**So überwachen Sie das /var/log/messages-Dateisystem unter Linux**

Ich werde Ihnen die Schritte zur Überwachung des /var/log/messages-Dateisystems demonstrieren, wenn eine große Anzahl von Logs aus verschiedenen Linux-Umgebungen eingeht.

Die Datei /var/log/messages in einem Linux-Dateisystem wird in der Regel vom Syslog- oder Rsyslog-Logging-Dienst erstellt und verwaltet. Sie dient als zentrale Protokolldatei, in der verschiedene Systemereignisse, Informationsmeldungen, Warnungen und Fehler aufgezeichnet werden. Die genaue Quelle der Nachrichten in dieser Datei kann jedoch je nach Systemkonfiguration variieren.

1. **Systemdienste** [Systemstart- und -abschaltungen]

**1.1 Kernel-Nachrichten**

**1.2 CRON-Job-Ausgaben** [Benutzeranwendungen oder benutzerdefinierte Skripte können auch Logs an Syslog senden, abhängig von ihrer Konfiguration.]

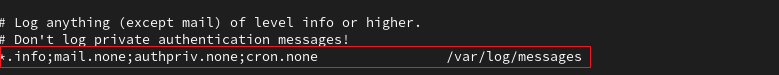
**1.3 Statusänderungen von Diensten** (z.B. SSH, Network Manager)

1. **Kernel-Logs** [z.B. Hardware-Initialisierung, Treibernachrichten werden oft hier protokolliert]
2. **Anwendungen und Prozesse**: Benutzeranwendungen oder benutzerdefinierte Skripte können auch Logs an Syslog senden, abhängig von ihrer Konfiguration.
3. **Netzwerkereignisse: Netzwerktools und -protokolle** (wie DHCP- oder DNS-Clients) protokollieren häufig Nachrichten im Zusammenhang mit ihren Aktivitäten.

Ich werde erklären, wie /var/log/messages gefüllt wird:

**Logging-Daemon**: Der rsyslog- oder syslog-Dienst ist in der Regel für das Sammeln und Weiterleiten von Log-Nachrichten zuständig. Er verwendet die Konfigurationsdatei /etc/rsyslog.conf, um zu bestimmen, wohin Logs gehen sollen.

Die Regel für /var/log/messages sieht in der /etc/rsyslog.conf in der Regel so aus:



Diese Zeile bedeutet:

Protokolliere alle Nachrichten mit einer Priorität von "info" oder höher (\*.info), mit Ausnahme von Mail-, Authpriv- und Cron-Nachrichten, in /var/log/messages.

**Kernel-Protokolle:**

Der Kernel protokolliert Nachrichten über den dmesg-Puffer, und einige davon werden an syslog weitergeleitet, um sie in /var/log/messages aufzunehmen.

**Anwendungs-Konfiguration:**

Anwendungen können so konfiguriert werden, dass sie syslog zum Protokollieren von Nachrichten verwenden. Ein Dienst könnte beispielsweise enthalten:

logger -p syslog.info "Dies ist eine Testnachricht"

Um die Anforderung zu erfüllen, habe ich ein Shell-Skript erstellt, das die folgenden Aufgaben ausführt, und ich habe es mit dem Befehl "***chmod +x monitor\_var\_log.sh***“ ausführbar gemacht.



Ein Bild, das Text, Screenshot, Software, Multimedia-Software enthält.

Automatisch generierte Beschreibung

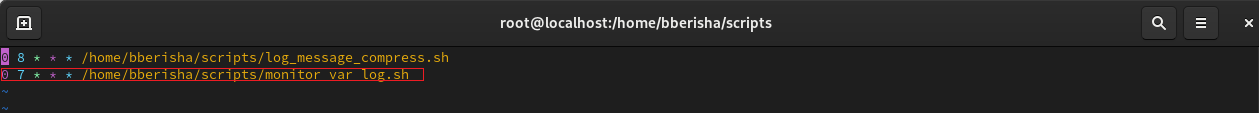
Dieses Shell-Skript überwacht die Nutzung des Verzeichnisses /var/log und die Datei **/var/log/messages.** Es führt folgende Schritte aus:

* **Variablen definieren:** Festlegung von Pfaden, Warn- und Kritikalitätsgrenzen sowie des Empfängers für E-Mails. Hier werden alle wichtigen Informationen in Variablen gespeichert, um das Skript flexibler zu gestalten.
* **Festplattennutzung überprüfen:** Prüft, ob die Nutzung von /var/log über 90% (kritisch) oder 80% (Warnung) liegt. Bei Überschreiten der Grenzen wird eine E-Mail an den Administrator gesendet. So wird sichergestellt, dass ausreichend Speicherplatz für neue Log-Einträge vorhanden ist.
* **Logdatei überprüfen:** Falls /var/log/messages existiert, wird sie auf Anomalien überprüft und die letzten 20 Zeilen angezeigt. Andernfalls wird gemeldet, dass die Datei fehlt. Dies hilft bei der schnellen Identifizierung von Problemen.

**Ich habe außerdem einen Cronjob konfiguriert, um die Ausführung des Skripts zu planen.**

Indem ich die Crontab bearbeitet habe, habe ich festgelegt, wann das Skript regelmäßig ausgeführt werden soll. **Cronjobs** sind ein leistungsstarkes Tool unter Linux, um Aufgaben zu automatisieren. Mit ihnen können Sie Skripte oder Befehle zu bestimmten Zeiten oder in bestimmten Intervallen ausführen lassen.

**Beispiel für einen Cronjob-Eintrag:**



Und auch mailutils ist so konfiguriert, dass die E-Mails ankommen.

Das ist alles! Vielen Dank.