

Netwatch

Portbasierte Lebend-Überwachung von Servern

Autor: Oliver Keim

Betreuer: Professor Dr. Alfred Scheerhorn

Benutzerhandbuch

Informationen zur Installation,
Bedienung und Fehleranalyse.

| | |
|---|----|
| Vorwort | 3 |
| Systemvoraussetzung | 4 |
| Installation | 6 |
| Hauptfenster | 8 |
| Konfiguration des Mailservers | 10 |
| Kontaktpersonen anlegen | 13 |
| Kontaktpersonen editieren..... | 15 |
| Kontaktpersonen entfernen | 16 |
| Server anlegen | 17 |
| Dienste eines Servers editieren | 19 |
| Kontaktpersonen eines Servers editieren | 21 |
| Server entfernen | 22 |
| Serverinformationen anzeigen..... | 23 |
| Speichern und Laden der Konfigurationen | 24 |
| Detail-Log | 25 |
| Error-Log..... | 27 |
| Verfügbarkeit eines Servers prüfen..... | 28 |
| Extras..... | 30 |
| Beenden des Tools | 30 |
| Vermeidung von Fehlalarmierungen..... | 31 |

Vorwort

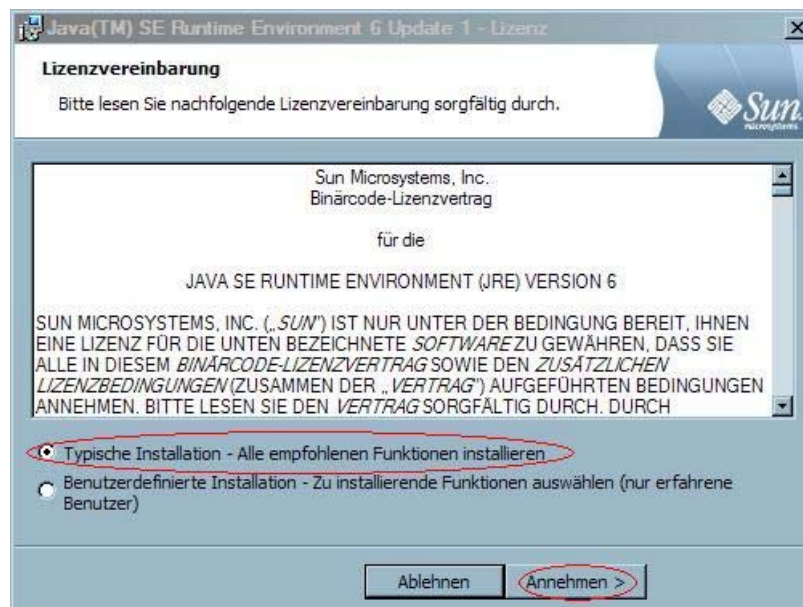
Die Lebend-Überwachung von Servern stellt in vielen Firmen einen wesentlichen Bestandteil des Systemmanagement dar. Besonders im Zeitalter des E-Commerce können Serverausfälle hohe Umsatzeinbußen mit sich bringen. Neben diesen finanziellen Schäden können häufige Serverausfälle auch zu einem Imageverlust führen. Kunden wenden sich ab und beziehen ihre Produkte und Dienstleistungen von konkurrierenden Unternehmen. Um ein möglichst schnelles Reagieren auf solche Ausfälle zu gewährleisten, werden spezielle Tools verwendet, die im Falle einer Störung eine möglichst effiziente Alarmierung durchführen.

Netwatch ist ein solches Tool, welches eine portbasierte Lebend-Überwachung von Servern ermöglicht. Hierbei verwaltet Netwatch nicht nur benutzerdefinierte Server mit ihren konfigurierten Diensten, sondern auch die zugehörigen Kontaktpersonen, die bei Ausfällen benachrichtigt werden. Das Tool baut in regelmäßigen, benutzerdefinierten Zeitabständen TCP -Verbindungen zu den zu überwachenden Diensten der konfigurierten Server auf und prüft somit die Verfügbarkeit dieser Dienste. Bemerkt Netwatch hierbei den Ausfall eines Dienstes, so werden sämtliche, an dem betroffenen Server angemeldete Kontaktpersonen, via E-Mail über den Ausfall benachrichtigt. Weiterhin führt das Tool Log-Dateien, die bei der Analyse und dem Eingrenzen von Fehlerursachen behilflich sein sollen.

Systemvoraussetzung

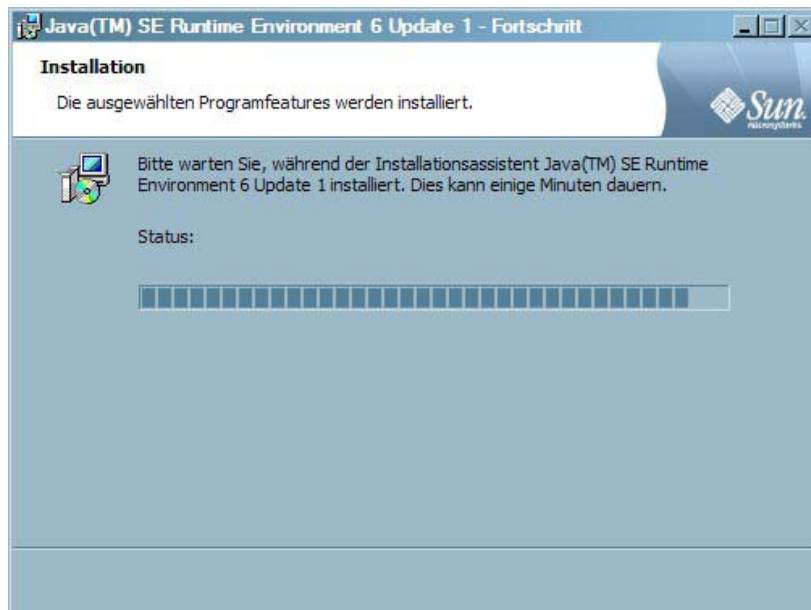
Netwatch wurde in der Programmiersprache Java implementiert. Die Verwendung des Tools ist somit weitgehend plattformunabhängig. Es wird eine Verwendung unter den Betriebssystemen Windows XP, Windows Vista, Mac OS X und den gängigen Linux- bzw. Windows-Servern empfohlen. Zusätzlich benötigt Netwatch eine Installation der Java Runtime Environment¹ (JRE). Das Tool ist lauffähig ab einer JRE in der Version 1.5.0 oder höher. Verwenden Sie bereits eine passende JRE auf Ihrem System, so fahren Sie bitte mit dem Kapitel *Installation* fort.

Falls auf Ihrem System keine JRE vorhanden ist, so können Sie die aktuelle JRE 6.0 installieren. Diese befindet sich auf der Netwatch Installations-CD im Verzeichnis *JRE*. Alternativ steht die JRE auch unter <http://java.sun.com/javase/downloads/index.jsp> auf den Seiten der Firma SUN zum Download bereit. Zum Installieren der JRE von CD starten Sie unter Windows die Datei *jre-6u1-windows-i586-p.exe*. Folgende Abbildungen führen Sie durch die Installation.



Installation JRE 6.0 - Lizenzvereinbarung

¹ Die Java Runtime Environment liefert unter anderem die Java Virtual Machine, welche zum Ausführen von Java Applikationen benötigt wird.



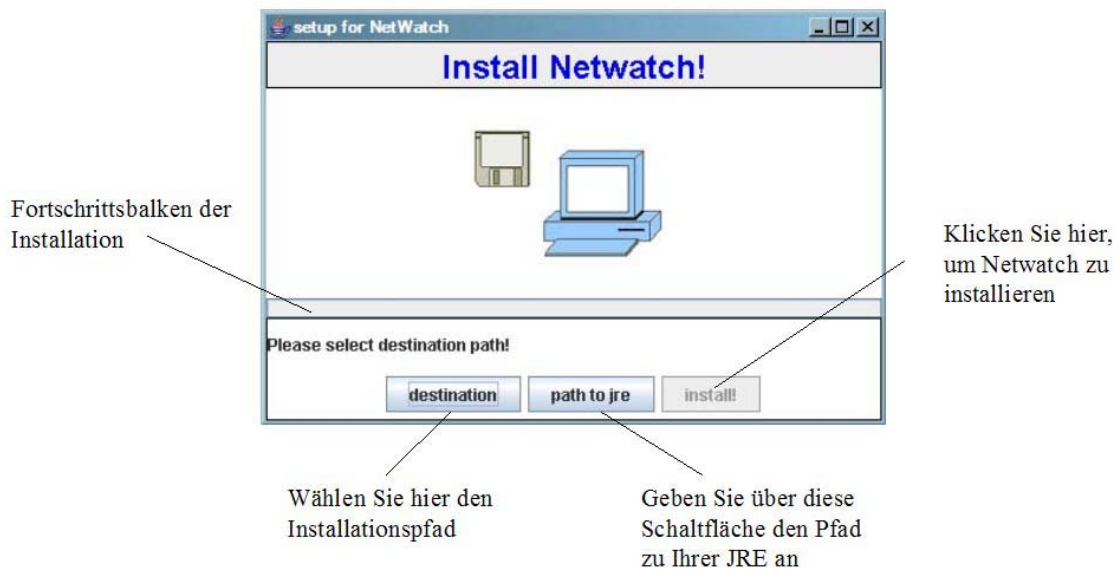
Installation JRE 6.0 - Kopiervorgang



Installation JRE 6.0 - Fertigstellen der Installation

Installation

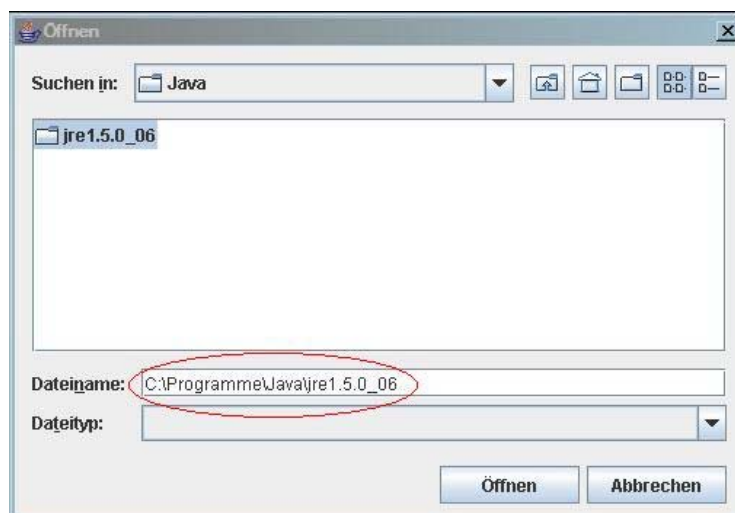
Um Netwatch auf Ihrer Festplatte zu installieren, führen Sie unter dem Betriebssystem Windows die Datei `setup.exe` aus. Falls Sie ein unixbasiertes Betriebssystem, wie z.B. Mac OS verwenden, dann starten Sie die Datei `install.jar`. Es öffnet sich folgender Installationsdialog.



`setup.exe / install.jar`

Wählen Sie den Installationspfad, indem Sie mit der Maus auf die Schaltfläche „destination“ klicken. Es erscheint ein Auswahlfenster, in welchem Sie den Pfad angeben können, unter dem das Tool installiert werden soll.

Damit Netwatch in der Lage ist, E-Mail-Benachrichtigungen durchzuführen, kopiert das Setup die beiden externen Bibliotheken `mail.jar` und `activation.jar` in den Pfad `..\lib\ext`, welcher sich im Verzeichnis Ihrer Java Runtime Environment befindet. Da die Position des Ordners Ihrer JRE auf der Festplatte variieren kann, wählen Sie bitte den korrekten Pfad über die Schaltfläche „path to jre“. Normalerweise befindet sich Ihre JRE unter dem Betriebssystem Windows im Verzeichnis `C:\Programme\Java` oder alternativ unter `C:\program files\Java`.



Pfadangabe zur Java Runtime Environment

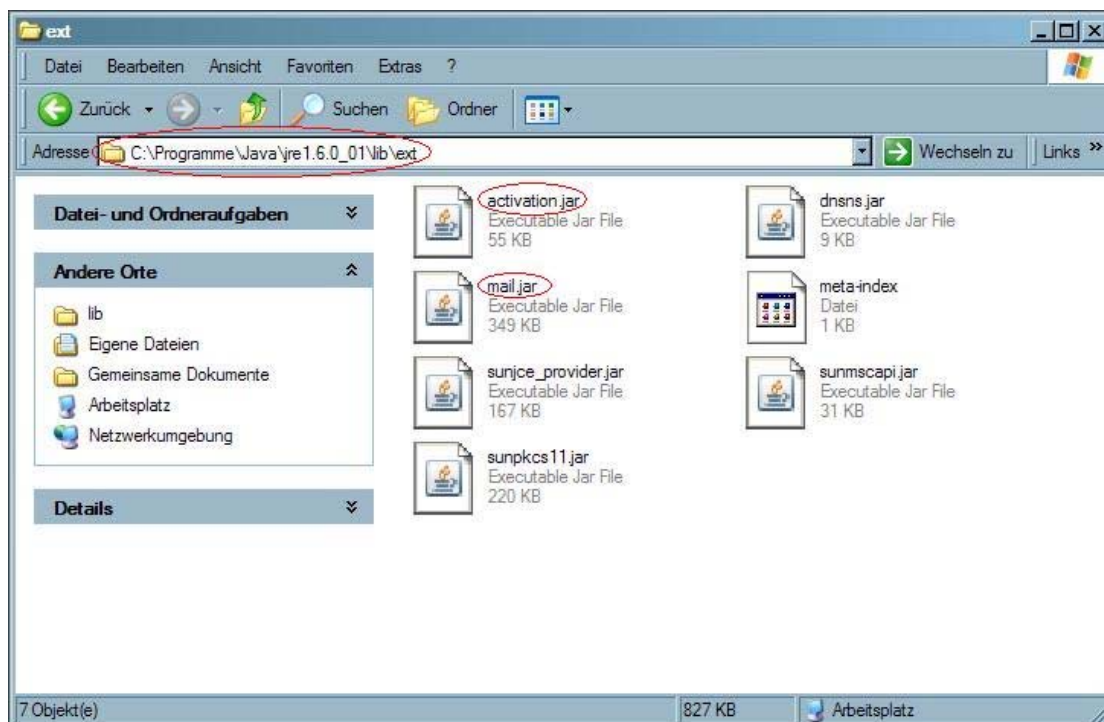
Falls Sie das Betriebssystem Mac OS verwenden, so befindet sich Ihre JRE im Verzeichnis *../Library/Java/Home*.

Nachdem Sie den Installationspfad gewählt, und den Pfad zu Ihrer JRE angegeben haben, klicken Sie auf die Schaltfläche „install“. Das Setup legt die benötigten Verzeichnisse an und kopiert die Programmdateien.

Um das Tool zu starten, wechseln Sie in das Installationsverzeichnis und starten die Datei *NetWatch.jar* durch einen Doppelklick mit der linken Maustaste. Falls Sie ein unix-basiertes Betriebssystem verwenden, welches das Ausführen von jar-Dateien durch einen Doppelklick nicht ermöglicht, so öffnen Sie ein Konsolenfenster. Wechseln Sie auch hier in das Installationsverzeichnis und starten Sie das Tool mit folgender Eingabe:

```
java -jar NetWatch.jar
```

Falls Sie Probleme bei der Benutzung des Setup haben, besteht die Möglichkeit, Netwatch auch manuell zu installieren. Hierzu erzeugen Sie mit Hilfe eines Datei-Managers, wie z.B. dem *Explorer* oder dem *Finder* an einer beliebigen Stelle auf Ihrer Festplatte ein Installationsverzeichnis. In diesem legen Sie den Ordner „detailLog“ an. Kopieren Sie von der Installations-CD das Verzeichnis *Images* und die Datei *NetWatch.jar* in das soeben erstellte Zielverzeichnis. Anschließend müssen die beiden Bibliotheken *mail.jar* und *activation.jar* im Verzeichnis Ihrer JRE in den Pfad *../lib/ext* kopiert werden. Liegt Ihre Java Runtime Environment beispielsweise unter dem Verzeichnis *C:\Programme\Java*, so müssen Sie die beiden Dateien in das Verzeichnis *C:\Programme\Java\jre.1.x.x_x\lib\ext* kopieren.



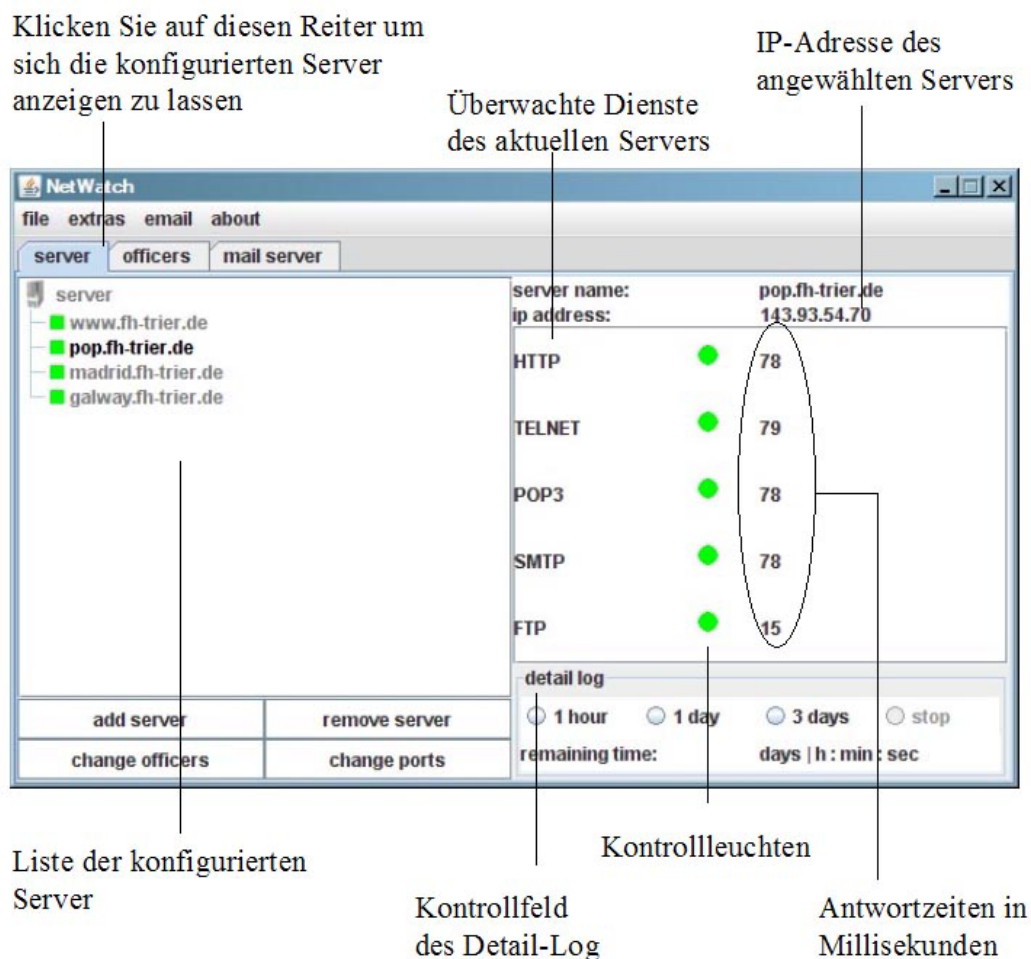
Kopieren der Bibliotheken in das entsprechende Verzeichnis der JRE

Hauptfenster

Netwatch besitzt drei Hauptfenster, zwischen denen Sie mit Hilfe der Reiter „servers“, „officers“ und „mail server“ umschalten können. Unter dem Reiter „server“ haben Sie die Möglichkeit beliebige Server zu verwalten und zu überwachen. Das Anzeigefenster unterteilt sich vertikal in zwei Abschnitte. Im linken Teil werden die Server in einer Baumstruktur verwaltet, während Sie im rechten Abschnitt den Servernamen, die IP-Adresse und die Verfügbarkeit der einzelnen Dienste des angewählten Servers angezeigt bekommen. Wir bezeichnen dieses Fenster als Detailansicht. Weiterhin befinden sich hier die Optionen für das Detail-Log, welche im entsprechenden Kapitel beschrieben werden.

Die Verfügbarkeitsanzeige in der Detailansicht ordnet die zu überwachenden Dienste zeilenweise untereinander an. Hierbei folgt zunächst der Name des Dienstes, sein Verfügbarkeitsstatus, sowie die aktuelle Antwortzeit. Die Verfügbarkeit wird anhand von Kontrollleuchten dargestellt, wobei es vier Zustände gibt. Wurde ein Server neu angelegt oder eine Serverliste geladen, so ist die Kontrollleuchte grau hinterlegt, und das Tool startet einen ersten Verbindungsversuch. Leuchtet die Kontrollleuchte grün, so ist der Dienst verfügbar, leuchtet sie rot, so ist der geprüfte Dienst ausgefallen. Bei einer Antwortzeit, die 80% der Timeout-Zeit überschreitet, leuchtet die Anzeige gelb.

Rechts neben den Kontrollleuchten befinden sich die Antwortzeiten bzw. die Dauer der einzelnen Verbindungen, welche in Millisekunden angezeigt wird.

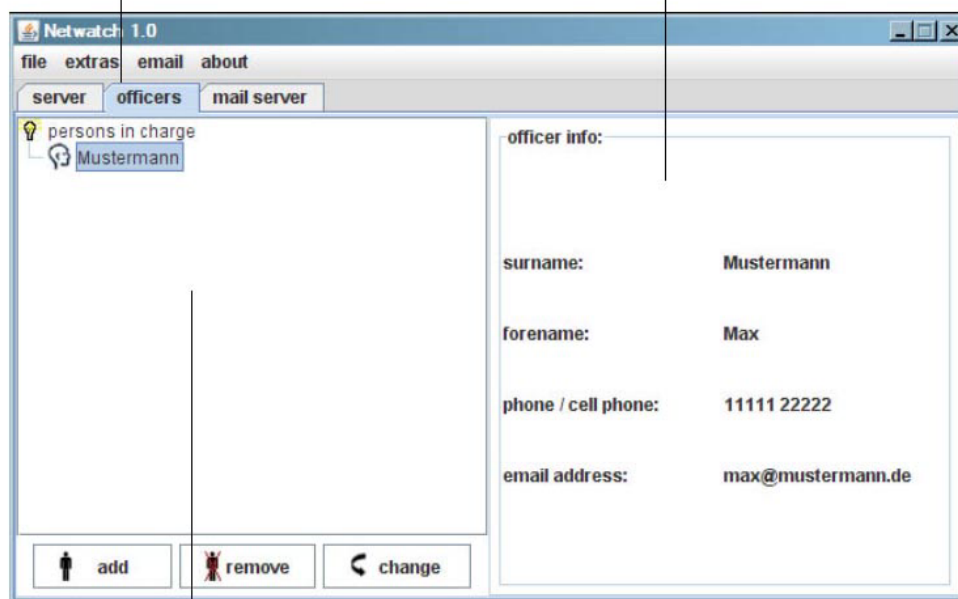


Hauptfenster der Serververwaltung

Unter dem Reiter „officers“ können die Kontaktpersonen angelegt werden, welche bei Störungen bzw. Ausfällen der Dienste benachrichtigt werden sollen. Auch hier ist das Fenster zweigeteilt, wobei sich auf der linken Seite des Fensters die Kontaktpersonen in einer Baumstruktur befinden. Auf der rechten Seite werden die Informationen zu der angewählten Kontaktperson angezeigt.

Klicken Sie auf diesen Reiter, um zur Verwaltung der Kontaktpersonen zu gelangen

Hier können Sie die aktuellen Informationen zu einer angewählten Person einsehen



In diesem Fenster werden die Kontaktpersonen in einer Baumstruktur abgelegt

Kontaktpersonenverwaltung

Durch Klicken auf den Reiter „mail server“ wechseln Sie zu dem Anzeigefenster Ihrer E-Mailkonfiguration. Hier können Sie alle Angaben über Ihren definierten Mailserver einsehen.

Klicken Sie auf diesen Reiter um sich die aktuelle Mailkonfiguration anzeigen zu lassen

Absender (Netwatch)

IP-Adresse des Server

Name des verwendeten SMTP-Servers

Gesetztes Passwort

Mail-Account des Tools

E-Mail Adresse des Tools

Anzeigefenster der Mailserver-Konfiguration

Konfiguration des Mailservers

Um die E-Mail-Funktion von Netwatch nutzen zu können, müssen Sie einen Mailserver definieren, der das SMTP (simple mail transfer protocol) verwendet. Hierbei können Mailserver (SMTP-Server) ohne, als auch mit Authentifizierung verwendet werden. Verlangt ein Server keine Authentifizierung, so arbeitet er als *Open Relay* und ermöglicht das Senden von E-Mails ohne Angabe von Benutzername und Passwort. Die meisten Mailserver benötigen allerdings eine Authentifizierung vor dem Versenden von E-Mails. Je nachdem, welche Art von Mailserver Sie verwenden möchten, haben Sie die Möglichkeit diesen entsprechend einzurichten.

Um den Mailserver zu konfigurieren klicken Sie in der Menüleiste auf den Punkt „email“ und wählen dort die Option „setup email“. Es öffnet sich das Fenster, in dem der Mailserver konfiguriert werden kann.

Unter dem Abschnitt „server authentication“ können Sie einstellen, ob Ihr Mailserver eine Authentifizierung verlangt, oder ob er auf diese verzichtet. Benötigt er keine Authentifizierung, so müssen sie lediglich das Textfeld „smtp server“ ausfüllen. Hier tragen Sie den zu verwendenden SMTP-Server ein. Anschließend klicken Sie auf die Schaltfläche „setup“.

The screenshot shows a window titled "e-mail setup" with a close button (X) in the top right corner. It is divided into two sections. The first section, "server authentication:", contains a checkbox labeled "server requires authentication" which is currently unchecked. The second section, "e-mail information:", contains four input fields: "smtp server:", "email account:", "email address:", and "password:". The "email account:" and "email address:" fields are pre-filled with the text "not required". At the bottom of the window is a button labeled "setup".

E-Mail Setup ohne Authentifizierung

Erfordert ihr SMTP-Server allerdings eine Authentifizierung, so aktivieren Sie das Häkchen in der entsprechenden Checkbox. Achten Sie darauf, dass Sie in diesem Fall alle Felder ausfüllen müssen, um die Konfiguration abzuschließen. Das Tool prüft nach dem Klicken auf die Schaltfläche „setup“, ob die eingegebene E-Mail-Adresse grammatikalisch korrekt ist.

The screenshot shows the same "e-mail setup" window. In this configuration, the checkbox "server requires authentication" is checked. The "email account:" and "email address:" fields are now empty, indicating they must be filled out. The "smtp server:" and "password:" fields remain empty. The "setup" button is still at the bottom.

E-Mail Setup mit Authentifizierung

Wechseln Sie nun über den Reiter „mail server“ zum Info-Fenster Ihres konfigurierten Mailservers. Kontrollieren Sie die Angaben. Falls es Netwatch nicht möglich ist, eine Verbindung zu Ihrem angegebenen Mailserver aufzubauen, so sieht der Inhalt des Fensters folgendermaßen aus.



Fehlgeschlagene Konfiguration eines Mailservers

Hierfür kann es folgende Ursachen geben:

- Ihre Netzwerkverbindung ist unterbrochen.
- Der konfigurierte Mailserver ist temporär nicht erreichbar.
- Eventuell haben Sie bei der Konfiguration einen falschen SMTP-Server eingetragen.

Versuchen Sie die Mail-Konfiguration nochmals durchzuführen. Hat dies keinen Erfolg, so versuchen Sie einen alternativen SMTP-Server einzurichten.

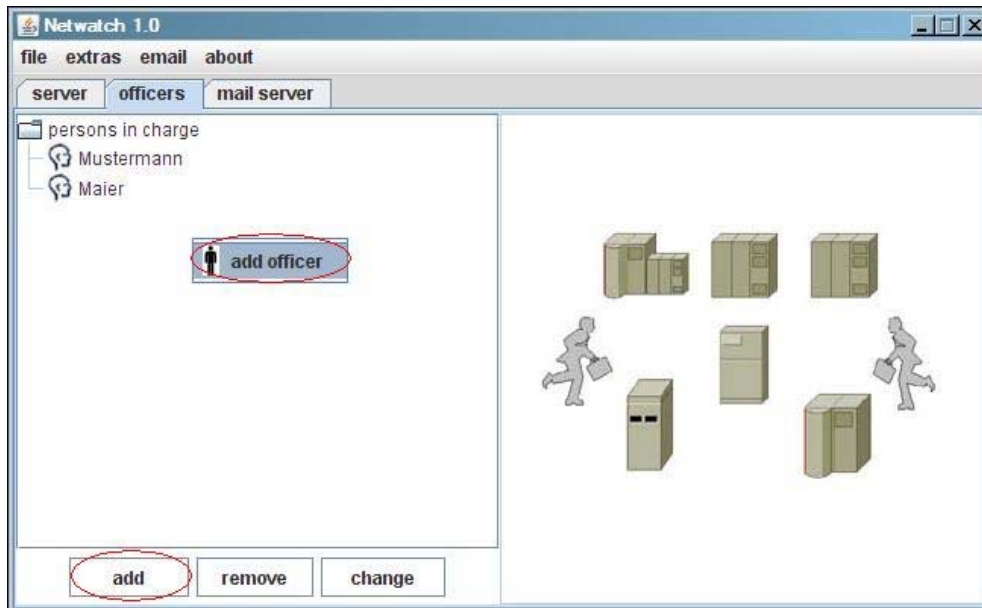
Wenn die Konfiguration erfolgreich war, und der SMTP-Server konfiguriert ist, versenden Sie eine Test-Mail, um sicher zu gehen, dass Ihre E-Mail-Benachrichtigung auch wirklich funktioniert! Haben Sie beispielsweise den Server korrekt angegeben, aber einen Schreibfehler in der Angabe Ihres Accounts oder Passwortes, so können Sie dies nur durch das Versenden einer Test-Mail feststellen.

Gehen Sie hierfür folgendermaßen vor. Klicken Sie in der Menüleiste auf den Punkt „email“ und wählen Sie dort die Option „check configuration“. Geben Sie im Eingabefeld eine E-Mail-Adresse ein, auf deren zugehöriges Postfach Sie Zugriff haben. Anschließend klicken Sie auf die Schaltfläche „send“.

Dieser Vorgang testet nur die Funktion Ihrer Mail-Konfiguration, d.h. ob Ihr Mailserver, der angegebene Account und das Passwort richtig eingerichtet sind. Hierbei wird die Richtigkeit der eingegebenen E-Mail-Adresse nicht berücksichtigt. Sehen Sie nach einer angemessenen Zeit in dem Postfach der verwendeten E-Mail-Adresse nach. Sie sollten eine Nachricht von *NetWatch* mit dem Betreff „Netwatch test mail!“ erhalten haben.

Kontaktpersonen anlegen

Damit eine Benachrichtigung im Falle einer Störung durchgeführt werden kann, müssen Sie Kontaktpersonen definiert haben. Um eine Kontaktperson zu erstellen, wechseln Sie über den Reiter „officers“ zur Kontaktpersonenverwaltung. Hier öffnen Sie das entsprechende Dialogfeld, indem Sie auf die Schaltfläche „add“ klicken, oder an einer beliebigen Stelle im Kontaktpersonenfeld das Popup-Menü öffnen und dort den Punkt „add officer“ anwählen.



Aufrufmöglichkeiten zum Hinzufügen einer neuen Kontaktperson

Es öffnet sich folgendes Dialogfeld, in welchem Sie die gewünschte Kontaktperson anlegen können. Hierbei ist es unbedingt notwendig, dass die Felder „surname“ und „e-mail“ belegt werden, da diese Informationen für die Alarmierung benötigt werden. Die Felder „forename“ und „phone“ werden nicht unbedingt benötigt. Soweit es Netwatch möglich ist, überprüft es die grammatikalische Korrektheit Ihrer Angaben in den Feldern „phone“ und „e-mail“. So können Sie beispielsweise keine Buchstaben in Ihrer Telefonnummer aufführen.



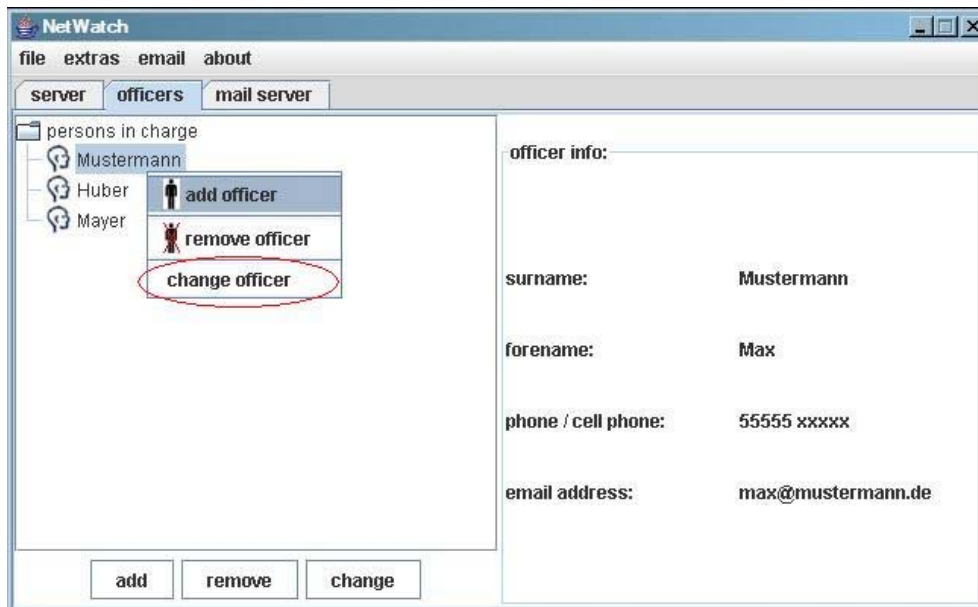
The image shows a Windows-style dialog box titled "officer information:". It has a close button (X) in the top right corner. Inside the dialog, there are four text input fields arranged vertically, each preceded by a label: "surname:", "forename:", "phone:", and "e-mail:". Below these fields, a red text message reads "surname and email are implicitly required!". At the bottom of the dialog, there are two buttons: "add officer" and "cancel".

Eingabemaske zum Anlegen einer neuen Kontaktperson

Nachdem Sie die entsprechenden Angaben zur Person gemacht haben, bestätigen Sie das Anlegen der Kontaktperson durch das Klicken auf die Schaltfläche „add officer“, oder drücken Sie im Feld „e-mail“ die Eingabetaste.

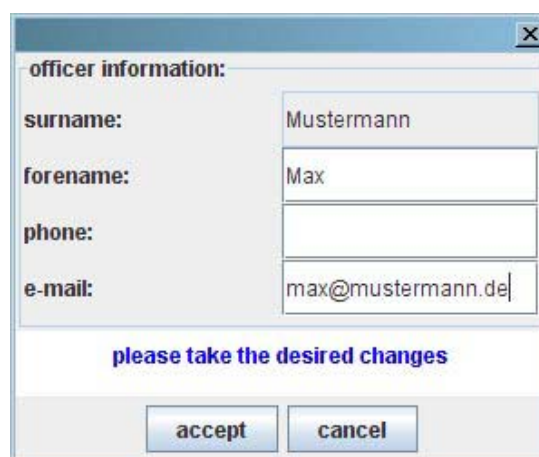
Kontaktpersonen editieren

Zum Editieren einer Kontaktperson, wählen Sie diese mit der linken Maustaste an, und klicken Sie auf die Schaltfläche „change“. Auch hier können Sie alternativ den Weg über das Popup-Menü nehmen.



Aufrufmöglichkeiten zum Editieren einer Kontaktperson

Es öffnet sich das entsprechende Dialogfeld, in welchem Sie Vorname, Telefon- bzw. Handynummer und die E-Mail-Adresse der Kontaktperson ändern können. Da die Kontaktpersonen durch ihren Nachnamen an die Server gebunden sind, lässt sich der Nachname an dieser Stelle nicht ändern.



Eingabemaske zum Editieren einer Kontaktperson

Nachdem Sie Ihre Änderungen in den einzelnen Feldern vorgenommen haben, bestätigen Sie diese durch das Klicken auf die Schaltfläche „accept“.

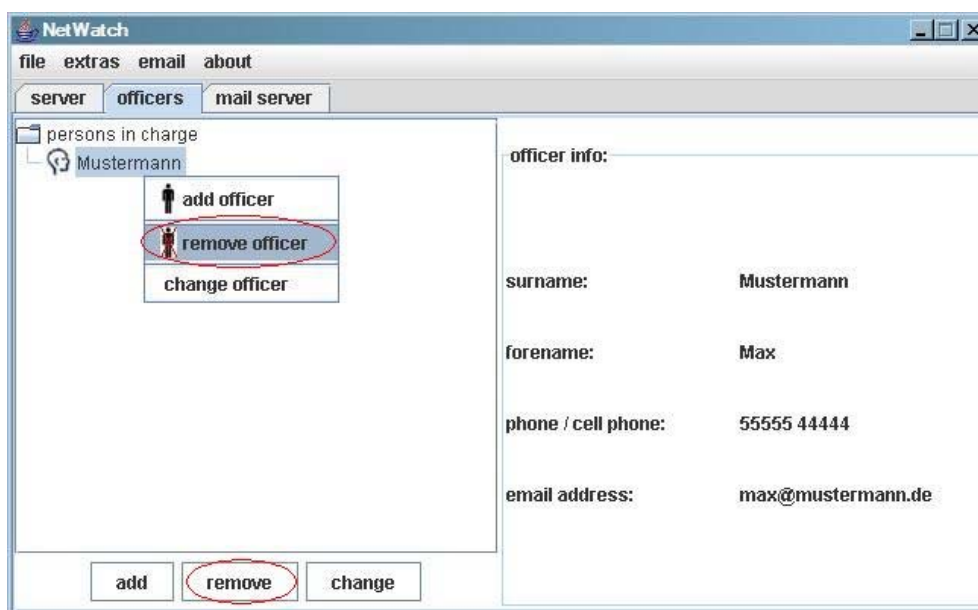
Achtung:

Wenn Sie das Betriebssystem Windows verwenden und das Popup-Menü nutzen, so müssen Sie zuerst die Kontaktperson mit der linken Maustaste anwählen, bevor Sie mit der rechten Maustaste das Popup-Menü zu dieser speziellen Person öffnen können. Unter dem Betriebssystem Mac OS genügt es, die Kontaktperson direkt mit der rechten Maustaste anzuwählen.

Halten Sie die Informationen über die Kontaktpersonen stets aktuell! Hat sich bei einer Person die E-Mail-Adresse geändert, so aktualisieren Sie dies bitte umgehend, damit keine Alarmierungen ins Leere laufen!

Kontaktpersonen entfernen

Um eine Kontaktperson zu entfernen, wählen Sie diese mit der linken Maustaste an. Klicken Sie auf die Schaltfläche „remove“ unter dem Kontaktpersonenfeld. Alternativ rufen Sie mit der rechten Maustaste das Popup-Menü auf und wählen dort die Option „remove officer“.

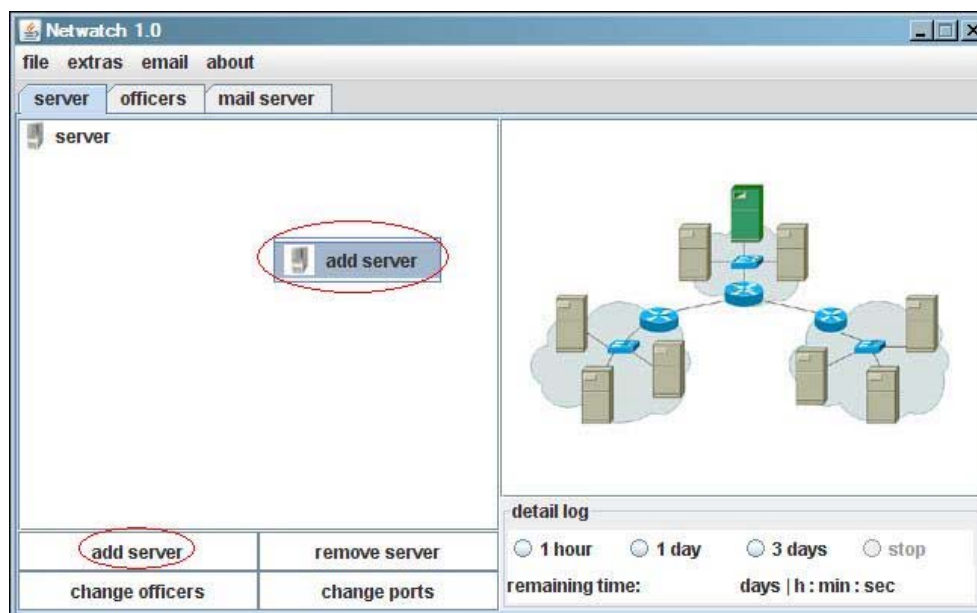


Achtung:

Entfernen Sie eine Kontaktperson, so wird diese automatisch an allen Servern, für die diese Person verantwortlich war, ausgetragen! Gibt es Server, für die nur diese besagte Kontaktperson verantwortlich war, dann erfolgt keine E-Mail-Benachrichtigung mehr, solange dort keine neue Kontaktperson eingetragen wird!

Server anlegen

Damit Sie einen Server und dessen Dienste überwachen können, müssen Sie diesen entsprechend konfigurieren. Das Fenster zum Einrichten eines Servers wird geöffnet, indem Sie entweder auf die Schaltfläche „add server“ klicken, oder das Popup-Menü aufrufen, indem Sie mit der rechten Maustaste in das Feld klicken, in welchem die Server verwaltet werden.



Aufrufmöglichkeiten des Dialoges zum Anlegen eines neuen Servers

Es öffnet sich ein Dialogfeld, welches es Ihnen ermöglicht, den zu überwachenden Server zu konfigurieren. Geben Sie zunächst im Feld „server name“ den Namen des gewünschten Servers ein, oder legen Sie diesen anhand seiner IP-Adresse im Feld „IP address“ an. Bestätigen Sie Ihre Angaben mit der Eingabetaste.

Das Tool baut eine Verbindung zu dem angegebenen Server auf und ergänzt die jeweils fehlende Information. Nachdem Sie den Server angegeben haben, können Sie die Konfiguration der zu überwachenden Dienste vornehmen. Gehen Sie dabei so vor, dass Sie zunächst über die Auswahlfelder unter den Abschnitten „time slice in minutes“ und „timeout in ms“ die gewünschte Einstellung vornehmen, bevor Sie das Häkchen an dem entsprechenden Dienst setzen. Der Punkt „time slice in minutes“ gibt hierbei die Abfrageperiode zwischen den einzelnen Verbindungsprüfungen an. Sie haben hierbei die Möglichkeit einen Wert zwischen einer halben Minute und 30 Minuten festzulegen. Es empfiehlt sich allerdings den Default-Wert von einer halben Minute zu verwenden, damit die Verfügbarkeitsprüfung möglichst genau ist, und die Benachrichtigung im Falle eines Ausfalls möglichst schnell erfolgen kann.

Unter dem Abschnitt „timeout in ms“ hingegen geben Sie die Timeout-Zeit des Dienstes an. Hier können Sie zwischen 500, 1000, 2000, 2500, 5000 und 10000 Millisekunden wählen. Der Default-Wert beträgt 2000 Millisekunden.

Möchten Sie einen Dienst überwachen, der sich nicht in der vordefinierten Liste befindet, so haben Sie die Möglichkeit, diesen in den Feldern „service“ und „port number“ zu spezifizieren und durch das Klicken auf die Schaltfläche „add“ der Überwachung hinzuzufügen. Beachten Sie hierbei, dass Sie im Feld „service“ einen Dienst eintragen, dessen Name maximal aus 20 Zeichen besteht. Im Feld „port number“ sind Eingabewerte zwischen 0 und 65000 zulässig.

Nachdem Sie Ihre Dienste angegeben haben, wählen Sie in der Combobox die Kontaktpersonen aus, welche im Falle einer Störung dieses Servers, benachrichtigt werden sollen. Alle Einstellungen, bis auf den Servernamen und die IP-Adresse, können Sie jederzeit wieder ändern. Das Editieren der Dienste und Kontaktpersonen ist in den folgenden beiden Kapiteln erläutert.

Gegen Sie an dieser Stelle wahlweise
Servernamen oder IP-Adresse ein

Wählen Sie hier die zu
überwachenden Dienste

Abfrageperiode
in Minuten

Timeout-Zeit in
Millisekunden

Erstellen Sie hier eigene
Dienste, falls diese nicht
vordefiniert sind

Legen Sie an dieser
Stelle die Kontakt-
personen für diesen
Server fest

Bestätigen Sie hier Ihre Eingaben

| port based services | time slice in minutes | timeout in ms. |
|---------------------------------|-----------------------|----------------|
| <input type="checkbox"/> HTTP | 0.5 | 2000 |
| <input type="checkbox"/> FTP | 0.5 | 2000 |
| <input type="checkbox"/> TELNET | 0.5 | 2000 |
| <input type="checkbox"/> POP3 | 0.5 | 2000 |
| <input type="checkbox"/> SMTP | 0.5 | 2000 |

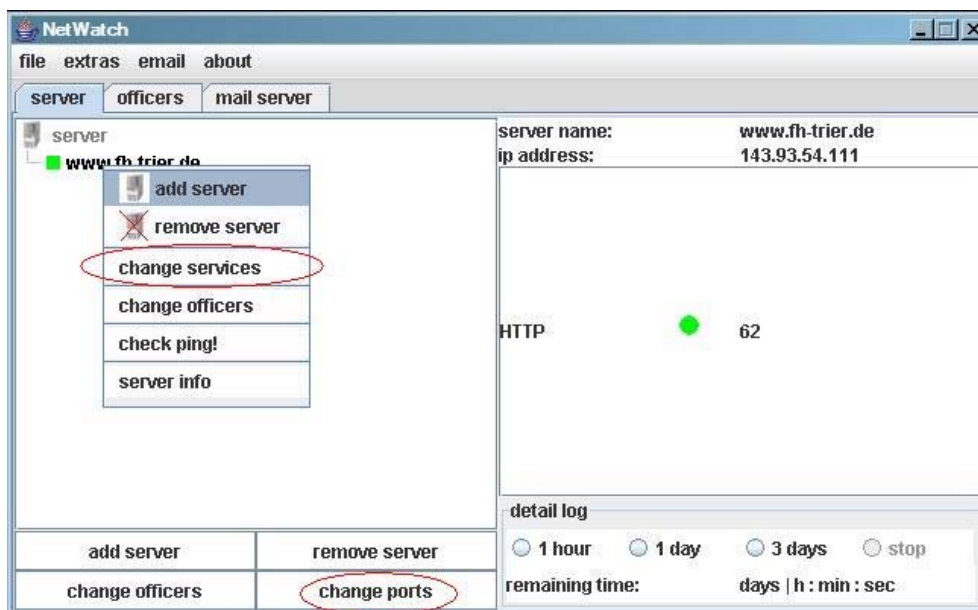
Dialogfeld zum Erzeugen eines neuen Servers

Dienste eines Servers editieren

Möchten Sie nachträglich die Konfiguration eines Servers ändern, so wählen Sie den Server mit der linken Maustaste im Serverfeld an. Klicken Sie auf die Schaltfläche „change ports“ oder klicken Sie im Serverfeld auf die rechte Maustaste, um die Option über das Popup-Menü anzuwählen.

Achtung:

Wenn Sie das Betriebssystem Windows verwenden und das Popup-Menü nutzen, so müssen Sie zuerst den Server mit der linken Maustaste anwählen, bevor Sie mit der rechten Maustaste das Popup-Menü zu diesem speziellen Server öffnen können. Unter dem Betriebssystem Mac OS genügt es, den Server direkt mit der rechten Maustaste anzuwählen.



Aufrufmöglichkeiten zum Editieren eines angelegten Servers

Haben Sie den zu editierenden Server angewählt, und die Funktion „change service“ aufgerufen, so öffnet sich folgendes Dialogfeld.

The dialog box is titled 'change service' and contains the following fields and sections:

- server name:** dublin.fh-trier.de
- IP address:** 143.93.54.28
- port-based services:** A table with columns 'service', 'time slice in minutes', and 'timeout in ms.'. It lists HTTP, FTP, TELNET, POP3, and SMTP. FTP, TELNET, and POP3 are checked.
- additional services:** A table with columns 'service', 'time slice in minutes', and 'timeout in ms.'. It lists ECHO, ICMP, and SQL. All three are checked.
- service:** A text input field.
- port number:** A text input field.
- time slice:** A dropdown menu with '0.5' selected.
- timeout:** A dropdown menu with '2000' selected.
- Buttons:** 'add', 'change server', and 'cancel'.

Annotations (German):

- Entfernen Sie einen konfigurierten Dienst, indem Sie das entsprechende Häkchen entfernen (points to the checkboxes in the 'port-based services' table).
- Fügen Sie weitere, vordefinierte Dienste hinzu, indem Sie an der entsprechenden Stelle ein Häkchen setzen (points to the checkboxes in the 'port-based services' table).
- Hier werden die benutzerdefinierten Dienste aufgeführt (points to the 'additional services' table).
- Bestätigen Sie an dieser Stelle Ihre Änderungen (points to the 'change server' button).
- Fügen Sie an dieser Stelle weitere Dienste hinzu (points to the 'add' button).

Dialogfeld zum Ändern der Dienste-Konfiguration

Möchten Sie einen Dienst hinzufügen, so gehen Sie bitte so vor, wie Sie es bereits beim Anlegen des Servers getan haben. Soll ein Dienst entfernt werden, so entfernen Sie das entsprechende Häkchen neben der Bezeichnung des Dienstes.

Möchten Sie die Abfrageperiode oder die Timeout-Zeit eines bereits eingetragenen Dienstes ändern, gehen Sie in folgender Reihenfolge vor. Entfernen Sie das Häkchen des zu ändernden Dienstes. Stellen Sie die gewünschte Abfrageperiode bzw. den gewünschten Timeout ein. Setzen Sie anschließend das entsprechende Häkchen, um den neu konfigurierten Dienst wieder einzutragen.

Im Feld „additional services“ finden Sie Ihre manuell eingetragenen Dienste, welche Sie an dieser Stelle ebenfalls editieren oder entfernen können.

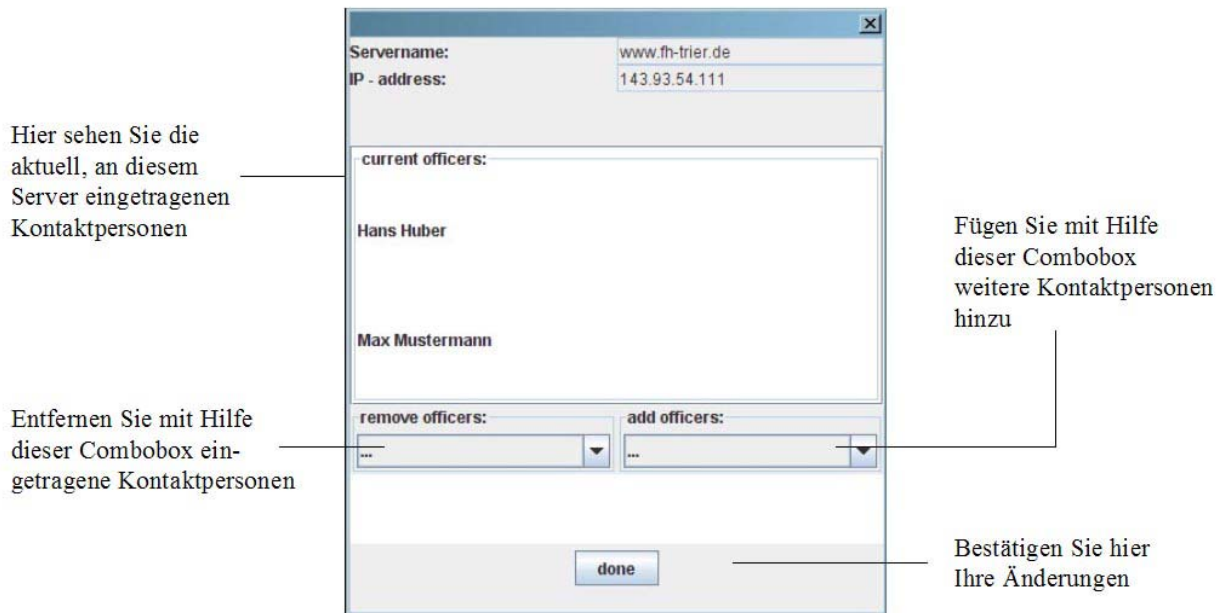
Schließen Sie die Änderungen mit einem Klick auf die Schaltfläche „change server“ ab.

Achtung:

Während Sie ein Detail-Log erstellen, können Sie die Dienste eines Servers nicht ändern, da neu hinzugefügte oder entfernte Dienste die Ergebnisse des Detail-Logs im Bezug auf die prozentuale Ausfallrate verfälschen könnten. In diesem Fall sind die Schaltflächen zum Editieren deaktiviert.

Kontaktpersonen eines Servers editieren

Ändern Sie die Konfiguration der Kontaktpersonen eines Servers, indem Sie den gewünschten Server anwählen und durch Klicken auf die Schaltfläche „change officers“ das entsprechende Dialogfeld öffnen. Alternativ können Sie, wie beim Editieren der Serverdienste, die Änderung auch über den Punkt „change officers“ im Popup-Menü durchführen.



Dialogfeld zum Editieren der Kontaktpersonen eines Servers

Unter dem Punkt „current officers“ sehen Sie alle, an diesem Server eingetragenen Kontaktpersonen. Möchten Sie nun weitere Personen hinzufügen, so wählen Sie diese aus der Combobox „add officers“ im unteren Drittel des Fensters aus. Die ausgewählten Personen werden dann automatisch zur Liste der Kontaktpersonen hinzugefügt. Netwatch prüft hierbei, dass keine Kontaktperson mehrfach eingetragen wird.

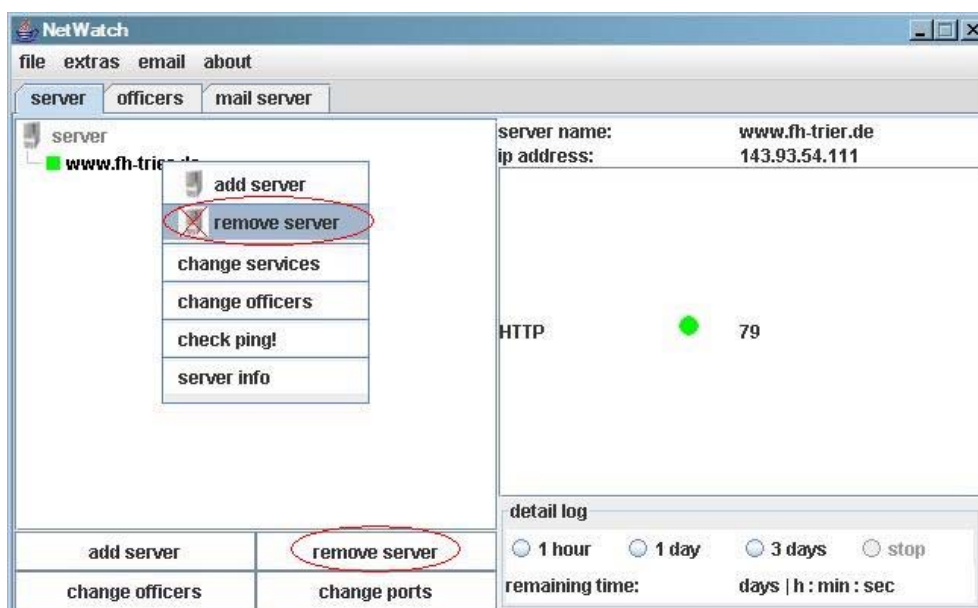
Möchten Sie Personen aus dieser Liste entfernen, so wählen Sie diese über die Combobox „remove officers“ an. Die ausgewählten Personen werden dadurch aus der Liste der Kontaktpersonen dieses Servers entfernt.

Server entfernen

Möchten Sie einen Server aus der Serverliste entfernen, so wählen Sie den entsprechenden Server in der Baumstruktur mit der linken Maustaste an, und klicken Sie auf die Schaltfläche „remove server“.

Ebenso wie beim Erstellen eines Servers haben Sie auch hier die Möglichkeit, das Entfernen eines Servers über das Popup-Menü durchzuführen. Wählen Sie hierfür den gewünschten Server im Baum an, und öffnen Sie mit der rechten Maustaste das Popup-Menü. Klicken Sie hier auf den Punkt „remove server“.

Das Entfernen eines Servers wird in der Log-Datei errorlog.txt, welche sich im Stammverzeichnis Ihres Tools befindet, festgehalten.

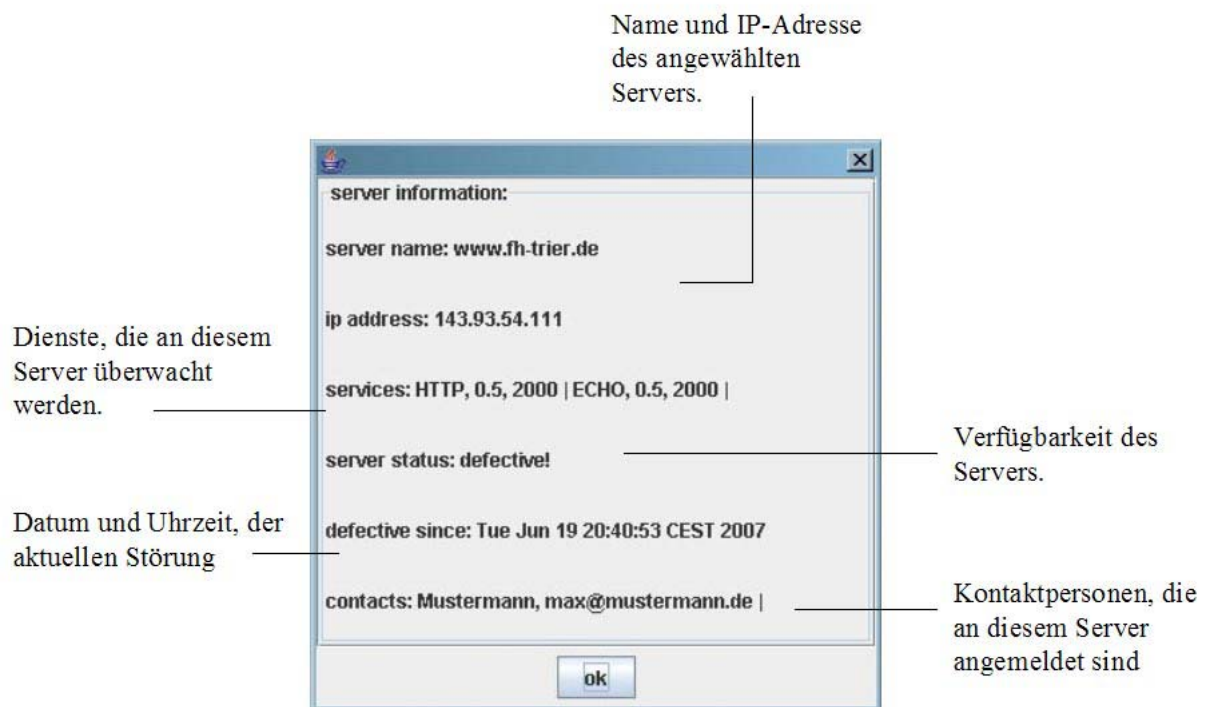


Entfernen eines angewählten Servers

Serverinformationen anzeigen

Die aktuellen Informationen zu einem Server erhalten Sie, indem Sie über das Popup-Menü den Punkt „server info“ anwählen. Es öffnet sich ein Fenster, in welchem Sie den Servernamen, die IP-Adresse und die zu überwachenden Dienste mit den zugehörigen Abfrageperioden und Timeout-Zeiten angezeigt bekommen.

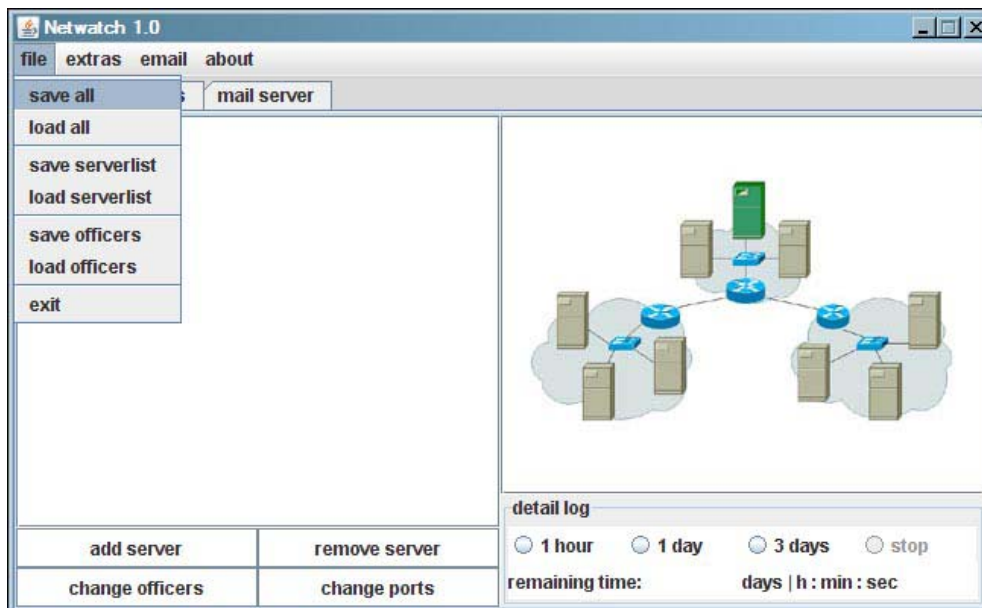
Unter dem Punkt „server status“ bekommen Sie die aktuelle Verfügbarkeit des Servers angezeigt. Hierbei bedeutet der Eintrag „available!“, dass alle Dienste des Servers erreichbar sind. Ist mindestens ein Dienst ausgefallen, so gilt der Server als gestört. In diesem Fall wird der Eintrag „defective!“ angezeigt. Der Punkt „defective since“ gibt an, zu welcher Zeit die aktuelle Störung aufgetreten ist. Weiterhin erhalten Sie über das Info-Fenster die Namen und E-Mail-Adressen der angemeldeten Kontaktpersonen.



Info-Fenster für eine Beispiel-Konfiguration

Speichern und Laden der Konfigurationen

Netwatch bietet die Möglichkeit, seine aktuelle Konfiguration zu speichern, um sie bei Bedarf wieder einlesen zu können. Hierbei kann die komplette Konfiguration, welche die Liste der Server, die Liste der Kontaktpersonen, sowie die aktuelle Mail-Konfiguration umfasst, auf einmal gespeichert bzw. geladen werden. Zum Speichern der kompletten Konfiguration öffnen Sie in der Menüleiste den Punkt „file“ und wählen dort die Option „save all“. Möchten Sie die gesamte Konfiguration wieder laden, so wählen Sie an dieser Stelle die Option „load all“.



Speichern der kompletten Konfiguration

Neben dem Speichern bzw. Laden der kompletten Konfiguration, besteht auch die Möglichkeit die Serverliste, sowie die Liste der Kontaktpersonen separat zu sichern und wieder einzulesen.

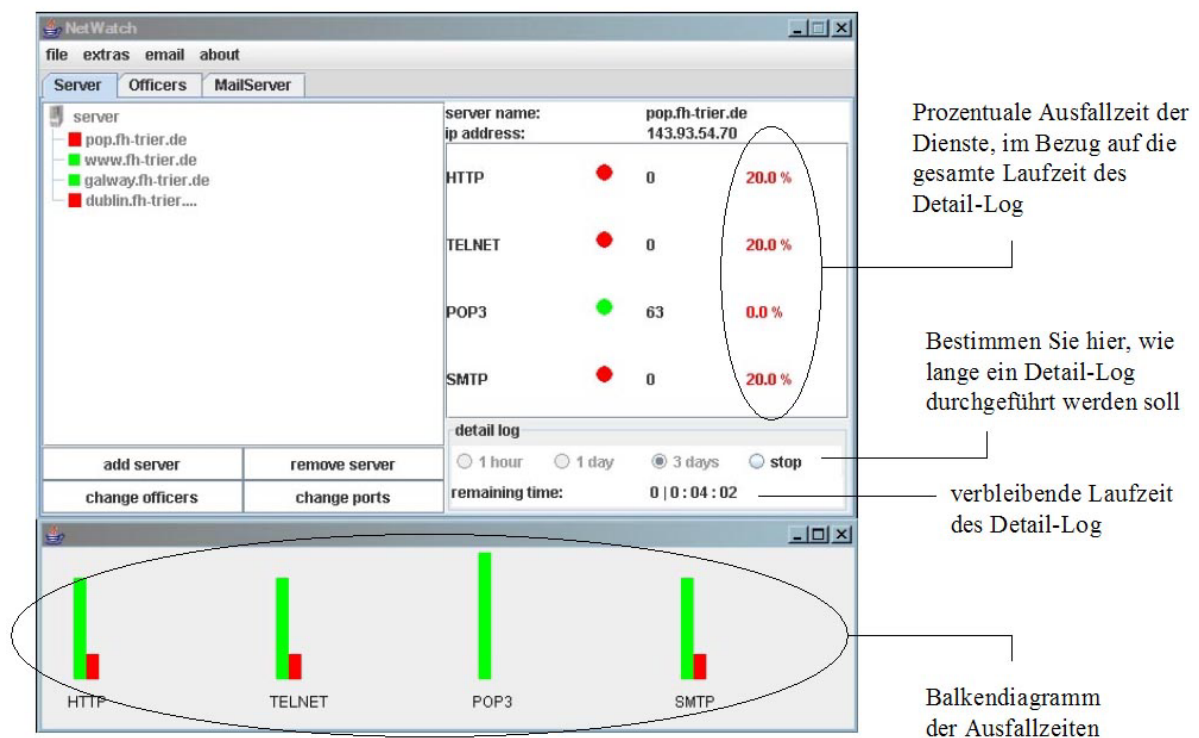
Falls Sie nur die aktuelle Mail-Konfiguration speichern bzw. laden möchten, so wählen Sie in der Menüleiste den Punkt „email“ an und klicken auf die Option „save mail configuration“ bzw. „load mail configuration“.

Detail-Log

Hauptaufgabe des Detail-Log ist es, die Ausfallzeiten der konfigurierten Dienste in Abhängigkeit einer bestimmten Zeit, prozentual darzustellen. Sie können das Detail-Log über einen Zeitraum von einer Stunde, einem Tag oder drei Tagen durchführen. Wenn Sie einen Server anwählen, während das Detail-Log läuft, wird Ihnen in der Detailansicht des Servers direkt hinter der Antwortzeit die Ausfallrate des Dienstes als Prozentwert angezeigt. Weiterhin wird diese Ausfallrate in Form eines Balkendiagramms für jeden Server bereitgestellt.

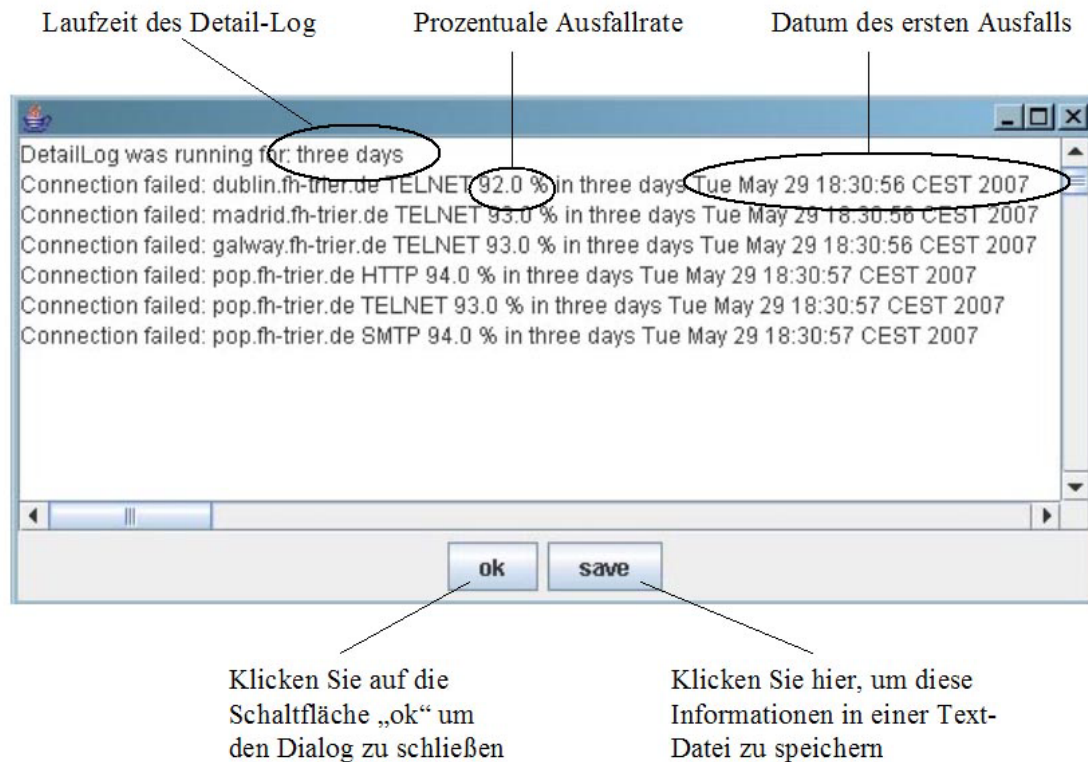
Beachten Sie hierbei, dass die prozentuale Ausfallrate eines Dienstes nur so genau dargestellt werden kann, wie die Abfrageperiode dieses Dienstes definiert ist. Haben Sie eine Abfrageperiode von einer halben Minute gewählt, so ist die Ausfallrate relativ genau. Der schlechteste Fall wäre in diesem Zusammenhang eine sehr hohe Abfrageperiode von 30 Minuten innerhalb eines Logs, dessen Laufzeit nur eine Stunde beträgt. Eine solche Einstellung verfehlt natürlich den Sinn des Detail-Log!

Es sollte also ein gesundes Verhältnis zwischen den Abfrageperioden und der Laufzeit des Detail-Log bestehen.



Ist das Detail-Log zuende gelaufen, so wird Ihnen eine Zusammenfassung angezeigt. In ihr werden die Laufzeit des Logs, sowie die ausgefallenen Dienste in dieser Zeit dargestellt. Zu jedem dieser Dienste wird die prozentuale Ausfallrate, sowie das Datum des ersten Ausfalls angezeigt. Diese Zusammenfassung können Sie bei Bedarf als Text-Datei auf der Festplatte speichern, indem Sie auf die Schaltfläche „save“ klicken. Klicken Sie nach Ablauf des Logs auf den Radiobutton „stop“, um die Ansicht des Detail-Logs zurückzusetzen.

Das Detail-Log legt im Ordner *detailLog* im Stammverzeichnis des Tools für jeden Server eine Datei an. In dieser Datei vermerkt Netwatch die Zustandswechsel der einzelnen Dienste. In diesem Zusammenhang nimmt ein Dienst den Zustand *ausgefallen* oder *verfügbar* ein. Fällt also ein Dienst aus, so protokolliert Netwatch in der entsprechenden Datei diesen Ausfall mit Datum und Uhrzeit. Sobald dieser Dienst wieder verfügbar ist, wird dies ebenfalls in der Datei mit Datum und Uhrzeit vermerkt. Da diese Einträge chronologisch immer aufeinander folgen, kann man sich leicht ein Bild über die gesamte Ausfallzeit der Dienste eines Servers machen.



Beispiel einer Zusammenfassung des Detail-Log

Sie haben die Möglichkeit, ein begonnenes Detail-Log vorzeitig abubrechen. Klicken Sie hierfür auf den Radiobutton „stop“ im entsprechenden Kontrollfeld. Auch hier wird Ihnen eine Zusammenfassung angezeigt. Diese enthält die aktuelle Laufzeit, sowie die prozentualen Ausfallraten innerhalb dieser Zeit. Sie haben die Möglichkeit, die Zusammenfassung an einer beliebigen Stelle, auf Ihrer Festplatte zu sichern.

Achtung:

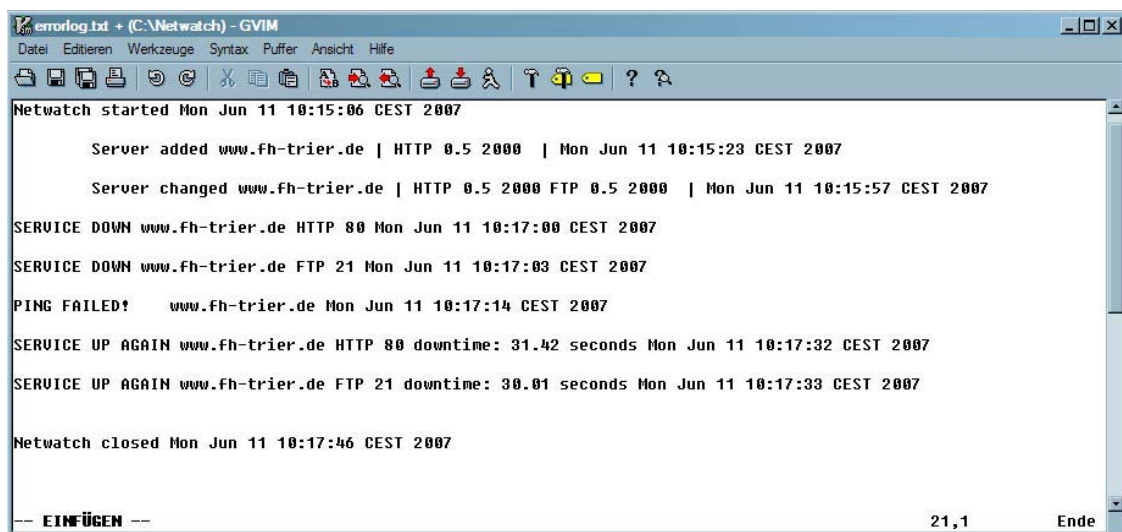
Solange ein Detail-Log läuft, können Sie keine Speicher- bzw. Ladevorgänge starten! Weiterhin ist es nicht möglich, die Dienste eines Servers während dieser Zeit zu ändern! Die entsprechenden Funktionen sind während des Detail-Log deaktiviert.

Error-Log

Das Error-Log stellt eine Log-Datei dar, welche sämtliche Serverkonfigurationen und Ausfälle chronologisch protokolliert. Sie finden die Log-Datei im Stammverzeichnis des Tools unter dem Namen *errorlog.txt*.

Netwatch vermerkt jedes Starten und Beenden im Error-Log, damit Sie stets nachvollziehen können, wann eine Überwachung der Server stattgefunden hat. Weiterhin werden sämtliche Konfigurationen der angelegten Server protokolliert. Hierbei vermerkt Netwatch den Namen des Servers, seine IP-Adresse, die zu überwachenden Dienste mit Abfrageperiode und Timeout-Zeit, sowie das genaue Datum der Erstellung des Servers. Weiterhin werden Konfigurationsänderungen, sowie das eventuelle Entfernen von Servern erfasst.

Im Error-Log werden nicht nur die Ausfälle von Diensten vermerkt, sondern auch deren zurückkehrende Verfügbarkeit. Hierbei wird ebenfalls die Ausfallzeit der Dienste berechnet. Alle Einträge, die mit einem Ausfall bzw. mit wiederkehrender Verfügbarkeit zu tun haben, werden durch Großbuchstaben gekennzeichnet und beginnen linksbündig im Error-Log. Einträge, die sich auf Konfigurationen beziehen, verzichten auf Großschreibung und sind in der Log-Datei nach rechts eingerückt. Diese Notation verleiht der Datei eine gewisse Übersichtlichkeit, wenn es darum geht bestimmte Sachverhalte im Log nachzuvollziehen.



```
errorlog.txt + (C:\Netwatch) - GVIM
Datei Editieren Werkzeuge Syntax Puffer Ansicht Hilfe

Netwatch started Mon Jun 11 10:15:06 CEST 2007

    Server added www.fh-trier.de | HTTP 0.5 2000 | Mon Jun 11 10:15:23 CEST 2007
    Server changed www.fh-trier.de | HTTP 0.5 2000 FTP 0.5 2000 | Mon Jun 11 10:15:57 CEST 2007

SERVICE DOWN www.fh-trier.de HTTP 80 Mon Jun 11 10:17:00 CEST 2007
SERVICE DOWN www.fh-trier.de FTP 21 Mon Jun 11 10:17:03 CEST 2007
PING FAILED!    www.fh-trier.de Mon Jun 11 10:17:14 CEST 2007
SERVICE UP AGAIN www.fh-trier.de HTTP 80 downtime: 31.42 seconds Mon Jun 11 10:17:32 CEST 2007
SERVICE UP AGAIN www.fh-trier.de FTP 21 downtime: 30.01 seconds Mon Jun 11 10:17:33 CEST 2007

Netwatch closed Mon Jun 11 10:17:46 CEST 2007

-- EINFÜGEN --                                     21,1      Ende
```

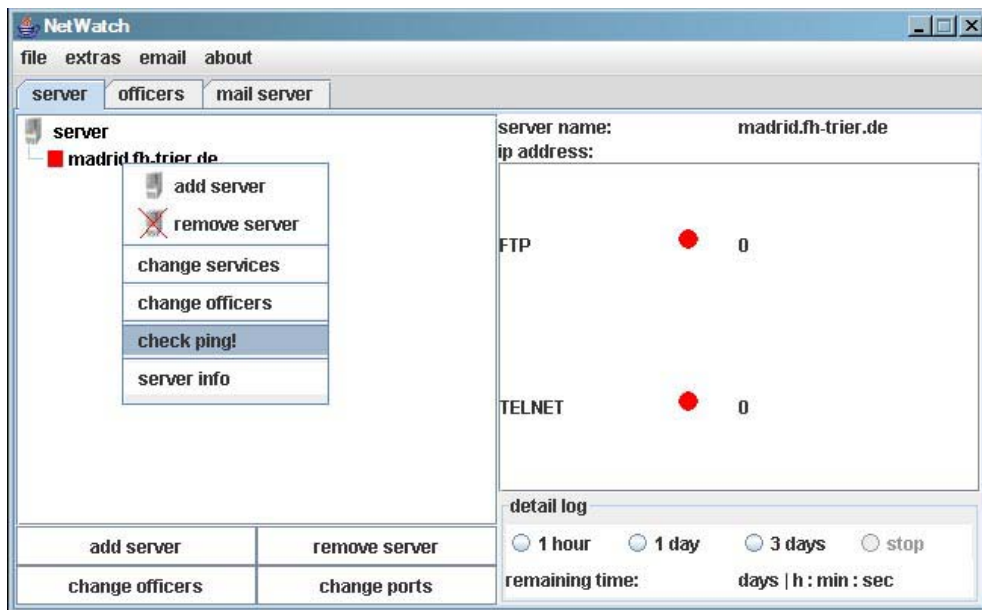
Beispiel eines Error-Logs

Achtung:

Jede, von Netwatch generierte Text-Datei, benutzt zum Zeilenumbruch das unixbasierte Newline-Zeichen. Wenn Sie den Standardeditor *Notepad* unter Windows verwenden, so wird der Dateiinhalt in einer Zeile dargestellt! Kompatible Programme, die den Text korrekt formatiert darstellen, sind beispielsweise der *vi*, *Wordpad* und *Microsoft Word*. Das Programm *Wordpad* finden Sie unter der Verwendung des Betriebssystems Windows in der Startleiste unter *Start – Programme – Zubehör – Wordpad*.

Verfügbarkeit eines Servers prüfen

Sind alle Dienste eines Servers ausgefallen, so stellt sich die Frage, ob sich die Störung wirklich nur auf die konfigurierten Dienste bezieht, oder ob der Server eventuell komplett ausgefallen ist. Um dies prüfen zu können, verfügt Netwatch über die Option „check ping!“, die im Popup-Menü eines Servers aufgerufen werden kann.



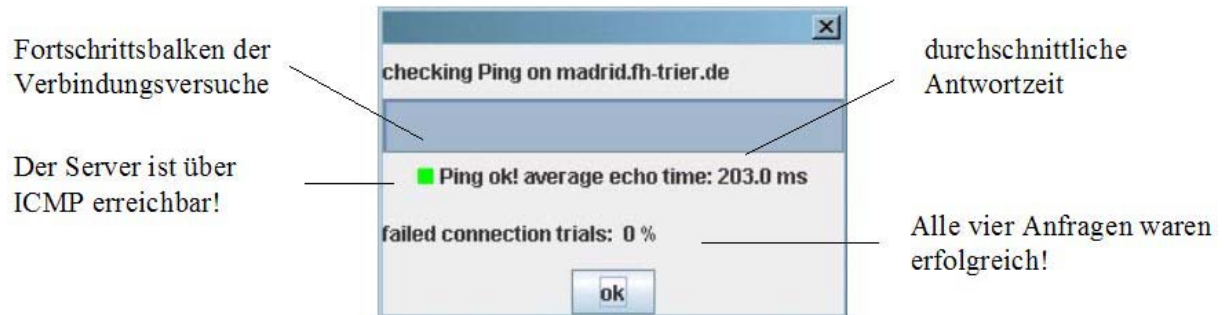
Aufruf der Funktion „check ping!“ auf dem Server madrid.fh-trier.de

Die Funktion „check ping!“ sendet ICMP-Anfragen an den gewünschten Server. Mit einer vorgegebenen Timeout-Zeit wartet Netwatch nach jeder Anfrage auf eine ICMP-Antwort. Bleibt die Antwort aus, so versucht Netwatch eine Socket-Verbindung auf Port 7 (Echo) aufzubauen. Schlägt auch dieser Verbindungsversuch fehl, wird der beschriebene Vorgang noch drei mal wiederholt. Bleiben auch diese Versuche erfolglos, so gilt der komplette Server als ausgefallen. In diesem Fall würden Sie folgendes Ergebnis angezeigt bekommen:



Fehlgeschlagener „check ping!“

Schlägt eine Verfügbarkeitsprüfung über die Funktion „check ping!“ wie in obigem Beispiel fehl, so wird dies zusätzlich in der Datei *errorlog.txt* festgehalten. Sind allerdings nur die Dienste des Servers ausgefallen, wobei der Server selbst noch verfügbar ist, so würde der Aufruf der Funktion „check ping!“ folgende Ausgabe erzeugen:



Erfolgreicher „check ping!“

Prinzipiell kann man die Funktionsweise von „check ping!“ mit der des Konsolenprogrammes *Ping* vergleichen.

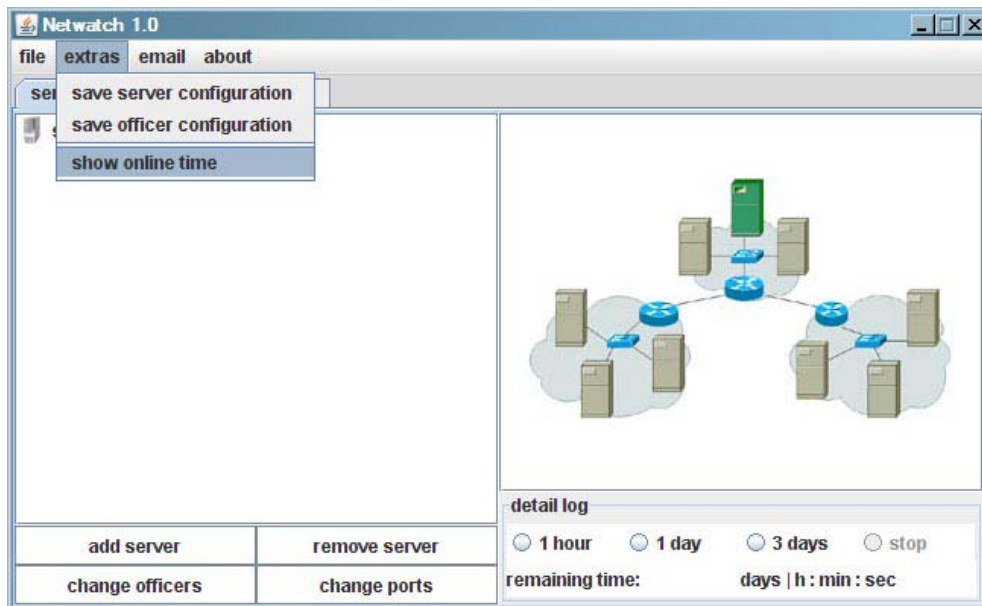
Achtung:

Einige Server sind so konfiguriert, dass sie ICMP-Anfragen ignorieren und somit verwerfen. Informieren Sie sich daher über die Konfiguration der zu überwachenden Server! Achten Sie auf Infrastrukturen und berücksichtigen Sie eventuelle Firewall-Konfigurationen bei Ihrer Fehleranalyse!

Extras

Sie haben unter dem Menüpunkt „extras“ in der Menüleiste die Möglichkeit, Ihre aktuelle Server- bzw. Kontaktpersonenliste im ASCII-Format zu speichern. Die erzeugten Dateien werden direkt im Stammverzeichnis des Tools abgelegt und können mit einem Editor, wie dem *vi* oder dem *Wordpad* geöffnet werden. Hierbei lautet die Dateibezeichnung der Serverliste *configuration.txt*, und die der Kontaktpersonen *officers.txt*.

Die Option „show online time“ zeigt Ihnen die aktuelle Laufzeit des Tools an.

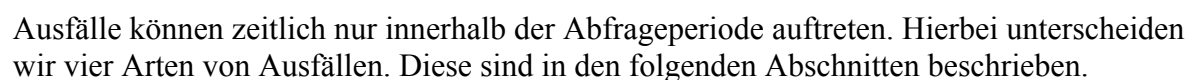


Menüeintrag „extras“

Beenden des Tools

Beenden Sie das Tool über den Punkt „exit“ unter dem Menüeintrag „file“ in der Menüleiste. Somit vermerkt Netwatch in der Log-Datei *errorlog.txt*, dass es zu diesem Zeitpunkt beendet wurde.

Netwatch besitzt einen Algorithmus zur Vermeidung von Fehlalarmierungen. Zwischen jeder Verfügbarkeitsprüfung wartet Netwatch für die Dauer der konfigurierten Abfrageperiode. Bemerkt Netwatch während eines Verbindungsversuches einen potentiellen Ausfall, so wartet das Tool 10 Sekunden, bevor ein zweiter Verbindungsversuch gestartet wird. Schlägt auch diese Verfügbarkeitsprüfung fehl, so wartet das Tool wiederum 10 Sekunden. Anschließend wird der dritte und letzte Versuch unternommen, eine Verbindung aufzubauen. Ist auch dieser Versuch erfolglos, so startet Netwatch seine E-Mail-Alarmierung und nimmt einen entsprechenden Eintrag im Error-Log vor. Folgende Abbildung verdeutlicht das beschriebene Vorgehen zur Vermeidung von Fehlalarmierungen.



Nicht erkannte Verfügbarkeitslücken

Diese enden bereits vor der Timeout-Zeit der ersten Verfügbarkeitsprüfung und werden daher von Netwatch nicht erkannt. Solche minimalen Störungen können beispielsweise aus schwankenden Broadcastlasten innerhalb eines Netzsegmentes resultieren. Weiterhin können sie auf zu geringen Timeout-Zeiten beruhen, insbesondere wenn ein Dienst über das Internet überwacht wird. Solche minimalen Verfügbarkeitslücken sind zu vernachlässigen.

Ausfälle ohne Alarmierung

Solche Ausfälle haben die Timeout-Zeit der ersten Prüfung bereits überschritten. Erst der zweite Versuch, eine Verbindung zum entsprechenden Dienst aufzubauen ist hierbei erfolgreich. Solche Verfügbarkeitslücken können beispielsweise dann auftreten, wenn ein Server nur eine bestimmte Anzahl an gleichzeitigen Verbindungen zulässt. Versucht Netwatch genau in diesem Moment eine Verbindung aufzubauen, in der die maximale Anzahl an Verbindungen bereits erreicht ist, so erhalten wir einen Timeout. In diesen Fällen ist der zweite Verbindungsversuch meist erfolgreich. Auch hier besteht kein Bedarf einer Alarmierung.

Ausfall mit optischer Alarmierung

Schlägt die zweite Verfügbarkeitsprüfung ebenfalls fehl, so handelt es sich um einen Ausfall, der eine optische Alarmierung auslöst. Hierbei wird Ihnen durch die entsprechenden Kontrollleuchten ein potentieller Ausfall signalisiert.

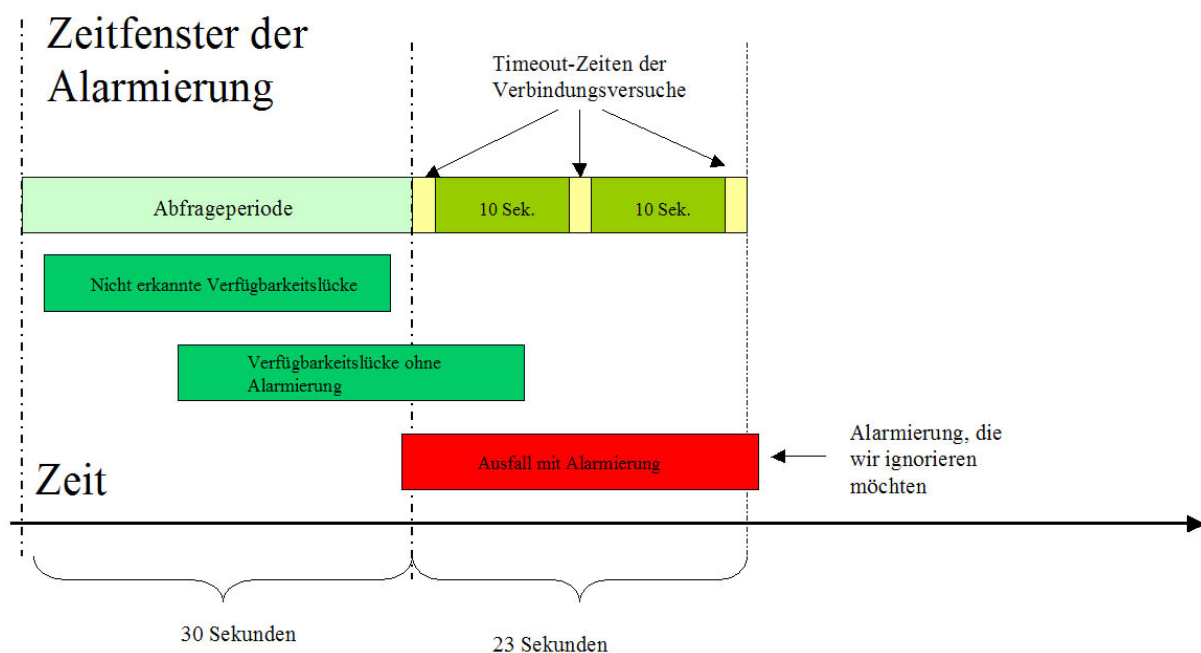
Ausfall mit optischer Alarmierung und E-Mail-Benachrichtigung

Nachdem der zweite Versuch fehlgeschlagen ist, und die optische Alarmierung vollzogen wurde, wartet das Tool weitere 10 Sekunden, bevor es die letzte Prüfung durchführt. Schlägt auch dieser Verbindungsversuch fehl, so protokolliert Netwatch den Ausfall im Error-Log und benachrichtigt alle, an diesem Server angemeldeten Kontaktpersonen über die Störung.

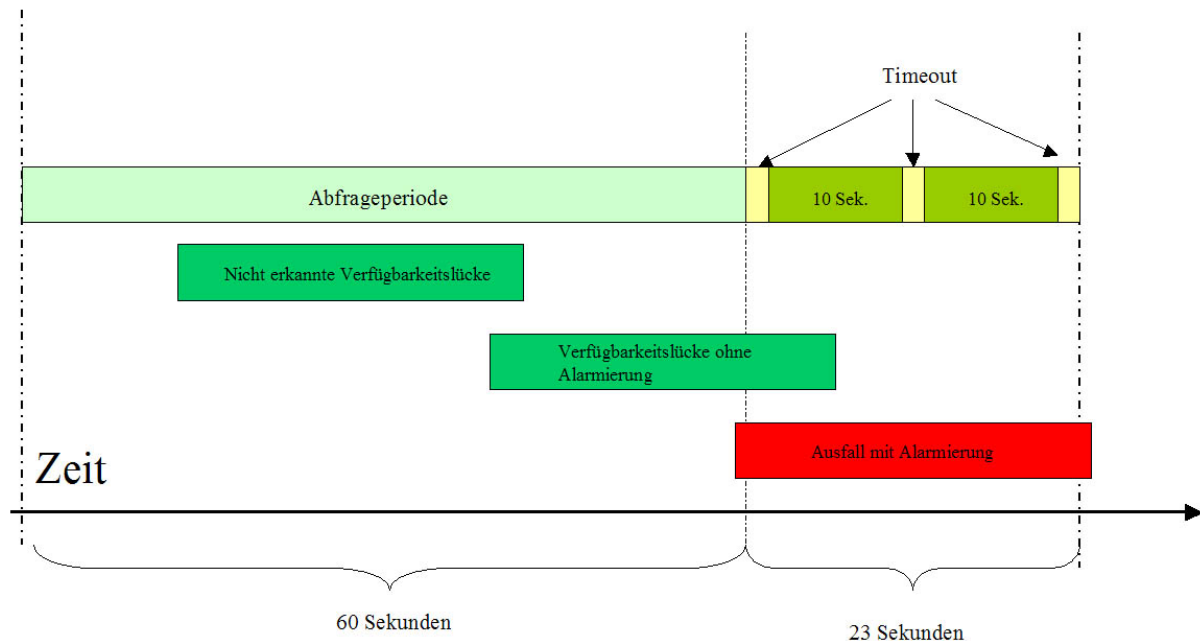
Im Hinblick auf die Infrastruktur eines Netzwerkes und der möglichen Störfaktoren, kann es unter Umständen Sinn machen, das soeben beschriebene Verhalten zur Vermeidung von Fehlalarmierungen auf die jeweilige Situation anzupassen. Möchten Sie einen Server überwachen, der sich in einem Netzsegment befindet, in dem Sie starke Schwankungen im Bezug auf Antwortzeiten beobachtet haben, so können Sie das Zeitintervall aus dem Alarmierungsdiagramm vergrößern, um einen Fehlalarm zu verhindern.

Beachten Sie hierbei unbedingt, dass das Erhöhen der Abfrageperiode in solchen Fällen nur bedingt Erfolg verspricht! Steuern Sie nämlich die Alarmierung über die Abfrageperiode und der Ausfall geschieht am Ende dieser Zeitspanne, so haben Sie nichts gewonnen! Möchten Sie kleinere Verbindungslücken von der Alarmierung ausschließen, so müssen Sie das Zeitintervall über die Timeout-Zeit anpassen. Folgendes Beispiel verdeutlicht die soeben beschriebene Vorgehensweise.

Wir möchten den Dienst HTTP eines Webserver über das Internet überwachen und wählen eine Abfrageperiode von 30 Sekunden und eine Timeout-Zeit von einer Sekunde. In den folgenden Tagen erhalten wir ab und zu eine E-Mail-Benachrichtigungen, dass der Dienst auf dem Server ausgefallen ist. Ein Blick in das Log-File bestätigt diese Ausfälle mit einer jeweiligen Offline-Zeit von etwa 0,5 Minuten, was normalerweise keine nennenswerten Ausfälle, sondern eher geringfügige Verfügbarkeitslücken darstellt. Folgende Abbildung zeigt die Situation im Zeit-Diagramm.



Wir deuten diese Alarmierungen als Fehlalarmierungen und möchten diese zukünftig außer acht lassen. Hierfür müssen wir das Zeitfenster so anpassen, dass die Dauer der Verfügbarkeitslücken endet bevor die Timeout-Zeit der dritten Verbindungsprüfung erreicht ist! Würden wir nun das Zeitintervall über die Abfrageperiode vergrößern, so wäre die Wahrscheinlichkeit einer Fehlalarmierung geringer. Allerdings würden wir nach wie vor eine Alarmierung erhalten, wenn die Verfügbarkeitslücke am Ende der Abfrageperiode aufträte. Folgende Abbildung verdeutlicht die neue Situation, bei der die Abfrageperiode auf eine Minute erhöht wurde.



Korrekt wäre es, die Alarmierung über die Timeout-Zeit zu steuern. So können auch solche Verfügbarkeitslücken keine Fehlalarmierung auslösen, welche am Ende der Abfrageperiode auftreten. Folgendes Zeitdiagramm stellt die Situation mit einer Timeout-Zeit von 5 Sekunden dar, wobei die Abfrageperiode nicht verändert wurde.

