

Betriebsanleitung Nagios-Box

Inhaltsverzeichnis:

1. Einleitung	Seite 2
1.1. Software	Seite 2
1.2. Hardwareanforderungen	Seite 3
2. Systemstart und Login	Seite 4
2.1. Einleitung	Seite 4
2.2. Login am System	Seite 5
2.3. Login via SSH	Seite 6
3. Erstmöglicher Start der Nagios Box	Seite 7
3.1. Ersteinrichtung starten	Seite 7
3.2. Systemzeit setzen	Seite 10
3.3. IP Konfiguration	Seite 12
4. Einrichtung und Administration der Nagios-Box	Seite 15
4.1. Anmeldung	Seite 15
4.2. Das Haupt-Menü	Seite 15
4.3. Administrationsprogramme	Seite 16
5. Auswertungen auf der Nagios-Box	Seite 47
6. Fehlerbilder und Lösungen	Seite 55
Anhang 1	Anleitung-Web-Oberfläche-Nagios
Anhang 2	Anleitung Auswertung-Nagios-Log

1. Einleitung

1.1 Die Software

Die Nagios-Box ist eine Ansammlung von Tools die zur Netzwerkanalyse in Netzwerken eingesetzt wird. Das Betriebssystem der Nagios-Box ist ein Debian 7 Linux System.

Das Kernprogramm zur Analyse von Netzwerken ist das Programm Nagios. Nagios unterliegt der GPL (General Public License) von GNU (GNU is NOT UNIX). Das Programm ist Quelloffen und auch im gewerblichen Gebrauch nicht Lizenzpflichtig.

Nagios überwacht Netzwerkgeräte, das können neben Computer alle Systeme sein die über eine eigene IP-Adresse besitzen, also bspw. Auch Router, Switches, Drucker, Kartenterminals etc. Nagios verfolgt dabei zwei Strategien, zum einen die Host-Überwachung zum anderen die Service-Überwachung. Die Host-Überwachung überprüft mit einem Keep-Alive-Test (ICMP), ob Systeme generell erreichbar sind. Die Service-Überprüfung überwacht, ob Dienste und Zustände von Systemen, beispielsweise läuft der Web-Server oder hat die Systemfestplatte noch genügend freien Speicherplatz. Nagios kann dabei pro-aktiv wie auch reaktiv benutzt werden. Pro-aktiv bedeutet, Nagios weist automatisch auf Fehler (per Mail, SMS etc.) hin. Reaktiv bedarf dagegen der eigenen Kontrolle. Besonders wichtig ist das permanente Aufzeichnen von Daten, so lassen sich Zustände bis zu einem Zeitraum von mehreren Jahren dokumentieren. Nagios bietet für die Auswertung mehrere Möglichkeiten. Im System selber lassen sich LOG-Dateien analysieren. Zusätzlich gibt es eine Web-Oberfläche, die sich über jeden im Netzwerk befindlichen Browser anzeigen lässt. Nagios selber benötigt dafür keine grafische Umgebung. In der Web-Oberfläche lassen sich die aktuellen Zustände ablesen, sowie die LOG Dateien auswerten. Zusätzlich gibt es eine rdd Schnittstelle die Graphen anlegt, diese lassen sich auch über den Browser als PDF exportieren.

Zusätzlich zu Nagios befindet sich auch das Programm NMAP auf dem System. NMAP unterliegt ebenfalls unterliegt der GPL von GNU. Auch dieses Programm ist Quelloffen und im gewerblichen Gebrauch ebenfalls nicht Lizenzpflichtig.

NMAP scannt Netzwerke, es sucht dabei nach erreichbaren Systemen, überprüft Routen und kann auch Systeminformationen auslesen, wie beispielsweise offene Ports, Betriebssysteme, Mac-Adressen und Hersteller IDs. **!! Der Gebrauch von NMAP ist daher nur in privaten Netzwerken erlaubt !!**

In der Nagios-Box lassen sich zusätzlich spezielle Dauerpings einrichten, die je nach Wunsch alle, nur erfolgreiche oder nur erfolglose Pings aufzeichnet.

Nagios und das Nagios-Logo sind in den USA eingetragene Warenzeichen von Ethan Galstad

1.2. Hardware-Anforderungen

Die gesamte Nagios-Box kann als Image auf ein System gespielt werden.

Das Zielsystem benötigt (minimum):

- 32 oder 64 Bit x86 CPU
- min 2 GB Ram
- min 80 GB HD
- Vesa kompatible Grafikkarte mit VGA,DVI oder HDMI Ausgang
- Eine 100 oder 1000 Mbit LAN-Netzwerkschnittstelle (weitere LAN Schnittstellen sollten zur Vermeidung von Fehlern abgeschaltet werden)
- 2 x USB 2.0 Schnittstelle
- Bios darf nicht Passwort geschützt sein, damit sich die Systemzeit anpassen lässt

2. Systemstart und Login

2.1 Einleitung

Es gibt drei Varianten sich in die Nagios-Box einzuloggen.

- Direkt am System
- Via SSH (Secure SHell) auf Port 2222

Das System verfügt über eine grafische und eine nichtgrafische Administrationsoberfläche.

Die grafische Oberfläche zu Problemen bei einigen Windows SSH-Clients, **Putty beispielsweise muss wie folgt angepasst werden:** Unter **Window -> Translation** sollte im **Remote character set UTF-8** ausgewählt werden und unter **Connection -> Data** sollte im **Terminal-type string linux** eingetragen werden.

Die nichtgrafische Oberfläche steht grundsätzlich zur Verfügung.

In dieser Anleitung wird nur die grafische beschrieben. Sie kann aber genauso für die nichtgrafische verwendet werden. Die System- und Menu-Abläufe sind identisch, nur die Form der Eingabe von Daten unterscheidet sich. Im Nagios System selbst ist eine Online-Hilfe verfügbar für die nichtgrafische Oberfläche.

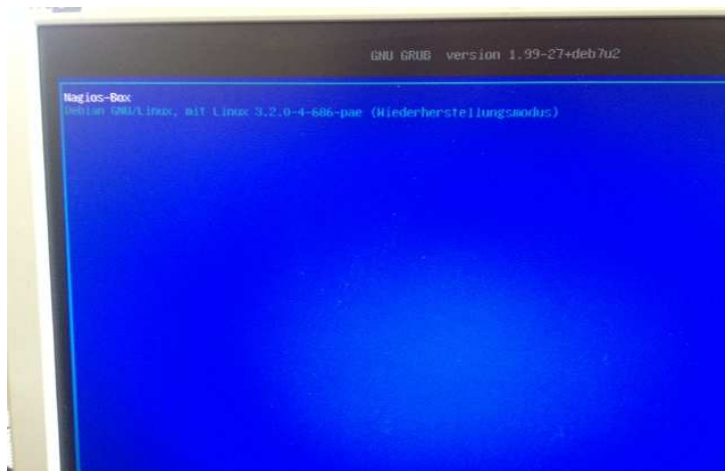
Anmerkung: Linux ist ein sogenanntes Key-Sensitive Betriebssystem, das bedeutet es unterscheidet zwischen Klein- und Großschreibung. Bitte immer Werte genauso eingeben wie sie geschrieben sind!

2.2 Login am System

Nachdem die Nagios-Box aufgestellt wurde, muss nun ein Bildschirm und eine Tastatur angeschlossen werden. Danach wird die Nagios-Box eingeschaltet.

Es erscheint folgender Bildschirm:

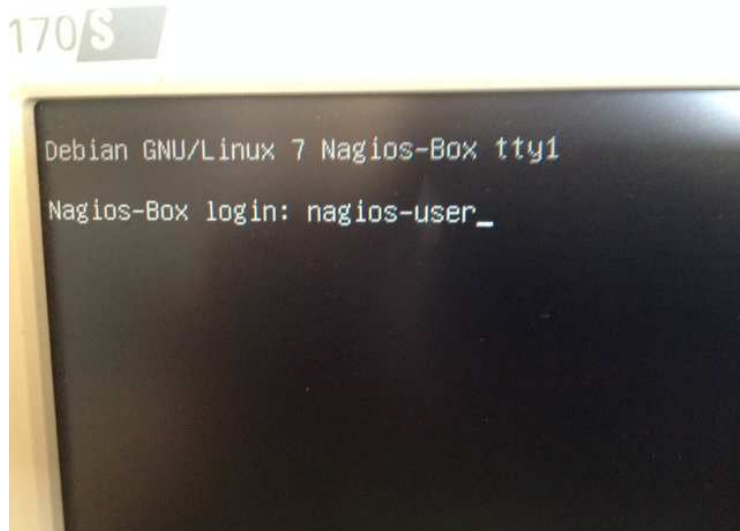
Hier bitte nichts eingeben das System startet automatisch



Nachdem das System hochgefahren ist erscheint das Login:



Bitte den Loginnamen „nagios-user“ eingeben und Enter-Taste drücken:



Danach das Passwort: 123456 eingeben und erneut die Enter-Taste drücken:
Bitte bei Punkt 4 Fortsetzen.

2.3 Login via SSH von anderem System

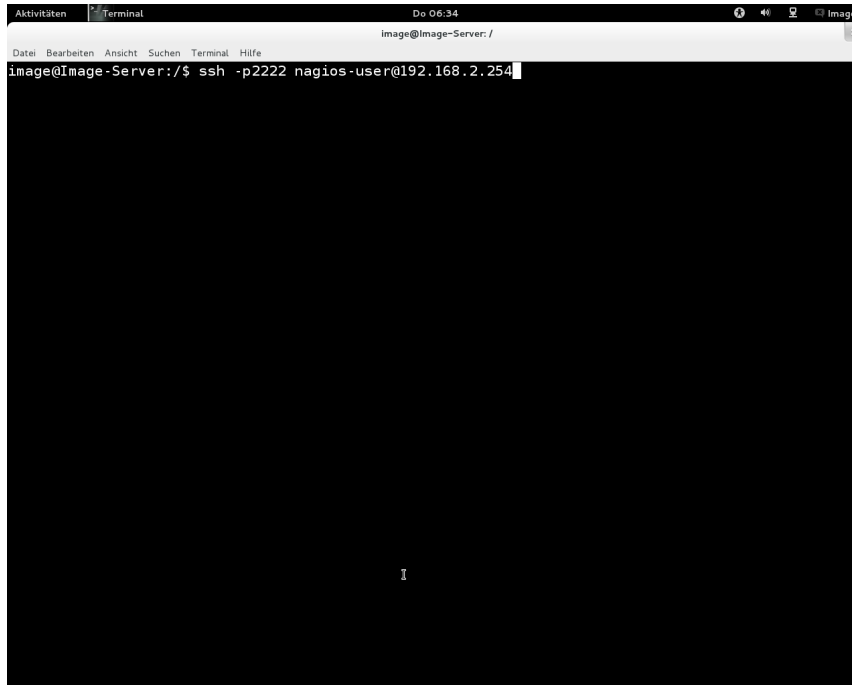
Hierbei muss die Nagios-Box nur im selben Netzwerk befinden. Das System bitte einschalten und ca. eine Minute warten bis das System hochgefahren ist.

Die Nagios-Box hat vor der Einrichtung die IP-Adresse **192.168.2.254**

Bitte Terminalprogramm öffnen (Putty (Windows) Shell Linux).

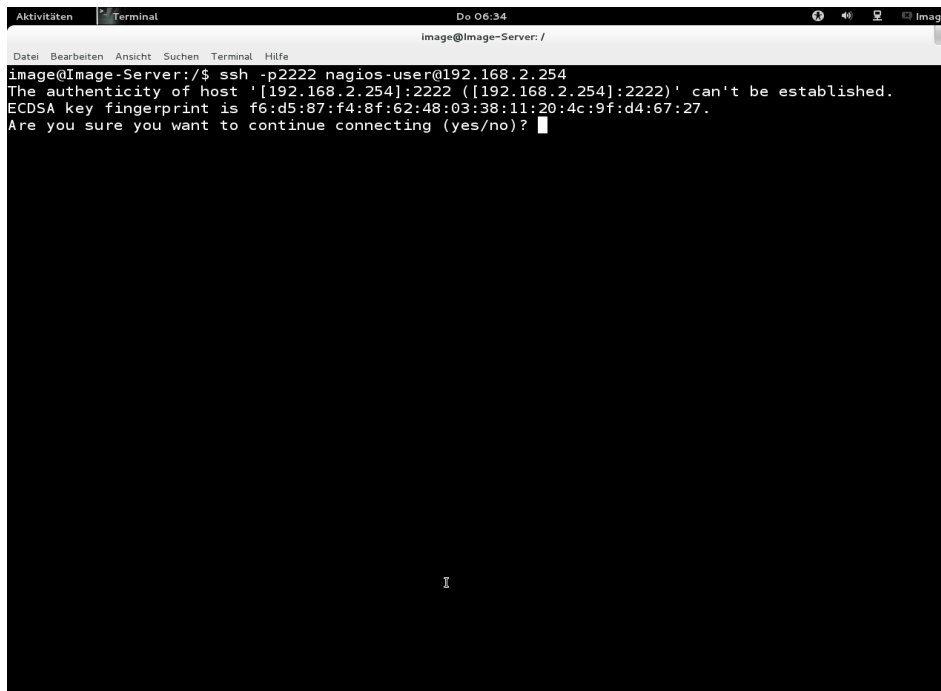
Anleitung Nagios-Box

im Terminal folgendes eingeben: `ssh nagios-user@192.168.2.254`



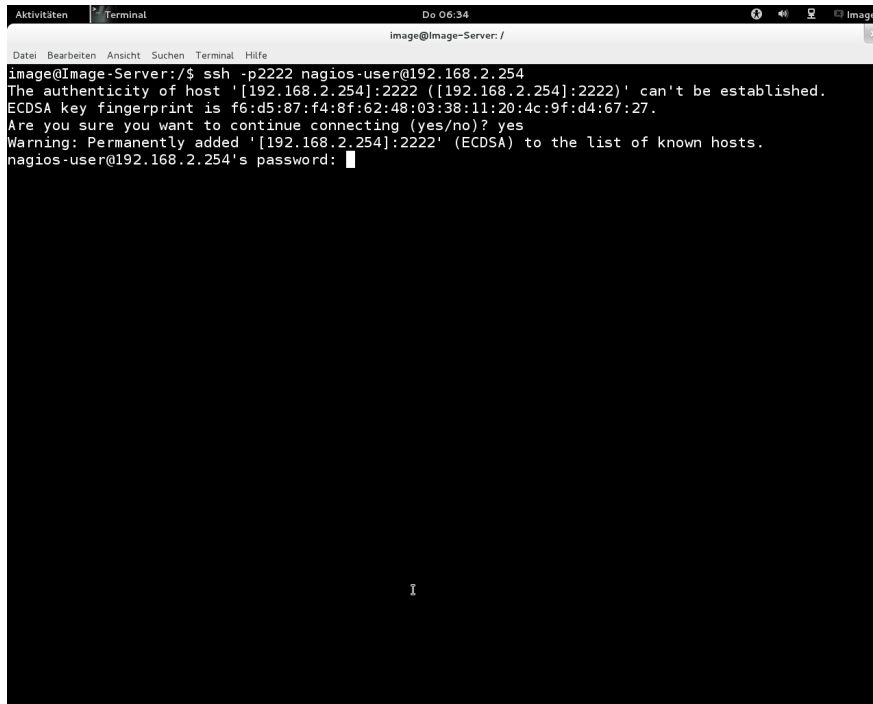
(Sollte ein Connection timed out kommen ist die Nagios-Box nicht resetet worden und besitzt eine unbekannte IP-Adresse, dann bitte anmelden wie unter Punkt 3.2)

Normalerweise wird bei der Erstanmeldung eines Users ein Fingerprint verlangt, bitte yes eingeben und anschließend der Enter-Taste bestätigen



Dann bitte das Passwort: `123456` eingeben und mit Enter bestätigen.

Anleitung Nagios-Box



```
image@Image-Server: /
Datei Bearbeiten Ansicht Suchen Terminal Hilfe
image@Image-Server:/$ ssh -p2222 nagios-user@192.168.2.254
The authenticity of host '[192.168.2.254]:2222 ([192.168.2.254]:2222)' can't be established.
ECDSA key fingerprint is f6:d5:87:f4:8f:62:48:03:38:11:20:4c:9f:d4:67:27.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[192.168.2.254]:2222' (ECDSA) to the list of known hosts.
nagios-user@192.168.2.254's password: █
```

Folgende User sind im System hinterlegt:

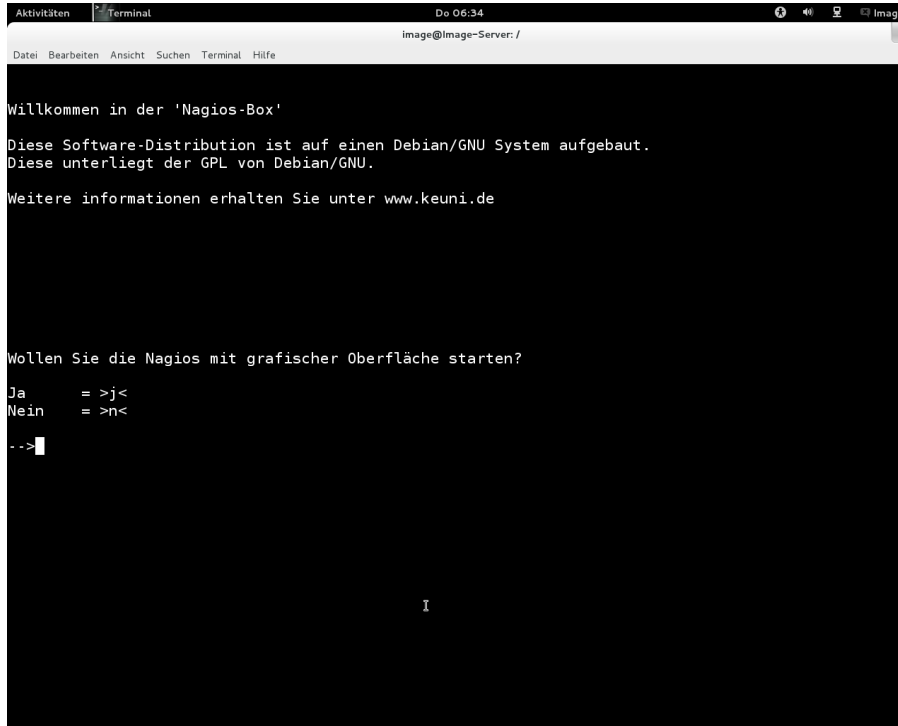
Nagios-user	Passwort 123456
Nagios-dummy	Passwort 123456
Root	Passwort 123456
Nagiosadmin	Passwort 123456 (Anmeldung nur auf der Weboberfläche)

3. Erstmaliges starten der Nagios-Box IP-Konfiguration

3.1 Ersteinrichtung

Ist die Nagios-Box nicht eingerichtet, ist wie folgt vorzugehen:

Wir bestätigen mit j das Starten der grafischen Oberfläche:

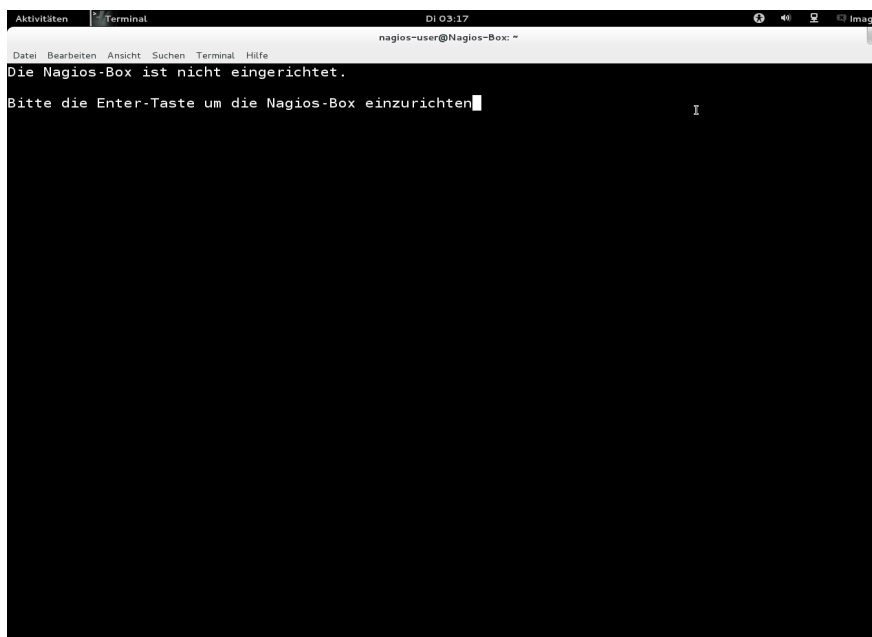


```
image@Image-Server: /
Datei Bearbeiten Ansicht Suchen Terminal Hilfe

Willkommen in der 'Nagios-Box'
Diese Software-Distribution ist auf einen Debian/GNU System aufgebaut.
Diese unterliegt der GPL von Debian/GNU.
Weitere Informationen erhalten Sie unter www.keuni.de

Wollen Sie die Nagios mit grafischer Oberfläche starten?
Ja      = >j<
Nein    = >n<
-->
```

Die folgende Meldung mit Enter bestätigen:



```
nagios-user@Nagios-Box: ~
Die Nagios-Box ist nicht eingerichtet.
Bitte die Enter-Taste um die Nagios-Box einzurichten.
```

Anleitung Nagios-Box

!!! WICHTIG Sollte nicht diese Meldung bei der ersten Anmeldung sondern das Haupt-Menü erscheinen (siehe Punkt 5.1 – 5.2) Ist die Nagios-Box nicht zurückgesetzt worden und enthält noch alte Daten. In diesem Fall muss die Nagios-Box zuerst resetet werden siehe **Menu Punkt 19**.

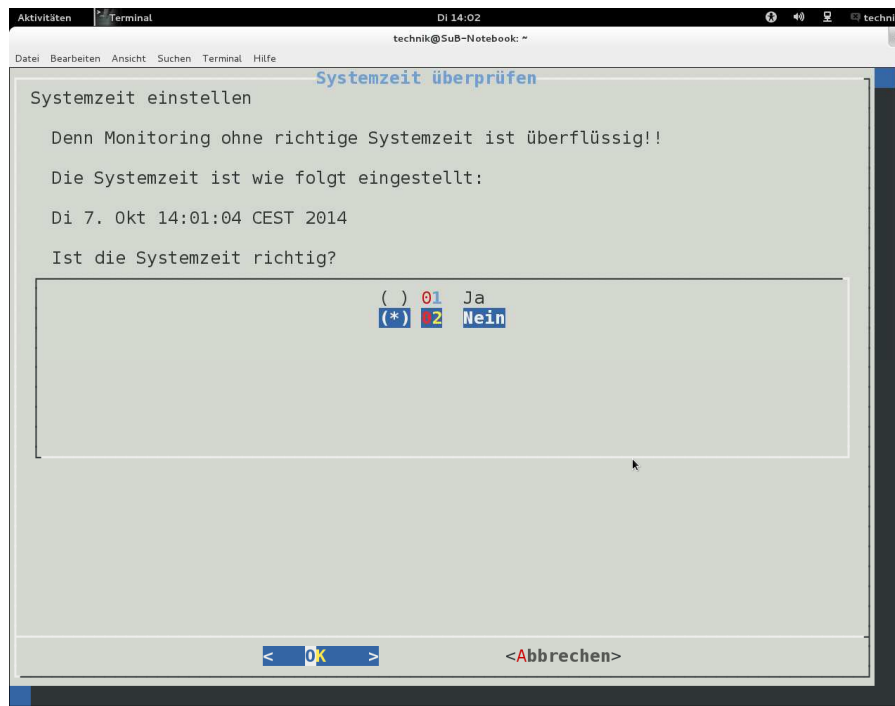
!! Achtung das beste Monitoring ist nichts wert, wenn die Systemzeit falsch ist. Alle aufgezeichneten Daten lassen sich nicht auswerten, wenn die Zeiten falsch sind. !!

Im nächsten Fenster wird angegeben ob die Systemzeit stimmt.

Dazu bitte mit den Pfeiltasten (hoch und runter) auf das gewünschte Feld wechseln. DIE MARKIERUNG FINDET MIT DER SPACE-TASTE STATT, NICHT DAS BLAU HINTERLEGTE FELD IST ANGEWÄHLT, SONDERN DAS MIT DEM STERNCHEN!! Bitte auch bei allen folgenden Auswahlen darauf achten. In diesem Fenster ist beispielsweise NEIN voreingestellt.

Mit den Pfeiltasten (rechts links) lässt sich zwischen OK und ABBRECHEN wechseln. Die Auswahl von ABBRECHEN ist aber zu keiner Zeit nötig.

Nachdem die Auswahl getroffen wurde bitte Enter-Taste drücken.

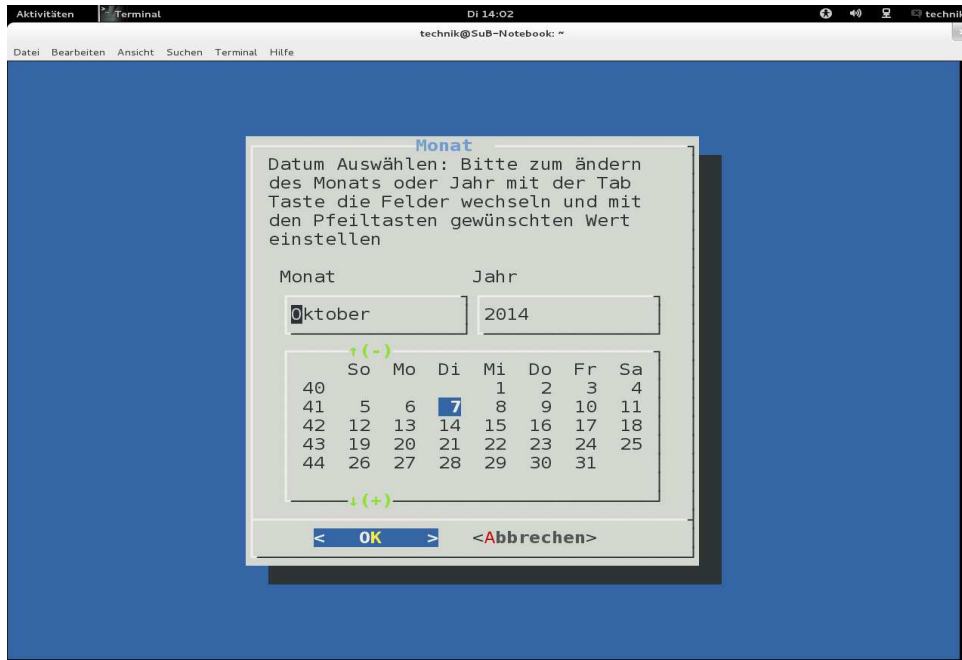


Anleitung Nagios-Box

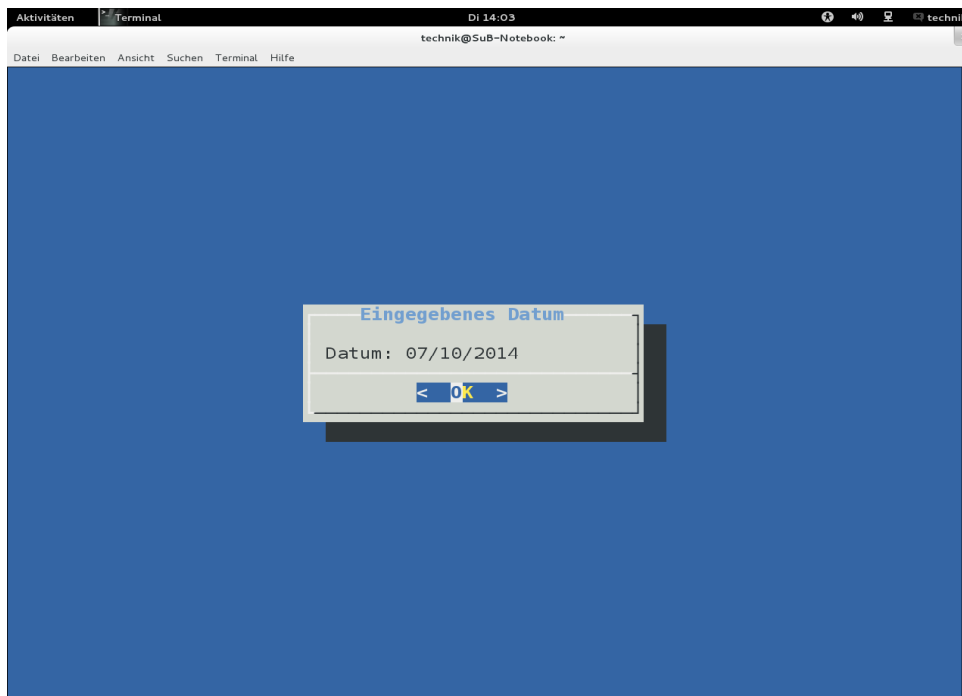
3.2 Einstellen der Systemzeit

Die folgende Meldung: Die Systemzeit ist falsch mit Enter bestätigen.

Das folgende Fenster dient zur Einstellung des Datums, die Felder können mit der TAB-Taste gewechselt und die Werte mit den Pfeiltasten verändert werden. Ist das richtige Datum ausgewählt mit Enter bestätigen.

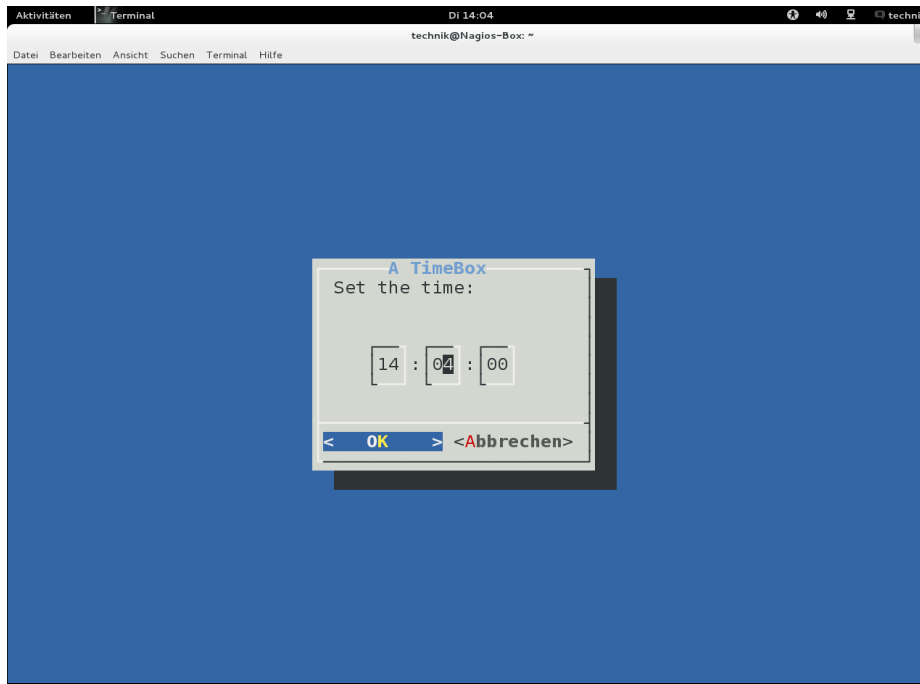


Kontrollanzeige mit Enter-Bestätigen:

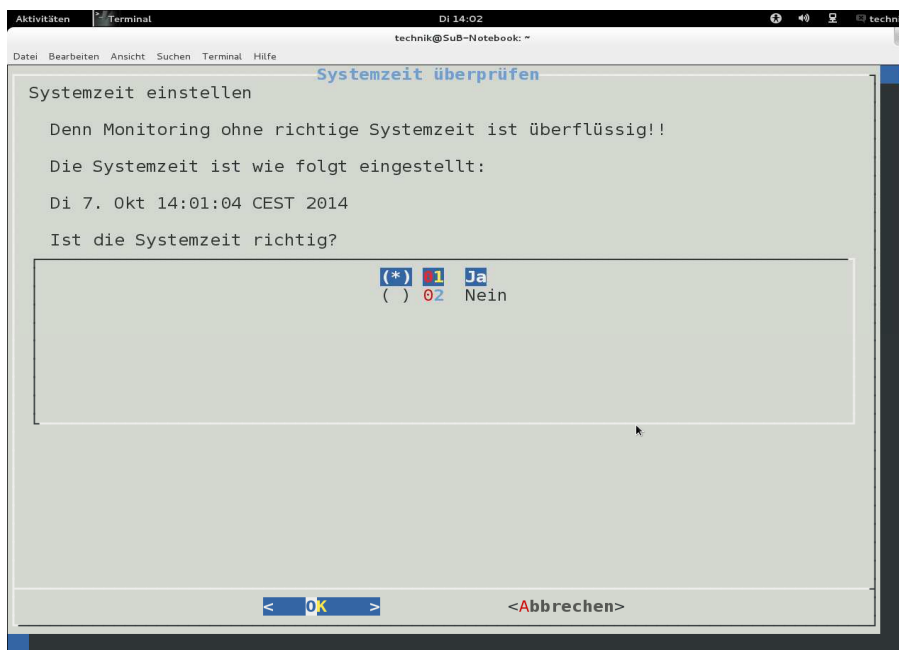


Anleitung Nagios-Box

Danach wird die Uhrzeit (Minutengenau!) eingestellt. Auch hier gilt, die Felder können mit der TAB-Taste gewechselt und die Werte mit den Pfeiltasten verändert werden und mit Enter bestätigt.

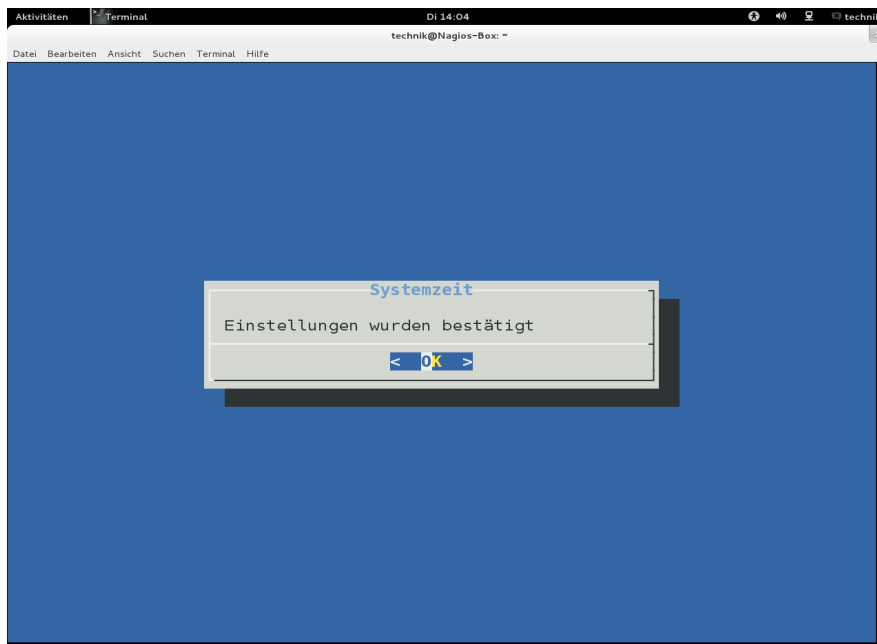


Es wird wieder das Fenster Systemzeit überprüfen, diesmal auf Ja wechseln und mit der Space-Taste markieren. Danach Enter drücken.



Anleitung Nagios-Box

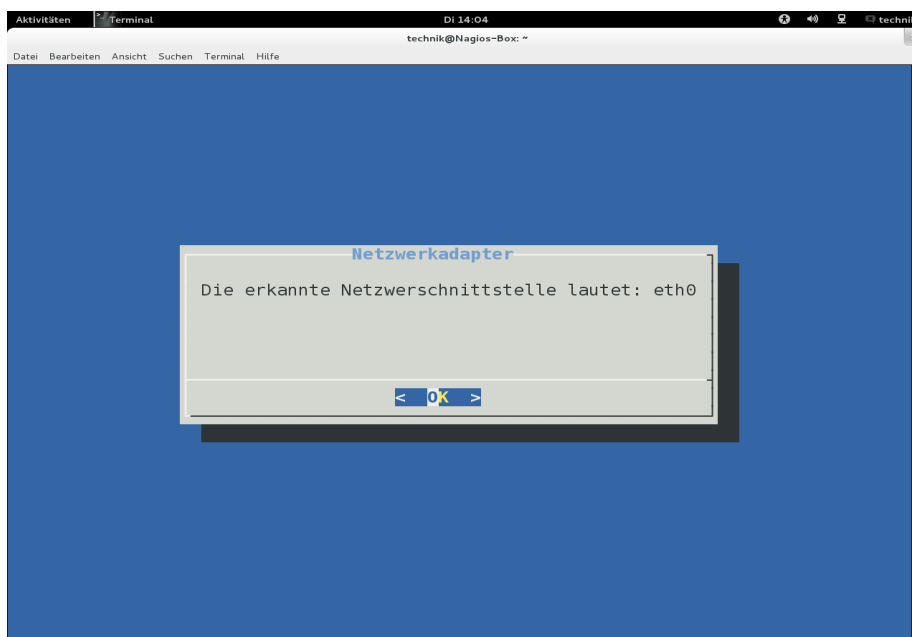
Bestätigungsdialog mit Enter schließen.



3.3 IP Konfiguration

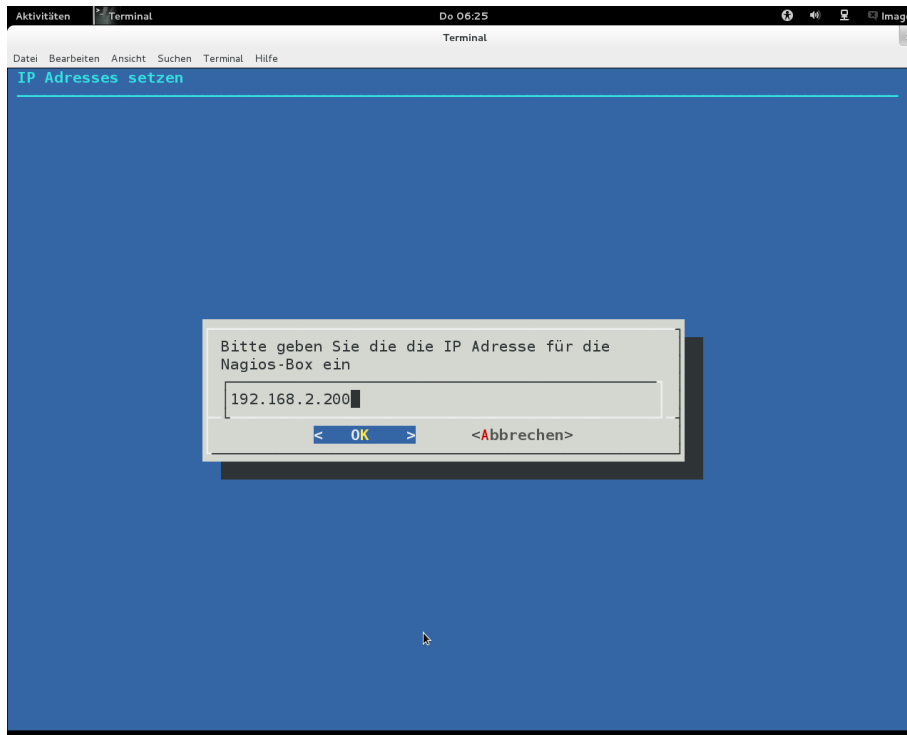
Anmerkung: Linux benennt Netzwerk nach TYP und NUMMER so lautet die erste Netzwerkschnittstelle vom Typ Ethernet: eth0 die zweite eth1 usw.

Danach wird die Netzwerkschnittstelle ermittelt:

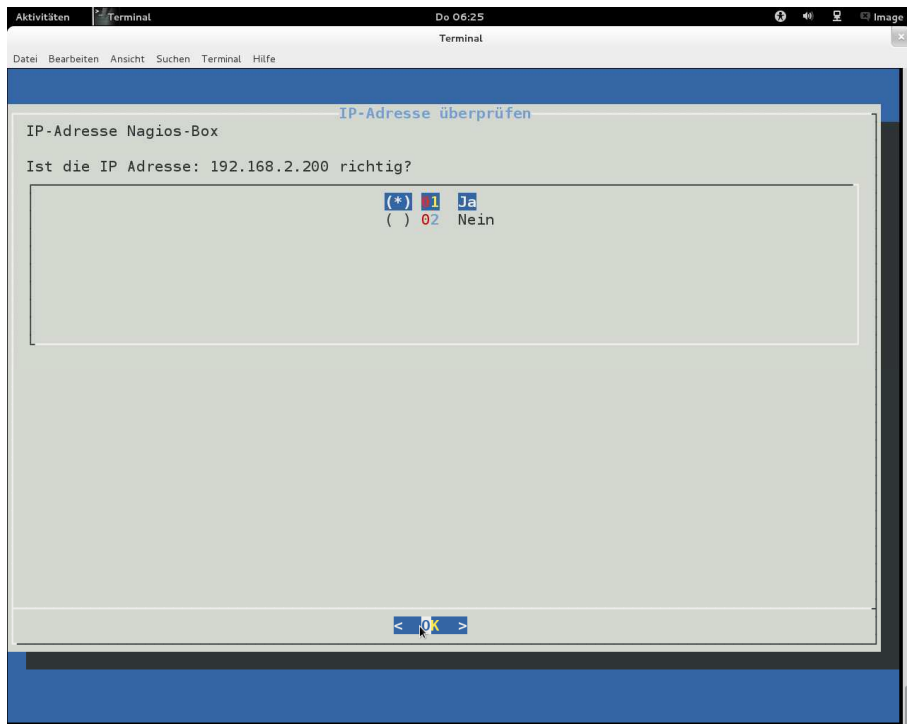


Anleitung Nagios-Box

Im nächsten Fenster wird die IP-Adresse die die Nagios-Box erhalten soll eingeben.

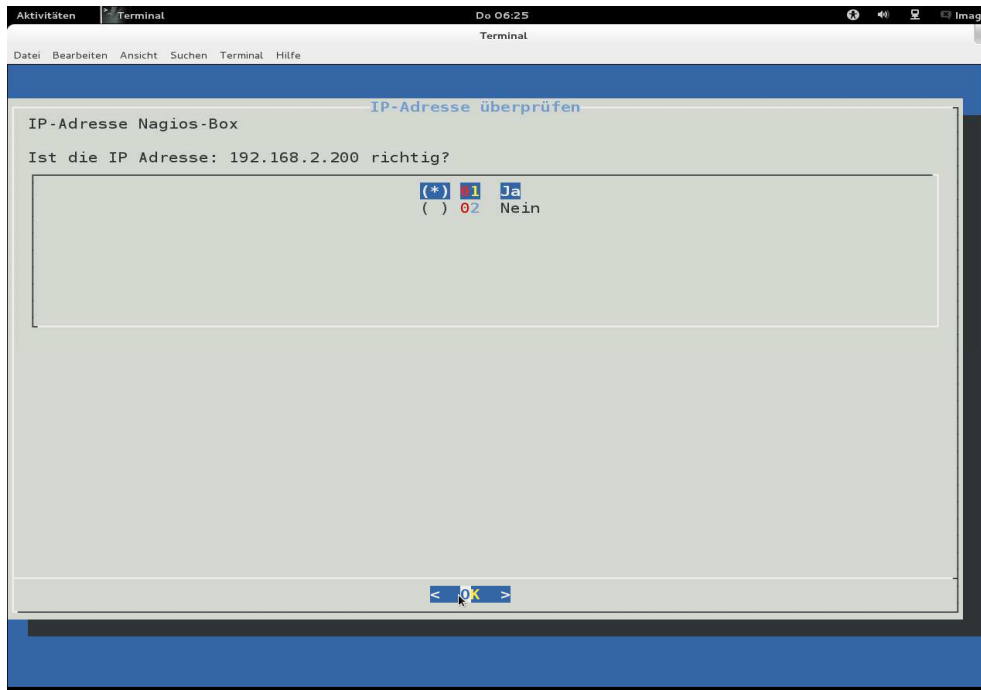


Danach bitte IP-Adresse überprüfen und wenn richtig mit Enter bestätigen oder erneut eingeben.



Anleitung Nagios-Box

Danach wird der im gleichen Netzbefindliche Gateway eingegeben. Bitte nur die letzte Ziffer der IP-Adresse:

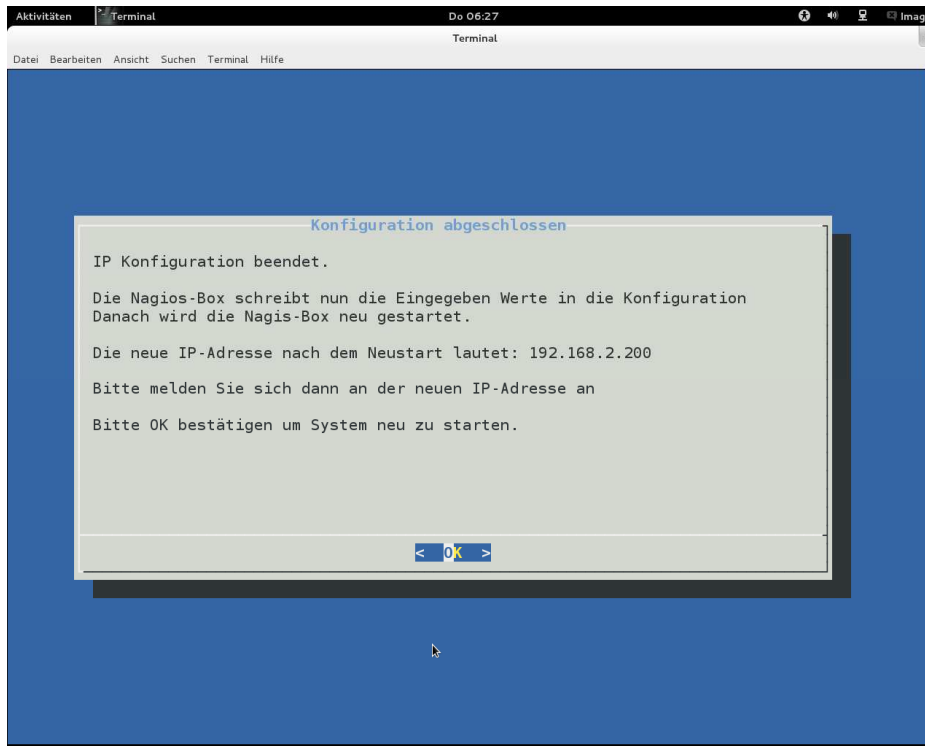


Die Eingabe der Gateway Adresse bestätigen:



Anleitung Nagios-Box

Zum Abschluss erscheint folgende Info-Box nach Bestätigung mit Enter wird die Box neu gestartet:



Die IP-Installation ist damit beendet.

Nach dem Neustart muss bei der Anmeldung über SSH an die Nagios-Box die neue IP Adresse verwendet werden.

4. Einrichtung und Administration der Nagios-Box

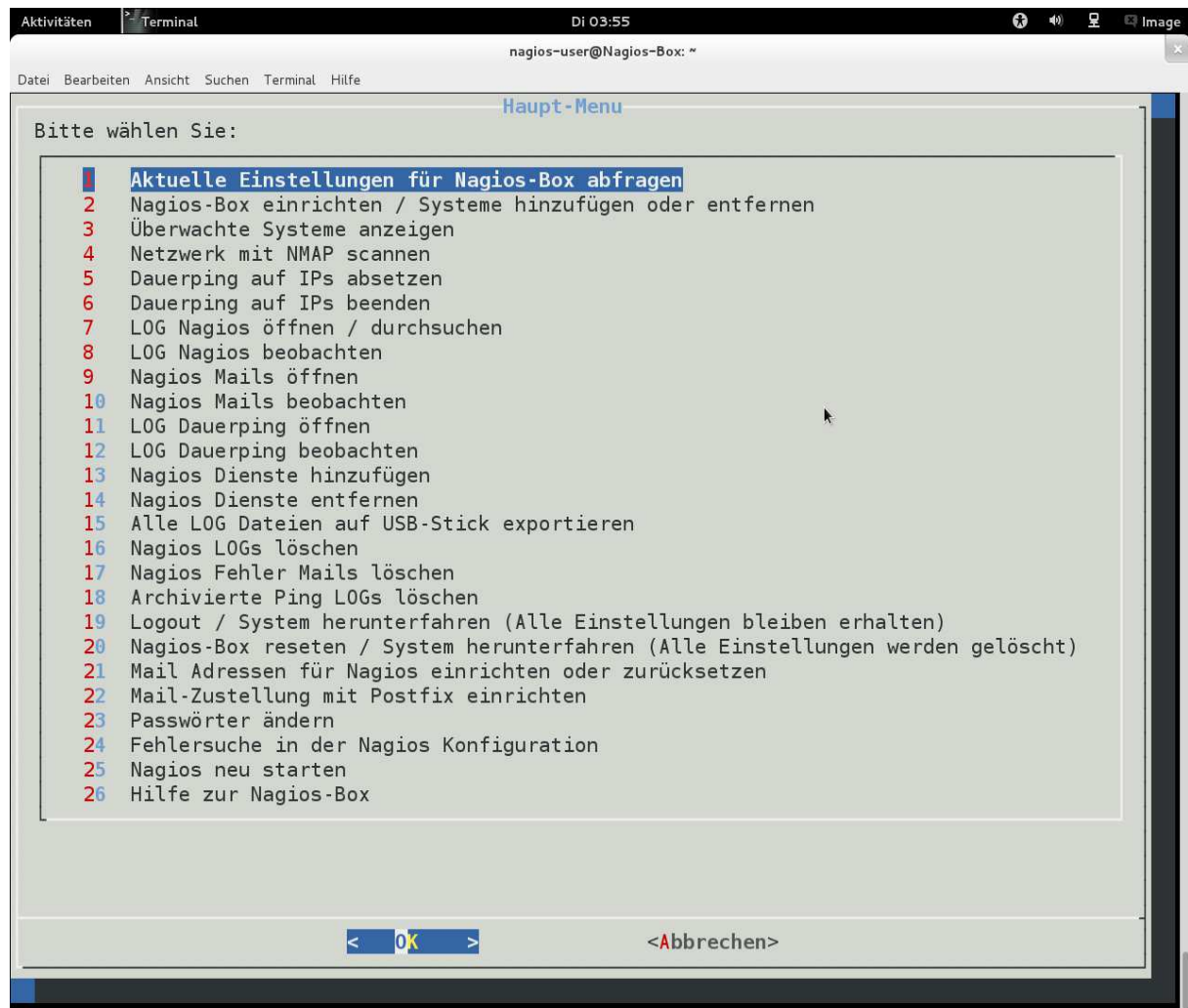
4.1 Anmeldung

Die Anmeldung erfolgt wie unter Punkt 3.2 bzw. 3.3 (mit neuer IP-Adresse) am System nach Auswahl der grafischen Oberfläche und der Willkommensnachricht erscheint das Haupt-Menü:

4.2 Das Haupt-Menü

Im Haupt-Menü sind alle Programme und Funktionalitäten hinterlegt. Dabei gibt es Administrations- und Auswertungsprogramme. Zuerst werden alle Administrations Programme erläutert.

Die Auswahl erfolgt über die Pfeil auf und ab Tasten mit Enter wird die Auswahl aktiviert.

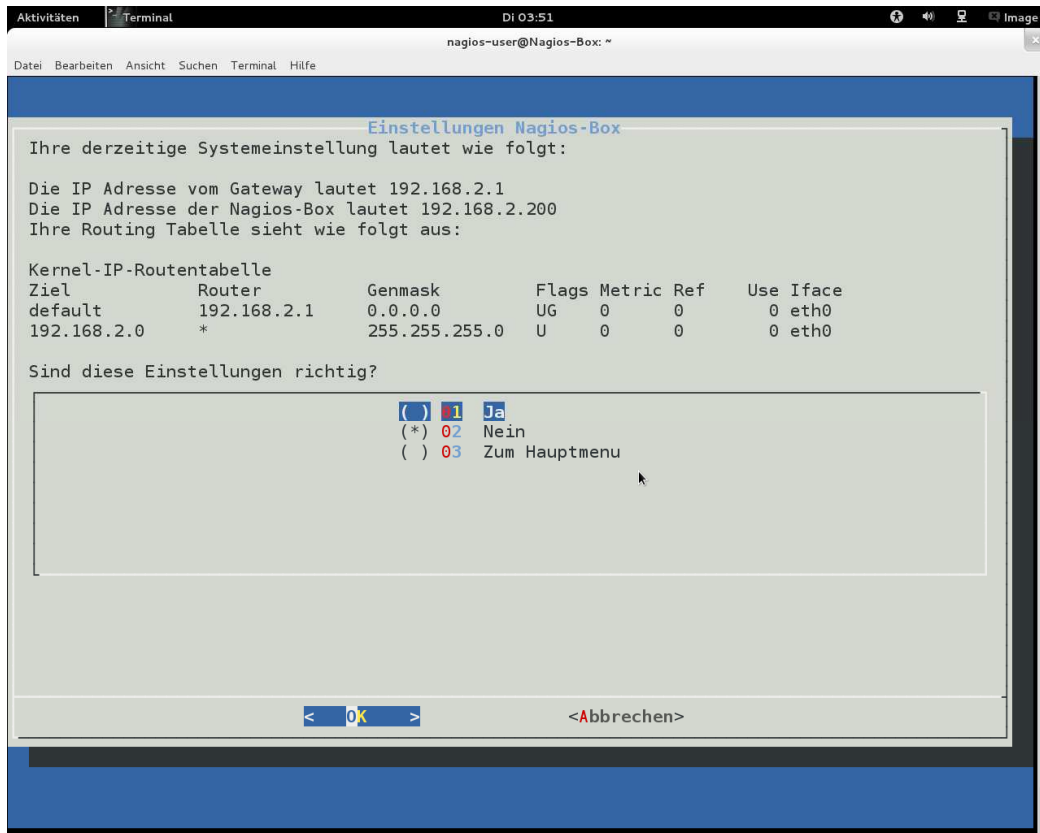


Anleitung Nagios-Box

4.3 Administrationsprogramme:

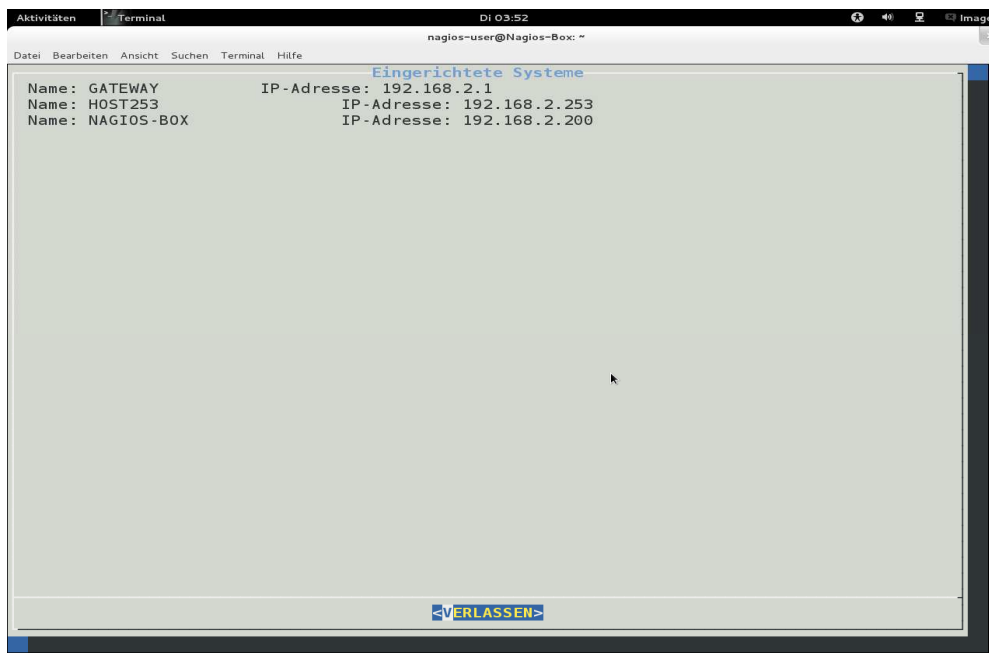
Menu Punkt 1: Aktuelle Einstellungen für Nagios-Box abfragen

Beim Aufruf des Menu Punkts erscheinen die aktuellen Systemeinstellungen:



Bestätigt man diese erscheint eine Info-Box *Einstellungen Bestätigt*

Nach drücken der Enter-Taste erscheinen die im Monitoring eingerichtet Systeme:



Anleitung Nagios-Box

Sollten noch keine Systeme eingerichtet sein erscheint eine Info-Box:

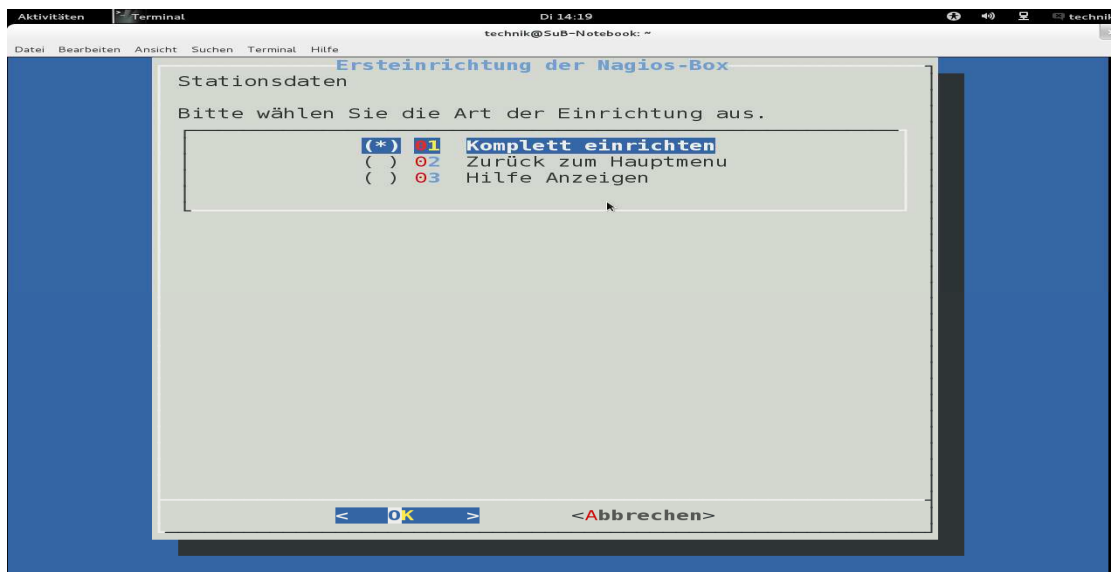
Es sind keine Systeme für das Monitoring hinterlegt

Durch Drücken der Enter-Taste gelangt man zurück ins Haupt-Menü

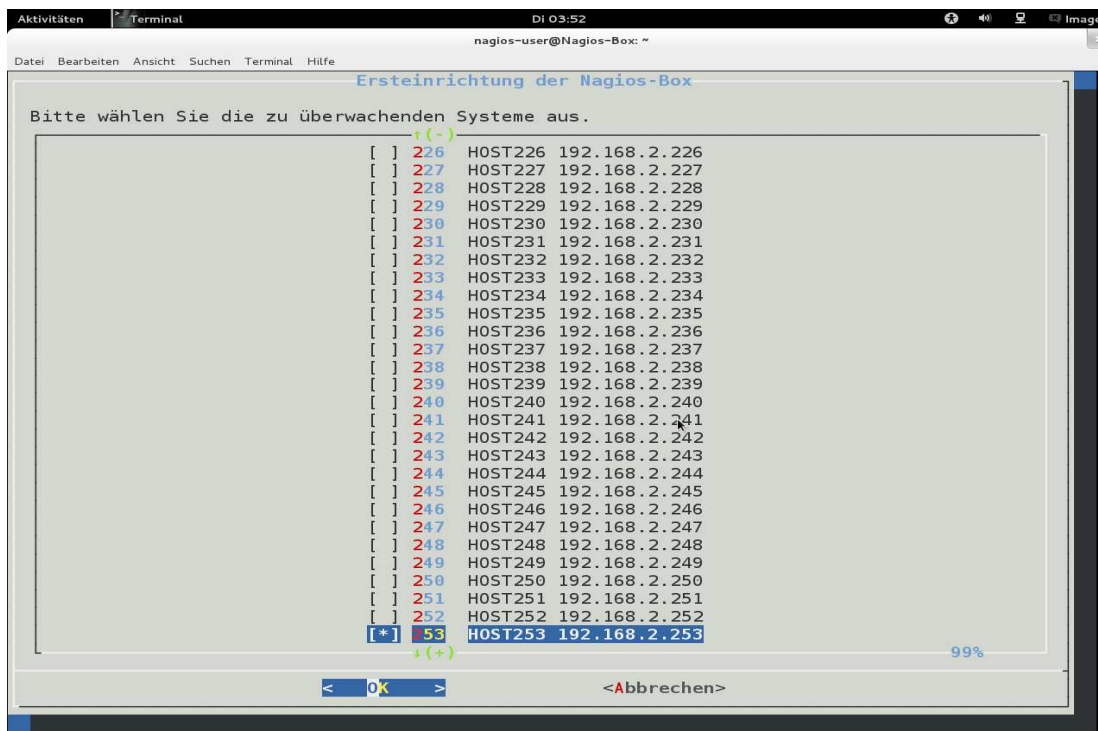
Menu Punkt 2: Nagios-Box einrichten / Systeme hinzufügen oder entfernen

Mit dem 2. Menu Punkt lassen sich die Systeme für das Monitoring festlegen. Es ist auch möglich Systeme wieder zu entfernen.

Bei der Ersteinrichtung erscheint folgendes Fenster:



Bestätigt man Komplette einrichten erscheint folgende Liste(nur im grafischen Modus):



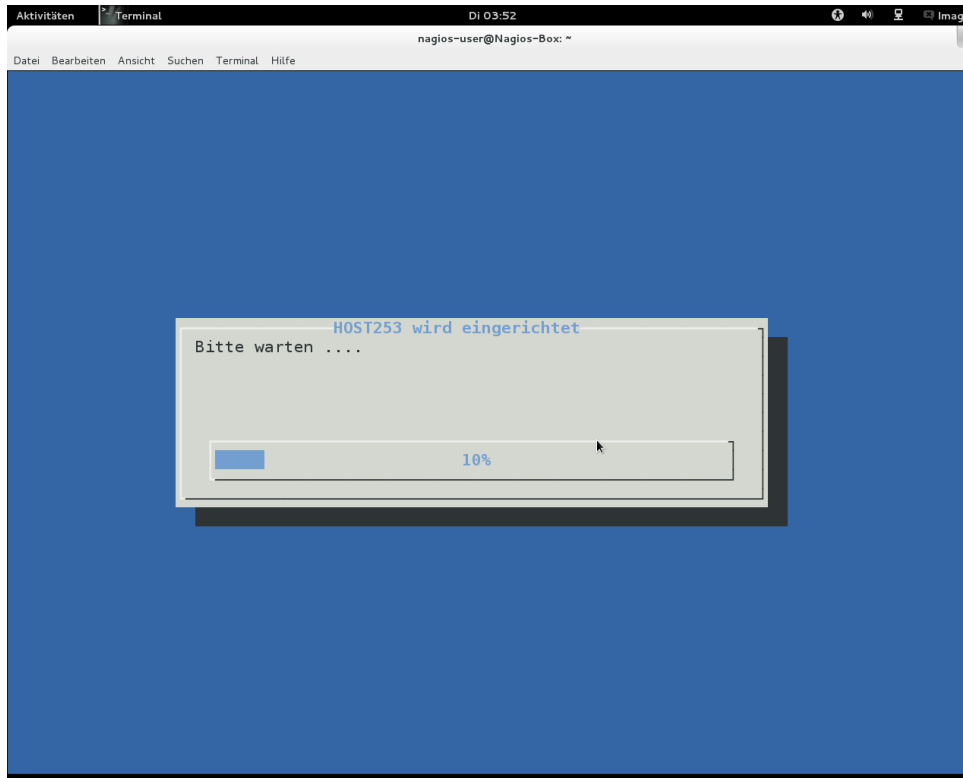
Anleitung Nagios-Box

Diese Liste enthält alle IP-Adressen des Subnetzes man kann auch kein System auswählen. Bitte nicht die Systeme der Nagios-Box selber oder des Gateways einrichten.

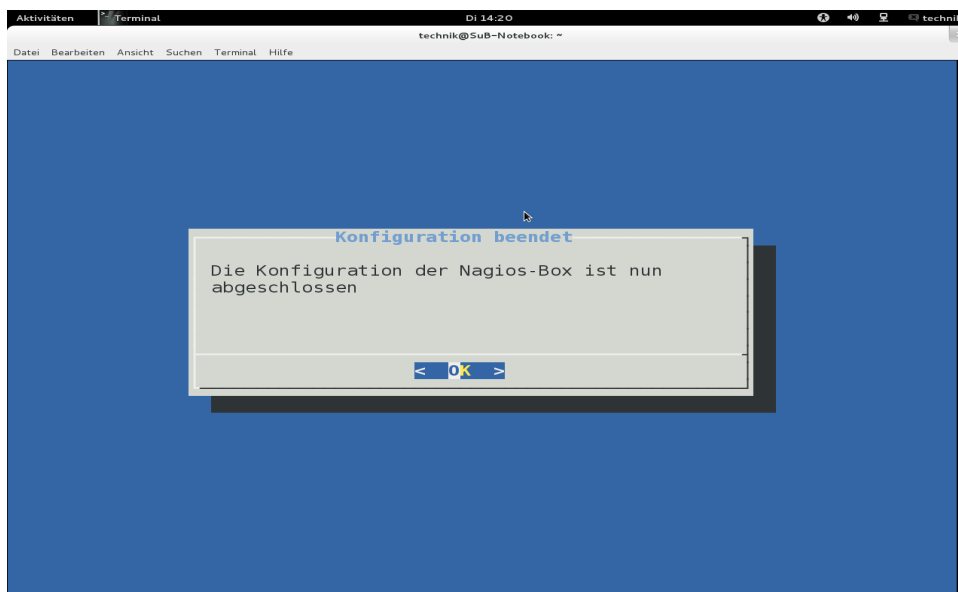
Mit den Pfeil Tasten hoch und runter navigiert man durch die Gesamtliste, mit der Space Taste können Systeme hinzu- oder abgewählt werden.

!!Achtung mit der Enter-Taste schließt man die Auswahl ab, diese Liste erscheint nur bei der Erstinstallation!! Also sorgfältig auswählen erspart die Nachpflege.

Mit der Bestätigung der Auswahl werden die Systeme eingerichtet:



Mit der Enter Taste wird die Konfiguration beendet:

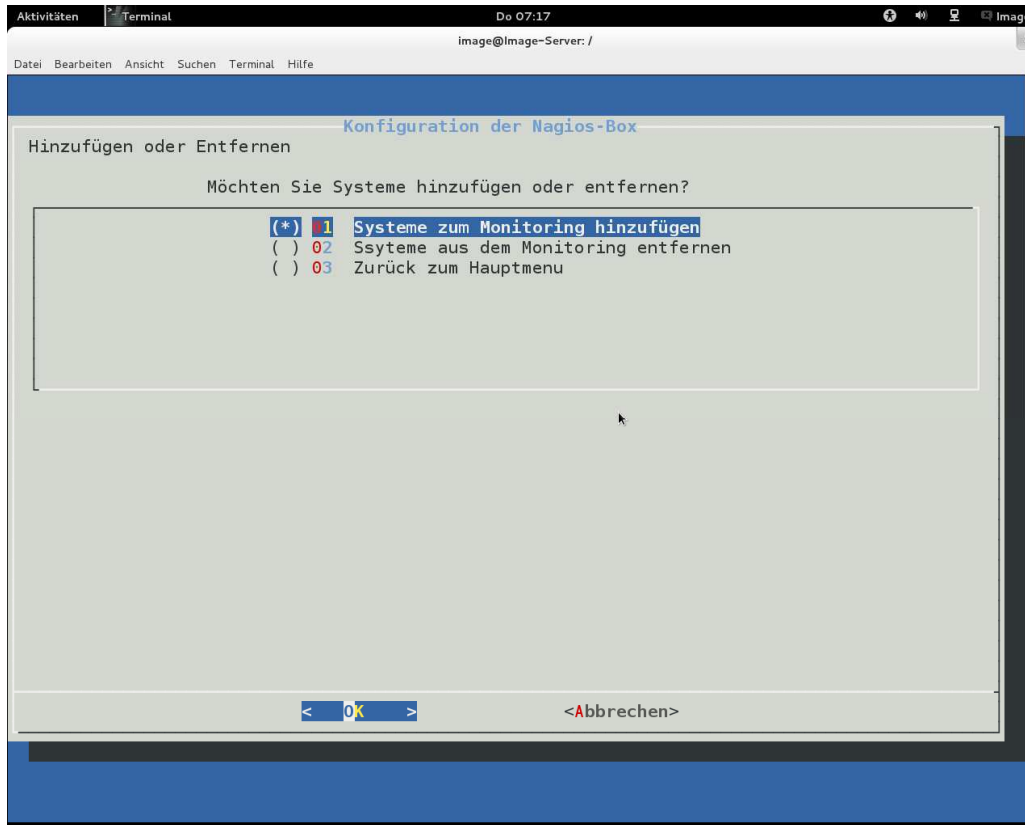


Anleitung Nagios-Box

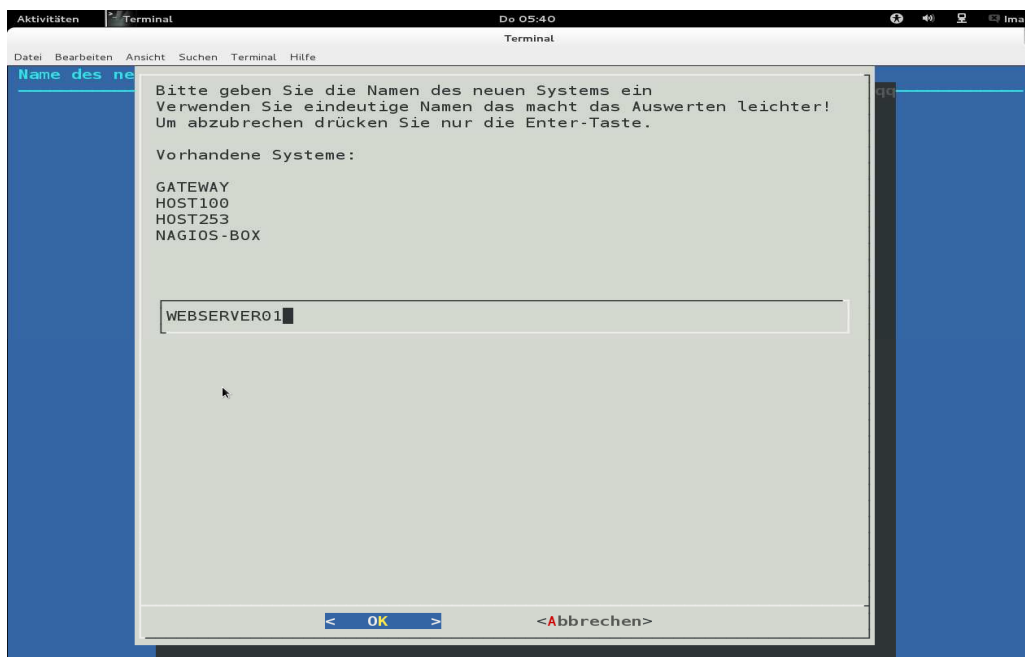
Man gelangt wieder ins Haupt-Menü:

Die Grundkonfiguration ist nun abgeschlossen. Auch wenn in der Liste kein System ausgewählt wurde, so werden die Nagios-Box und der Gateway selbstständig immer eingerichtet. Diese können auch später nicht aus dem Monitoring entfernt werden.

Ruft man nach der Erstinstallation den Menu Punkt 2 auf erscheint immer folgendes Fenster: (sofern mehr Systeme als die Grundsysteme installiert sind).



Wird hinzufügen ausgewählt, bitte den Namen des neuen Systems eingeben und mit Enter bestätigen:

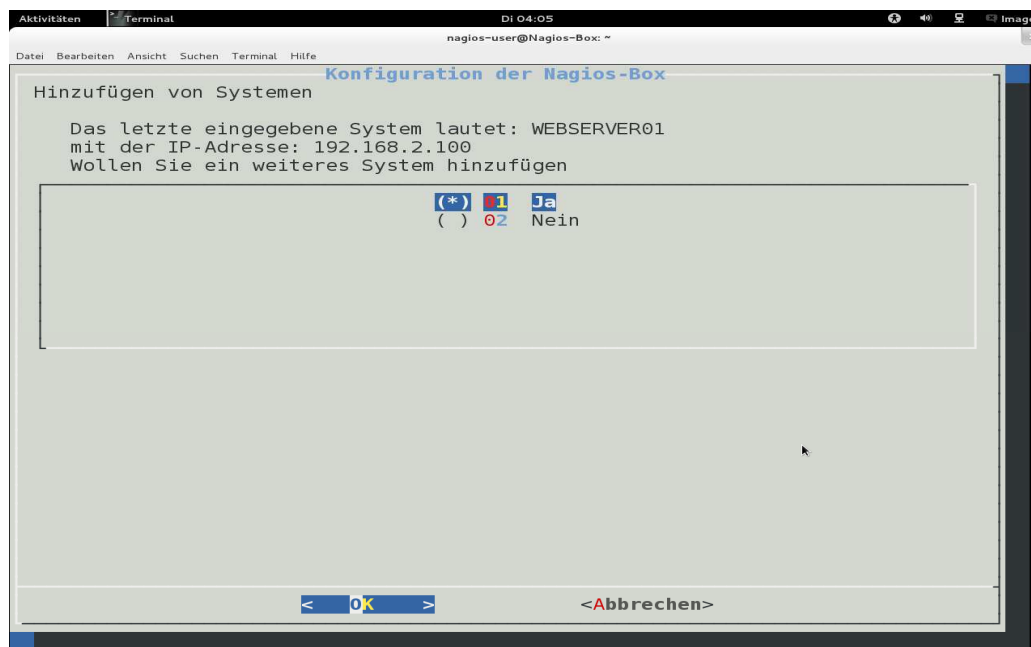


Anleitung Nagios-Box

Danach die IP Adresse eingeben und mit Enter bestätigen:



Sie können ggf. weitere Systeme hinzufügen:

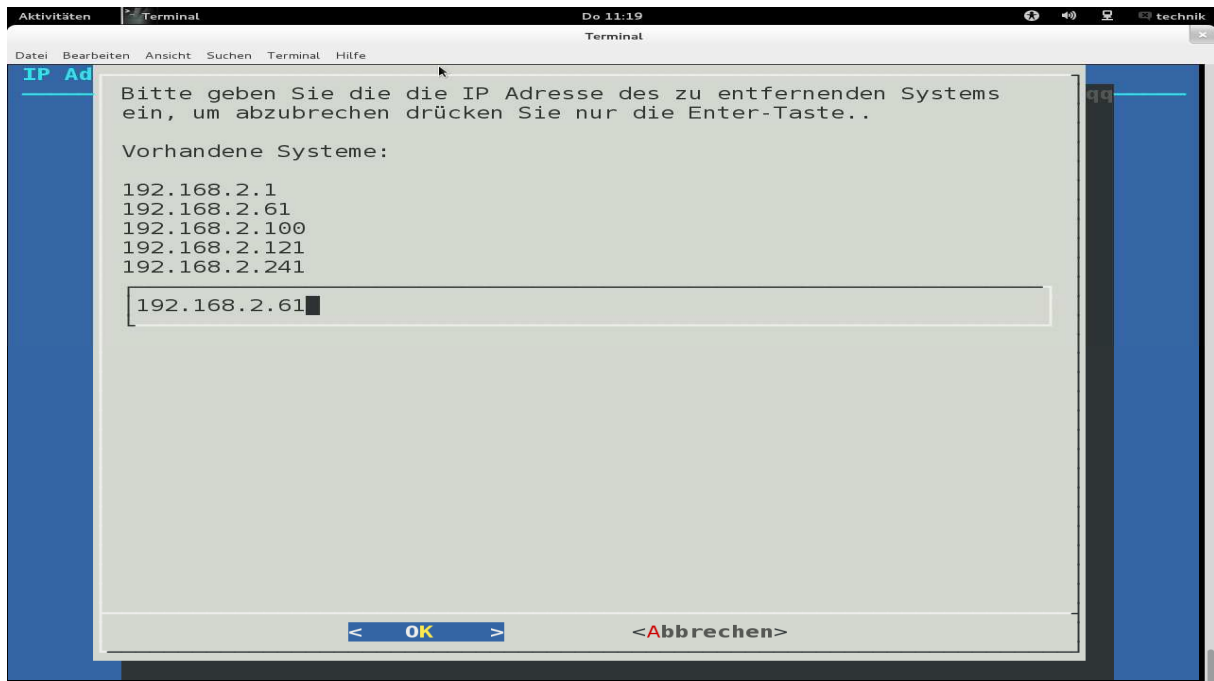


Mit ja können weitere Systeme hinzugefügt werden.

Mit nein wird die Konfiguration abgeschlossen.

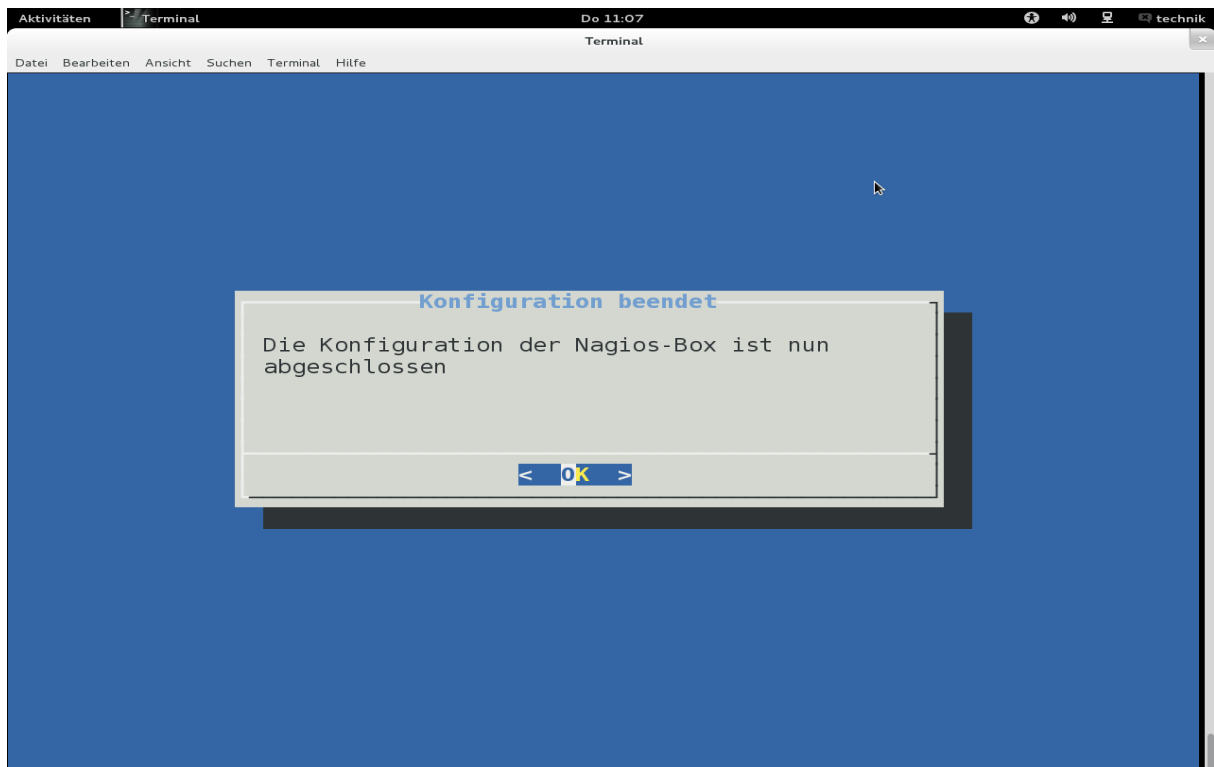
Anleitung Nagios-Box

Wird Systeme entfernen ausgewählt, wird nur die IP des Systems eingeben und mit Enter bestätigen:



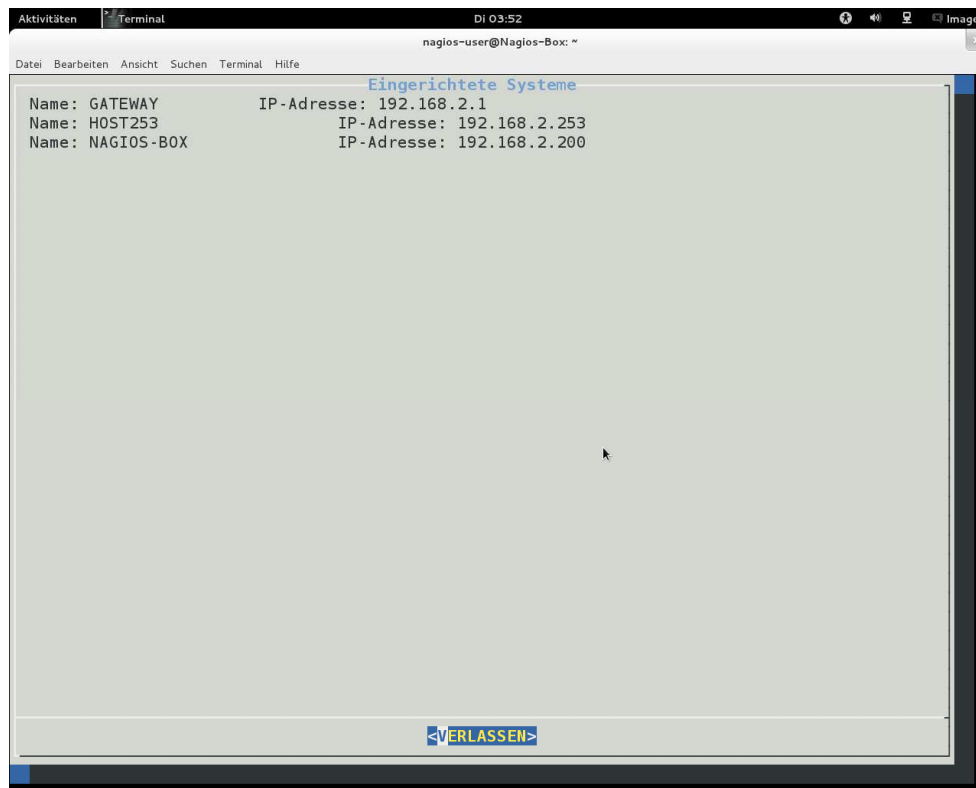
Auch dieser Vorgang kann beliebig wiederholt werden.

Wenn keine weiteren Systeme entfernt werden, wird die Änderung durchgeführt



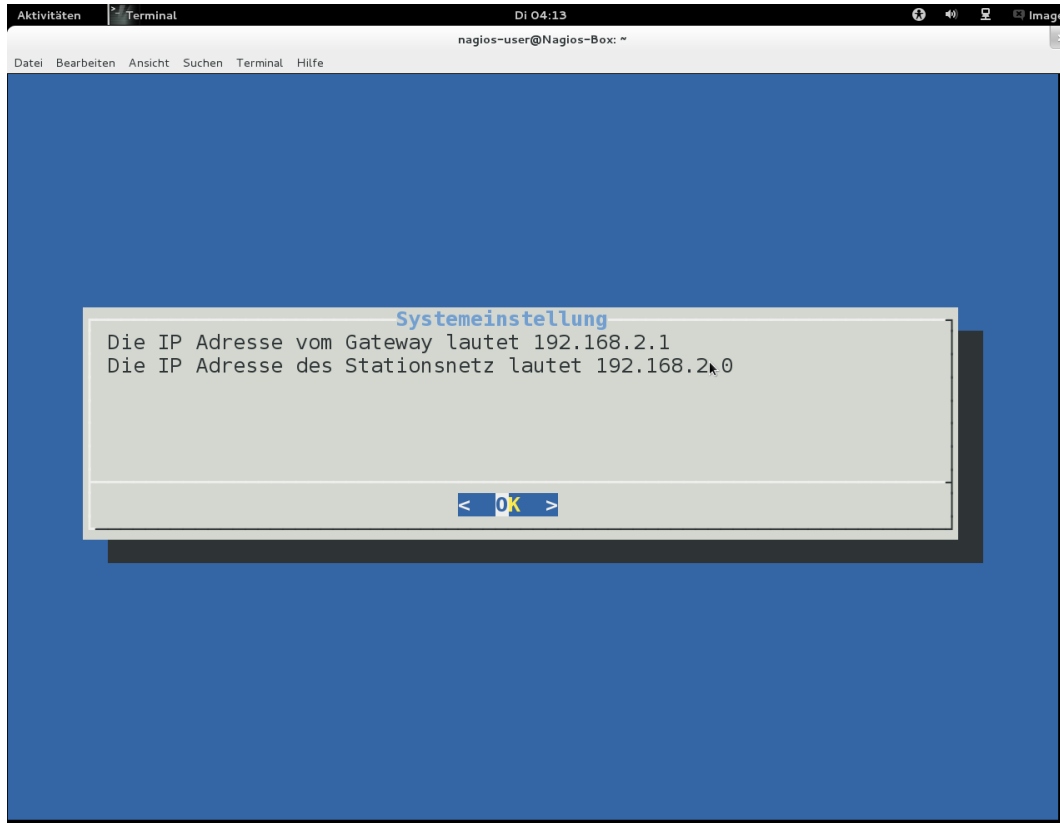
Menu Punkt 3: Überwachte Systeme anzeigen

Beim Aufruf von Menu Punkt 3 wird die Liste der sich derzeit im Monitoring befindlichen Systeme angezeigt:

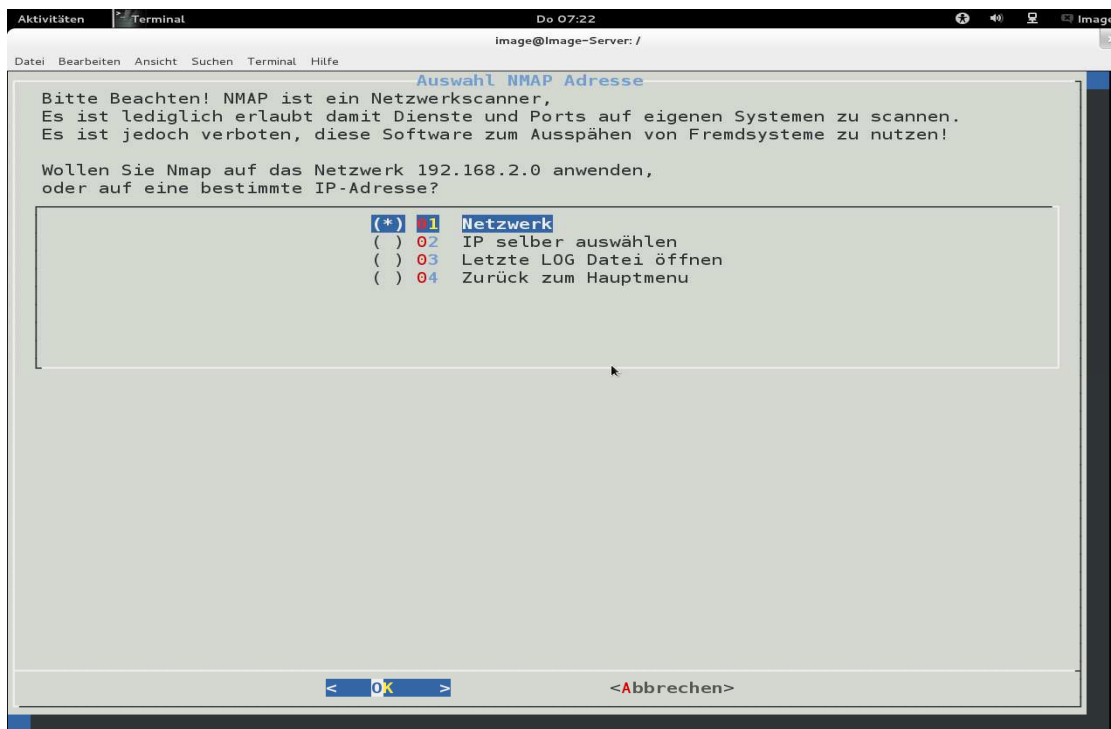


Menu Punkt 4: Netzwerk mit NMAP scannen

Wie bereits in der Einleitung beschrieben, ist NMAP ein Tool, welches ein Netzwerk nach Systemen scannt, es kann sowohl ganze Netzwerke als auch einzelne IP-Adressen scannen. Beim Aufruf des Menu Punktes wird zunächst die Aktuelle Einstellung angezeigt:

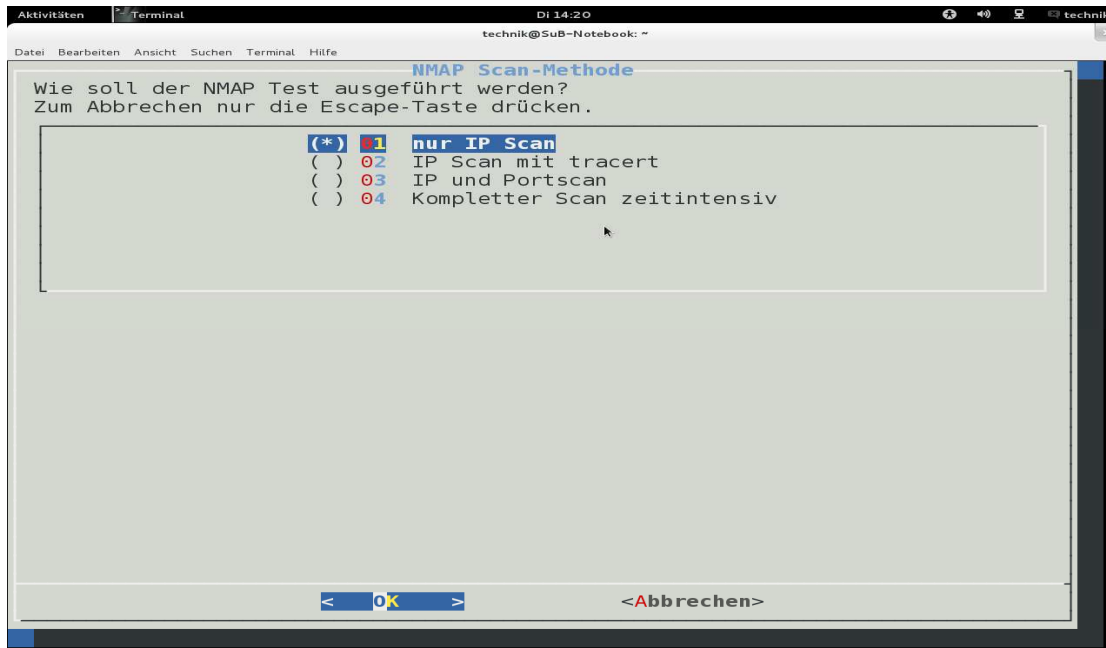


Nach Bestätigung kann man Wählen Stationsnetz, einzelne IP scannen oder sich die letzte Log-Datei anzeigen lassen:



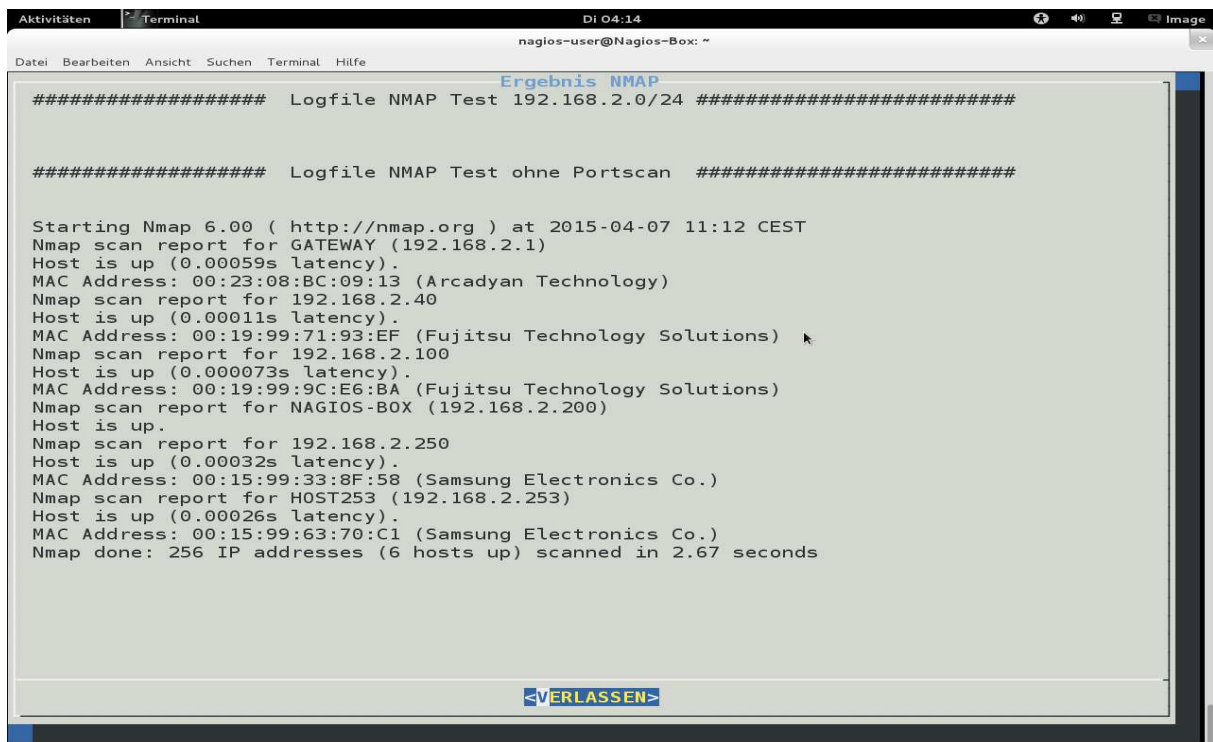
Anleitung Nagios-Box

Nach der Auswahl Stationsnetz oder Eingabe der IP-Adresse lässt sich die Scan-Methode auswählen:



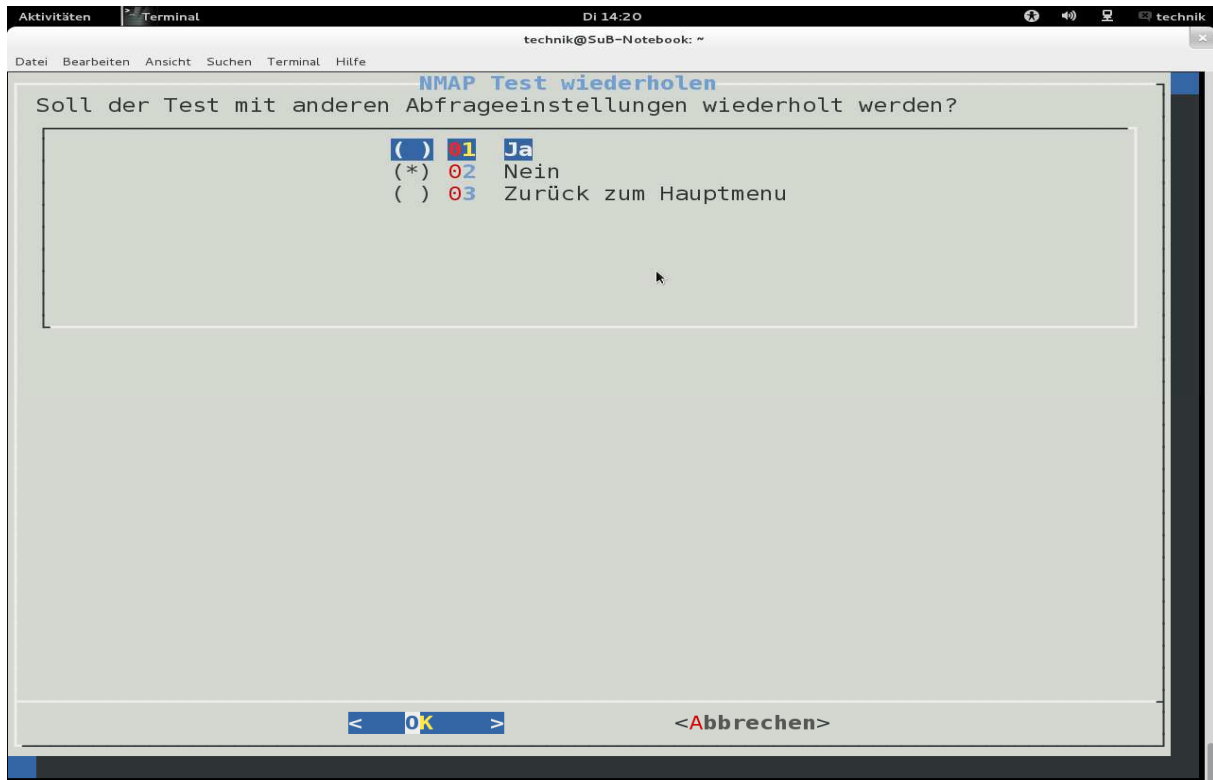
IP Scan sucht nur nach Adressen. Mit traceroute werden zusätzlich die Routen angegeben, mit Portscan werden außerdem die offenen Ports angezeigt, Komplettsammelt alle verfügbaren Informationen über gefundenen Systeme dauert aber mehrere Minuten. Das Tool ist hilfreich um Systeme zunächst einmal zu finden.

Am Ende wird eine Log Datei ausgegeben:



Anleitung Nagios-Box

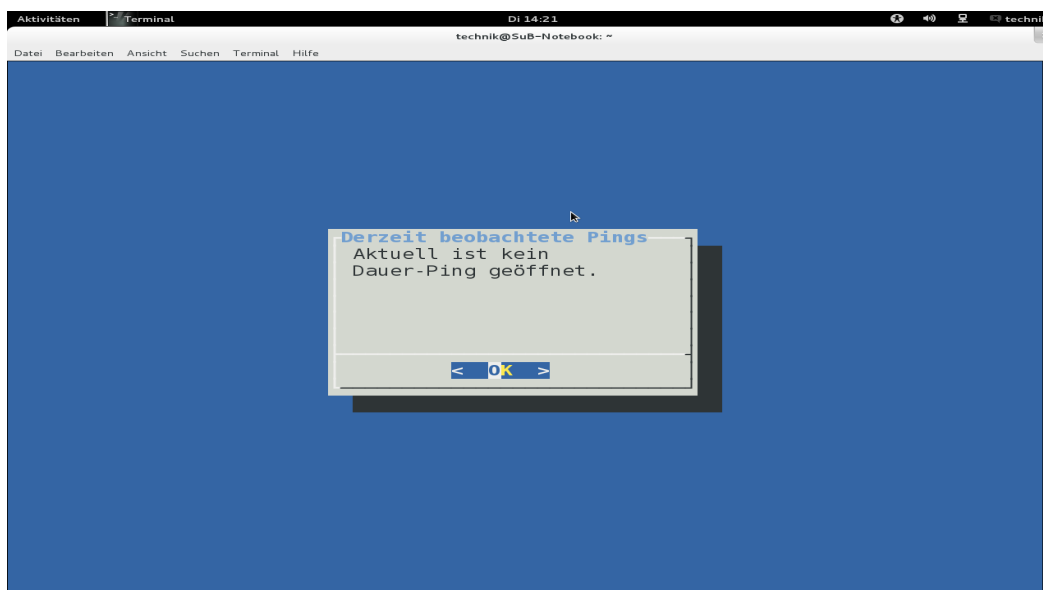
Der Test kann mit anderer Scan-Methode wiederholt werden, das Ergebnis wird an die Log Datei angehängt.



Menu Punkt 5: Dauerping auf IPs Absetzen

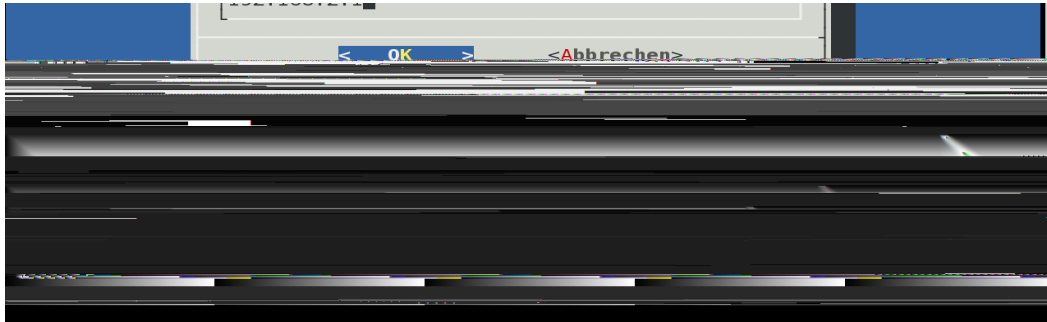
Hiermit lassen sich protokollierte Dauerpings auf Systeme absetzen. Dabei ist es möglich die Protokollierung zu bestimmen: Es werden alle, nur erfolgreiche oder nur erfolglose Pings dokumentiert. Dauerpings werden nur alle 20 Sek pro System ausgeführt damit das Netz nicht überlastet wird.

Beim Aufruf wird überprüft, ob bereits Dauerpings ausgeführt werden:

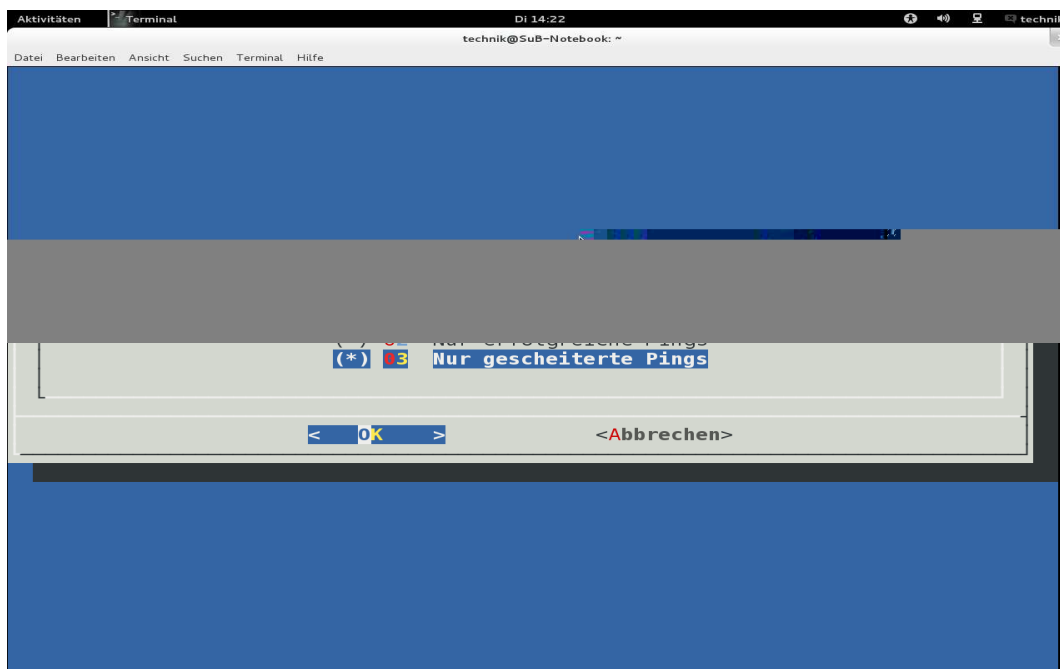


Sollten bereits Dauerpings laufen werden die IP-Adressen angezeigt, es können aber beliebig viele hinzugefügt werden.

Man gibt zunächst die IP-Adresse ein:



Danach wird die Art der Protokollierung gewählt:



Anleitung Nagios-Box

Der Pingtest wird gestartet:

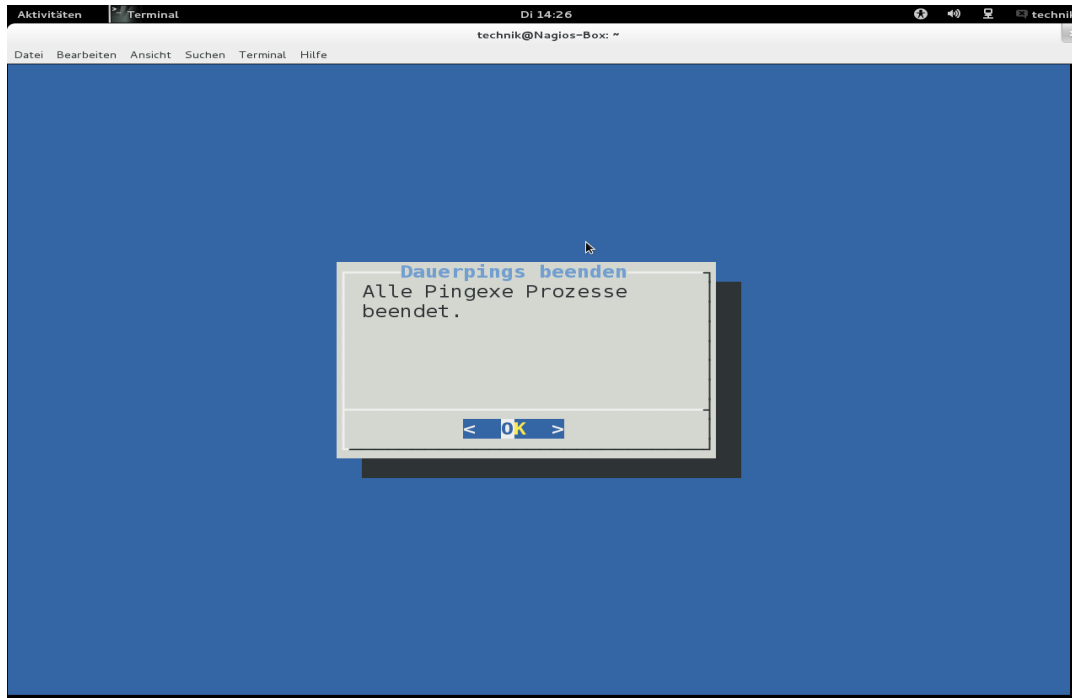
Es können dann weitere IP-Adressen hinzufügen:



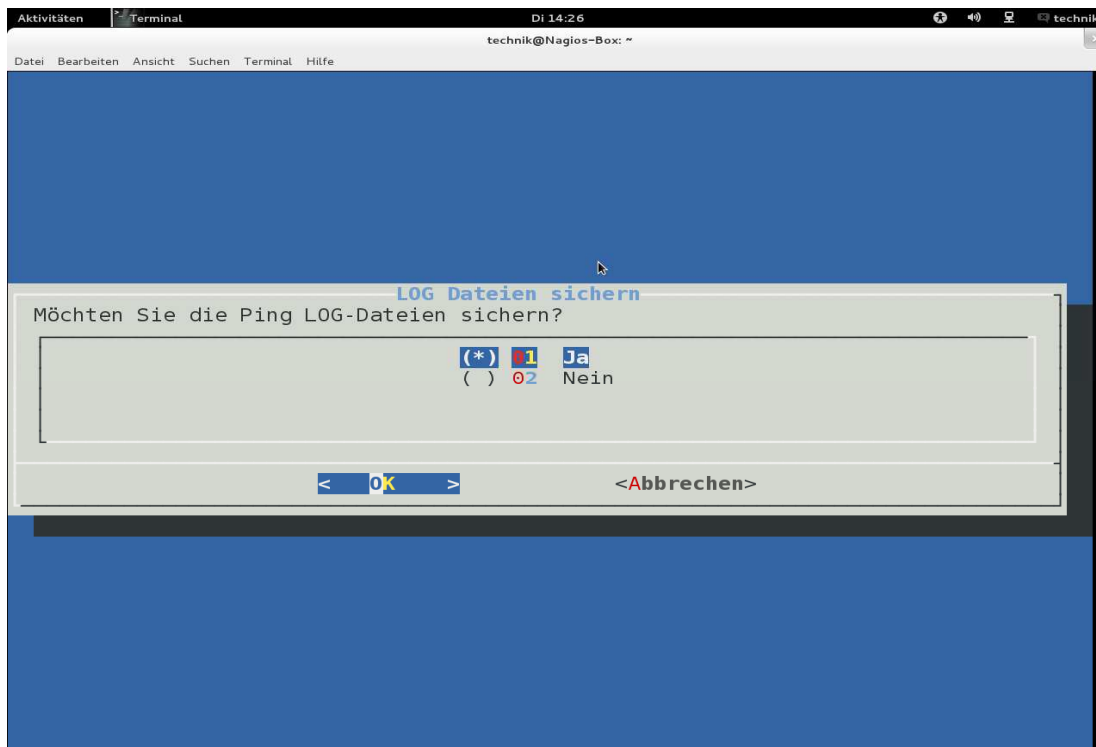
Menu Punkt 6: Dauerping auf IPs beenden

Derzeit werden immer ALLE Dauerpings beendet: (wird in einer späteren Version angepasst)

Nach Aufruf des Menu Punkts werden die Dauerpings beendet, danach erscheint die Meldung:

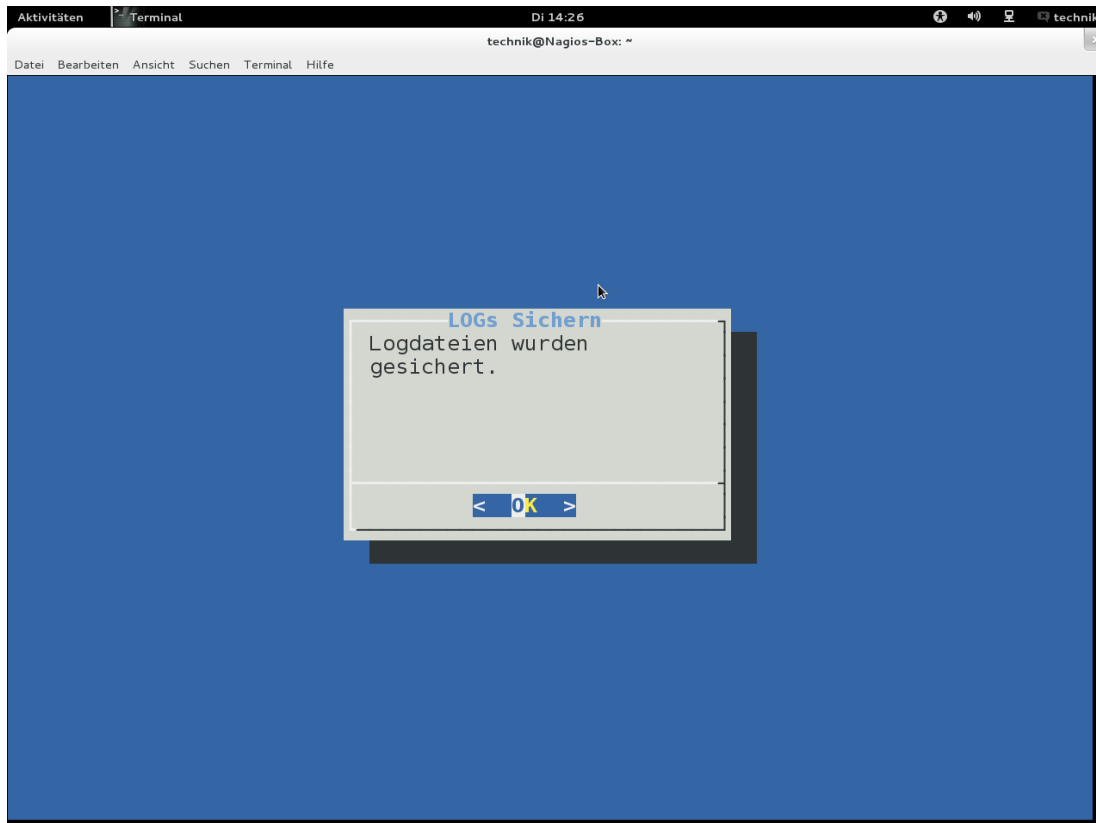


Die bisher angelegten Log Dateien der Dauerpings können nun gesichert werden:



Anleitung Nagios-Box

Nach erfolgreicher Sicherung erscheint folgende Info-Box:

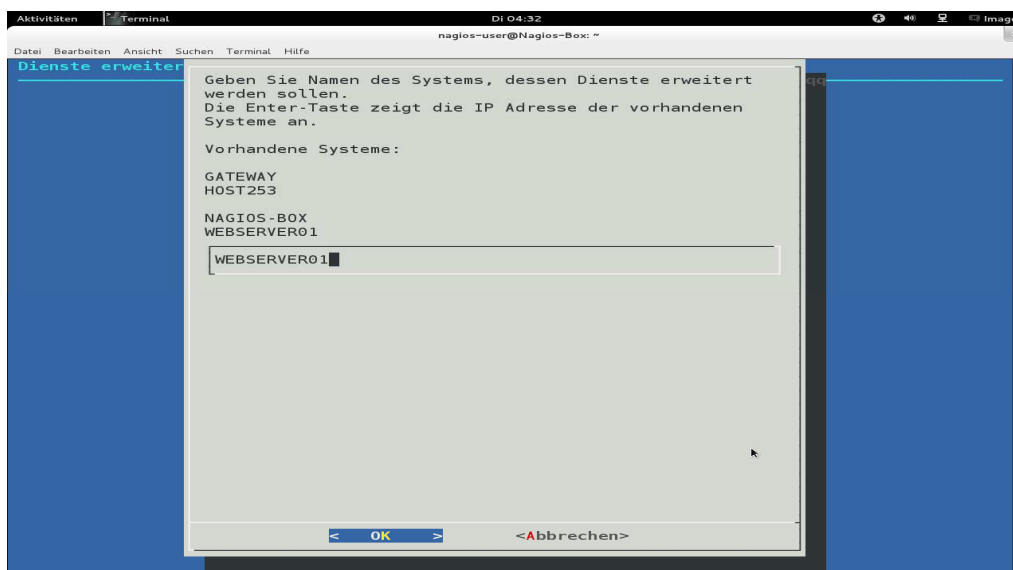


Menu Punkte 7 -12 gehören zur Auswertung und werden unter Punkt 6 behandelt:

Menu Punkt 13: Nagios-Dienste erweitern

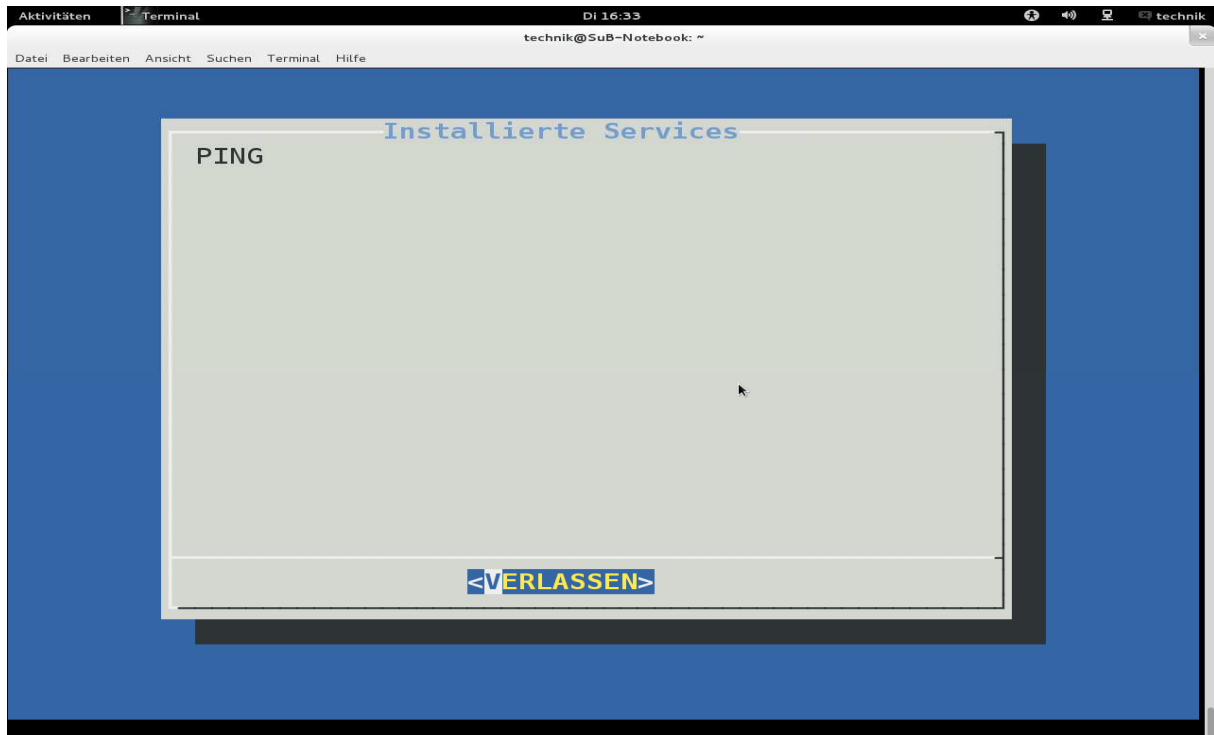
Nagios überwacht bei jedem System standardmäßig PING als Dienst. Es können jedoch weitere Dienste überwacht werden. Die Funktionen der Dienste sind im Anhang erläutert.

Nach Aufruf des Menu Punktes werden die Überwachten Systeme angezeigt, man wählt das zu erweiternde System aus:

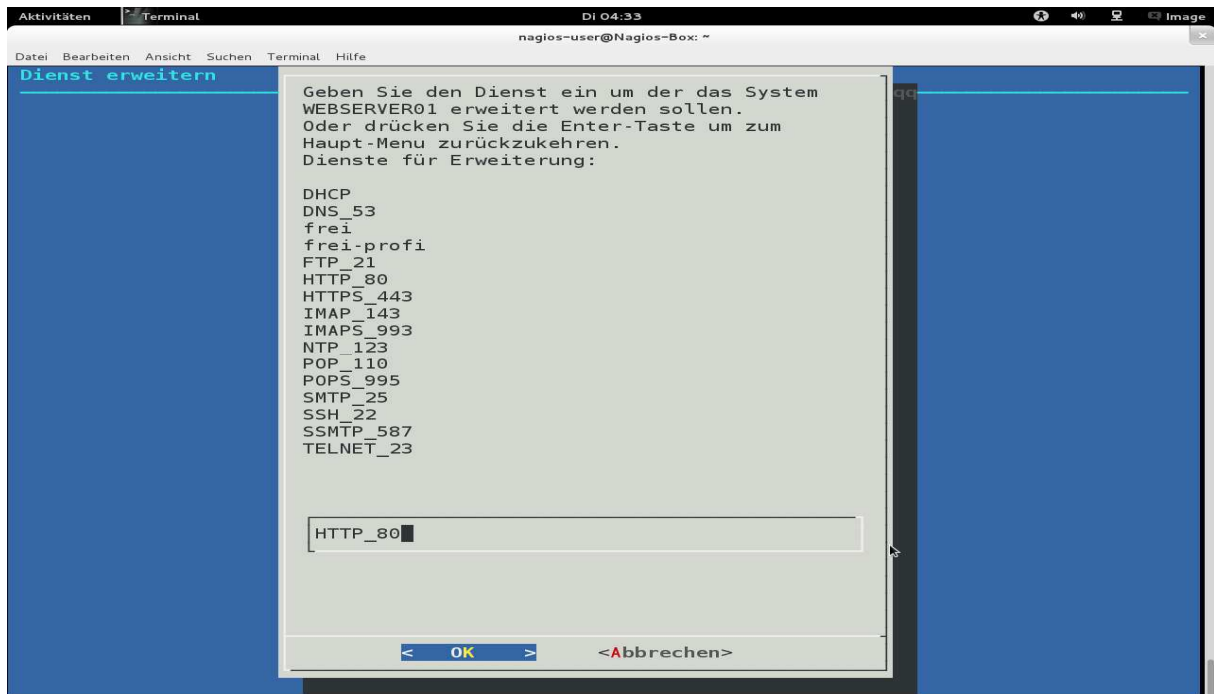


Anleitung Nagios-Box

Danach werden die bereits eingerichteten Dienste für das System angezeigt:



Dann lassen sich die zur Verfügung stehenden zusätzlichen Dienste angezeigt, hier gibt man den zuzufügenden Dienst ein:

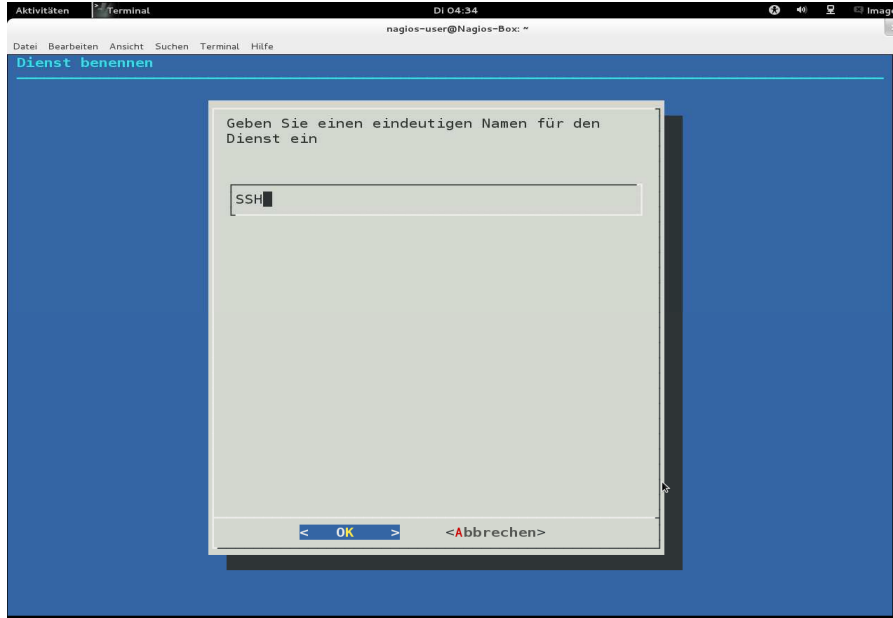


Danach wird der Dienst importiert und das Haupt-Menu geöffnet.

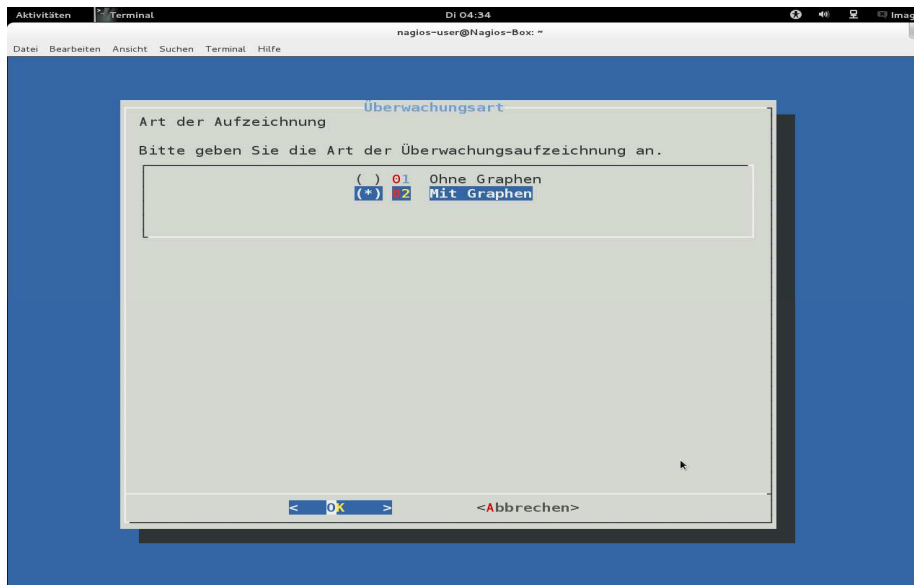
Dienste frei und frei-profi:

Wählt man den Dienst **frei** aus, hat man die Möglichkeit TCP oder UDP Dienste mit eigener Portvergabe auszuwählen:

Zunächst muss der Dienst eine Bezeichnung erhalten:

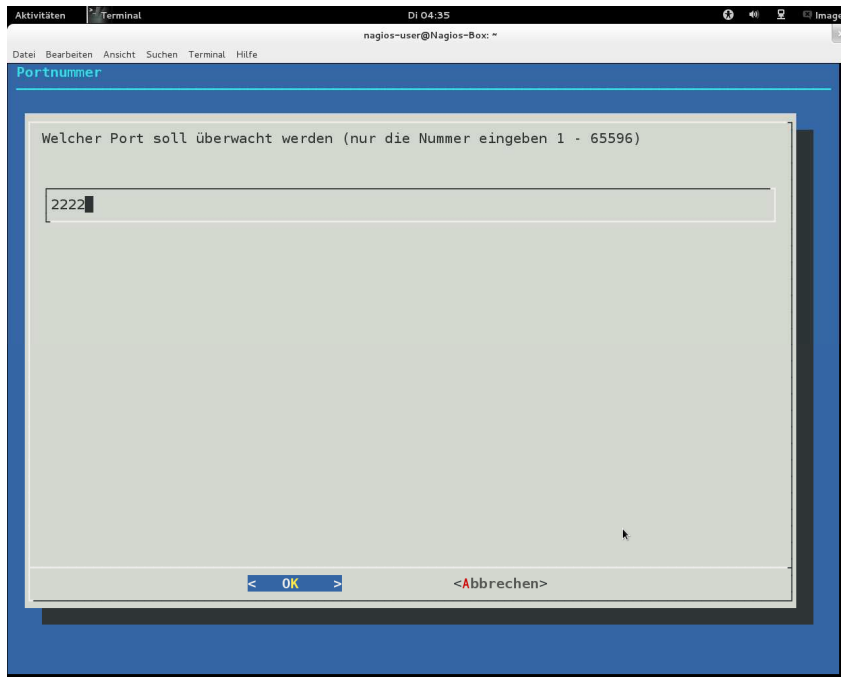


Danach entscheidet man, ob ein Dienst einen Graph erzeugen soll, der in der Auswertung auf der Weboberfläche betrachtet werden kann (Siehe Anhang 1 Anleitung-Web-Oberfläche-Nagios):

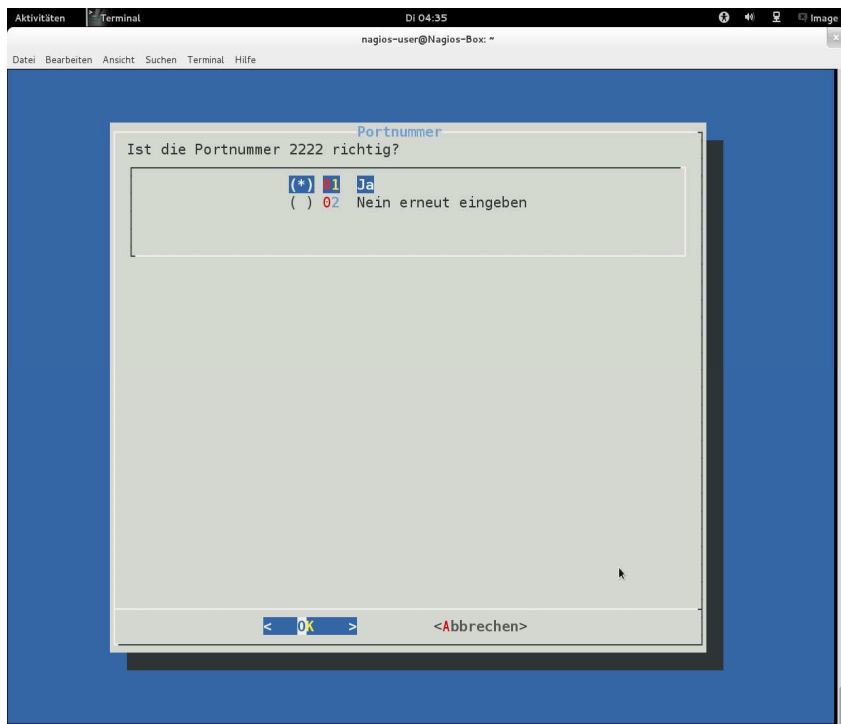


Anleitung Nagios-Box

Es wird nun der zu überwachende Port festgelegt:

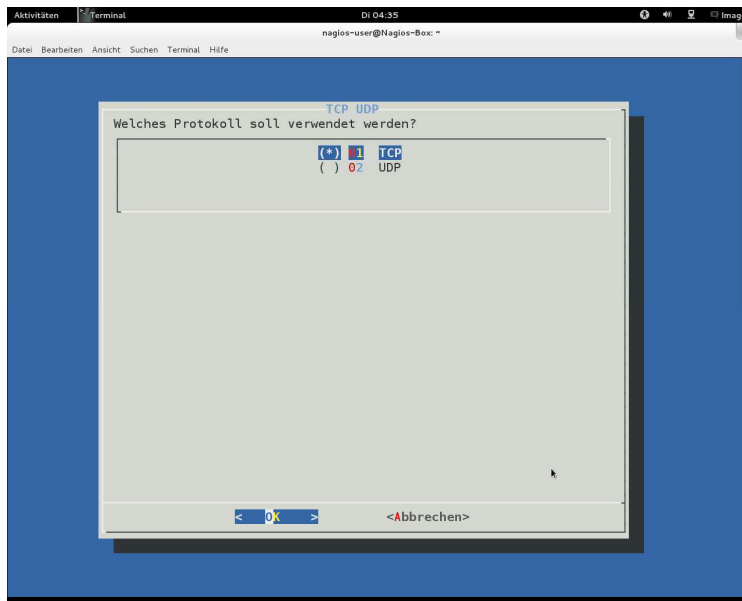


Danach wird der Port bestätigt:



Anleitung Nagios-Box

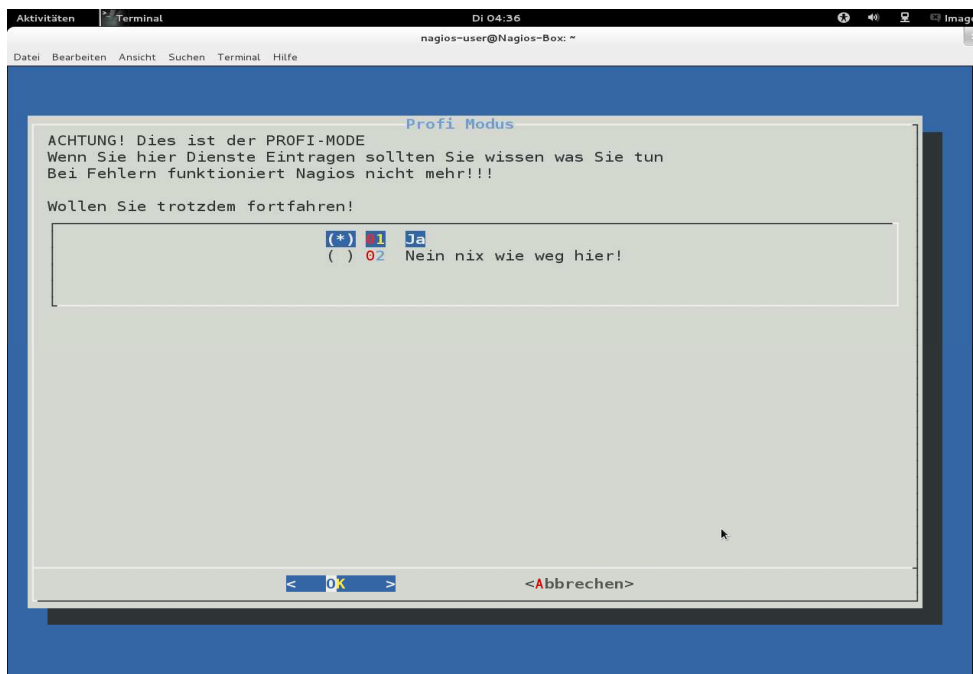
Zuletzt wird das Protokoll auf dem der Dienst zu erreichen ist angegeben:



Danach wird der Dienst implementiert und die Überwachung gestartet:

Anmerkung: Nicht alle Dienste können so angesprochen werden, da evtl. Argumente notwendig sind, in diesem Fall kann ein Dienst auch wieder entfernt werden. Müssen Dienste mit Argumenten oder Adressen versehen werden so ist der Dienst frei-profi zu wählen.

Wir der Dienst frei-profi gewählt erscheint zunächst folgende Meldung:



Anleitung Nagios-Box

Kurze Einführung zum Verständnis: Nagios funktioniert auf zwei Ebenen, einer HOST-Ebene und einer Service Ebene. Die HOST-Ebene wird unter Menüpunkt 2 eingerichtet, diese wird in eine Datei geschrieben und enthält unter anderem den Namen des Hosts und seine IP Adresse.

Die zweite Ebene ist die Service Ebene diese wird in der selben Datei angelegt und ist damit auch nur für einen Host zuständig.

Die Service sind festgelegte Abfrage Programme, denen Argumente oder auch IP-Adressen übergeben werden können. Eine Kommandokette sieht in etwa so aus:

Kommando `-H <Hostadresse> -ARG1 <Argument1>, -ARG2 <Argument2>` usw.

Beispiel mit dem Kommando `check_dig`, welches Informationen zu einer Domain bei einem Nameserver abfragt.

`check_dig -H 8.8.8.8 -I www.keuni.de` das Kommando fragt hier Informationen zu der Domain www.keuni.de bei der Adresse 8.8.8.8 (was sinnvoller Weise ein Nameserver sein sollte) ab.

Die Programme von Nagios liegen unter `/usr/lib/nagios/plugins/`

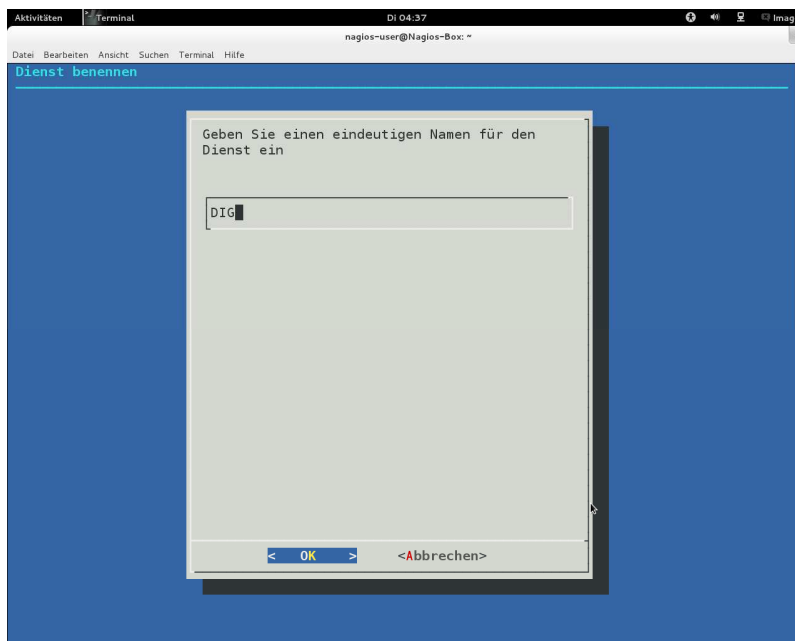
Gibt man in der Konsole `~$ /usr/lib/nagios/plugins/ check_dig -H 8.8.8.8 -I www.keuni.de` ein. Sollte man ein **DNS OK** zurückbekommen. (Sofern es die Domain gibt und die Nagios-Box selber Online ist)

In der Konfiguration von Nagios wird das Kommando so eingefügt. `Check_dig!8.8.8.8!www.keuni.de`

Man braucht also nur die Hostadresse `8.8.8.8` und als Argument `www.keuni.de`, einzugeben, die Ausführungszeichen sind nur Trennzeichen, die das Programm alleine übergibt.

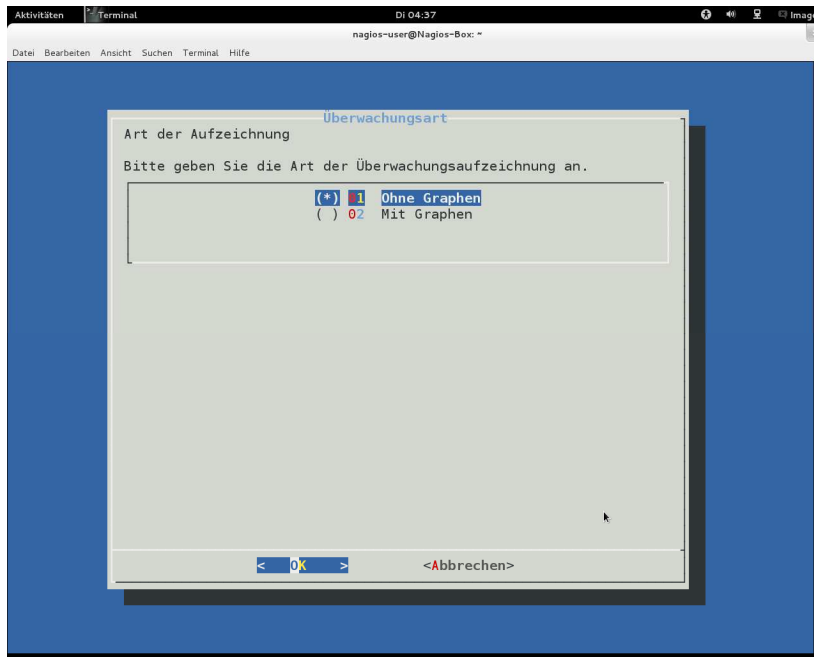
!!Achtung Fehlerhafte Eingaben können Nagios dazu bringen, dass es nicht mehr startet. Bitte merken Sie sich, welchen Dienst Sie zuletzt eingerichtet haben, um ihn ggf. wieder zu entfernen.

Zuerst geben Sie den Dienst ein:

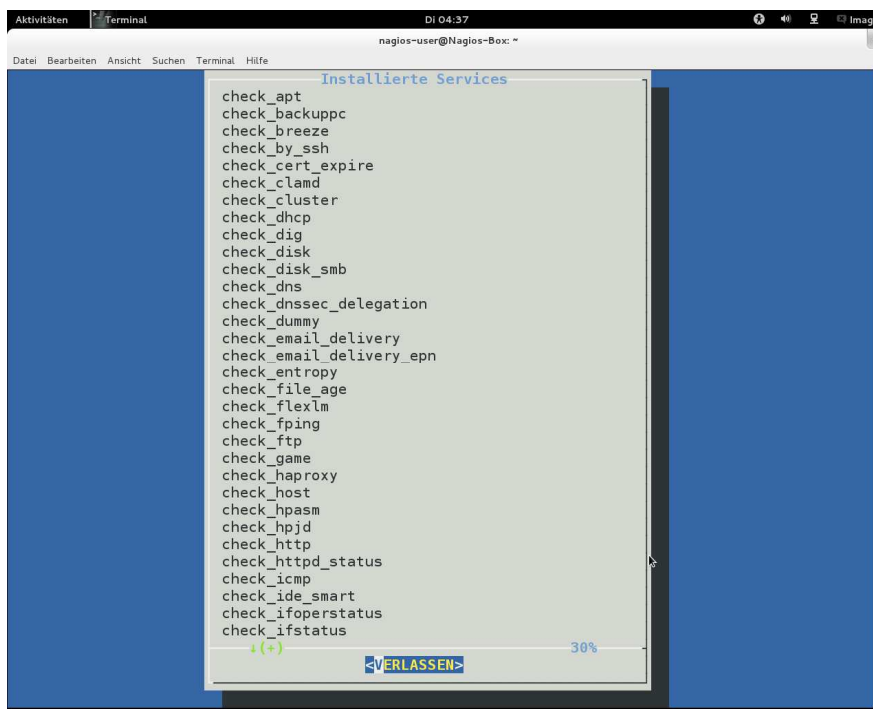


Anleitung Nagios-Box

Danach wieder die Aufzeichnungsart:

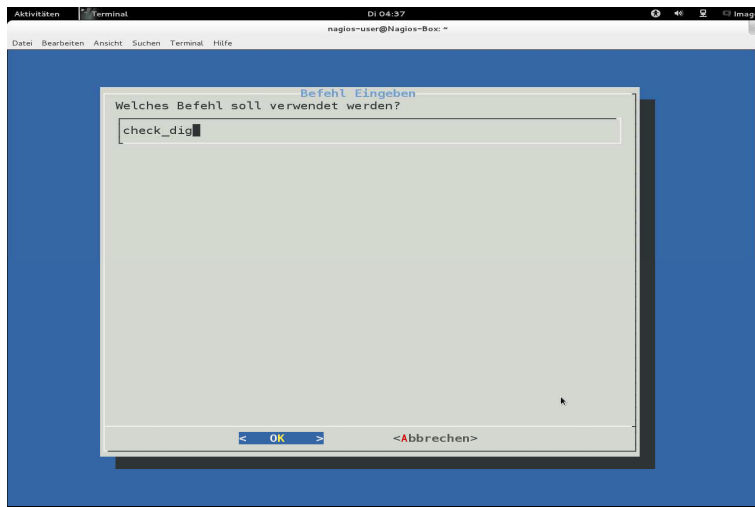


Es werden daraufhin alle verfügbaren Kommandos angezeigt:

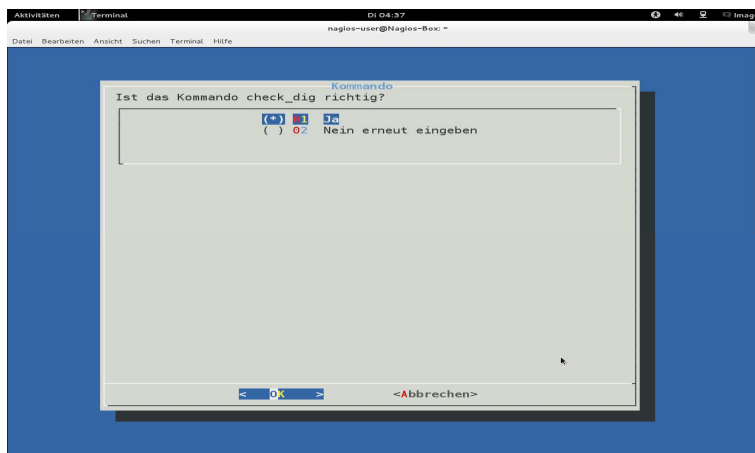


Anleitung Nagios-Box

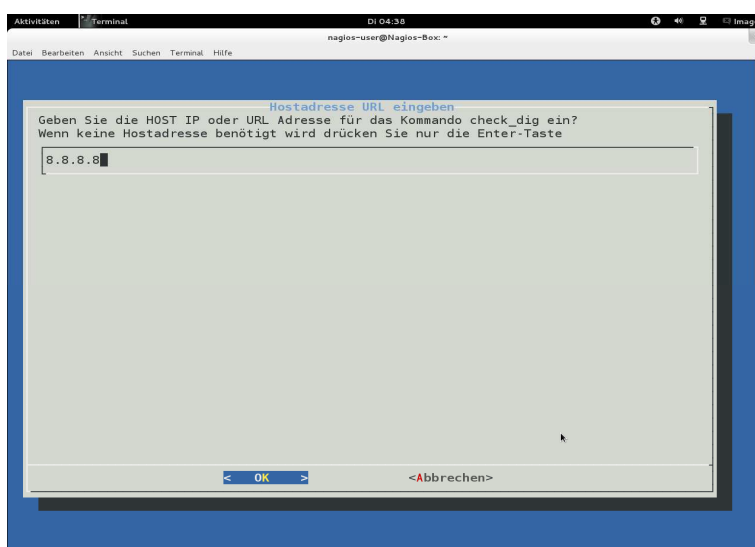
Wenn Sie das Kommando gefunden haben geben Sie dieses ein:



Dann bestätigen:

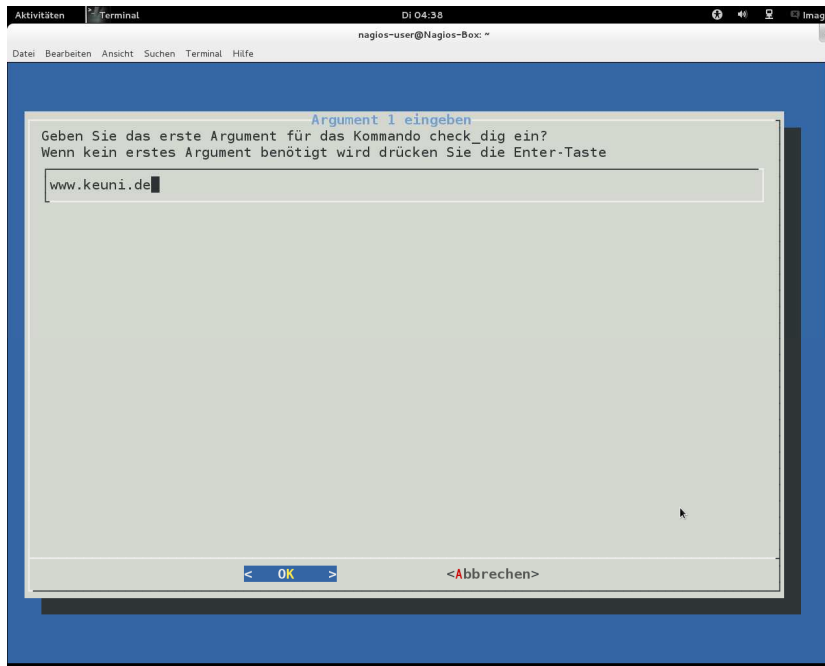


Danach Adresse oder URL:

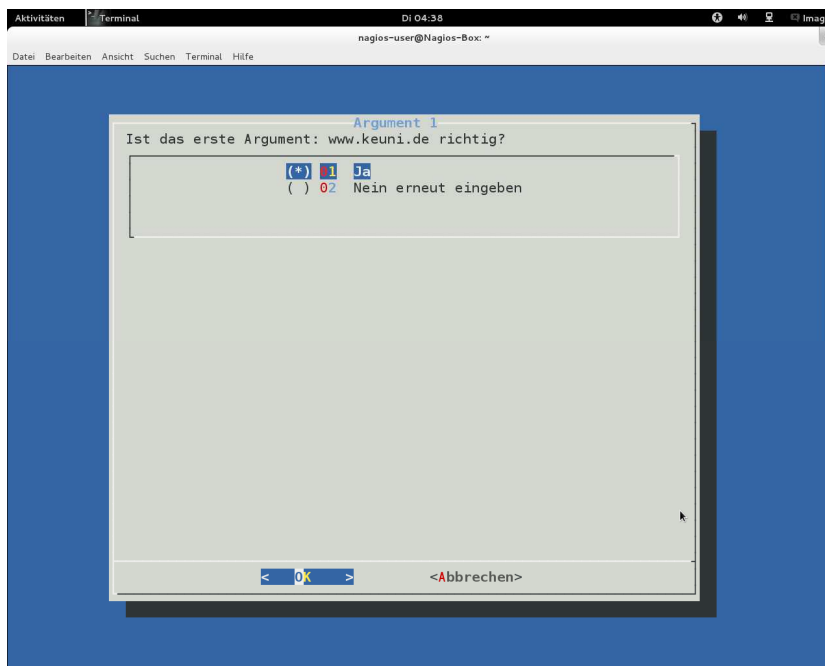


Anleitung Nagios-Box

Dann das erste Argument:



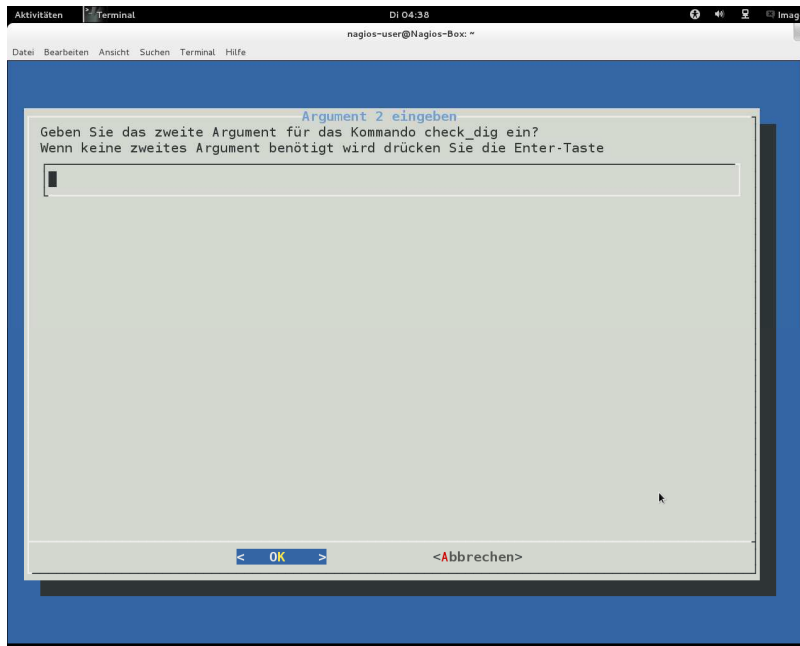
Wieder Betätigen:



Usw.....

Anleitung Nagios-Box

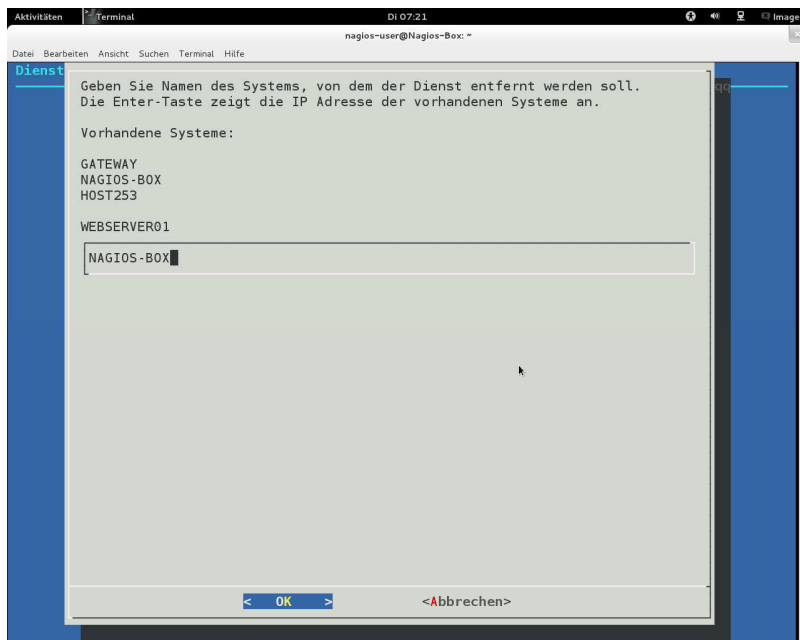
Soll kein Argument mehr hinzugefügt werden nur die Enter-Taste drücken:



Nach dem fünften Argument wird die Konfiguration übernommen.

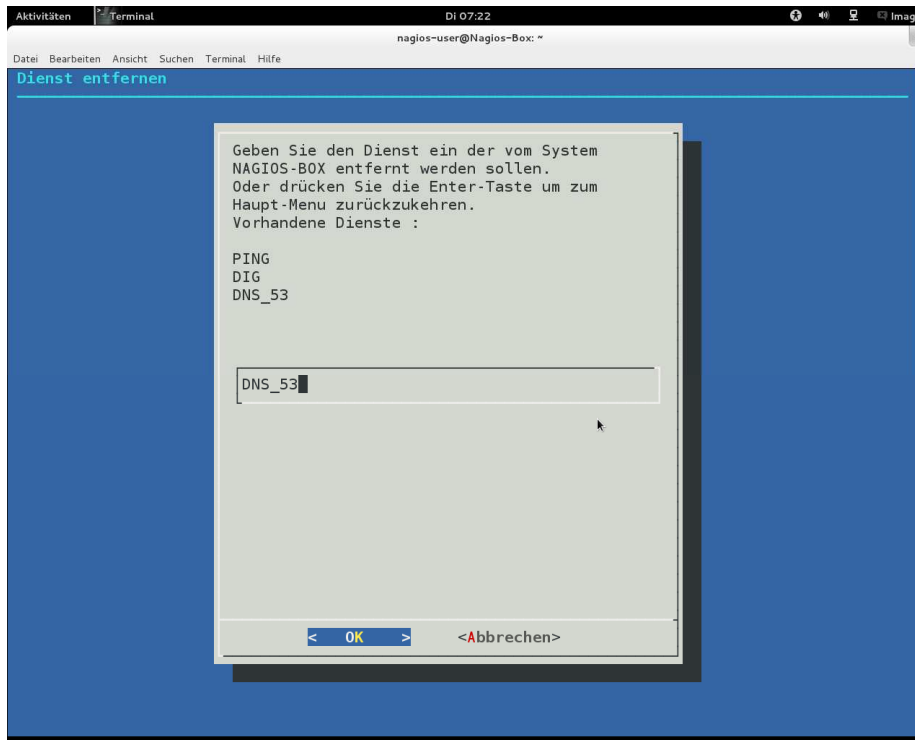
Menu Punkt 14: Nagios Dienste entfernen

Nach Aufruf des Menu Punktes wird zunächst das System ausgewählt:



Anleitung Nagios-Box

Danach den zu entfernenden Dienst eingeben:

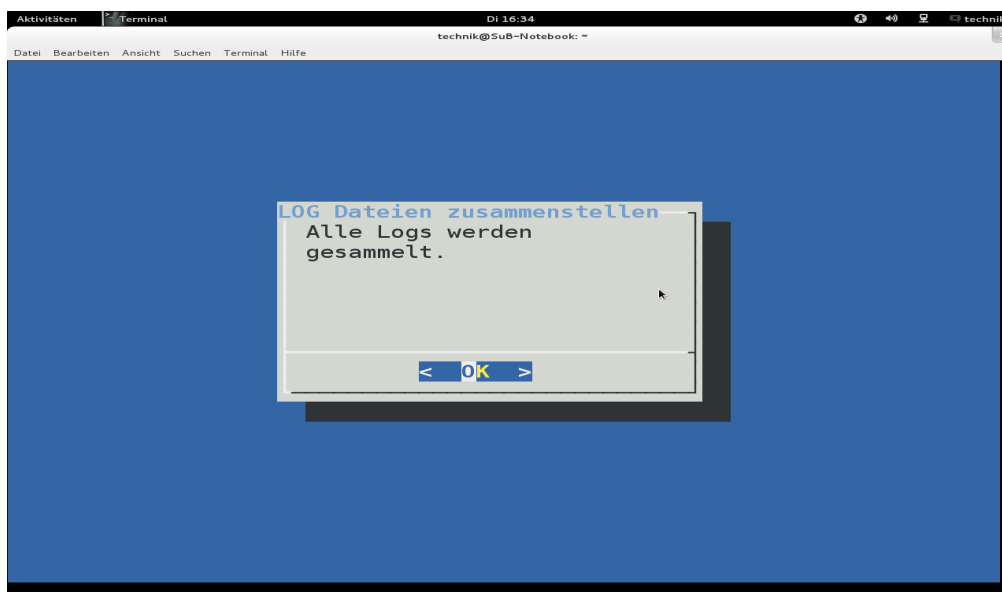


Der Dienst wird entfernt und die neue Konfiguration übernommen.

Menu Punkt 15: Alle LOG Dateien auf USB-Stick exportieren

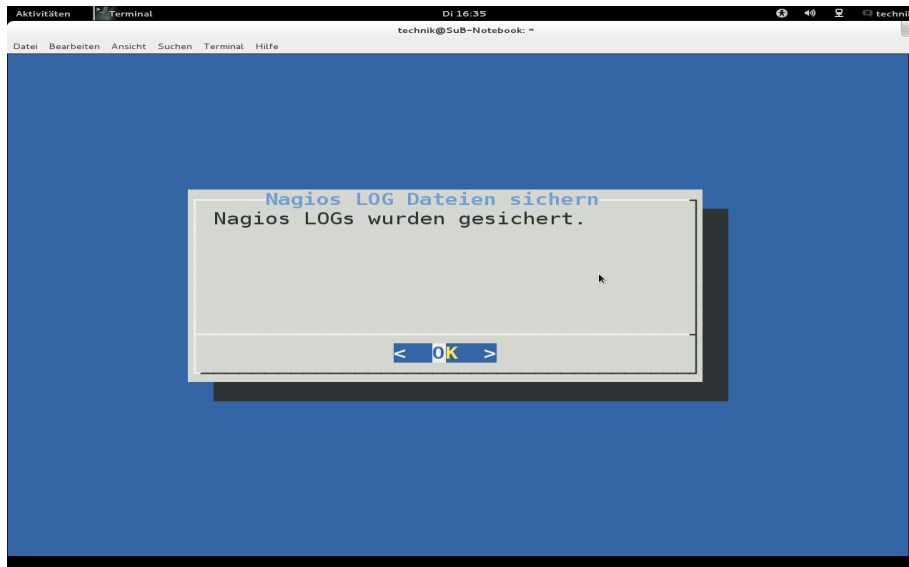
Alle Log Dateien sollten vor Abbau einer Nagios-Box gesichert werden. Dazu benötigt man einen mit Fat formatierten USB Stick.

Nach öffnen des Menu Punktes werden die Log Dateien gesammelt wenn die folgende Info-Box bestätigt wird:



Anleitung Nagios-Box

Zuerst die Nagios Logs:



Dann die Mails:

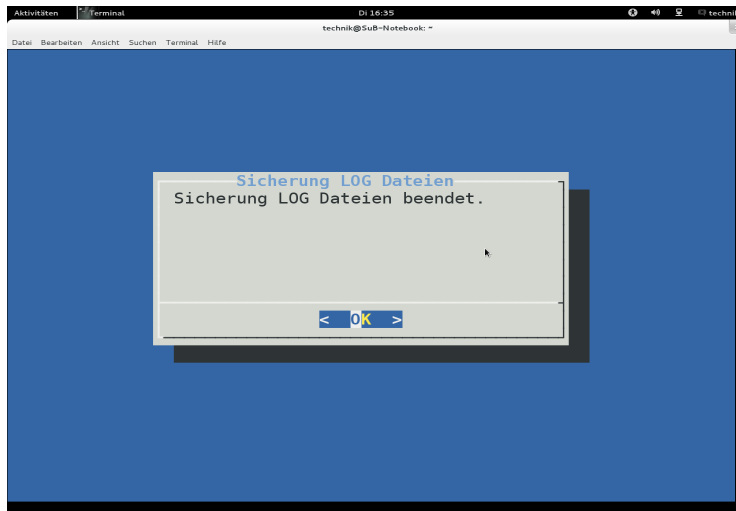


Zuletzt die Ping Logs:



Anleitung Nagios-Box

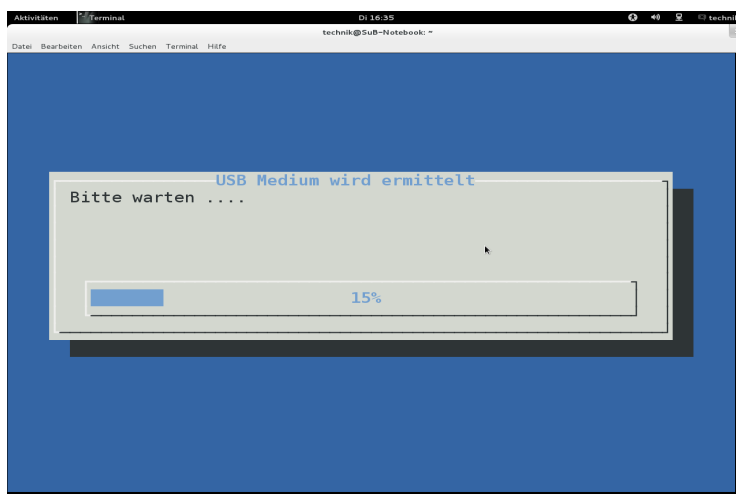
Nach der Bestätigung der Sicherung:



Wird der USB Stick an die Nagios-Box angeschlossen:

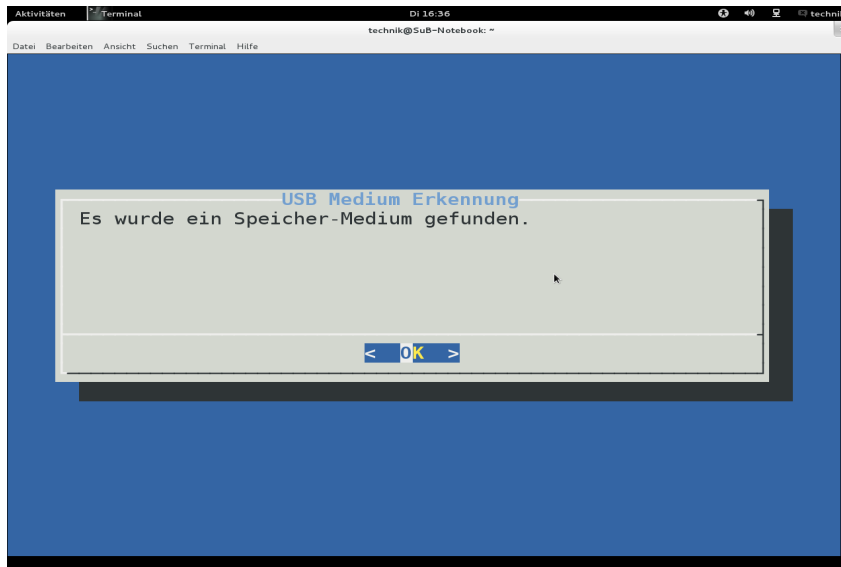


Wurde der Stick erfolgreich gesucht:

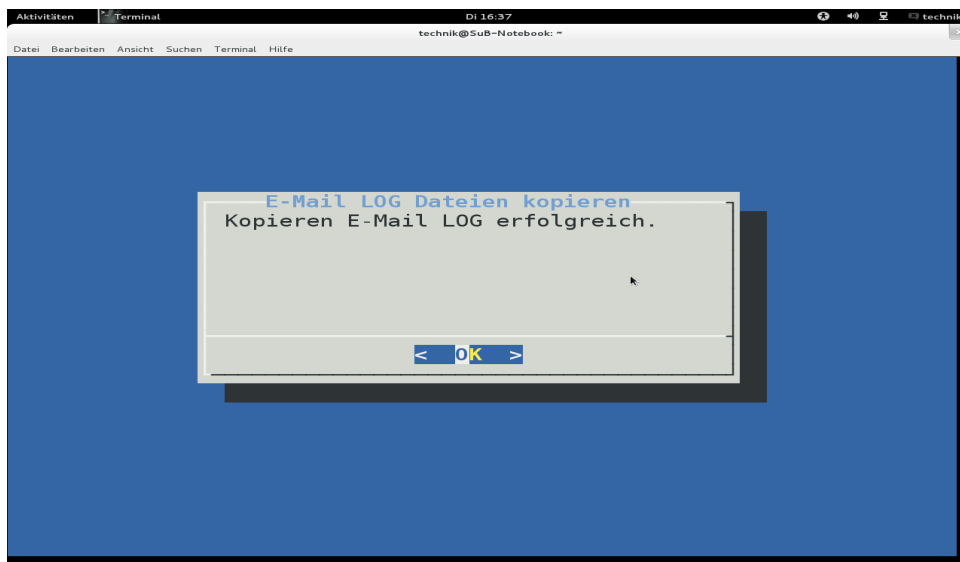
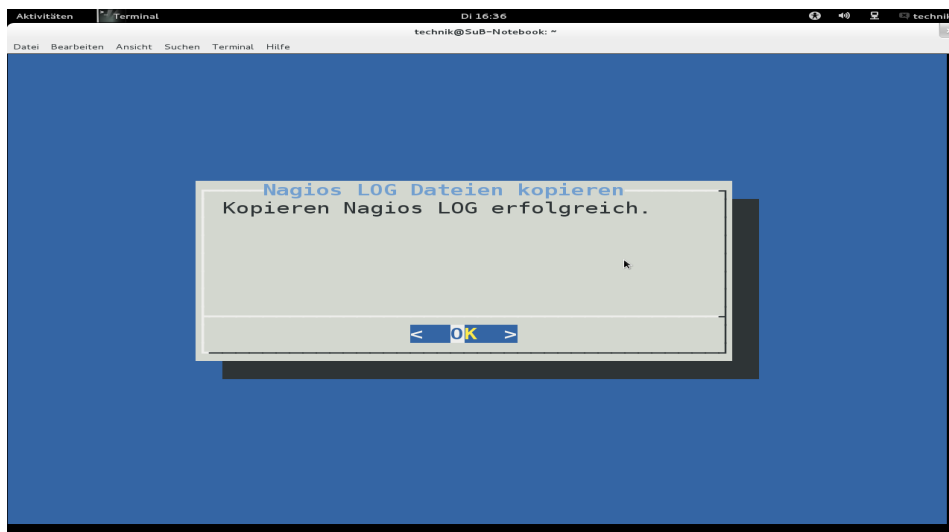


Anleitung Nagios-Box

Erscheint folgendes Fenster:



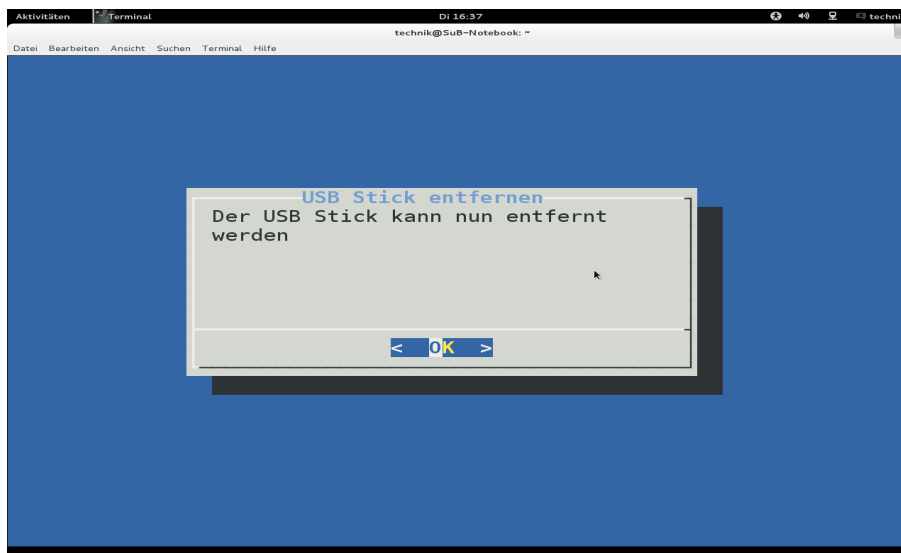
Nachbestätigung werden die Dateien gesichert:



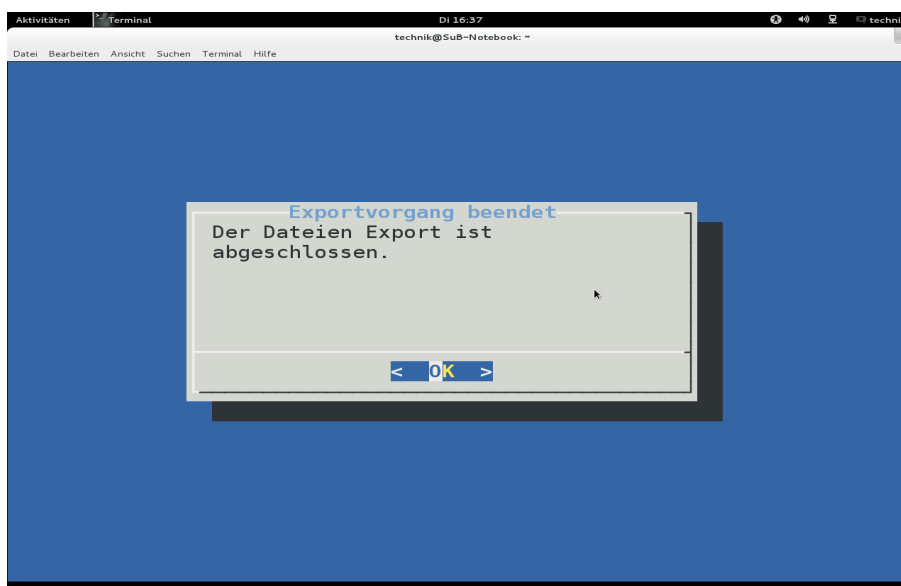
Anleitung Nagios-Box



Nach Bestätigung der Sicherungen wird der USB-Stick entbunden:

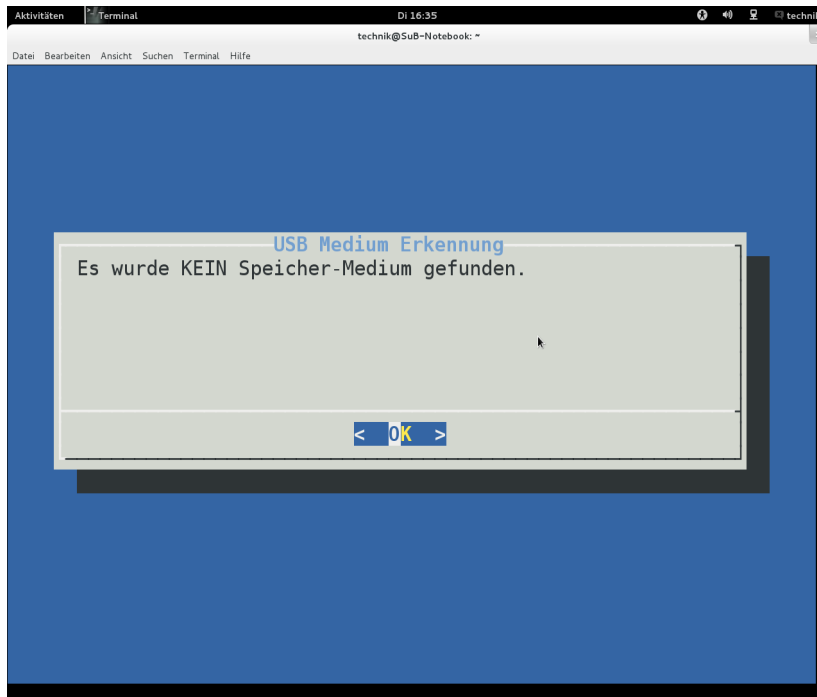


Danach ist der Export abgeschlossen und nach Bestätigung gelangt man ins Haupt-Menu:

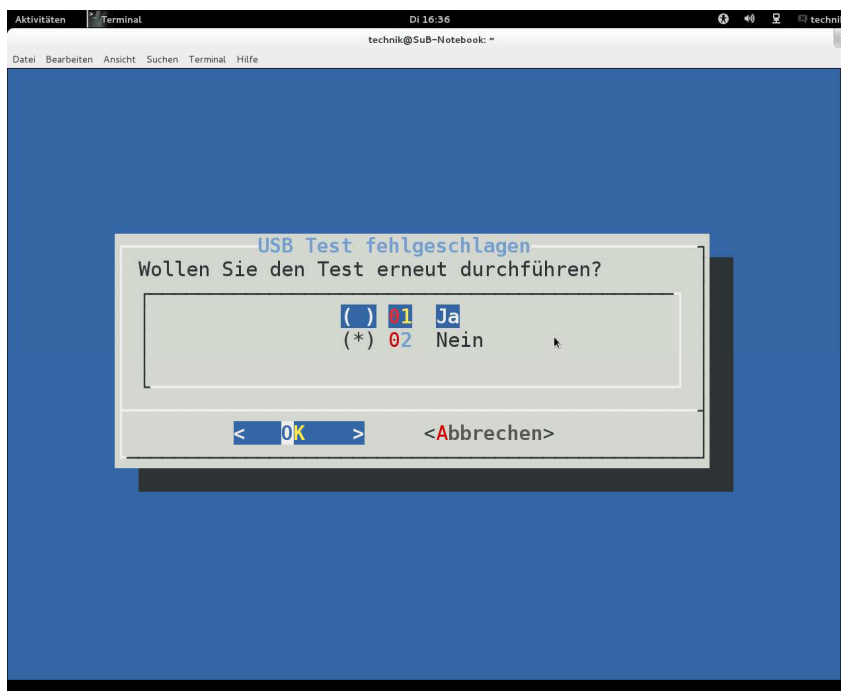


Anleitung Nagios-Box

Sollte der USB Stick nicht gefunden werden.



Der Test kann dann erneut durchgeführt werden, dazu bitte den USB Stick entfernen und erneut einstecken:

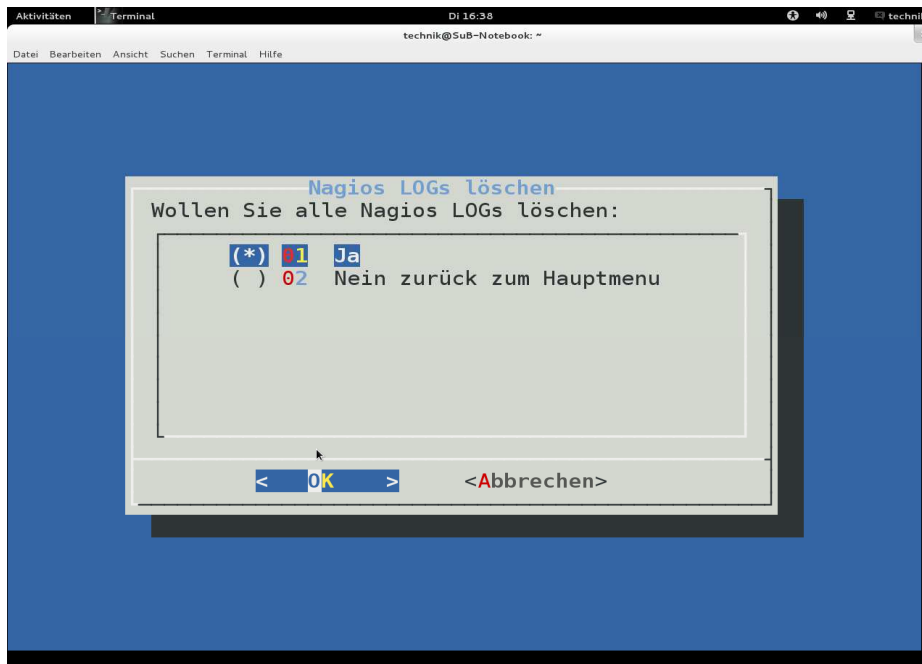


Anleitung Nagios-Box

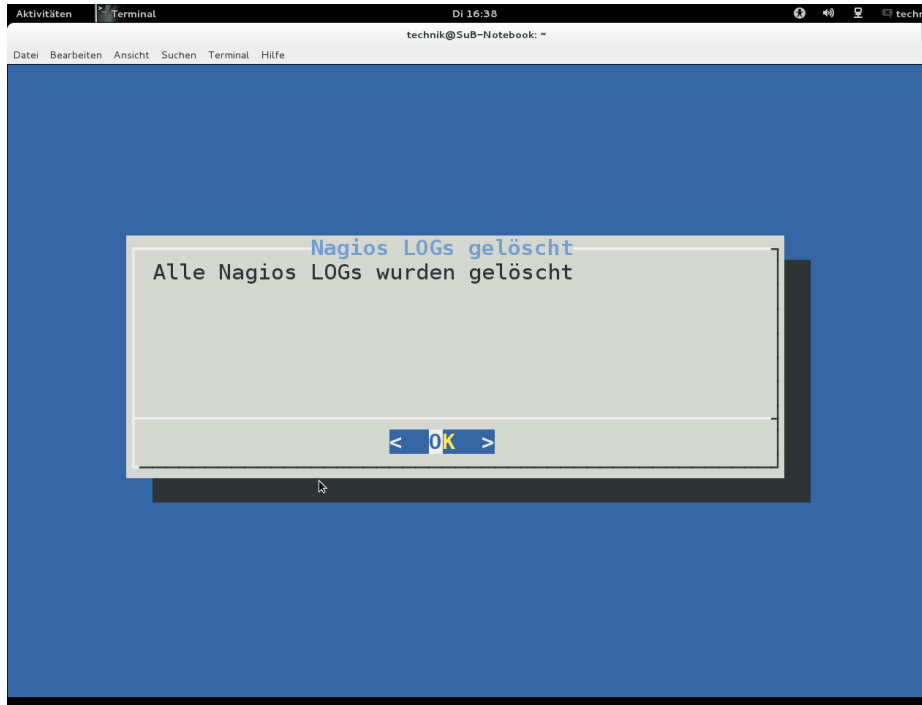
Menu Punkt 16: Alle Nagios Logs löschen

Es werden hierbei alle Nagios Logs gelöscht, ohne sie zu archivieren!

Beim Aufruf erscheint das Fenster:



Und nach Bestätigung:

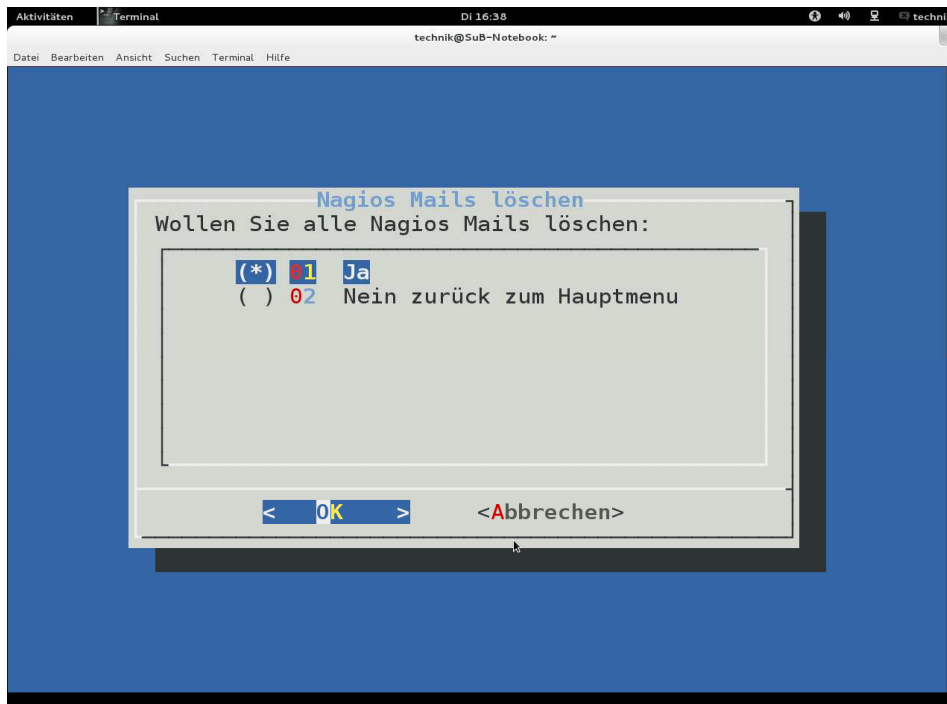


Anleitung Nagios-Box

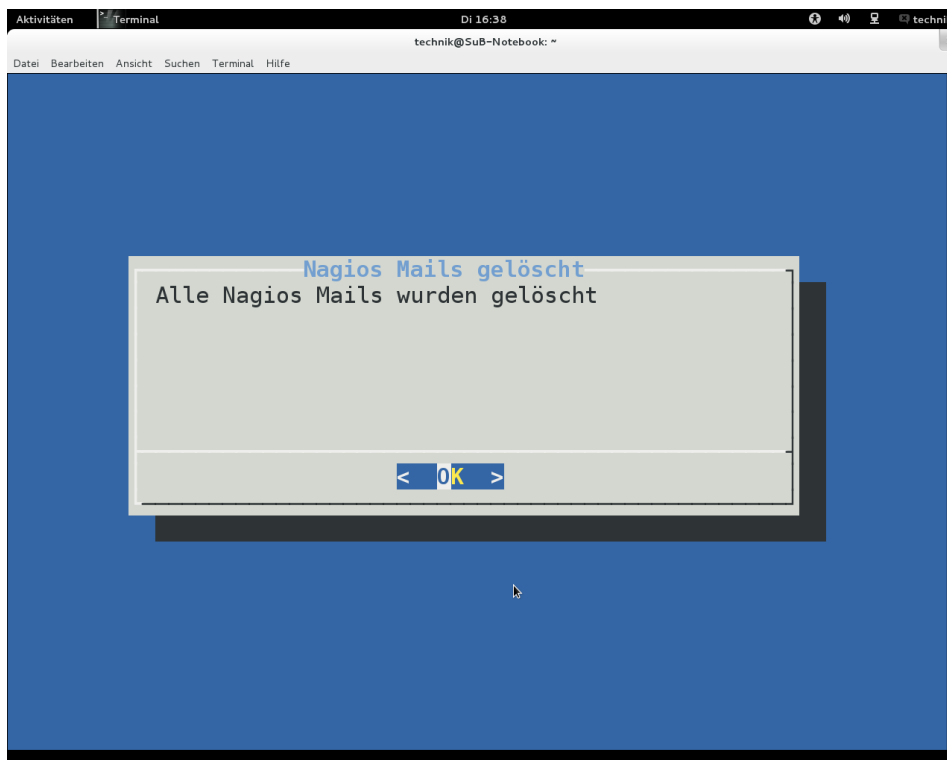
Menu Punkt 17: Alle Nagios Fehler Mails löschen

Es werden hierbei alle Nagios Fehler Mails gelöscht, ohne sie zu archivieren!

Beim Aufruf erscheint das Fenster:



Und nach Bestätigung:

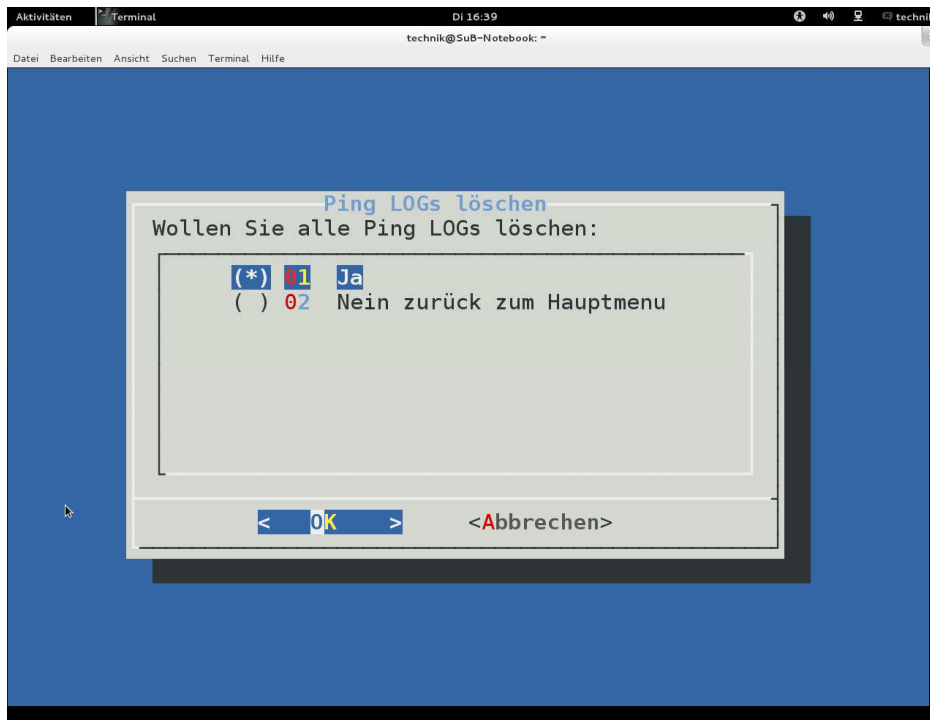


Anleitung Nagios-Box

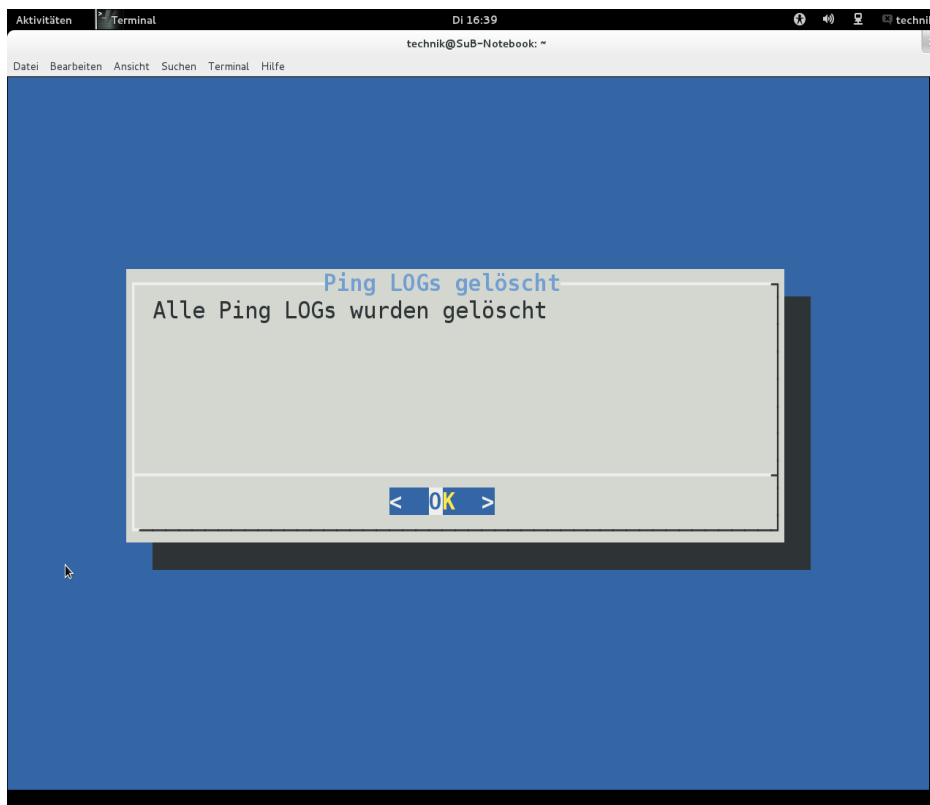
Menu Punkt 18: Archivierte Ping Logs löschen

Es werden hierbei alle archivierten Ping Logs gelöscht (nicht die aktiven)!

Beim Aufruf erscheint das Fenster:



Und nach Bestätigung:



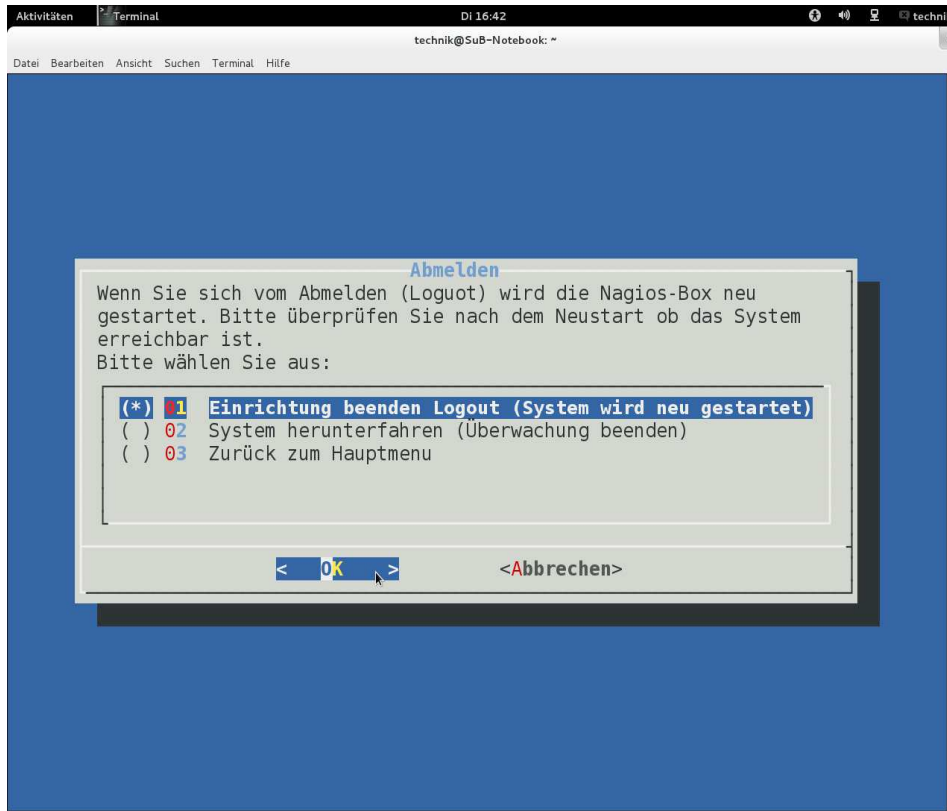
Menu Punkt 19: Logout / System herunterfahren (Alle Einstellungen bleiben erhalten)

Nach Abschluss der Einrichtung oder Administration wird das System unter diesem Menüpunkt verlassen.

Zum verlassen des Systems wird ein Neustart durchgeführt, es können alle angeschlossene Geräte nach dem Neustart entfernt werden. (aber bitte nicht erneut anmelden am System)

Unter diesem Menu Punkt kann das System auch ausgeschaltet werden, nach dem Ausschalten zeichnet das Gerät nichts mehr auf!! Dazu muss das Gerät erst wieder eingeschaltet werden.

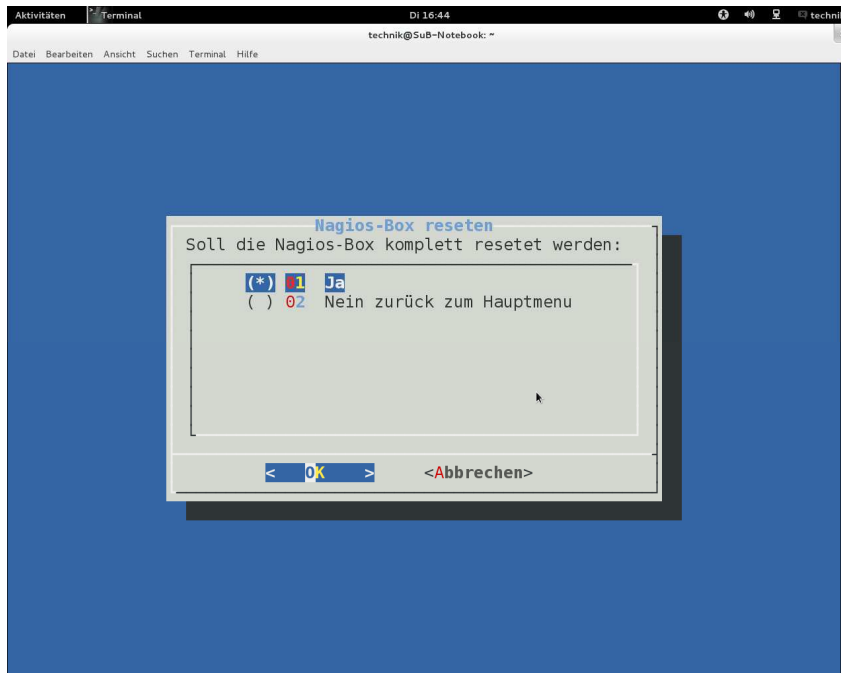
Nach Aufruf des Menu Punktes erscheint:



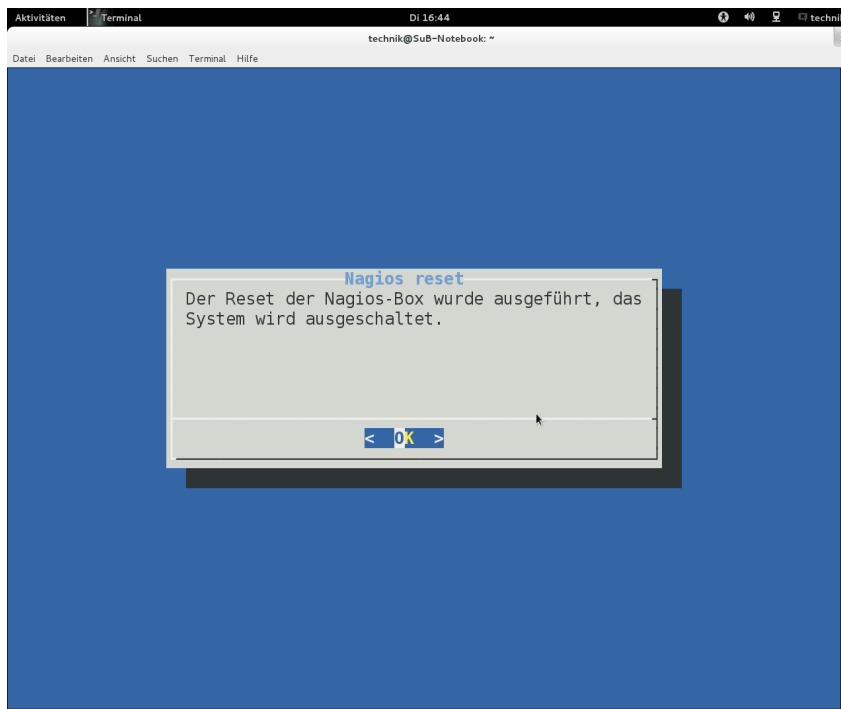
Nach der Auswahl wird mit der Enter Taste der Reboot oder der Shutdown ausgeführt:

Menu Punkt 20: Nagios-Box reseten / System herunterfahren (Einstellungen werden gelöscht)

Ein Reset setzt die Nagios-Box Kompletz zurück alle Logs und Einstellungen werden gelöscht:



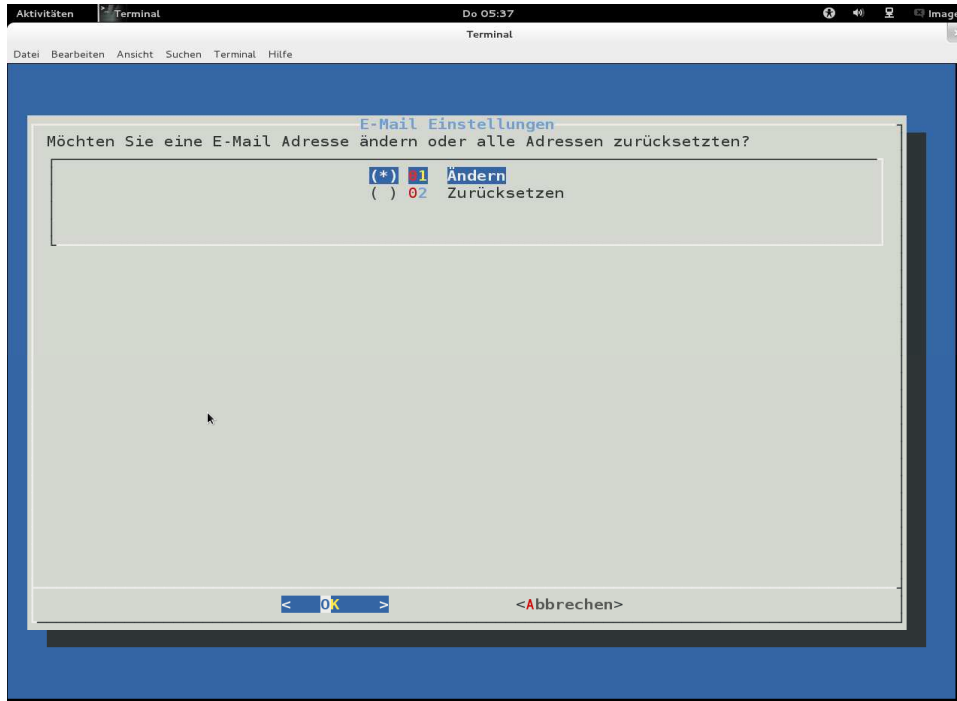
Nach dem Reset wird das System ausgeschaltet:



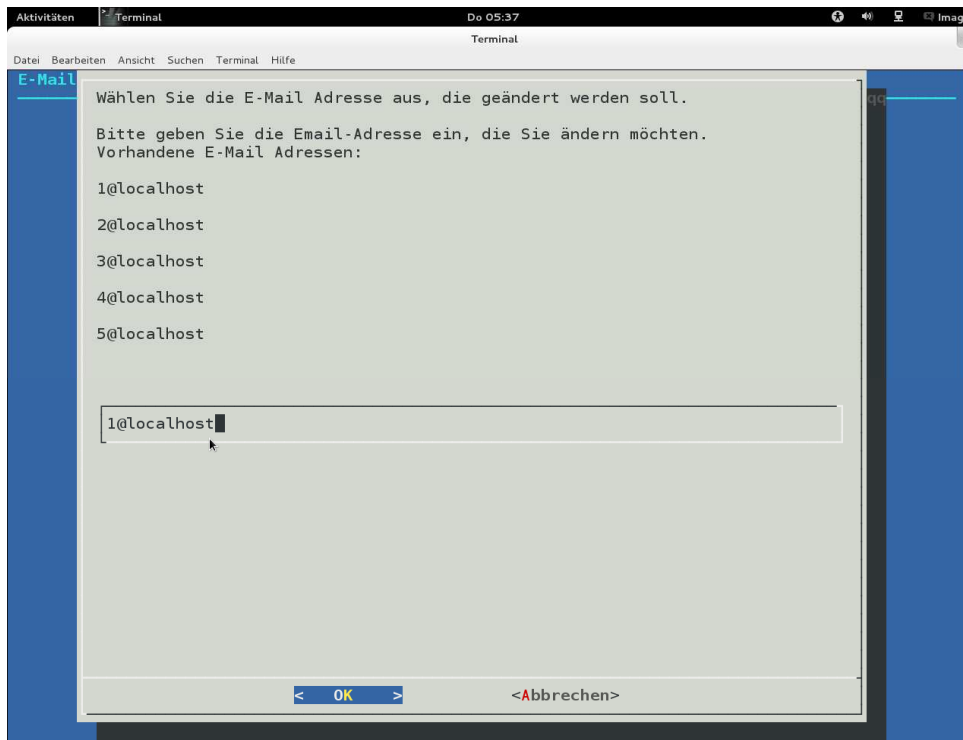
Menu Punkt 21: Mail Adressen für Nagios einrichten oder zurücksetzen

Unter diesem Punkt lassen sich Mailadressen einrichten an die Nagios Fehler-Mails sendet, sollten HOST oder Services ausfallen.

Nach dem Start kommt die Abfrage, ob Mail Adressen ändern oder alle zurücksetzen möchte:

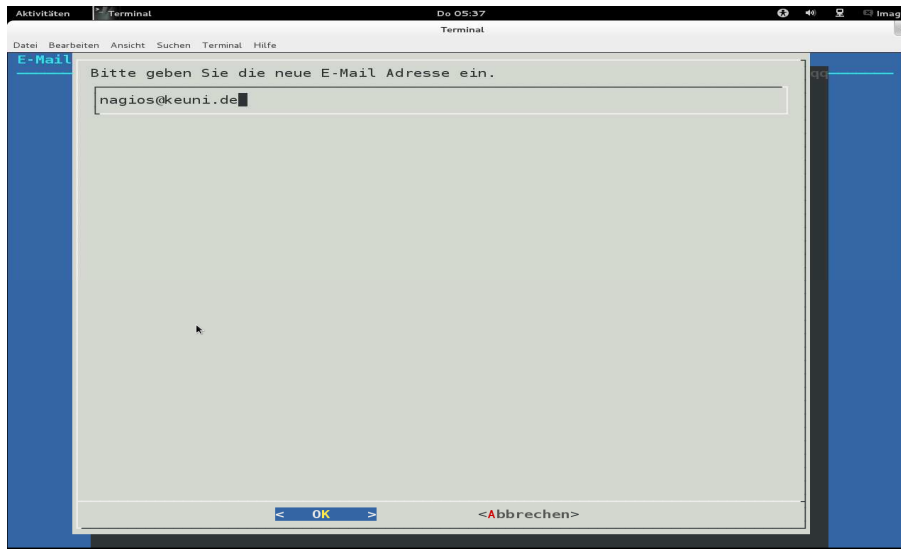


Sind alle Adressen zurückgesetzt sehen die Mail-Adressen wie folgt aus, geben Sie nun die zu ändernde Mail-Adresse ein:

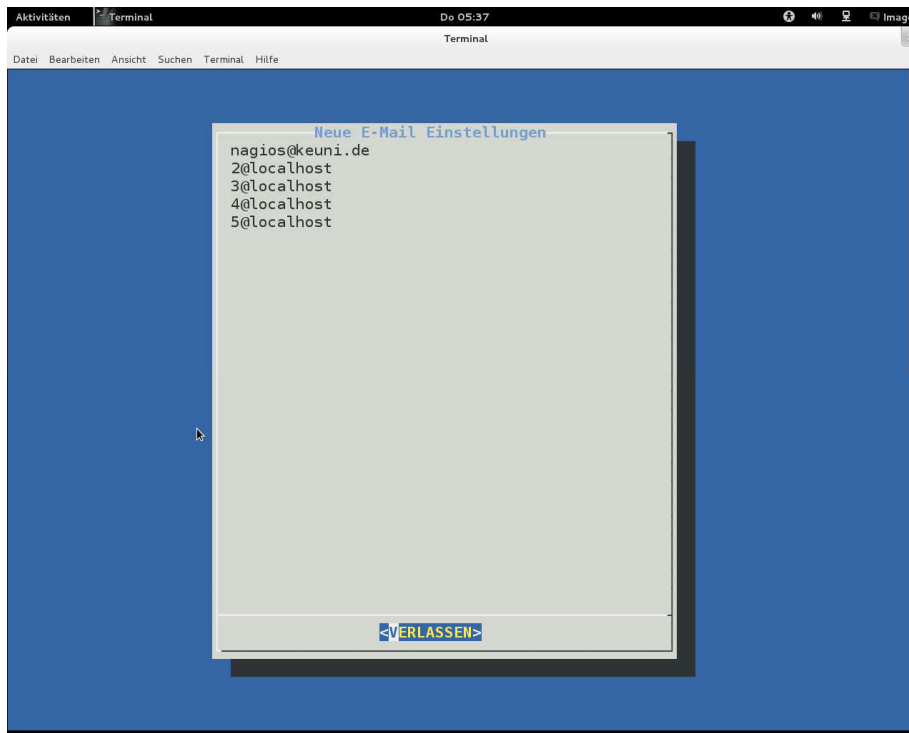


Anleitung Nagios-Box

Danach geben Sie die neue Mail Adresse ein:



Zuletzt werden die neuen Mail Adressen Einstellungen angezeigt:



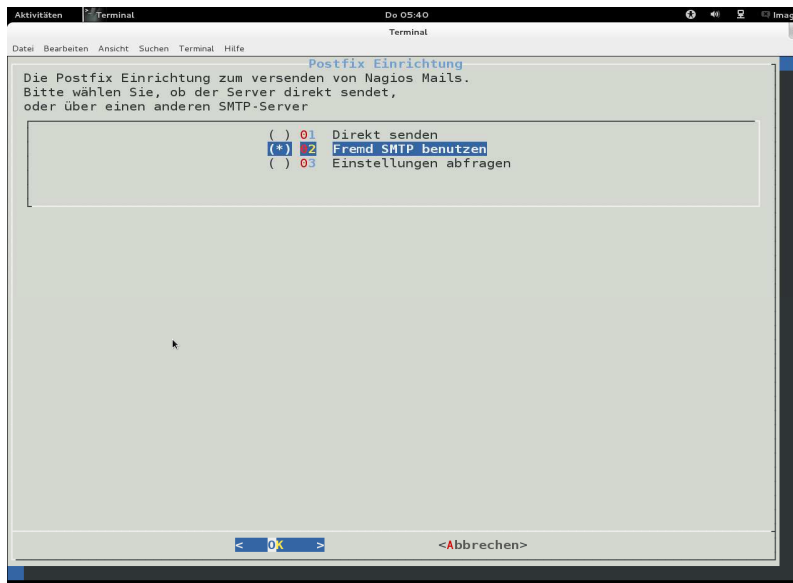
Nach Verlassen der Ansicht werden die neuen Adressen übernommen.

Menu Punkt 22: Mail-Zustellung mit Postfix einrichten

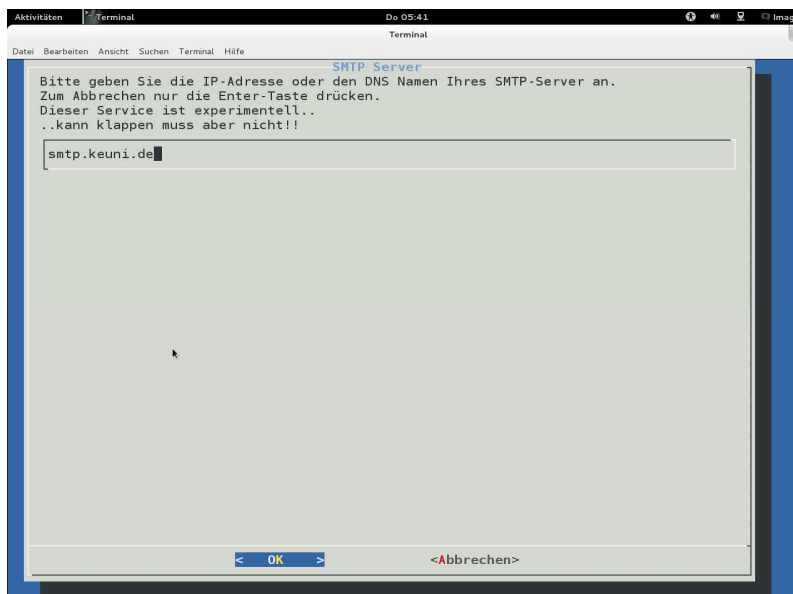
Die Nagios-Box verfügt mit Postfix über einen vollständigen Mail-Server. Der Mail-Server ist standardmäßig so konfiguriert, dass er Mails direkt sendet. Dieses funktioniert aber nur, wenn die Nagios-Box über eine feste Internetadresse verfügt. Dynamische IP-Adressen werden von allen Providern (t-online, web.de gmx, g-mail etc.) nicht akzeptiert und damit abgewiesen. Man kann in diesem Fall einen Fremd SMTP-Server (Relayhost) einrichten.

Leider haben fast alle Provider unterschiedliche Anmeldebedingungen, dies kann Klappen muss aber nicht. (getestet habe ich es mit web.de und domainfactory beim ersten gings nicht beim zweiten schon.)

Nach dem Start wählt man aus (Direkt senden ist Standard):



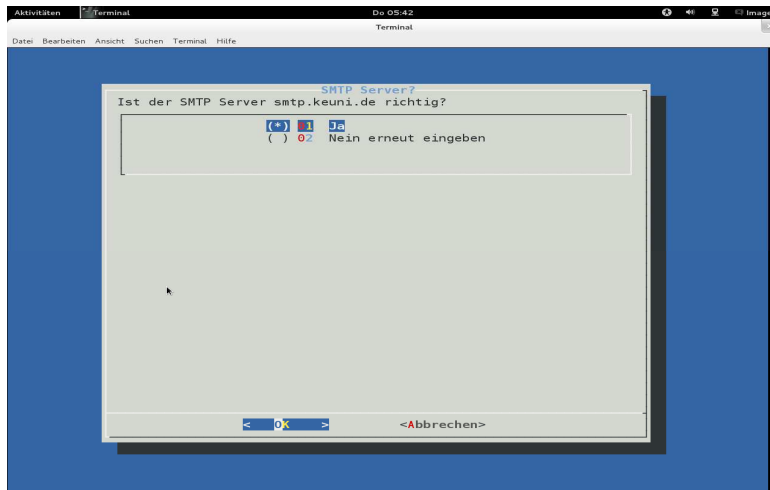
Wählt man Fremd SMTP aus muss man zunächst den SMTP Server eintragen:



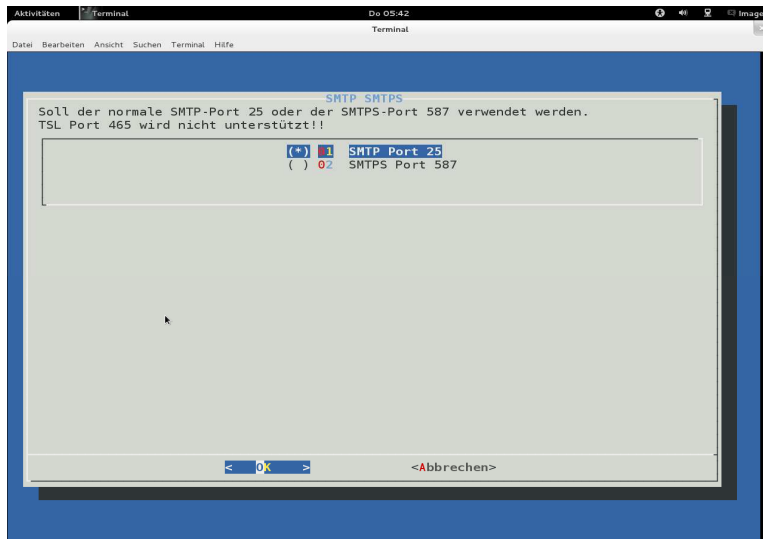
Sofern es kein eigener Mail-Server ist, ist es ratsam den DNS Namen einzugeben.

Anleitung Nagios-Box

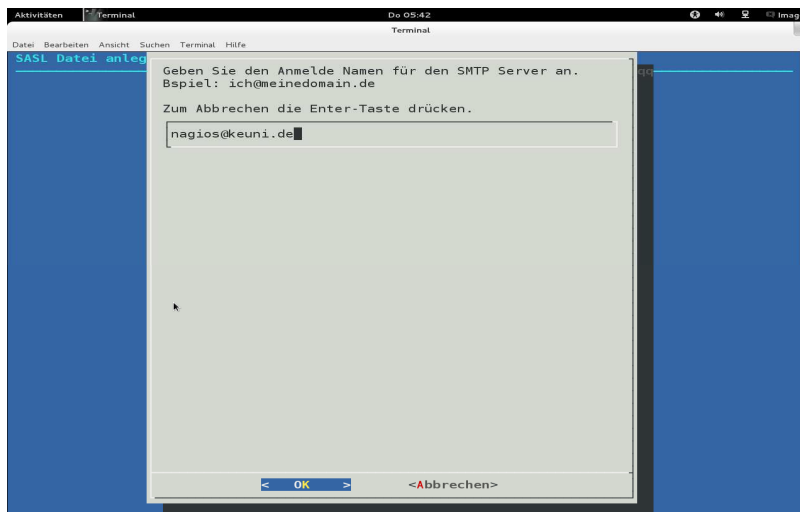
Die Eingabe bestätigen:



Nun wird der Port angegeben SMTP oder SMTPS (der veraltete Secure-Port 465 wird nicht unterstützt):

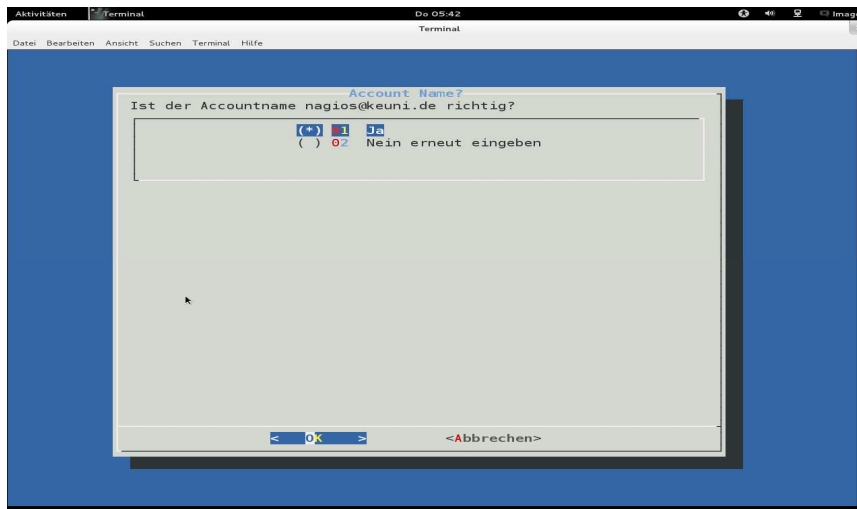


Danach wird der zu verwendende Account eingegeben:

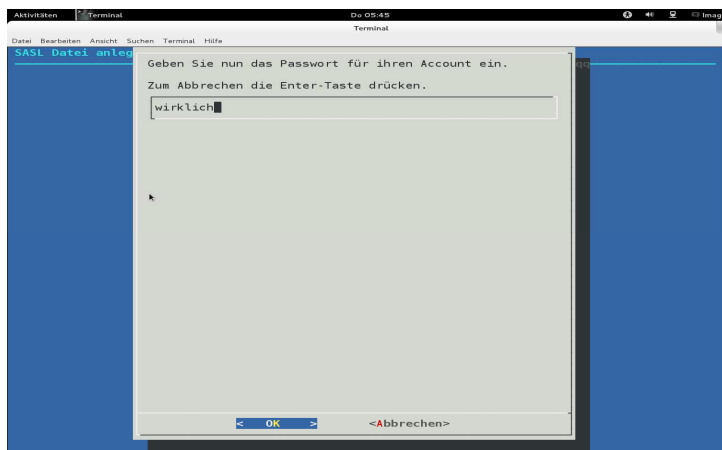


Anleitung Nagios-Box

Den Account-Namen bestätigen:

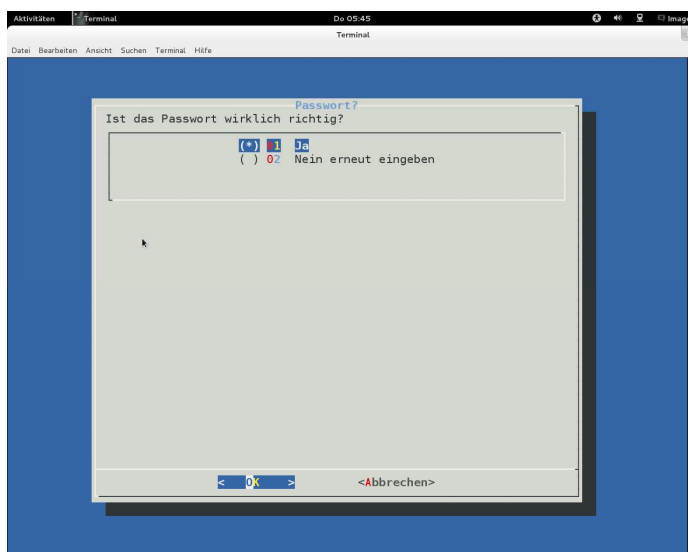


Danach bitte noch das Passwort eingeben:



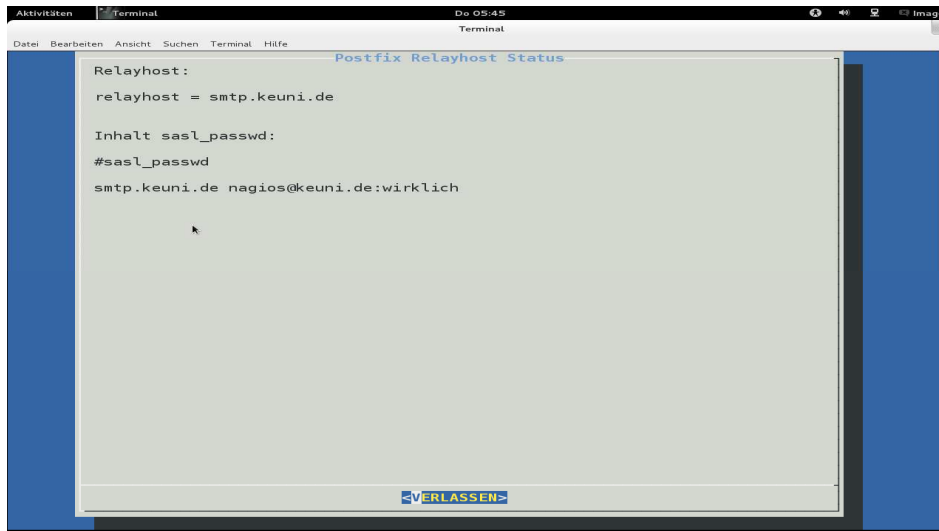
Anmerkung: Das Passwort wird als Hash gespeichert und nicht unverschlüsselt an den Fremd SMTP übergeben:

Das Passwort bitte auch bestätigen:



Anleitung Nagios-Box

Am Ende wird die Konfiguration gezeigt und nach Verlassen der Ansicht übernommen.



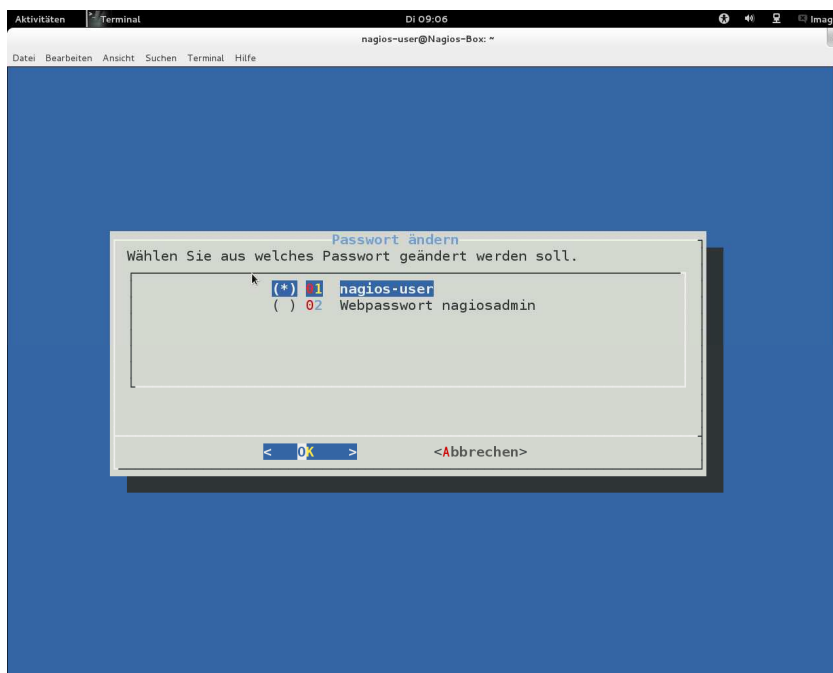
Testen der gesamten Mail Konfiguration:

Am einfachsten richtet man sich dazu ein System im Nagios ein, welches man zu Testzwecken aus dem Netzwerk entfernen kann. Sobald Nagios den Verlust der Erreichbarkeit bemerkt, sollte die Nagios-Box an die eingetragene Adresse eine Mail Senden. Ob eine Mail gesendet wurde kann man auch lokal überprüfen unter Menu Punkt 9 und 10. Dieses wird genauer im nächsten Kapitel beschrieben.

Menu Punkt 23: Passwörter ändern

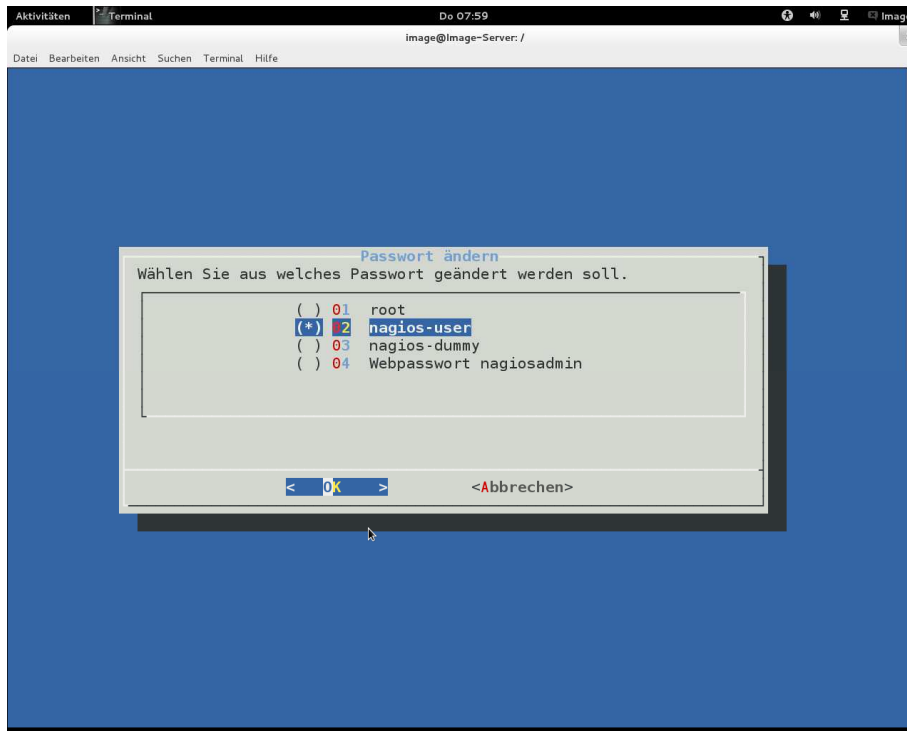
!!Es wird dringend empfohlen, alle Passwörter zu Beginn zu ändern!!

Nach Aufruf des Menu Punktes wird folgender Dialog geöffnet:

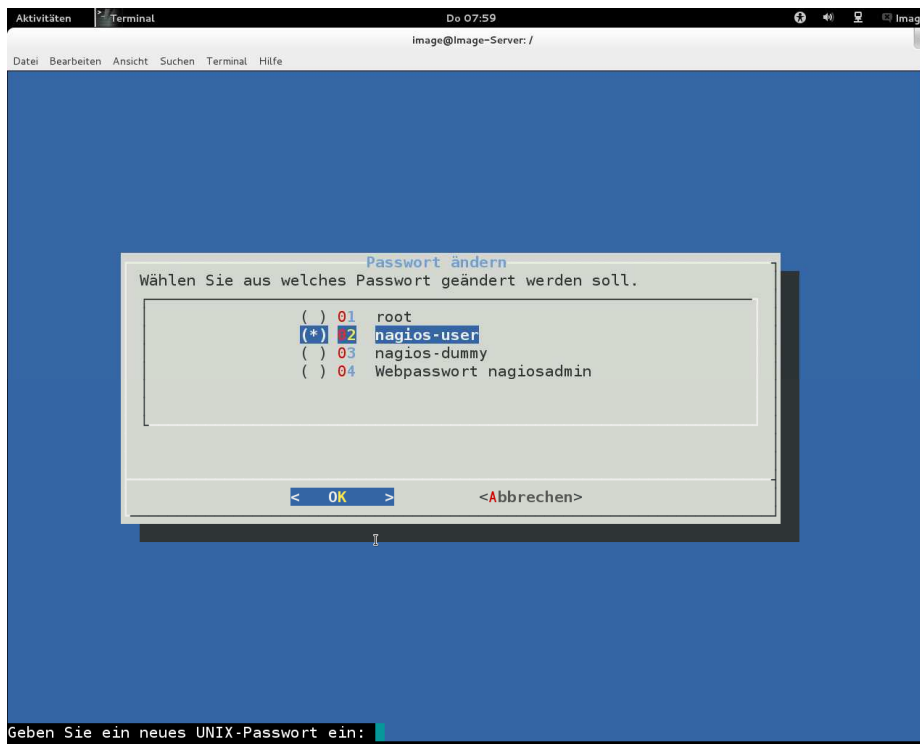


Anleitung Nagios-Box

Es kann nur das eigene Passwort oder das Webpasswort geändert werden. Nur root darf alle Passwörter ändern, ruft root also den Menu Punkt auf erscheint:

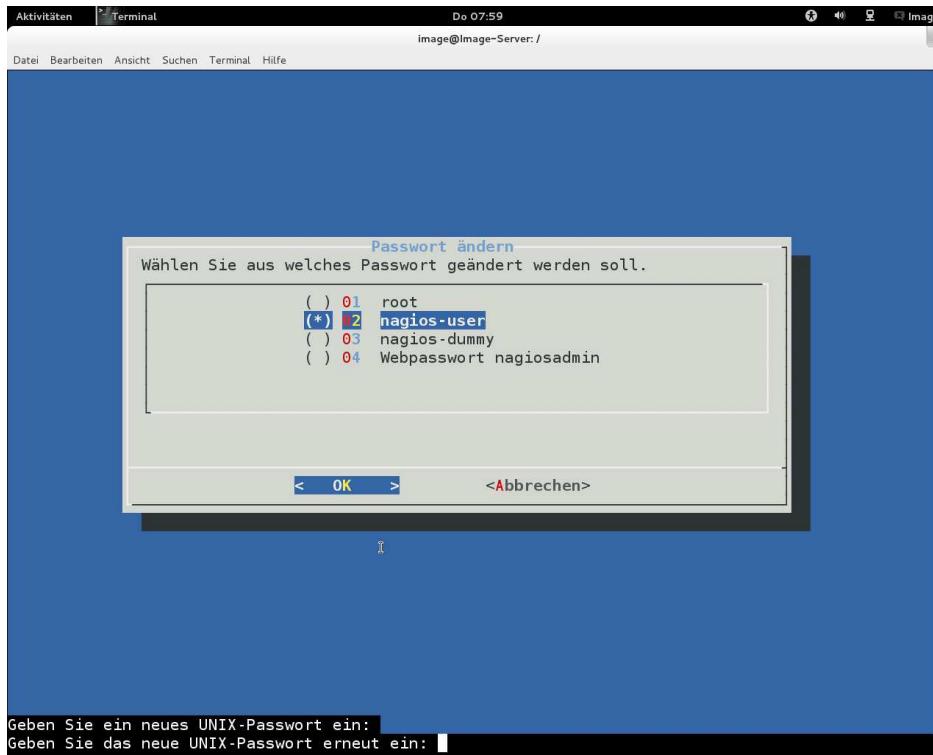


Hat man das zu ändernde Passwort ausgewählt, erscheint am unteren Bildrand die Eingabemöglichkeit für das neue Passwort:

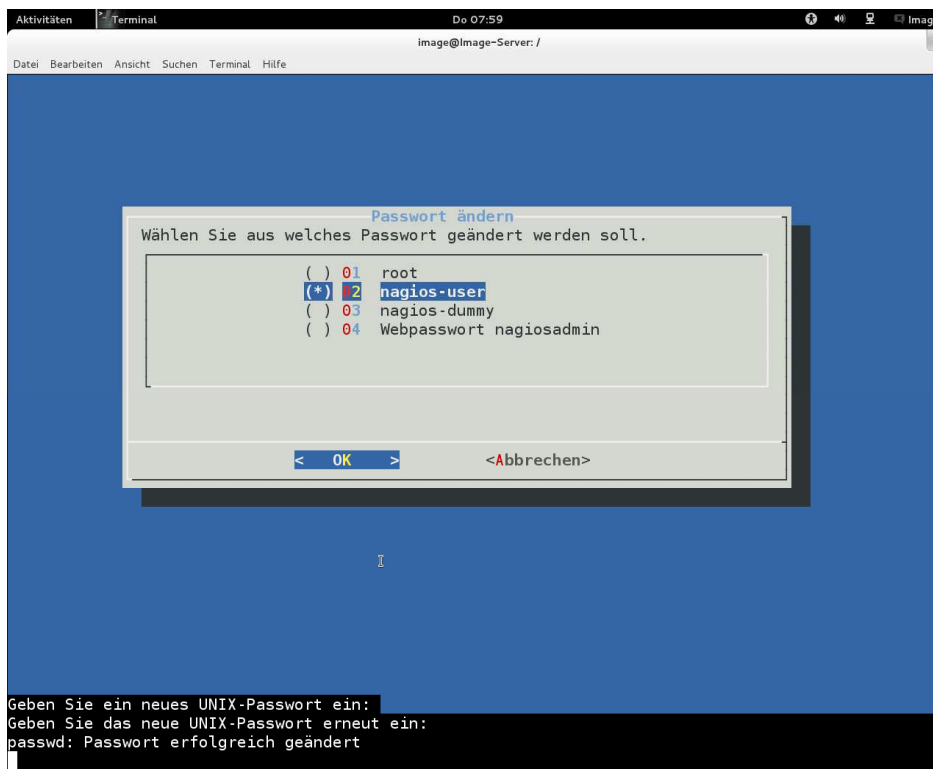


Anleitung Nagios-Box

Das Passwort muss zweimal eingegeben werden:



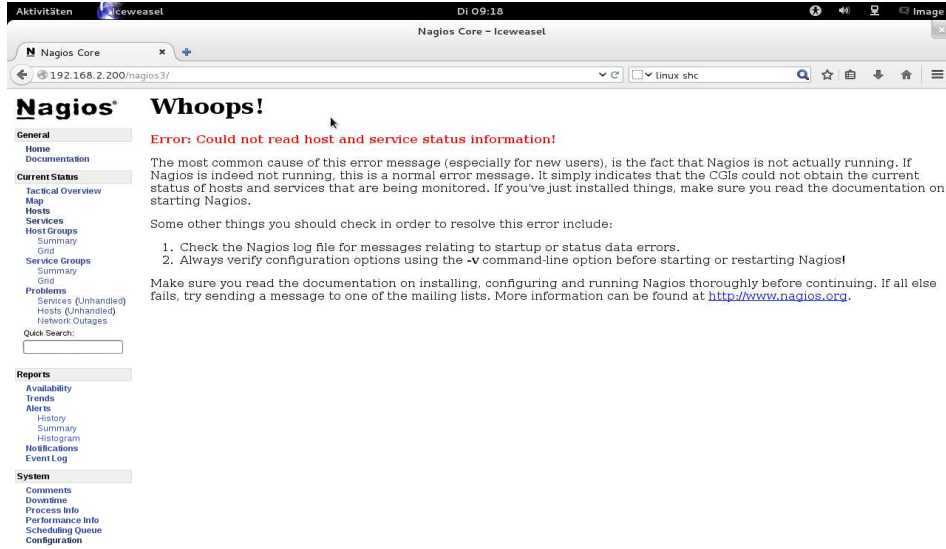
Die Passwortänderung wird bestätigt danach gelangt man wieder ins Haupt-Menü:



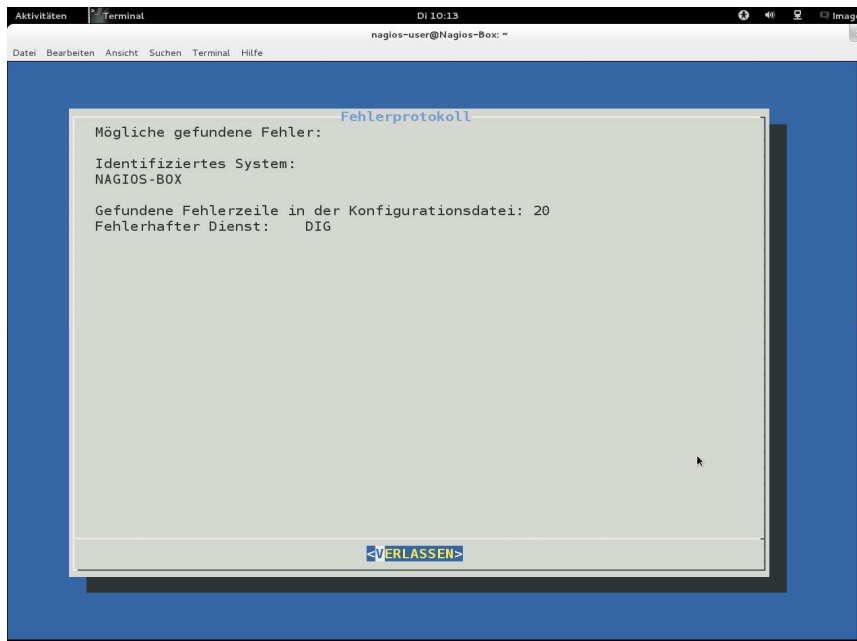
Menu Punkt 24: Fehlersuche Nagios-Konfiguration

Sollte Nagios nicht richtig laufen, oder gar nicht mehr funktionieren kann mit dem Menu Punkt überprüft werden woran dies liegt.

Sollte in der grafischen Oberfläche folgendes erscheinen:



Dann bitte das Programm starten, sollte ein Fehler gefunden werden escheint:



Bitte den Dienst entfernen über Menu Punkt 14 und erneut die Fehlersuche ausführen.

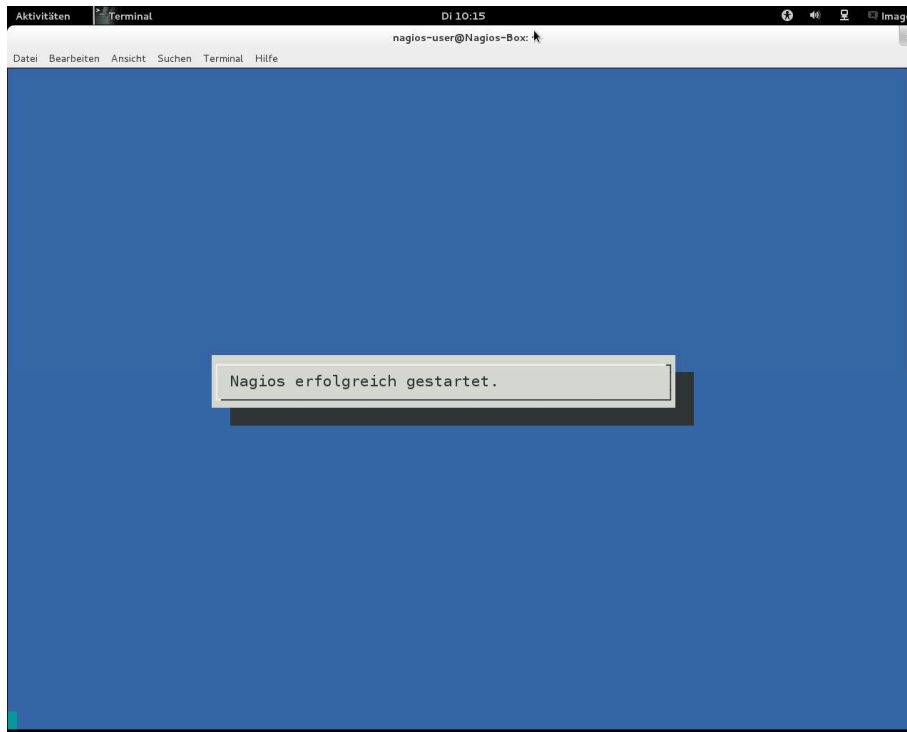
Ist die Konfiguration ok erscheint, „Es konnten keine Fehler gefunden werden.“

Anleitung Nagios-Box

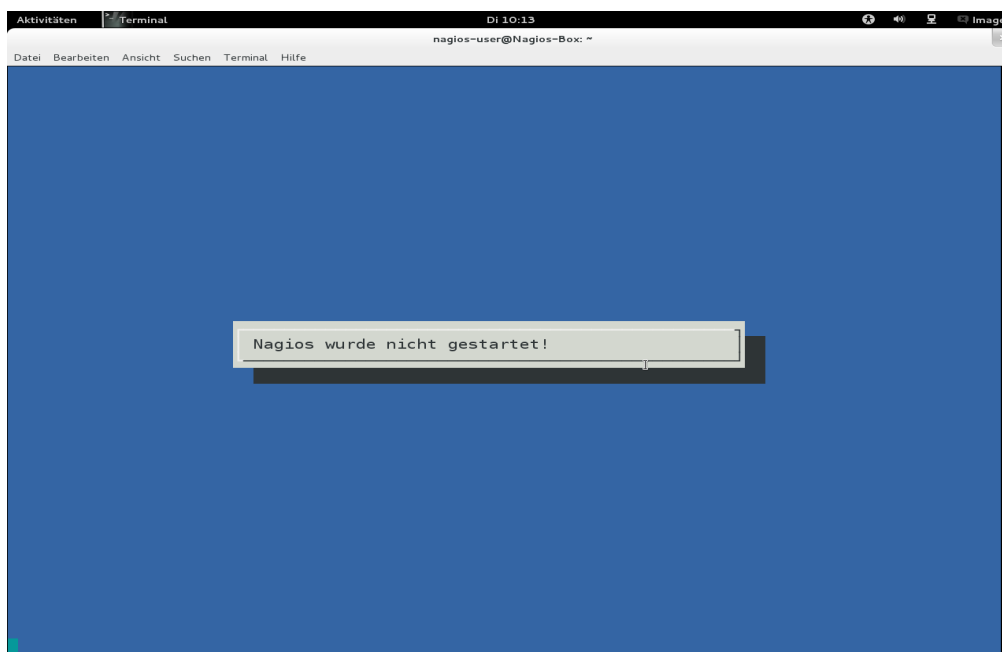
Menu Punkt 25: Nagios neu starten

Beim Ausführen des Menu Punktes wird Nagios neu gestartet.

Ist der Start erfolgreich kommt die Meldung:



Ist der Start nicht erfolgreich kommt die Meldung:



Dann bitte die Fehlersuche durchführen.

Menu Punkt 26: Hilfe zur Nagios-Box

Ruft die Hilfe für das nichtgrafische System auf

5. Auswertungen auf der Nagios-Box

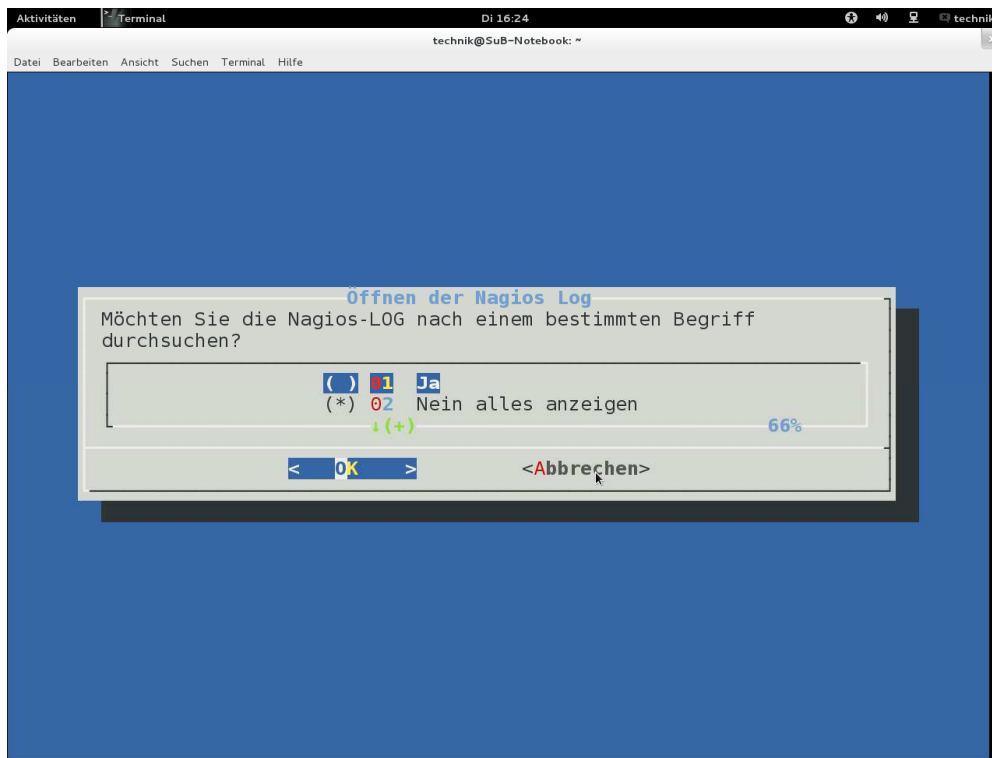
Die Auswertung der Nagios-Box findet im Wesentlichen über eine Web-Oberfläche statt. Einige Auswertungen können aber auch direkt an der Box vorgenommen werden

Einerseits lassen sich Log Dateien öffnen bzw. durchsuchen, es ist aber auch möglich Vorgänge zu beobachten, dabei wird das Ende einer Log Datei angezeigt und sekundlich aktualisiert, man beobachtet da bei in Echtzeit das Verhalten des Systems

Menu Punkt 7: LOG Nagios öffnen / durchsuchen

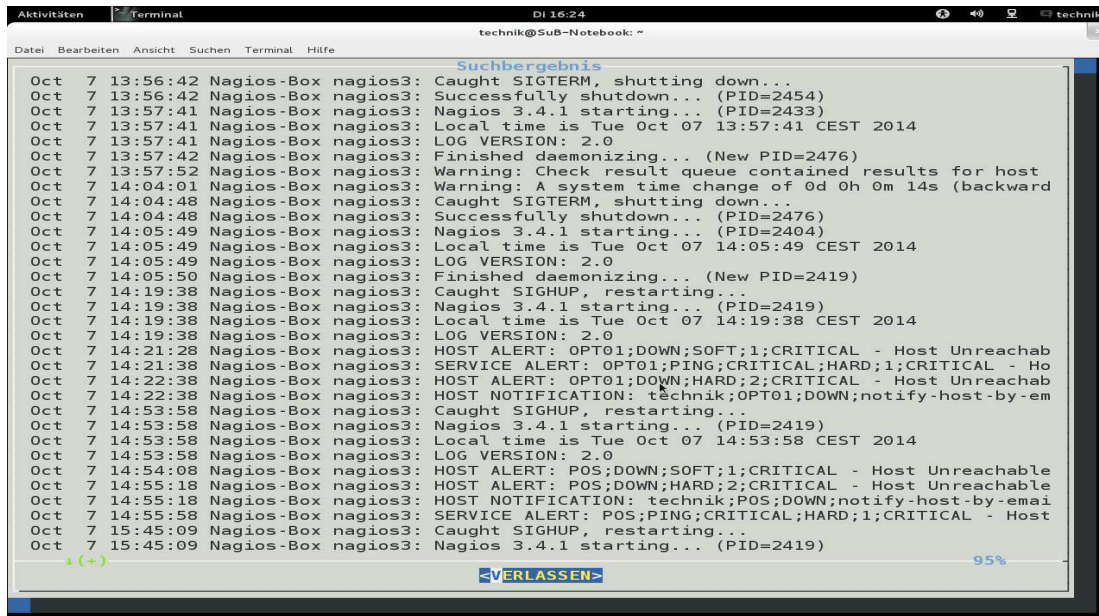
Unter diesem Menu Punkt lässt sich die Nagios Log Datei öffnen bzw. nach bestimmten Ereignissen durchsuchen.

Nach dem Öffnen des Menu Punkts erscheint folgende Auswahl:



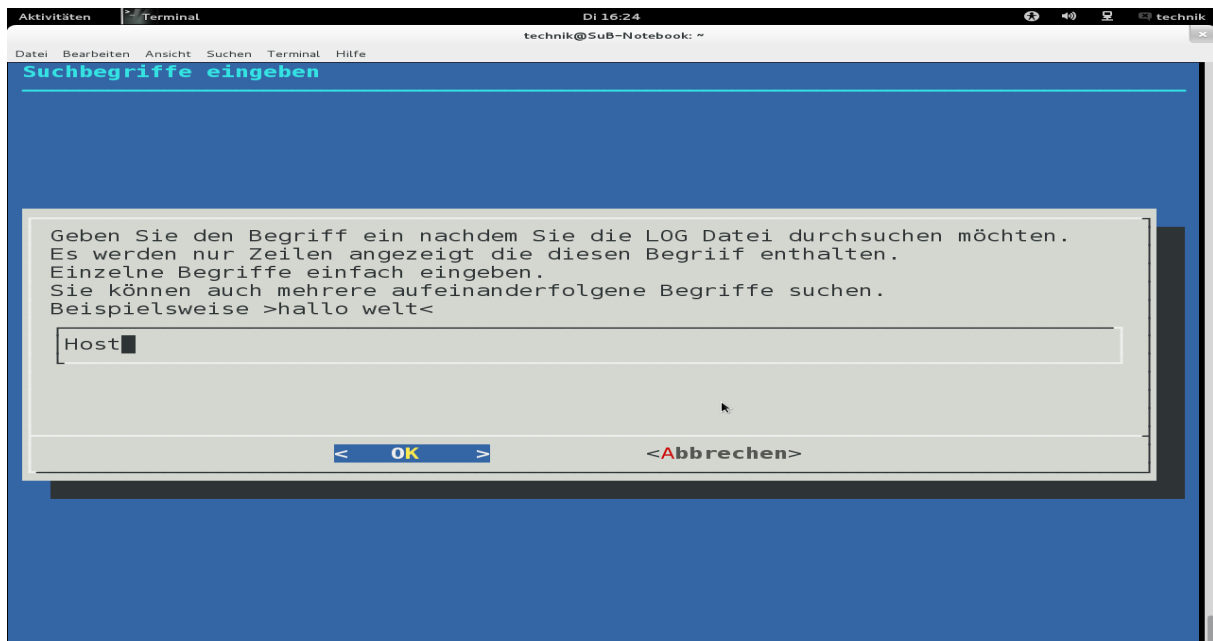
Anleitung Nagios-Box

Wählt man Alles Anzeigen so wird die gesamte Logdatei angezeigt.



```
Oct 7 13:56:42 Nagios-Box nagios3: Caught SIGTERM, shutting down...
Oct 7 13:56:42 Nagios-Box nagios3: Successfully shutdown... (PID=2454)
Oct 7 13:57:41 Nagios-Box nagios3: Nagios 3.4.1 starting... (PID=2433)
Oct 7 13:57:41 Nagios-Box nagios3: Local time is Tue Oct 07 13:57:41 CEST 2014
Oct 7 13:57:41 Nagios-Box nagios3: LOG VERSION: 2.0
Oct 7 13:57:42 Nagios-Box nagios3: Finished daemonizing... (New PID=2476)
Oct 7 13:57:52 Nagios-Box nagios3: Warning: Check result queue contained results for host
Oct 7 14:04:01 Nagios-Box nagios3: Warning: A system time change of 0d 0h 0m 14s (backward
Oct 7 14:04:48 Nagios-Box nagios3: Caught SIGTERM, shutting down...
Oct 7 14:04:48 Nagios-Box nagios3: Successfully shutdown... (PID=2476)
Oct 7 14:05:49 Nagios-Box nagios3: Nagios 3.4.1 starting... (PID=2404)
Oct 7 14:05:49 Nagios-Box nagios3: Local time is Tue Oct 07 14:05:49 CEST 2014
Oct 7 14:05:49 Nagios-Box nagios3: LOG VERSION: 2.0
Oct 7 14:05:50 Nagios-Box nagios3: Finished daemonizing... (New PID=2419)
Oct 7 14:19:38 Nagios-Box nagios3: Caught SIGHUP, restarting...
Oct 7 14:19:38 Nagios-Box nagios3: Nagios 3.4.1 starting... (PID=2419)
Oct 7 14:19:38 Nagios-Box nagios3: Local time is Tue Oct 07 14:19:38 CEST 2014
Oct 7 14:19:38 Nagios-Box nagios3: LOG VERSION: 2.0
Oct 7 14:21:28 Nagios-Box nagios3: HOST ALERT: OPT01;DOWN;SOFT;1;CRITICAL - Host Unreachab
Oct 7 14:21:38 Nagios-Box nagios3: SERVICE ALERT: OPT01;PING;CRITICAL;HARD;1;CRITICAL - Ho
Oct 7 14:22:38 Nagios-Box nagios3: HOST ALERT: OPT01;DOWN;HARD;2;CRITICAL - Host Unreachab
Oct 7 14:22:38 Nagios-Box nagios3: HOST NOTIFICATION: technik;OPT01;DOWN;notify-host-by-em
Oct 7 14:53:58 Nagios-Box nagios3: Caught SIGHUP, restarting...
Oct 7 14:53:58 Nagios-Box nagios3: Nagios 3.4.1 starting... (PID=2419)
Oct 7 14:53:58 Nagios-Box nagios3: Local time is Tue Oct 07 14:53:58 CEST 2014
Oct 7 14:53:58 Nagios-Box nagios3: LOG VERSION: 2.0
Oct 7 14:54:08 Nagios-Box nagios3: HOST ALERT: POS;DOWN;SOFT;1;CRITICAL - Host Unreachable
Oct 7 14:55:18 Nagios-Box nagios3: HOST ALERT: POS;DOWN;HARD;2;CRITICAL - Host Unreachable
Oct 7 14:55:18 Nagios-Box nagios3: HOST NOTIFICATION: technik;POS;DOWN;notify-host-by-emai
Oct 7 14:55:58 Nagios-Box nagios3: SERVICE ALERT: POS;PING;CRITICAL;HARD;1;CRITICAL - Host
Oct 7 15:45:09 Nagios-Box nagios3: Caught SIGHUP, restarting...
Oct 7 15:45:09 Nagios-Box nagios3: Nagios 3.4.1 starting... (PID=2419)
```

Im Falle der Auswahl durchsuchen öffnet sich folgendes Fenster hier lassen sich einzelne Wörter:



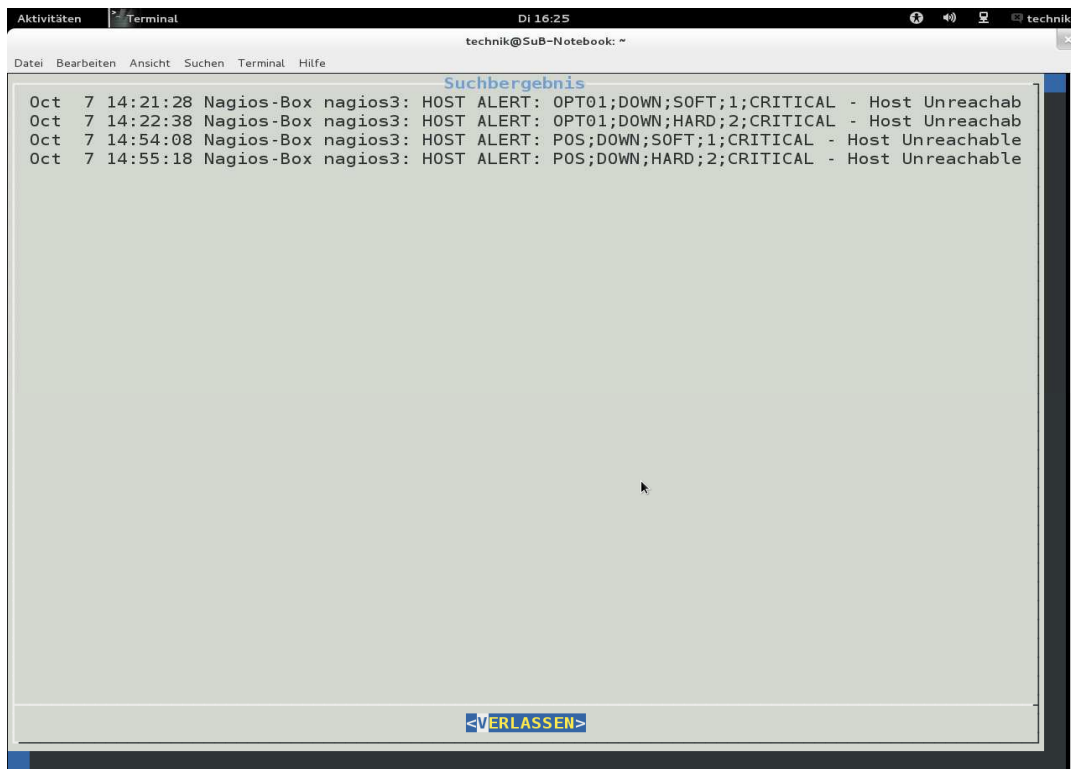
Anleitung Nagios-Box

Oder Zusammenhängende Strings eingeben (Groß und Kleinschreibung ist hier mal egal!):



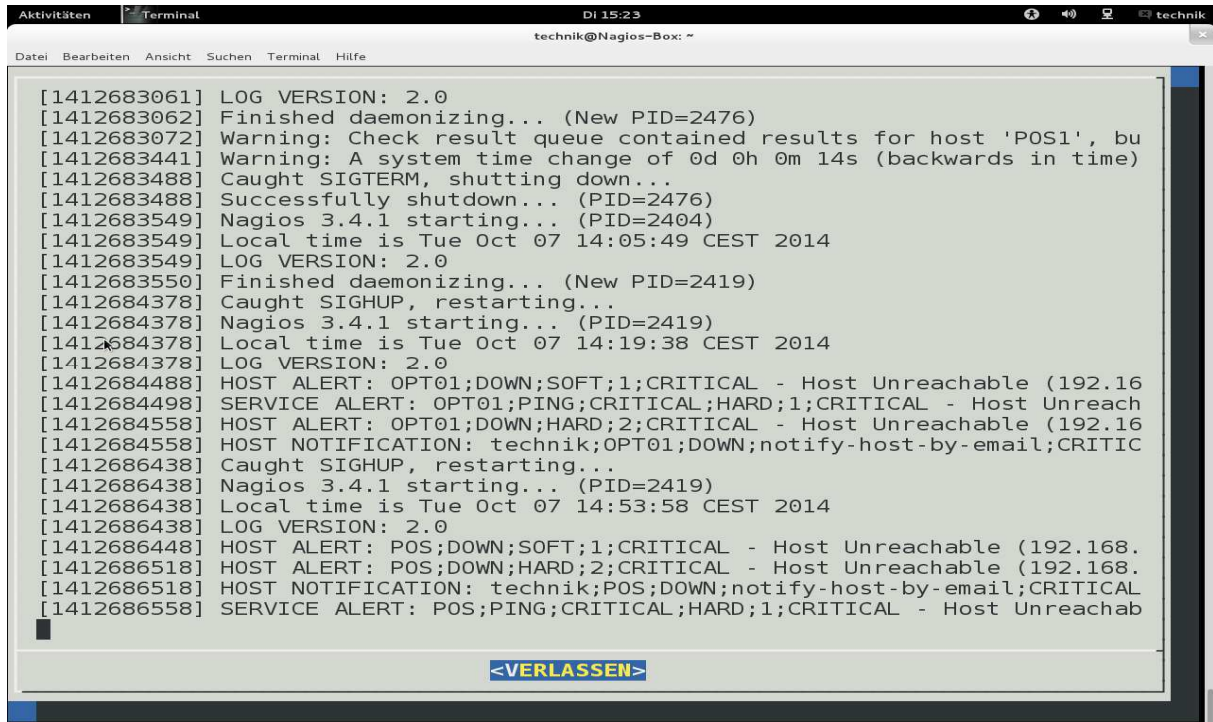
(Sinnvolle Suchstrings werden im Anhang *Anleitung Nagios LOG* erläutert!))

Die Log Datei wird dann nach dem String durchsucht mit folgendem Ergebnis:



Menu Punkt 8: LOG Nagios beobachten

Wie oben bereits erwähnt, beobachtet man hierbei die Nagios Log Datei in Echtzeit:

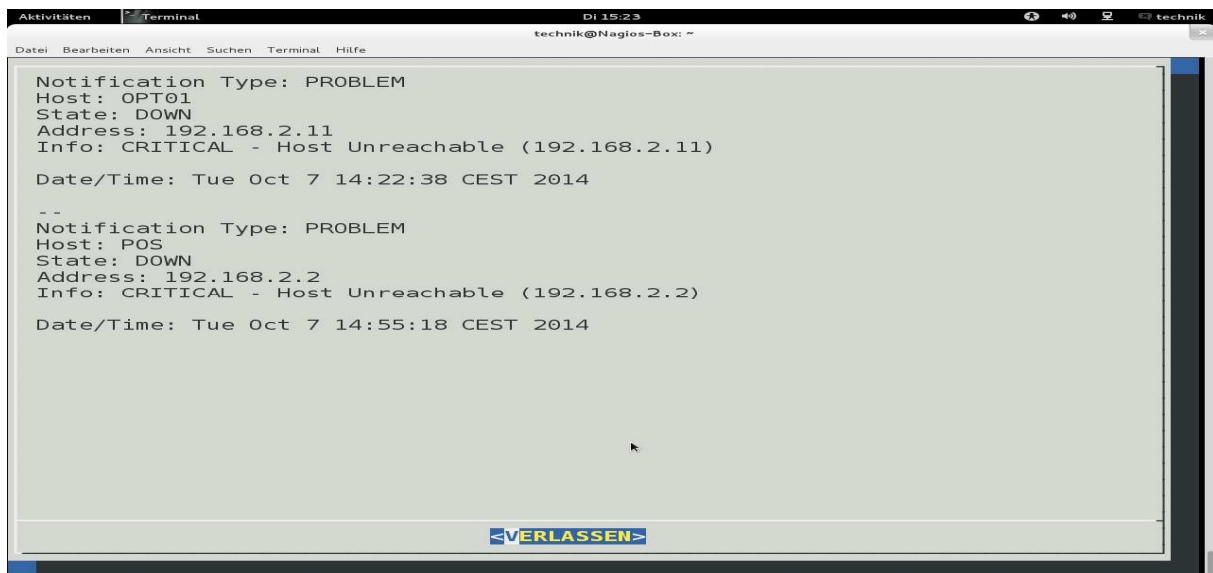


```
[1412683061] LOG VERSION: 2.0
[1412683062] Finished daemonizing... (New PID=2476)
[1412683072] Warning: Check result queue contained results for host 'POS1', bu
[1412683441] Warning: A system time change of 0d 0h 0m 14s (backwards in time)
[1412683488] Caught SIGTERM, shutting down...
[1412683488] Successfully shutdown... (PID=2476)
[1412683549] Nagios 3.4.1 starting... (PID=2404)
[1412683549] Local time is Tue Oct 07 14:05:49 CEST 2014
[1412683549] LOG VERSION: 2.0
[1412683550] Finished daemonizing... (New PID=2419)
[1412684378] Caught SIGHUP, restarting...
[1412684378] Nagios 3.4.1 starting... (PID=2419)
[1412684378] Local time is Tue Oct 07 14:19:38 CEST 2014
[1412684378] LOG VERSION: 2.0
[1412684488] HOST ALERT: OPT01;DOWN;SOFT;1;CRITICAL - Host Unreachable (192.16
[1412684498] SERVICE ALERT: OPT01;PING;CRITICAL;HARD;1;CRITICAL - Host Unreach
[1412684558] HOST ALERT: OPT01;DOWN;HARD;2;CRITICAL - Host Unreachable (192.16
[1412684558] HOST NOTIFICATION: technik;OPT01;DOWN;notify-host-by-email;CRITIC
[1412686438] Caught SIGHUP, restarting...
[1412686438] Nagios 3.4.1 starting... (PID=2419)
[1412686438] Local time is Tue Oct 07 14:53:58 CEST 2014
[1412686438] LOG VERSION: 2.0
[1412686448] HOST ALERT: POS;DOWN;SOFT;1;CRITICAL - Host Unreachable (192.168.
[1412686518] HOST ALERT: POS;DOWN;HARD;2;CRITICAL - Host Unreachable (192.168.
[1412686518] HOST NOTIFICATION: technik;POS;DOWN;notify-host-by-email;CRITICAL
[1412686558] SERVICE ALERT: POS;PING;CRITICAL;HARD;1;CRITICAL - Host Unreachab
```

[<VERLASSEN>](#)

Menu Punkt 9: Nagios Mails öffnen

Hier kann man sogenannte Nagios Notification Mails anzeigen lassen. Diese Mails werden immer dann generiert, wenn sich der Zustand eines Hosts oder Dienstes ändert. Es werden Problems, Warnings und Recoverys angezeigt:



```
Notification Type: PROBLEM
Host: OPT01
State: DOWN
Address: 192.168.2.11
Info: CRITICAL - Host Unreachable (192.168.2.11)

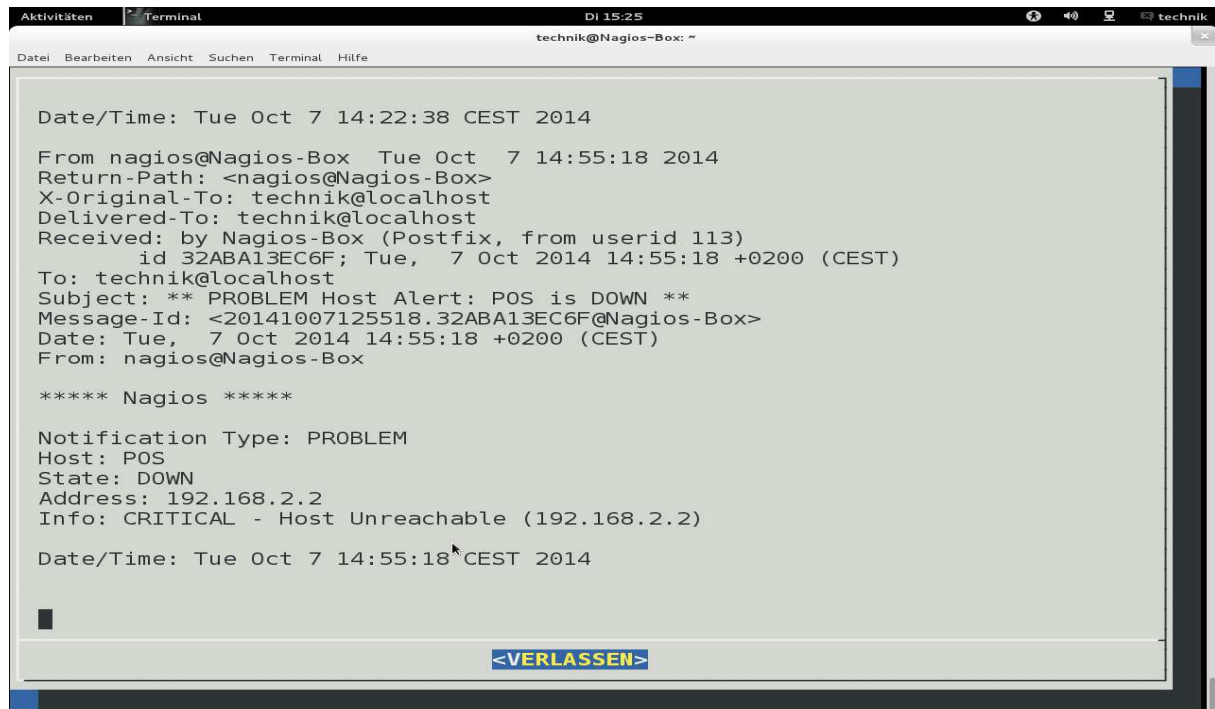
Date/Time: Tue Oct 7 14:22:38 CEST 2014
--
Notification Type: PROBLEM
Host: POS
State: DOWN
Address: 192.168.2.2
Info: CRITICAL - Host Unreachable (192.168.2.2)

Date/Time: Tue Oct 7 14:55:18 CEST 2014
```

[<VERLASSEN>](#)

Menu Punkt 10: Nagios Mails beobachten

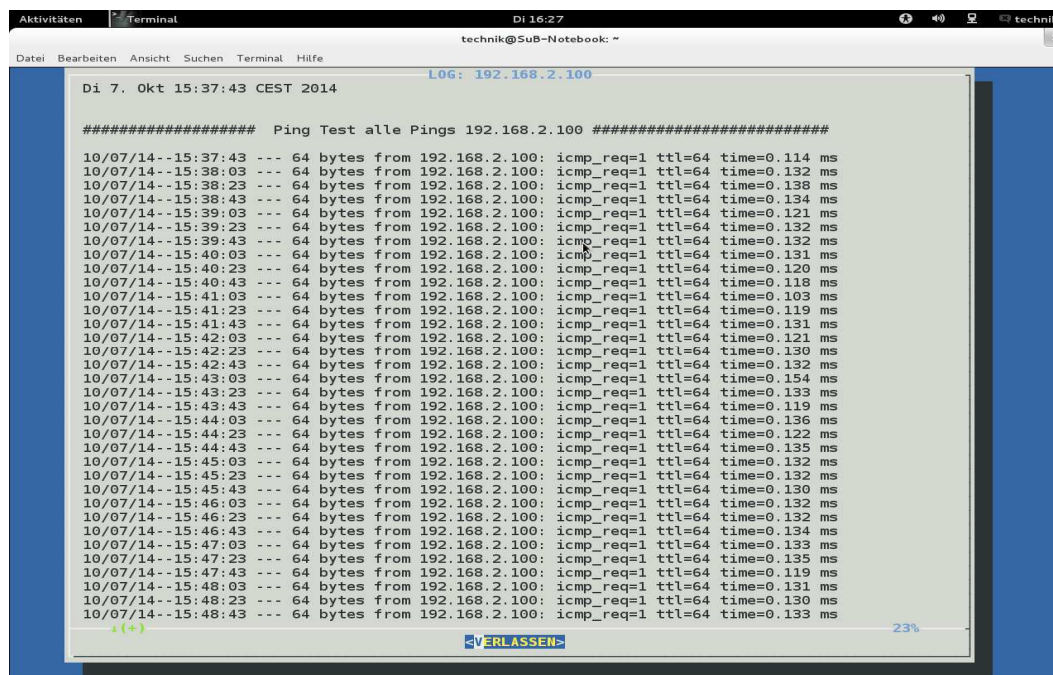
Hierbei werden alle System-Mails in Echtzeit beobachtet:



Menu Punkt 11: LOG Dauerping öffnen

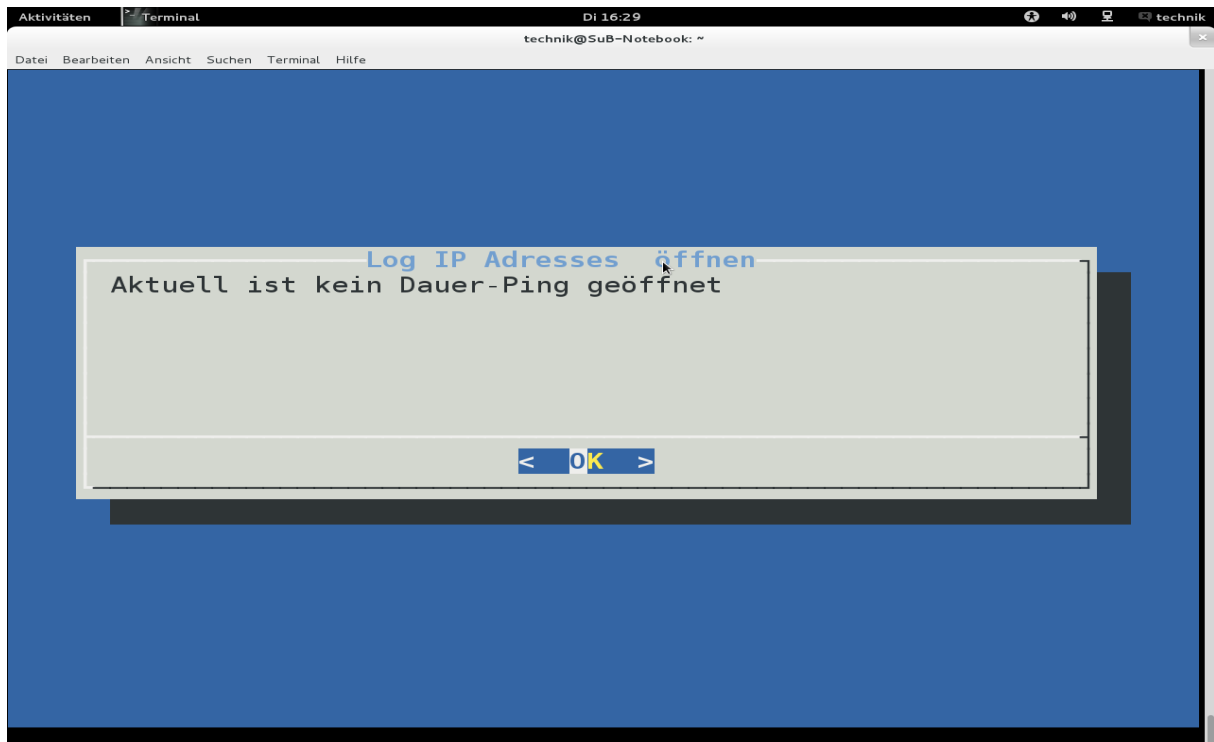
Unter Diesem Menu Punkt lassen sich aktive und archivierte Dauerping Protokolle anzeigen:

Zuerst werden die aktiven Dauerpings angezeigt durch Eingabe der gewünschten IP wird die dazu gehörige Log Datei angezeigt:



Anleitung Nagios-Box

Sind keine Dauerpings aktiv erscheint:

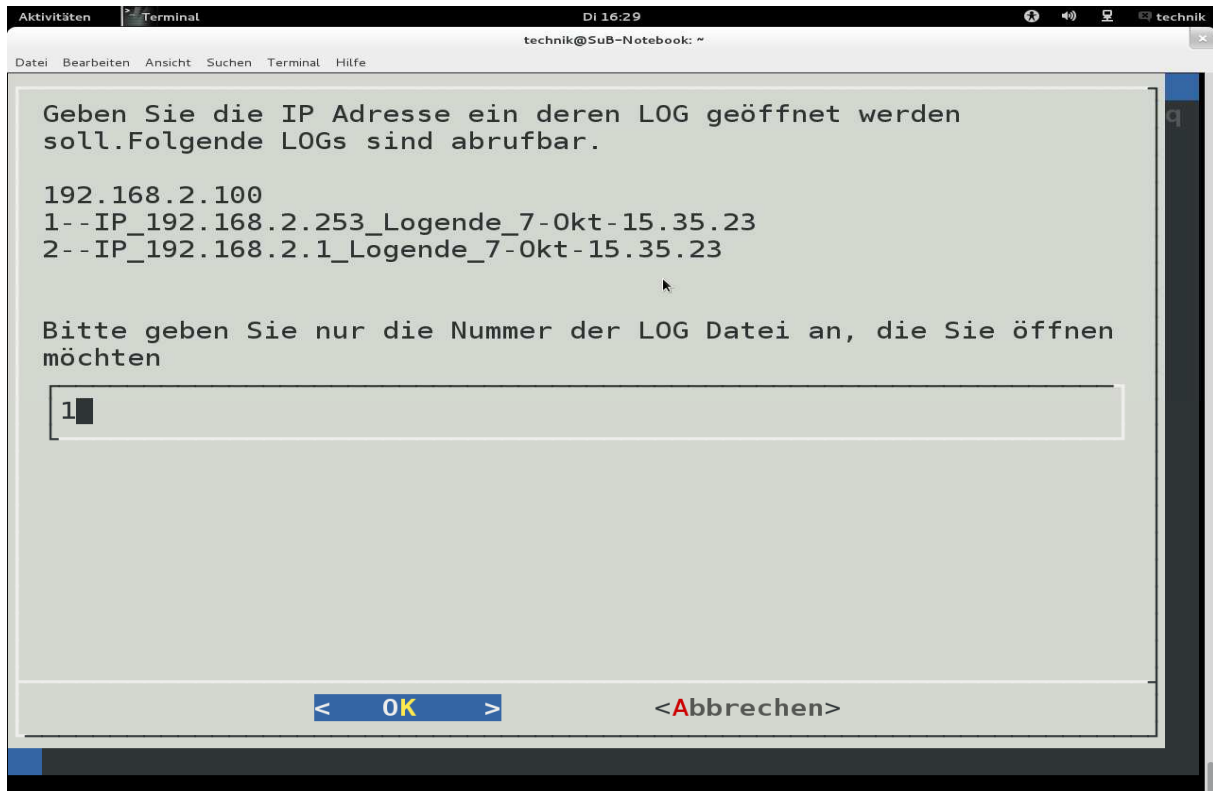


Wenn Protokolle archiviert sind können diese auf Wunsch danach angezeigt werden:

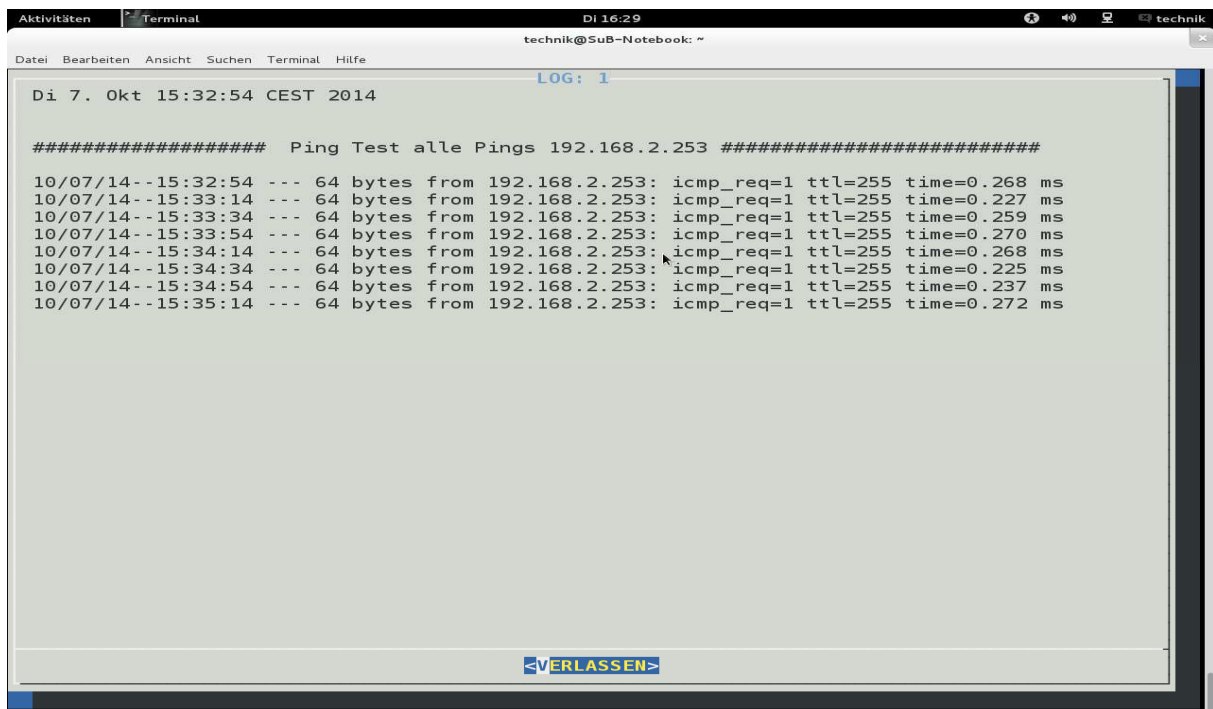


Anleitung Nagios-Box

Man sucht sich die passende Log Datei aus:

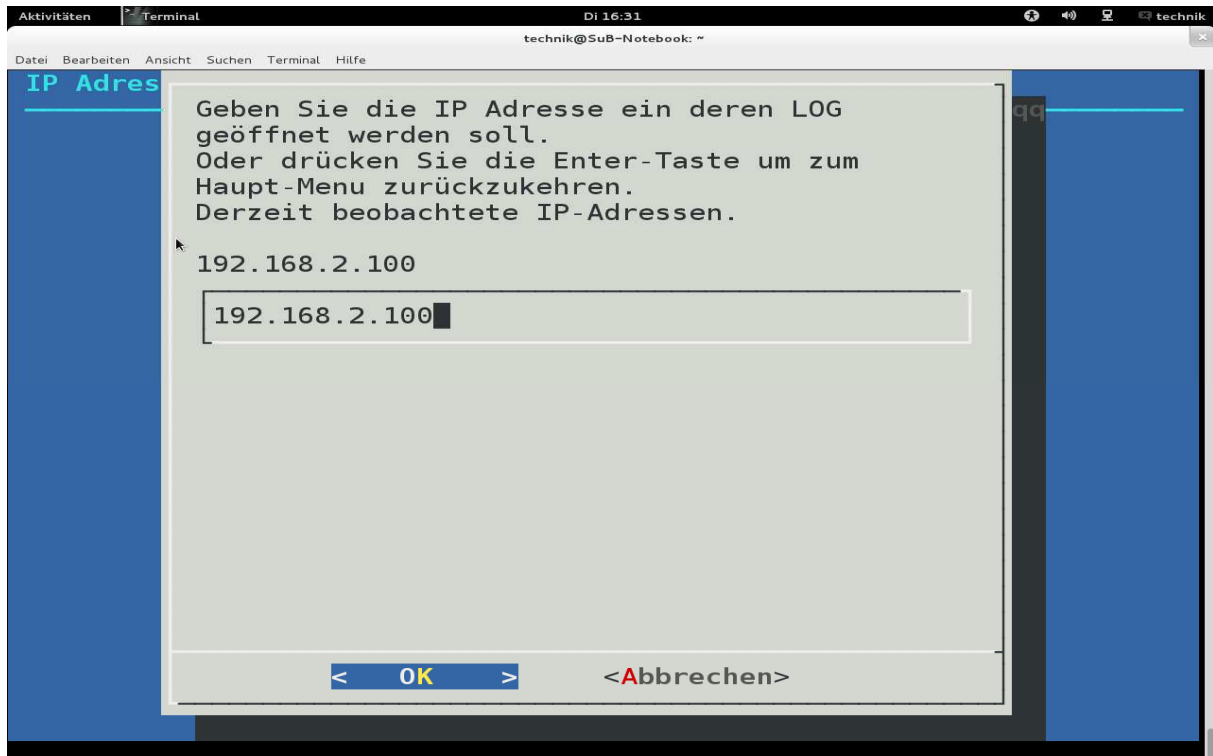


Und erhält folgende Ausgabe:

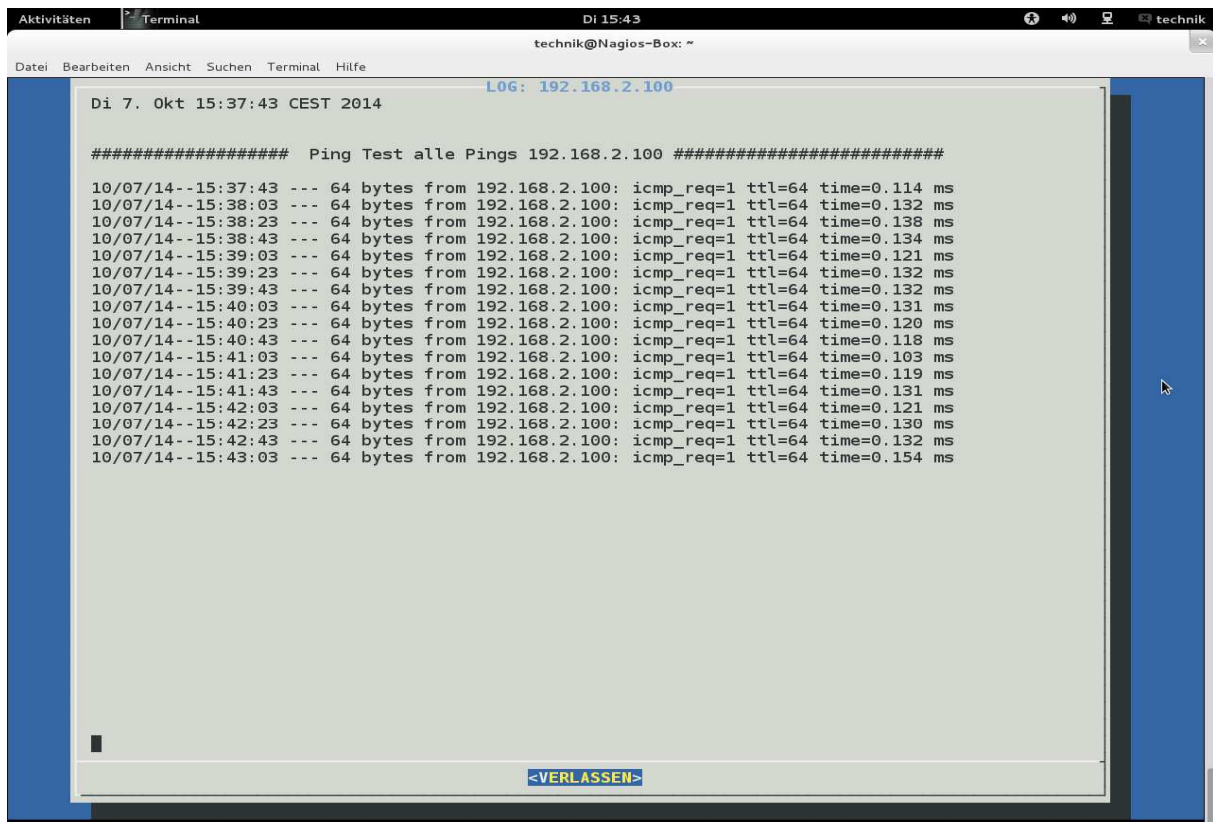


Menu Punkt 12: LOG Dauerping beobachten

Hier lassen sich aktive Dauerpings in Echtzeit beobachten:



Nach der Auswahl wird der aktive Dauerping beobachtet:

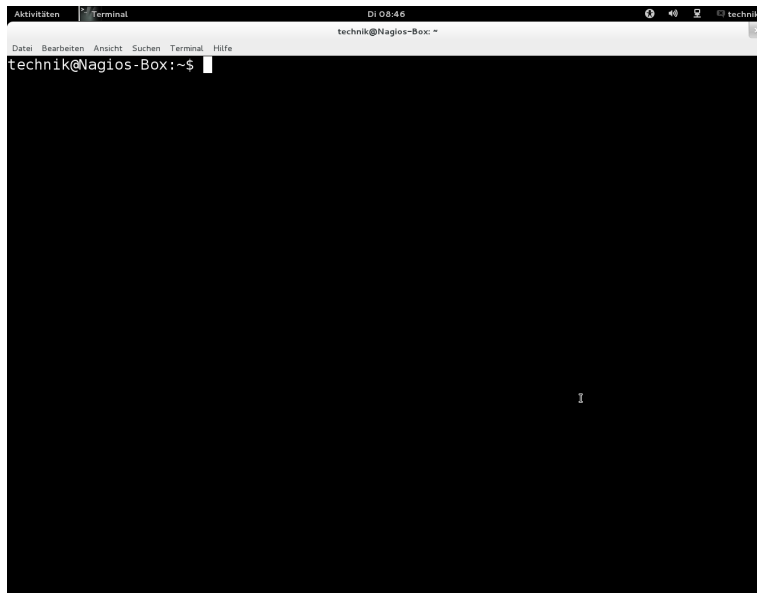


7. Fehlerbilder und Lösungen

Fehler: Das System bootet nicht bis in den Login

- Lösung:**
- a) Nagios-Box bootet gar nicht: Stimmt die BIOS Einstellung?
 - b) System bleibt beim Booten stehen: Sollte sich länger als 4 Minuten nichts mehr passieren, System abschalten, 10 Sek. Warten und neu starten.
 - c) System bleibt erneut stehen: Bitte notieren was zuletzt angezeigt wurde und beim Projektsupport melden

Fehler: Das Nagios Programm wurde nicht automatisch gestartet, nach dem nach dem Login erscheint:



Lösung: Wenn nach erfolgreichem Login das Programm nicht automatisch startet, oder das Programm plötzlich abbricht.

```
nagios-user@Nagios-Box:~$start
```

An der Konsole einfach start eingeben und die Enter-Taste drücken. Das Menu wird dann gestartet.

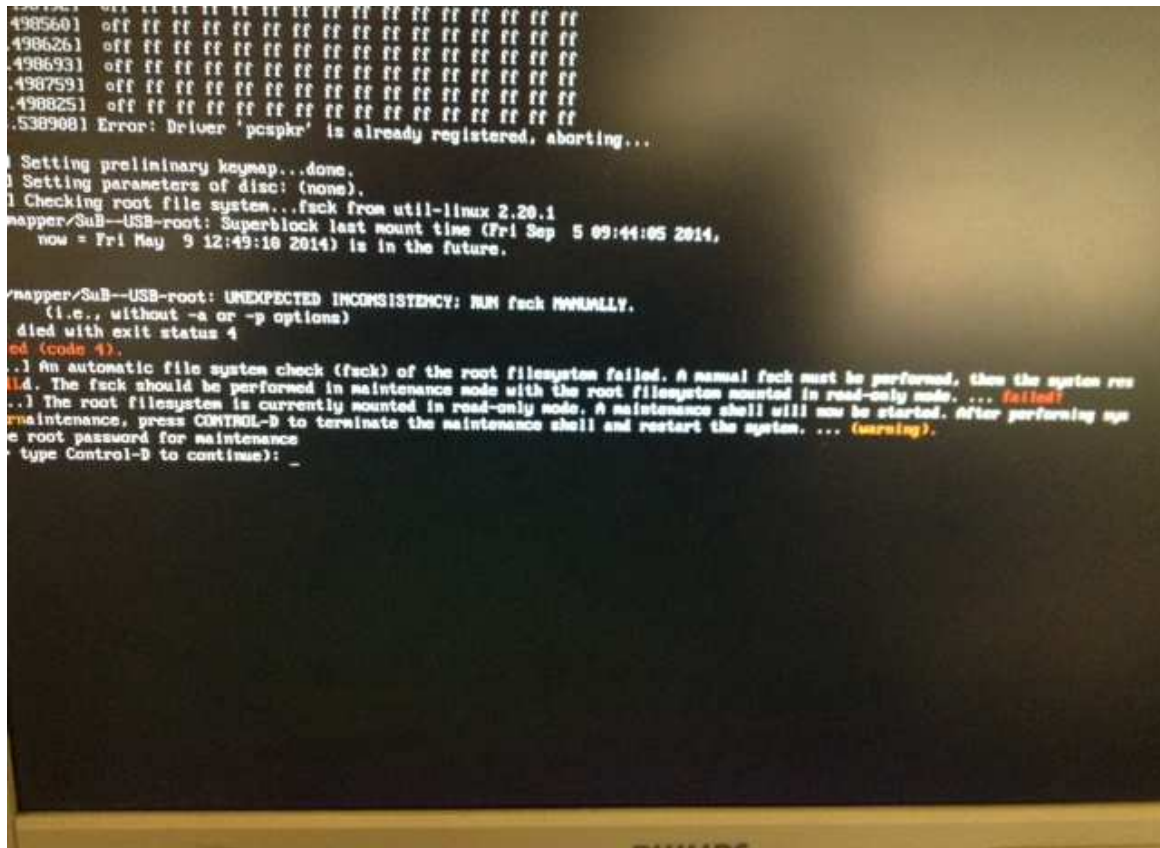
```
nagios-user@Nagios-Box:~$stop
```

Die Eingabe von stop am Eingabeprompt führt ins Shutdown Menu.

Fehler: Nach Auswahl von reboot fährt das System nicht wieder hoch

Lösung: Sollte das Problem bestehen, dass das System nach der Eingabe von reboot nicht neu startet, System ausschalten und nach 10 Sek. wieder anschalten.

Fehler: Nagios-Box bleibt beim Boot mit diesem Bildschirm hängen



Lösung: Bitte System mit der Tastenkombination „Strg“ „d“ neu starten und das Datum und die Zeit im BIOS kontrollieren und ggf. aktualisieren.

Sollte der Boot erneut dort hängen bleiben, ist die Nagios-Box defekt.

Fehler: Das Datum oder die Zeit der Nagios-Box lassen sich im Programm nicht ändern.

Lösung: Dieser Fehler tritt auf, wenn das BIOS mit einem Passwort gesichert ist, in diesem Fall entweder das Datum und die Uhrzeit direkt im BIOS einstellen oder das Passwort entfernen.

Fehler: Nach einem Neustart funktioniert das Netzwerk nichtmehr.

Lösung1: Direkt am System anmelden und IP-Einstellung überprüfen ob die Einträge korrekt sind.

Lösung2: Überprüfen ob sich eine zweite aktive Netzwerkkarte im System befindet.