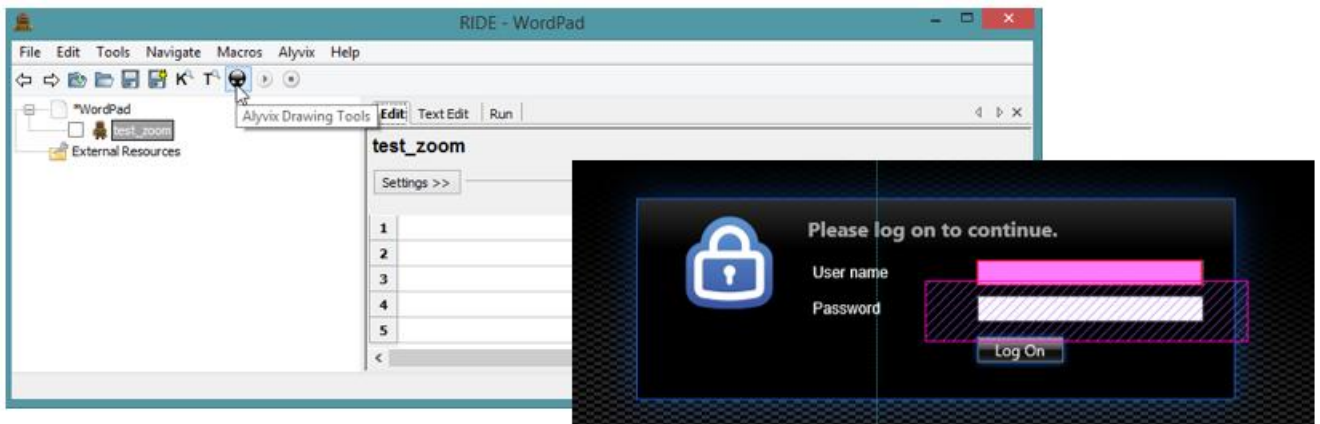
Additionally to the management of computers, network device, servers and printers, the entire lifecycle of other devices as for example smartphones can be managed.

Therefore, the asset management becomes a central place for the management of all devices and their components. Furthermore, the connection with user accounts from the active directory allows the mapping of an organizational structure and the information transfer to the service desk.

### **4. End User Experience: Continuous Monitoring of Application Performance from the End User's Perspective**

To simplify the identification of performance and reliability deficiencies on business critical applications such as Citrix, SAP, Terminal Server, etc. the following enhancements were implemented:

- Straightforward creation of test cases directly from the user interface (no Python knowledge required)
- Enhanced security through the encryption of passwords in test cases
- Deployment in two simple steps
- Better computer vision algorithms to correctly recognize objects
- Automatic creation of HTML reports including screenshots of the tested application to support troubleshooting
- API to create new plugins
- Less CPU consumption
- Custom configuration of log retention



[Alyvix](#), the engine to monitor application performance from the end user's perspective, continuously simulates a certain transaction sequence on any application (exactly in the way a real user would perform the transaction). In this way, suddenly occurring deviations can be recognized and immediately removed.

## 5. Real User Experience: Release of RUE 1.9

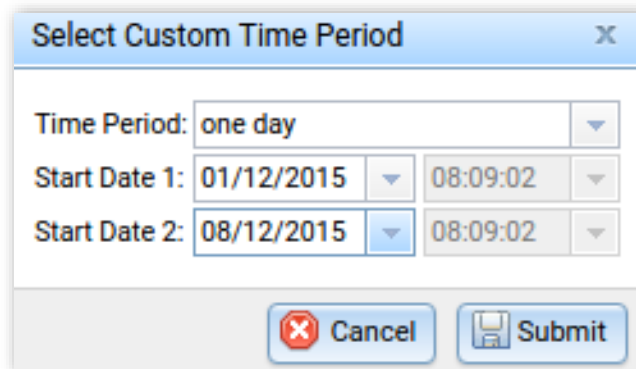
The combination of **Application Performance Monitoring (APM)** and **Network Performance Monitoring (NPM)** to an **Application Aware Network Performance Monitoring (ANPM)** provides information about the real performance situation of a company network. Due to the actuality of this topic and the immediate impacts on the business result, the recent version of NetEye Real User Experience, RUE 1.9 was extended by the following functionalities:

- **Illustration of changes on the baseline**

Changes on the baseline values are now marked through a vertical line on the timeline in the dashboard. Major information about the change are reported through a relative tooltip, to get all relevant information at a glance. In this way a genuine view of the situation is made available.

- **Individual definition of comparative periods**

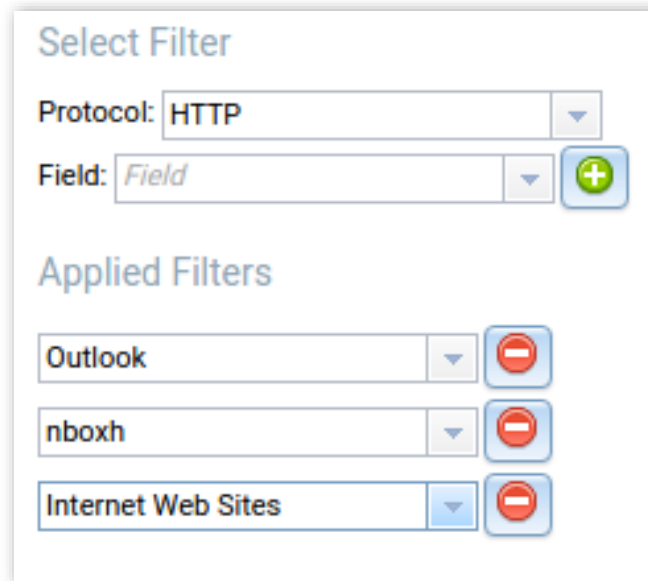
To trace performance developments over a certain period of time and for the visualization of performance changes, it is necessary to compare performance data of two time spans. To allow such a comparison, RUE 1.9 gives the possibility to individually set the periods to be compared.



- **Detailed analysis through the definition of individual filters**

In RUE, key performance indicators (KPIs) are calculated from the collected performance data. These indicators can be aggregated to deduce valuable information. The application of further filters allows a more precise evaluation regarding network and application performance.

RUE 1.9 allows to use all available fields (see [RUE\\_KPI.pdf](#)) to filter data.



The screenshot shows a web interface for selecting filters. At the top, there is a 'Select Filter' section. It contains two dropdown menus: 'Protocol' with 'HTTP' selected and 'Field' with 'Field' selected. To the right of the 'Field' dropdown is a green plus button. Below this is an 'Applied Filters' section. It contains three filter entries, each with a dropdown menu and a red minus button to the right: 'Outlook', 'nboxh', and 'Internet Web Sites'.

- **New KPIs**

Two further KPIs were introduced:

- Explicit Congestion Notification
- Inflight Bytes

- **New configuration panel for the network probe of ntop**

For the analysis of data which are protected by a SSL certificate the recorded traffic has to be encrypted. This is done by the network probe (nBox provided by ntop), which needs the private key of the certificate. The required keys can now be easily uploaded through a new configuration panel.

- **Configuration validation and recovery**

Changes on the monitoring configuration affect the calculated performance metrics, therefore configuration modifications are important to be noted for an exact performance evaluation. If, for example, on one or more subnets are excluded from the monitoring of the throughput, it is obvious that the collected performance values change.

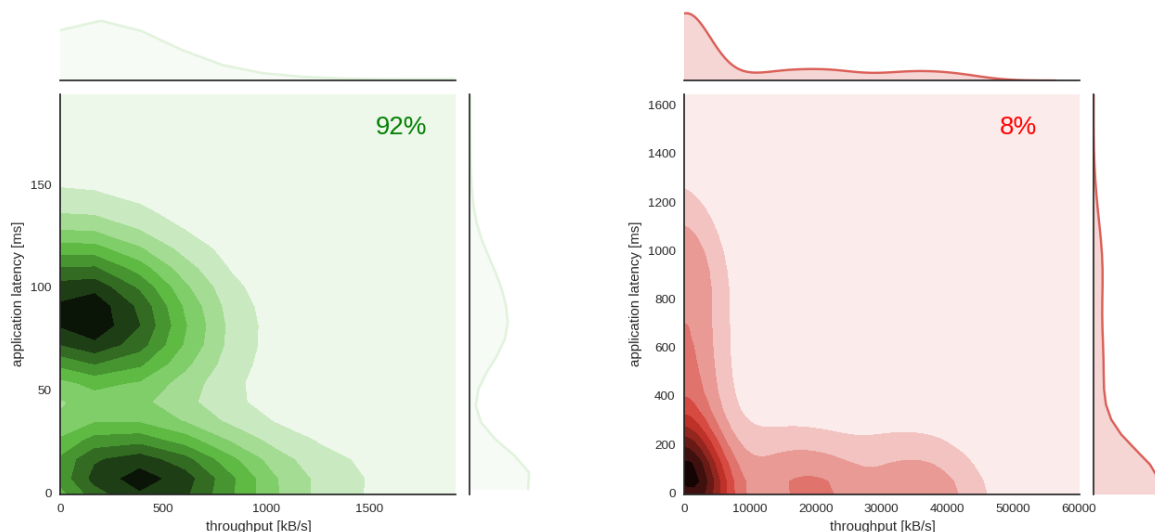
In RUE 1.9 each new configuration is validated before its application. In this way, configuration errors can be showed and removed. Furthermore, from the frontend, the last valid configuration can be restored.

- **First Machine Learning functionalities**

As described in the Würth Phoenix white paper “[Statistics and Machine Learning Techniques for Real User Experience](#)“, NetEye Real User Experience is going to be extended by analysis methods from the fields of machine learning and advanced statistics. Version 1.9 already contains two visualization methods, which provide an abstract, more general overview of network and application performance and therefore simplifies problem detection at an early stage. There is the possibility to let the system generate two completely new plot-types: a series of density plots, which show the averaged density distribution of requests in a multi-dimensional space (latency vs. throughput), as well as performance trends, which effectively visualize how traffic is changing over time.

- Density plots

In the field of network and application traffic monitoring it is disadvantageous to characterize data just by their mean value because that way information concerning the real data distribution gets lost.



*Density Plots of traffic from a single day; 92% are dense standard traffic (left graph in green), 8% are detected as sparse traffic (right graph in red). During the day under analysis it is very likely to find requests with an application latency of ca. 90 ms and a throughput of 150 kB/s or alternatively requests with an application latency of 10 ms and a throughput of ca. 400 kB/s. The probability distribution of the application latency has two maxima. There exist also requests with much more extreme values regarding throughput and application latency, but these extreme values represent at most 8% of the complete traffic of the day under analysis.*

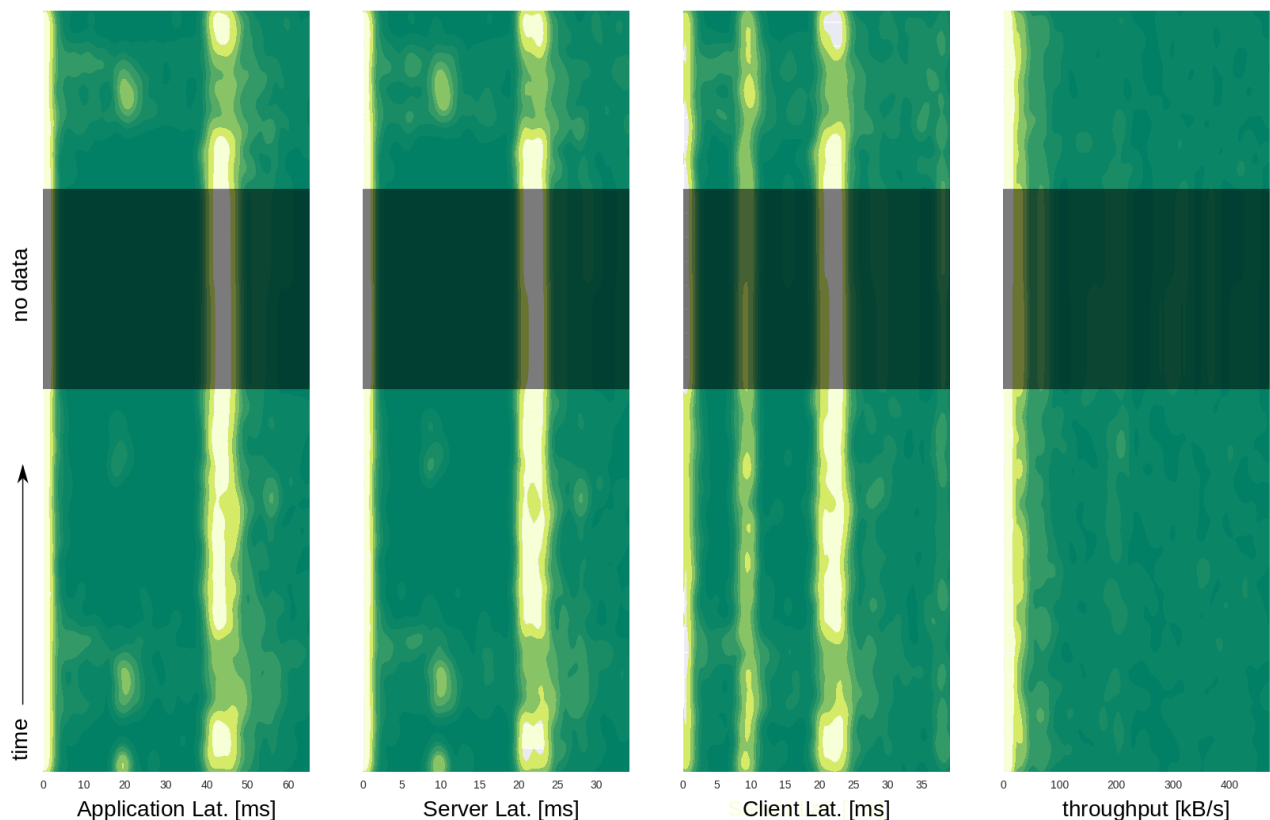
From Version 1.9 of RUE onwards density plots are available in addition to mean-based “warnings” and “criticals”. First, the entire traffic of each day is divided into standard traffic (green) and sparse traffic (red). Each of the three latencies (application latency, server latency, client latency) is then plotted for both traffic types against the throughput. From this graphs it can easily be seen, which the most likely values on the day of interest are and how large the percentage of standard traffic was compared to the entire traffic.

- Performance Trends

This tool allows to visualize high-level performance trends (PTs), which can be used for application performance monitoring as well as for network performance monitoring. Performance trends bring available data to a certain level of abstraction to get a better overview about the performance and to plan targeted drill downs.

Such PT-graphs can be used to compare data from different networks or applications within the same period.

The interpretation of PT plots is straightforward. Shades of green correspond to requests appearing at low frequency, shades of yellow characterize high-frequency requests. Vertically, continuous areas form when traffic is constant over time. Less regular traffic produces dots and smaller regions instead. Areas covered in gray mark periods for which there are not enough data available to allow conclusions about their distribution.



*Performance Trends; traffic on the day under analysis is almost constant (Server Latency 22 ms, Client Latency 22 ms, Throughput < 25 kB/s). Beside the frequent values also all latencies show values near 0. In the case of client latency, traffic with ca. 10 ms coexists besides the already described traffic. This regards fewer requests, as those which lie around 22 ms. For a short period no data is available, this region is covered in gray.*



## **6. NetEye 3.6 Log Management Update Note**

To update to the Log Management of NetEye 3.6 the following requirements have to be fulfilled:

- On SBS systems the present log archiving using the NetEye 3.5 Log Manager and rsyslog is still supported. The extension of Elasticsearch and Kibana cannot be granted.
- The following minimum hardware requirements have to be fulfilled for the installation of Elasticsearch and Kibana:
  - CPU Quad-Core
  - RAM 12 GB
  - Disk 500 GB