Enterprise Monitoring mit Linux

Alexander Schreiber <als@thangorodrim.de>

http://www.thangorodrim.de/

Chemnitzer Linux-Tage 2006

You can't control what you can't measure.

– Tom DeMarco

Übersicht

1. Einführung
2. Monitoringerfahrungen
3. Ende

Enterprise Monitoring - Übersicht

- Servicemonitoring
- Performancemonitoring
- Logüberwachung

Enterprise Monitoring - Übersicht

- Servicemonitoring
- Performancemonitoring
- Logüberwachung

Enterprise Monitoring - Übersicht

- Servicemonitoring
- Performancemonitoring
- Logüberwachung

Enterprise Monitoring - Übersicht

- Servicemonitoring
- Performancemonitoring
- Logüberwachung

Servicemonitoring

- Verfügbarkeit von Hosts & Diensten überwachen
- Benachrichtigung bei Zustandsänderungen
- Zustände: OK/Warnung/kritisch/unbekannt
- Beispiele:
  - Nagios
  - BigBrother
  - Zabbix

Servicemonitoring

- Verfügbarkeit von Hosts & Diensten überwachen
- Benachrichtigung bei Zustandsänderungen
- Zustände: OK/Warnung/kritisch/unbekannt
- Beispiele:
  - Nagios
  - BigBrother
  - Zabbix

Servicemonitoring

- Verfügbarkeit von Hosts & Diensten überwachen
- Benachrichtigung bei Zustandsänderungen
- Zustände: OK/Warnung/kritisch/unbekannt
- Beispiele:
  - Nagios
  - BigBrother
  - Zabbix

Servicemonitoring

- Verfügbarkeit von Hosts & Diensten überwachen
- Benachrichtigung bei Zustandsänderungen
- Zustände: OK/Warnung/kritisch/unbekannt
- Beispiele:
  - Nagios
  - BigBrother
  - Zabbix

Servicemonitoring

- Verfügbarkeit von Hosts & Diensten überwachen
- Benachrichtigung bei Zustandsänderungen
- Zustände: OK/Warnung/kritisch/unbekannt
- Beispiele:
  - Nagios
  - BigBrother
  - Zabbix

Servicemonitoring

- Verfügbarkeit von Hosts & Diensten überwachen
- Benachrichtigung bei Zustandsänderungen
- Zustände: OK/Warnung/kritisch/unbekannt
- Beispiele:
  - Nagios
  - BigBrother
  - Zabbix

Servicemonitoring

- Verfügbarkeit von Hosts & Diensten überwachen
- Benachrichtigung bei Zustandsänderungen
- Zustände: OK/Warnung/kritisch/unbekannt
- Beispiele:
  - Nagios
  - BigBrother
  - Zabbix

Servicemonitoring

- Verfügbarkeit von Hosts & Diensten überwachen
- Benachrichtigung bei Zustandsänderungen
- Zustände: OK/Warnung/kritisch/unbekannt
- Beispiele:
  - Nagios
  - BigBrother
  - Zabbix

Performancemonitoring

- kontinuierliche Aufzeichnung von Parametern
- graphische Darstellung
  $\longrightarrow$ schnelle Trenderkennung
- Beispiele:
  - mrtg
  - rrdstats
  - cacti

Performancemonitoring

- kontinuierliche Aufzeichnung von Parametern
- graphische Darstellung
  $\longrightarrow$ schnelle Trenderkennung
- Beispiele:
  - mrtg
  - rrdstats
  - cacti

Performancemonitoring

- kontinuierliche Aufzeichnung von Parametern
- graphische Darstellung
  $\longrightarrow$ schnelle Trenderkennung
- Beispiele:
  - mrtg
  - rrdstats
  - cacti

Performancemonitoring

- kontinuierliche Aufzeichnung von Parametern
- graphische Darstellung
  $\longrightarrow$ schnelle Trenderkennung
- Beispiele:
  - mrtg
  - rrdstats
  - cacti

Performancemonitoring

- kontinuierliche Aufzeichnung von Parametern
- graphische Darstellung
  $\longrightarrow$ schnelle Trenderkennung
- Beispiele:
  - mrtg
  - rrdstats
  - cacti

Performancemonitoring

- kontinuierliche Aufzeichnung von Parametern
- graphische Darstellung
  $\longrightarrow$ schnelle Trenderkennung
- Beispiele:
  - mrtg
  - rrdstats
  - cacti

Performancemonitoring

- kontinuierliche Aufzeichnung von Parametern
- graphische Darstellung
  $\longrightarrow$ schnelle Trenderkennung
- Beispiele:
  - mrtg
  - rrdstats
  - cacti

Performancemonitoring

- kontinuierliche Aufzeichnung von Parametern
- graphische Darstellung
  $\longrightarrow$ schnelle Trenderkennung
- Beispiele:
  - mrtg
  - rrdstats
  - cacti

Logüberwachung

- Systemlogs, ggf. Anwendungslogs
- Analyse der gesammelten Logmeldungen
- Zustandsermittlung, Problemerkennung
- Beispiele:
  - swatch
  - tenshi

Logüberwachung

- Systemlogs, ggf. Anwendungslogs
- Analyse der gesammelten Logmeldungen
- Zustandsermittlung, Problemerkennung
- Beispiele:
  - swatch
  - tenshi

Logüberwachung

- Systemlogs, ggf. Anwendungslogs
- Analyse der gesammelten Logmeldungen
- Zustandsermittlung, Problemerkennung
- Beispiele:
  - swatch
  - tenshi

Logüberwachung

- Systemlogs, ggf. Anwendungslogs
- Analyse der gesammelten Logmeldungen
- Zustandsermittlung, Problemerkennung
- Beispiele:
  - swatch
  - tenshi

Logüberwachung

- Systemlogs, ggf. Anwendungslogs
- Analyse der gesammelten Logmeldungen
- Zustandsermittlung, Problemerkennung
- Beispiele:
  - swatch
  - tenshi

Logüberwachung

- Systemlogs, ggf. Anwendungslogs
- Analyse der gesammelten Logmeldungen
- Zustandsermittlung, Problemerkennung
- Beispiele:
  - swatch
  - tenshi

Logüberwachung

- Systemlogs, ggf. Anwendungslogs
- Analyse der gesammelten Logmeldungen
- Zustandsermittlung, Problemerkennung
- Beispiele:
  - swatch
  - tenshi

Monitoringerfahrungen – Übersicht

- Servicemonitoring: Nagios
- Performancemonitoring: WebPerfMon (inhouse)
- Logüberwachung: EventlogDB (inhouse)

Monitoringerfahrungen – Übersicht

- Servicemonitoring: Nagios
- Performancemonitoring: WebPerfMon (inhouse)
- Logüberwachung: EventlogDB (inhouse)

Monitoringerfahrungen – Übersicht

- Servicemonitoring: Nagios
- Performancemonitoring: WebPerfMon (inhouse)
- Logüberwachung: EventlogDB (inhouse)

Monitoringerfahrungen – Übersicht

- Servicemonitoring: Nagios
- Performancemonitoring: WebPerfMon (inhouse)
- Logüberwachung: EventlogDB (inhouse)

Nagios – Kurzübersicht

- zentralisiertes Host- & Servicemonitoring
- besteht aus Kernsystem & Plugins
- sehr flexibles Benachrichtigungssystem
- einfache Erweiterbarkeit durch Plugin-System

Nagios – Kurzübersicht

- zentralisiertes Host- & Servicemonitoring
- besteht aus Kernsystem & Plugins
- sehr flexibles Benachrichtigungssystem
- einfache Erweiterbarkeit durch Plugin-System

Nagios – Kurzübersicht

- zentralisiertes Host- & Servicemonitoring
- besteht aus Kernsystem & Plugins
- sehr flexibles Benachrichtigungssystem
- einfache Erweiterbarkeit durch Plugin-System

Nagios – Kurzübersicht

- zentralisiertes Host- & Servicemonitoring
- besteht aus Kernsystem & Plugins
- sehr flexibles Benachrichtigungssystem
- einfache Erweiterbarkeit durch Plugin-System

Nagios – Kurzübersicht

- zentralisiertes Host- & Servicemonitoring
- besteht aus Kernsystem & Plugins
- sehr flexibles Benachrichtigungssystem
- einfache Erweiterbarkeit durch Plugin-System

Nagios – Umgebung

- weit über tausend Hosts
- verteilt über Europa
- heterogen: Linux, Windows NT/2003, ...
- Systemparameter, Anwendungen, Systemprotokoll, ...

Nagios – Umgebung

- weit über tausend Hosts
- verteilt über Europa
- heterogen: Linux, Windows NT/2003, ...
- Systemparameter, Anwendungen, Systemprotokoll, ...

Nagios – Umgebung

- weit über tausend Hosts
- verteilt über Europa
- heterogen: Linux, Windows NT/2003, ...
- Systemparameter, Anwendungen, Systemprotokoll, ...

Nagios – Umgebung

- weit über tausend Hosts
- verteilt über Europa
- heterogen: Linux, Windows NT/2003, ...
- Systemparameter, Anwendungen, Systemprotokoll, ...

Nagios – Umgebung

- weit über tausend Hosts
- verteilt über Europa
- heterogen: Linux, Windows NT/2003, ...
- Systemparameter, Anwendungen, Systemprotokoll, ...

Nagios - Server

- Primärsystem: 4x Xeon 1.9 GHz, 2 GB RAM, 6x 36 GB Disk
- Backupsystem: 1x Xeon 2.6 GHz, 2 GB RAM, 6x 36 GB Disk
- Nagios: 900 Hosts, 9500 Services und wachsend ...
- EventlogDB
- Systemauslastung Primärsystem: mittel
- Systemauslastung Backupsystem: hoch

Nagios - Server

- Primärsystem: 4x Xeon 1.9 GHz, 2 GB RAM, 6x 36 GB Disk
- Backupsystem: 1x Xeon 2.6 GHz, 2 GB RAM, 6x 36 GB Disk
- Nagios: 900 Hosts, 9500 Services und wachsend ...
- EventlogDB
- Systemauslastung Primärsystem: mittel
- Systemauslastung Backupsystem: hoch

Nagios - Server

- Primärsystem: 4x Xeon 1.9 GHz, 2 GB RAM, 6x 36 GB Disk
- Backupsystem: 1x Xeon 2.6 GHz, 2 GB RAM, 6x 36 GB Disk
- Nagios: 900 Hosts, 9500 Services und wachsend . . .
- EventlogDB
- Systemauslastung Primärsystem: mittel
- Systemauslastung Backupsystem: hoch

Nagios - Server

- Primärsystem: 4x Xeon 1.9 GHz, 2 GB RAM, 6x 36 GB Disk
- Backupsystem: 1x Xeon 2.6 GHz, 2 GB RAM, 6x 36 GB Disk
- Nagios: 900 Hosts, 9500 Services und wachsend ...
- EventlogDB
- Systemauslastung Primärsystem: mittel
- Systemauslastung Backupsystem: hoch

Nagios - Server

- Primärsystem: 4x Xeon 1.9 GHz, 2 GB RAM, 6x 36 GB Disk
- Backupsystem: 1x Xeon 2.6 GHz, 2 GB RAM, 6x 36 GB Disk
- Nagios: 900 Hosts, 9500 Services und wachsend ...
- EventlogDB
- Systemauslastung Primärsystem: mittel
- Systemauslastung Backupsystem: hoch

Nagios - Server

- Primärsystem: 4x Xeon 1.9 GHz, 2 GB RAM, 6x 36 GB Disk
- Backupsystem: 1x Xeon 2.6 GHz, 2 GB RAM, 6x 36 GB Disk
- Nagios: 900 Hosts, 9500 Services und wachsend ...
- EventlogDB
- Systemauslastung Primärsystem: mittel
- Systemauslastung Backupsystem: hoch

Nagios - Server

- Primärsystem: 4x Xeon 1.9 GHz, 2 GB RAM, 6x 36 GB Disk
- Backupsystem: 1x Xeon 2.6 GHz, 2 GB RAM, 6x 36 GB Disk
- Nagios: 900 Hosts, 9500 Services und wachsend ...
- EventlogDB
- Systemauslastung Primärsystem: mittel
- Systemauslastung Backupsystem: hoch

Nagios – Sensoren

- Standardsensoren:
  - nsclient: Windows Performancecounter & mehr
  - nrpe/nrpe_nt: remote ausgeführte Plugins
  - nsca: passiv erfaßte Sensormeldungen
- Eigenentwicklungen:
  - RAID-Status, Backupstatus, Systemzeit (via nrpe)
  - physical memory W2K3 (SNMP)
  - Eventlog-Auswertung
  - Zustand In-House Anwendungen (via nsca)

Nagios – Sensoren

- Standardsensoren:
  - nsclient: Windows Performancecounter & mehr
  - nrpe/nrpe_nt: remote ausgeführte Plugins
  - nsca: passiv erfaßte Sensormeldungen
- Eigenentwicklungen:
  - RAID-Status, Backupstatus, Systemzeit (via nrpe)
  - physical memory W2K3 (SNMP)
  - Eventlog-Auswertung
  - Zustand In-House Anwendungen (via nsca)

Nagios – Sensoren

- Standardsensoren:
  - nsclient: Windows Performancecounter & mehr
  - nrpe/nrpe_nt: remote ausgeführte Plugins
  - nsca: passiv erfaßte Sensormeldungen
- Eigenentwicklungen:
  - RAID-Status, Backupstatus, Systemzeit (via nrpe)
  - physical memory W2K3 (SNMP)
  - Eventlog-Auswertung
  - Zustand In-House Anwendungen (via nsca)

Nagios – Sensoren

- Standardsensoren:
  - nsclient: Windows Performancecounter & mehr
  - nrpe/nrpe_nt: remote ausgeführte Plugins
  - nsca: passiv erfaßte Sensormeldungen
- Eigenentwicklungen:
  - RAID-Status, Backupstatus, Systemzeit (via nrpe)
  - physical memory W2K3 (SNMP)
  - Eventlog-Auswertung
  - Zustand In-House Anwendungen (via nsca)

Nagios – Sensoren

- Standardsensoren:
  - nsclient: Windows Performancecounter & mehr
  - nrpe/nrpe_nt: remote ausgeführte Plugins
  - nsca: passiv erfaßte Sensormeldungen
- Eigenentwicklungen:
  - RAID-Status, Backupstatus, Systemzeit (via nrpe)
  - physical memory W2K3 (SNMP)
  - Eventlog-Auswertung
  - Zustand In-House Anwendungen (via nsca)

Nagios – Sensoren

- Standardsensoren:
  - nsclient: Windows Performancecounter & mehr
  - nrpe/nrpe_nt: remote ausgeführte Plugins
  - nsca: passiv erfaßte Sensormeldungen
- Eigenentwicklungen:
  - RAID-Status, Backupstatus, Systemzeit (via nrpe)
  - physical memory W2K3 (SNMP)
  - Eventlog-Auswertung
  - Zustand In-House Anwendungen (via nsca)

Nagios – Sensoren

- Standardsensoren:
  - nsclient: Windows Performancecounter & mehr
  - nrpe/nrpe_nt: remote ausgeführte Plugins
  - nsca: passiv erfaßte Sensormeldungen
- Eigenentwicklungen:
  - RAID-Status, Backupstatus, Systemzeit (via nrpe)
  - physical memory W2K3 (SNMP)
  - Eventlog-Auswertung
  - Zustand In-House Anwendungen (via nsca)

Nagios – Sensoren

- Standardsensoren:
  - nsclient: Windows Performancecounter & mehr
  - nrpe/nrpe_nt: remote ausgeführte Plugins
  - nsca: passiv erfaßte Sensormeldungen
- Eigenentwicklungen:
  - RAID-Status, Backupstatus, Systemzeit (via nrpe)
  - physical memory W2K3 (SNMP)
  - Eventlog-Auswertung
  - Zustand In-House Anwendungen (via nsca)

Nagios – Sensoren

- Standardsensoren:
  - nsclient: Windows Performancecounter & mehr
  - nrpe/nrpe_nt: remote ausgeführte Plugins
  - nsca: passiv erfaßte Sensormeldungen
- Eigenentwicklungen:
  - RAID-Status, Backupstatus, Systemzeit (via nrpe)
  - physical memory W2K3 (SNMP)
  - Eventlog-Auswertung
  - Zustand In-House Anwendungen (via nsca)

Nagios – Sensoren

- Standardsensoren:
  - nsclient: Windows Performancecounter & mehr
  - nrpe/nrpe_nt: remote ausgeführte Plugins
  - nsca: passiv erfaßte Sensormeldungen
- Eigenentwicklungen:
  - RAID-Status, Backupstatus, Systemzeit (via nrpe)
  - physical memory W2K3 (SNMP)
  - Eventlog-Auswertung
  - Zustand In-House Anwendungen (via nsca)

Nagios – Erfahrungen

- Umstieg Nagios 1.x auf Nagios 2.x:
  - viel bessere Performance Webfrontend
  - neue Features
- Flexibilität Nagios sehr wichtig
- Skalierungsschmerzen:
  - Konfigurationstools für Nagios
  - Benachrichtigungen: „Spamflut“

Nagios – Erfahrungen

- Umstieg Nagios 1.x auf Nagios 2.x:
  - viel bessere Performance Webfrontend
  - neue Features
- Flexibilität Nagios sehr wichtig
- Skalierungsschmerzen:
  - Konfigurationstools für Nagios
  - Benachrichtigungen: „Spamflut“

Nagios – Erfahrungen

- Umstieg Nagios 1.x auf Nagios 2.x:
  - viel bessere Performance Webfrontend
  - neue Features
- Flexibilität Nagios sehr wichtig
- Skalierungsschmerzen:
  - Konfigurationstools für Nagios
  - Benachrichtigungen: „Spamflut“

Nagios – Erfahrungen

- Umstieg Nagios 1.x auf Nagios 2.x:
  - viel bessere Performance Webfrontend
  - neue Features
- Flexibilität Nagios sehr wichtig
- Skalierungsschmerzen:
  - Konfigurationstools für Nagios
  - Benachrichtigungen: „Spamflut“

Nagios – Erfahrungen

- Umstieg Nagios 1.x auf Nagios 2.x:
  - viel bessere Performance Webfrontend
  - neue Features
- Flexibilität Nagios sehr wichtig
- Skalierungsschmerzen:
  - Konfigurationstools für Nagios
  - Benachrichtigungen: „Spamflut“

Nagios – Erfahrungen

- Umstieg Nagios 1.x auf Nagios 2.x:
  - viel bessere Performance Webfrontend
  - neue Features
- Flexibilität Nagios sehr wichtig
- Skalierungsschmerzen:
  - Konfigurationstools für Nagios
  - Benachrichtigungen: „Spamflut“

Nagios – Erfahrungen

- Umstieg Nagios 1.x auf Nagios 2.x:
  - viel bessere Performance Webfrontend
  - neue Features
- Flexibilität Nagios sehr wichtig
- Skalierungsschmerzen:
  - Konfigurationstools für Nagios
  - Benachrichtigungen: „Spamflut“

Nagios – Erfahrungen

- Umstieg Nagios 1.x auf Nagios 2.x:
  - viel bessere Performance Webfrontend
  - neue Features
- Flexibilität Nagios sehr wichtig
- Skalierungsschmerzen:
  - Konfigurationstools für Nagios
  - Benachrichtigungen: „Spamflut“

WebPerfMon – Überblick

- Überwachung diverser Performanceparameter
- webbasiertes Werkzeug
- kontinuierliche Datensammlung
- verschiedene Datenquellen
- genaue Langzeitaufzeichnung, exakte Daten auch später auswertbar

WebPerfMon – Überblick

- Überwachung diverser Performanceparameter
- webbasiertes Werkzeug
- kontinuierliche Datensammlung
- verschiedene Datenquellen
- genaue Langzeitaufzeichnung, exakte Daten auch später auswertbar

WebPerfMon – Überblick

- Überwachung diverser Performanceparameter
- webbasiertes Werkzeug
- kontinuierliche Datensammlung
- verschiedene Datenquellen
- genaue Langzeitaufzeichnung, exakte Daten auch später auswertbar

WebPerfMon – Überblick

- Überwachung diverser Performanceparameter
- webbasiertes Werkzeug
- kontinuierliche Datensammlung
- verschiedene Datenquellen
- genaue Langzeitaufzeichnung, exakte Daten auch später auswertbar

WebPerfMon – Überblick

- Überwachung diverser Performanceparameter
- webbasiertes Werkzeug
- kontinuierliche Datensammlung
- verschiedene Datenquellen
- genaue Langzeitaufzeichnung, exakte Daten auch später auswertbar

WebPerfMon – Überblick

- Überwachung diverser Performanceparameter
- webbasiertes Werkzeug
- kontinuierliche Datensammlung
- verschiedene Datenquellen
- genaue Langzeitaufzeichnung, exakte Daten auch später auswertbar

WebPerfMon – Technik

- Datensammler:
  - Gruppe von Daemons, ein Daemon/Sensor
  - Datenprotokollierung: eine Textdatei/Sensor/Host/Tag
- Graphenerstellung
  - aus Textdateien per gnuplot, imagemagick für Thumbnails
  - Cronjob, alle 5 Minuten, alle Graphen
- Webfrontend
  - verlinkte Webseiten, nach Gruppen & Hosts, Thumbnails
  - generiert per Cronjob alle 5 min nach Sensorkonfiguration

WebPerfMon – Technik

- Datensammler:
  - Gruppe von Daemons, ein Daemon/Sensor
  - Datenprotokollierung: eine Textdatei/Sensor/Host/Tag
- Graphenerstellung
  - aus Textdateien per gnuplot, imagemagick für Thumbnails
  - Cronjob, alle 5 Minuten, alle Graphen
- Webfrontend
  - verlinkte Webseiten, nach Gruppen & Hosts, Thumbnails
  - generiert per Cronjob alle 5 min nach Sensorkonfiguration

WebPerfMon – Technik

- Datensammler:
  - Gruppe von Daemons, ein Daemon/Sensor
  - Datenprotokollierung: eine Textdatei/Sensor/Host/Tag
- Graphenerstellung
  - aus Textdateien per gnuplot, imagemagick für Thumbnails
  - Cronjob, alle 5 Minuten, alle Graphen
- Webfrontend
  - verlinkte Webseiten, nach Gruppen & Hosts, Thumbnails
  - generiert per Cronjob alle 5 min nach Sensorkonfiguration

WebPerfMon – Technik

- Datensammler:
  - Gruppe von Daemons, ein Daemon/Sensor
  - Datenprotokollierung: eine Textdatei/Sensor/Host/Tag
- Graphenerstellung
  - aus Textdateien per gnuplot, imagemagick für Thumbnails
  - Cronjob, alle 5 Minuten, alle Graphen
- Webfrontend
  - verlinkte Webseiten, nach Gruppen & Hosts, Thumbnails
  - generiert per Cronjob alle 5 min nach Sensorkonfiguration

WebPerfMon – Technik

- Datensammler:
  - Gruppe von Daemons, ein Daemon/Sensor
  - Datenprotokollierung: eine Textdatei/Sensor/Host/Tag
- Graphenerstellung
  - aus Textdateien per gnuplot, imagemagick für Thumbnails
  - Cronjob, alle 5 Minuten, alle Graphen
- Webfrontend
  - verlinkte Webseiten, nach Gruppen & Hosts, Thumbnails
  - generiert per Cronjob alle 5 min nach Sensorkonfiguration

WebPerfMon – Technik

- Datensammler:
  - Gruppe von Daemons, ein Daemon/Sensor
  - Datenprotokollierung: eine Textdatei/Sensor/Host/Tag
- Graphenerstellung
  - aus Textdateien per gnuplot, imagemagick für Thumbnails
  - Cronjob, alle 5 Minuten, alle Graphen
- Webfrontend
  - verlinkte Webseiten, nach Gruppen & Hosts, Thumbnails
  - generiert per Cronjob alle 5 min nach Sensorkonfiguration

WebPerfMon – Technik

- Datensammler:
  - Gruppe von Daemons, ein Daemon/Sensor
  - Datenprotokollierung: eine Textdatei/Sensor/Host/Tag
- Graphenerstellung
  - aus Textdateien per gnuplot, imagemagick für Thumbnails
  - Cronjob, alle 5 Minuten, alle Graphen
- Webfrontend
  - verlinkte Webseiten, nach Gruppen & Hosts, Thumbnails
  - generiert per Cronjob alle 5 min nach Sensorkonfiguration

WebPerfMon – Technik

- Datensammler:
  - Gruppe von Daemons, ein Daemon/Sensor
  - Datenprotokollierung: eine Textdatei/Sensor/Host/Tag
- Graphenerstellung
  - aus Textdateien per gnuplot, imagemagick für Thumbnails
  - Cronjob, alle 5 Minuten, alle Graphen
- Webfrontend
  - verlinkte Webseiten, nach Gruppen & Hosts, Thumbnails
  - generiert per Cronjob alle 5 min nach Sensorkonfiguration

WebPerfMon – Technik

- Datensammler:
  - Gruppe von Daemons, ein Daemon/Sensor
  - Datenprotokollierung: eine Textdatei/Sensor/Host/Tag
- Graphenerstellung
  - aus Textdateien per gnuplot, imagemagick für Thumbnails
  - Cronjob, alle 5 Minuten, alle Graphen
- Webfrontend
  - verlinkte Webseiten, nach Gruppen & Hosts, Thumbnails
  - generiert per Cronjob alle 5 min nach Sensorkonfiguration

WebPerfMon – Technik

- Datensammler:
  - Gruppe von Daemons, ein Daemon/Sensor
  - Datenprotokollierung: eine Textdatei/Sensor/Host/Tag
- Graphenerstellung
  - aus Textdateien per gnuplot, imagemagick für Thumbnails
  - Cronjob, alle 5 Minuten, alle Graphen
- Webfrontend
  - verlinkte Webseiten, nach Gruppen & Hosts, Thumbnails
  - generiert per Cronjob alle 5 min nach Sensorkonfiguration

WebPerfMon – Erfahrungen

- Entwickelt als schnelle Lösung für Testsysteme
- mehrfache Erweiterung (Sensoren) nach Anwenderwünschen
- Anpassungen, Performanceoptimierungen
- Performancemonitoring kritischer Produktivsysteme
- 24/7 Aufzeichnung, hohe Auflösung (30 Sekunden)
- Langzeitarchivierung, beliebige Auszüge für Detailanalyse

WebPerfMon – Erfahrungen

- Entwickelt als schnelle Lösung für Testsysteme
- mehrfache Erweiterung (Sensoren) nach Anwenderwünschen
- Anpassungen, Performanceoptimierungen
- Performancemonitoring kritischer Produktivsysteme
- 24/7 Aufzeichnung, hohe Auflösung (30 Sekunden)
- Langzeitarchivierung, beliebige Auszüge für Detailanalyse

WebPerfMon – Erfahrungen

- Entwickelt als schnelle Lösung für Testsysteme
- mehrfache Erweiterung (Sensoren) nach Anwenderwünschen
- Anpassungen, Performanceoptimierungen
- Performancemonitoring kritischer Produktivsysteme
- 24/7 Aufzeichnung, hohe Auflösung (30 Sekunden)
- Langzeitarchivierung, beliebige Auszüge für Detailanalyse

WebPerfMon – Erfahrungen

- Entwickelt als schnelle Lösung für Testsysteme
- mehrfache Erweiterung (Sensoren) nach Anwenderwünschen
- Anpassungen, Performanceoptimierungen
- Performancemonitoring kritischer Produktivsysteme
- 24/7 Aufzeichnung, hohe Auflösung (30 Sekunden)
- Langzeitarchivierung, beliebige Auszüge für Detailanalyse

WebPerfMon – Erfahrungen

- Entwickelt als schnelle Lösung für Testsysteme
- mehrfache Erweiterung (Sensoren) nach Anwenderwünschen
- Anpassungen, Performanceoptimierungen
- Performancemonitoring kritischer Produktivsysteme
- 24/7 Aufzeichnung, hohe Auflösung (30 Sekunden)
- Langzeitarchivierung, beliebige Auszüge für Detailanalyse

WebPerfMon – Erfahrungen

- Entwickelt als schnelle Lösung für Testsysteme
- mehrfache Erweiterung (Sensoren) nach Anwenderwünschen
- Anpassungen, Performanceoptimierungen
- Performancemonitoring kritischer Produktivsysteme
- 24/7 Aufzeichnung, hohe Auflösung (30 Sekunden)
- Langzeitarchivierung, beliebige Auszüge für Detailanalyse

WebPerfMon – Erfahrungen

- Entwickelt als schnelle Lösung für Testsysteme
- mehrfache Erweiterung (Sensoren) nach Anwenderwünschen
- Anpassungen, Performanceoptimierungen
- Performancemonitoring kritischer Produktivsysteme
- 24/7 Aufzeichnung, hohe Auflösung (30 Sekunden)
- Langzeitarchivierung, beliebige Auszüge für Detailanalyse

EventlogDB – Übersicht

- Problem: NT-Eventlog nur lokal, viele Server
- zentrale Eventlogarchivierung & Auswertung für W2K3-Server
- Snare als lokaler Eventlogsensor, Echtzeiterfassung
- Weiterleitung auf Syslog-Server
- UNIX-Syslog normal auf Syslog-Server
- Archivierung in Filesystem
- Laden in DB in fast Echtzeit für Analyse

EventlogDB – Übersicht

- Problem: NT-Eventlog nur lokal, viele Server
- zentrale Eventlogarchivierung & Auswertung für W2K3-Server
- Snare als lokaler Eventlogsensor, Echtzeiterfassung
- Weiterleitung auf Syslog-Server
- UNIX-Syslog normal auf Syslog-Server
- Archivierung in Filesystem
- Laden in DB in fast Echtzeit für Analyse

EventlogDB – Übersicht

- Problem: NT-Eventlog nur lokal, viele Server
- zentrale Eventlogarchivierung & Auswertung für W2K3-Server
- Snare als lokaler Eventlogsensor, Echtzeiterfassung
- Weiterleitung auf Syslog-Server
- UNIX-Syslog normal auf Syslog-Server
- Archivierung in Filesystem
- Laden in DB in fast Echtzeit für Analyse

EventlogDB – Übersicht

- Problem: NT-Eventlog nur lokal, viele Server
- zentrale Eventlogarchivierung & Auswertung für W2K3-Server
- Snare als lokaler Eventlogsensor, Echtzeiterfassung
- Weiterleitung auf Syslog-Server
- UNIX-Syslog normal auf Syslog-Server
- Archivierung in Filesystem
- Laden in DB in fast Echtzeit für Analyse

EventlogDB – Übersicht

- Problem: NT-Eventlog nur lokal, viele Server
- zentrale Eventlogarchivierung & Auswertung für W2K3-Server
- Snare als lokaler Eventlogsensor, Echtzeiterfassung
- Weiterleitung auf Syslog-Server
- UNIX-Syslog normal auf Syslog-Server
- Archivierung in Filesystem
- Laden in DB in fast Echtzeit für Analyse

EventlogDB – Übersicht

- Problem: NT-Eventlog nur lokal, viele Server
- zentrale Eventlogarchivierung & Auswertung für W2K3-Server
- Snare als lokaler Eventlogsensor, Echtzeiterfassung
- Weiterleitung auf Syslog-Server
- UNIX-Syslog normal auf Syslog-Server
- Archivierung in Filesystem
- Laden in DB in fast Echtzeit für Analyse

EventlogDB – Übersicht

- Problem: NT-Eventlog nur lokal, viele Server
- zentrale Eventlogarchivierung & Auswertung für W2K3-Server
- Snare als lokaler Eventlogsensor, Echtzeiterfassung
- Weiterleitung auf Syslog-Server
- UNIX-Syslog normal auf Syslog-Server
- Archivierung in Filesystem
- Laden in DB in fast Echtzeit für Analyse

EventlogDB – Übersicht

- Problem: NT-Eventlog nur lokal, viele Server
- zentrale Eventlogarchivierung & Auswertung für W2K3-Server
- Snare als lokaler Eventlogsensor, Echtzeiterfassung
- Weiterleitung auf Syslog-Server
- UNIX-Syslog normal auf Syslog-Server
- Archivierung in Filesystem
- Laden in DB in fast Echtzeit für Analyse

EventlogDB – Technik

- PostgreSQL 8.1
- flaches Datenmodell, jeweils eine Tabelle Syslog/Eventlog
- Eventlog: 62 Tage, 160 Hosts aktiv, 60 Millionen Rows
- Syslog: 62 Tage, 26 Millionen Rows
- on-disk: 50 GB aktuell
- Loader:
  - läuft jede Minute $\longrightarrow$ praktisch Echtzeit
  - ausfiltern uninteressanter Events
  - 1 min Daten in $<<$ 1 Minute
  - bis zu 30K Events/min, bis zu 80% ausgefiltert
- DB *ausschließlich* zur Analyse (Datamining-DB)
- tägliche Analysejobs

EventlogDB – Technik

- PostgreSQL 8.1
- flaches Datenmodell, jeweils eine Tabelle Syslog/Eventlog
- Eventlog: 62 Tage, 160 Hosts aktiv, 60 Millionen Rows
- Syslog: 62 Tage, 26 Millionen Rows
- on-disk: 50 GB aktuell
- Loader:
  - läuft jede Minute $\longrightarrow$ praktisch Echtzeit
  - ausfiltern uninteressanter Events
  - 1 min Daten in $<<$ 1 Minute
  - bis zu 30K Events/min, bis zu 80% ausgefiltert
- DB *ausschließlich* zur Analyse (Datamining-DB)
- tägliche Analysejobs

EventlogDB – Technik

- PostgreSQL 8.1
- flaches Datenmodell, jeweils eine Tabelle Syslog/Eventlog
- Eventlog: 62 Tage, 160 Hosts aktiv, 60 Millionen Rows
- Syslog: 62 Tage, 26 Millionen Rows
- on-disk: 50 GB aktuell
- Loader:
  - läuft jede Minute $\longrightarrow$ praktisch Echtzeit
  - ausfiltern uninteressanter Events
  - 1 min Daten in $<<$ 1 Minute
  - bis zu 30K Events/min, bis zu 80% ausgefiltert
- DB *ausschließlich* zur Analyse (Datamining-DB)
- tägliche Analysejobs

EventlogDB – Technik

- PostgreSQL 8.1
- flaches Datenmodell, jeweils eine Tabelle Syslog/Eventlog
- Eventlog: 62 Tage, 160 Hosts aktiv, 60 Millionen Rows
- Syslog: 62 Tage, 26 Millionen Rows
- on-disk: 50 GB aktuell
- Loader:
  - läuft jede Minute $\longrightarrow$ praktisch Echtzeit
  - ausfiltern uninteressanter Events
  - 1 min Daten in $<<$ 1 Minute
  - bis zu 30K Events/min, bis zu 80% ausgefiltert
- DB *ausschließlich* zur Analyse (Datamining-DB)
- tägliche Analysejobs

EventlogDB – Technik

- PostgreSQL 8.1
- flaches Datenmodell, jeweils eine Tabelle Syslog/Eventlog
- Eventlog: 62 Tage, 160 Hosts aktiv, 60 Millionen Rows
- Syslog: 62 Tage, 26 Millionen Rows
- on-disk: 50 GB aktuell
- Loader:
  - läuft jede Minute $\longrightarrow$ praktisch Echtzeit
  - ausfiltern uninteressanter Events
  - 1 min Daten in $<<$ 1 Minute
  - bis zu 30K Events/min, bis zu 80% ausgefiltert
- DB *ausschließlich* zur Analyse (Datamining-DB)
- tägliche Analysejobs

EventlogDB – Technik

- PostgreSQL 8.1
- flaches Datenmodell, jeweils eine Tabelle Syslog/Eventlog
- Eventlog: 62 Tage, 160 Hosts aktiv, 60 Millionen Rows
- Syslog: 62 Tage, 26 Millionen Rows
- on-disk: 50 GB aktuell
- Loader:
  - läuft jede Minute $\longrightarrow$ praktisch Echtzeit
  - ausfiltern uninteressanter Events
  - 1 min Daten in $<<$ 1 Minute
  - bis zu 30K Events/min, bis zu 80% ausgefiltert
- DB *ausschließlich* zur Analyse (Datamining-DB)
- tägliche Analysejobs

EventlogDB – Technik

- PostgreSQL 8.1
- flaches Datenmodell, jeweils eine Tabelle Syslog/Eventlog
- Eventlog: 62 Tage, 160 Hosts aktiv, 60 Millionen Rows
- Syslog: 62 Tage, 26 Millionen Rows
- on-disk: 50 GB aktuell
- Loader:
  - läuft jede Minute $\longrightarrow$ praktisch Echtzeit
  - ausfiltern uninteressanter Events
  - 1 min Daten in $<<$ 1 Minute
  - bis zu 30K Events/min, bis zu 80% ausgefiltert
- DB *ausschließlich* zur Analyse (Datamining-DB)
- tägliche Analysejobs

EventlogDB – Technik

- PostgreSQL 8.1
- flaches Datenmodell, jeweils eine Tabelle Syslog/Eventlog
- Eventlog: 62 Tage, 160 Hosts aktiv, 60 Millionen Rows
- Syslog: 62 Tage, 26 Millionen Rows
- on-disk: 50 GB aktuell
- Loader:
  - läuft jede Minute $\longrightarrow$ praktisch Echtzeit
  - ausfiltern uninteressanter Events
  - 1 min Daten in $<<$ 1 Minute
  - bis zu 30K Events/min, bis zu 80% ausgefiltert
- DB *ausschließlich* zur Analyse (Datamining-DB)
- tägliche Analysejobs

EventlogDB – Technik

- PostgreSQL 8.1
- flaches Datenmodell, jeweils eine Tabelle Syslog/Eventlog
- Eventlog: 62 Tage, 160 Hosts aktiv, 60 Millionen Rows
- Syslog: 62 Tage, 26 Millionen Rows
- on-disk: 50 GB aktuell
- Loader:
  - läuft jede Minute $\longrightarrow$ praktisch Echtzeit
  - ausfiltern uninteressanter Events
  - 1 min Daten in $<<$ 1 Minute
  - bis zu 30K Events/min, bis zu 80% ausgefiltert
- DB *ausschließlich* zur Analyse (Datamining-DB)
- tägliche Analysejobs

EventlogDB – Technik

- PostgreSQL 8.1
- flaches Datenmodell, jeweils eine Tabelle Syslog/Eventlog
- Eventlog: 62 Tage, 160 Hosts aktiv, 60 Millionen Rows
- Syslog: 62 Tage, 26 Millionen Rows
- on-disk: 50 GB aktuell
- Loader:
  - läuft jede Minute $\longrightarrow$ praktisch Echtzeit
  - ausfiltern uninteressanter Events
  - 1 min Daten in $<<$ 1 Minute
  - bis zu 30K Events/min, bis zu 80% ausgefiltert
- DB *ausschließlich* zur Analyse (Datamining-DB)
- tägliche Analysejobs

EventlogDB – Technik

- PostgreSQL 8.1
- flaches Datenmodell, jeweils eine Tabelle Syslog/Eventlog
- Eventlog: 62 Tage, 160 Hosts aktiv, 60 Millionen Rows
- Syslog: 62 Tage, 26 Millionen Rows
- on-disk: 50 GB aktuell
- Loader:
  - läuft jede Minute $\longrightarrow$ praktisch Echtzeit
  - ausfiltern uninteressanter Events
  - 1 min Daten in $<<$ 1 Minute
  - bis zu 30K Events/min, bis zu 80% ausgefiltert
- DB *ausschließlich* zur Analyse (Datamining-DB)
- tägliche Analysejobs

EventlogDB – Technik

- PostgreSQL 8.1
- flaches Datenmodell, jeweils eine Tabelle Syslog/Eventlog
- Eventlog: 62 Tage, 160 Hosts aktiv, 60 Millionen Rows
- Syslog: 62 Tage, 26 Millionen Rows
- on-disk: 50 GB aktuell
- Loader:
  - läuft jede Minute $\longrightarrow$ praktisch Echtzeit
  - ausfiltern uninteressanter Events
  - 1 min Daten in $<<$ 1 Minute
  - bis zu 30K Events/min, bis zu 80% ausgefiltert
- DB *ausschließlich* zur Analyse (Datamining-DB)
- tägliche Analysejobs

EventlogDB – Technik

- PostgreSQL 8.1
- flaches Datenmodell, jeweils eine Tabelle Syslog/Eventlog
- Eventlog: 62 Tage, 160 Hosts aktiv, 60 Millionen Rows
- Syslog: 62 Tage, 26 Millionen Rows
- on-disk: 50 GB aktuell
- Loader:
  - läuft jede Minute $\longrightarrow$ praktisch Echtzeit
  - ausfiltern uninteressanter Events
  - 1 min Daten in $<<$ 1 Minute
  - bis zu 30K Events/min, bis zu 80% ausgefiltert
- DB *ausschließlich* zur Analyse (Datamining-DB)
- tägliche Analysejobs

EventlogDB – Erfahrungen

- PostgreSQL 8.1 sehr performant
- Queryperformance unkritisch, Insertperformance kritisch!
- PostgreSQL Tuning lohnt sich:
  - Filesystem: XFS
  - Speicherzuweisung an PostgreSQL: großzügig
  - Logwriter tunen
  - Performancekiller: Trigger, Normalisierung, Rules $\longrightarrow$ KISS
  - Daten in großen Transaktionen laden, SERIALIZABLE

EventlogDB – Erfahrungen

- PostgreSQL 8.1 sehr performant
- Queryperformance unkritisch, Insertperformance kritisch!
- PostgreSQL Tuning lohnt sich:
  - Filesystem: XFS
  - Speicherzuweisung an PostgreSQL: großzügig
  - Logwriter tunen
  - Performancekiller: Trigger, Normalisierung, Rules $\longrightarrow$ KISS
  - Daten in großen Transaktionen laden, SERIALIZABLE

EventlogDB – Erfahrungen

- PostgreSQL 8.1 sehr performant
- Queryperformance unkritisch, Insertperformance kritisch!
- PostgreSQL Tuning lohnt sich:
  - Filesystem: XFS
  - Speicherzuweisung an PostgreSQL: großzügig
  - Logwriter tunen
  - Performancekiller: Trigger, Normalisierung, Rules $\longrightarrow$ KISS
  - Daten in großen Transaktionen laden, SERIALIZABLE

EventlogDB – Erfahrungen

- PostgreSQL 8.1 sehr performant
- Queryperformance unkritisch, Insertperformance kritisch!
- PostgreSQL Tuning lohnt sich:
  - Filesystem: XFS
  - Speicherzuweisung an PostgreSQL: großzügig
  - Logwriter tunen
  - Performancekiller: Trigger, Normalisierung, Rules $\longrightarrow$ KISS
  - Daten in großen Transaktionen laden, SERIALIZABLE

EventlogDB – Erfahrungen

- PostgreSQL 8.1 sehr performant
- Queryperformance unkritisch, Insertperformance kritisch!
- PostgreSQL Tuning lohnt sich:
  - Filesystem: XFS
  - Speicherzuweisung an PostgreSQL: großzügig
  - Logwriter tunen
  - Performancekiller: Trigger, Normalisierung, Rules $\longrightarrow$ KISS
  - Daten in großen Transaktionen laden, SERIALIZABLE

EventlogDB – Erfahrungen

- PostgreSQL 8.1 sehr performant
- Queryperformance unkritisch, Insertperformance kritisch!
- PostgreSQL Tuning lohnt sich:
  - Filesystem: XFS
  - Speicherzuweisung an PostgreSQL: großzügig
  - Logwriter tunen
  - Performancekiller: Trigger, Normalisierung, Rules $\longrightarrow$ KISS
  - Daten in großen Transaktionen laden, SERIALIZABLE

EventlogDB – Erfahrungen

- PostgreSQL 8.1 sehr performant
- Queryperformance unkritisch, Insertperformance kritisch!
- PostgreSQL Tuning lohnt sich:
  - Filesystem: XFS
  - Speicherzuweisung an PostgreSQL: großzügig
  - Logwriter tunen
  - Performancekiller: Trigger, Normalisierung, Rules $\longrightarrow$ KISS
  - Daten in großen Transaktionen laden, SERIALIZABLE

EventlogDB – Erfahrungen

- PostgreSQL 8.1 sehr performant
- Queryperformance unkritisch, Insertperformance kritisch!
- PostgreSQL Tuning lohnt sich:
  - Filesystem: XFS
  - Speicherzuweisung an PostgreSQL: großzügig
  - Logwriter tunen
  - Performancekiller: Trigger, Normalisierung, Rules $\longrightarrow$ KISS
  - Daten in großen Transaktionen laden, SERIALIZABLE

EventlogDB – Erfahrungen

- PostgreSQL 8.1 sehr performant
- Queryperformance unkritisch, Insertperformance kritisch!
- PostgreSQL Tuning lohnt sich:
  - Filesystem: XFS
  - Speicherzuweisung an PostgreSQL: großzügig
  - Logwriter tunen
  - Performancekiller: Trigger, Normalisierung, Rules $\longrightarrow$ KISS
  - Daten in großen Transaktionen laden, SERIALIZABLE

Zusammenfassung Erfahrungen

- Nagios: flexibel, sehr gut erweiterbar, leistungsfähig
- Flexibilität von OpenSource-Lösungen als Schlüsselvorteil
- schnelle Reaktion auf neue Anforderungen
- überraschend geringer Hardwarebedarf für viel Leistung
- Kosten nur für Hardware und deren Betrieb
- qualifiziertes Personal für Entwicklung und Deployment
- Lösungen von Anwendern sehr gut angenommen

Zusammenfassung Erfahrungen

- Nagios: flexibel, sehr gut erweiterbar, leistungsfähig
- Flexibilität von OpenSource-Lösungen als Schlüsselvorteil
- schnelle Reaktion auf neue Anforderungen
- überraschend geringer Hardwarebedarf für viel Leistung
- Kosten nur für Hardware und deren Betrieb
- qualifiziertes Personal für Entwicklung und Deployment
- Lösungen von Anwendern sehr gut angenommen

Zusammenfassung Erfahrungen

- Nagios: flexibel, sehr gut erweiterbar, leistungsfähig
- Flexibilität von OpenSource-Lösungen als Schlüsselvorteil
- schnelle Reaktion auf neue Anforderungen
- überraschend geringer Hardwarebedarf für viel Leistung
- Kosten nur für Hardware und deren Betrieb
- qualifiziertes Personal für Entwicklung und Deployment
- Lösungen von Anwendern sehr gut angenommen

Zusammenfassung Erfahrungen

- Nagios: flexibel, sehr gut erweiterbar, leistungsfähig
- Flexibilität von OpenSource-Lösungen als Schlüsselvorteil
- schnelle Reaktion auf neue Anforderungen
- überraschend geringer Hardwarebedarf für viel Leistung
- Kosten nur für Hardware und deren Betrieb
- qualifiziertes Personal für Entwicklung und Deployment
- Lösungen von Anwendern sehr gut angenommen

Zusammenfassung Erfahrungen

- Nagios: flexibel, sehr gut erweiterbar, leistungsfähig
- Flexibilität von OpenSource-Lösungen als Schlüsselvorteil
- schnelle Reaktion auf neue Anforderungen
- überraschend geringer Hardwarebedarf für viel Leistung
- Kosten nur für Hardware und deren Betrieb
- qualifiziertes Personal für Entwicklung und Deployment
- Lösungen von Anwendern sehr gut angenommen

Zusammenfassung Erfahrungen

- Nagios: flexibel, sehr gut erweiterbar, leistungsfähig
- Flexibilität von OpenSource-Lösungen als Schlüsselvorteil
- schnelle Reaktion auf neue Anforderungen
- überraschend geringer Hardwarebedarf für viel Leistung
- Kosten nur für Hardware und deren Betrieb
- qualifiziertes Personal für Entwicklung und Deployment
- Lösungen von Anwendern sehr gut angenommen

Zusammenfassung Erfahrungen

- Nagios: flexibel, sehr gut erweiterbar, leistungsfähig
- Flexibilität von OpenSource-Lösungen als Schlüsselvorteil
- schnelle Reaktion auf neue Anforderungen
- überraschend geringer Hardwarebedarf für viel Leistung
- Kosten nur für Hardware und deren Betrieb
- qualifiziertes Personal für Entwicklung und Deployment
- Lösungen von Anwendern sehr gut angenommen

Zusammenfassung Erfahrungen

- Nagios: flexibel, sehr gut erweiterbar, leistungsfähig
- Flexibilität von OpenSource-Lösungen als Schlüsselvorteil
- schnelle Reaktion auf neue Anforderungen
- überraschend geringer Hardwarebedarf für viel Leistung
- Kosten nur für Hardware und deren Betrieb
- qualifiziertes Personal für Entwicklung und Deployment
- Lösungen von Anwendern sehr gut angenommen

URLs

- http://www.postgresql.org/
- http://www.gnuplot.info/
- http://www.nagios.org/
- http://www.intersectalliance.com/projects/SnareWindows/
- http://nsclient.ready2run.nl/

URLs

- http://www.postgresql.org/
- http://www.gnuplot.info/
- http://www.nagios.org/
- http://www.intersectalliance.com/projects/SnareWindows/
- http://nsclient.ready2run.nl/

Ende

Vielen Dank für Ihr Interesse!