Beratung und Support
Technische Plattform
Support-Netz-Portal

paedML® – stabil und zuverlässig vernetzen

Installationsanleitung

Neu-Installation von paedML Novell Filr 5.0.0.1

Stand 24.04.2023

paedML® Novell

Version: 4.5

paedML N

LMZ LANDESMEDIENZENTRUM BADEN-WÜRTTEMBERG

Impressum

Herausgeber

Landesmedienzentrum Baden-Württemberg (LMZ)
Support-Netz
Rotenbergstraße 111

70190 Stuttgart

Autoren

der Zentralen Expertengruppe Netze (ZEN),
Support-Netz, LMZ

Stefan Falk
Ulrich Frei
Carl Heinz Gutjahr
Stephan Kluge
Uwe Labs
Alfred Wackler

Endredaktion

Alfred Wackler

Bildnachweis Symbole Titelseite

Symbole von “The Noun Project” (www.thenounproject.com)

Weitere Informationen

www.lmz-bw.de

Änderungen und Irrtümer vorbehalten.

Veröffentlicht: 2023

Inhaltsverzeichnis

Vorwort

Diese Anleitung beschreibt die Einrichtung des *Micro Focus (Novell) Filr 5*-Servers in Version 5.0.0.1.

Micro Focus Filr ist die sichere Alternative zu cloudbasierten File-Sharing Diensten wie beispielsweise **DropBox. Statt auf externe Angebote zu setzen, ermöglicht der Einsatz von *Filr* eine eigene DSGVO-konforme Cloud auf den Schulservern.**

Zusätzlich zu der Collaboration-Software *Micro Focus (Novell) Vibe* auf dem KServer erhalten Sie mit *Micro Focus Filr* eine Anwendung, mit der ein schneller Zugriff auf Daten auf dem schulischen Fileserver realisiert wird – das Teilen von Dateien wird hierdurch zu einem Kinderspiel.

Micro Focus Filr arbeitet mit dem eDirectory zusammen, benötigt aber keine Neuanlage von Zugriffsrechten. *Filr* verwendet die bereits vorhanden Rechte auf den NSS-Volumes des GServer03, so dass der Zugriff von außen mit denselben in der *paedML Novell* konfigurierten Rechten wie im Intranet erfolgt. Dabei behält der Netzwerkberater die volle Kontrolle über das Teilen von Dateien. Dateien werden auch nicht zwischen *Filr* und GServer03 hin- und her kopiert, sondern bleiben an ihrem Ursprungsort auf dem GServer, beispielsweise im Homeverzeichnis.

Micro Focus Filr ist von überall aus erreichbar: von Ihrem Desktop aus, über einen Browser und von mobilen Geräten, wie Tablets oder Smartphones. Der Zugriff kann aus dem pädagogischen Netz, aber vor allem auch von außerhalb der Schule (sofern eingerichtet) erfolgen. Es gibt auch kostenlose Apps für iOS und Android im jeweiligen App-Store. Der Zugriff erfolgt verschlüsselt. Novell warb für den *Filr* mit dem Spruch: „Feels like DropBox, acts like Fort Knox – Fühlt sich an wie DropBox, agiert aber wie Fort Knox“.

Mit *Micro Focus Filr* und auch *Vibe* hat eine substantielle Erweiterung Einzug in die *paedML Novell* gehalten. **Hiermit haben wir eine schuleigene Cloud.**

Der hier vorgestellte Server ist ein *SLES 15 SP4* -Server mit 64 Bit, auf dem *Micro Focus Filr 5.0* installiert und für den Einsatz in der *paedML Novell* vorkonfiguriert ist.

Diese Maschine liegt als virtuelle Maschine in Form von OVA-Dateien vor. Zum Virtualisierungskonzept innerhalb der *paedML Novell* lesen Sie bitte auch das Dokument *OVA_paedML-Novell.pdf*

Die hier vorliegende Anleitung ist beispielhaft für ein *VMware ESXi*-System beschrieben.

Der *paedML Novell Filr Server* ist fertig eingerichtet. Sie müssen lediglich schulspezifische Anpassungen innerhalb von *Filr* nachtragen.

Filr bietet außerdem einen „Dropbox-Ersatz“. So lässt sich z.B. ein Ordner auf dem heimischen PC mit dem *Filr Desktop* komfortabel mit einem Ordner im eigenen Homeverzeichnis auf dem GServer03 synchronisieren. Im Gegensatz zur Dropbox wissen die Lehrkräfte ganz genau, wo ihre Daten liegen: Im eigenen Schulnetz; datenschutzrechtliche Belange bleiben gewahrt.

Für die Arbeiten dieses Dokuments benötigen Sie aus dem LMZ-Paket:

- *Filr5001.ova* virtuelle Maschine
- Zusatzdokumente: (alles zusammen in *filr5001zusatz.zip*)
  OVA_paedML-Novell.pdf
  Installation-Filr-DesktopAPP-Office.pdf
  wpad-ML333.pdf

ChangeText.exe
Zertifikate-Anleitung.pdf

1. Voraussetzungen

Um den *paedML Novell Filr* Server einzusetzen, benötigen Sie einen Virtualisierungsserver, z.B. auf Basis von *VMware ESXi*, auf dem genügend Speicherplatz im DataStore für die **neue virtuelle Maschine** ist.

Micro Focus Filr wird von Micro Focus/Novell als eine sogenannte virtuelle Appliance geliefert, die normalerweise in mehreren Schritten auf dem Virtualisierungshost installiert werden muss. Die von der ZEN Novell vorbereitete virtuelle Maschine ist – nach dem Einspielen in VMware – sofort einsatzbereit.

Das Installationsverfahren haben wir mit dem hier vorliegenden Paket schon zusammengefasst und konfiguriert.

Filr 5 wird auf drei virtuellen Platten installiert. Auf der ersten Platte befindet das Linux-Datei-System. Auf der zweiten Platte mit der Partition */vastorage* befinden sich sämtliche Konfigurations-Dateien und ggf. Nutzerdaten. Die dritte Platte enthält die */var*-Partition. Durch diese Aufteilung vereinfacht sich ein zukünftiger Update-Prozess! Bei neuen *Filr*-Versionen wird im Wesentlichen nur das System, also die erste Platte, ausgetauscht. Alle Anwenderdaten und die Konfigurationsdateien bleiben dabei erhalten.

Novell erlaubt eine *Filr*-Installation für kleinere bis sehr große Systeme. Für Schulen ist das sogenannte „Small Deployment“ ausreichend. Diese Konfiguration wurde im *paedML Novell Filr*-System umgesetzt. Hierbei laufen *Filr*, *PostgreSQL* und die zugehörige Suchmaschine auf einem Server.

Systemvoraussetzungen

Ab *Filr 5* wird die paedML Novell 4.5 und höher vorausgesetzt. (OES 2018 SP3)

Wie aus dem Gesagten hervorgeht, ist der *Filr* also ein eigener Server. Er benötigt CPUs/Kerne, Arbeitsspeicher und Festplattenplatz. Für unsere Zwecke wurde eine virtuelle Maschine erstellt, die die folgenden Hardwarevoraussetzungen mit sich bringt:

- 4 CPUs (besser 2 CPUs mit je zwei Kernen)
- 20 GB RAM
- Java Heap min/max 12/12 GB
- Erste Festplatte ist nach Micro Focus-Vorgabe voreingestellt auf 50 GB
- Zweite Festplatte ist voreingestellt auf 200 GB, allerdings in Thin-Provisioning[1], so dass sie nicht sofort diese Größe belegt, sondern „wächst“. Je nachdem, ob es auf dem *Filr* zusätzliche

[1] https://de.wikipedia.org/wiki/Thin_Provisioning

persönliche Arbeitsbereiche geben soll oder nicht, sollte die Größe folgendermaßen abgeschätzt und ggf. vergrößert werden:
200 GB + geplante Speicherplatzgröße pro Benutzer

- Dritte Festplatte ist voreingestellt auf 76 GB und enthält die */var*-Partition. Nach Novell-Vorgabe berechnet sich die Größe nach der Formel 4 + 3 x RAM-Größe, also eigentlich 64 GB; wir haben 76 GB gewählt, um noch eine RAM-Erweiterung auf 24 GB zuzulassen.

Die genannten Ressourcen müssen dem *Filr*-Server zur Verfügung gestellt werden.

Aus Sicherheitsgründen sollte der *Filr* in der DMZ betrieben werden. Dazu ist es entweder erforderlich, dass eine Firewall (normalerweise die Sophos UTM/SG) oder wenigstens ein Router vorhanden ist, der zwischen der DMZ und dem GServer03 im internen Netz routen kann.

Alternativ können Sie die im Dokument *Zertifikate-Anleitung.pdf* (Gesicherter-Zugriff auf die paedML Novell mit Zertifikaten - *meineschule.de)* beschriebene Methode verwenden, die den externen Zugriff auf paedML Ressourcen im Schulnetz beschreibt. Unser *Filr-System* hat die IP-Adresse **192.168.1.38**.

Der *Filr 5* setzt die *paedML Novell 4.5 (*also *OES 2018 SP3)* voraus. Damit sind etliche Einstellungen im eDirectory und im Filesystem bereits erledigt.

Eine weniger technische Planung ist die Überlegung, wer Zugriff auf den *Filr* haben soll.

Zu Beginn kann es ratsam sein, die Benutzung des *Filr* zunächst auf Lehrkräfte zu beschränken, um Erfahrungen zu sammeln.

Soll der *Filr* auch Schülern zur Verfügung stehen, sollten weitere Überlegungen angestellt werden. Zum einen könnten dies nicht-technische Überlegungen sein:

- *Wird die Schule möglicherweise zum Provider? Welche Konsequenzen könnten sich daraus ergeben?*
- *Ist der Zugriff auf das Homeverzeichnis oder auf Projektverzeichnisse gewünscht?*
- ...

Zum anderen könnten dies auch technische Überlegungen sein:

- *Verfügt die Schule über genügend Bandbreite, wenn viele Schüler gleichzeitig von außen auf das Schulnetz zugreifen?*
- ...

2. Installation von Filr 5

2.1 Datenträger

Der vom LMZ ausgelieferte *Filr* enthält einen lauffähigen *Filr 5*-Server, der als virtuelle Maschine auf dem ESXi-Host installiert werden kann.

2.2 Einspielen des Filr 5

Kopieren Sie die vom LMZ erhaltene Datei *filr5001.ova* auf eine Arbeitsstation, die den *vSphere Client* installiert hat bzw. für den Web *vSphere Client* geeignet ist.

Je nachdem, ob Sie die kostenfreie ESXi-Version verwenden oder die Essential Plus, haben Sie eine einfachere Version des *VMware vSphere Client* oder greifen mit diesen auf das *vCenter* zu. Je nach ESXi-Version (z.B. 5.5, 6.7, 7, 8) verwenden Sie den klassischen *VMware vSphere Client oder die Web-Version*.

Wie Sie prinzipiell eine OVA-Datei auf Ihren ESXi-Host hochladen, lesen Sie bitte im beiliegenden Dokument *OVA_paedML-Novell.pdf* im Kap. 1.1, 1.2 oder 1.3 nach. Abweichungen und Besonderheiten führen wir im Folgenden anhand des *Web-VMware vSphere Client* auf.

Geben Sie dieser neuen virtuellen Maschine dabei den Namen **Filr5**. Für das Festplattenformat schlagen wir das Thin-Modell vor. Bei der Netzwerkzuordnung wählen Sie die DMZ (also den 192.168er Bereich).

Der *Filr* wird mit drei virtuellen Platten ausgeliefert.

- Das Linux-System (SLES15SP4) befindet sich auf einer 50 GB Platte,
- die *Filr*-Daten sind auf der zweiten 200-GB-Platte in */vastorage* eingehängt,
- die variablen Daten sind auf einer 76 GB Platte in */var* eingehängt.

Falls Ihnen die Größe von */vastorage* nicht ausreicht, müssen Sie diese virtuelle Festplatte ggf. nach Maßgabe von Kap. 1 vergrößern. Wie eine solche Vergrößerung durchgeführt wird, lesen Sie bitte in der zwar veralteten und für eine alte Version von ZServer geschriebene Anleitung im folgenden Dokument: *paedML-Novell-ZServer-Festplatte-vergroessern.pdf*, die aber das prinzipielle Vorgehen beschreibt.

Die *bereitgestellte Größe* sollte dem tatsächlich benötigten Platz entsprechen. Beachten Sie die *maximale Größe* (freier Speicherplatz des Datastores).

2.3 Überlegungen zum Filr-Backup

Dieses Kapitel gilt ggf. nur, wenn Sie später eigenständig ein größeres Filr-Versionsupdate durchführen wollen. Für die vorliegende Installation spielt dieses Kapitel keine Rolle.

Verwenden Sie für die Sicherung Ihrer Server ein Backup-System, das auf der *VMware-Snapshot-Technologie* basiert, wie z.B. *Veeam*, besteht das Problem, dass sogenannte unabhängige virtuelle Festplatten (independent) nicht mit gesichert werden. Der *Filr* **kann** aber eine unabhängige virtuelle Platte enthalten, nämlich die, auf der */vastorage* liegt. Diese enthält die *Filr*-Konfiguration und möglicherweise persönliche und weitere Daten.

Diese unabhängige */vastorage*-Platte im *Filr* würde also bei einer Snapshot-Technologie nicht gesichert werden.

Glücklicherweise ist es laut Novell-Support unproblematisch, diese Platte zu einer abhängigen virtuellen Festplatte zu machen.

Bei einem Update des *Filr* müssen Sie daran denken, dass vor dem Update, also dem Kopieren der virtuellen Platte, die den */vastorage* enthält, keine Snapshots existieren dürfen.

Aus diesem Grund hat Novell vermutlich diese Platte auf unabhängig gesetzt.

2.4 Filr starten

Nachdem nun alles eingestellt ist, können Sie den *Filr* starten.

Abb. 1

Möglicherweise erschein dann:

Abb. 2

(Wenn Sie mehr sehen wollen, drücken Sie an dieser Stelle schnell die Taste ESC.)

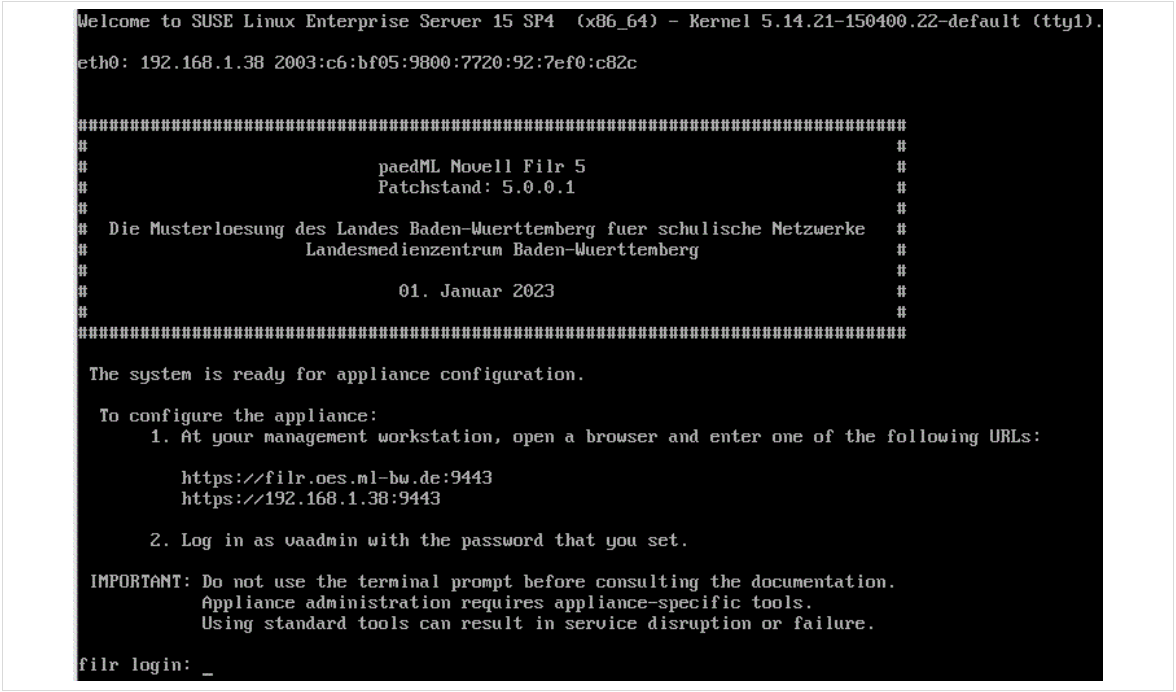


Abb. 3

2.5 VMware Tools im Filr

Die Filr Appliance enthält bereits die Open-VMware Tools. Hier sollte man tunlichst keine eigene Installation erzwingen.

2.6 Automatisches Starten/Herunterfahren der Gäste des ESXi-Servers

Siehe hierzu das Dokument *OVA_paedML-Novell.pdf*, Kap 1.5.

2.7 Passworte, Domain ändern und Java-Heap setzen

Im Auslieferungszustand sind das *root*-Passwort auf den Wert „*54321*“ und das *vaadmin*-Passwort (technischer Administrator des *Filr-Servers)* auf den Wert „*12345*“ gesetzt. Ändern Sie die Standard-Passworte in starke Passworte.

Im Folgenden wird der Zugriff auf die *Filr*-Administration für den *vaadmin* benötigt.

Der Standardaufruf ist *https://192.168.1.38:9443*. Je nach Stand der GServer03 bzw. der dortigen Konfiguration, kann es sein, dass dieser Aufruf nicht funktioniert. Versuchen Sie dann zunächst den Aufruf *https://filr.oes.ml-bw.de:9443*.

Sollte dieser auch nicht funktionieren, muss eine Änderung in der *squid*-Konfigruation des GServer03 vorgenommen werden:

In diesem Fall muss im Proxy der Port 9443 für den Zugriff auf die Admin-Konsole freigeschaltet werden. Editieren Sie dafür auf dem GServer03 die Datei */etc/squid/squid.conf* und verändern Sie folgende Zeile:

vorher:

```
acl SSL_Ports port 443 563
```

nachher:

```
acl SSL_Ports port 443 563 9443
```

Nach der Änderung bitte abspeichern und den *Squid* mit `systemctl restart squid.service` neu starten.

Von einer Arbeitsstation aus starten Sie im Browser die *Filr*-Administration mit *https://192.168.1.38:9443* und loggen sich als *vaadmin* (oder auch als *root*) mit dem Passwort `12345` im blauen Login-Fenster ein:

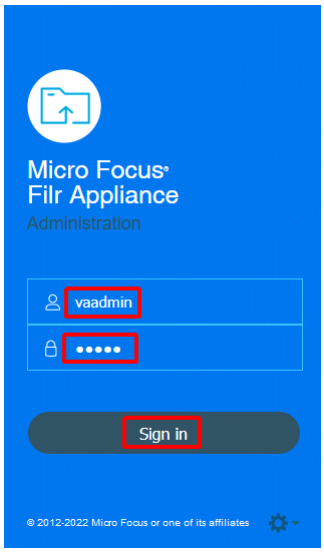
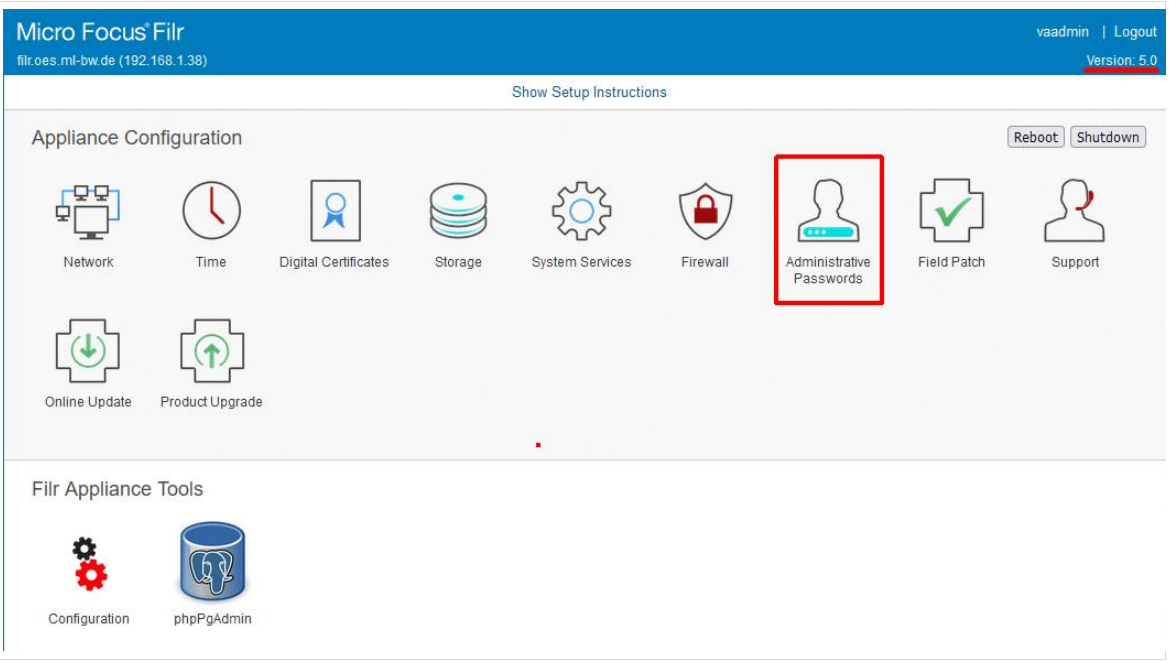


Abb. 4



Gehen Sie nun zu *„Administrative Passwords"* unter „Appliance *Configuration"* und geben Sie hier ein Passwort für den Benutzer *„vaadmin"* (dies ist der technische Administrator des *Filr*) ein.

Überlegen Sie, ob Sie als Benutzer *root* per SSH auf den Server zugreifen wollen (z.B. per PuTTy), und setzen oder löschen Sie das Häkchen bei *„Allow root access to SSH“*. Beenden Sie den Dialog mit *“OK“*.

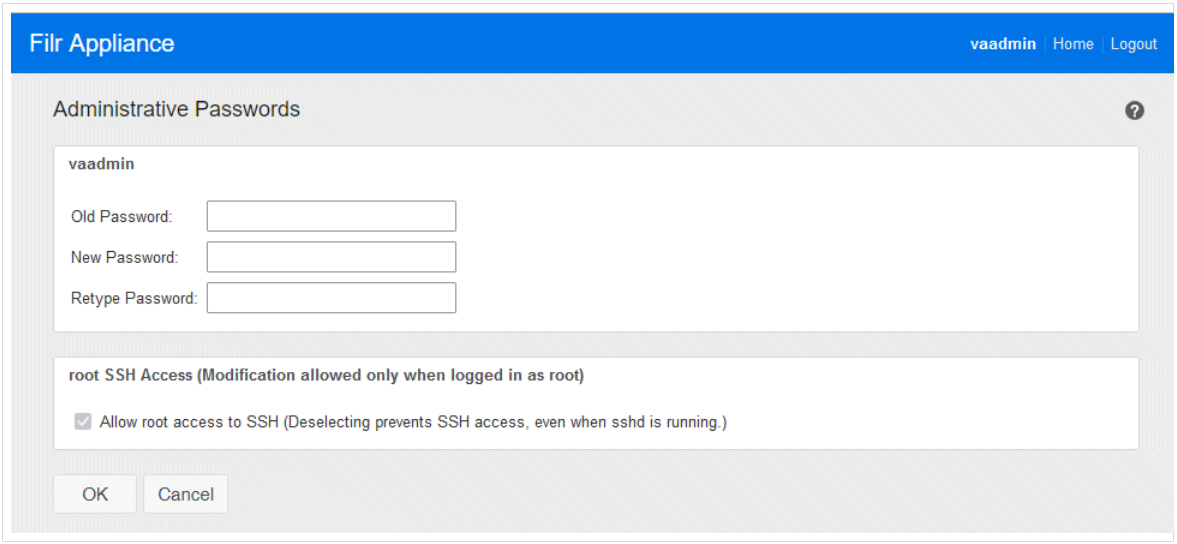


Abb. 5

(Wenn Sie sich statt mit *vaadmin* mit *root* anmelden, können Sie an dieser Stelle auch das *root*-Passwort ändern.)

Haben Sie eine eigene Domäne für Ihre Schule und den *Filr*, so können Sie diese in der *„Appliance Configuration“* (siehe Bild Abb. 7) unter *„Network“* eingeben, zunächst die *„Search Domain“* und mit einem Klick auf *„eth0“* den Rest:

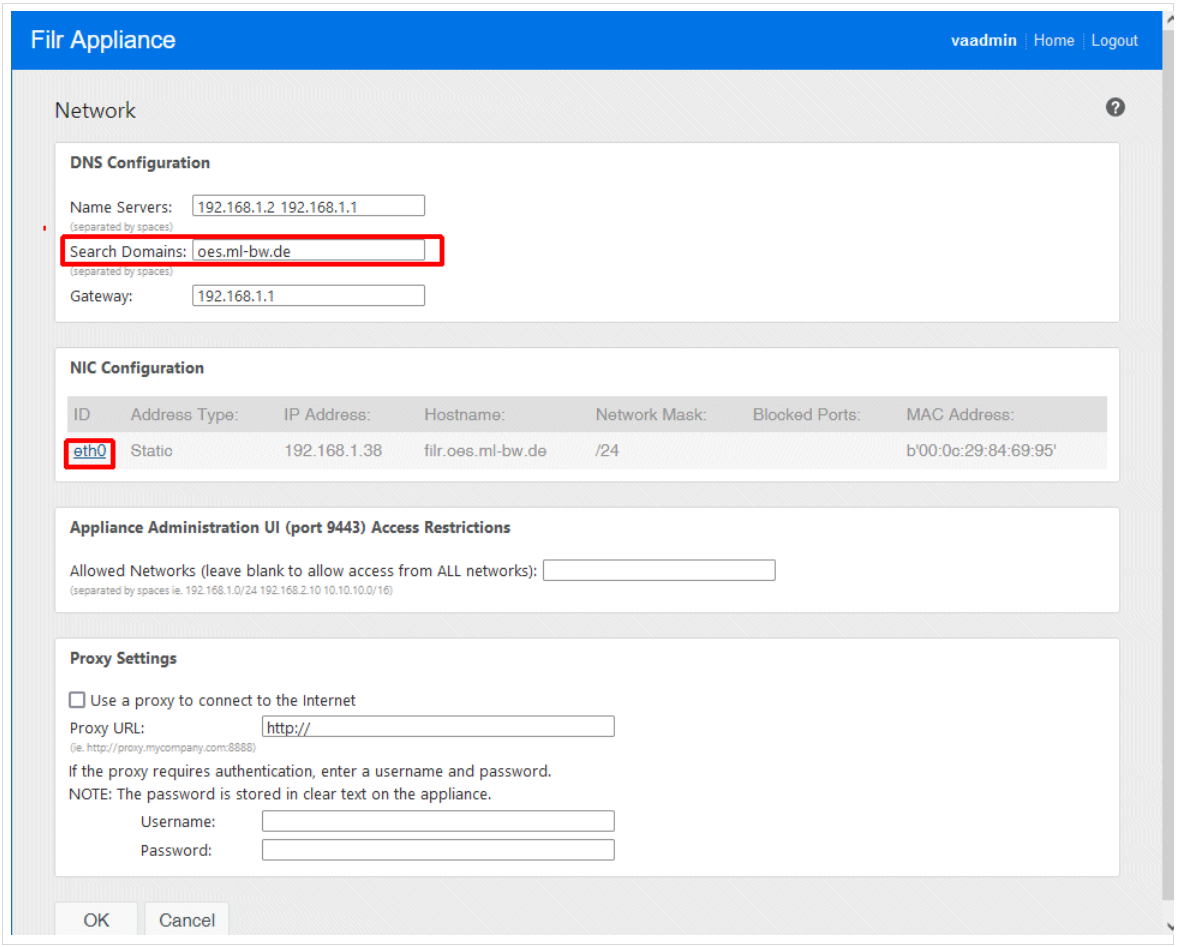


Abb. 6

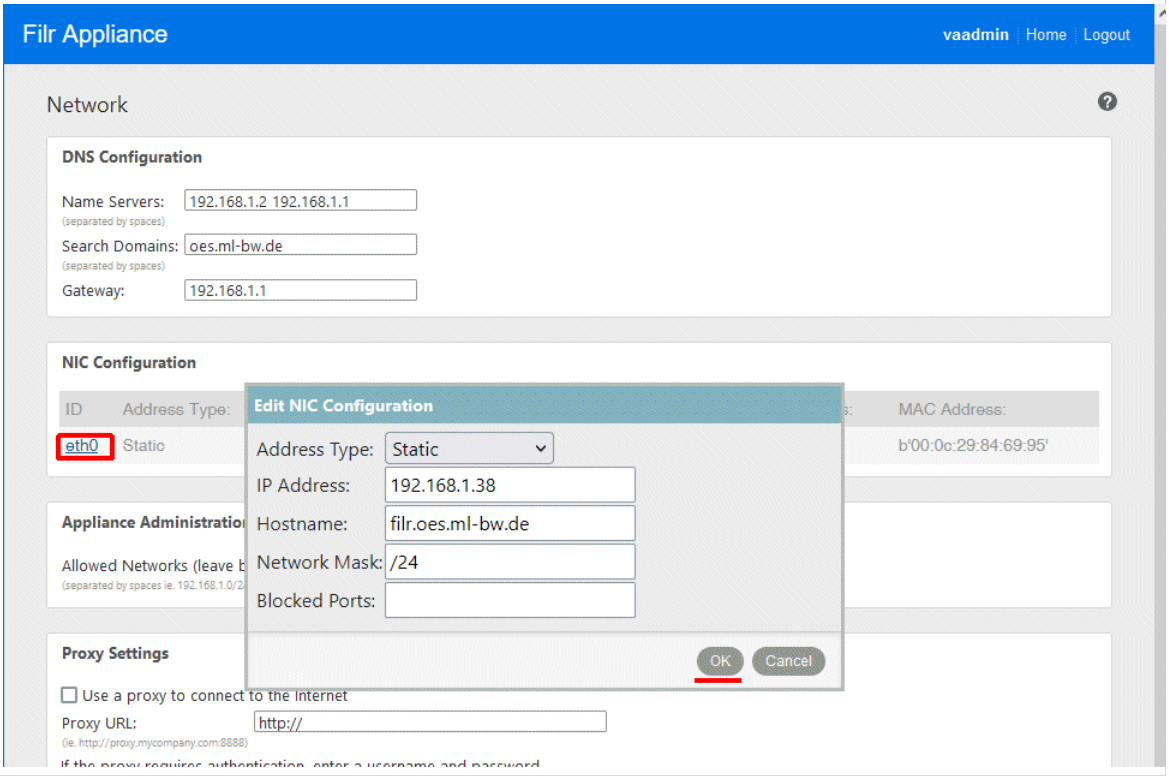


Abb. 7

In der *„Appliance Configuration“* unter *„Time“* überprüfen Sie die korrekte Einstellung des Zeitservers (hier die Sophos Firewall) und korrigieren sie ggf.:

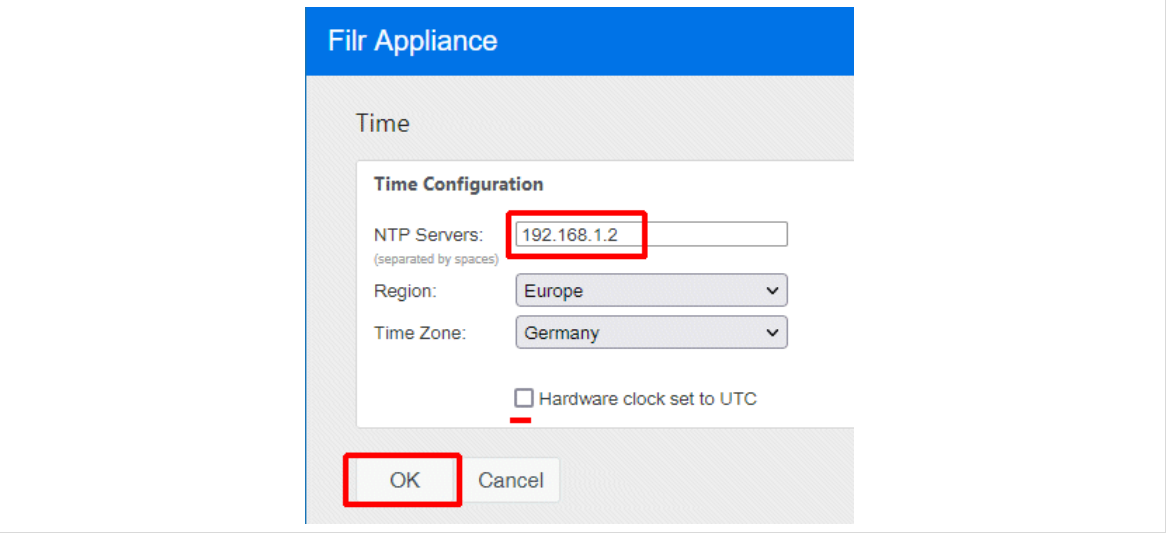


Abb. 8

Hier könnte man auch die Sophos-Firewall angeben: 192.168.1.1.

Prüfen Sie unter *„Filr Appliance Tools“ / Configuration [Abb. mit den Zahnrädern] / Outbound Email*, ob die Zeitzone korrekt eingestellt ist und korrigieren Sie dies ggf. Kein Häkchen sollte bei *Use Local Postfix Mail Server* stehen. Auch kann es sinnvoll sein, ein Häkchen bei *Force HTTPS links* zu setzen, wenn Ihre Schule von außen nur per https erreichbar ist und Sie aus *Filr* heraus Emails versenden möchten:

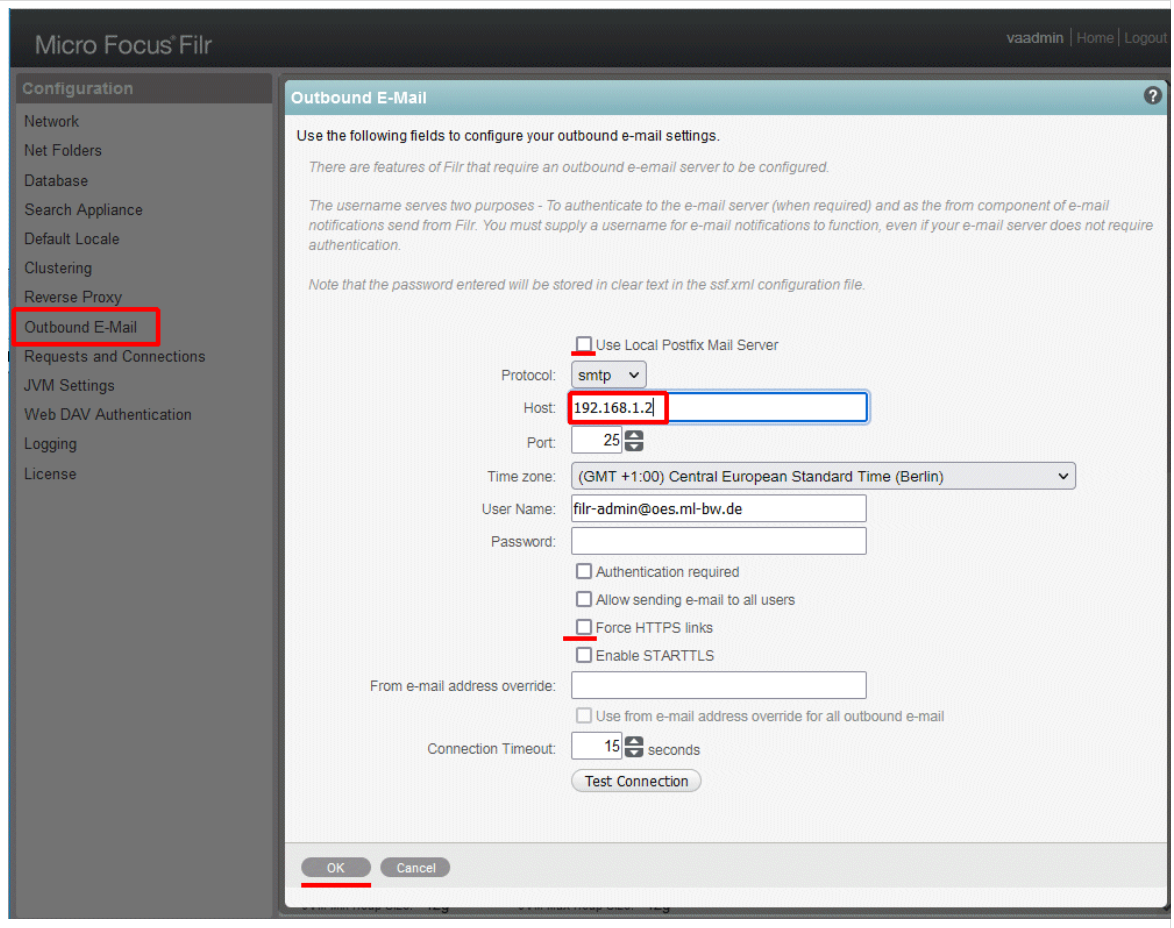


Abb. 9

Navigieren Sie nun links zu *JVM Settings*. Für den Java-Heap empfiehlt Micro Focus: ca. *"60% of the RAM should be dedicated to the Java heap."* Wir haben 12 GB gesetzt. (Bei 24 GB RAM sollten Sie hier 16 GB setzen.)

Setzen Sie also den gewünschten Wert in Feld *JVM Max Heap Size*:

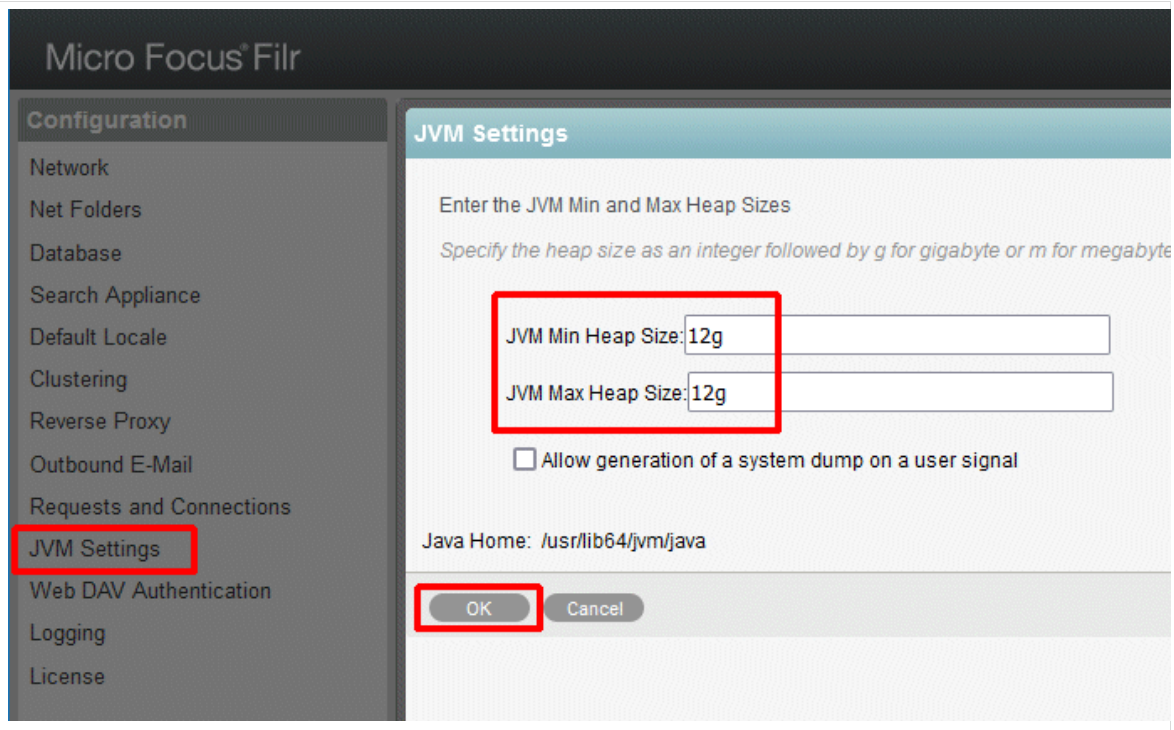


Abb. 10

→ *OK*.

Hinweis: Von einem Micro Focus Supporter haben wir gesagt bekommen: Bei vielen Benutzern (also Lehrer + Schüler) sei es sinnvoll die RAM-Größe auf 24 GB und die beiden Java-Heap Werte auf 16/16 zu setzen.

Nach Änderungen müssen Sie ein *Reconfigure Filr Server* mit dem gleichnamigen Button durchführen:

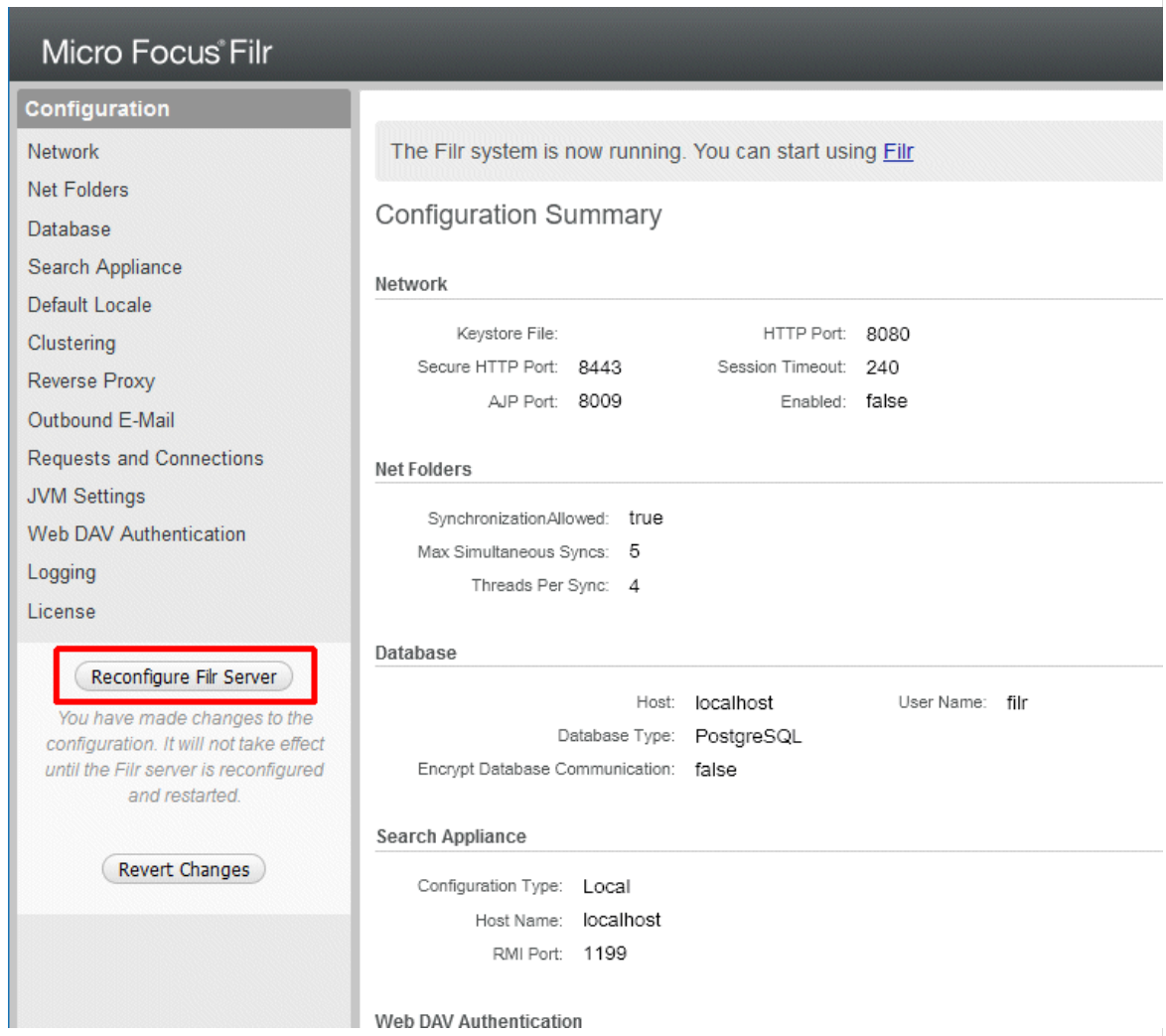


Abb. 11

→ *Reconfigure Filr Server*.

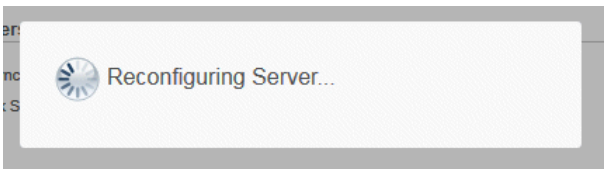


Abb. 12:

Obwohl alles weitere voreingestellt ist, können Sie sich auf der Seite „*Filr Appliance Tools - Configuration* bei dieser Gelegenheit noch ein wenig „umschauen“. Oben rechts über „*Home“* gelangen Sie wieder zur *vaadmin*-Hauptseite.

Loggen Sie sich anschließend aus (oben rechts: „*Logout“*).

Nachdem alle Einstellungen vorgenommen wurden, können Sie sich über die URL *https://192.168.1.38* am *Filr* anmelden als Benutzer *admin* mit dem Passwort `12345`:

Abb. 13

Vergeben Sie für den *admin*, der **nicht** mit dem *admin* aus dem eDirectory des GServer03 identisch ist, ein starkes Passwort:

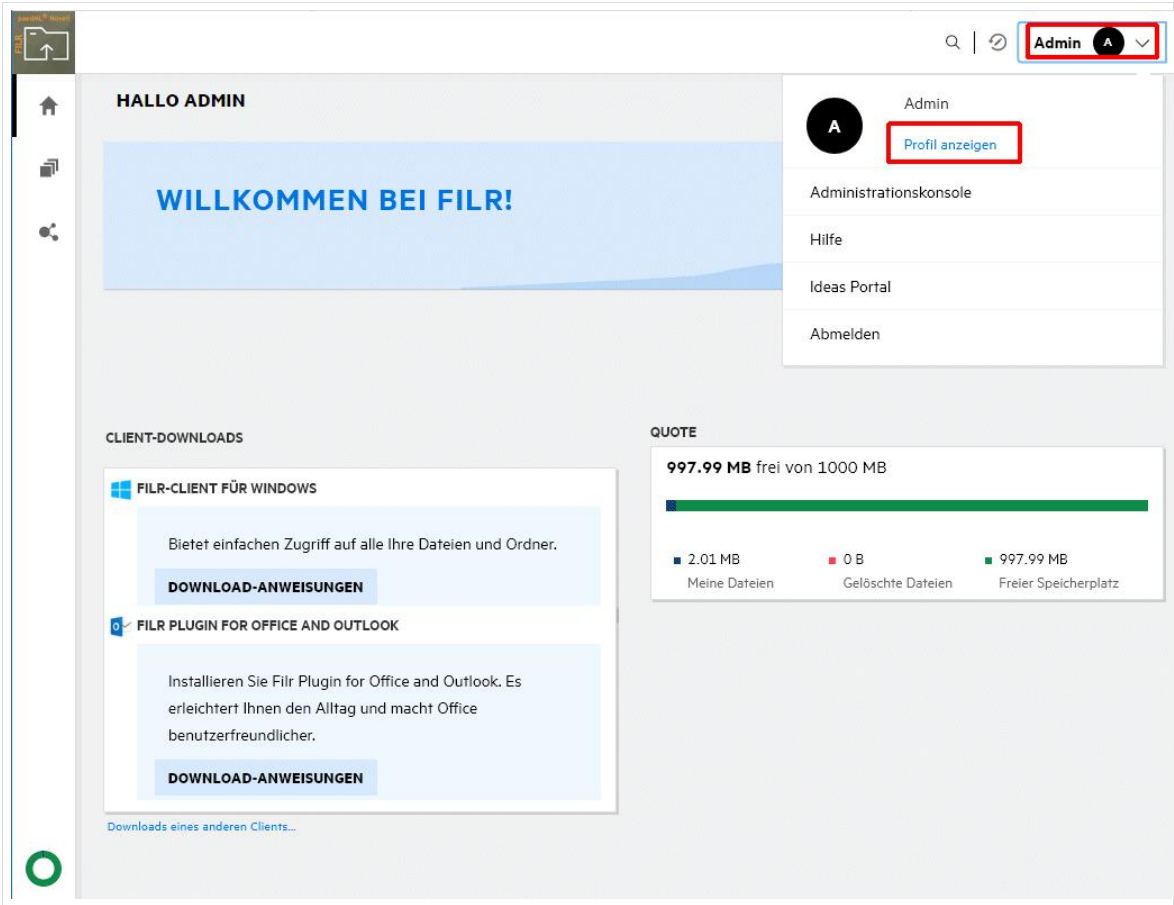


Abb. 14

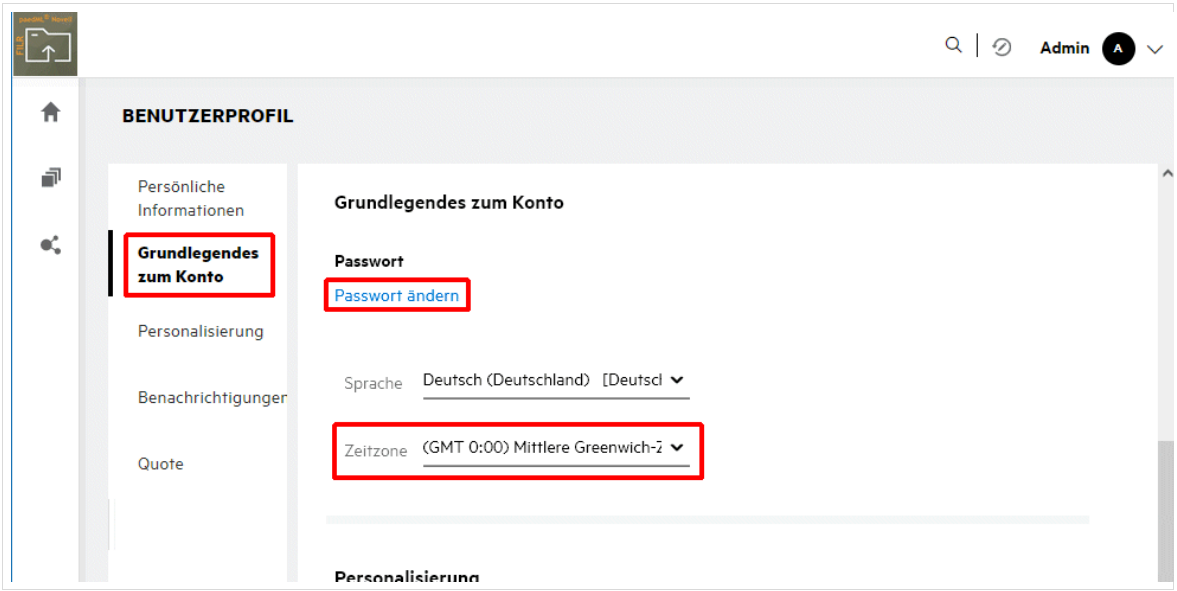


Abb. 15

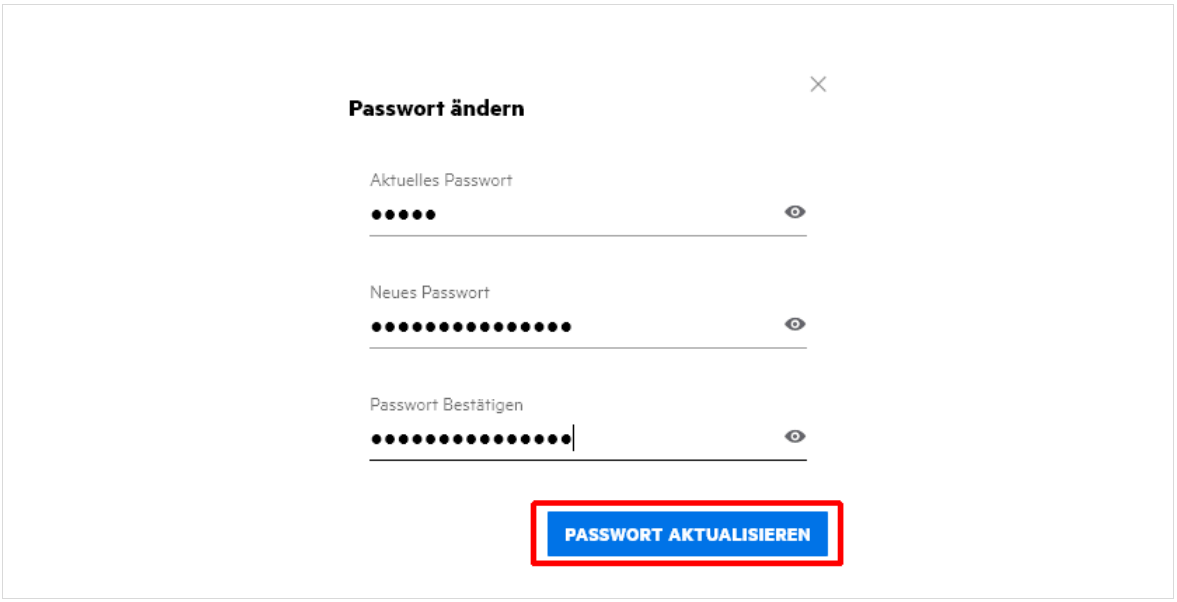


Abb. 16

Überprüfen und korrigieren Sie ggf. auch die Zeiteinstellung:

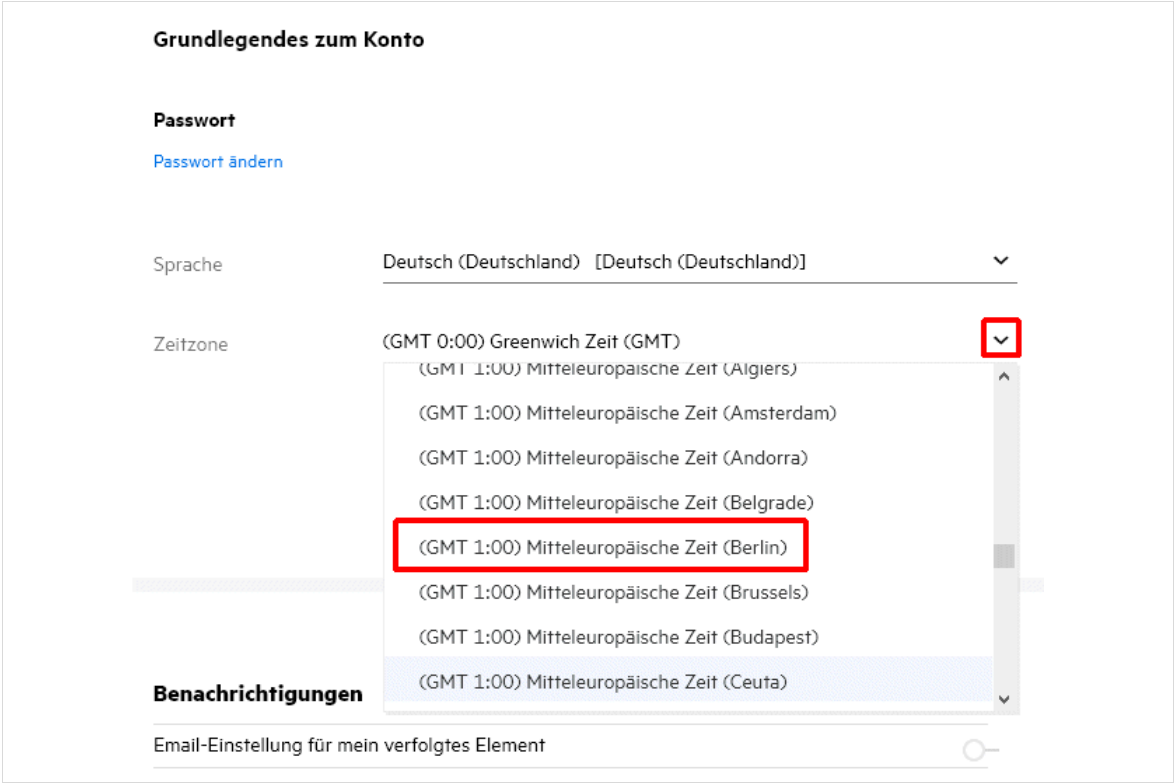


Abb. 17

2.8 Benutzerquelle

Wechseln Sie nach erfolgter Anmeldung auf die Administrationskonsole:

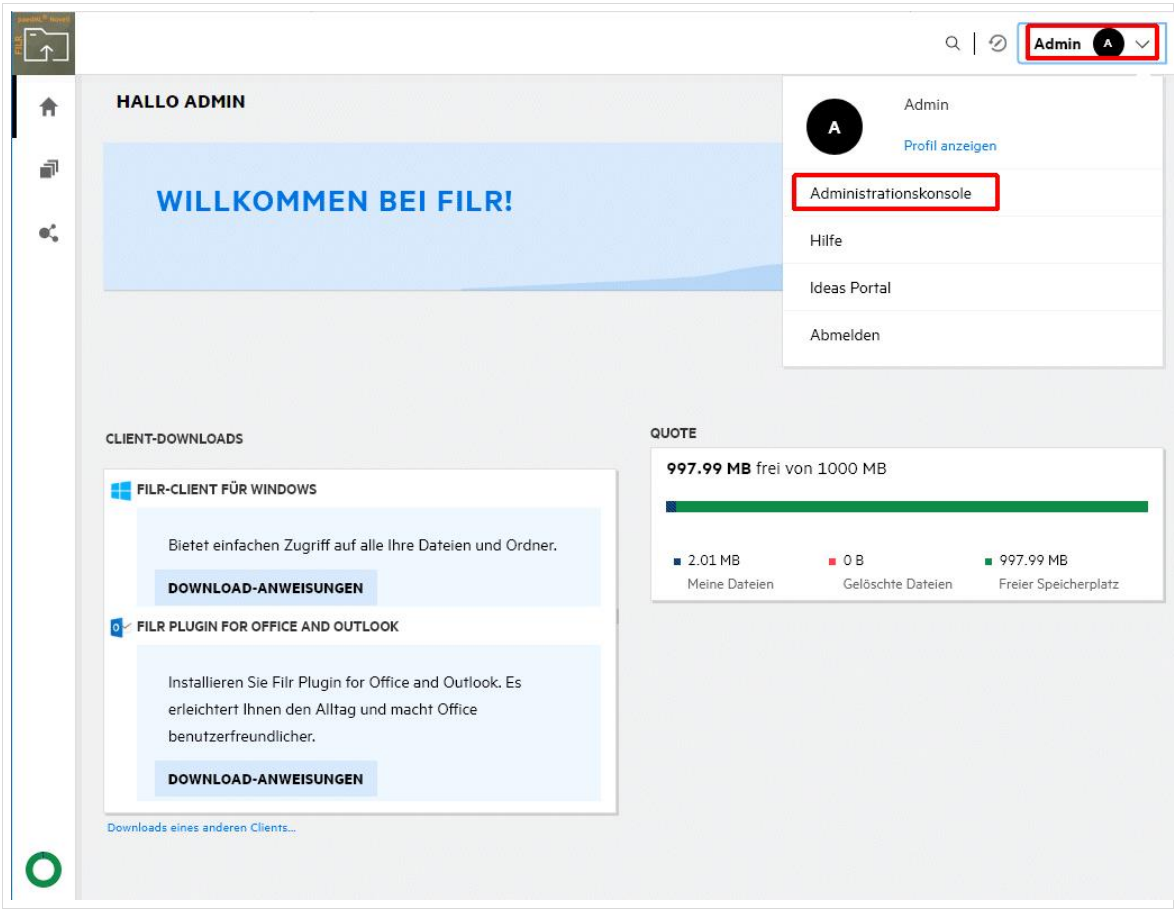


Abb. 18

Klicken Sie links unter „*System*“ auf „*LDAP*“

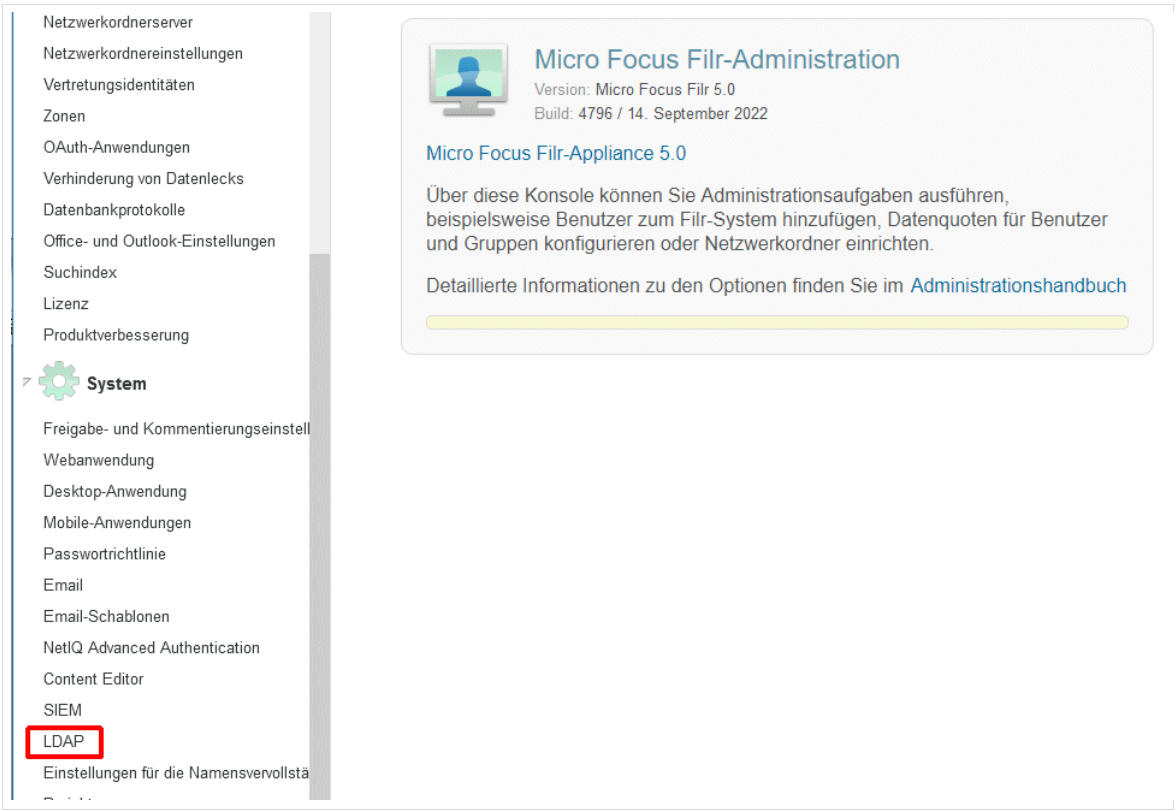


Abb. 19

und anschließend rechts auf den Link „*ldap://192.168.1.2*“. Im nächsten Dialog geben Sie über den Reiter *Serverinformationen* das Passwort, das Sie im eDirectory des GServer03 für den *ldapuserfilr* gesetzt haben, in der Zeile „*Passwort*“ ein:

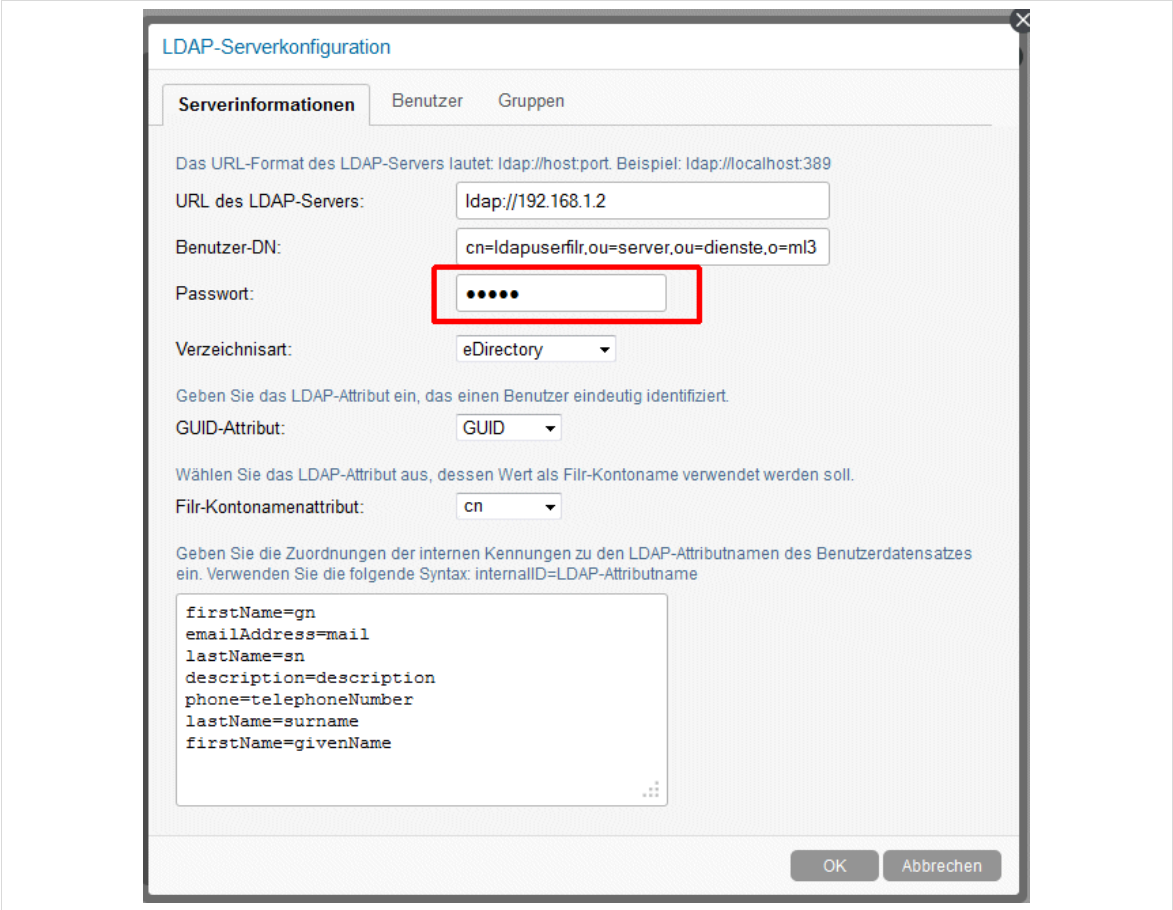


Abb. 20

Über den Reiter „*Benutzer*“, können Sie den Kontext für Ihre Schule ändern. Hier können Sie auch weitere Benutzerkontexte eingeben.

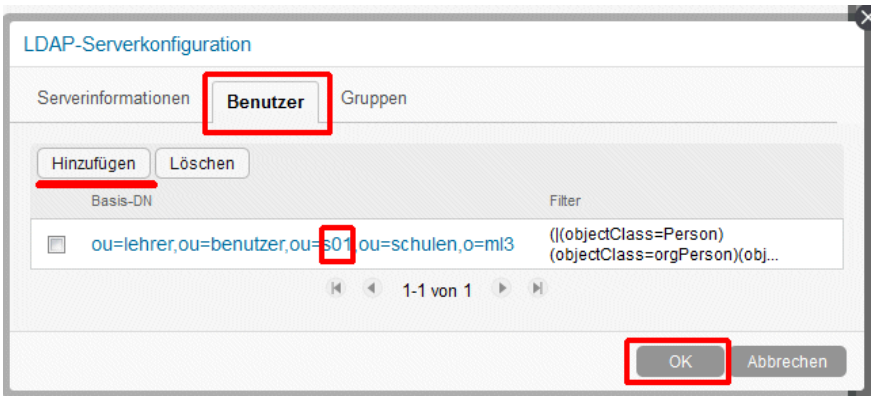


Abb. 21

In der LDAP-Konfiguration werden über die Buttons zur Synchronisierung die gewünschten Benutzer eingelesen.

2.9 Weitere Einstellungen

2.9.1 Filr-Konfiguration

Die Einstellungen für die Netzwerkordnerserver sind bereits gesetzt für die Volumes *DATA* und *DOCS*.

Allerdings müssen Sie noch das Passwort des *proxyuserfilr*, das in eDirectory gesetzt wurde, eingeben. Falls dies im eDirectory noch das Standardpasswort 12345 sein sollte, ändern Sie es zuerst dort in ein starkes Passwort. Dieses Passwort muss nun auch im *Filr* hinterlegt werden: Gehen Sie dazu in der *Administrationskonsole* des *admin* zu „Verwaltung | *Netzwerkordnerserver / 10.1.1.32-DOCS*“. Im nächsten Dialog öffnen Sie den Reiter: *Authentifizierung* und geben dort das Passwort ein.

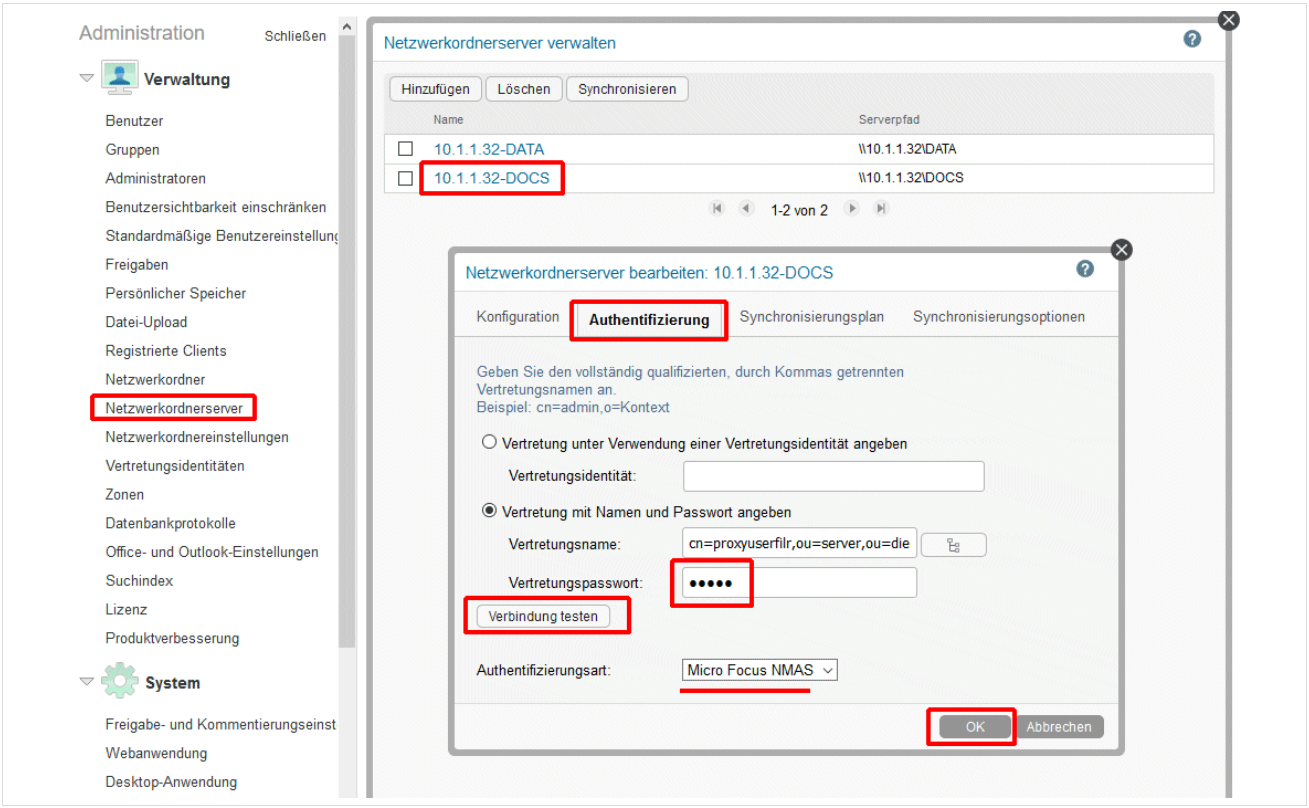


Abb. 22

Über „Verbindung testen“ überprüfen Sie, ob die Verbindung klappt.

Verfahren Sie genauso für *10.1.1.32-DATA*.

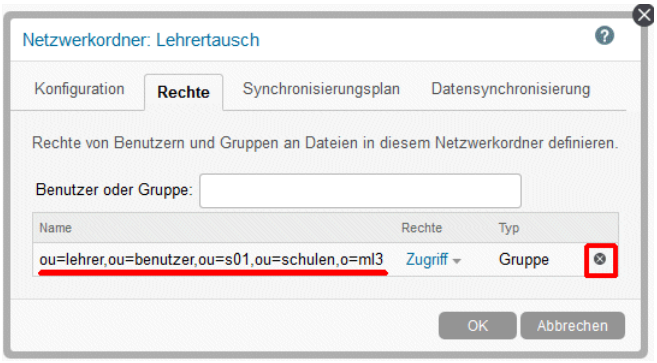
Gesetzt sind auch die Einstellungen für die Netzwerkordner für das Homeverzeichnis des *eDirectory-admin*, das Projektverzeichnis und das Lehrertauschverzeichnis für die Lehrer der Schule S01. Das jeweilige Homeverzeichnis des gerade angemeldeten (eDirectory-) Benutzers erscheint unter „*Meine Dateien*“ als Ordner „*Start*“. Als LDAP-Benutzer sind die Lehrer der Schule S01 bzw. Ihrer Schule (siehe Ihre Änderung in Kap.2.8) konfiguriert, aber noch nicht eingelesen. Diese Übernahme finden Sie in der Administrationskonsole des *admin* unter „*System / LDAP / Alles Synchronisieren*“. Ebenso ist die Übernahme von Gruppen konfiguriert, die sich in der Lehrer-OU der Schule S01 bzw. Ihrer Schule (siehe Ihre Änderung in Kap.2.8) befinden.

Anschließend öffnen Sie die Einstellungen für „*Netzwerkordner / Projekte*“ bzw. „*Lehrertausch*“. Im nächsten Dialog wählen Sie den Reiter „*Rechte*“. Dort können Sie passende Benutzer oder Gruppen eintragen. I.d.R. sollen alle Lehrer den Zugriff auf den Lehrertausch haben. Dann ist es am einfachsten, den Eintrag „*Alle internen Benutzer*“ zu wählen. Sollen hier aber Einschränkungen vorgenommen werden,

so ist der Einsatz von eDirectory-Gruppen zu erwägen. Hier haben wir die Einstellung im *Filr* so gewählt, dass Gruppen in der OU Lehrer vom *Filr* eingelesen werden. So könnte es in der OU *lehrer.benutzer.<Schule>.schulen.ml3* z.B. die Gruppe *G_Lehrer* , *G_Mathe*, *G_Physik*,... geben, die alle oder einen Teil der Lehrer enthalten.

Die folgenden Screenshots demonstrieren dies am Beispiel von „*Lehrertausch*".

Für die weiteren Einstellungen hier eine Vorbemerkung: Bei den Einstellungen für den *Netzwerkordner Lehrertausch* ist in der Auslieferungsversion beim Reiter *Rechte* der Eintrag *ou=lehrer,ou=benutzer,ou=s01,ou=schulen,o=ml3* gesetzt, was, obwohl dies eigentlich keine Gruppe ist, auch funktioniert. Wollen Sie diesen Eintrag löschen so verwenden Sie das kleine Löschsymbol rechts neben dem Eintrag.



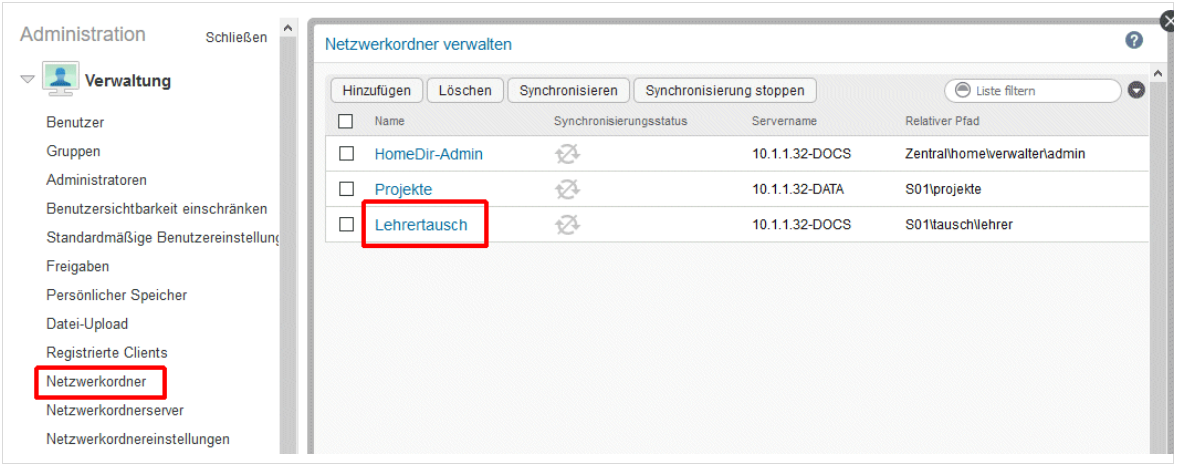


Abb. 23

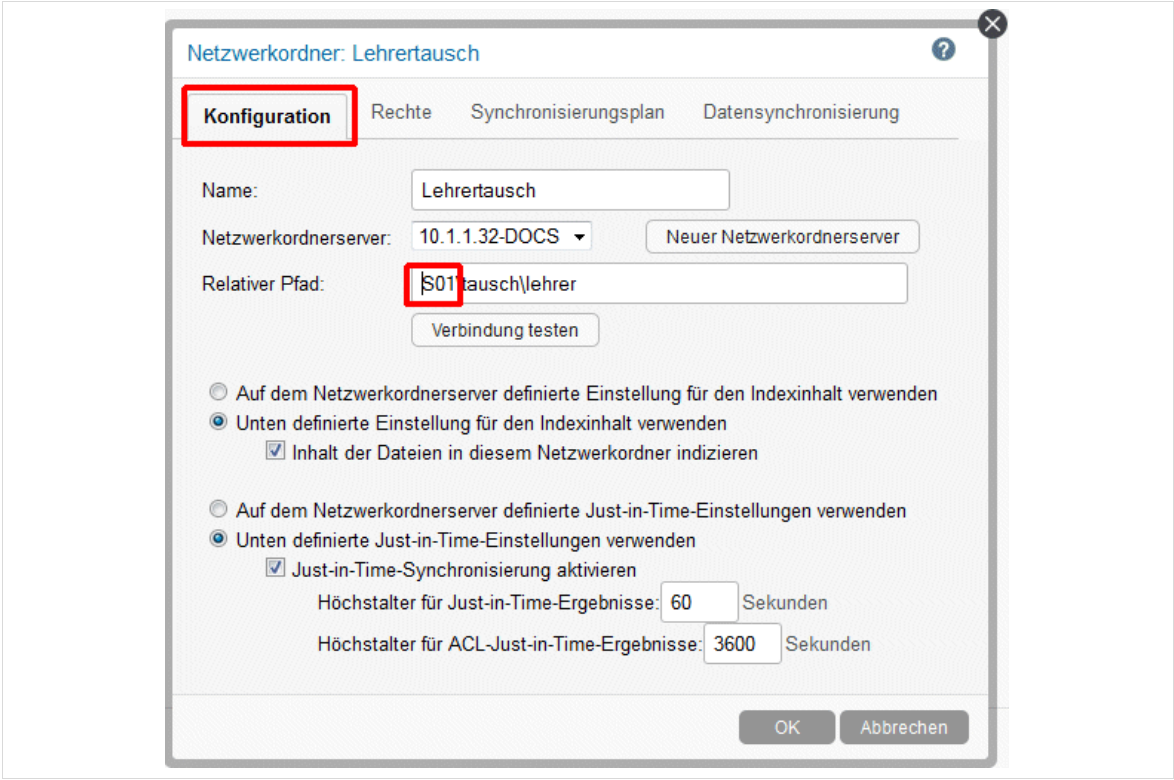


Abb. 24

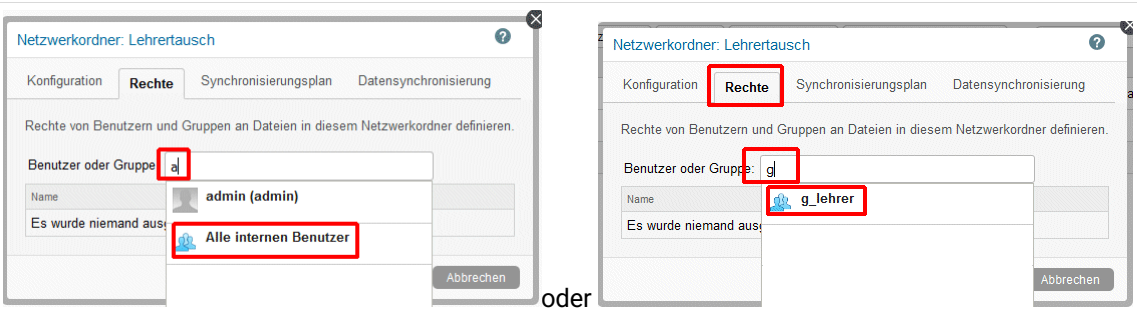


Abb. 25

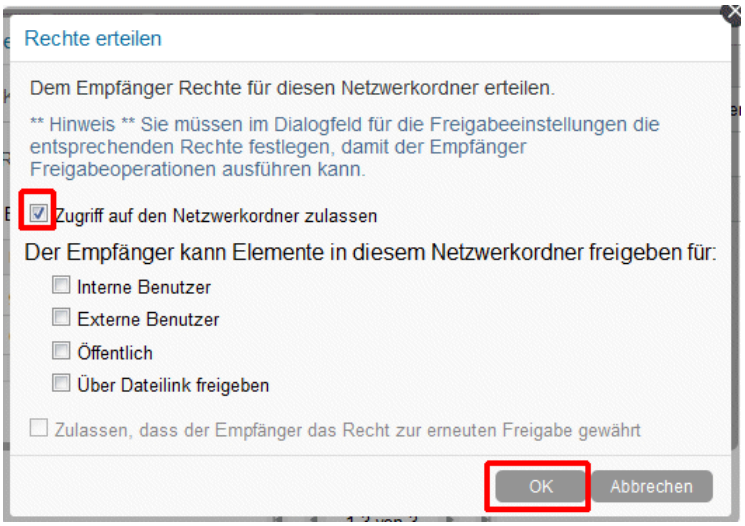


Abb. 26

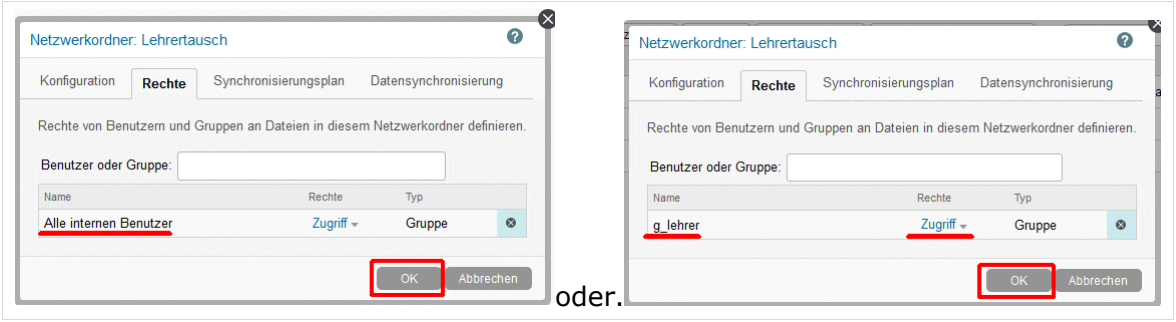


Abb. 27

Um Datenschutzrichtlinien Genüge zu tun, ist in der Administrationskonsole des Benutzers *admin* unter *„Verwaltung / Datenbankprotokolle“* die Berichtszeit auf 30 Tage eingestellt.

Im Ordner *„Meine Dateien“* des *admin* befinden sich im Ordner *Filr-Hilfen* einige der aktuellen *Filr*-Handbücher. (Leider waren zum Zeitpunkt der Erstellung dieser Anleitung fast alle Handbücher nur auf Englisch vorhanden.) Eventuell können Sie diesen Ordner für alle Benutzer freigeben. (Häkchen vor *Filr-Hilfen*, dann der Button *Freigeben*.)

Falls Sie diese Handbücher aktualisieren wollen, finden Sie die jeweils aktuellen unter: https://www.microfocus.com/documentation/filr/filr-5.

Derzeit ist die Voreinstellung für *„Meine Dateien“* für die Benutzer so gesetzt, dass Benutzer dort Dateien ablegen können. Die Quota ist auf 100 MB gesetzt; in der Administrationskonsole können Sie diesen Wert über den Menüpunkt Verwaltung / *Persönlicher Speicher* ändern.

Diese Dateien liegen dann aber auf dem *Filr* und nicht auf dem *GServer03*. Eventuell sollten Sie diese Option abschalten, dazu „persönlicher Speicherbereich für LDAP User zulassen“ deaktivieren, da Sie sonst eine „doppelte Datenhaltung“ haben (Homeverzeichnisse auf dem *GServer03* **und** im *Filr*), was möglicherweise zu Unübersichtlichkeiten und Missverständnissen führen kann.

Für den Benutzer *admin* ist die Quota auf 1000 MB gesetzt.

Für die weitere Bedienung des *Filr* verweisen wir hier auf die Materialien der Lehrerfortbildung, z.B. in https://lehrerfortbildung-bw.de/st_digital/netz/muster/novell/filr/.

2.10 Browser für Zugriff auf Filr konfigurieren

Es ist möglich, dass im Browser nichts konfiguriert werden muss, um auf den *Filr* zugreifen zu können!

In der *paedML Novell 4.x* sind die notwendigen Konfigurationen für die WPAD-Technologie im Auslieferungszustand umgesetzt.

Verwenden Sie **nicht** die WPAD-Technologie, sondern normale Proxy-Einstellungen mit Ausnahmen in Ihren Browsern, so sollte in diesen Ausnahmen die *Vibe*-Adresse *192.168.1.36*, nicht aber die *Filr*-Adresse *192.168.1.38* enthalten sein.

Ist dies bereits der Fall, so können Sie das Kap. 2.10 überspringen und bei Kap. 3 weitermachen.

Andernfalls kann es sinnvoll sein, den Rest von Kap. 2.10 zu lesen, um festzustellen, ob weitere Anpassungen nötig sind.

2.10.1 Firefox

Beim Programm *Firefox* kann die Proxy-Einstellung nicht über Richtlinien erfolgen.

2.10.1.1 Firefox - prefs.js anpassen

Damit die WPAD-Technik mit Firefox funktioniert, muss die Proxy-Einstellung im Firefox auf *Automatische Proxy-Konfigurations-URL* gestellt sein zusammen mit dem Eintrag *http://10.1.1.32/wpad.dat*.

Dazu müssen in der Datei *prefs.js* in allen Firefox-Profilen folgende Einträge stehen:

```
user_pref("network.proxy.autoconfig_url", "http://10.1.1.32/wpad.dat");
user_pref("network.proxy.type",2);
```

Falls die Datei *prefs.js* des Firefox-Profils aber in **allen** Homeverzeichnissen liegt, also z.B. in *L:\LFB\home\schueler\klasse1a\GrossA-LFB\Firefox\prefs.js* usw., können Sie dies mit dem Programm ***Changetext*** erledigen. Dieses Programm liegt bei.

Suchen Sie mit einem Editor (am besten Notepad) in einer von Ihnen verwendeten *prefs.js* den Eintrag *user_pref("network.proxy.type", 1);*

Vielleicht steht bei Ihnen auch eine andere Nummer als „1“. Übernehmen Sie diesen Eintrag in die Zwischenablage, um sie gleich in die ***„Darin wird der Text“*** -Eingabe im *TextChanger* wieder exakt einzusetzen.

Die Eingabe für unser Beispiel im Fenster *TextChanger* müsste also etwa so aussehen:

Darin wird der Text: `user_pref("network.proxy.type", 1);`

geändert in: `user_pref("network.proxy.autoconfig_url", "http://10.1.1.32/wpad.dat"); user_pref("network.proxy.type",2);`

Hinweis: Gibt es in Ihren *prefs.js*-Dateien keine Zeile `user_pref("network.proxy.type", 1);`

dann funktioniert dieses Verfahren nicht und Sie müssen eine andere Technik verwenden, z.B. Verteilung per ZENworks.

2.10.1.2 Firefox ohne WPAD-Einstellung betreiben

Falls Sie keine WPAD benutzen wollen, ist für den *Filr* keine Änderung der Datei *prefs.js* nötig.

Im Hinblick auf *Vibe* und dem Aufruf per Domainname sollten Sie jedoch die Datei *prefs.js* in allen Firefox-Profilen ändern. So muss (falls die erforderlichen Eintragungen noch nicht vorhanden sind) die Zeile

```
user_pref("network.proxy.no_proxies_on", "localhost, 127.0.0.1,
10.1.0.0/16");
```

zu

```
user_pref("network.proxy.no_proxies_on", "localhost, 127.0.0.1,
10.1.0.0/16, 192.168.1.36, .meineschule.de ");
```

geändert werden.

Achtung: Bei *„zu … geändert“* alles in eine(!) Zeile und *meineschule.de* durch ihre echte Domain ersetzen.

Falls die Datei *prefs.js* des Firefox-Profils aber in **allen** Homeverzeichnissen liegt, also z.B. in *L:\LFB\home\schueler\klasse1a\GrossA-LFB\Firefox\prefs.js* usw., können Sie dies mit dem Programm ***Changetext*** erledigen. Dieses Programm liegt bei.

Suchen Sie mit einem Editor (am besten Notepad) in einer solchen von Ihnen verwendeten *prefs.js* den Eintrag

```
user_pref("network.proxy.no_proxies_on", "localhost, 127.0.0.1,
10.1.0.0/16");
```

Vielleicht steht bei Ihnen darin noch mehr. Übernehmen Sie diesen Eintrag in die Zwischenablage, um sie gleich in die ***„Darin wird der Text“*** -Eingabe im *TextChanger* wieder exakt einzusetzen.

Die Eingabe für unser Beispiel im Fenster *TextChanger* müsste also etwa so aussehen:

Darin wird der Text: `user_pref("network.proxy.no_proxies_on", "localhost, 127.0.0.1, 10.1.0.0/16");`

geändert in: `user_pref("network.proxy.no_proxies_on", "localhost, 127.0.0.1, 10.1.0.0/16, 192.168.1.36, .meineschule.de ");`

Achtung: Bei *„geändert in“* alles in eine(!) Zeile.

Sollten Sie bei den Ausnahmen (in IE bzw. Firefox) Eintragungen vom ESXi-Managementnetz haben, belassen Sie diese natürlich.

Überprüfen Sie, ob *Vibe* bei aktivierter Internetsperre erreichbar ist, *Filr* jedoch nicht. Dies ist für Klassenarbeiten relevant, wo ein Zugriff auf Homeverzeichnisse oder auf Tausch-/Klassenverzeichnisse über den *Filr* unterbunden sein sollte.

2.10.2 Internet Explorer

Falls Sie überhaupt noch den *IE* verwenden ...

IE ist so konfiguriert, dass der Browser beim Aufruf des *Filr* den Proxy umgeht. Wenn für die Schüler dann das Internet gesperrt ist, ist die DMZ, in der der *Filr* steht, nicht mehr erreichbar. Sie erreichen dies, indem Sie Ihre(n) Browser in der Verbindungskonfiguration für den Proxy entsprechend konfigurieren.

Haben Sie bereits die WPAD-Technik im Einsatz **und** ist auf den Arbeitsstationen bei den IE-Internetoptionen unter *Verbindungen/LAN-Einstellungen* ein Häkchen bei *Einstellungen automatisch erkennen*, dann brauchen Sie nichts weiter zu unternehmen. Fahren Sie fort mit Kapitel 3.

Haben Sie bereits die WPAD-Technik im Einsatz, **aber nicht** diese IE-Einstellung auf Ihren Arbeitsstationen, so können Sie

- entweder diese Einstellung im Master-Image setzen und dieses neu verteilen

- oder per ZCM für alle Computer im Registry-Key
  HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
  das 9. Byte auf *09* setzen. Z.B. können Sie mit Windows-Registrierungseditor *regedit.exe* den Key
  HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
  exportieren und in eine Datei abspeichern. Anschließend bearbeiten Sie diese Datei mit einem Editor (z.B. Notepad). Löschen Sie nicht-relevante Zeilen heraus und ändern Sie das 9. Byte des Eintrags *DefaultConnectionSettings* auf *09*. Speichern Sie diese Datei ab, die dann etwa so aussieht

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\Connections]
"DefaultConnectionSettings"=hex:46,00,00,00,07,0b,00,00,09,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,04,00,00,00,00,00,00,00,a6,81,0f,64,ce,20,ce,01,\
  00,00,00,00,00,00,00,00,00,00,00,00,05,00,00,00,02,00,00,00,0a,01,01,66,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,02,00,00,00,c0,a8,\
  01,66,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,c0,a8,01,01,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  02,00,00,00,c0,a8,71,01,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,17,00,00,00,00,00,00,00,20,01,00,00,5e,f5,79,fd,14,0f,0f,5a,f5,fe,\
  fe,99,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00
```

  und benutzen Sie diese für die Erstellung eines ZCM-Bundles.

Oder besser den Browser *Firefox* verwenden.

Ohne WPAD-Technik sollten Sie im Hinblick auf *Vibe* auf den Arbeitsstationen bei den IE-Internetoptionen unter *Verbindungen/LAN-Einstellungen* bei *Proxy/Erweitert* und dort bei den *Ausnahmen* die IP 192.168.1.36 hinzufügen. Die Alternativen hierzu wären

- entweder diese Einstellung im Master-Image setzen und dieses neu verteilen
- oder per ZCM für alle Computer im Registry-Key
  HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\ Proxy Exceptions = ProxyOverride
  die IP 192.168.1.36 hinzufügen
- oder besser den Firefox verwenden.

3. Zugriff von außen auf Filr

Um alle Möglichkeiten der Zusammenarbeit durch die Schul-Cloud ausschöpfen zu können, sollte *Filr* jederzeit von außerhalb der Schule erreichbar sein. Dazu ist eine Konfiguration der Firewall notwendig.

Bitte beachten Sie bei den folgenden Abbildungen, dass die gezeigten nicht *Filr*-bezogenen Bilder nicht eins zu eins mit denen Ihrer *Sophos*-Firewall entsprechen müssen. Die Farben einzelner Gruppen könnten bei Ihnen also auch anders aussehen als hier gezeigt. Manche IP-Adressen sind aus datenschutzrechtlichen Gründen unkenntlich gemacht.

Je nach Ihrer Konfiguration entscheiden Sie sich für Kap. 3.1 oder Kap. 3.2, um den Zugriff von außen umzusetzen!

Wenn Sie die im Dokument *Zertifikate-Anleitung.pdf* beschriebene Apache-2-Erweiterung bzw. die *paedML Novell 4.5* betreiben, können Sie auch ohne eine Änderung der Firewall-Einstellungen auskommen. (Siehe Kap.3.3.)

Wenn Sie eine *Sophos* -Firewall als Software-Appliance benutzen, die als virtuelle Maschine unter ESXi läuft, stellen Sie bitte sicher, dass als Netzwerkkarten für diese Maschine die *Intel E1000* oder besser *VMXNET3* konfiguriert sind. Sie könnten sonst eventuell Performance-Probleme beim Zugriff von außen auf das interne Netz bekommen.

Überprüfen Sie die Netzwerkkonfiguration Ihrer virtuellen Maschine im *vSphere Client / Web-Client* (rechter Maus-Klick auf die virtuelle Maschine): *„Einstellungen bearbeiten“*, (in älteren Versionen Reiter *„Hardware“*), indem Sie auf die *„Netzwerkadapter“* der Maschine klicken. Sie bekommen einen *Adaptertyp* angezeigt. Wenn Sie hier *E1000* stehen haben, setzen Sie dort *VMXNET3* (dafür muss der Filr heruntergefahren sein).

Loggen Sie sich im Web-Interface der Sophos als *admin* ein. Richten Sie über *„Definitions & Users / Network Definitions“* eine Definition *„DMZ Filr“* für den *Filr* ein:

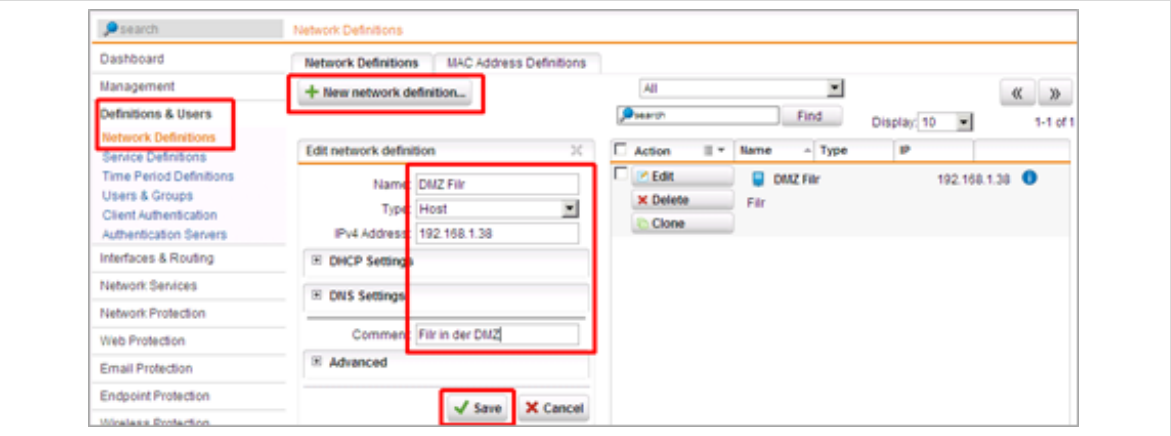


Abb. 28

3.1 Zugriff von außen bei gleicher IP Adresse

Wenn Sie die im Dokument *Zertifikate-Anleitung.pdf* beschriebene Apache-2-Erweiterung bzw. die *paedML Novell 4.5* betreiben, können Sie auch ohne eine Änderung der Firewall-Einstellungen auskommen. (Siehe Kap.3.3.)

Wenn Sie dem *Filr* keine eigene öffentliche Adresse vergeben (können), ist ein Zugriff von außen nur über eine Portweiterleitung über die *Sophos*-Firewall möglich. In Ihrer *Sophos*-Firewall ist die Portnummer 51443 für das Intranet bereits eingerichtet. Sie dient dem Zugriff auf den GServer03. Für

den externen Zugriff auf den KServer (*Vibe*) wurde von uns die Portnummer 52443 vorgeschlagen. Für *Filr* schlagen wir als Portnummer 53443 vor, also *https://öffentliche-IP-Adresse_der Astaro_oder_Domainname:53443*.

Eine Netzwerkdefinition für den *Filr* haben wir bereits weiter oben angelegt. Loggen Sie sich an Ihrer *Sophos* -Firewall als *admin* ein.

Für das HTTPS-Protokoll über den Port 52443 existiert schon eine Definition. Wählen Sie *Definitions & Users / Service Definitions*, klonen die Definition für HTTPS 52443 und modifizieren, wie folgt:

```
Name:                    HTTPS 53443
Type of Definition :     TCP
Destination port:        53443
Source port:        1:65535
Comment::           https alternativ fuer Filr
```

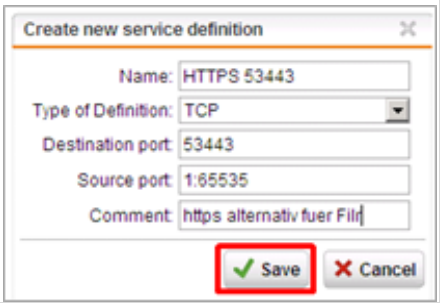


Abb. 29

Für den Zugriff von außen existiert schon eine Regel in der *Sophos* -Firewall. Diese Regel ist für den GServer03-(Port 52443) vorkonfiguriert. Diese Regel können Sie in der *Sophos* klonen und als Ziel *DMZ Filr* angeben. Wählen Sie *Network Protection/NAT/NAT* und modifizieren Sie die DNAT-Regel *ASG-52443* wie folgt:

```
Group:               ASG
Position:            <eine höher, als angezeigt>
Rule Type:           DNAT (Destination)
For traffic from:    Any    (oder Any over External)
Using service:       HTTPS 53443
Going to:            External (Address)
Change the destination to: DMZ Filr
And the service to:HTTPS
Comment:             ASG-53443-Filr IN
```

Abb. 30

Schalten Sie die Regel mit dem Schieberegler auf grün.

Abb. 31

Außer der DNAT-Regel müssen Sie zwei Firewall-Regeln einrichten, um den Zugriff von außen nach innen und umgekehrt zu erlauben. Gehen Sie über *Network Protection/Firewall*, klicken Sie auf *New rule* und legen Sie die zwei Regeln an, die Sie wie folgt konfigurieren:

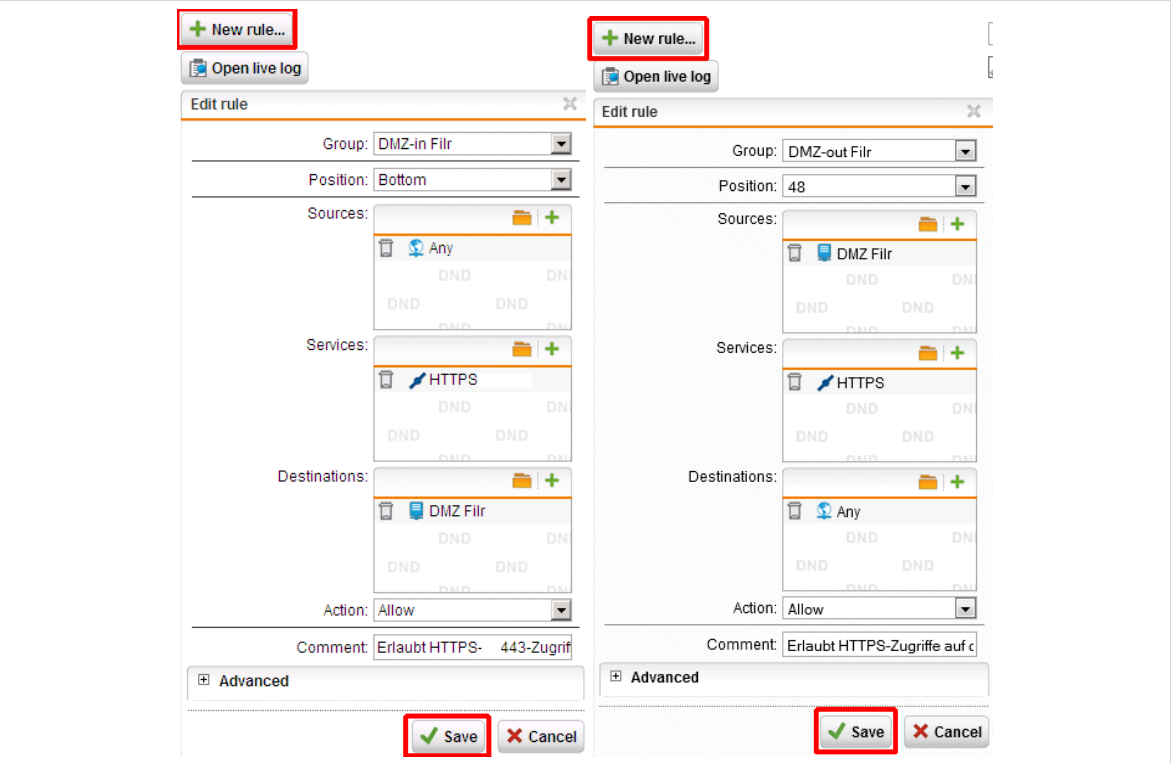


Abb. 32

Speichern Sie die modifizierten Regeln mit Klick auf *Save*. Sie erhalten dann zwei Regeln, die Sie noch jeweils aktiv schalten, indem Sie auf den Schieberegler klicken. Der „Schalter" springt dadurch auf Grün.

Abb. 33

Lassen Sie den Port 53443 bei Ihrem Provider freischalten.

An dieser Stelle verzichten wir darauf, einen Zugriff von außen für den *vaadmin* über Port 9443 zu beschreiben, weil wir der Ansicht sind, dass dieser Zugriff von außen nicht so wichtig ist und besser innerhalb der Schule (oder über eine Remote-Verbindung auf einen Administrationscomputer) erfolgen sollte. Wollen Sie dies trotzdem ermöglichen, so benötigen Sie, ähnlich wie oben beschrieben, eine HTTPS-9443-Definition und zusätzliche Regeln.

3.2 Zugriff von außen bei separater IP Adresse

Wenn Sie die im Dokument *Zertifikate-Anleitung.pdf* beschriebene Apache-2-Erweiterung bzw. die *paedML Novell 4.5* betreiben, können Sie auch ohne eine Änderung der Firewall-Einstellungen auskommen (siehe Kap. 3.3).

Provider stellen normalerweise mehrere offizielle IP-Adressen zur Verfügung. An der Belwü-typischen Subnetzmaske 255.255.255.248 (z.B.) erkennen Sie ein kleines Netz mit acht verfügbaren Adressen. Davon entfällt eine Adresse für das Netz selbst, eine für den Belwü-Router, eine für Broadcast und eine für den GServer03. In der Regel stehen dann noch vier Adressen zur Verfügung. Davon wählen Sie eine Adresse aus und bitten Belwü, dafür den DNS-Eintrag auf *filr.<Ihre Schuldomain>* mit dem freigeschalteten Port *443* zu setzen.

Starten Sie auf einem Browser mit *http://10.1.1.30:4444* die Verwaltungsoberfläche der *Sophos* und loggen Sie sich als *admin* ein.

Zunächst erweitern wir *eth1* mit der neuen IP-Adresse.

Unter *Interfaces & Routing/Interfaces/Additional Addresses /New Additional Address* klonen Sie *External [SRV]* und modifizieren Sie wie folgt:

```
Name:          Filr
On interface:External
IPv4 Address:<Ihre offizielle IP-Adresse
               für Filr>
Netmask:       /29 (255.255.255.248)
Comment:       x.IP mit DNAT auf Filr
               (x durch passende
                Ziffer ersetzen)
```

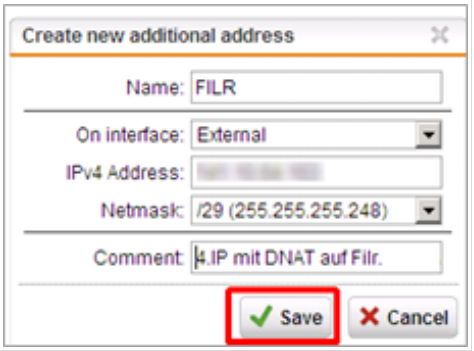


Abb. 34

Schalten Sie den neuen Eintrag mit dem Schieberegler aktiv.

Für den Zugriff von außen existiert schon eine Regel in der Sophos Firewall. Diese Regel ist für den Webserver vorkonfiguriert. Klonen Sie die Regel in der Sophos und geben Sie als Ziel *DMZ Filr* an. Wählen Sie *Network Protection/NAT/NAT* und modifizieren Sie die geklonte DNAT-Regel ASG-443 wie folgt:

```
Group:              ASG
Position:           <eine höher, als angezeigt>
Rule Type:          DNAT (Destination)
For traffic from:   Any (oder Any over External)
Using service:      HTTPS
Going to:           External [Filr](Address)
Change the destination to:DMZ Filr
And the service to:HTTPS
Comment:            ASG-443-Filr IN
```

Abb. 35

Schalten Sie den neuen Eintrag mit dem Schieberegler aktiv.

Abb. 36

Außer der DNAT-Regel müssen Sie zwei Firewall-Regeln einrichten, um den Zugriff von außen nach innen und umgekehrt zu erlauben. Gehen Sie über *Network Protection/Firewall*, klicken Sie auf *New rule* und legen Sie die zwei Regeln an, die Sie wie folgt konfigurieren:

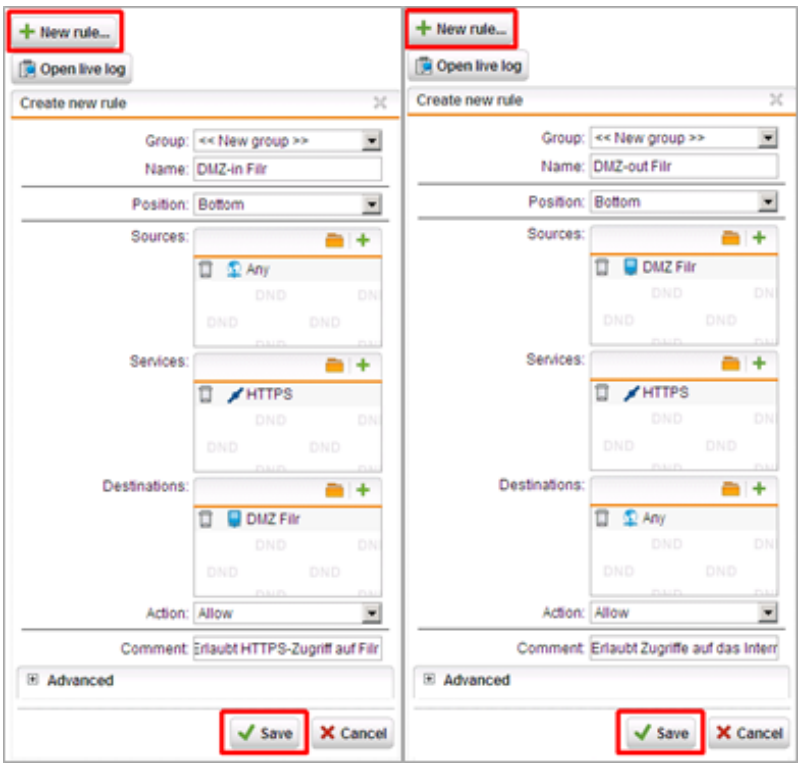


Abb. 37

Speichern Sie die modifizierten Regeln mit Klick auf *Save*. Sie erhalten dann zwei Regeln, die Sie noch jeweils aktiv schalten.

Abb. 38

An dieser Stelle verzichten wir darauf, einen Zugriff von außen für den *vaadmin* über Port 9443 zu beschreiben, weil wir der Ansicht sind, dass dieser Zugriff von außen nicht so wichtig ist und besser innerhalb der Schule (oder über eine Remote-Verbindung auf einen Administrationscomputer) erfolgen sollte. Wollen Sie dies trotzdem ermöglichen, so benötigen Sie HTTPS-9443-Definition und zusätzliche Regeln und eine Portfreischaltung bei Ihrem Provider (z.B. *Belwü*).

3.3 Aufruf von innen und außen über denselben Domain-Namen

Es wäre schön, wenn man mit derselben URL, die Ihre Schul-Domäne enthält, sowohl von innerhalb als auch von außerhalb der Schule auf *Filr* zugreifen könnte.

Wer *Filr* nicht nur über eine offizielle IP-Adresse, sondern per URL mit der eigenen Schuldomain ansprechen will, sollte sich bei seinem Provider, z.B. Belwü, einen DNS-Eintrag setzen lassen. Wir schlagen vor:

filr.<Ihre Schuldomain>

Beispiel: Angenommen, Ihre Schul-Domäne wäre *meineschule.de* und Sie würden gerne mit *http://filr.meineschule.de* von innen und von außen auf *Filr* zugreifen. Dann ist es notwendig, dass innerhalb der Schule entsprechende DNS-Einträge vorliegen. Dies ist relativ einfach zu erreichen, wenn Sie die DNS-Einstellungen vornehmen. Die Beschreibung folgt weiter unten.

Schwieriger ist der Zugriff von außen. Vielleicht haben Sie schon eine Zugriffsmöglichkeit auf Ihr Intranet per

http://server.meineschule.de/intranet/schulweb

oder *https://server.meineschule.de:51443/intranet/schulweb*

In diesem Fall haben Sie sich einen entsprechenden DNS-Eintrag bei Ihrem Provider (z.B. Belwü) setzen lassen. Wenn Sie keine Portnummer verwenden möchten, benötigen Sie mehrere offizielle IP-Adressen, was in der Regel bei Belwü möglich ist (siehe oben).

Wie Sie mit nur einer IP-Adresse auskommen können, finden Sie in der Beschreibung des Dokuments *Zertifikate-Anleitung.pdf*. Die *paedML Novell 4.5* hat die nötigen Einstellungen bereits.

An dieser Stelle fahren wir mit den internen GServer03-DNS-Einstellungen fort:

Wechseln Sie als *root* in das Verzeichnis */var/lib/named/master*.

Kopieren (!) Sie dort die Datei *oes.ml-bw.de* auf eine Datei im gleichen Verzeichnis, die Ihrem echten Domain-Namen entspricht, am obigen Beispiel also:

```
cp oes.ml-bw.de meineschule.de
```

Vielleicht existiert eine solche Datei bei Ihnen auch schon. In diesem Fall müssen Sie sie ggf. nur anpassen.

Editieren Sie die Datei *meineschule.de* jetzt mit einem Editor und fügen Sie die folgende Zeile ein:

```
filr                    IN A        192.168.1.38
```

Editieren Sie nun die Datei */etc/named.conf*. Fügen Sie dort (falls noch nicht vorhanden) hinter dem Abschnitt

```
zone "oes.ml-bw.de" in {
        file "master/oes.ml-bw.de";
        type master;
};
```

den folgenden Abschnitt ein:

```
zone " meineschule.de " in {
        file "master/meineschule.de ";
        type master;
};
```

Nun ersetzen Sie wieder `meineschule.de` durch Ihre echte Domain.

Speichern Sie ab und starten Sie den Nameserver neu mit `systemctl restart named.service`.

4. Vertrauenswürdiges Zertifikat für den Filr

In der Auslieferungsversion des *Filr* ist nur ein sogenanntes selbst signiertes Zertifikat enthalten. Dies hat bei Zugriffen über einen Browser den Nachteil, dass im Browser eine Warnung wegen eines nicht vertrauenswürdigen Zertifikats erscheint, das dann manuell akzeptiert werden muss.

Dies ist lästig und nicht im Sinne einer sicherheitsbewussten Handhabung des Internets.

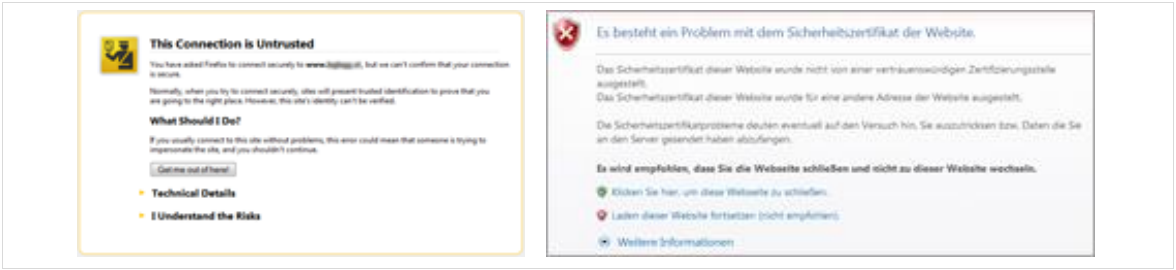


Abb. 39

Weiter oben wurde schon mehrfach das Dokument *Zertifikate-Anleitung.pdf* genannt. In diesem Dokument ist nicht nur die Verwendung einer einzigen IP-Adresse für alle *paedML Novell* Server beschrieben, sondern vor allem der Einsatz eines einzigen Wildcard-Zertifikats auf dem GServer03, der weitere Zertifikate für die anderen Server überflüssig macht.

Wenn Sie diese Technik einsetzen wollen, sollten Sie die *Zertifikate-Anleitung.pdf* durchführen. In der *paedML Novell 4.x* sind große Teile der dort beschriebenen Vorarbeiten bereits erledigt. Fahren Sie in diesem Fall hier im Dokument mit Kap.5 fort.

Falls Sie diese Methode nicht verwenden wollen, benötigen Sie ein Einzel-Zertifikat, dessen Einsatz wir im Folgenden beschreiben.

(Manche der folgenden Bilder stammen noch von älteren *Filr*-Versionen, gelten aber auch in *Filr 5*.)

In der *Filr*-VA-Konfiguration gibt es eine vergleichsweise einfache Möglichkeit, ein solches Zertifikat zu importieren. Hier beschreiben wir den Einsatz eines *Nicht-Wildcard-Zertifikats*, das recht günstig eingekauft werden kann, auch als z.B. 2-Jahreszertifikat. Eine ganze Reihe von Firmen und Organisationen bieten solche Zertifikate an; z.B. PSW, Verisign, CAcert, Trustico, Deutsche Post und viele mehr.

Loggen Sie sich über *https://<filr-ip-oder dns>:9443* als *vaadmin* ein und gehen Sie über *Appliance Configuration* mit einem Klick auf *Digital Certificates* in die Zertifikatsbearbeitung.

Wechseln Sie dort den *Key Store* auf *Web Application Certificates* und gehen dann über das *File*-Menü nach *New Certificate (Key Pair)*.

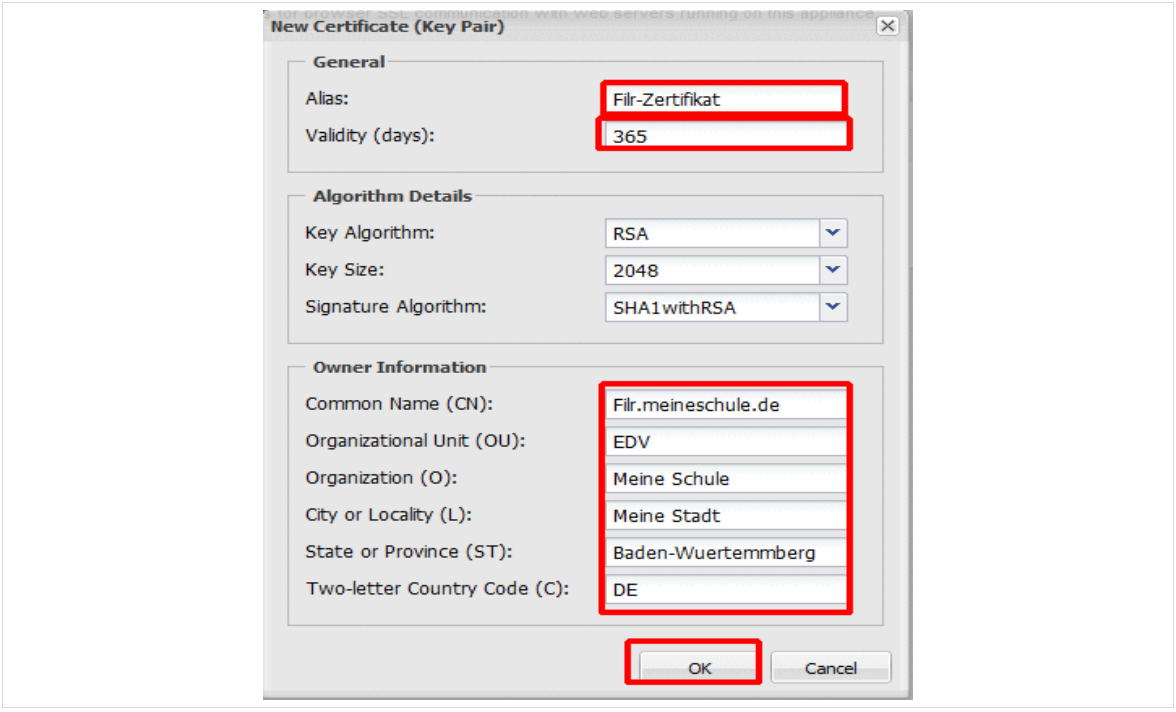


Abb. 40

Geben Sie Ihre *echten* Daten ein:

Nach Klick auf *OK* erscheint kurz ein Fortschrittsbalken (Restart-Fenster bestätigen) und das neue *Key Pair* wird angezeigt. (Das vorhandene *filrzertifikat* können Sie über *Edit* auch löschen.)

Markieren Sie *filr-zertifikat*

Abb. 41

und gehen Sie über das *File*-Menü zu *Certification Request* / *Generate CSR*:

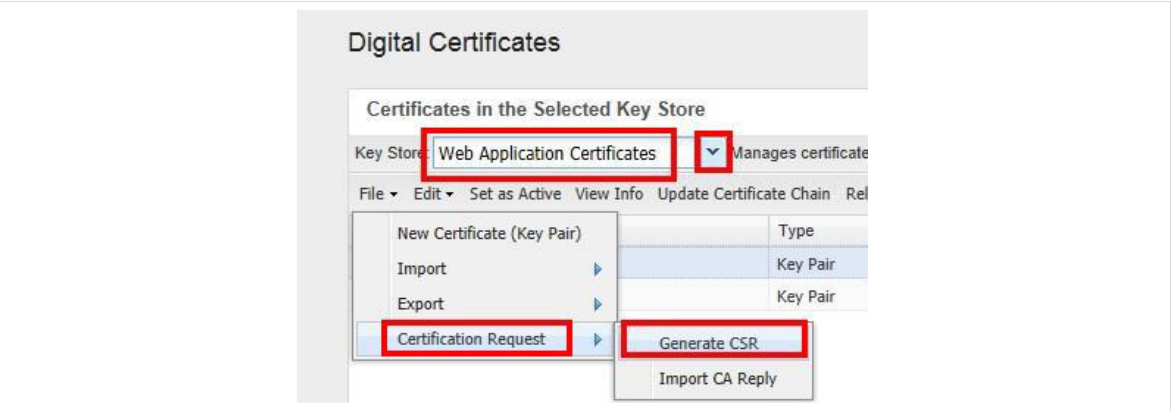


Abb. 42

Es erscheint dann, je nach Browser, ein Fenster zum Abspeichern oder die direkte Anzeige des CSRs im Browserfenster. Wählen Sie einen Speicherort, an dem Sie für das Online-Absenden an eine Zertifizierungsstelle leicht herankommen oder speichern Sie das CSR über *copy & paste* in eine Textdatei.

Je nach Anbieter für die vertrauenswürdigen Zertifikate geht es jetzt unterschiedlich weiter. Öffnen Sie mit einem Texteditor die Datei *filr-zertifikat.csr,* deren Inhalt etwa so aussieht:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICXzCCAUcCAQAwHDEaMBgGA1UEAwwRd3d3Lm15Y29tcGFueS5jb20wggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC7JM0y/LNjvVWQbwV7A7kb+R8fiuNa
rFFY0IErnZzzWRnQXTlX20rgNph2ekJGyUjmt9G8mT5GWoW9BOjGXd4lUiL9K/Pa
h6zXSMlf6QoOICM5lY3q6Dc5OmOL1/NWqYCVrMKtH3P7Oy0nTcqcY0bBC4akEIQG
yP9Yl4u90FTLPXp0ktmAFSEjYzRREPxkOB1nqbaFkRv23vsCykJ5CAqbugvCeZqL
ZEcVU/t66OQsvNQgHQS6LQ5gc6LpG6fgducfeMbbNO4qRnmizRiiCAjiVqEB45X1
fo/6iEhJfp9SVi4CCcOJ40aBg43beyqlJj5sXtl6tBowzpjTFBzs1dEXAgMBAAEw
DQYJKoZIhvcNAQEFBQADggEBADUfhQQlqtJur+/kpR5YYB/M9iirauugUyaidORt
M8Q505T5h8MDQGWFax8o9zaGYQjyOSd2aQC75HUExaBfFjanU6ZVuPDvSfmYowJz
gen6JtgeqWy5xsrenfd9LmRp6g7eMr5EkwziY0XqXBi18+9/0iWYrFjxbDpeQehU
Ns7gMkuAm9eVSuOYsa1Oja1mW6bZdz7xmdBQ5OZTSH1ig/EAl+HLfHZF1dDuDnNG
ZGTHxOrYXjLJMWRm//pdbtrE9ASstJJFAO/qP7bPpTWynJFZHoXxoxo8nzh1m6jW
ULM3YKho4P3PQJYu5SbbTFm7l8EUSq5DSFis5+5MW3aMEK4=
-----END CERTIFICATE REQUEST-----
```

Diese Datei muss nun an den Anbieter geschickt und ein Tomcat Zertifikat bestellt werden. Sie erhalten dann ein Paket mit verschiedenen Zertifikatsdateien und der Zertifikatskette (certificate chain) zurück. In der folgenden beispielhaften Beschreibung erfahren Sie, wie Sie jetzt im *Filr* fortfahren.

Die Auflistung der im Verzeichnis enthaltenen Dateien sieht etwa so aus:

```
certificate.crt
intermediate1.crt
intermediate2.crt
root.crt
```

Gehen Sie als *vaadmin* nun wieder zu den *Digital Certificates* und laden Sie über *File / Import / Trusted Certificate*...

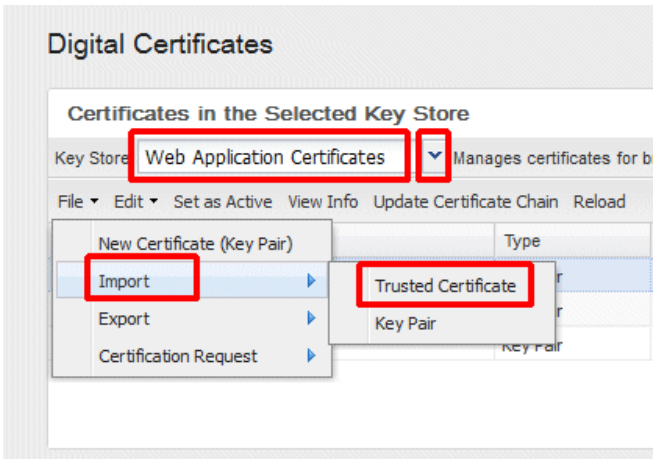


Abb. 43

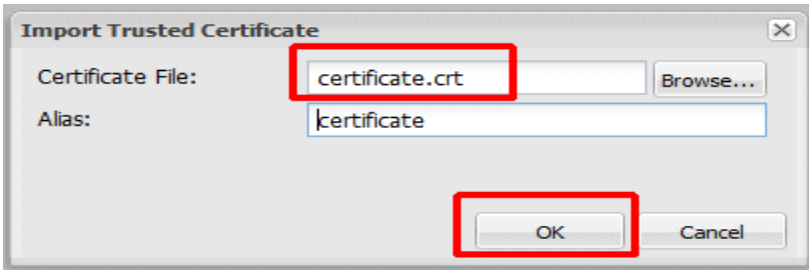


Abb. 44

… die Datei *certificate.crt* und ebenso die Dateien *intermediate1.crt*, *intermediate2.crt* und *root.crt*.

Markieren Sie anschließend das *filr-zertifikat* und setzen Sie es auf aktiv.

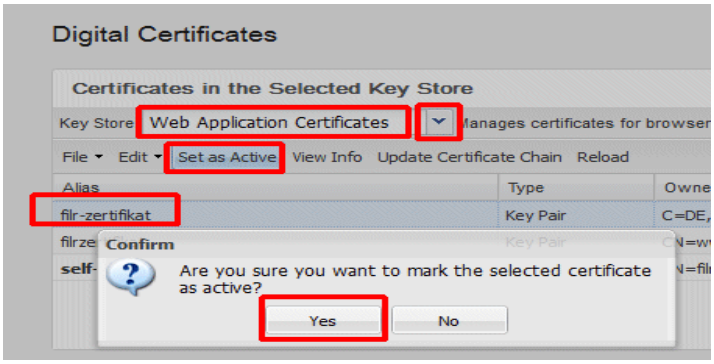


Abb. 45

Abb. 46

→ *Close*.

Der Neustart kann im *vaadmin* Home unter *Appliance Configuration* über den Button *Reboot* ausgeführt werden. Nach einiger Zeit müssen Sie sich dann natürlich wieder neu über *https://<filr-ip-oder dns>:9443* als *vaadmin* anmelden und zu *Appliance Configuration / Digital Certificates* gehen. Markieren Sie unter *Web Application Certificates* die Zeile mit *filr-zertifikat* und verbinden Sie dieses mit dem vertrauenswürdigen Zertifikat über das Menü *File / Certification Request / Import CA Reply*.

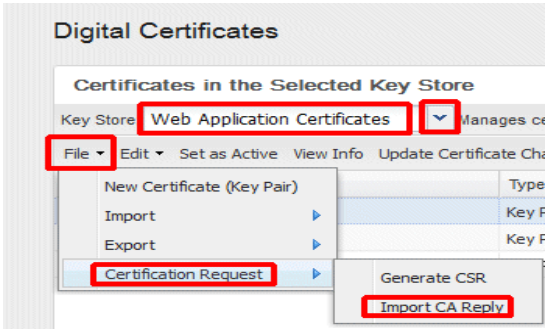


Abb. 47

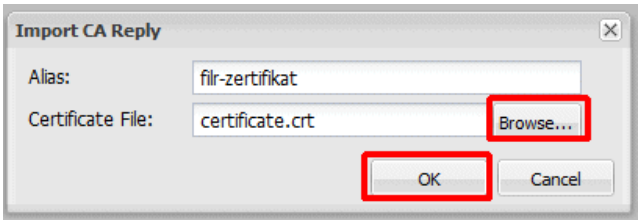


Abb. 48

Anschließend sehen Sie in der Spalte *Issuer,* dass das *filr-zertifikat* nun durch die CA beglaubigt ist.

(Sollte dies bei Ihnen nicht klappen, wiederholen Sie bitte den letzten Schritt noch einmal.)

Prüfen Sie nun mit einem Browser und dem normalen Aufruf des *Filr* mit *https://<filr-ip-oder dns>*, ob dem Zertifikat vertraut wird.

Dies wird möglicherweise nicht der Fall sein! Laut TID 7016002 ist dann folgendermaßen vorzugehen:

Markieren Sie *filr-zertifikat* und klicken dann auf den Menüpunkt *Update Certificate Chain*. Bestätigen Sie mit *Yes*:

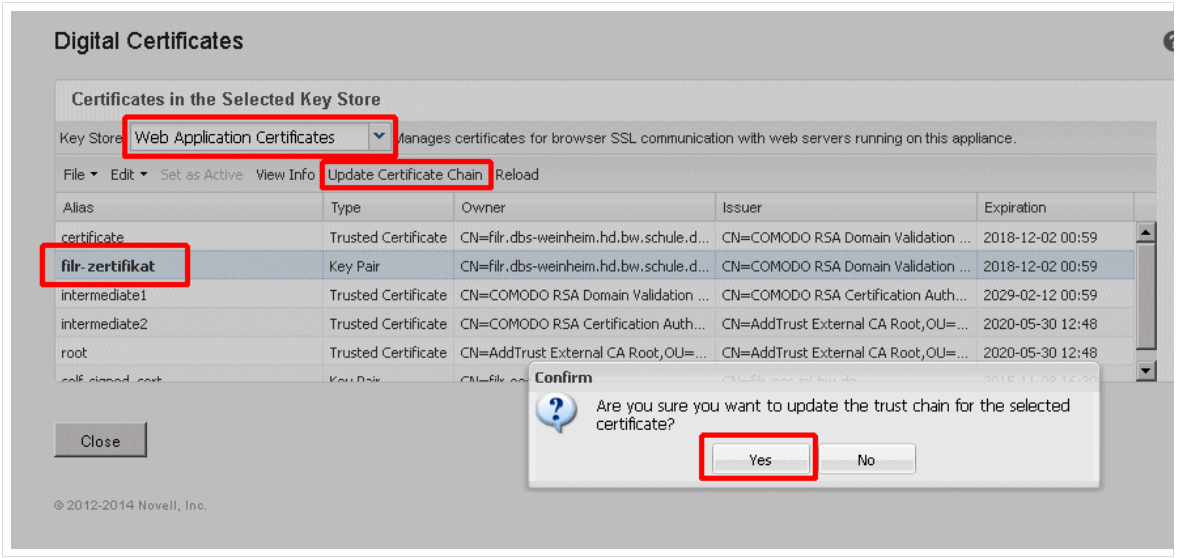


Abb. 49

Anschließend markieren Sie das Key Pair *self-signed-cert* und klicken auf den Menüpunkt *Set as Active* und bestätigen. Und direkt danach markieren Sie wieder unser *filr-zertifikat* und klicken erneut auf *Set as Active*. Starten Sie jetzt den *Filr* neu! Danach sollte der Aufruf des *Filr im Browser* ohne Bestätigung funktionieren.

5. Filr Desktop, Office-PlugIn

In der neuen Vollversion sind auch neue *Filr Desktop Apps* und das Office-PlugIn enthalten, in denen ebenfalls viele Fehler beseitigt wurden. Lesen Sie hierzu das Dokument *Installation-Filr-DesktopAPP-Office-Mobile.pdf*.

6. Schluss

Wir von der ZEN-Novell sind der Ansicht, dass der *Filr* ein ausgesprochen nützliches Werkzeug ist, mit dem weitere Cloud-Features auf sicherem Wege in die *paedML Novell* gebracht werden können. Im Vergleich zu *NetStorage* bietet *Filr* weitaus mehr Möglichkeiten und er erlaubt uns ein sehr komfortables Arbeiten mit Dateien im Schulnetz, von überall aus und mit den verschiedensten Geräten.

Weitergehende Informationen zur Anwendung des Filr finden Sie auf den Seiten der Lehrerfortbildung unter https://lehrerfortbildung-bw.de/st_digital/netz/muster/novell/filr.

Wir hoffen, dass Ihnen der *Filr* gefällt und wünschen Ihnen viel Erfolg damit.

Ihre ZEN-Novell.

Landesmedienzentrum Baden-Württemberg (LMZ)
Support Netz
Rotenbergstraße 111

70190 Stuttgart

paedML N

LMZ Landesmedienzentrum Baden-Württemberg