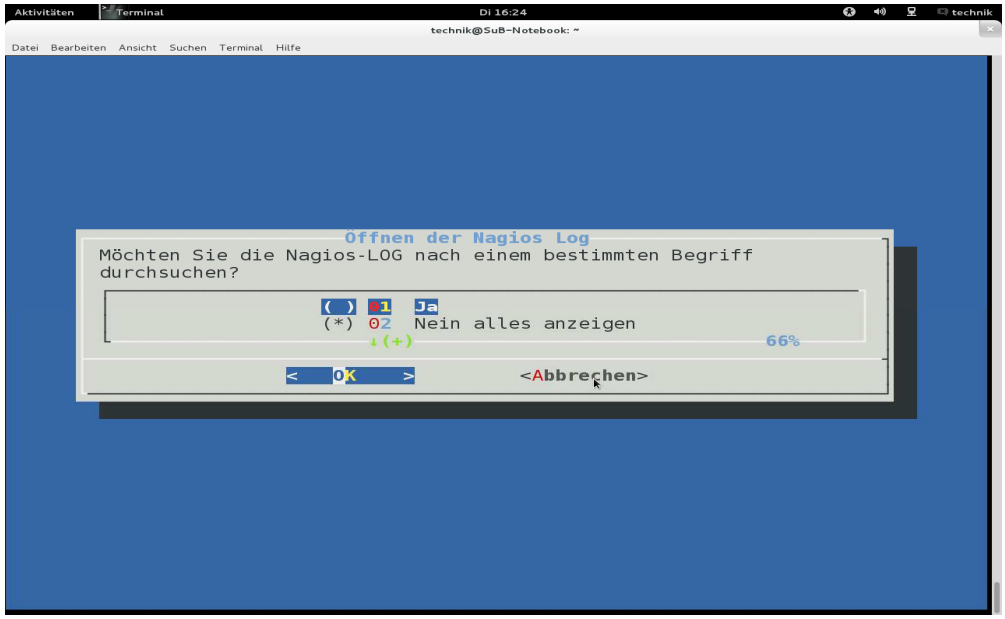
Benutzung der Suchfunktion für die Nagios-Log:

1. Einleitung

   Innerhalb der Nagios-Box gibt es im Hauptmenu unter dem Menu Punkt *„7 LOG Nagios öffnen / durchsuchen“* Zwei Möglichkeiten der Auswahl:



   Im Falle der Eingabe *„Nein alles Anzeigen“* wird die gesamte Log Datei geöffnet.

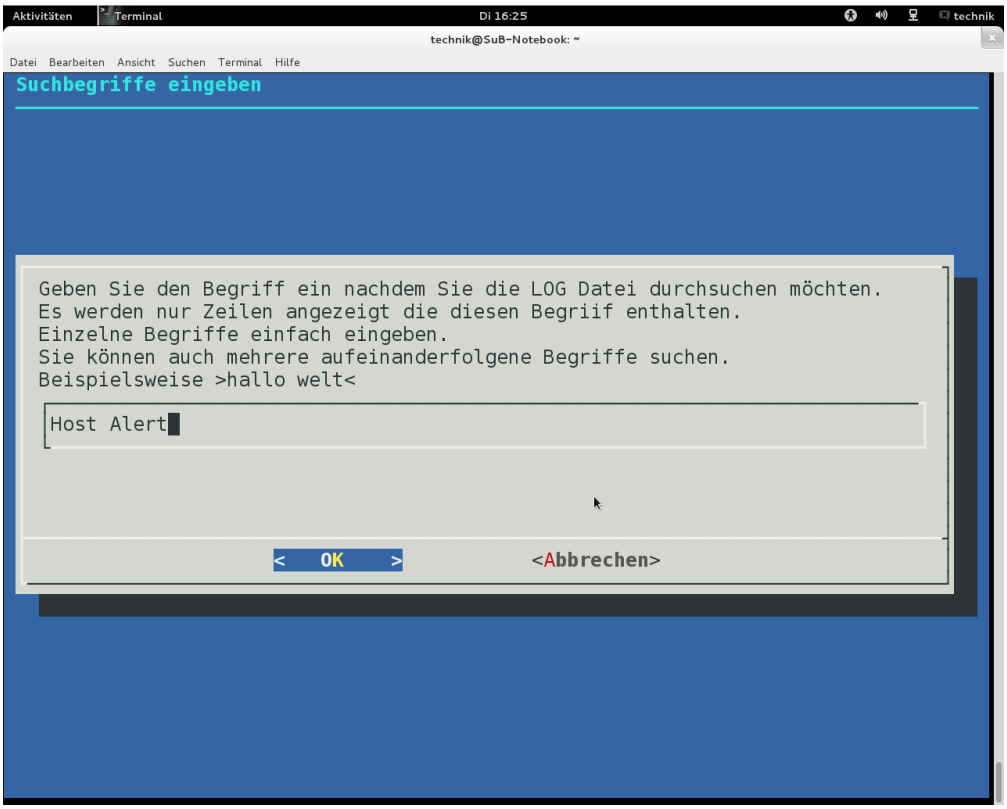
   Dieses kann im Falle von sehr langen Log Dateien sehr unkomfortabel sein da die gesamte Log Datei durchsucht werden.

   Um die Nagios Log Dateien gezielt zu durchsuchen, sollte man mit *„Ja“* bestätigen

2. Anwendung

   Wenn man mit Ja bestätigt hat wird ein Eingabe Feld geöffnet. Hier können einzelne Begriffe oder Strings angegeben werden.

Es können einzelne Wörter oder auch Strings eingegeben werden.



Groß und Kleinschreibung sind bei der Eingabe egal, Wörter werden in beiden Fällen gefunden. Es kann auch (*) als Wilcard benutzt werden, aber es darf nur am Ende eines Begriff gesetzt werden, in Strings kann es nicht verwendet werden:

HOS* = ok

*OST = nicht möglich

HOST A* = nicht möglich

Bei Strings ist zwar Groß- und Kleinschreibung egal, aber ein String muss auch exakt so vorkommen.

So gibt es Beispielsweise den String „HOST ALERT“, um diesen zu finden, muss er in der Log vorhanden sein.

Suchmethoden:

„Host alert“ = ok
„Host-alert“ = nicht möglich
„Hostalert“ = nicht möglich
„host ale“ = ok
„host a“ = ok (würde aber auch „HOST AND“ ausgeben.)

Würd nichts ausgegeben so ist es auch möglich, das Begriff oder String nicht in der Log vorhanden ist.

3. Sinnvolle Suchbegriffe

   Sinnvoll bei der suche können viel Begriffe und Strings sein:

   HOST = Zeigt alle Meldungen zu Systemen an.

   SERVICE = Zeigt alle Meldungen zu Diensten an.

   ALERT = Zeigt alle Alarmmeldungen an

   WARNING = Zeigt alle Warnmeldungen an

   NOTIFICATION = Zeigt die Wiederherstellung eines Dienstes oder Systems an

   „HOST ALERT“ = Zeigt alle System Alarmmeldungen an.

   „SERVICE ALERT“ = Zeigt alle Alarmmeldungen für Dienste an

   (Kombination auch mit WARNING und NOTIFICATION möglich)

   STATE = Zeigt letzte Statusmeldung an

   „SERVICE STATE“ = Zeigt letzte Statusmeldung von Diensten an

   „HOST STATE“ = Zeigt letzte Statusmeldung von Systemen an

   PING = Zeigt alle Ereignisse zur PING Überwachung an

   DOWN = Zeigt nicht erreichbare Systeme an

   Notify = Zeigt abgesetzte Meldungen an

   Printer = Zeigt alle Ereignisse zum System Printer an (es kann jedes System eingegeben werden.)

   SSH = Zeigt jede Meldung zum Dienst SSH an.

   „OCT 20“ = Zeigt alle Ereignisse vom 20 Oktober an

Man findet noch weitere Möglichkeiten dazu sollte man sich die Nagios Log einfach mal genau durchlesen.