

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

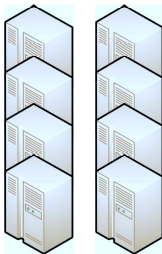
Panic

Don't Panic

Ziele

Remote Logging

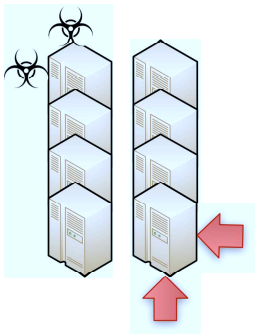
Problem



Systemadministrator

Remote Logging

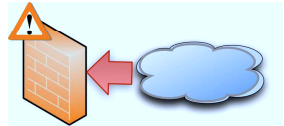
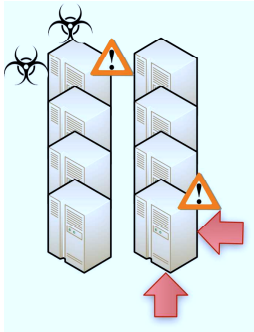
Panic



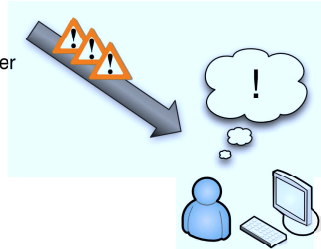
Systemadministrator

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 crashed !!!
```

```
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
- personalisierbare 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



Sprache auswählen
 Style auswählen
 Quelle auswählen
 Anzeige auswählen

Deutsch
 default
 Syslog all Hosts
 Syslog Fields

Suchen Meldungen Statistiken Hilfe Suche in der Wissensdatenbank Administration Abmeldung

Angemeldet als "admin"

Bitte berücksichtigen Sie bei Ihrer Suche folgende Kriterien

Zeitliche Abgrenzung
 Zeitraum auswählen Kompletter Zeitraum

Syslog Kategorie/Facility
 KERN
USER
MAIL
DAEMON
AUTH
SYSLOG
LPR
NEWS

Syslog Dringlichkeit/Severity
 EMERG
ALERT
CRIT
ERR
WARNING
NOTICE
INFO
DEBUG

Meldungs Typ
 Syslog
WinEventLog
File Monitor

Syslogging
 Quelle (Hostname)

Erweiterte Suche starten

Made by Adiscon GmbH (2008-2011)
 Adiscon LogAnalyzer Version 3.2.1
 Partners: Rsyslog | WinSyslog
 Seite generiert in: 0.6111 Sekunden | DB Abfragen: 8 | GZIP-erweitern: yes | Max. Skript Laufzeit: 30 Sekunden

phpLogCon - Webinterface

Meldungen

LogAnalyzer
ANALYSIS & REPORTING

Sprache auswählen: Deutsch
 Style auswählen: default
 Quelle auswählen: Syslog all Hosts
 Anzeige auswählen: Syslog Fields

Angemeldet als "admi"

Suche (Filter): Vordefinierte Suchkriterien
 Erweiterte Suche (sample: facility:local0 severity:warning)

Suche in der Wersmedatenbank Administration Abmeldung

Suche (Filter):

Seite 1

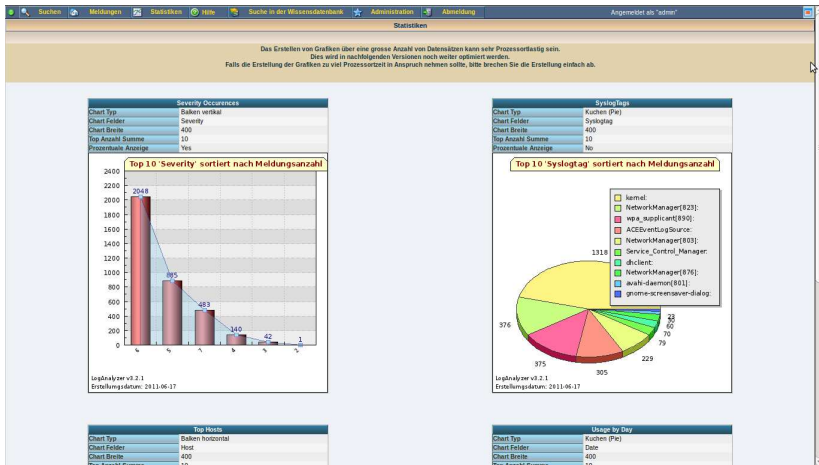
Date	Facility	Severity	Host	Message
2011-06-14 20:52:33	AUTH	NOTICE	ubuntu	Syslog Errors
2011-06-14 20:52:32	AUTH	NOTICE	ubuntu	Syslog Warnings and Errors
2011-06-14 20:36:01	KERN	INFO	ubuntu	kernel: Syslog
2011-06-14 20:36:01	KERN	INFO	ubuntu	kernel: Syslog
2011-06-14 20:36:00	KERN	INFO	ubuntu	kernel: Syslog
2011-06-04 11:19:12	DAEMON	WARNING	ubuntu	rm-dspatcher.action:
2011-06-04 10:55:17	KERN	INFO	ubuntu	kernel: Syslog
2011-06-16 12:22:46	KERN	INFO	ubuntu	kernel: Syslog
2011-06-03 16:17:46	DAEMON	NOTICE	GAMING-PC	cdrom: Syslog
2011-06-03 15:53:17	KERN	INFO	ubuntu	kernel: Syslog
2011-06-03 15:53:16	KERN	ERR	ubuntu	kernel: Syslog
2011-06-03 15:53:04	KERN	INFO	ubuntu	kernel: Syslog
2011-06-03 15:52:57	KERN	INFO	ubuntu	kernel: Syslog
2011-06-03 15:52:56	KERN	ERR	ubuntu	kernel: Syslog
2011-06-03 15:52:54	KERN	INFO	ubuntu	kernel: Syslog
2011-06-03 15:52:32	DAEMON	NOTICE	GAMING-PC	ACEEventLogSource: Syslog
2011-06-03 15:52:32	DAEMON	NOTICE	GAMING-PC	ACEEventLogSource: Syslog
2011-06-03 15:52:32	DAEMON	NOTICE	GAMING-PC	ACEEventLogSource: Syslog
2011-06-03 15:52:32	DAEMON	NOTICE	GAMING-PC	ACEEventLogSource: Syslog
2011-06-03 15:52:23	KERN	INFO	ubuntu	kernel: Syslog
2011-06-03 15:52:22	KERN	ERR	ubuntu	kernel: Syslog
2011-06-03 11:37:27	KERN	INFO	ubuntu	kernel: Syslog
2011-06-03 09:40:06	DAEMON	NOTICE	GAMING-PC	ACEEventLogSource: Syslog
2011-06-03 09:40:06	DAEMON	NOTICE	GAMING-PC	ACEEventLogSource: Syslog
2011-06-03 09:40:06	DAEMON	NOTICE	GAMING-PC	ACEEventLogSource: Syslog
2011-06-03 09:40:06	DAEMON	NOTICE	GAMING-PC	ACEEventLogSource: Syslog
2011-06-03 09:40:05	DAEMON	NOTICE	GAMING-PC	ACEEventLogSource: Syslog

Message
 [system] Rejected send message, 2 matched rules: type="method_call", sender="1 ...
 [system] Rejected send message, 2 matched rules: type="method_call", sender="1 ...
 [2734.318399] evince-dumbina[334]: segfault at 0 ip (null) sp bfb5c35c em ...
 [2733.845154] evince-dumbina[334]: segfault at 0 ip (null) sp bfb5c35c em ...
 [2733.377089] evince-dumbina[334]: segfault at 0 ip (null) sp bfb5c35c em ...
 Script '/etc/network/ManagerDispatcher.d/01updown' exited with error status 1 ...
 [2695.964792] evince[3626]: segfault at a0 ip 0aad50f4 sp bfb3bea0 error 4 in 1 ...
 [8910.463667] soffice-bin[1888]: segfault at d ip 0020333d sp bfb47434 error 4 ...
 133: Das Gerät "DeviceCDRom0" ist für exklusiven Zugriff gesperrt.
 [7308.118407] EXT4-fs (loop0): re-mounted. Opts: enosr-mount-to-commit=0
 [7307.199766] [jdm:dm_mode_get] "ERROR" invalid handlefor id
 [7298.922267] EXT4-fs (loop0): re-mounted. Opts: enosr-mount-to-commit=0
 [7292.468435] EXT4-fs (loop0): re-mounted. Opts: enosr-mount-to-commit=0
 [7291.489740] [jdm:dm_mode_get] "ERROR" invalid handlefor id
 [7283.307551] EXT4-fs (loop0): re-mounted. Opts: enosr-mount-to-commit=0
 [0:000000033: 2011-06-03 13:52:32:132 FAILED ADL_Display_SLSignd_Caps and retu ...
 [0:000000032: 2011-06-03 13:52:32:127 FAILED ADL_Display_SLSignd_Caps and retu ...
 [0:000000031: 2011-06-03 13:52:32:127 FAILED ADL_Display_SLSignd_Caps and retu ...
 [0:000000030: 2011-06-03 13:52:30:457 FAILED ADL_Display_SLSignd_Caps and retu ...
 [7262.108979] EXT4-fs (loop0): re-mounted. Opts: enosr-mount-to-commit=0
 [7261.354045] [jdm:dm_mode_get] "ERROR" invalid handlefor id
 [7251.439255] EXT4-fs (loop0): re-mounted. Opts: enosr-mount-to-commit=0
 [0:000000029: 2011-06-03 09:40:06:092 FAILED ADL_Display_SLSignd_Caps and retu ...
 [0:000000028: 2011-06-03 09:40:06:092 FAILED ADL_Display_SLSignd_Caps and retu ...
 [0:000000024: 2011-06-03 09:40:06:092 FAILED ADL_Display_SLSignd_Caps and retu ...
 [0:000000023: 2011-06-03 09:40:06:092 FAILED ADL_Display_SLSignd_Caps and retu ...
 [0:000000022: 2011-06-03 09:40:05:957 FAILED ADL_Display_SLSignd_Caps and retu ...
 [0:000000021: 2011-06-03 09:40:05:957 FAILED ADL_Display_SLSignd_Caps and retu ...



phpLogCon - Webinterface

Statistiken



phpLogCon - Webinterface

Administration

Suchen Meldungen Statistiken Hilfe Suche in der Wissensdatenbank Administration Anmeldung

Einstellungen Quellen Filter Anzeigen Suchen Charts Meldungs-Parser Report-Modul Konfigurations Benutzer Gruppen

Angemeldet als "admin"

Einstellungen

Hier klicken um persönliche Optionen zu aktivieren
Persönliche (Benutzerbezogene) Werte

Option Name	Globale Werte
Globale Anzeige Optionen	
Standard Style	dark
Standard Sprache	Deutsch
Standard Anzeige	Syslog Fields
Standard Quelle	Syslog all Hosts
Diese Zeichenfolge im Titel mit anzeigen	
Anzahl der Zeichen im Meldungsfenster in der Hauptanzeige	80
Anzahl der Zeichen in Feldern	30
Anzahl der Zeilen pro Seite	50
Ermögliche automatisches neu laden der Seite nach Sekunden	0
Reloadtime in Adminpanel	
Pop-upmenü Anzeige für Millisekunden	3000
Benutzerdefinierte Such-Titel	I'd like to feel sad
Benutzerdefinierte Such-Zeichenfolge	error
Anzeige von 'Today' ausnd 'Yesterday' in den Zeitfeldern	☒
Benutze Pop-up-Fenster um alle Meldungsdetails anzuzeigen	☒
Enable Contextlinks (Question marks)	☒
Ermitteln der IP-Adresse durch DNS-Abfragen	☒
Doppelte Meldungen nur einmal anzeigen	☐
Treat filters of not found fields as true	☐
Show Onlinesearch icons within fields	☒
Verschiedene Optionen	
Anzeige von Debug Meldungen	☐
Anzeige Debug Meldungssumme	☐
Anzeige Status des Seiten-Renderers	☒
Ermögliche GDP komprimierte Ausgabe	☒
Nur Globale Optionen	
PHP Skript max. Laufzeit in Sekunden	30
Optionale LogAnalyzer-Logo-URL. Bitte für das Standard-Logo leer lassen.	
Leave empty if you do not want to use a mirror server! If not to	



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