# NetEye Release Notes 2015 – Version 3.6


*Dieses Dokument enthält eine Aufstellung der neuen Funktionen und der Verbesserungen, die für die neue Version 3.6 von WÜRTHPHOENIX NetEye implementiert wurden.*

## Gezielteres Log Auditing, aussagekräftigere Reports und bessere Integration der Module

Die neue Version NetEye 3.6 verfügt über einige grundlegende Verbesserungen. Um sowohl den Ansprüchen der Kunden, als auch den stetig steigenden Anforderungen in der komplexen Welt des IT-Monitorings gerecht zu werden, wurden verschiedenen Anpassungen und Neuerungen vorgenommen.

Die größten Investitionen wurden in den Bereichen Reporting und SLA-Berechnung vorgenommen. Durch die Vereinheitlichung der Datenstruktur wird die Zusammenführung der dezentral erhobenen Daten, in einer einheitlichen Reporting-Datenbank ermöglicht.

Dank der kontinuierlichen Weiterentwicklungen, basierend auf den Ergebnissen der jährlichen Kundenumfragen, Usergroups und Trends in der Open Source Community, erreicht NetEye den Status einer Unified Monitoring Lösung, welche auch den hohen Ansprüchen von Kunden im Enterprise-Umfeld gerecht werden kann.

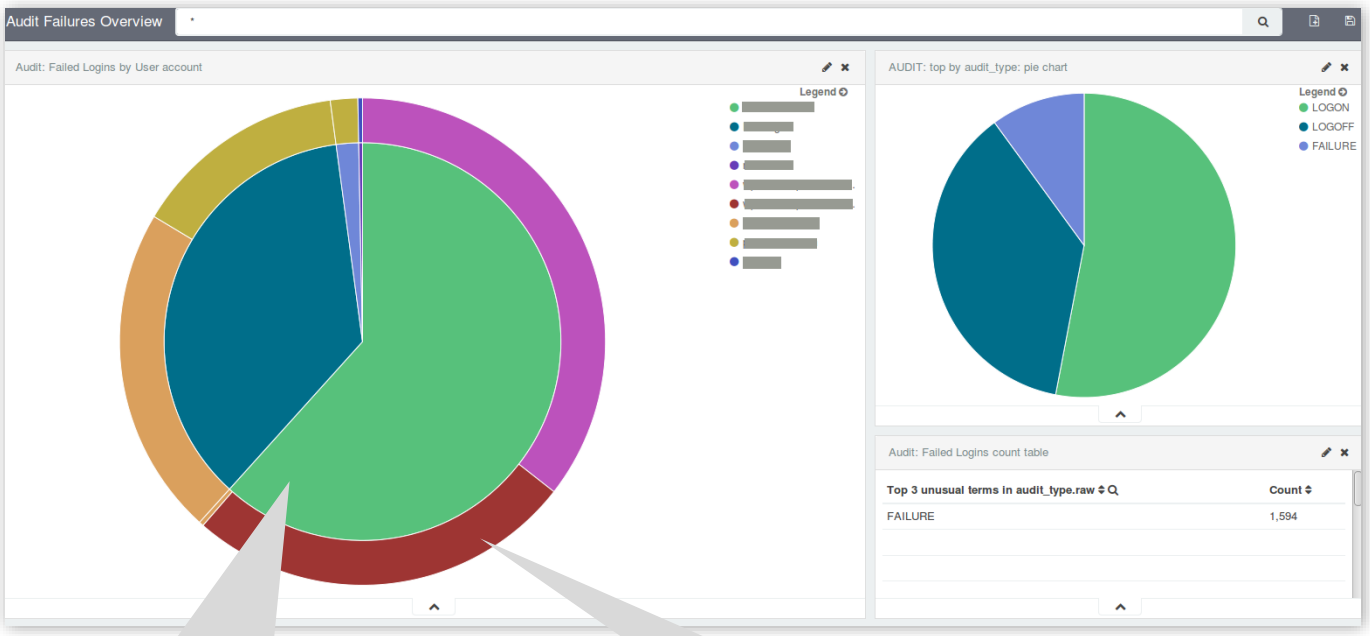
# 1. Daten werden zu Informationen: Log-Analyse und Event-Korrelierung im neuen Log Management

In der heutigen Zeit nimmt Security Auditing für Unternehmen aller Dimensionen einen immer wichtigeren Stellenwert ein. Ein strukturiertes Log Management ist einerseits unerlässlich für die Einhaltung gesetzlicher Richtlinien, andererseits liefert es vielsagende Informationen in Hinsicht auf die Sicherheit des Unternehmensnetzwerks.

Das Log Management von NetEye 3.6 ermöglicht es, aus gesammelten Logs aufschlussreiche Informationen zu extrahieren. Hierfür werden die Inhalte der gesammelten Datensätze indexiert, klassifiziert und in einer Datenstruktur für Abfragen vorgehalten. So ist es möglich sehr effiziente Abfragen über eine beliebig große Anzahl an Daten durchzuführen und deren Inhalte in einem bestimmten Kontext zu beleuchten, um gezielte Aussagen zu den gesammelten Informationen treffen zu können.

Im erweiterten Log Management von NetEye 3.6 kann zentral auf alle gesammelten Daten, wie z.B. Systemfehlermeldungen, Authentifizierungs- und Ereignislogs, zugegriffen werden, um diese sinnvoll zu filtern, zu aggregieren und anschließend grafisch abzubilden. Diese Darstellung ermöglicht die intuitive Erkennung von Zusammenhängen, Trends, Anomalien sowie eventueller Sicherheitsschwachstellen.

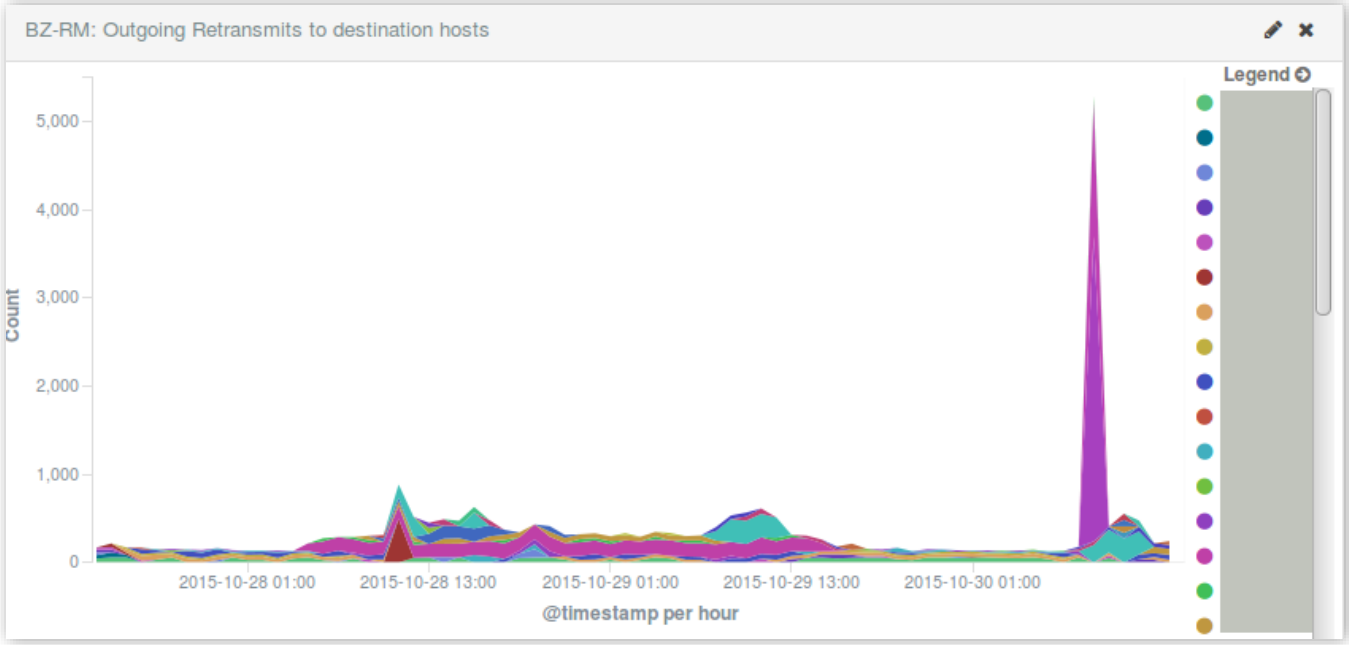
Mit dieser Methode ist es möglich ein Security Audit zu implementieren, woraus die Anzahl der fehlgeschlagenen Login-Versuche ersichtlich werden. In einer erweiterten Darstellung, können die Ereignisse auf die betroffenen Benutzerkonten heruntergebrochen werden, um darzustellen welche Accounts die fehlerhaften Logins verursacht haben.




Drill Down der Hosts, auf welche Login-Versuche vorgenommen wurden, die jedoch fehlgeschlagen sind.

Informationen zu den Benutzern welche den fehlgeschlagenen Logins verursacht haben.

In einem weiteren Einsatzbeispiel können durch die Identifizierung von Auffälligkeiten (Spitzen) ungewollte Netzwerkaktivität abgeleitet werden.
Durch die Darstellung fehlerhaft zugestellter Datenpakete können Probleme bei der Datenübertragung erkannt werden.




Die oben angeführten Beispiele sollen einen Eindruck der verschiedenen Einsatzmöglichkeiten des erweiterten Log Management von NetEye 3.6 vermitteln.
Durch die Integration des Elastic Stack (bestehend aus Elasticsearch, Logstash und Kibana) ist die Organisation anfangs unübersichtlicher Datenmassen und die Definition individueller Alarmierungen ein Leichtes. Auch die Größe der Datenmenge stellt nun keine Einschränkung mehr dar.

*N.B.: Aufgrund der Integration von Kibana 4 wird Internet Explorer 9 nicht mehr unterstützt.*

## 2. Genaueres Reporting: Verwaltung der Verfügbarkeitsdaten zur Kontrolle der SLAs

Wenn es um die Sicherstellung eines gewissen Qualitäts-Niveaus der geschäftskritischen IT-Dienste geht, ist die gezielte Überwachung der vereinbarten Service Level Agreements (SLAs) unumgänglich.

Mit NetEye 3.6 werden neue Möglichkeiten zur Verwaltung der Verfügbarkeitsdaten geboten. Die aufgezeichneten Monitoring-Events, welche für die Bewertung der Einhaltung vordefinierter SLAs ausschlaggebend sind, können auf Richtigkeit überprüft und angepasst werden. Es ist nun möglich die erfassten Daten an die effektive Wahrnehmung beim Service-Empfänger anzupassen. Beispielsweise können Downtimes richtiggestellt und mit den erforderlichen Informationen ergänzt werden. Dies ist hilfreich wenn eine Störung nicht vom Service-Anbieter verursacht wurde und daher keinen Einfluss auf die SLA-Einhaltung hat. Außerdem können Downtimes innerhalb der vorgesehenen Wartungsfenster gekennzeichnet und nachträglich aus dem SLA-Reporting ausgeschlossen werden.
Die nachträgliche Korrektur von Monitoring-Events unterstützt somit die Exaktheit der Berichterstattung in Bezug auf die SLA-Einhaltung.

Diese Funktionalität wird auch bei der automatisierten Report-Versendung gewährleistet, wobei definiert werden kann ob die vorgenommenen Anpassungen berücksichtigt werden sollen oder nicht.

## 3. Verbesserte Integration: Datenaustausch zwischen Modulen

Ein reibungsloses Zusammenspiel der einzelnen Module und somit der Austausch der Datenbestände innerhalb NetEye, sind besonders wichtig für eine zuverlässige Verwaltung aller Unternehmens-Assets.

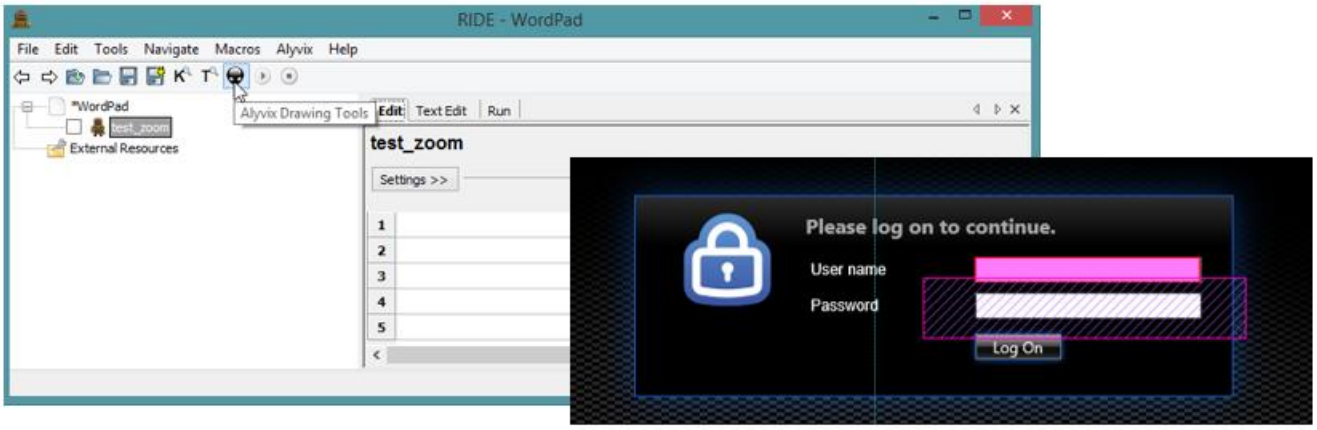
Durch die letzten Verbesserungen können die vom Netzwerk-Discovery erfassten Daten vollständig an das Asset Management übergeben werden. Alle Geräte können nun mit den entsprechenden Wartungs- und Supportverträgen im Asset Management verlinkt werden. Neben dem Netzwerkgerät selbst, können auch dessen Komponenten und sein Verwendungsstatus im Asset Management abgebildet werden.
Die vom Netzwerk-Discovery erfassten Informationen, als auch die im Asset Management gespeicherten Daten, können für die Definition von Kontrollen verwendet werden.
Neben der Verwaltung von Computern, Netzwerkgeräten, Servern und Druckern, kann auch der gesamte Lebenszyklus anderer Geräte wie z.B. Smartphones verwaltet werden.

Das Asset Management wird somit zum zentralen Verwaltungspunkt aller Geräte und Komponenten. Die Verknüpfung mit Benutzerkonten aus der Active Directory ermöglicht außerdem die Abbildung einer organisatorischen Struktur und die Weitergabe dieser Informationen an den Service Desk.

## 4. End User Experience: Kontinuierliche Überwachung der Application Performance aus der Sicht der End-User

Um die Identifizierung von Leistungs- und Zuverlässigkeitsmängeln an geschäftskritischen Applikationen wie Citrix, SAP, Terminal Server usw. zu vereinfachen, wurden folgende Verbesserungen vorgenommen:

- Intuitive und geführte Erstellung der Testszenarien direkt über die Benutzeroberfläche (keine Programmier-Kenntnisse erforderlich)
- Mehr Sicherheit durch die Verschlüsselung von Passwörtern innerhalb der Test Cases
- Implementierung in zwei einfachen Schritten
- Verbesserung der Computer Vision Algorithmen zur sicheren Erkennung von Objekten
- Automatisierte Erstellung von HTML-Reports inklusive Screenshots der getesteten Anwendung zur Unterstützung des Troubleshootings
- API zur Entwicklung neuer Plugins
- Geringerer CPU-Verbrauch
- Individuell konfigurierbare Log Retention




Alyvix, die Engine für die Überwachung der Application Performance aus der Perspektive des Benutzers, simuliert kontinuierlich eine bestimmte Transaktionsabfolge auf der zu testenden Applikation (genauso, wie es auch ein tatsächlicher User machen würde). So können plötzlich auftretende Abweichungen sofort erkannt und unmittelbar behoben werden.

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

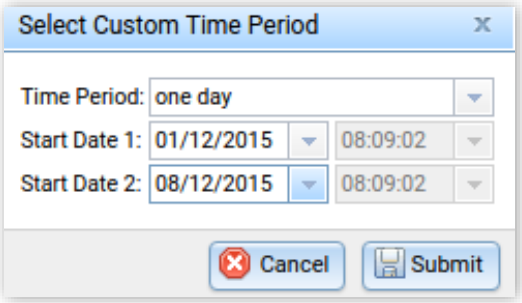
Die Vereinigung von **Application Performance Monitoring** (APM) und **Network Performance Monitoring** (NPM) zu einem **Application Aware Network Performance Monitoring** (ANPM) verschafft Aufschluss über die tatsächliche Performance-Situation eines Unternehmensnetzwerks. Aufgrund der Aktualität des Themas und der unmittelbaren Auswirkungen auf den Geschäftserfolg, wurde die neueste Version der NetEye Real User Experience, RUE 1.9, um folgende Funktionen erweitert.

- **Abbildung von Änderungen an der Baseline**

Veränderungen der Baseline-Werte werden mit einer entsprechenden Linie auf der Zeitachse im Dashboard gekennzeichnet. Über ein Tooltip werden die wichtigsten Informationen der Anpassung auf einen Blick angezeigt. Dadurch wird ein unverfälschtes Bild der Situation dargestellt.

- **Individuelle Definition der Vergleichsperioden**

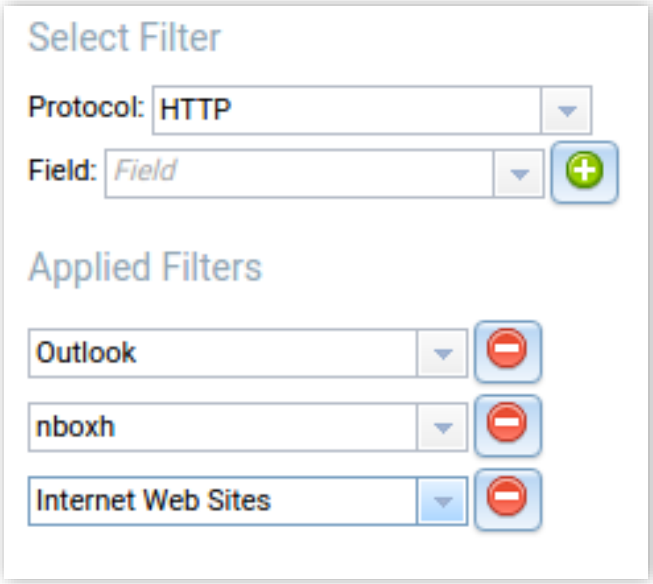
Zur Verfolgung der Performance-Entwicklung über einen längeren Zeitraum und zur Abbildung von Leistungs-Veränderungen, ist es notwendig die erfassten Werte zweier Zeitspannen grafisch gegenüberzustellen. Um diese Vergleichsmöglichkeiten zu erweitern steht mit RUE 1.9 die Möglichkeit zur Verfügung die Vergleichsperioden individuell einzustellen.



- **Gezieltere Analysen durch die Definition individueller Filter**

In RUE werden aus den gesammelten Daten Leistungsindikatoren (KPIs) errechnet. Diese Indikatoren, können aggregiert werden, um aussagekräftige Information abzuleiten. Die weitere Verwendung individueller Filter ermöglicht die gezielte Bewertung, um zutreffende Aussagen in Bezug auf die Netzwerk- und Application Performance treffen zu können.

In RUE 1.9 können alle zur Verfügung stehenden Felder (siehe RUE_KPI.pdf) zur Erstellung individueller Filter verwendet werden.




- **Neue KPIs**

Die Ermittlung zwei weiterer KPIs wurde hinzugefügt:

- Explicit Congestion Notification
- Inflight Bytes

- **Neues Konfigurationspanel für die Netzwerk-Sonde von ntop**

Für eine Analyse von Daten, welche beispielsweise durch ein SSL-Zertifikat geschützt sind, muss der erfasste Traffic entschlüsselt werden. Dies wird von der Netzwerk-Sonde (nBox von ntop) erledigt, welche hierfür den Private Key des Zertifikats verwendet. Über ein integriertes Konfigurationspanel können die verschiedenen Schlüssel komfortabel hochgeladen werden.

- **Validierung und Wiederherstellung früherer Konfigurationen**

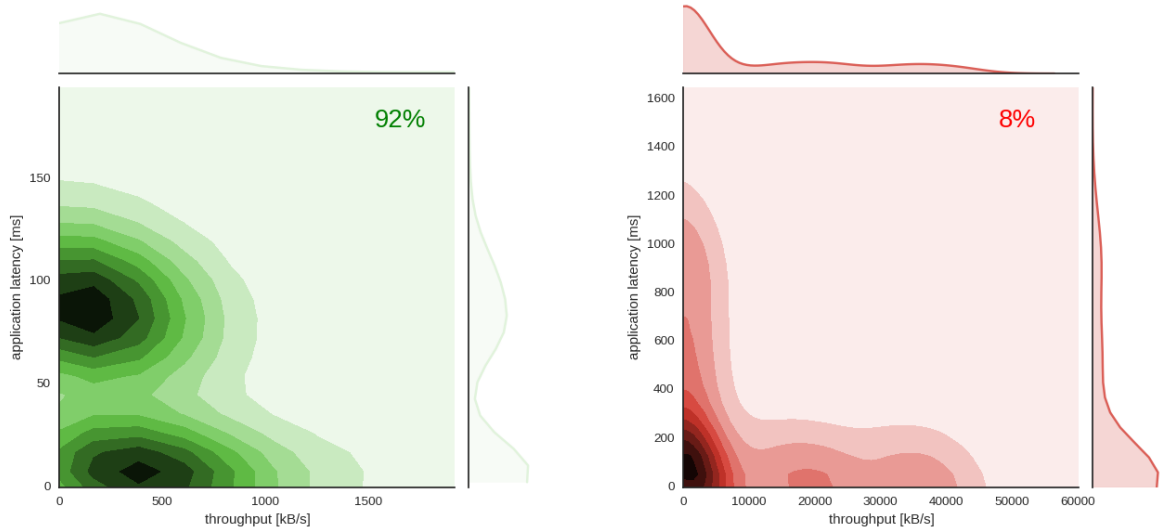
Veränderungen der Monitoring-Konfiguration wirken sich auf die Leistungs-Metriken aus, daher sind Modifikationen an den Konfigurationen für die Leistungsbewertung relevant. Werden beispielsweise von der Überwachung des Throughputs, zwei Subnetze ausgeschlossen, verändern sich in Folge auch die erfassten Werte zur Netzwerk-Performance.
In RUE 1.9 wird jede neue Konfiguration validiert bevor sie angewandt wird. So werden Konfigurationsfehler angezeigt und können vom User behoben werden. Über das Frontend kann außerdem die letzte gültige Konfiguration widerhergestellt werden.

- **Erste Machine Learning Funktionen**

Wie in im White Paper „Statistics and Machine Learning Techniques for Real User Experience“ beschrieben, soll die Real User Experience in Zukunft mit Analysemethoden aus dem Gebiet Machine Learning und Statistik erweitert werden. Version 1.9 enthält bereits erste Visualisierungsmethoden, die einen abstrakten, eher generellen Überblick über die Performance des Netzwerks oder der Applikation ermöglichen und somit die frühe Phase der Problemerkennung unterstützen. Im Detail handelt es sich um die Möglichkeit zwei vollkommen neue Graphiken erzeugen zu lassen: eine Serie von Density Plots, die die Dichteverteilung der Requests im mehrdimensionalen Raum (Latency vs. Throughput) über den Tag gemittelt zeigen, sowie Performance Trends, die temporäre Veränderungen des Traffics sichtbar werden lassen.

- Density Plots

Werden in den Bereichen Netzwerk- und Application Traffic Monitoring die Daten nur über einen Mittelwert charakterisieren hat dies den Nachteil, dass auf diese Weise Informationen bezüglich der Datenverteilung verloren gehen

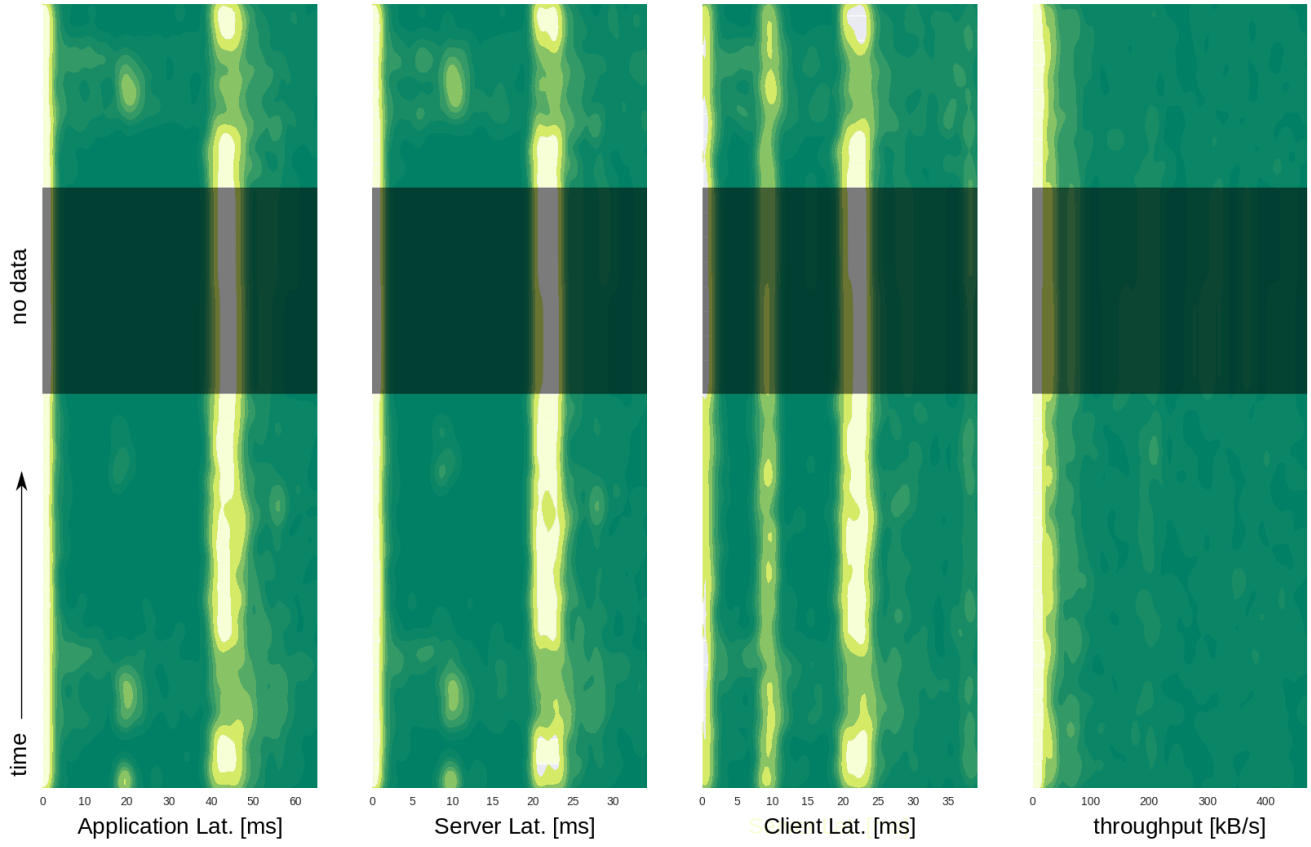



*Density Plots eines Tages; 92% sind dichter Standardtraffic (linke Grafik in grün), 8% werden als weniger dichter Traffic (rechte Grafik in rot) detektiert. Es ist sehr wahrscheinlich am zu untersuchenden Tag Requests mit einer Application Latency von ca. 90 ms und einem Troughput von 150 kB/s zu finden alternativ Requests mit einer Application Latency von 10 ms und einem Throughput von ca. 400 kB/s. Die Wahrscheinlichkeitsverteilung der Application Latency hat zwei Maxima. Es gibt auch Requests mit viel extremeren Werten was Throughput bzw. Application Latency betrifft, aber diese extremeren Werte machen am zu untersuchenden Tag maximal 8% des totalen Traffics aus.*

Neben den auf Mittelwerten basierten „Warnings“ und „Criticals“ stehen ab RUE 1.9 außerdem Density Plots zur Verfügung. Der gesamte Traffic eines Tages wird zunächst in Standardtraffic (grün) und weniger dichten Traffic (rot) geteilt. Jede der drei Latencies ist dann jeweils für den Throughput der beiden Traffics aufgetragen. Aus diesen Graphiken lässt sich einfach ablesen, welche Werte die wahrscheinlichsten am zu untersuchenden Tag waren und welchen Anteil der Standardtraffic am Gesamttraffic hatte.

- Performance Trends

Dieses Tool erlaubt die Darstellung von high-level Performance Trends (PTs), welche sowohl für das Application Performance Monitoring als auch für das Netzwerk Performance Monitoring eingesetzt werden kann. Der Performance Trend bringt die gesammelten Daten auf eine gewisse Abstraktionsebene, um eine bessere Übersicht über die Performance zu erhalten und gezielte Drill Downs zu planen.
Zum Vergleich der Performance verschiedener Netzwerke oder Applikationen im selben Zeitraum, können solche PT-Grafiken gegenübergestellt und miteinander verglichen werden.
Die Interpretation der PT Plots ist unkompliziert. Grüntöne entsprechen einer geringeren Query-Häufigkeit, Gelbtöne stehen für höhere Query-Häufigkeit. Weite Bereiche und vertikale Streifen kennzeichnen zeitlich konstanten Traffic. Kleinere, gleichfarbige Bereiche, sowie Punkte und Inseln entstehen, wenn der Traffic zum Unterbrechen neigt. Verdunkelte Flächen (grau) markieren Zeiträume, in denen nicht ausreichend Daten vorliegen um verlässliche Rückschlüsse über die Verteilung zu ermöglichen.




*Performance Trends; Traffic ist an den zu analysierenden Tagen annähernd konstant (Application Latency: 42 ms, Server Latency 22 ms, Client Latency 22 ms, Throughput < 25 kB/s). Neben den sehr häufigen Werten treten bei allen Latencies auch Werte von annähernd 0 ms auf. Im Fall der Client Latency koexistiert Traffic mit ca. 10 ms neben dem bereits beschriebenen. Es handelt sich allerdings um weniger Requests als bei denen die um die 22 ms liegen. Von einem kurzen Zeitraum liegen keine Daten vor, der Bereich wurde grau überlagert.*

## 6. NetEye 3.6 Log Management Update Hinweise

Für das Update auf das Log Management von NetEye 3.6 sind folgende Hardware Voraussetzungen zu berücksichtigen:

- Auf SBS Systemen wird die bisherige Log Archivierung mit dem NetEye Log Management und rsyslog weiterhin unterstützt. Die Erweiterung von Elasticsearch und Kibana kann nicht garantiert werden.

- Folgende Hardware-Mindestvoraussetzungen müssen für die Installation von Elasticsearch und Kibana gegeben sein:
    - CPU Quad-Core
    - RAM 12 GB
    - Disk 500 GB