

NetEye Release Notes – Version 3.7



Dieses Dokument enthält eine Aufstellung der neuen Funktionen und der Verbesserungen, die für die neue Version 3.7 von WÜRTHPHOENIX NetEye implementiert wurden.

Neue Release-Strategie

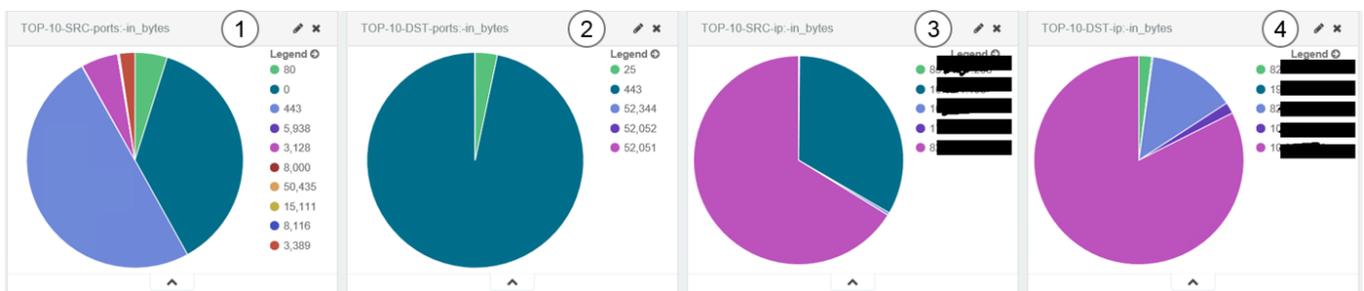
Mit 2016 wird für NetEye eine neue Release-Strategie eingeführt, welche drei Minor-Releases pro Jahr vorsieht. Dadurch können neue Funktionen schneller an die Anwender weitergegeben und Update-Vorgänge wesentlich vereinfacht werden. Basierend auf der mitgelieferten Dokumentation, können Updates in Zukunft direkt vom NetEye Anwender selbst vorgenommen werden.

Erweitertes Log Management und genaueres Service Level Management

Die wesentlichsten Neuerungen betreffen die Bereiche Log Management und Service Level Management. Für die entsprechenden Module wurden neue Funktionalitäten entwickelt, welche den Anwendern erhebliche Zeiteinsparungen ermöglichen.

1. Erweiterung für NetFlow im Log Management

Die Integration des Elastic Stack in das NetEye Log Management hat zusätzlich zur Verbesserung der Verwaltung klassischer Log-Daten auch den großen Vorteil, dass die Analyse und Visualisierung von NetFlow Daten stark vereinfacht und beschleunigt wird. Neben der bestehenden Analyse mit NfSen, können die Netzwerkkommunikationen nun auch über intuitive Dashboards visualisiert und analysiert werden. Ein weiteres Plus der anschaulichen Dashboards, ist die klare und verständliche Berichterstattung an die Geschäftsleitung.



- (1) Top 10 Quell-Ports, welche den meisten Traffic generieren.
- (2) Top 10 Ziel-Ports, welche den meisten Traffic generieren.
- (3) Top 10 Quell-IPs, welche den meisten Traffic generieren.
- (4) Top 10 Ziel-IPs, welche den meisten Traffic generieren.

Für die Archivierung der NetFlows wird eine Datenhaltung von einer Woche empfohlen.

2. Verbesserung der Einplanung von Wartungsfenstern

In NetEye 3.7 ist es möglich, geplante Wartungsfenster auf alle Geschäftsprozesse zu übertragen die mit dem zu wartenden Host oder Service in Verbindung stehen. Neben einer erheblichen Zeitersparnis hat diese Übertragung den Vorteil, dass auf einen Blick ersichtlich wird welche Prozesse aktuell nicht verfügbar sind und welcher Host oder Service dem Downtime zu Grunde liegt. Außerdem können die Auswirkungen geplanter Arbeiten auf das Unternehmensgeschehen, vorab ersichtlich gemacht werden. Dies unterstützt wiederum die Zeitplanung der Wartungsfenster.

Während der Definition der Downtime am Host oder Service, können aus der Liste der betroffenen Geschäftsprozesse jene ausgewählt werden, für welche die Downtime ebenfalls angezeigt werden soll. Durch die simple Auswahlmöglichkeit per Klick, muss der System Administrator die Wartungsfenster nicht auf allen betroffenen Prozessen einzeln definieren und profitiert somit von einer erheblichen Zeitersparnis.

select all - unselect all - all problems - all with downtime

Command:	Add Downtime
Comment:	
Start:	2016-03-21 16:15:00
End:	2016-03-21 18:15:00
Options:	Child Hosts: Do nothing with child hosts Type: Fixed
Business Processes:	<input checked="" type="checkbox"/> SharePoint_2010 (Impacted) <input type="checkbox"/> WP_Core_services (Impacted) <input type="checkbox"/> wp-mail (Impacted) <input type="checkbox"/> core-switch-1 (Impacted) <input type="checkbox"/> VoIP (Impacted) <input type="checkbox"/> ERP System (Impacted) <input type="checkbox"/> core-switches (Impacted) <input type="checkbox"/> WP_Published_services (Impacted) <input type="checkbox"/> WP_Published_services (Impacted) <input type="checkbox"/> Exchange Server 2007 (Impacted) <input type="checkbox"/> main-connectivity (Impacted) <input type="checkbox"/> BZ_user_services select all - select impacted - clear all
submit command for 1 host and 0 Business Processes	

3. Genauere SLA Reports

Die Vorteile des, seit NetEye 3.6 verfügbaren, Event Correction Moduls gelten nun auch für das SLA-Reporting. Unterbrechungen welche nicht in die Berechnung der SLA-Einhaltung mit einfließen sollen, können korrigiert und dadurch von der Berichterstattung ausgeschlossen werden.

Konkret bedeutet dies, dass Wartungsfenster und andere Events nachträglich gekennzeichnet und von der SLA-Berechnung ausgeschlossen werden können. Die ursprünglichen und die manuell erstellten Events werden als getrennte Einträge beibehalten. Somit können sowohl Reports zu den korrigierten, als auch zu den ursprünglichen Ereignissen generiert werden.

4. Erkennung der HTTP-Anfragemethode POST

Durch die Erfassung der POST Daten von HTTP-Anfragen können die Aufrufe von Webdiensten in NetEye Real User Experience gezielter analysiert werden. Durch diese Erweiterung ist es möglich unterschiedliche Anfragen an ein und denselben Web-Dienst (z.B. eine URL in SharePoint) klar zu unterscheiden.

So lässt sich beispielsweise die Anfrage zum Lesen von Daten, von jener zum Verarbeiten von Daten klar unterscheiden. Daraus resultiert die Möglichkeit differenzierte Baselines für unterschiedliche Operationen auf einem Web-Dienst zu definieren.

Requests for all From 23/03/16 10:28:00 To 23/03/16 10:33:00 Select Protocol HTTP Aggregate by

URL	L7 Protocol	Method	Params	Bytes	Throughput	Load Time (ms)	Client Lat (ms)	Server Lat (ms)	App Lat (ms)
1199 of 1199 items shown. Clear filter									
http://mobile.../traveler	HTTP	POST	s=otElyQAA&action=sync&orig=sp&deviceId=Android_b3c8e1a5e165a089	4,6 kB	18,21 kB/s	252.440	4.008	5.686	22.508
http://mobile.../traveler	HTTP	POST	s=otElyQAA&action=sync&orig=sp&deviceId=Android_b3c8e1a5e165a089	9,67 kB	27,33 kB/s	353.803	5.555	5.712	110.993
http://mobile.../traveler	HTTP	POST	s=otDvEAAA&action=sync&orig=sp&deviceId=Android_b3c8e1a5e165a089	5,13 kB	19,29 kB/s	265.817	4.312	4.717	31.647
http://mobile.../traveler	HTTP	POST	s=otDvEAAA&action=sync&orig=sp&deviceId=Android_b3c8e1a5e165a089	4,71 kB	16,61 kB/s	283.251	3.945	11.466	32.935
http://mobile.../traveler	HTTP	POST	s=os8H%2FQAA&action=sync&orig=sp&deviceId=Android_cdac6c5df25684ec	5,49 kB	20,35 kB/s	269.619	4.058	4.871	35.785
http://mobile.../traveler	HTTP	POST	s=os8H%2FQAA&action=sync&orig=sp&deviceId=Android_cdac6c5df25684ec	4,7 kB	18,16 kB/s	258.723	4.468	5.883	22.086
http://mobile.../traveler	HTTP	POST	s=os2RtQAA&action=sync&orig=sp&deviceId=Android_bc3e93bf434db461	7,66 kB	26,94 kB/s	284.286	4.020	5.572	44.963
http://mobile.../traveler	HTTP	POST	s=os2RtQAA&action=sync&orig=sp&deviceId=Android_bc3e93bf434db461	4,68 kB	18,53 kB/s	252.715	4.734	6.886	30.075
http://mobile.../traveler	HTTP	POST	action=sync&orig=sp&deviceId=Android_cdac6c5df25684ec	4,63 kB	18,43 kB/s	251.439	5.025	5.049	29.918
http://mobile.../traveler	HTTP	POST	action=sync&orig=sp&deviceId=Android_bc3e93bf434db461	4,62 kB	18,33 kB/s	252.262	3.909	6.053	26.718
http://mobile.../traveler	HTTP	POST	action=sync&orig=sp&deviceId=Android_bc3e93bf434db461	4,62 kB	17,59 kB/s	262.618	4.777	6.102	30.207
http://mobile.../traveler	HTTP	POST	action=sync&orig=sp&deviceId=Android_b3c8e1a5e165a089	4,61 kB	17,68 kB/s	260.706	4.060	6.190	28.666
http://mobile.../traveler	HTTP	POST	action=sync&orig=sp&deviceId=Android_b3c8e1a5e165a089	4,61 kB	17,3 kB/s	266.494	4.980	5.578	29.929
http://mobile.../traveler	HTTP	POST	action=push&deviceId=Android_caff3415b68a5e88	3,45 kB	12,62 kB/s	272.926	5.126	14.103	28.206
http://mobile.../traveler	HTTP	POST	action=push&deviceId=Android_bc3e93bf434db461	3,74 kB	15,25 kB/s	245.438	4.761	6.204	21.547
http://mobile.../traveler	HTTP	POST	action=push&deviceId=Android_b3c8e1a5e165a089	3,55 kB	320 B/s	11,379.727	4.899	9.901	11,149.693

5. NetEye 3.7 Upgrade-Hinweise

Das Upgrade von NetEye 3.6 auf NetEye 3.7 kann anhand der in NetEye 3.6 zur Verfügung gestellten Dokumentation autonom vorgenommen werden.

Schritt 1: Update des Dokumentationspaketes in NetEye 3.6 durch folgenden Befehl
 "yum --enablerepo=neteye update neteye-documentation"

Schritt 2: Ausführung der in der aktualisierten Dokumentation beschriebenen Upgrade-Prozedur.

Das autonome Upgrade wird für alle zukünftigen Minor NetEye Releases möglich sein. Voraussetzung hierfür ist eine auf CentOS 6 basierende NetEye Installation (alle Versionen ab NetEye 3.6).