Logdateien - Zwiesprache mit dem Betriebssystem

Edgar 'Fast Edi' Hoffmann

Community FreieSoftwareOG

kontakt@freiesoftwareog.org

7. Oktober 2015

Logdateien
Begriffserklärung

Logdateien
Begriffserklärung

- Eine Logdatei (auch Ereignisprotokolldatei; englisch log file) enthält das automatisch geführte Protokoll aller oder bestimmter Aktionen von Prozessen auf einem Computersystem. Die korrekte Bezeichnung dafür ist deshalb Protokolldatei

Logdateien
Begriffserklärung

- Eine Logdatei (auch Ereignisprotokolldatei; englisch log file) enthält das automatisch geführte Protokoll aller oder bestimmter Aktionen von Prozessen auf einem Computersystem. Die korrekte Bezeichnung dafür ist deshalb Protokolldatei
- Wichtige Anwendungen finden sich vor allem bei der Prozesskontrolle und Automatisierung

Logdateien
Begriffserklärung

- Eine Logdatei (auch Ereignisprotokolldatei; englisch log file) enthält das automatisch geführte Protokoll aller oder bestimmter Aktionen von Prozessen auf einem Computersystem. Die korrekte Bezeichnung dafür ist deshalb Protokolldatei
- Wichtige Anwendungen finden sich vor allem bei der Prozesskontrolle und Automatisierung
- Prinzipiell werden alle Aktionen mitgeschrieben, die für eine spätere Untersuchung (Audit) erforderlich sind oder sein könnten

Logdateien
Begriffserklärung

- Eine Logdatei (auch Ereignisprotokolldatei; englisch log file) enthält das automatisch geführte Protokoll aller oder bestimmter Aktionen von Prozessen auf einem Computersystem. Die korrekte Bezeichnung dafür ist deshalb Protokolldatei
- Wichtige Anwendungen finden sich vor allem bei der Prozesskontrolle und Automatisierung
- Prinzipiell werden alle Aktionen mitgeschrieben, die für eine spätere Untersuchung (Audit) erforderlich sind oder sein könnten
- Der Flugschreiber in Flugzeugen ist ein Beispiel für kontinuierliche Protokollierung, die jedoch selten ausgewertet wird, zum Beispiel nach einem Unfall

Logdateien
Begriffserklärung

- Eine Logdatei (auch Ereignisprotokolldatei; englisch log file) enthält das automatisch geführte Protokoll aller oder bestimmter Aktionen von Prozessen auf einem Computersystem. Die korrekte Bezeichnung dafür ist deshalb Protokolldatei
- Wichtige Anwendungen finden sich vor allem bei der Prozesskontrolle und Automatisierung
- Prinzipiell werden alle Aktionen mitgeschrieben, die für eine spätere Untersuchung (Audit) erforderlich sind oder sein könnten
- Der Flugschreiber in Flugzeugen ist ein Beispiel für kontinuierliche Protokollierung, die jedoch selten ausgewertet wird, zum Beispiel nach einem Unfall
- Im Bereich der Datenbanken bezeichnet Logfile die Protokolldatei in der Änderungen an der Datenbank von korrekt abgeschlossenen Transaktionen (per Commit abgeschlossen) festgehalten werden, um im Fall eines Fehlers (z. B. Systemabsturz) den aktuellen Datenbestand wiederherstellen zu können

Logdateien
Grundlagen

Logdateien
Grundlagen

Auf einem PC können Protokolldateien bestimmter Aktionen von einem oder mehreren Nutzern an einem Rechner geschrieben werden, ohne dass diese es bemerken oder ihre Arbeit beeinflusst wird.

Logdateien
Grundlagen

Auf einem PC können Protokolldateien bestimmter Aktionen von einem oder mehreren Nutzern an einem Rechner geschrieben werden, ohne dass diese es bemerken oder ihre Arbeit beeinflusst wird.

Wesentlich ist hierzu das Systemlogbuch (unter Linux meist in /var/log/messages, aber auch Windows NT und Nachfolger schreiben entsprechende Einträge in eines oder mehrere Ereignisprotokolle), wenn sie entsprechend konfiguriert werden.

Logdateien
Grundlagen

Logdateien
Grundlagen

Darin können u. a. die Anmeldungen am System protokolliert werden, aber auch andere wichtige Informationen.

Logdateien
Grundlagen

Darin können u. a. die Anmeldungen am System protokolliert werden, aber auch andere wichtige Informationen.

Außer dem Betriebssystem selbst schreiben meist Hintergrundprogramme (z. B. ein E-Mail-Server, ein Proxyserver und anderes) in Logdateien, um Aktionsmeldungen, Fehlermeldungen und Hinweise persistent (dauernd) oder temporär verfügbar zu halten.

Logdateien
Grundlagen

Darin können u. a. die Anmeldungen am System protokolliert werden, aber auch andere wichtige Informationen.

Außer dem Betriebssystem selbst schreiben meist Hintergrundprogramme (z. B. ein E-Mail-Server, ein Proxyserver und anderes) in Logdateien, um Aktionsmeldungen, Fehlermeldungen und Hinweise persistent (dauernd) oder temporär verfügbar zu halten.

Ähnliches gilt für Installationsprogramme, Firewalls, Virenscanner und dergleichen.

Logdateien
Grundlagen

Darin können u. a. die Anmeldungen am System protokolliert werden, aber auch andere wichtige Informationen.

Außer dem Betriebssystem selbst schreiben meist Hintergrundprogramme (z. B. ein E-Mail-Server, ein Proxyserver und anderes) in Logdateien, um Aktionsmeldungen, Fehlermeldungen und Hinweise persistent (dauernd) oder temporär verfügbar zu halten.

Ähnliches gilt für Installationsprogramme, Firewalls, Virenscanner und dergleichen.

Logdateien werden auch von Webservern erstellt, können aber auch außerhalb des Internets bei Untersuchungen der Benutzerfreundlichkeit von Programmen, allgemeinem Nutzerverhalten oder der Fehlersuche in einem System genutzt werden.

Logdateien
Grundlagen

Darin können u. a. die Anmeldungen am System protokolliert werden, aber auch andere wichtige Informationen.

Außer dem Betriebssystem selbst schreiben meist Hintergrundprogramme (z. B. ein E-Mail-Server, ein Proxyserver und anderes) in Logdateien, um Aktionsmeldungen, Fehlermeldungen und Hinweise persistent (dauernd) oder temporär verfügbar zu halten.

Ähnliches gilt für Installationsprogramme, Firewalls, Virenscanner und dergleichen.

Logdateien werden auch von Webservern erstellt, können aber auch außerhalb des Internets bei Untersuchungen der Benutzerfreundlichkeit von Programmen, allgemeinem Nutzerverhalten oder der Fehlersuche in einem System genutzt werden.

Die Logdatei wird bei der Logdateianalyse untersucht.

Logdateien
Linux Logdateien

Logdateien
Linux Logdateien

Das Utility syslogd schreibt verschiedene Systemaktivitäten mit, so zum Beispiel die Debugging-Meldungen von sendmail und Warnungen des Kernels.

Logdateien
Linux Logdateien

Das Utility syslogd schreibt verschiedene Systemaktivitäten mit, so zum Beispiel die Debugging-Meldungen von sendmail und Warnungen des Kernels.

syslogd läuft als Dämon und wird in der Regel beim Booten aus einer der rc-Dateien gestartet.

Logdateien
Linux Logdateien

Das Utility syslogd schreibt verschiedene Systemaktivitäten mit, so zum Beispiel die Debugging-Meldungen von sendmail und Warnungen des Kernels.

syslogd läuft als Dämon und wird in der Regel beim Booten aus einer der rc-Dateien gestartet.

Die Datei /etc/syslog.conf wird benutzt, um festzulegen, wo syslogd Informationen ablegt. Diese Datei könnte folgendermaßen aussehen:

Logdateien
Linux Logdateien

Das Utility syslogd schreibt verschiedene Systemaktivitäten mit, so zum Beispiel die Debugging-Meldungen von sendmail und Warnungen des Kernels.

syslogd läuft als Dämon und wird in der Regel beim Booten aus einer der rc-Dateien gestartet.

Die Datei /etc/syslog.conf wird benutzt, um festzulegen, wo syslogd Informationen ablegt. Diese Datei könnte folgendermaßen aussehen:

```
*.info;*.notice /var/log/messages
mail.debug /var/log/maillog
*.warn /var/log/syslog
kern.emerg /dev/console
```

Logdateien
Linux Logdateien

Das Utility syslogd schreibt verschiedene Systemaktivitäten mit, so zum Beispiel die Debugging-Meldungen von sendmail und Warnungen des Kernels.

syslogd läuft als Dämon und wird in der Regel beim Booten aus einer der rc-Dateien gestartet.

Die Datei /etc/syslog.conf wird benutzt, um festzulegen, wo syslogd Informationen ablegt. Diese Datei könnte folgendermaßen aussehen:

```
*.info;*.notice /var/log/messages
mail.debug /var/log/maillog
*.warn /var/log/syslog
kern.emerg /dev/console
```

Das erste Feld jeder Zeile bestimmt, welche Meldungen protokolliert werden sollen, und das zweite Feld gibt an, wohin die Meldungen geschrieben werden.

Logdateien
Linux Logdateien

Logdateien
Linux Logdateien

Das erste Feld hat das Format: Ursprung.Level [;Ursprung.Level...]

Logdateien
Linux Logdateien

Das erste Feld hat das Format: Ursprung.Level [;Ursprung.Level...]

Dabei bezeichnet der Ursprung das Systemprogramm oder die Komponente des Systems, die die Meldung verursacht, und der Level gibt an, wie schwerwiegend die Meldung ist.

Logdateien
Linux Logdateien

Das erste Feld hat das Format: Ursprung.Level [;Ursprung.Level...]

Dabei bezeichnet der Ursprung das Systemprogramm oder die Komponente des Systems, die die Meldung verursacht, und der Level gibt an, wie schwerwiegend die Meldung ist.

Beispiele für den Ursprung

Logdateien
Linux Logdateien

Das erste Feld hat das Format: Ursprung.Level [;Ursprung.Level...]

Dabei bezeichnet der Ursprung das Systemprogramm oder die Komponente des Systems, die die Meldung verursacht, und der Level gibt an, wie schwerwiegend die Meldung ist.

Beispiele für den Ursprung

- mail (für den Mail-Dämon)

Logdateien
Linux Logdateien

Das erste Feld hat das Format: Ursprung.Level [;Ursprung.Level...]

Dabei bezeichnet der Ursprung das Systemprogramm oder die Komponente des Systems, die die Meldung verursacht, und der Level gibt an, wie schwerwiegend die Meldung ist.

Beispiele für den Ursprung

- mail (für den Mail-Dämon)
- kern (für den Kernel)

Logdateien
Linux Logdateien

Das erste Feld hat das Format: Ursprung.Level [;Ursprung.Level...]

Dabei bezeichnet der Ursprung das Systemprogramm oder die Komponente des Systems, die die Meldung verursacht, und der Level gibt an, wie schwerwiegend die Meldung ist.

Beispiele für den Ursprung

- mail (für den Mail-Dämon)
- kern (für den Kernel)
- user (für Benutzerprogramme)

Logdateien
Linux Logdateien

Das erste Feld hat das Format: Ursprung.Level [;Ursprung.Level...]

Dabei bezeichnet der Ursprung das Systemprogramm oder die Komponente des Systems, die die Meldung verursacht, und der Level gibt an, wie schwerwiegend die Meldung ist.

Beispiele für den Ursprung

- mail (für den Mail-Dämon)
- kern (für den Kernel)
- user (für Benutzerprogramme)
- auth (für Programme, die den Zugang zum System kontrollieren, wie etwa login oder su)

Logdateien
Linux Logdateien

Das erste Feld hat das Format: Ursprung.Level [;Ursprung.Level...]

Dabei bezeichnet der Ursprung das Systemprogramm oder die Komponente des Systems, die die Meldung verursacht, und der Level gibt an, wie schwerwiegend die Meldung ist.

Beispiele für den Ursprung

- mail (für den Mail-Dämon)
- kern (für den Kernel)
- user (für Benutzerprogramme)
- auth (für Programme, die den Zugang zum System kontrollieren, wie etwa login oder su)

Logdateien
Linux Logdateien

Das erste Feld hat das Format: Ursprung.Level [;Ursprung.Level...]

Dabei bezeichnet der Ursprung das Systemprogramm oder die Komponente des Systems, die die Meldung verursacht, und der Level gibt an, wie schwerwiegend die Meldung ist.

Beispiele für den Ursprung

- mail (für den Mail-Dämon)
- kern (für den Kernel)
- user (für Benutzerprogramme)
- auth (für Programme, die den Zugang zum System kontrollieren, wie etwa login oder su)

Ein Stern in diesem Feld steht für Meldungen aus allen Quellen.

Logdateien
Linux Logdateien

Logdateien
Linux Logdateien

Als Level (mit zunehmender Wichtigkeit) kann folgendes angegeben werden:

Logdateien
Linux Logdateien

Als Level (mit zunehmender Wichtigkeit) kann folgendes angegeben werden:

- debug

Logdateien
Linux Logdateien

Als Level (mit zunehmender Wichtigkeit) kann folgendes angegeben werden:

- debug
- info

Logdateien
Linux Logdateien

Als Level (mit zunehmender Wichtigkeit) kann folgendes angegeben werden:

- debug
- info
- notice

Logdateien
Linux Logdateien

Als Level (mit zunehmender Wichtigkeit) kann folgendes angegeben werden:

- debug
- info
- notice
- warning

Logdateien
Linux Logdateien

Als Level (mit zunehmender Wichtigkeit) kann folgendes angegeben werden:

- debug
- info
- notice
- warning
- err

Logdateien
Linux Logdateien

Als Level (mit zunehmender Wichtigkeit) kann folgendes angegeben werden:

- debug
- info
- notice
- warning
- err
- crit

Logdateien
Linux Logdateien

Als Level (mit zunehmender Wichtigkeit) kann folgendes angegeben werden:

- debug
- info
- notice
- warning
- err
- crit
- alert

Logdateien
Linux Logdateien

Als Level (mit zunehmender Wichtigkeit) kann folgendes angegeben werden:

- debug
- info
- notice
- warning
- err
- crit
- alert
- emerg

Logdateien
Wichtige Logdateien (Auszug)

Logdateien
Wichtige Logdateien (Auszug)

Logdatei	Inhalt/Quelle
acpid	Ausgaben der Energieverwaltung
auth.log	Alle Versuche sich am System anzumelden werden hier protokolliert
dmesg	Letzte Meldungen des Kernels. Die Informationen stammen aus einem Ringpuffer, sodaß alte Meldungen überschrieben werden. Die Datei kern.log enthält dagegen auch ältere Meldungen
dpkg / history.log in apt	Log der Paketverwaltung. Hier findet man, wann welches Programm installiert, gelöscht oder aktualisiert wurde
messages	Allgemeine Informationen des Systems. Zusammen mit dem syslog eine der wichtigsten Logdateien des Systems
syslog	Die Ausgabe des syslogd. Eine Alternative zu Syslog ist das um einige Funktionen erweiterte syslog-ng
Xorg.0.log	Ausgabe des XServers
~/.xsession-errors	Ausgaben zahlreicher grafischer Programme in einer versteckten Datei im Homeverzeichnis jedes Benutzers

Logdateien
Grafische Werkzeuge

Logdateien
Grafische Werkzeuge

Logdateien sind immer Textdateien.

Logdateien
Grafische Werkzeuge

Logdateien sind immer Textdateien.

Man kann sie mit jedem beliebigen Texteditor oder Dateibetrachter ansehen.

Logdateien
Grafische Werkzeuge

Logdateien sind immer Textdateien.

Man kann sie mit jedem beliebigen Texteditor oder Dateibetrachter ansehen.

Die Desktopumgebungen bringen Werkzeuge mit, um die Logs mit etwas Komfort zu analysieren.

Logdateien
Grafische Werkzeuge

Logdateien sind immer Textdateien.

Man kann sie mit jedem beliebigen Texteditor oder Dateibetrachter ansehen.

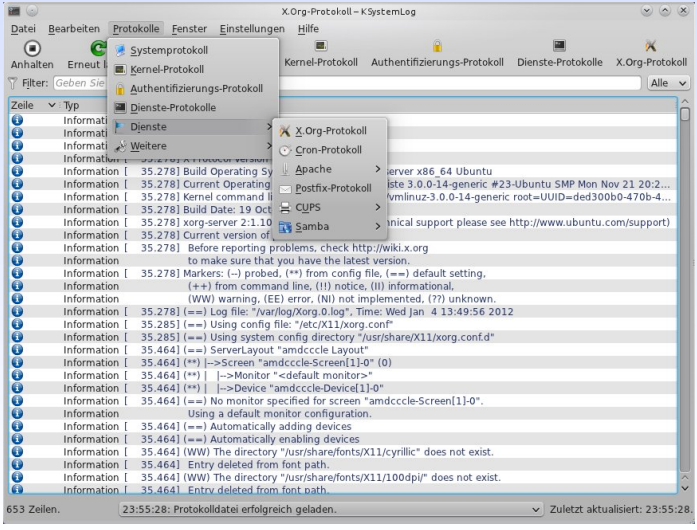
Die Desktopumgebungen bringen Werkzeuge mit, um die Logs mit etwas Komfort zu analysieren.

Auch in einem Terminal können Logs sehr effektiv betrachtet werden.

Logdateien
Grafische Werkzeuge

Logdateien
Grafische Werkzeuge

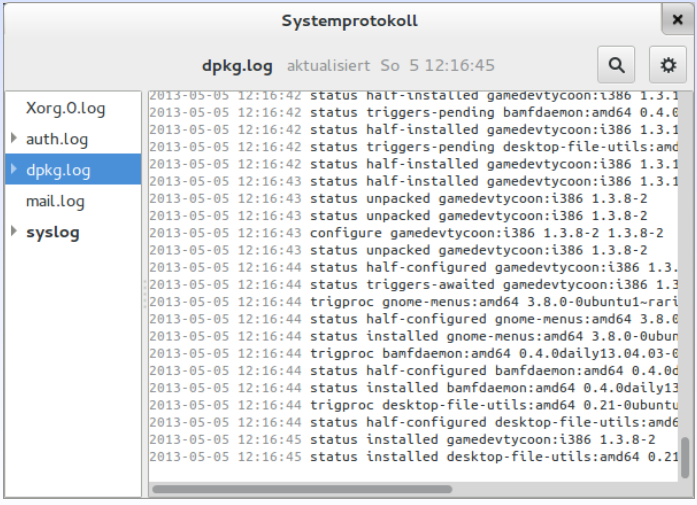
- Systemprotokollbetrachter (in gnome-utils)



Logdateien
Grafische Werkzeuge

Logdateien
Grafische Werkzeuge

- ksystemlog



Logdateien
Konsolenwerkzeuge

Logdateien
Konsolenwerkzeuge

Logs lassen sich auch relativ komfortabel in einer Konsole betrachten.

Logdateien
Konsolenwerkzeuge

Logs lassen sich auch relativ komfortabel in einer Konsole betrachten.

- less (less /var/log/syslog)

Logdateien
Konsolenwerkzeuge

Logs lassen sich auch relativ komfortabel in einer Konsole betrachten.

- less (less /var/log/syslog)
- zless (zless /var/log/syslog.1.gz)

Logdateien
Konsolenwerkzeuge

Logs lassen sich auch relativ komfortabel in einer Konsole betrachten.

- less (less /var/log/syslog)
- zless (zless /var/log/syslog.1.gz)
- tail (tail -f -n 0 /var/log/syslog)

Logdateien
Konsolenwerkzeuge

Logs lassen sich auch relativ komfortabel in einer Konsole betrachten.

- less (less /var/log/syslog)
- zless (zless /var/log/syslog.1.gz)
- tail (tail -f -n 0 /var/log/syslog)
- multitail

Logdateien
Spezifische Angaben ausgeben

Logdateien
Spezifische Angaben ausgeben

Mit grep bzw. egrep kann man sehr einfach lange Logdateien nach bestimmten Schlagworten filtern.

Logdateien
Spezifische Angaben ausgeben

Mit grep bzw. egrep kann man sehr einfach lange Logdateien nach bestimmten Schlagworten filtern.

tail -f - n 0 /var/log/syslog — grep usb
führt zur Ausgabe:

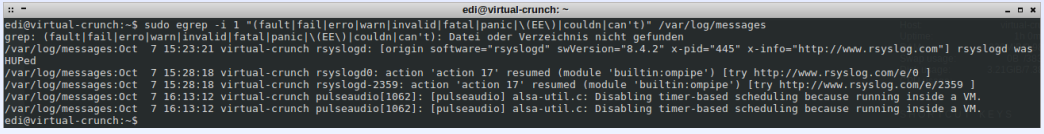
```
edi@Virtual-Ubuntu:~$ tail -f -n 0 /var/log/syslog | grep usb
Oct  5 22:27:55 Virtual-Ubuntu kernel: [ 1176.472169] usb 1-1: new high-speed USB device number 2 using ehci-pci
Oct  5 22:27:55 Virtual-Ubuntu kernel: [ 1177.353278] usb 1-1: New USB device found, idVendor=0781, idProduct=556b
Oct  5 22:27:55 Virtual-Ubuntu kernel: [ 1177.353278] usb 1-1: New USB device strings: Mfr=1, Product=2, SerialNumber=3
Oct  5 22:27:55 Virtual-Ubuntu kernel: [ 1177.353278] usb 1-1: Product: Cruzer Edge
Oct  5 22:27:55 Virtual-Ubuntu kernel: [ 1177.353278] usb 1-1: Manufacturer: SanDisk
Oct  5 22:27:55 Virtual-Ubuntu kernel: [ 1177.353278] usb 1-1: SerialNumber: 20042204500A804088E5
Oct  5 22:27:56 Virtual-Ubuntu mtp-probe: checking bus 1, device 2: "/sys/devices/pci0000:00/0000:00:0b.0/usb1/1-1"
Oct  5 22:27:57 Virtual-Ubuntu kernel: [ 1178.584179] usb-storage 1-1:1.0: USB Mass Storage device detected
Oct  5 22:27:57 Virtual-Ubuntu kernel: [ 1178.592167] scsi3 : usb-storage 1-1:1.0
Oct  5 22:27:57 Virtual-Ubuntu kernel: [ 1178.596926] usbcore: registered new interface driver usb-storage
```

Logdateien
Spezifische Angaben ausgeben

Logdateien
Spezifische Angaben ausgeben

```
egrep -i 1 "(fault|fail|erro|warn|invalid|fatal|panic|\(EE\)|couldn|can't)" /var/log/messages
```

führt zur Ausgabe:



Damit werden alle Zeilen, welche die Worte fault, fail ... enthalten, ausgegeben.
Durch die Option 1 wird immer eine Zeile vor und hinter dem Treffer ausgegeben, durch -i die Groß-/Kleinschreibung für die Suche ignoriert.

Logdateien
Interne Verwaltung der Logdateien

Logdateien
Interne Verwaltung der Logdateien

Damit Logdateien nicht immer weiter wachsen und irgendwann mal die komplette Festplatte belegen, wird bei der Installation eines Linux Systems meistens auch gleich der Dienst „logrotate“installiert.

Logdateien
Interne Verwaltung der Logdateien

Damit Logdateien nicht immer weiter wachsen und irgendwann mal die komplette Festplatte belegen, wird bei der Installation eines Linux Systems meistens auch gleich der Dienst „logrotate“installiert.

Logrotate wurde entwickelt, um die Verwaltung von Logs zu vereinfachen.

Logdateien
Interne Verwaltung der Logdateien

Damit Logdateien nicht immer weiter wachsen und irgendwann mal die komplette Festplatte belegen, wird bei der Installation eines Linux Systems meistens auch gleich der Dienst „logrotate“installiert.

Logrotate wurde entwickelt, um die Verwaltung von Logs zu vereinfachen.

Der Dienst erlaubt es, automatisch Logs zu komprimieren, zu löschen oder per Mail zu verschicken.

Logdateien
Interne Verwaltung der Logdateien

Damit Logdateien nicht immer weiter wachsen und irgendwann mal die komplette Festplatte belegen, wird bei der Installation eines Linux Systems meistens auch gleich der Dienst „logrotate“installiert.

Logrotate wurde entwickelt, um die Verwaltung von Logs zu vereinfachen.

Der Dienst erlaubt es, automatisch Logs zu komprimieren, zu löschen oder per Mail zu verschicken.

Logrotate kann dies täglich, wöchentlich, monatlich durchführen oder wenn eine Logdatei eine vorgegebene Größe überschreitet.

Logdateien
Interne Verwaltung der Logdateien

Damit Logdateien nicht immer weiter wachsen und irgendwann mal die komplette Festplatte belegen, wird bei der Installation eines Linux Systems meistens auch gleich der Dienst „logrotate“installiert.

Logrotate wurde entwickelt, um die Verwaltung von Logs zu vereinfachen.

Der Dienst erlaubt es, automatisch Logs zu komprimieren, zu löschen oder per Mail zu verschicken.

Logrotate kann dies täglich, wöchentlich, monatlich durchführen oder wenn eine Logdatei eine vorgegebene Größe überschreitet.

Üblicherweise wird Logrotate einmal am Tag aktiv.

Logdateien
Interne Verwaltung der Logdateien

Logdateien
Interne Verwaltung der Logdateien

Am Beispiel des „Syslogs“kann man sehen, wie logrotate arbeitet.

Logdateien
Interne Verwaltung der Logdateien

Am Beispiel des „Syslogs“kann man sehen, wie logrotate arbeitet.

Schaut man sich die Dateien in /var/log an, die den Namen „syslog“tragen:

Logdateien
Interne Verwaltung der Logdateien

Am Beispiel des „Syslogs“kann man sehen, wie logrotate arbeitet.

Schaut man sich die Dateien in /var/log an, die den Namen „syslog“tragen:

ls -al /var/log/syslog*

Logdateien
Interne Verwaltung der Logdateien

Am Beispiel des „Syslogs“kann man sehen, wie logrotate arbeitet.

Schaut man sich die Dateien in /var/log an, die den Namen „syslog“tragen:

ls -al /var/log/syslog*

so sieht man acht Dateien.

Logdateien
Interne Verwaltung der Logdateien

Am Beispiel des „Syslogs“kann man sehen, wie logrotate arbeitet.

Schaut man sich die Dateien in /var/log an, die den Namen „syslog“tragen:

ls -al /var/log/syslog*

so sieht man acht Dateien.

Die aktuelle syslog, die unkomprimierte syslog.0 vom Vortag und die Syslogs der sechs Tage davor, die in der Zwischenzeit komprimiert wurden.

Logdateien
Interne Verwaltung der Logdateien

Am Beispiel des „Syslogs“kann man sehen, wie logrotate arbeitet.

Schaut man sich die Dateien in /var/log an, die den Namen „syslog“tragen:

ls -al /var/log/syslog*

so sieht man acht Dateien.

Die aktuelle syslog, die unkomprimierte syslog.0 vom Vortag und die Syslogs der sechs Tage davor, die in der Zwischenzeit komprimiert wurden.

Am achten Tag werden dann die Logs gelöscht.

Logdateien
Fehlersuche mit Logdateien

Logdateien
Fehlersuche mit Logdateien

Log-Dateien sind der Segen für Linux-Admins.
In Log-Dateien legen Daemons/Dienste und Programme ihre Informationen ab.
Das ermöglicht gezieltes Suchen nach Fehlern, was unter MS-Windows oft nicht möglich ist.

Logdateien
Fehlersuche mit Logdateien

Log-Dateien sind der Segen für Linux-Admins.
In Log-Dateien legen Daemons/Dienste und Programme ihre Informationen ab.
Das ermöglicht gezieltes Suchen nach Fehlern, was unter MS-Windows oft nicht möglich ist.

Die Log-Dateien sollten daher die erste Anlaufstelle bei einer Fehlersuche sein.
Linux und darauf laufende Daemons/Dienste schreiben meist relativ viel Informationen in Log-Dateien, es gilt, die entscheidenden zu finden.

Logdateien
Fehlersuche mit Logdateien

Logdateien
Fehlersuche mit Logdateien

Logdateien liegen meist unter /var/log/.
Eine zentrale Log-Datei für System-Meldungen ist die /var/log/messages
Die einzelnen Server-Dienste (Daemons) haben oft eigene Log-Dateien unter /var/log, manche in eigenen Unterverzeichnissen, wie z.B. /var/log/samba/
Selbst kompilierte Programme legen die Log-Dateien oft ganz woanders ab

Logdateien
Fehlersuche mit Logdateien

Logdateien liegen meist unter /var/log/.
Eine zentrale Log-Datei für System-Meldungen ist die /var/log/messages
Die einzelnen Server-Dienste (Daemons) haben oft eigene Log-Dateien unter /var/log, manche in eigenen Unterverzeichnissen, wie z.B. /var/log/samba/
Selbst kompilierte Programme legen die Log-Dateien oft ganz woanders ab Wenn nicht

erkennbar ist, welche Log-Datei die rettende Fehlermeldungen enthalten könnten, hilft es oft, zunächst zu ermitteln, welche Dateien am neuesten sind und diese anzuschauen.
Eine sortierte Ausgabe des Verzeichnisses /var/log nach der Reihenfolge der letzten Änderung erhält man mit:

Logdateien
Fehlersuche mit Logdateien

Logdateien liegen meist unter /var/log/.
Eine zentrale Log-Datei für System-Meldungen ist die /var/log/messages
Die einzelnen Server-Dienste (Daemons) haben oft eigene Log-Dateien unter /var/log, manche in eigenen Unterverzeichnissen, wie z.B. /var/log/samba/
Selbst kompilierte Programme legen die Log-Dateien oft ganz woanders ab Wenn nicht

erkennbar ist, welche Log-Datei die rettende Fehlermeldungen enthalten könnten, hilft es oft, zunächst zu ermitteln, welche Dateien am neuesten sind und diese anzuschauen.
Eine sortierte Ausgabe des Verzeichnisses /var/log nach der Reihenfolge der letzten Änderung erhält man mit:

ls -lt /var/log/ — less

Logdateien
Fehlersuche mit Logdateien

Logdateien liegen meist unter /var/log/.
Eine zentrale Log-Datei für System-Meldungen ist die /var/log/messages
Die einzelnen Server-Dienste (Daemons) haben oft eigene Log-Dateien unter /var/log, manche in eigenen Unterverzeichnissen, wie z.B. /var/log/samba/
Selbst kompilierte Programme legen die Log-Dateien oft ganz woanders ab Wenn nicht

erkennbar ist, welche Log-Datei die rettende Fehlermeldungen enthalten könnten, hilft es oft, zunächst zu ermitteln, welche Dateien am neuesten sind und diese anzuschauen.
Eine sortierte Ausgabe des Verzeichnisses /var/log nach der Reihenfolge der letzten Änderung erhält man mit:

ls -lt /var/log/ — less

Eine Ausgabe aller Dateien einschließlich der Unterverzeichnisse, die jünger als 10 Minuten sind, erhält man mit:

Logdateien
Fehlersuche mit Logdateien

Logdateien liegen meist unter /var/log/.
Eine zentrale Log-Datei für System-Meldungen ist die /var/log/messages
Die einzelnen Server-Dienste (Daemons) haben oft eigene Log-Dateien unter /var/log, manche in eigenen Unterverzeichnissen, wie z.B. /var/log/samba/
Selbst kompilierte Programme legen die Log-Dateien oft ganz woanders ab Wenn nicht

erkennbar ist, welche Log-Datei die rettende Fehlermeldungen enthalten könnten, hilft es oft, zunächst zu ermitteln, welche Dateien am neuesten sind und diese anzuschauen.
Eine sortierte Ausgabe des Verzeichnisses /var/log nach der Reihenfolge der letzten Änderung erhält man mit:

ls -lt /var/log/ — less

Eine Ausgabe aller Dateien einschließlich der Unterverzeichnisse, die jünger als 10 Minuten sind, erhält man mit:

find /var/log/ -mmin -10

Links zur Präsentation

http://www.oreilly.de/german/freebooks/rlinux3ger/ch084.html
https://wiki.ubuntuusers.de/logdateien
http://linuxwiki.de/SystemStatus

Weitere Informationen bekommen Sie hier:

http://www.FreieSoftwareOG.org
und
Kontakt@FreieSoftwareOG.org

oder kommen Sie doch einfach zu unserem regelmäßigen Treffen,
jeden 1. Mittwoch im Monat ab 20:00 Uhr.
(Treffpunkt und Thema laut Webseite)

FreieSoftwareOG.org