Remote Logging mit rsyslog

Inklusive Tools zur Überwachung und Verwaltung

Thomas Merkel Arkadiusz Rawa Janik Lemcke

Hochschule Ravensburg-Weingarten

17. Juni 2011

Inhaltsverzeichnis

Remote Logging

rsyslog

tenshi

phpLogCon

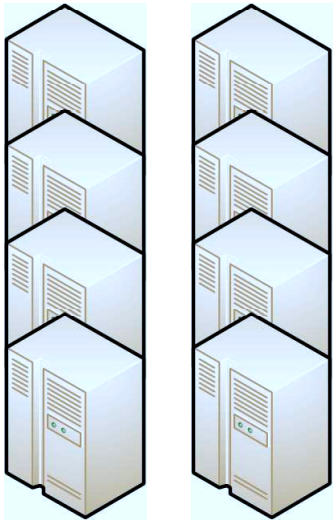
Diskussion

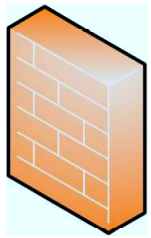
Inhalt

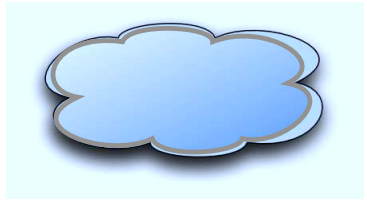
Remote Logging
- Problem
- Panic
- Don't Panic
- Ziele

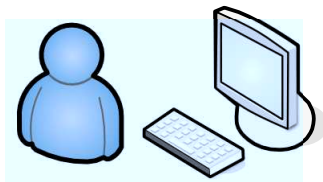
Remote Logging

Problem





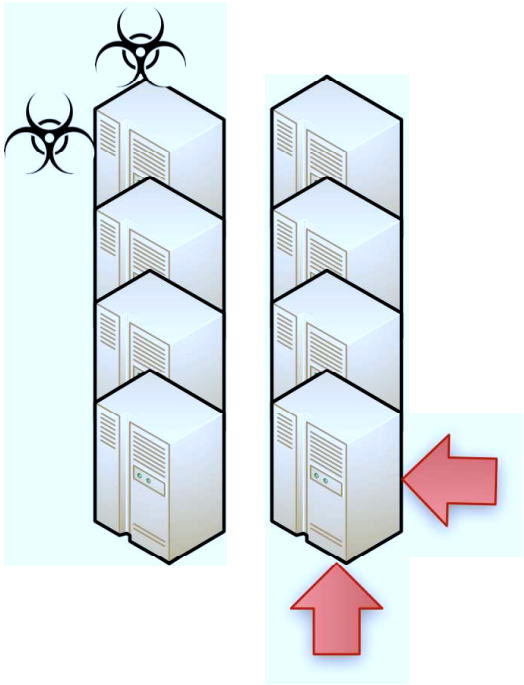


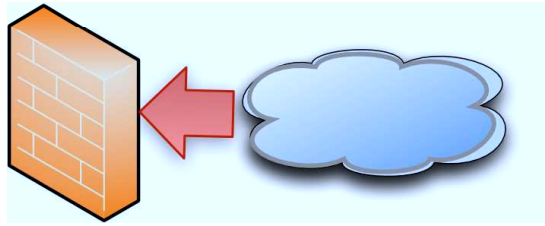


Systemadministrator

Remote Logging

Panic

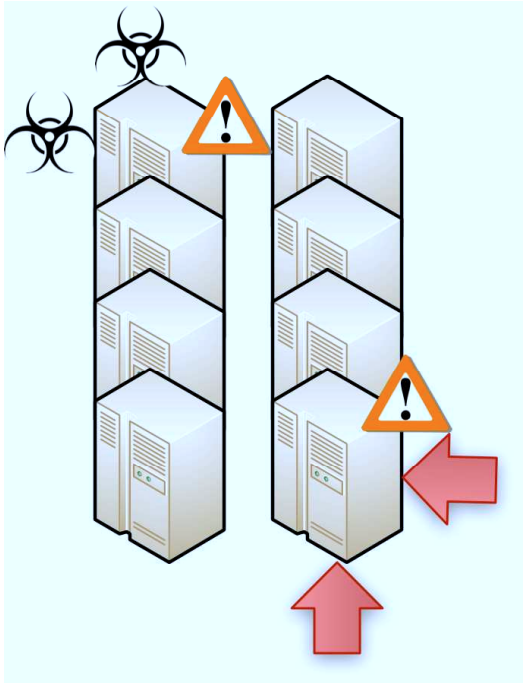


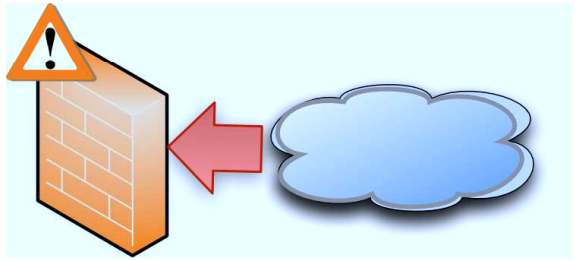


Systemadministrator

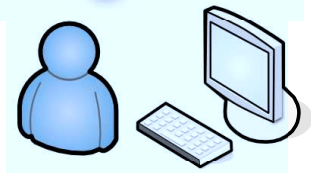
Remote Logging

Don't Panic





rsyslog Server



Systemadministrator

Remote Logging

Ziele

- Alle Informationen an einem zentralen System
- Archivierung ist zentralisiert
- Alarmierung
- Monitoring

Inhalt

rsyslog
- Überblick
- Vorteile
- Installation
- Konfiguration

rsyslog

Überblick

- Alternativer syslog-Daemon
- Standard bei Debian-basierten Distributionen

```
2011-06-13T10:14:50 bayamo rsyslogd: -- MARK --
2011-06-13T10:14:55 bayamo sshd[11015]: Accepted publickey for tm from 172.22.175.51 port 49425
2011-06-13T10:14:55 bayamo sshd[11015]: pam_unix(sshd:session): session opened for user tm uid=0
2011-06-13T10:14:56 bayamo sudo:       tm : TTY=pts/0 ; PWD=/home/tm ; USER=root ; COMMAND=/bin/su
2011-06-13T10:14:56 bayamo su[11083]: Successful su for root by root
2011-06-13T10:14:56 bayamo su[11083]: + /dev/pts/0 root:root
2011-06-13T10:14:56 bayamo su[11083]: pam_unix(su:session): session opened for user root by tm
```

rsyslog

Vorteile

- Bessere Sicherheitskontrolle
- Mehr Möglichkeiten für die Filterung
- Einfaches remote logging
- Protokollieren in die Datenbank

rsyslog

Installation

Paketmanager des Systems ist zu empfehlen

Debian, Ubuntu

```
apt-get install rsyslog
```

rsyslog

Konfigurationsdateien

Dateien und Verzeichnisse

`/etc/rsyslog.conf`
`/etc/rsyslog.d/*.conf`

Sortierung erfolgt durch Nummerierung:

- `/etc/rsyslog.d/00-AllowedHosts.conf`
- `/etc/rsyslog.d/10-RemoteLinuxServers.conf`
- `/etc/rsyslog.d/99-Default.conf`

rsyslog (server)

Remote Logging aktivieren

In `/etc/rsyslog.conf`, folgende Zeile einfügen:

```
$ModLoad imudp
$UDPServerRun 514
```

rsyslog (Server)

Remote Logging aktivieren

Zugriffssteuerung in
`/etc/rsyslog.d/00-AllowRemoteLogging.conf`

```
# Ein Host
$AllowedSender UDP, 192.168.56.100
# Alle Hosts aus einem Subnetz
$AllowedSender UDP, 192.168.56.0/24
# Jeder von kernel.org
$AllowedSender UDP, *.kernel.org
```

rsyslog (Linux Client)

Remote Logging aktivieren

Eintrag in `/etc/rsyslog.d/00-RemoteLogging.conf`

```
*.* @192.168.56.1
```

Viele syslog-Daemons werden unterstützt

Inhalt

tenshi
- Überblick
- Vorteile
- Installation
- Konfiguration

tenshi

Überblick

Tenshi ...

- ist ein Log Analyse Tool
- informiert
- wird als Dienst ausgeführt

tenshi

Vorteile

- Einfach
- Schnelle Installation und Konfiguration
- Benutzerdefinierte Suchausdrücke
- Ziel und Zeit der Ausgabe ist flexibel
- E-Mail Benachrichtigung möglich

tenshi

Installation

Eine Installation ist mit dem Paketmanager möglich.

Debian, Ubuntu

```
apt-get install tenshi
```

tenshi

Konfigurationsdateien

Grundeinstellungen

```
/etc/tenshi/tenshi.conf
```

Ordner für Regeln

```
/etc/tenshi/includes-active
/etc/tenshi/includes-available
```

tenshi

Logs / Mailserver

Welche Dateien sollen überwacht werden?

```
set logfile /var/log/auth.log
set logfile /var/log/remote-logs/webserver1.log
```

Über welchen Mailserver werden E-Mails versendet?

```
set mailserver localhost
```

tenshi

Message - Queues

Message-Queues ...

- sind Verteiler
- können verschiedene Empfänger haben
- haben einen flexiblen Intervall

Syntax

```
set queue <queue_name> <mail_from> <mail_to><interval>

set queue foo SrcMail DstMail [now] Server crushed !!!
set queue bar SrcMail2 DstMail2 [0 9 -17/2 * * *] Important !
```

tenshi

Gruppen

Gruppen ...

- beinhalten Regeln
- verkürzen die Suchdauer
- werden in den Ordnern abgelegt
  `/etc/tenshi/includes-active`
  `/etc/tenshi/includes-available`
- Beispielgruppen sind vorhanden (loginsusudo, ssh, ...)

tenshi

Ein Beispiel

- Auszug aus der Datei `auth.log`

```
Jun 1 17:19 loki su[1768]: Successful su for root by jowhite
Jun 1 17:19 loki su[1768]: + /dev/pts/1 jowhite:root
Jun 1 17:19 loki su[1768]: pam_unix(su:session): session opened for user root by jowhite(uid=1000)
Jun 1 17:19 loki su[1768]: pam_unix(su:session): session closed for user root
```

- Definition der Gruppe

```
group ^su\(pam_unix\):
su      ^su: pam_unix\(su:session\): session opened for user root(?: by \(uid=.+\))?
su      ^su: pam_unix\(su:session\): session closed for user root
su      ^su: Successful su for .+ by .+
group_end
```

Inhalt

phpLogCon
- Überblick
- Installation
- Webinterface
- Alternativen

phpLogCon

Überblick

- php-Webinterface mit MySql-Datenbank
- tabellarische Darstellung
- personalsierbare Ansichten und Filterungen
- Diagrammauswertung für besseren Überblick

phpLogCon

Installation

Die Installation ist so nur unter Ubuntu möglich

Debian, Ubuntu

```
Lamp Server
apt-get install rsyslog-mysql
apt-get install rsyslog-relp
```

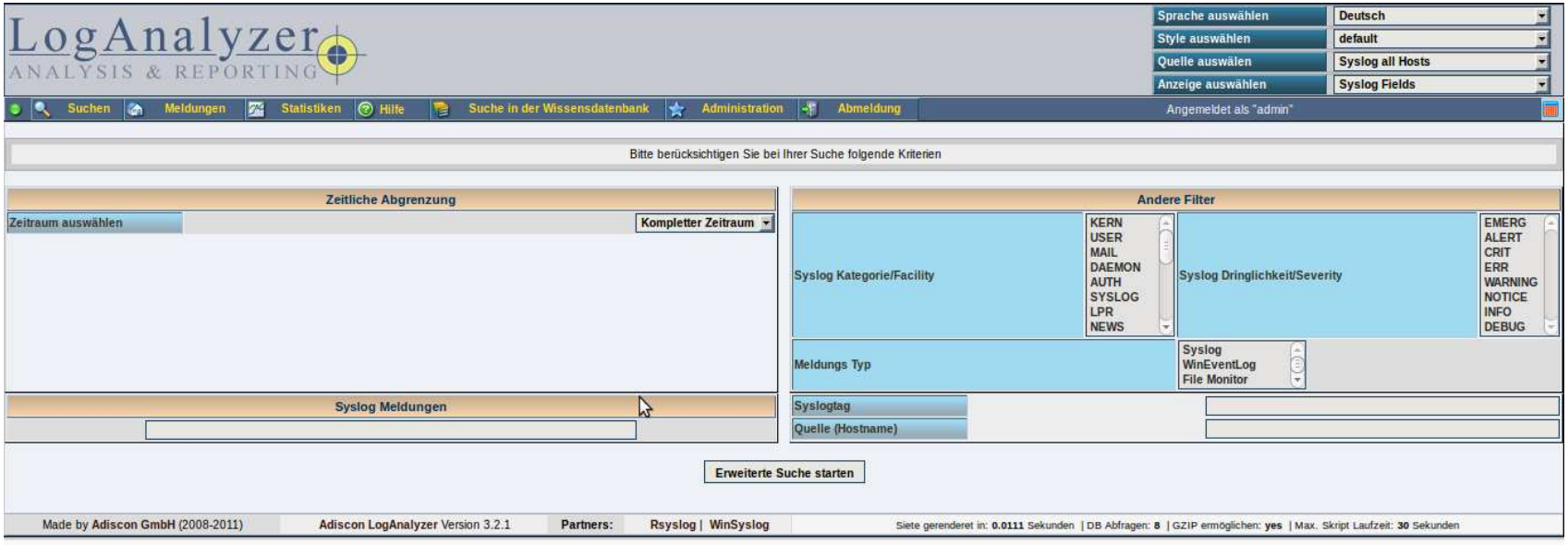
phpLogCon

Webinterface

- Suche
- Meldungen
- Statistiken
- Administration

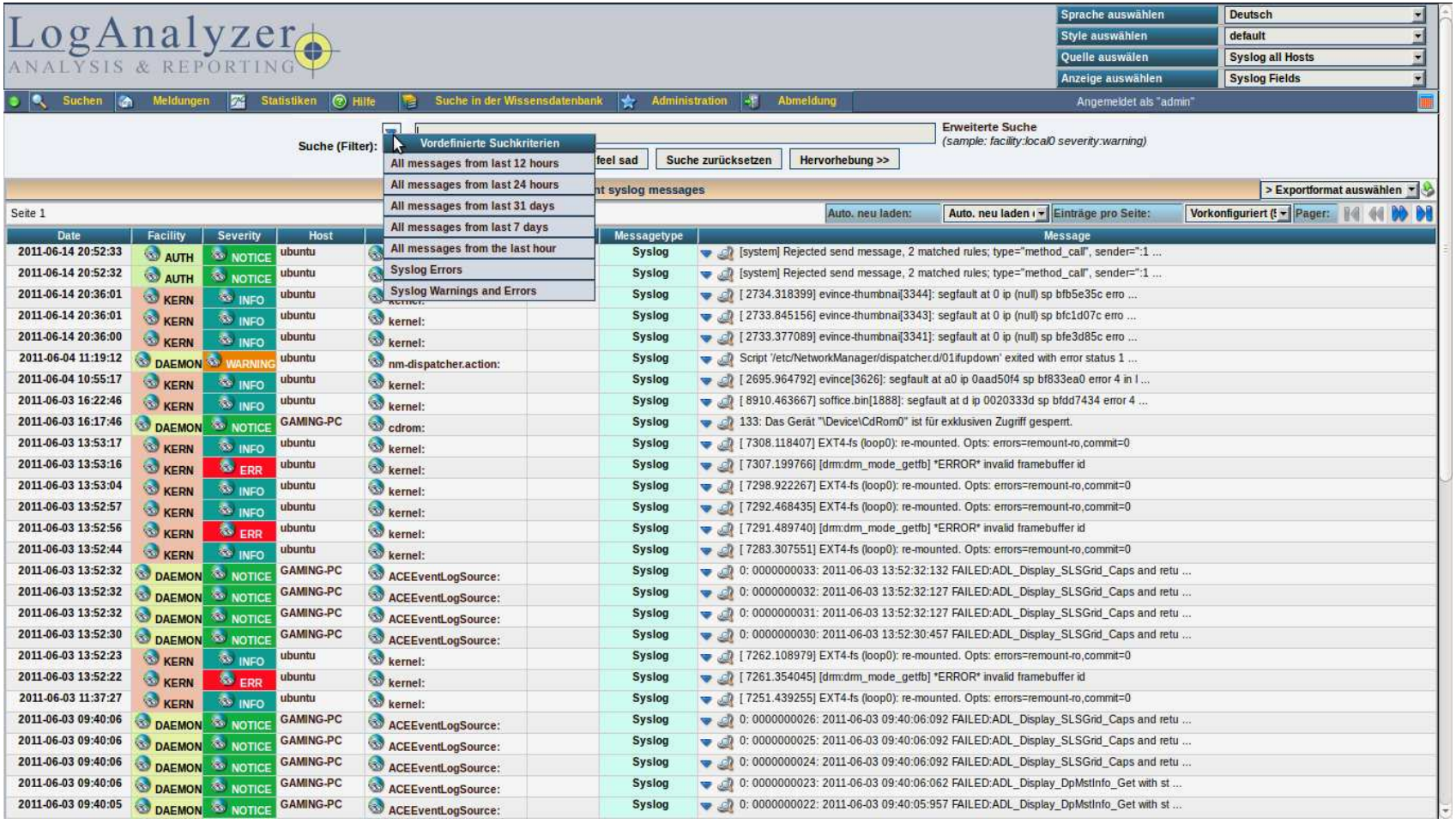
phpLogCon - Webinterface

Suche



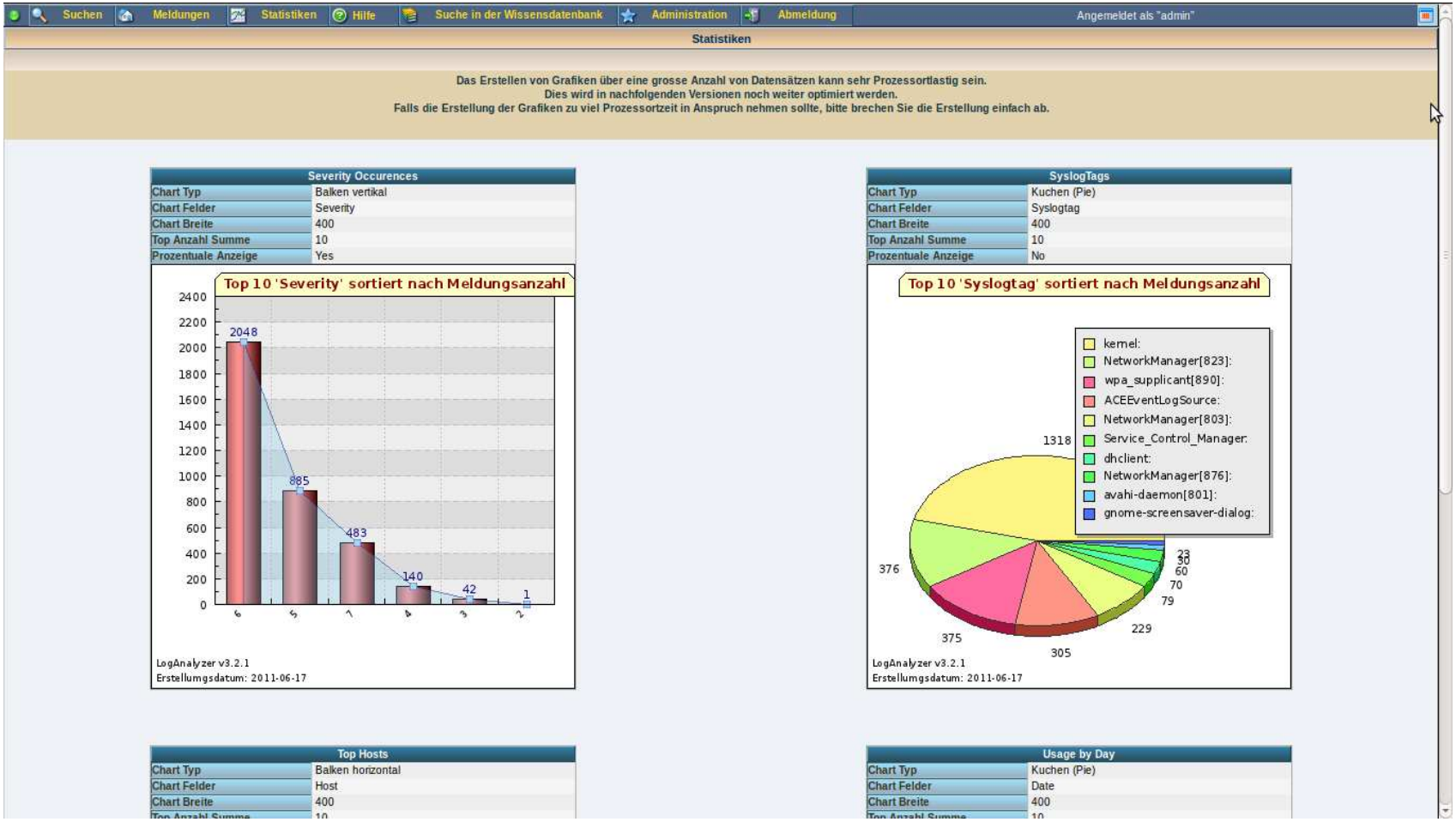
phpLogCon - Webinterface

Meldungen



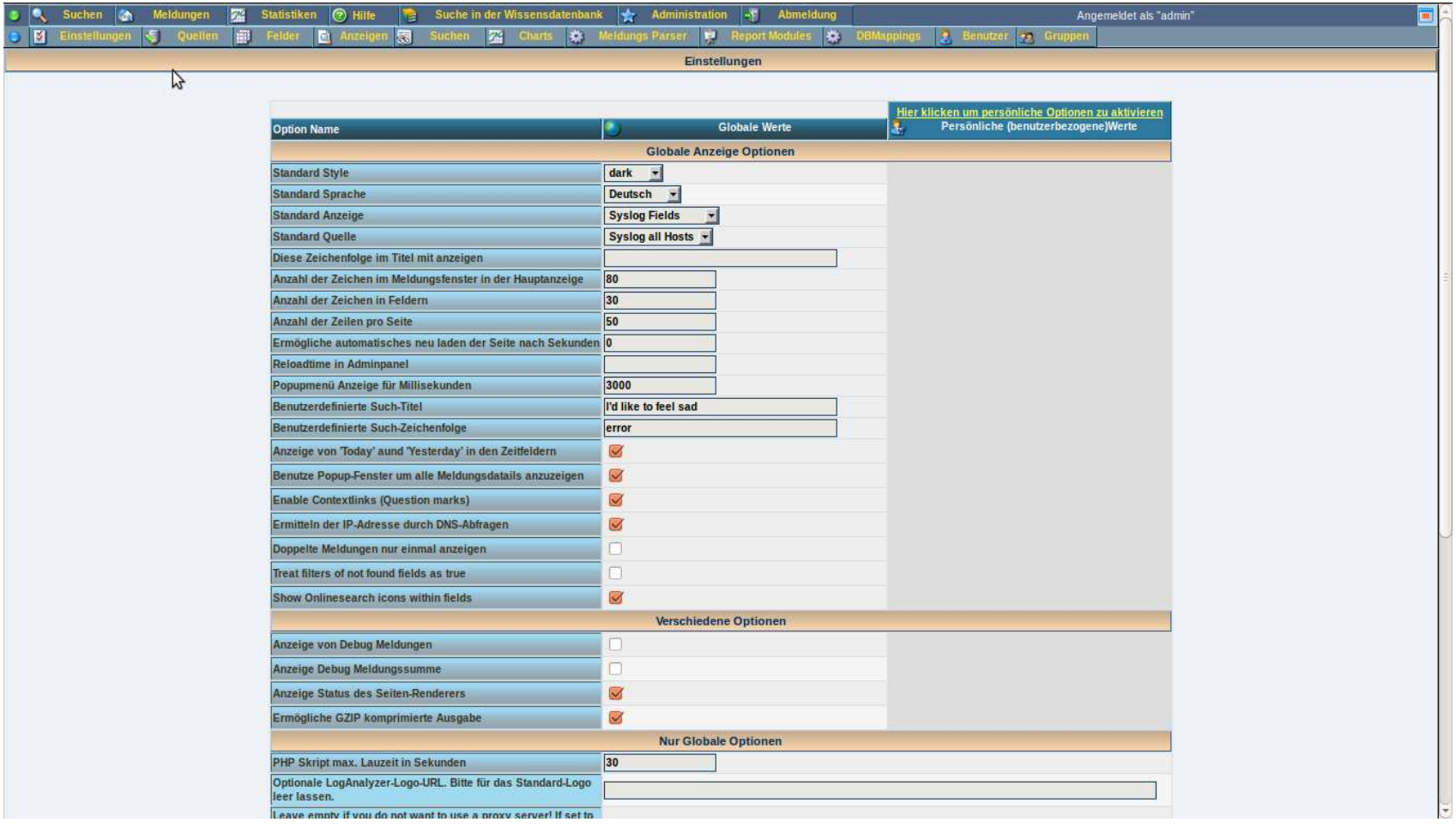
phpLogCon - Webinterface

Statistiken



phpLogCon - Webinterface

Administration



phpLogCon

Alternative: Logzilla

- Vollinstallation inkl. Betriebssystem
- Mehr Möglichkeiten der Analyse
- Zusätzliche Funktionen integriert
- Shareware, direkter Support möglich

Inhalt

Diskussion

Diskussion

Fragen, Anregungen, Wünsche

- Workshop am nächsten Termin der Linux User Group Weingarten
- Alle Unterlagen unter `https://github.com/drscream/rsyslog-workshop`

Danke an Paul Nijjar für seine Präsentation:

Remote Logging with Rsyslog - How I Learned to Start Worrying and Love the Panopticon