Installation logsurfer auf MAC

Inhaltsverzeichnis

1 Vorbemerkungen

Die hier beschriebene Installation war VOR OS X 10.9.4 erstellt worden.[1]

Änderungen, Anpassungen, die für OS X 10.9.4 notwendig wurden, sind entsprechend vermerkt. (Anmerkung „Mavericks“)

die alte Installation funktioniert auch unter Yosemite (derzeit 10.10.5) weiter. Lediglich der Start der Überwachung beim Systemstart ist bei der Installation entfernt worden. (Prüfung und Start der Software beim User-Login klappt nach wie vor..)

1 2014-07-24 habe ich „Lion“ auf „Mavericks“ (OS X 10.9.4) upgraded.

2 Voraussetzungen

2.1 Voraussetzungen für lauffähigen Logsurfer

Zugriff auf Rechner

- als Admin

    Installation der Software

- als Normaler User („Logsurfer Operator User“)

    Betrieb der Software

        KEINE Admin-Rechte für logsurfer-Prozess notwendig

        KEINE Admin-Rechte erwünscht, um Manipulationen zu verhindern

2.2 Voraussetzungen für eMail-Benachrichtigung

EMail (Command-Line-Modus) muss funktionieren und aktiv sein.

Test (senden):

    > mail -s test-subject <userid>

    >.

Test (empfangene Mails anzeigen)

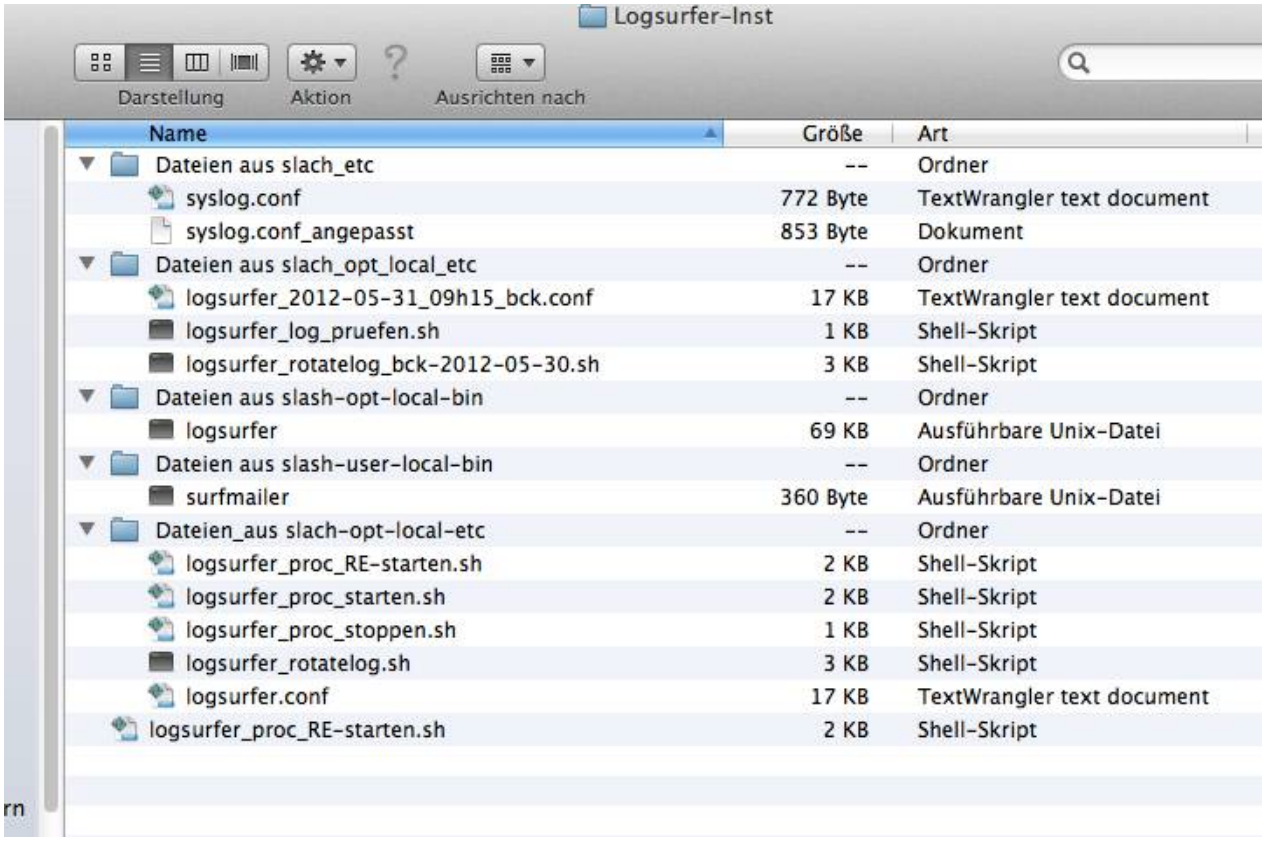
    entweder

        > mail

    oder

        > mail | grep test-subject

2.3 Version auf „meinem“ MAC vor-kompilieren und zum Zielrechner übertragen



Name	Größe	Art
Dateien aus slach_etc	--	Ordner
syslog.conf	772 Byte	TextWrangler text document
syslog.conf_angepasst	853 Byte	Dokument
Dateien aus slach_opt_local_etc	--	Ordner
logsurfer_2012-05-31_09h15_bck.conf	17 KB	TextWrangler text document
logsurfer_log_pruefen.sh	1 KB	Shell-Skript
logsurfer_rotatelog_bck-2012-05-30.sh	3 KB	Shell-Skript
Dateien aus slash-opt-local-bin	--	Ordner
logsurfer	69 KB	Ausführbare Unix-Datei
Dateien aus slash-user-local-bin	--	Ordner
surfmailer	360 Byte	Ausführbare Unix-Datei
Dateien_aus slach-opt-local-etc	--	Ordner
logsurfer_proc_RE-starten.sh	2 KB	Shell-Skript
logsurfer_proc_starten.sh	2 KB	Shell-Skript
logsurfer_proc_stoppen.sh	1 KB	Shell-Skript
logsurfer_rotatelog.sh	3 KB	Shell-Skript
logsurfer.conf	17 KB	TextWrangler text document
logsurfer_proc_RE-starten.sh	2 KB	Shell-Skript

2.3.1 Software und Konfigurationen auf Zielrechner verteilen

Als Admin einloggen:

„Umleitung“ für Systemlogs → Logsurfer.log konfigurieren

> sudo cp /etc/syslog.conf /Users/juergen/logsurfer/Logsurfer-Inst/\ Dateien\ aus\ slach_etc/syslog.conf_bck

(Unterschied: neuer Eintrag am Ende: „alles nach /var/log/logsurfer.log)

„Anmerkung Mavericks“

in älteren OS X wurde viele verschiedene Logfiles durch die syslog.conf erzeugt.

Unter 10.9.4 erscheint nur noch ein Logfile:

```
# Note that flat file logs are now configured in /etc/asl.conf

install.*                                                @127.0.0.1:32376
```

neues Logfile erzeugen, Umleitung aktivieren:

> sudo touch /var/log/logsurfer.log

> sudo cp ~/logsurfer/Logsurfer-Inst/\ Dateien\ aus\ slach_etc/syslog.conf_angepasst /etc/syslog.conf

> sudo launchctl unload /System/Library/LaunchDaemons/com.apple.syslogd.plist

> sudo launchctl load /System/Library/LaunchDaemons/com.apple.syslogd.plist

Anmerkung „Mavericks“

Schritt 2 habe ich durch „sudo vi..“ ersetzt und die entsprechende Zeilen am Ende eingebaut:

```
# 2014-07-25 wg. logsurfer:
# logsurfer Definition (2011-12-15, ca 10h30):
*.*                                                      /var/log/logsurfer.log
```

Die Schritte 3 und 4 waren erfolgreich, der Test im nächsten Kapitel (tail) klappte.

Trotz der Bemerkung (s.o. → asl.conf funktioniert das Logging nach logsurfer.log

„Umleitung“ für Systemlogs → Logsurfer.log testen

> tail /var/log/logsurfer.log

oder

> tail -f /var/log/logsurfer.log

„Umschalten“ des Systemlogs wenn Logfile „Size-Limit“ überschreitet

- **Skript /opt/local/etc/logsurfer_rotatelog.sh muss von „logsurfer-Operator“ mit Admin-Rechten benutzt werden könen, d.h es muss in der „sudoers-Liste“ aufgeführt sein:**

laeppy-wlan:~ jurgenblaser$ sudo grep logsurfer_rotatelog.sh /etc/sudoers

juergen ALL=(ALL) NOPASSWD: /opt/local/etc/logsurfer_rotatelog.sh

logsurfer ALL=(ALL) NOPASSWD: /opt/local/etc/logsurfer_rotatelog.sh

Anmerkung „Mavericks“

```
lappy:~ jurgenblaser$ sudo grep logsurfer_rotatelog.sh  /etc/sudoers
Password:
juergen ALL=(ALL) NOPASSWD: /opt/local/etc/logsurfer_rotatelog.sh
logsurfer ALL=(ALL) NOPASSWD: /opt/local/etc/logsurfer_rotatelog.sh
juergen ALL=(ALL) NOPASSWD: /Users/juergen/testls/logsurfer_rotatelog.sh
lappy:~ jurgenblaser$
```

- **ggf. Skript opt/local/etc/logsurfer_rotatelog.sh in der „sudoers-Liste“ eintragen**

  s. Muster in …. /\ Dateien\ aus\ slach_etc/sudoers

  sudo vi, copy, paste

Dateien verteilen (ggf. Folder neu erzeugen)

Vor-Bemerkung: Dateistruktur inzwischen geändert, [2]

> sudo cp ~/logsurfer/Logsurfer-Inst/\ Dateien\ aus\ slach_opt_local_etc/logsurfer_2012-05-31_09h15_bck.conf /opt/local/etc/logsurfer.conf

> sudo cp ~/logsurfer/Logsurfer-Inst/\ Dateien\ aus\ slach_opt_local_etc/logsurfer_rotatelog_bck-2012-05-30.sh /opt/local/etc/logsurfer_rotatelog.sh

> sudo cp ~/logsurfer/Logsurfer-Inst/\ Dateien\ aus\ slach_opt_local_etc/logsurfer_laeuft_test.sh /opt/local/etc/logsurfer_laeuft_test.sh

> sudo cp ~/logsurfer/Logsurfer-Inst/\ Dateien\ aus\ slash-opt-local-bin/logsurfer /opt/local/bin/

> sudo cp ~/logsurfer/Logsurfer-Inst/\ Dateien_aus\ slach-opt-local-etc/logsurfer_proc_RE-starten.sh /opt/local/etc/

> sudo cp ~/logsurfer/Logsurfer-Inst/\ Dateien_aus\ slach-opt-local-etc/logsurfer_proc_starten.sh /opt/local/etc/

> sudo cp ~/logsurfer/Logsurfer-Inst/\ Dateien_aus\ slach-opt-local-etc/logsurfer_rotatelog.sh /opt/local/etc/

> sudo cp ~/logsurfer/Logsurfer-Inst/\ Dateien_aus\ slach-opt-local-etc/logsurfer.conf /opt/local/etc/

> sudo cp ~/logsurfer/Logsurfer-Inst/\ Dateien\ aus\ slash-user-local-bin/surfmailer /usr/local/bin/

prüfen, ob die Dateien lesbar und ggf. ausführbar sind:

> ls -al /opt/local/etc/

total <xxx>

drwxr-xr-x 11 root admin 374 4 Apr 13:18 .

2 Dateien liegen unter /Users/juergen/Documents/computer/Sicherheit/Logsurfer/\$_Logsurfer-Installation-und-Konfiguration/Installation\ auf\ MAC\ \"von\ Hand\"_2012-05-30_VM-Lion/Logsurfer-Inst_Software+Konfig_Package/

```
drwxr-xr-x  11 root    admin    374  3 Apr 13:47 ..
-rw-r--r--@  1 root    admin  16954  3 Apr 15:57 logsurfer.conf
-rw-r--r--   1 juergen  admin      5  4 Apr 13:11 logsurfer.pid
-rwxr--r--   1 root    admin    325  4 Apr 13:18 logsurfer_laeuft_test.sh
-rwxr-xr-x@  1 root    admin   1245  3 Apr 15:49 logsurfer_log_pruefen.sh
-rwxr-xr-x@  1 root    admin    626  3 Apr 15:54 logsurfer_proc_RE-starten.sh
-rwxr-xr-x@  1 root    admin    761  3 Apr 15:54 logsurfer_proc_starten.sh
-rwxr-xr-x@  1 root    admin     77  3 Apr 15:54 logsurfer_proc_stoppen.sh
-rwxr-xr--@  1 root    admin   3131  3 Apr 15:54 logsurfer_rotatelog.sh
....
>
```

> ls -al /opt/local/bin/logsurfer

-rwxr-xr-x 1 root admin 68568 Jun 1 11:23 /opt/local/bin/logsurfer

PID-Datei …

> sudo touch /opt/local/etc/logsurfer.pid

> sudo chown <Logsurfer Operator User> /opt/local/etc/logsurfer.pid

logsurfer.conf an aktuelle Umgebung anpassen:

→ eMails an jeweiligen „Logsurfer Operator User“

(Achtung, funktioniert nur, wenn lokales eMail aktiv!)

→ sudo vi /opt/local/etc/logsurfer.conf

„/usr/local/bin/surfmailer -r juergen „ suchen und Ziel-User anpassen

als normalen User einloggen:

- logsurfer-Prozess starten und eingehende Mails prüfen:

  entweder (zum ersten Mal)

  > /opt/local/etc/logsurfer_proc_starten.sh

  oder (nach Umkonfiguration)

  > /opt/local/etc/logsurfer_proc_RE-starten.sh

  (Test starten:)

  $ /opt/local/etc/logsurfer_laeuft_test.sh

  (Ausgabe:)

  Logsurfer Prozess gefunden

  504 2713   1   0 1:11pm ttys001   0:16.75 /opt/local/bin/logsurfer -c /opt/local/etc/logsurfer.conf -r ^.{15,}

(.*) logsurfer-start 2013-04-04_13:11:33 -f -p /opt/local/etc/logsurfer.pid -s -t /var/log/logsurfer.log

> mail

Mail version 8.1 6/6/93. Type ? for help.

"/var/mail/<user>": 4 messages 4 new

>N 1 <user>@ichs-Mac.loc Fri Jun 1 11:42 13/533 "Logsurfer stopped at Jun 1 11:42:51 ichs-Mac"

N 2 <user>@ichs-Mac.loc Fri Jun 1 11:42 13/533 "Logsurfer stopped at Jun 1 11:42:51 ichs-Mac"

N 3 <user>@ichs-Mac.loc Fri Jun 1 11:42 13/538 "Logsurfer restarted at Jun 1 11:42:53 ichs-Mac"

N 4<user>Logsurfer stopped@ichs-Mac.loc Fri Jun 1 11:42 13/538 "Logsurfer restarted at Jun 1 11:42:53 ichs-Mac"

?

- „rotate-log“ (Haupt-Skript) in Crontab (non-priv user) eintragen

  # Logsurfer Logfile auf Groesse pruefen und ggf. "rotieren", 2011-12-15

  0 * * * * /opt/local/etc/logsurfer_log_pruefen.sh

- Sub-Skripte in „/etc/sudoers“ (am Datei-Ende) eintragen

  # rotate syslog file

  # 2011-12-15, JB

  juergen ALL=(ALL) NOPASSWD: /opt/local/etc/logsurfer_rotatelog.sh

  size-Limit sehr klein setzen und per Skript /opt/local/etc/logsurfer_rotatelog.sh prüfen (oder manuell) prüfen, ob „dieser User“ ein neues Log anlegen kann

2.4 Logsurfer automatisch starten

2.4.1 Logsurfer beim login eines bestimmten users starten

Systemeinstellungen → Benutzer und Gruppen → (betreffenden User wählen) → Anmedeobjekte → /opt/local/etc/logsurfer_proc_starten.sh auswählen

2.4.2 Logsurfer beim Systemboot starten

Notwendig:

/Library/LaunchDaemons/com.tools-and-pictures.logsurferboot.plist[3]

3 Hat nach Installation Yosemite gefehlt

/opt/local/etc/logsurfer.sh[4]

/opt/local/etc/logsurfer_boot.sh (in /etc/sudoers mit korrektem user eingetragen)

Beispiel einer „/etc/sudoers“ s. Unter S. 8 → 2.4.3 Prozesse mit „fremden“ Rechten starten:

siehe Skripte unter:

„/Users/juergen/Documents/computer/Sicherheit/Logsurfer/\$_Logsurfer-Installation-und-Konfiguration/“

→ „Installation\ auf\ MAC\ \"von\ Hand\"_2012-06-19\ Logsurfer\ bei\ boot\ starten“

siehe Anleitung unter: „/Users/juergen/Documents/computer/Sicherheit/Logsurfer/\$\$_\ Logsurfer_als_Produkt/99_Hilfsprogramme_Tests_etc/\ logsurfer\ Start\ bei\ boot\ Doku/su\ plus\ command_Ausführung.rtf“

2.4.3 Prozesse mit „fremden“ Rechten starten:

Ausschnitt aus /etc/sudoers:

```
#
# rotate syslog file (6x)
# 2011-12-15, JB
juergen ALL=(ALL) NOPASSWD: /opt/local/etc/logsurfer_rotatelog.sh
logsurfer ALL=(ALL) NOPASSWD: /opt/local/etc/logsurfer_rotatelog.sh
#
# 2012-06-19 start logsurfer daemon during system startup
jurgenblaser ALL=(ALL) NOPASSWD: /opt/local/etc/logsurfer_boot.sh
root ALL=(ALL) NOPASSWD: /opt/local/etc/logsurfer_boot.sh
#
```

Anmerkung:

user logsurfer wurde später nicht mehr benutzt..

2.5 aktuell offene Punkte:

2012-06-01

Derzeit wird jede Mail doppelt an den „logsurfer operator user“ verschickt.

Ursache unklar.

4 Wird über die .plist aufgerufen

3 Fehlersuche

3.1 Start von logsurfer

$ /opt/local/etc/logsurfer_proc_starten.sh

$ unable to find inputline for start_regex

Ursache:

Logfile ist leer

Prüfung:

$ ls -al /var/log/logsurfer.log

-rw-r--r-- 1 root wheel 0 5 Apr 17:58 /var/log/logsurfer.log

Abhilfe:[5]

Umleitung der Log-Einträge in Syslog.conf überprüfen, ggf. korrigieren.

An Datei anhängen:

logsurfer Definition (2011-12-15, ca 10h30):

. /var/log/logsurfer.log

Umleitung aktivieren

laeppy-wlan:~ jurgenblaser$ sudo launchctl unload /System/Library/LaunchDaemons/com.apple.syslogd.plist

laeppy-wlan:~ jurgenblaser$ sudo launchctl load /System/Library/LaunchDaemons/com.apple.syslogd.plist

Logfile prüfen:

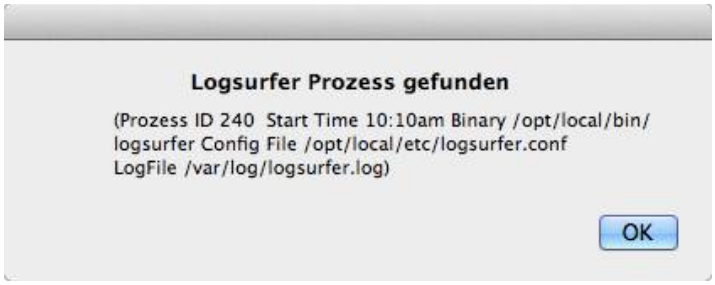
5 Verweis auf entsprechenden Abschnitt einfügen!

3.1.1 Prüfung ob Logsurfer Prozess beim boot gestartet wurde

In manchen Fällen kann es vorkommen, dass der automatische Start von Logsurfer nicht klappt.

Für diesen Zweck sollte ein Testscript bei jedem Administrator ein Skript in der „Autostart“ gestartet werden. Es überprüft, ob der Prozess vorhanden ist und versucht im Fehlerfalle, das Analysetool „nachzustarten.

Falls der Prozess gefunden wird, erscheint ein Fenster wie folgt:



3.1.1.1 Logsurfer Prozess prüfen, ggf. „nachstarten“

Falls der Prozess nicht gestartet wurde wird folgende Meldung ausgegeben:

Im Erfolgsfalle erscheint dann eine Meldung wie oben in 3.1.1

Fehlerbeseitigung siehe 4.1 Logsurfer wird beim Boot des Rechners nicht gestartet

3.1.1.2 Logsurfer Prozess doppelt

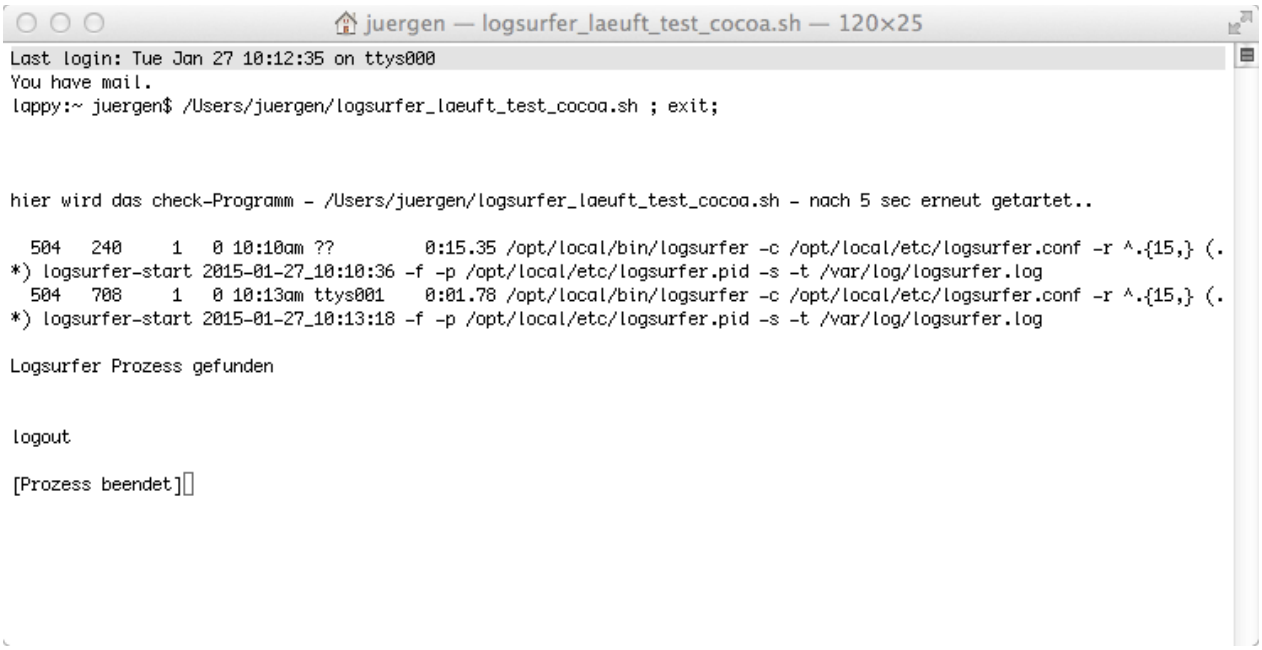
In seltenen Fällen können sich beide Aufgaben

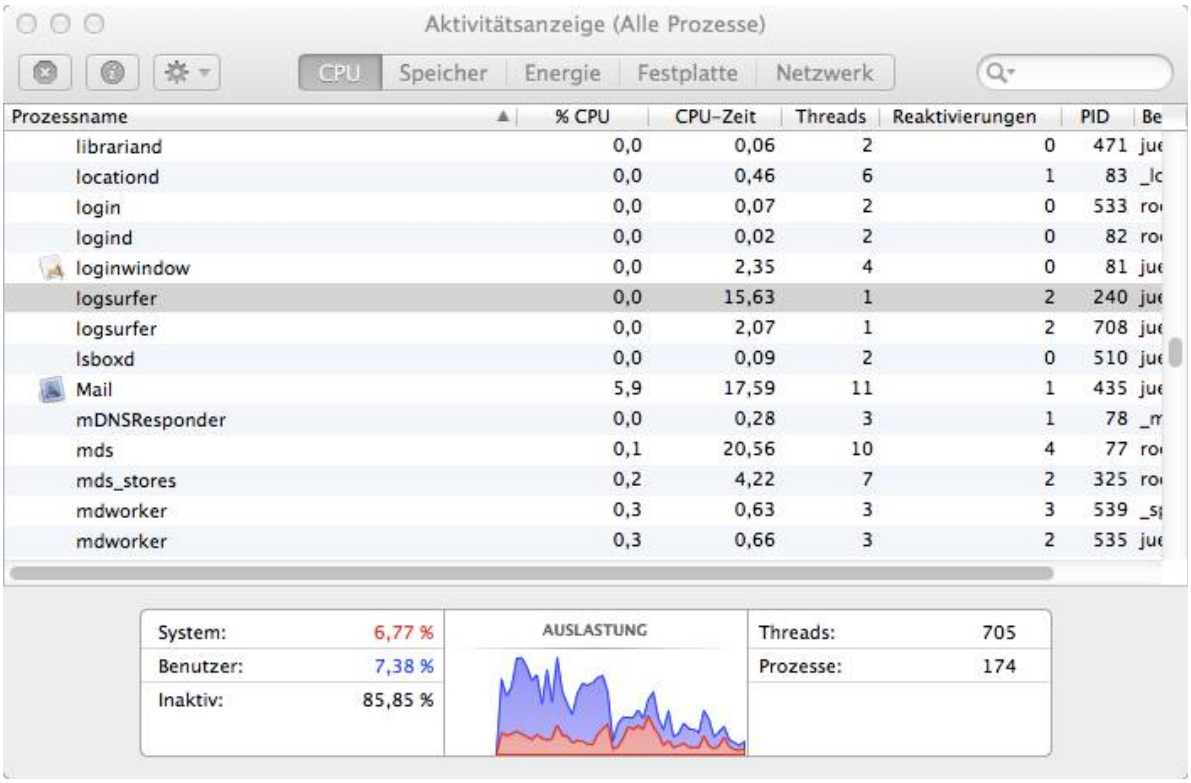
- Start des Prozesses beim boot

und

- Überprüfung, ob der Prozess beim boot gestartet wurde

zeitlich überlappen. D.h. der Prozess wird durch den Bootvorgang zeitlich während oder nach der Prüfung gestartet. Die Folge ist, dass der Analyse-Job „logsurfer“ dann doppelt vorhanden ist:


juergen — logsurfer_laeuft_test_cocoa.sh — 120×25
Last login: Tue Jan 27 10:12:35 on ttys000
You have mail.
lappy:~ juergen$ /Users/juergen/logsurfer_laeuft_test_cocoa.sh ; exit;
hier wird das check-Programm - /Users/juergen/logsurfer_laeuft_test_cocoa.sh - nach 5 sec erneut getartet..
504 240 1 0 10:10am ?? 0:15.35 /opt/local/bin/logsurfer -c /opt/local/etc/logsurfer.conf -r ^.{15,} (.
*) logsurfer-start 2015-01-27_10:10:36 -f -p /opt/local/etc/logsurfer.pid -s -t /var/log/logsurfer.log
504 708 1 0 10:13am ttys001 0:01.78 /opt/local/bin/logsurfer -c /opt/local/etc/logsurfer.conf -r ^.{15,} (.
*) logsurfer-start 2015-01-27_10:13:18 -f -p /opt/local/etc/logsurfer.pid -s -t /var/log/logsurfer.log
Logsurfer Prozess gefunden
logout
[Prozess beendet]


Aktivitätsanzeige (Alle Prozesse)
CPU
Speicher
Energie
Festplatte
Netzwerk
Prozessname
% CPU
CPU-Zeit
Threads
Reaktivierungen
PID
librariand 0,0 0,06 2 0 471
locationd 0,0 0,46 6 1 83
login 0,0 0,07 2 0 533
logind 0,0 0,02 2 0 82
loginwindow 0,0 2,35 4 0 81
logsurfer 0,0 15,63 1 2 240
logsurfer 0,0 2,07 1 2 708
lsboxd 0,0 0,09 2 0 510
Mail 5,9 17,59 11 1 435
mDNSResponder 0,0 0,28 3 1 78
mds 0,1 20,56 10 4 77
mds_stores 0,2 4,22 7 2 325
mdworker 0,3 0,63 3 3 539
mdworker 0,3 0,66 3 2 535
System: 6,77 %
Benutzer: 7,38 %
Inaktiv: 85,85 %
AUSLASTUNG
Threads: 705
Prozesse: 174

4 Fehlerbeseitigung

4.1 Logsurfer wird beim Boot des Rechners nicht gestartet

Prüfung, ob logsurfer „da“ ist, siehe 3.1.1 Prüfung ob Logsurfer Prozess beim boot gestartet wurde

4.2 Prüfung der Ursache:

4.2.1 notwendige Dateien

```
lappy:~ juergen$
lappy:~ juergen$ ls -al /opt/local/bin/logsurfer
-rwxr-xr-x  1 root  admin  68568  3 Apr  2013 /opt/local/bin/logsurfer
lappy:~ juergen$ ls -al /opt/local/etc/logsurfer.conf
-rw-r--r--  1 root  admin  17049  7 Mai  2013 /opt/local/etc/logsurfer.conf
lappy:~ juergen$ ls -al /opt/local/etc/logsurfer.pid
-rw-r--r--  1 juergen  admin  4 16 Feb 13:20 /opt/local/etc/logsurfer.pid
lappy:~ juergen$ ls -al /var/log/logsurfer.log
-rw-r--r--@ 1 root  wheel  21364615 14 Feb 10:03 /var/log/logsurfer.log
lappy:~ juergen$ ls -al /var/tmp/logsurfer_proc_starten.sh.log
-rw-r--r--  1 juergen  wheel  0 16 Feb 13:20 /var/tmp/logsurfer_proc_starten.sh.log
lappy:~ juergen$ ls -al /var/log/logsurfer.log
-rw-r--r--@ 1 root  wheel  21364615 14 Feb 10:03 /var/log/logsurfer.log
lappy:~ juergen$
```

→ sieht alles „gut“ aus ..

4.2.2 Konfiguration der Logmeldung-Umleitung:

Mit „tail var/log/logsurfer.log“ kann man überprüfen, ob neue System-Meldungen ins Logfile eingetragen werden. Hier sollte zumindest alle paar Minuten „etwas passieren“ ...
Wenn hier mur alte Meldungen (oder gar keine..) angezeigt werden, steht zu vermuten, dass die Umleitung der System-Meldungen ins Logsurfer-Logfile nicht (mehr) klappt.

```
lappy:~ juergen$ su - <admin-account>
Password:
lappy:~ $ sudo vi /etc/syslog.conf                    ← ich bevorzuge den vi, da er keine ungewollten Änderungen (Formatierung etc) einbaut..

WARNING: Improper use of the sudo command could lead to data loss
or the deletion of important system files. Please double-check your
typing when using sudo. Type "man sudo" for more information.

To proceed, enter your password, or type Ctrl-C to abort.

Password:

# hier geht es in den „Uralt-Editor“ vi :
# angezeigt wurde

< ----------------- Datei-Inhalt (Anfang) ----------------------------->
# Note that flat file logs are now configured in /etc/asl.conf

install.*                                   @127.0.0.1:32376
~
~
~
< ----------------- Datei-Inhalt (Ende)   ----------------------------->


# d.h. die „Umleitung“ der Log-Einträge war (durch die Installation des neuen OS) entfernt worden.
```

hier sollte nur derjenige etwas ÄNDERN, der sich auskennt.
Die Einträge des Logsurfers werden aus diesem Grunde HINTEN ANGEFÜGT:
—> Eintrag für logsurfer hinzufügen:

(im vi i für Inster-Mode)
———————————— Änderungen für Logsurfer (Anfang) ————————————
logsurfer Definition (2011-12-15, ca 10h30):
. /var/log/logsurfer.log
———————————— Änderungen für Logsurfer (Ende) ————————————

die aktuelle Version (2016-02-16) sieht anschließend „so“ aus:

< ---------- Datei-Inhalt (Anfang) ---------->

Note that flat file logs are now configured in /etc/asl.conf

install.* @127.0.0.1:32376

logsurfer Definition (2011-12-15, ca 10h30):
. /var/log/logsurfer.log

~
~
~
~
< ---------- Datei-Inhalt (Ende) ---------->

vi Edit-Mode mit <ESC> beenden

Editor mit :wg verlassen.

lappy:~ neuer$

reboot des rechners