Aufbau einer zentralen Log-Infrastruktur mit syslog-ng

Jens Link jenslink@quux.de

German Unix User Group guug
Frühjahrs Fach2005 Gespräch

Übersicht

- Motivation / Aufbau des Netzes
- syslog Protokoll
- syslog/syslog-ng
- Konfiguration der Server
- Konfiguration der Clients
- Verwaltung und Auswertung
- Todo

Motivation

- Zusammenfassung mehrere kleiner Insellösungen zu einem Netz
- Neue Server
- Neue und mehr Netzwerkhardware

=> Mehr Arbeit für die Admins

=> Bessere Möglichkeiten zur Fehlersuche

German Unix User Group
guug
Frühjahrs Fach2005 Gespräch

Aufbau des Netzwerks

- Windows Server (AD, File u. Print, Lotus Domino, SUS, Antivirus, ...)
- Linux Server (Web, DNS, OTRS, Radius, ...)
- Cisco Router und Switche
- diverse andere Hard-/Software

German Unix User Group guug Frühjahrs Fach2005 Gespräch

Syslog Protokoll

- Verwendet UDP (Port 514)
- Jede Nachricht besteht aus einer Zeile Text, diese setzt sich zusammen aus:
  - **Facility:** Von welcher Komponente / Applikation kommt die Meldung
  - **Level** (severity): Wie wichtig ist die Meldung?
  - **Text**

Syslog Protokoll: Syslog Facilities (1)

kern	kernel
user	application or user processes (this is the default if the application sending a message does not specify the facility)
mail/ news/ UUCP/ cron	electronic mail/ NNTP/ UUCP/ cron subsystems
daemon	system daemons
auth	authentication and authorization related commands
lpr	line printer spooling subsystem
mark	inserts timestamp into log data at regular intervals

Quelle: http://www.precision-guesswork.com/sage-guide/syslog-overview.html

German Unix User Group guug

Frühjahrs Fach2005 Gespräch

Syslog Protokoll
Syslog Facilities (2)

local0- local7	8 facilities for customized auditing
syslog itself	internal messages generated by syslog
authpriv	non- system authorization messages
* - -	on most versions of UNIX, refers to all facilities except mark

Quelle: http:// www.precision- guesswork.com/ sage- guide/ syslog- overview.html

German Unix User Group
guug
Frühjahrs Fach2005 Gespräch

Syslog Protokoll
Syslog Levels

emerg	system is or will be unusable if situation is not resolved
alert	immediate action required
crit	critical situations
warning	recoverable errors
notice	unusual situation that merits investigation; a significant event that is typically part of normal day-to-day operation
info	informational messages
debug	verbose data for debugging

Quelle: http://www.precision-guesswork.com/sage-guide/syslog-overview.html

German Unix User Group guug Frühjahrs Fach2005 Gespräch

Syslog: syslog.conf

Welche Nachricht kommt in welches Logfile?

```
auth,authpriv.*                 /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
#cron.*                         /var/log/cron.log
daemon.*                        -/var/log/daemon.log
kern.*                          -/var/log/kern.log
news.crit                       /var/log/news/news.crit
news.err                        /var/log/news/news.err
```

German Unix User Group guug Frühjahrs Fach2005 Gespräch

syslog-ng

- Besser Möglichkeiten zur Filterung
- Verschlüsselung über stunnel/ssh möglich
- Kann auch Nachrichten auch über TCP senden/empfangen

German Unix User Group guug Frühjahrs Fach2005 Gespräch

syslog-ng.conf: Source

Wo kommen die Daten her?

```
source src {
        file("/proc/kmsg") log_prefix("kernel: ");
        unix-stream("/dev/log");
        internal();
        udp();
        tcp();
};
```

German Unix User Group guug Frühjahrs Fach2005 Gespräch

syslog-ng.conf: Destination

In welchen Dateien sollen die Daten später liegen?

```
destination authlog { file("/var/log/auth.log"); };
destination syslog { file("/var/log/syslog"); };
destination cron { file("/var/log/cron.log"); };
destination daemon { file("/var/log/daemon.log"); };
destination kern { file("/var/log/kern.log"); };
destination lpr { file("/var/log/lpr.log"); };
destination user { file("/var/log/user.log"); };

destination console_all { file("/dev/tty8"); };
```

German Unix User Group guug Frühjahrs Fach2005 Gespräch

syslog-ng.conf: Filter

Wie sollen die die Meldungen verteilt werden:

```
filter f_authpriv { facility(auth, authpriv); };
filter f_syslog { not facility(auth, authpriv) and not facility
  (mail); };

filter f_ssh_login_attempt {
        program("sshd.*")
        and match("failure”)
};
```

syslog-ng.conf: Log

Wo sollen die Daten hin?

```
log { source(src); filter(f_authpriv); destination(authlog); };
log { source(src); filter(f_syslog); destination(syslog); };
log { source(src); filter(f_cron); destination(cron); };
log { source(src); filter(f_daemon); destination(daemon); };
```

German Unix User Group guug
Frühjahrs Fach2005 Gespräch

Client Konfiguration: Linux

```
destination loghost {
        tcp("192.168.1.100" port(514));
};


log {
        source(src);
        destination(loghost);
};
```

German Unix User Group guug

Frühjahrs Fach2005 Gespräch

Client Konfiguration: Cisco IOS

switch#(config)logging 192.168.1.100

switch#(config)logging 192.168.10.100

Evtl. Anppassen des Log-Levels durch:

switch#(config)logging trap level

German Unix User Group guug

Frühjahrs Fach2005 Gespräch

Client Konfiguration: Windows

- Windows unterstützt keine Möglichkeit direkt auf einen syslog-Server zu schreiben
- Es gibt aber diverse Zusatztools um das Ziel zu erreichen

German Unix User Group
guug
Frühjahrs Fach2005 Gespräch

Client Konfiguration: Windows, ntsyslog

1. Versuch: ntsyslog
(http://ntsyslog.sourceforge.net/)

- Sehr klein
- Nur wenige Features
- Funktionierte allerdings nicht, da einige Berechtigungen auf die Windows-Registry fehlten

German Unix User Group guug
Frühjahrs Fach2005 Gespräch

Client Konfiguration: Windows, SNARE(1)

2. Versuch: Snare

- Ebenfalls recht klein
- Mehr Funktionen
- Vorsicht: Snare kann bei der Installation die Logging Einstellungen under Windows ändern

German Unix User Group guug Frühjahrs Fach2005 Gespräch

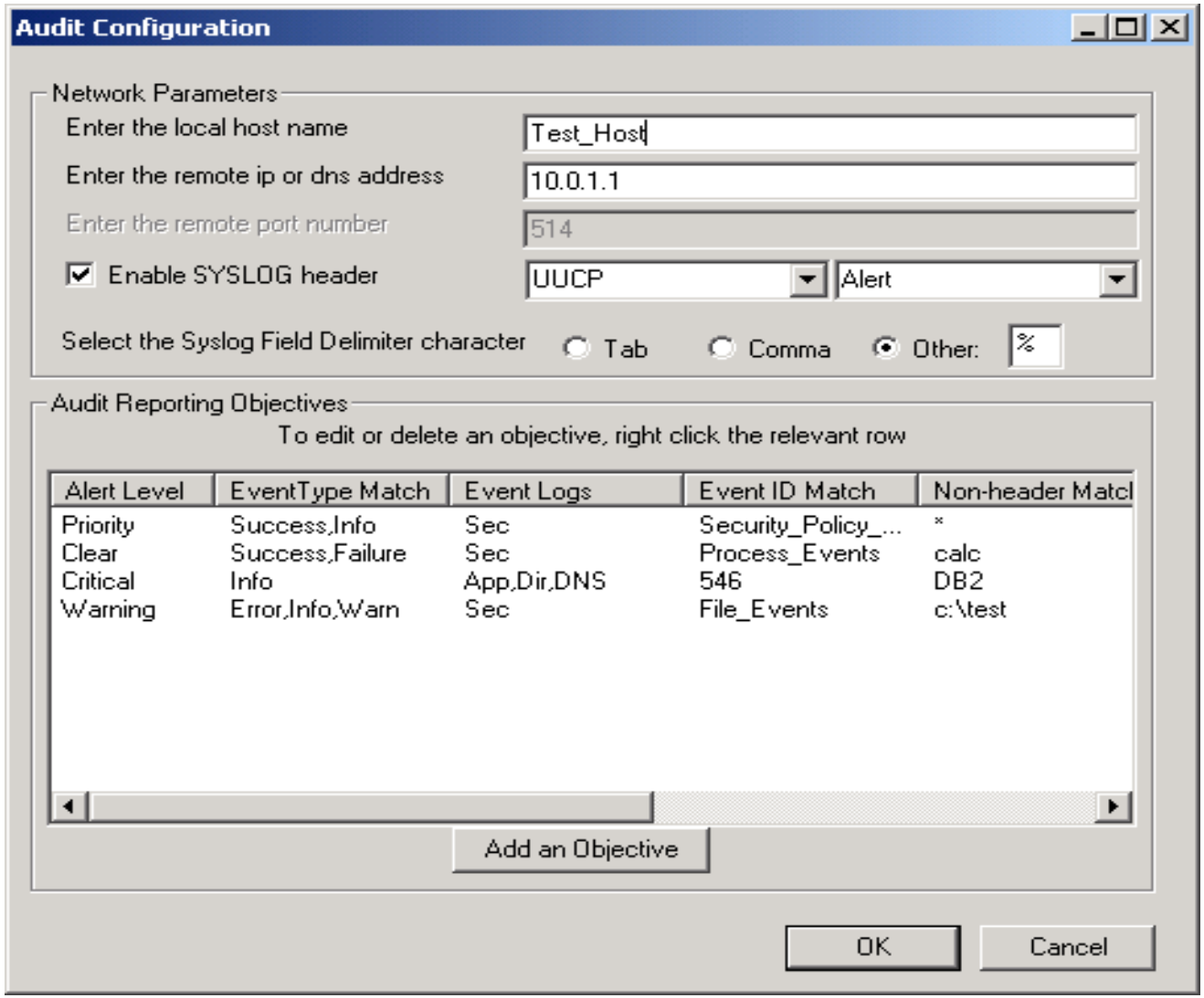
Client Konfiguration: Windows, SNARE(2)

- Installation über GUI
- Vorsicht bei der Abfrage, ob SNARE die Logging einstellungen unter Windows ändern soll

German Unix User Group guug

Frühjahrs Fach2005 Gespräch

Client Konfiguration: Windows, SNARE(3)



http://www.intersectalliance.com/projects/SnareWindows/index.html#ScreenShots

German Unix User Group guug

Frühjahrs Fach2005 Gespräch

Client Konfiguration: Andere Clients

Diverse andere Komponenten/Applikationen, wie z.B. Printserver, bieten die Möglichkeit Daten auf einem Syslog-Server zu speichern. Diese werden u.U. später in das zentrale Logging intergriert.

Andere Komponenten/Applicationen bieten diese Möglichkeit leider nicht, Beispiele hierfür:

- Lotus Domino
- MS SUS
- ArcServ

German Unix User Group guug
Frühjahrs Fach2005 Gespräch

Verwaltung und Auswertung (1)

- Die Daten werden in einzelnen Dateien gespeichert
- Auswertung über Standardtools bzw. eigene Scripte
- Logs des Apache werden noch nicht über syslog verwaltet

Verwaltung und Auswertung (1)

Verwaltung der Logfiles durch logrotate:

```
# rotate log files weekly
weekly
# keep 4 weeks worth of backlogs
rotate 4
# create new (empty) log files after rotating old ones
create
# uncomment this if you want your log files
compressed

include /etc/logrotate.d
```

German Unix User Group guug
Frühjahrs Fach2005 Gespräch

Verwaltung und Auswertung (2)

```
/var/log/apache/*.log {
    weekly
    missingok
    rotate 5
    compress
    delaycompress
    notifempty
    create 640 root adm
    sharedscripts
    postrotate
      if [ -f /var/run/apache.pid ]; then \
        if [ -x /usr/sbin/invoke-rc.d ]; then \
         invoke-rc.d apache reload > /dev/null; \
        else \
           /etc/init.d/apache reload > /dev/null; \
        fi; \
      fi;
    endscript
}
```

German Unix User Group
guug
Frühjahrs Fach2005 Gespräch

ToDo

- Auswertung und Alarmierung verfeinern
- Evtl. Datenspeicherung in einer Datenbank

German Unix User Group guug
Frühjahrs Fach2005 Gespräch

Resourcen

Snare:
http://www.intersectalliance.com/projects/index.html

Syslog-ng:http://www.balabit.com/products/syslog_ng

http://www.loganalysis.org/

ftp://ftp.rfc-editor.org/in-notes/rfc3164.txt

http://www.sans.org/rr/whitepapers/logging

http://www.campin.net/syslog-ng/faq.html

Michael D. Bauer
Building Secure Serves with Linux
O'Reilly

German Unix User Group

guug

Frühjahrs Fach2005 Gespräch

Fragen?