

14. Log-Dateien

Autor: Thomas Geiger

Stand: Juni 2009

Inhaltsverzeichnis

14. Log-Dateien.....	1
14.1. Protokollierung der Benutzeranmeldungen.....	1
14.2. Server-Log-Dateien.....	9
14.3. Protokoll-Datei mit „supportconfig“ erstellen.....	11
14.4. Protokollierung der Internetzugriffe.....	12

Gelegentlich treten im Schulnetz unangenehme Situationen auf, in denen man als Netzwerkberater gerne wüsste, wer für diese Situationen verantwortlich ist.

Einige Beispiele:

- An einem PC wurden schwerwiegende Hard- oder Softwareveränderungen vorgenommen; wer hat zuletzt an dem PC gearbeitet?
- In Internetforen wurden von der Schuladresse aus rechtswidrige Äußerungen verbreitet; von wem stammen diese?

Um Missbrauch im Schulnetz zu verhindern und eventuelle Übeltäter ausfindig machen zu können, ist es deshalb unbedingt notwendig, dass bestimmte Benutzertätigkeiten protokolliert werden. Es versteht sich von selbst, dass die Benutzer darauf hingewiesen werden müssen, welche Aktivitäten überwacht und gespeichert werden. Diese Hinweise müssen in der Benutzerordnung für das Schulnetz für jeden zugänglich sein!

14.1. Protokollierung der Benutzeranmeldungen

Die Protokollierung der Benutzeranmeldungen ist im Auslieferungszustand standardmäßig nicht implementiert. Mit Hilfe von *ZenWorks* kann sie jedoch leicht eingerichtet werden. Durch Erstellung eines einfachen Anwendungsobjekts mit Berichtsfunktion können alle Benutzeranmeldungen protokolliert werden. [1]

Vergleichen Sie hierzu auch das Kapitel „Programminstallation“!

Hinweis zum Rollenkonzept:

Üblicherweise werden in der Musterlösung Anwendungsobjekte und Installationen vom `PgmAdmin-LFB` durchgeführt. Da dem `PgmAdmin-LFB` aber die Rechte für die



Erstellung des benötigten Ordners fehlen, führen Sie die Tätigkeit ausnahmsweise als SchulAdmin-LFB durch!

Zur Erstellung der Anwendung gehen Sie wie folgt vor:

1. Melden Sie sich an ML3-PC1 als SchulAdmin-LFB an!
2. Legen Sie auf \\Gserver03\Data ein Verzeichnis logs und in diesem ein Unterverzeichnis loginlog an!

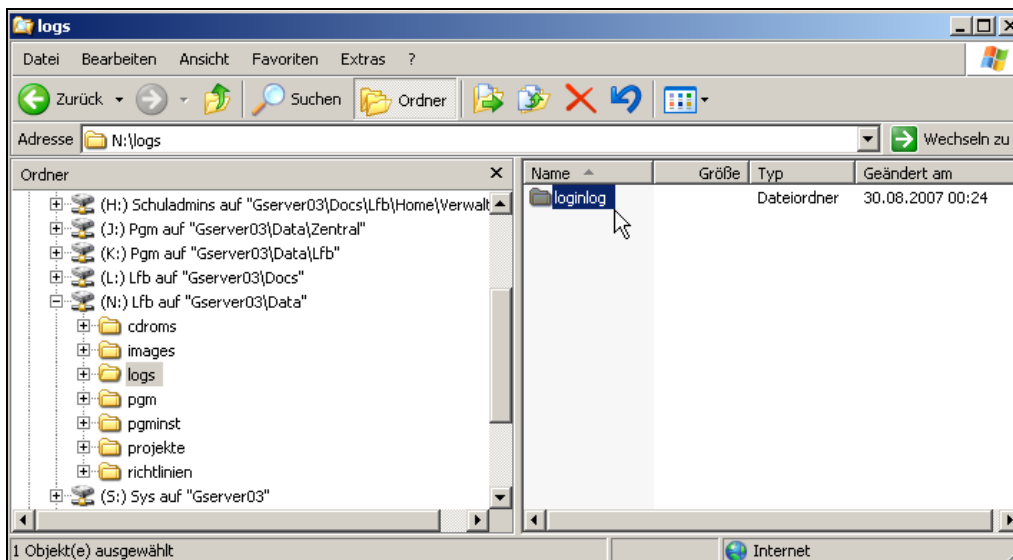


Abbildung 14.1.: Verzeichnis für die Anmeldeprotokollierung

3. Erstellen Sie in dem Verzeichnis mit einem Editor eine Textdatei loginlog.txt!

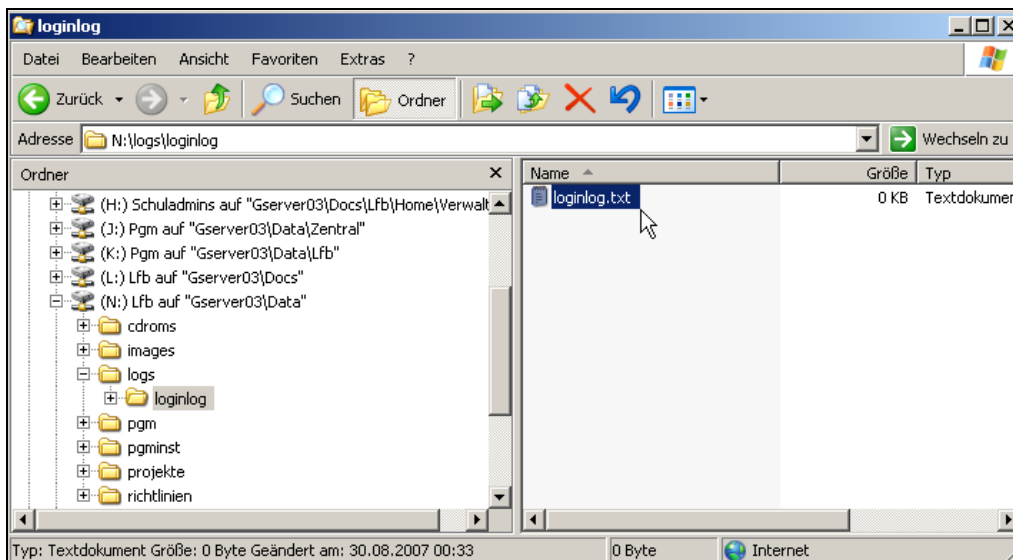


Abbildung 14.2.: Erstellen der Log-Datei

4. Starten Sie die *ConsoleOne* und navigieren Sie zur OU *Tools in ml3.SCHULEN.LFB.Anwendungen!*
5. Erstellen Sie mit *Rechtsklick / Neu* eine neue *Anwendung!*

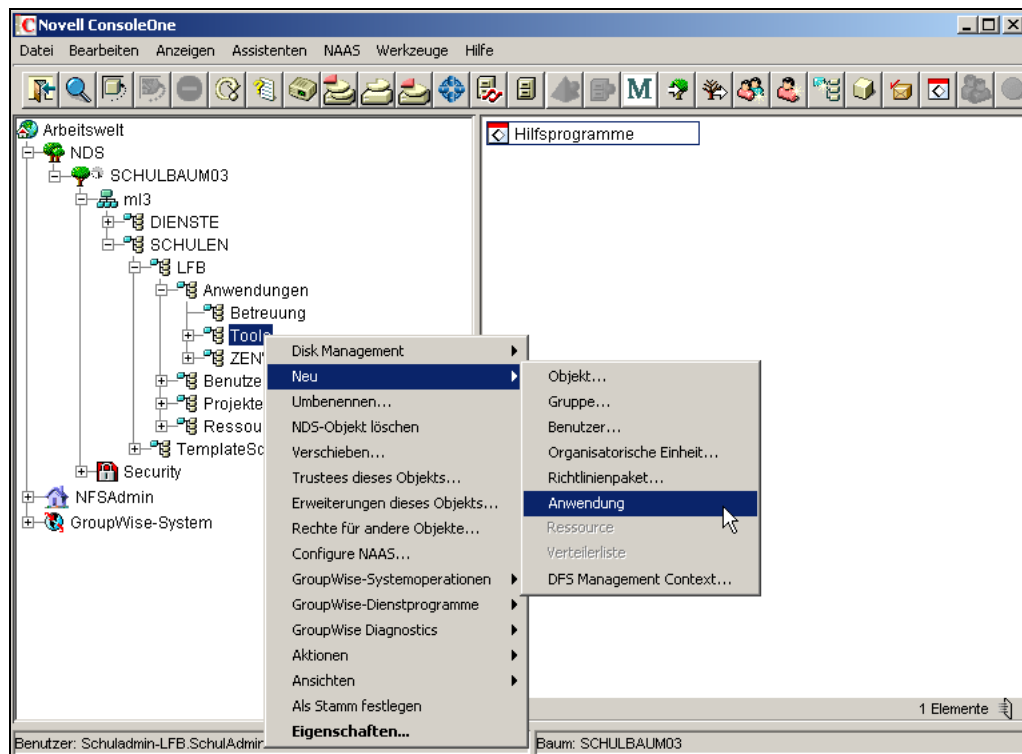


Abbildung 14.3.: Erstellen der Anwendung LoginLog

6. Als Typ wählen Sie *Eine einfache Anwendung (keine .AOT/.AXT/MSI-Datei)*

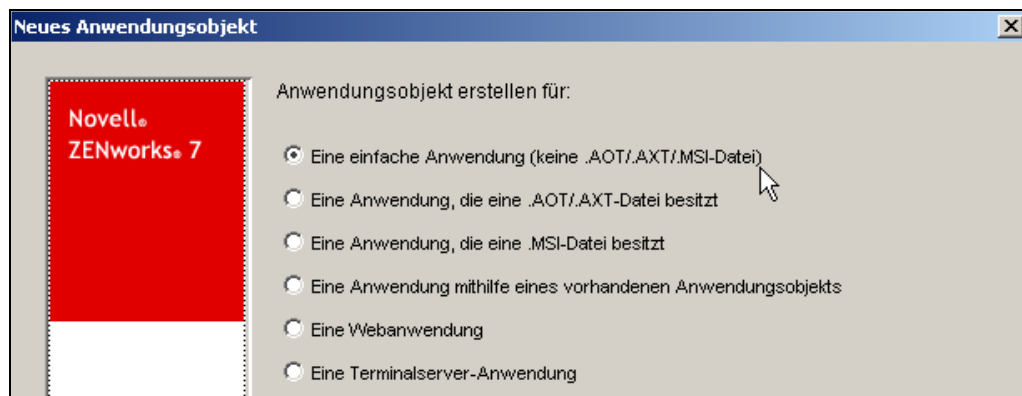


Abbildung 14.4.: Typ der Anwendung

7. Vergeben Sie den Namen: LoginLog

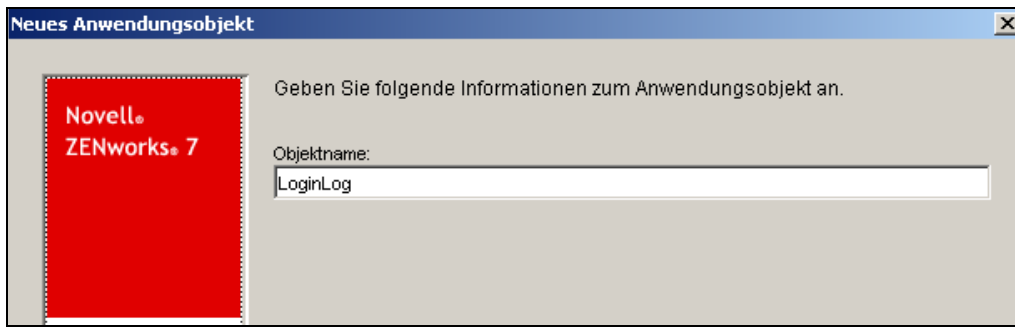


Abbildung 14.5.: Name des Anwendungsobjektes

8. Den Pfad zur Datei lassen Sie leer

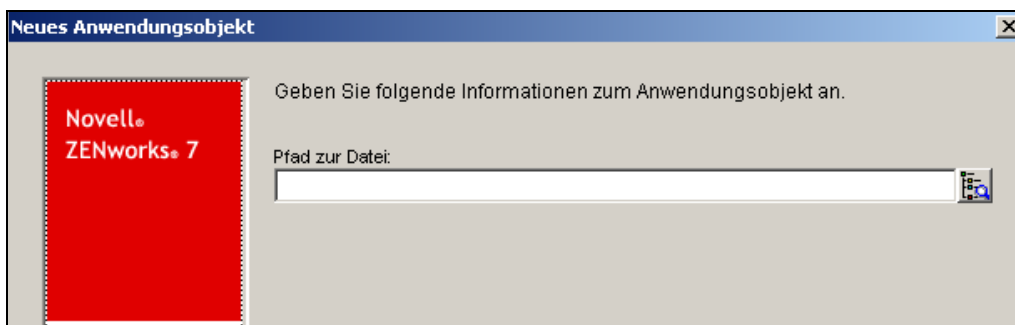


Abbildung 14.6.: Pfad zur Datei: leer!

9. Bei den Regeln müssen Sie festlegen, für welche Client-Betriebssysteme (Plattform) die Anwendung verfügbar sein soll.
Hier wird die Anwendung für Windows-Versionen **ab** Windows 2000 konfiguriert.

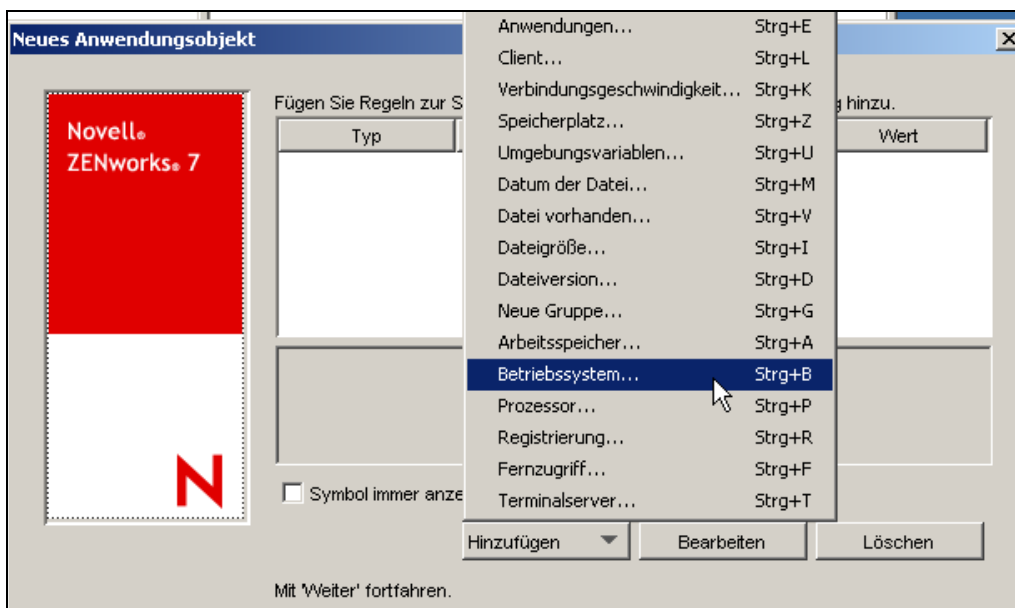


Abbildung 14.7.: Betriebssystem-Verfügbarkeit

10. Information zu den Versionsnummern: Windows 2000: 5.0, Windows XP: 5.1

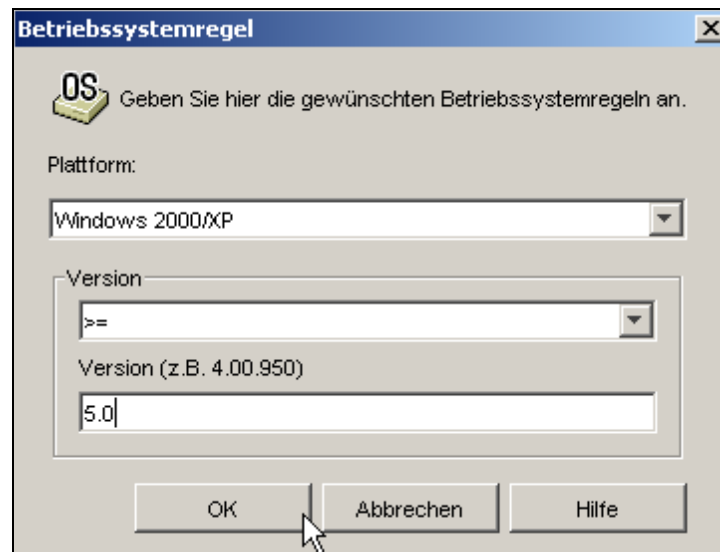


Abbildung 14.8.: Windows-Versionsnummer

11. Jetzt müssen Sie festlegen, für wen die Anmeldungen protokolliert werden sollen. Wenn ALLE Anmeldungen im Schulnetz erfasst werden sollen, wählen Sie `Benutzer.LFB.SCHULEN.m13`! Wenn die Anmeldungen der Verwalter beispielsweise NICHT protokolliert werden sollen, müssen Sie alle anderen Benutzer-OU's einzeln hinzufügen. Es ist wichtig, das Häkchen im ersten Kontrollkästchen zu setzen; dies bedeutet, dass die Ausführung erzwungen wird (Force run).

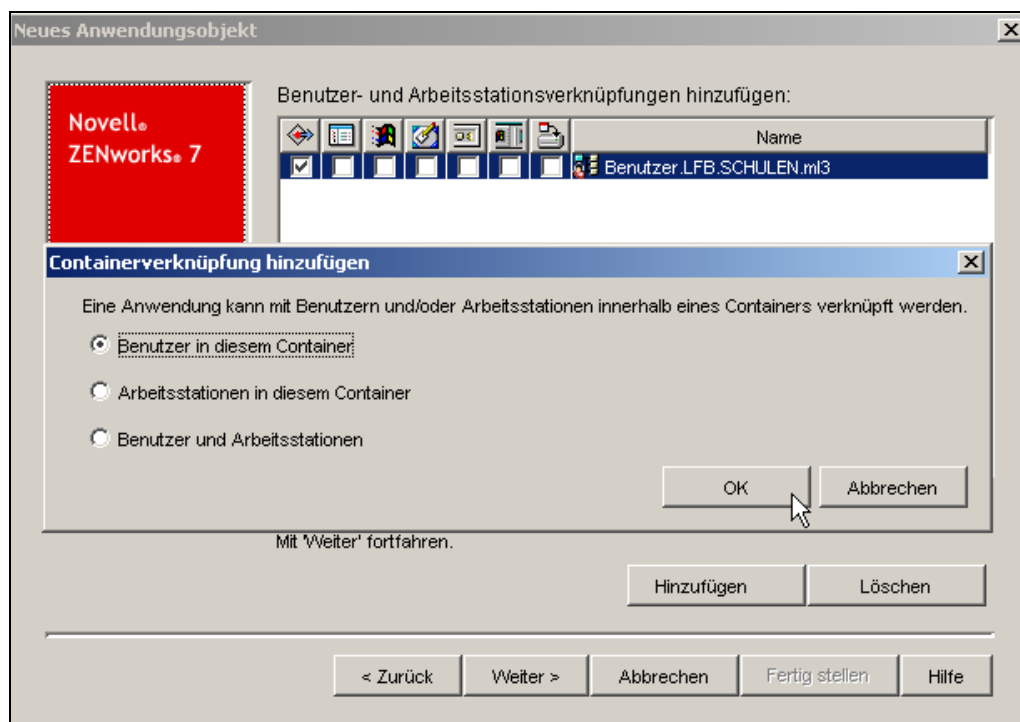


Abbildung 14.9.: Verknüpfungen mit Benutzergruppen

12. Mit dem Klick auf *OK* bzw. *Weiter* wird eine Zusammenfassung angezeigt; da noch weitere Einstellungen nötig sind, aktivieren Sie *Details nach der Erstellung anzeigen!*

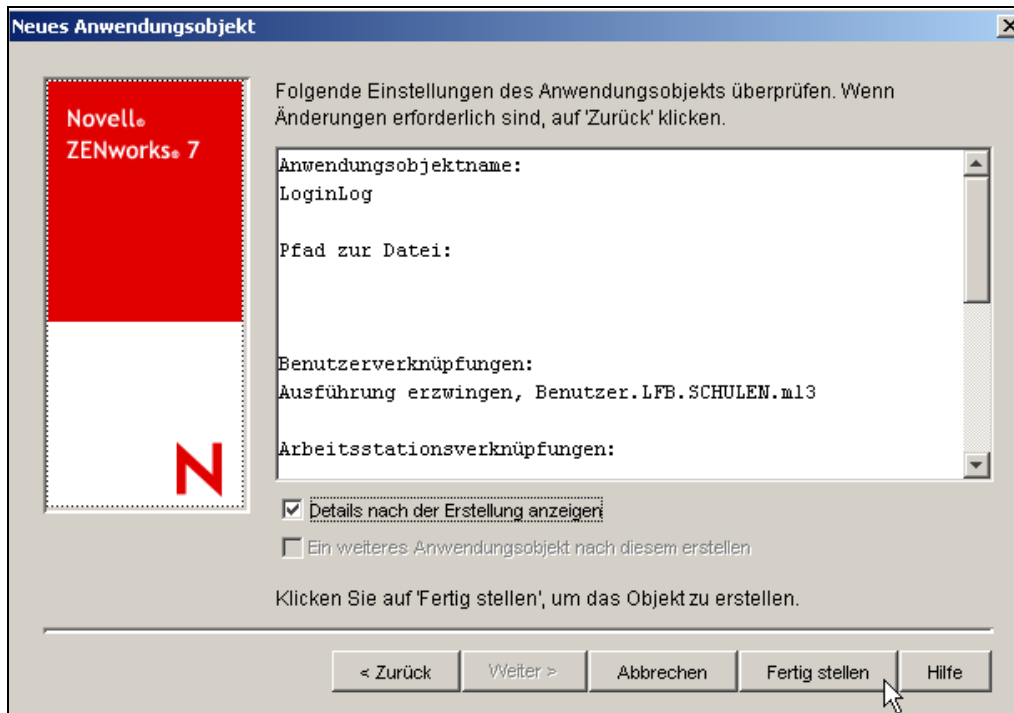


Abbildung 14.10.: Zusammenfassung

13. Wählen Sie *Verteilungsoptionen / Optionen* und setzen Sie die Häkchen wie folgt:

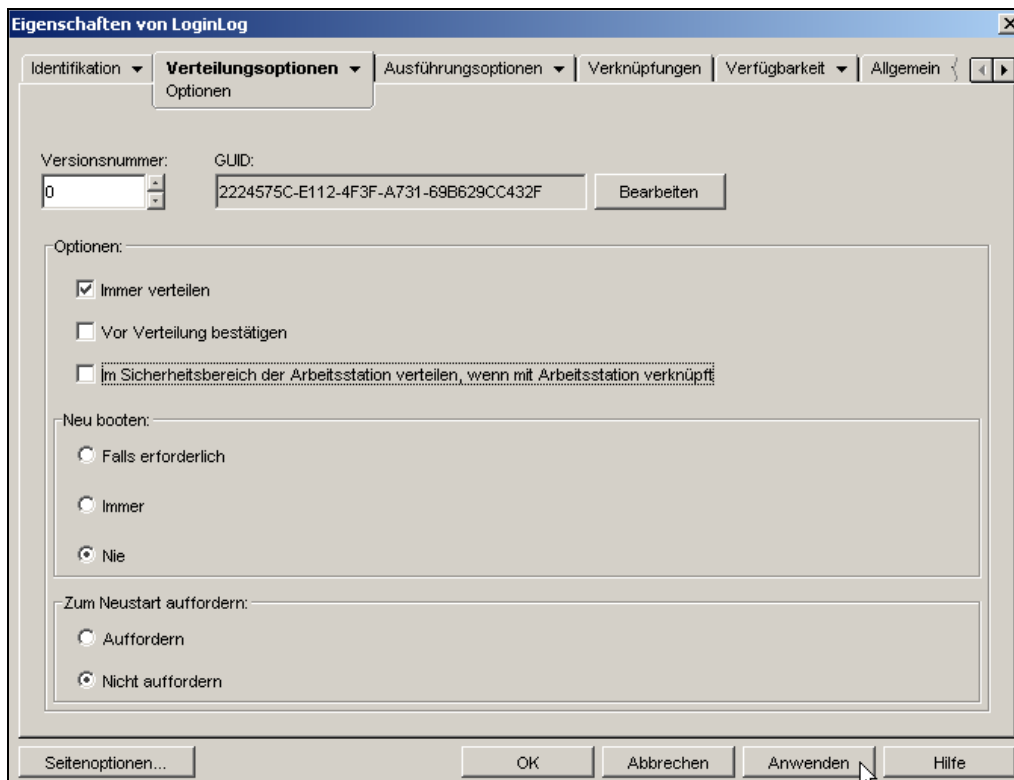


Abbildung 14.11.: Verteilungsoptionen einstellen

14. Über *Allgemein* / *Dateirechte* müssen Sie dem Objekt noch die Rechte *Lesen* und *Schreiben* (!) auf die Datei im entsprechenden Verzeichnis geben. Da die Anmeldungen ja in der Datei `loginlog.txt` protokolliert werden sollen, ist hier ausnahmsweise das Recht *Schreiben* notwendig! Es genügt jedoch, diese Rechte direkt auf die Datei `loginlog.txt` zu vergeben. So können Benutzer nichts in das Verzeichnis `loginlog` schreiben. Da das Recht *Dateiabfrage* **nicht** gesetzt ist, ist die Datei auch im Windows-Explorer im Sinne des Datenschutzes nicht zu sehen.

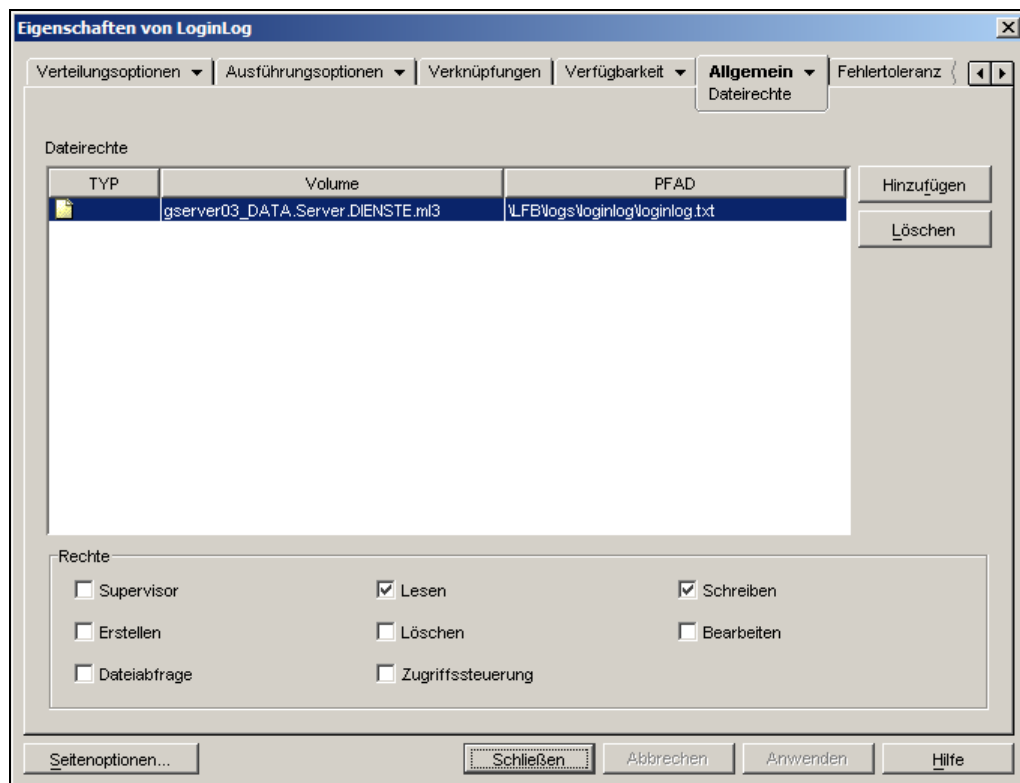


Abbildung 14.12.: Rechte im Verzeichnis (Schreiben!)

15. Die entscheidende Einstellung nehmen Sie unter *Allgemein* / *Bericht* vor. Mit dieser Einstellung legen Sie fest, dass die ordnungsgemäße Verteilung der Anwendung in die ausgewählte Datei protokolliert wird. Beachten Sie, dass hier ein UNC-Pfad notwendig ist, da nicht sicher ist, ob der jeweilige Benutzer ein Mapping auf das Laufwerk `N:` hat. (Dieses könnten Sie als `SchulAdmin-LFB` mit dem Browse-Button auswählen und einstellen)

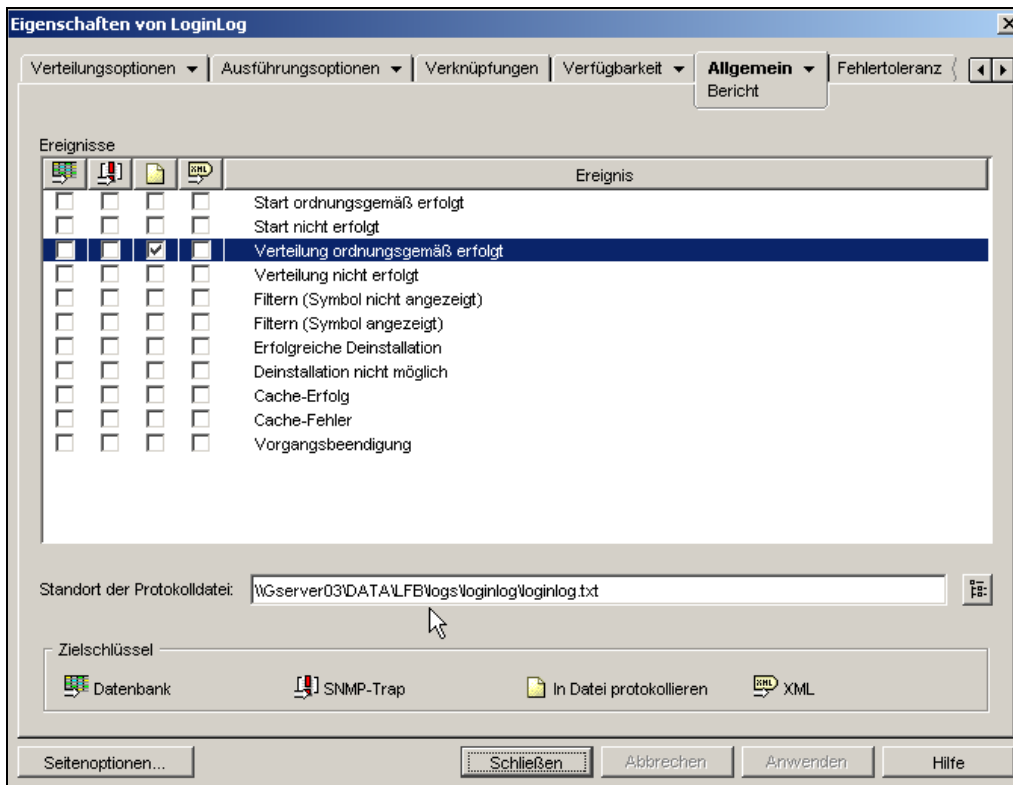


Abbildung 14.13.: Einstellungen für den Bericht (UNC-Pfad)

- Über die Hilfe der *ConsoleOne* können Sie sich noch kundig machen, welche Daten in die Protokolldatei geschrieben werden. Leider lässt sich die Auswahl der Daten nicht reduzieren, notwendig wären eigentlich nur Datum, Anmeldenname und Station. Damit ist die Erstellung des Objekts abgeschlossen. Nach Klick auf *Anwenden* bzw. *OK* können Sie die *ConsoleOne* schließen.

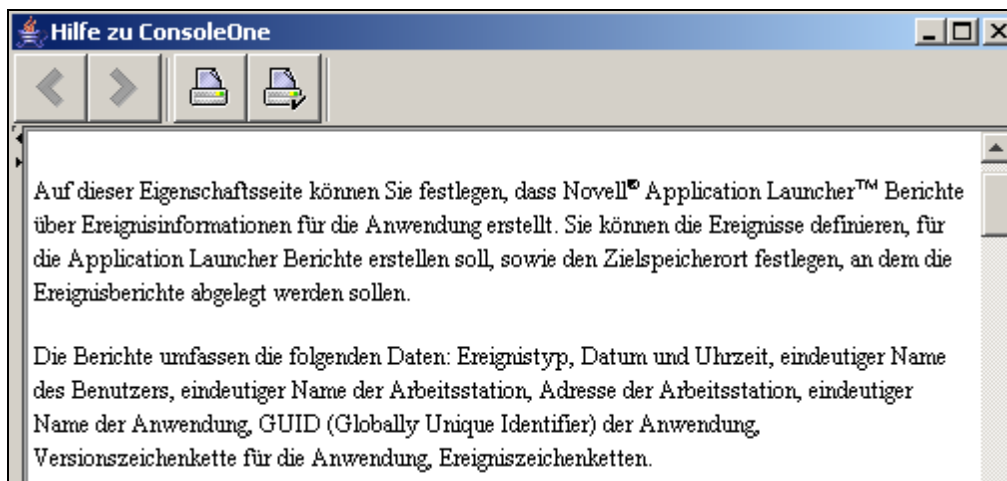


Abbildung 14.14.: Daten des Berichts

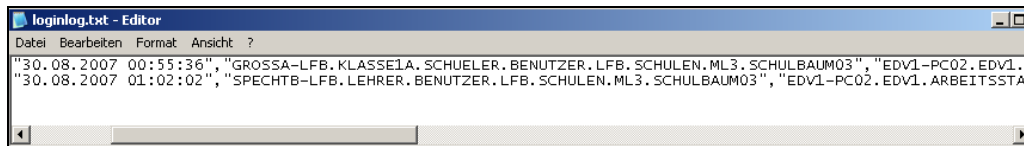


Abbildung 14.15.: Protokolldatei mit einigen Anmeldedaten

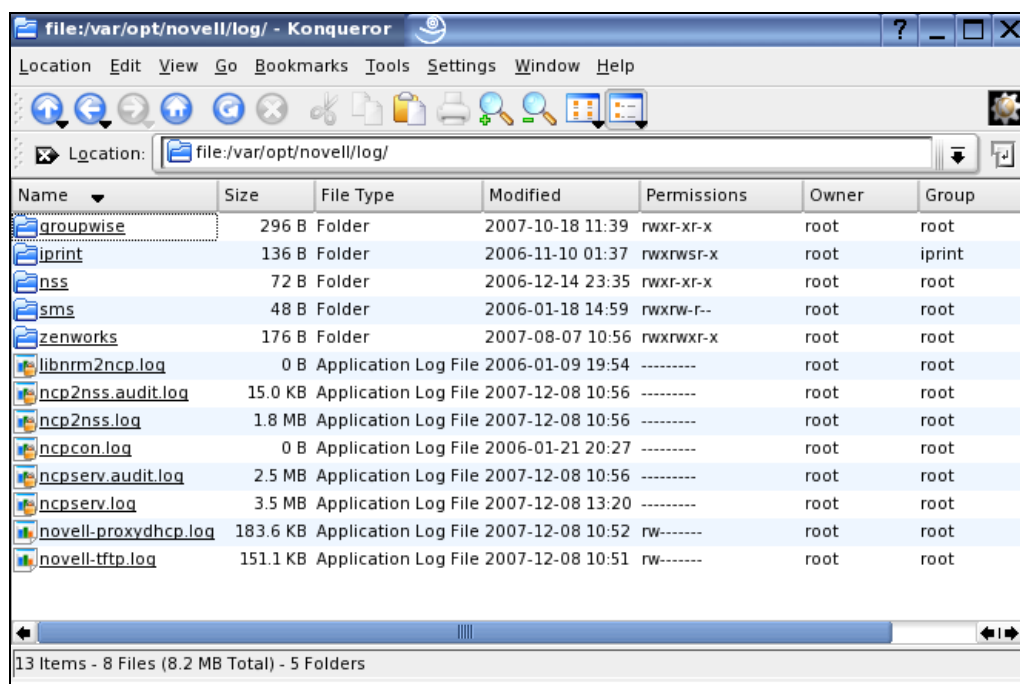
17. Zur Kontrolle der ordnungsgemäßen Funktion melden Sie sich an ML3-PC2 einige Male als Schüler / Lehrer an und überprüfen an ML3-PC1 als `SchulAdmin-LFB` die Protokolldatei!

14.2. Server-Log-Dateien

Für den Fall, dass bei Fehlfunktionen am Server mit Hilfe der Hotline eine gezielte Fehlersuche vorgenommen werden soll, ist notwendig, den Speicherort der Server-Log-Dateien zu kennen. Diese Dateien können dann bei Bedarf in gepackter Form zur Analyse an die Hotline geschickt werden. Damit Sie die von der Hotline verlangten Dateien auch finden, werden im Folgenden die verschiedenen Ordner mit diversen Log-Dateien kurz vorgestellt.

Gehen Sie wie folgt vor:

1. Melden Sie sich am Server als `root` mit dem Passwort `54321` an!
2. Starten Sie die grafische Oberfläche mit `gserver03:~ # startx`
3. Navigieren Sie mit dem *Konqueror* zu `/var/opt/novell/log` !
Sie sehen viele Log-Dateien und weitere Verzeichnisse:

Abbildung 14.16.: Log-Dateien in `/var/opt/novell/log`

4. Navigieren Sie mit dem *Konqueror* zu `/var/log` !
Hier finden Sie beispielsweise die `boot.msg`, die Informationen über das korrekte bzw. fehlerhafte Booten des Servers enthalten kann:

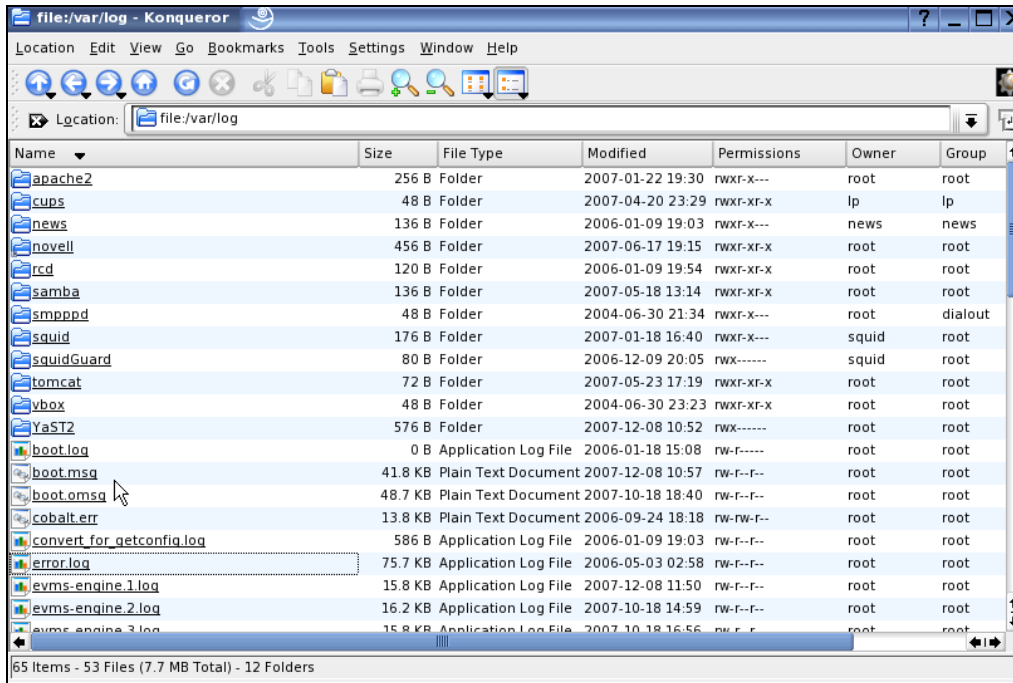


Abbildung 14.17.: Log-Dateien in `/var/log` mit `boot.msg`

5. Navigieren Sie mit dem *Konqueror* zu `/var/log/squidg` !
In diesem Ordner finden Sie die Datei, in der Squid die Internetzugriffe protokolliert. Angezeigt werden die ip-Adresse des Absenders und die besucht Seite im Internet:

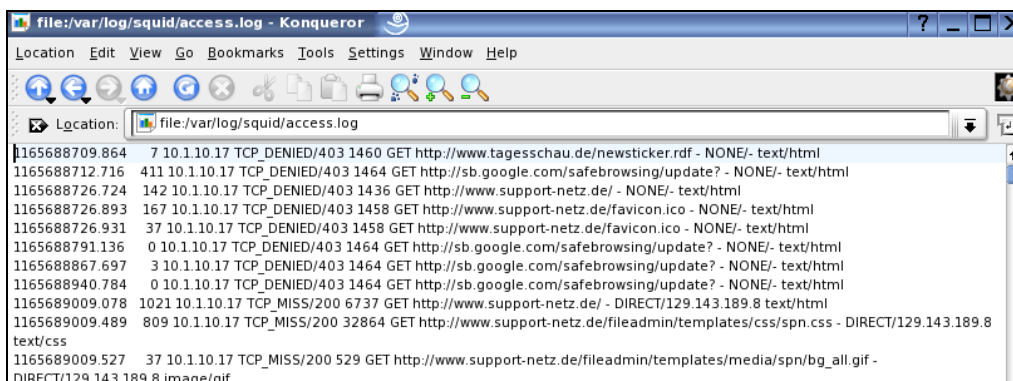


Abbildung 14.18.: Protokolldatei von Squid

Damit haben Sie einen kleinen Einblick in die ausführlichen Log-Dateien des Servers erhalten. Bei Bedarf sollten Sie nun in der Lage sein, benötigte Dateien zu finden und zur Analyse an die Hotline zu senden.

14.3. Protokoll-Datei mit „supportconfig“ erstellen

Für besonders hartnäckige Fehlerfälle bietet die Hotline die Möglichkeit, mit Hilfe eines Programms *supportconfig* eine Protokolldatei zur Auswertung zu erstellen. Dieses Tool erhalten Sie direkt von der Hotline, es muss installiert werden!

Gehen Sie wie folgt vor:

1. Installieren Sie das Tool *supportconfig* mit:
`rpm -Uvh supportconfig-2.16-01.noarch.rpm`
oder über: *Konqueror* | *Rechtsklick* | *Installieren mit Yast*
2. Öffnen Sie eine *Shell* und starten Sie das Programm:

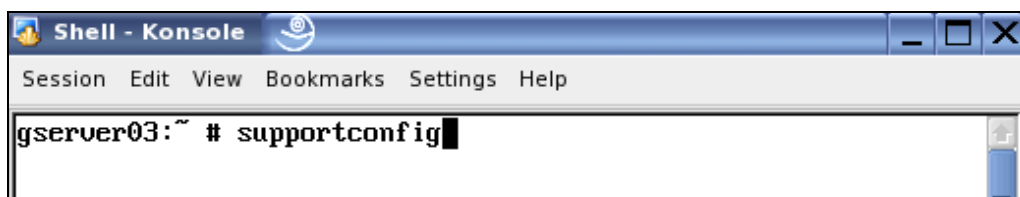


Abbildung 14.19.: Starten von *supportconfig*

3. Das Programm „sammelt“ nun eine Menge von Informationen und zeigt (nach mehreren Minuten) folgenden Abschlussbericht:

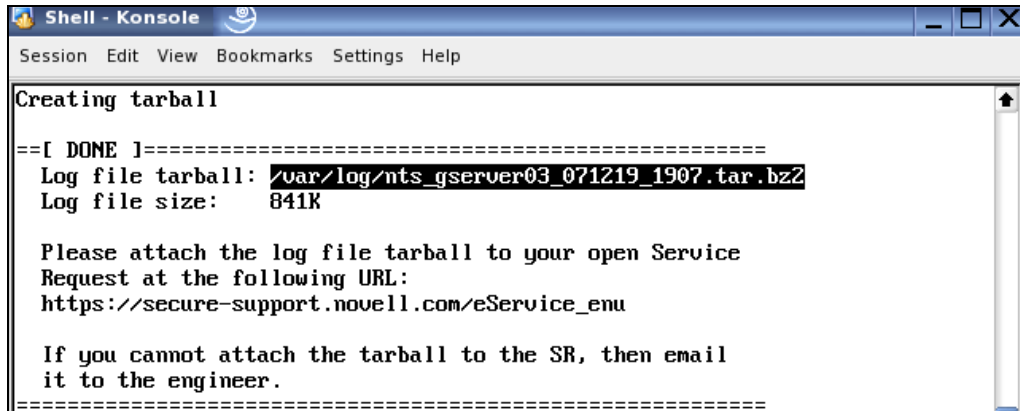


Abbildung 14.20.: Fertigstellung der Protokolldatei

4. Die Protokolldatei finden Sie unter dem Namen:
`nts_gserver03_Datum_Nummer.tar.bz2` in `/var/log`:
(Datum und Nummer werden immer wieder angepasst.)

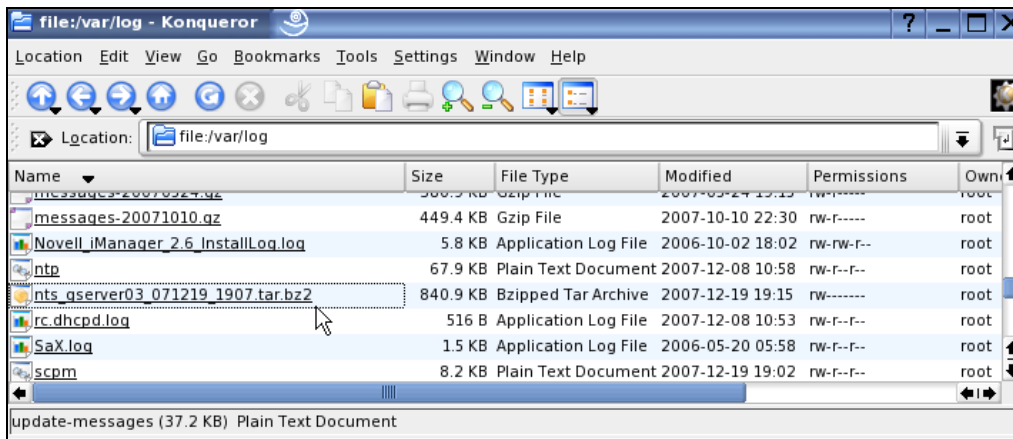


Abbildung 14.21.: Speicherort der Protokolldatei

- Die gepackte Datei könnten Sie nun zur Analyse an die Hotline schicken.
- Wir wollen natürlich wissen, was alles in der Datei zu finden ist. Dazu entpacken wir diese mit *Rechtsklick | Actions | Extract here* und erhalten sehr viele lesbare Textdateien, die eine große Menge an Informationen zum Server enthalten:

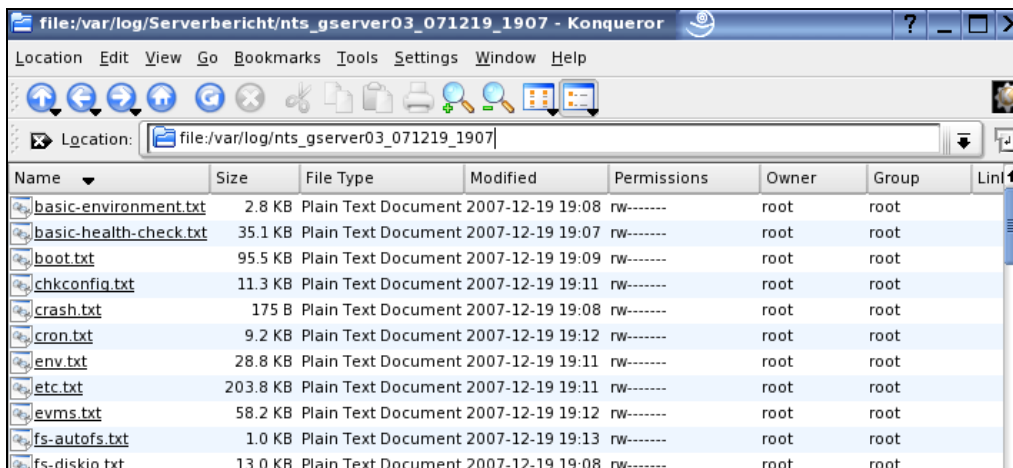


Abbildung 14.22.: Extrahierte Berichtsdateien

14.4. Protokollierung der Internetzugriffe

Die personenbezogene Protokollierung der Internetzugriffe ist z. Zt. (Mai 2009) noch nicht implementiert. Es wird lediglich protokolliert, von welchen ip-Adressen aus welche Seiten zu welcher Zeit aufgerufen wurden.

Literaturverzeichnis zm Kapitel 14:

- [1] Mailing-Liste *nwmuster* zur paedML Novell Beitrag von P. Stock, Sindelfingen
- [2] Download-Adresse für *supportconfig*:
<http://www.novell.com/coolsolutions/tools/16106.html> (Stand: Dez. 2007)