



Benutzerhandbuch

Dateidienste

Version: 1.3

Erstellt am: 17.06.08 17:06

Zuletzt geändert am: 13.08.08 11:15

Erstellt von: Christoph Biardzki

Zuletzt geändert von: Christoph Biardzki

Verzeichnisse

Inhaltsverzeichnis

Verzeichnisse	2
Inhaltsverzeichnis	2
Abbildungsverzeichnis	3
Tabellenverzeichnis	3
1 Einleitung und Übersicht	4
1.1 Übersicht	4
1.2 Begriffe	4
1.3 Support	6
1.4 Sprache	6
2 Zugangsvoraussetzungen	7
2.1.1 Nutzungsberechtigung	7
2.1.2 Benutzerkennung	7
2.1.3 Software	7
2.1.4 Netzwerkverbindung	7
2.2 Persönliche Dateiablage	8
2.3 Dateiablagen für Lehrstühle und Einrichtungen	8
2.3.1 Fakultäts-Speicherplatz	8
2.3.2 Dateiablagen innerhalb der Fakultätsbereiche	9
2.4 Temporäre Dateiablage	11
3 Zugang zum NAS-Filer mit unterschiedlichen Betriebssystemen	12
3.1 Windows	12
3.1.1 Windows-Rechner innerhalb der ads.mwn.de-Domäne	12
3.1.2 Andere Windows-Rechner (nicht in der ads.mwn-Domäne)	13
3.1.3 Trennen der Verbindung zur Dateiablage	14
3.1.4 Verbinden der Dateiablagen über die Kommandozeile	15
3.2 Linux	15
3.2.1 Einstellen von Zugriffsrechten	15
3.2.2 Zugriff mit KDE und GNOME	16
3.2.3 Weitere Informationsquellen	16
3.3 Mac OS X	17
3.4 Java-CIFS-Client jCIFS	18
4 Snapshots	19
4.1 Einführung	19

4.2 Zugriff auf Snapshots unter Windows.....21
4.3 Verwendung mit anderen Betriebssystemen22

Abbildungsverzeichnis

Abbildung 1 Gesamtüberblick 4
Abbildung 2 Ansicht der Dateiablagen im Windows-Explorer 9
Abbildung 3 Zugriff auf die Shares der Untereinheiten 10
Abbildung 4 Verbinden eines Netzlaufwerks unter Windows 12
Abbildung 5 Eingabe des Servernamens und der Freigabenamen 13
Abbildung 6 Fertig verbundene Dateiablage 13
Abbildung 7 Windows-Dialog für Benutzername und Kennwort 14
Abbildung 8 Trennen eines Netzlaufwerks..... 14
Abbildung 9 Mac OS X: Mit Server verbinden..... 17
Abbildung 10 Mac OS X: Eingabe des Server- und Freigabenamens 17
Abbildung 11 Mac OS X: Eingabe der Benutzerkennung und des Passworts 17
Abbildung 12 Verschiedene Szenarien bei Snapshots 20
Abbildung 13 Zugang zum „Eigenschaften“-Dialog eines Ordners oder einer Dateiablage..... 21
Abbildung 14 Liste verfügbarer Snapshots im „Eigenschaften“-Dialog 21
Abbildung 15 Liste von Snapshot-Untereinheiten im „~snapshot“-Verzeichnis 22
Abbildung 16 Mac OS X: Direkte Navigation zu einem Snapshot-Ordner 22

Tabellenverzeichnis

Tabelle 1 Begriffsdefinitionen 6
Tabelle 2 Fakultäten und Einrichtungen der TUM und ihre Projektshares 9
Tabelle 3 Zeitplan und Aufbewahrung von Snapshots 19

Versionen

- 1.0 initial
- 1.1 Anmerkungen K. Vellguth
- 1.2 Anmerkungen R. Freund, R. Borgeest, W. Baur
- 1.3 Ergänzungen/Korrekturen Linux-Anleitung H.Selzle, A.Volf

1 Einleitung und Übersicht

1.1 Übersicht

Das Leibniz-Rechenzentrum (LRZ) bietet allen Studierenden, Mitarbeitern und Gästen (im folgenden *Benutzern*) der TU München Speicherplatz für die Ablage von Dokumenten.

All diese verfügen über eine persönliche Dateiablage mit einer Kapazität von derzeit 3 GB in maximal 30.000 Dateien. Auf den persönlichen Bereich können nur die Eigentümer selbst zugreifen.

Fakultäten, Lehrstühle sowie andere Einrichtungen können darüber hinaus gemeinsame Dateiablagen einrichten. Hier sind größere Speicherkapazitäten möglich und die Zugriffsrechte können feingranular vergeben werden.

Schließlich existiert auch ein temporärer Bereich, der für einen schnellen und unkomplizierten Datenaustausch verwendet werden kann.

Das Speichersystem verwendet das CIFS-Protokoll und unterstützt die Betriebssysteme Windows, Linux/Unix sowie Mac OS X.

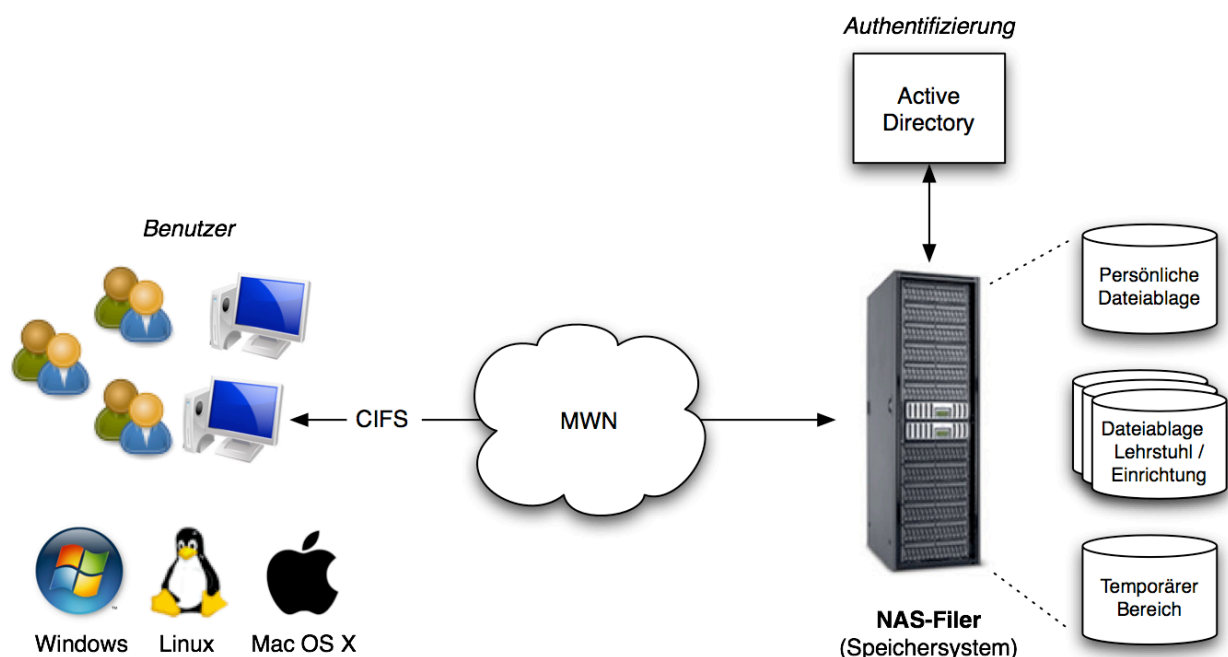


Abbildung 1 Gesamtüberblick

1.2 Begriffe

Begriff	Beschreibung
NAS-Filer (auch Filer)	Bezeichnung für das vom LRZ verwendete Speichersystem – NAS-Filer sind spezialisierte Fileserver mit einem integrierten Festplattensubsystem.
Active Directory (AD)	Ein auf Microsoft Windows basierender Authentifizierungs-
13.08.08 11:15	Version: 1.3
	4/22

Begriff	Beschreibung
	und Verzeichnisdienst. Im Kontext der Dateidienste handelt es sich um das MWN-weite ads.mwn.de -Directory, das automatisch mit allen Benutzerkennungen der TU München und in Zukunft auch der LMU sowie der Bayerischen Akademie der Wissenschaften und anderen Einrichtungen versorgt wird. Dadurch wird ein hochschulübergreifender Datenaustausch möglich.
MyTUM (Portal)	Das aktuelle Web-Portal der TU München: http://www.mytum.de
LRZ-Kennung	Eine 7-stellige, alphanumerische Benutzerkennung, die vom LRZ vergeben wird und lebenslang erhalten bleibt. Die eigene LRZ-Kennung können TUM-Benutzer im MyTUM-Portal unter „persönliche Einstellungen“ nachschauen. Für den Zugriff auf die Dateidienste können (derzeit) keine bestehenden Kennungen aus separat beantragten LRZ-Projekten verwendet werden: es ist stets die im MyTUM-Portal hinterlegte LRZ-Kennung nötig.
Service-Desk	Der TUM IT-Service-Desk (it-support@tum.de) ist Ansprechpartner für alle Anfragen bezüglich der Dateidienste.
Münchner Wissenschaftsnetz (MWN)	Das MWN bezeichnet das gesamte vom LRZ betriebene Netz an der TUM, der LMU sowie weiteren Hochschul- und Forschungseinrichtungen.
Virtual Private Network (VPN)	Ein VPN-Server am LRZ ermöglicht den Zugang zum MWN vom Internet aus, indem ein „Tunnel“ zwischen einem Rechner im Internet und dem MWN aufgebaut wird. Das VPN wird benötigt um auf die Dateidienste aus dem Internet heraus zuzugreifen. Auch für WLAN-Verbindungen kann eine VPN-Verbindung nötig sein. Weitere Informationen: http://www.lrz-muenchen.de/services/netz/mobil/vpn/
Common Internet File System (CIFS)	Ein verteiltes Dateisystem, das primär durch seine Verwendung in Fileservern für Windows bekannt geworden ist. Benutzer können aus ihren Anwendungen heraus Dateien auf einem Server direkt lesen und schreiben ohne sie beispielsweise (wie bei FTP) herunterladen zu müssen. CIFS unterstützt komplexe Berechtigungen und Attribute („ACLs“) sowie Sperren auf Dateien.
Share / CIFS-Share	Der Zugangspunkt zu einer Dateiablage, der eine bestimmte Dateiablage auf einem bestimmten Filer eindeutig bestimmt. Shares werden üblicherweise in der Schreibweise <code>\\filename\sharename</code> geschrieben. Besitzt ein Share ein Dollarzeichen („\$“) am Ende (z.B. <code>\\filename\share\$</code>), dann wird es beim Auflisten aller verfügbaren Shares nicht angezeigt, sondern bleibt „versteckt“.
Access Control List (ACL)	Mit dem Begriff „ACL“ werden die Zugriffsberechtigungen für eine Datei oder ein Verzeichnis bezeichnet. Eine ACL

Begriff	Beschreibung
	besteht aus mehreren Einträgen (daher „List“) von einzelnen Berechtigungen, beispielsweise „Benutzer A darf Lesen“, „Benutzer B darf Lesen und Schreiben“ und „Gruppe C darf Lesen“. Damit kann der Zugriff auf Daten feingranular gesteuert werden.
Access Based Enumeration (ABE)	Die ABE sorgt dafür, dass Benutzer nur die Dateien und Verzeichnisse sehen, die sie auch lesen oder anschauen dürfen. Andere Dateien und Verzeichnisse bleiben unsichtbar.
Quota	Bezeichnung für eine Beschränkung des verfügbaren Speicherplatzes oder der Anzahl der Dateien. Quotas sollen eine faire Aufteilung des Speicherplatzes sicherstellen.
Snapshot	(dt. „Schnappschuss“) Eine bequeme Art der Datensicherung, bei der in regelmäßigen Abständen (z.B. täglich) alle Daten „eingefroren“ und mehrere solche Schnappschüsse aufbewahrt werden. Benutzer können bei Bedarf gelöschte oder beschädigte Dateien selbst aus einem Snapshot zurückkopieren ohne einen Administrator fragen zu müssen.
Case-insensitiv	Bei Dateinamen unterscheiden Windows und Mac OS X nicht zwischen Groß- und Kleinschreibung: „Dokument.txt“ und „dokument.txt“ meinen die gleiche Datei, auch wenn die Schreibweise beibehalten wird. Linux und die meisten Unixe würden hier unterschiedliche Dateien sehen. Die Dateiablagen auf dem Filer sind case-insensitiv, unterscheiden also nicht zwischen Groß- und Kleinschreibung von Dateinamen.

Tabelle 1 Begriffsdefinitionen

1.3 Support

Bei Fragen und Problemen kann der IT-Service Desk der TU München kontaktiert werden.

E-Mail: it-support@tum.de

Telefon: 089-28917123

WWW: <http://portal.mytum.de/iuk/service/servicedesk/support/>

1.4 Sprache

In diesem Handbuch haben wir uns generell um geschlechtsneutrale Formulierungen bemüht. An Stellen, an denen aus Gründen besserer Lesbarkeit das generische Maskulinum zu finden ist, sind selbstverständlich stets Frauen und Männer gleichermaßen gemeint.

2 Zugangsvoraussetzungen

2.1.1 Nutzungsberechtigung

Die Dateiablagen können von allen Benutzern der TU München ohne weitere Kosten genutzt werden. Es gelten die Nutzungsbedingungen des Leibniz Rechenzentrums – insbesondere dürfen andere nicht gestört oder behindert werden.

2.1.2 Benutzerkennung

Alle Benutzer benötigen eine gültige LRZ-Kennung. LRZ-Kennungen sind 7-stellige Buchstaben-Zahlenkombinationen wie „ne23mek“. Die eigene LRZ-Kennung kann im MyTUM-Portal in den persönlichen Einstellungen abgerufen werden.

Das zugehörige Passwort ist das MyTUM-Passwort. Es kann über das MyTUM-Portal neu gesetzt werden.

2.1.3 Software

Die Dateiablagen arbeiten mit dem CIFS-Dateiprotokoll. Entsprechende Clientsoftware gehört zum Lieferumfang der meisten Betriebssysteme.

Offizieller Support besteht für folgende Betriebssysteme:

- Windows: ab Windows XP
- Mac OS X: ab Mac OS X 10.4
- Linux: Suse Linux Enterprise Desktop 10

Andere Versionen (z.B. Windows 2000, Mac OS X 10.3, andere Linux-Distributionen, andere Unixes wie Solaris) funktionieren ebenfalls, können aber nicht vollständig unterstützt werden.

2.1.4 Netzwerkverbindung

Das Speichersystem hat den Hostnamen **nas.ads.mwn.de**. Der interne Rechnername, der gelegentlich angezeigt wird, ist BADWLRZ-FNNAS – in der Regel ist das Alias „nas.ads.mwn.de“ einfacher zu merken.

Grundsätzlich ist der Zugang zum Speichersystem für alle Rechner innerhalb des Münchner Wissenschaftsnetzes (MWN) freigeschaltet. Im Einzelfall können lokale Firewalls der einzelnen Institute die CIFS-typischen Ports (Port 135, 137, 138, 139 und 445) blockieren. Hier müssen zuständige Administratoren gebeten werden, den Zugang freizuschalten.

Befindet sich ein Client-Rechner außerhalb des MWN, kann über eine LRZ-VPN-Verbindung auf das Speichersystem zugegriffen werden. Je nach Latenz und Bandbreite der verwendeten Anbindung kann die Geschwindigkeit jedoch stark reduziert sein (alternativ bietet sich hier die Webdisk an).

2.2 Persönliche Dateiablage

Das persönliche Verzeichnis ist über den Pfad `\\nas.ads.mwn.de\<Kennung>` erreichbar (z.B. `\\nas.ads.mwn.de\ne23mek`). Auf diesem Weg ist nur das eigene Verzeichnis sichtbar – persönliche Dateiablagen anderer Benutzer können nicht eingesehen werden.

Jeder Benutzer verfügt über ein persönliches Verzeichnis mit einer Kapazität von derzeit **3 GB** und einem Limit von **30000 Dateien**. Die verbleibende Speicherkapazität wird von der Client-Software angezeigt, für die Anzahl der Dateien gibt es derzeit keine Anzeige.

Es ist nicht vorgesehen, das Quota zu erhöhen – wenn Benutzer mehr Speicherplatz benötigen sollten sie ein Projektverzeichnis in ihrer Fakultät oder – für kurzfristigen Datenaustausch – das temporäre Verzeichnis nutzen.

Da andere Benutzer nicht auf die persönliche Dateiablage zugreifen können macht auch eine Rechtevergabe mit ACLs wenig Sinn (obwohl prinzipiell möglich).

In der persönlichen Dateiablage stehen Snapshots als Datensicherung zur Verfügung. Damit können Benutzer auf mehrere ältere Dateisystem-Zustände zurückgreifen, die bis zu vier Wochen zurückliegen.

2.3 Dateiablagen für Lehrstühle und Einrichtungen

Für die Zusammenarbeit und den Datenaustausch mit anderen Benutzern stehen dedizierte Dateiablagen bereit. Diese Dateiablagen sind anhand der Organisationsstruktur aufgebaut.

2.3.1 Fakultäts-Speicherplatz

Fakultäten, zentrale Einrichtungen sowie die Bibliothek der TUM verfügen jeweils über einen eigenen Ablagebereich (Tabelle 2). Jedem Ablagebereich ist ein CIFS-Share zugeordnet.

Die Größe des Ablagebereiches ist pro Fakultät limitiert: der Anteil einer jeden Fakultät wird anhand des WAP-Schlüssels als Prozentanteil des gesamten Speicherplatzes bestimmt.

Einrichtung/Fakultät	Kürzel	Share
Zentrum Mathematik	MA	\\nas.ads.mwn.de\tuma
Physik Department	PH	\\nas.ads.mwn.de\tuph
Fakultät für Chemie	CH	\\nas.ads.mwn.de\tuch
Fakultät für Wirtschaftswissenschaften	WI	\\nas.ads.mwn.de\tuwi
Fakultät für Bauingenieur- und Vermessungswesen	BV	\\nas.ads.mwn.de\tubv
Fakultät für Architektur	AR	\\nas.ads.mwn.de\tuar
Fakultät für Maschinenwesen	MW	\\nas.ads.mwn.de\tumw
Fakultät für Elektrotechnik und Informationstechnik	EI	\\nas.ads.mwn.de\tuei
Fakultät für Informatik	IN	\\nas.ads.mwn.de\tuin
Wissenschaftszentrum Weihenstephan	WZ	\\nas.ads.mwn.de\tuwz
Fakultät für Medizin	ME	\\nas.ads.mwn.de\tume

Einrichtung/Fakultät	Kürzel	Share
Fakultät für Sportwissenschaft	SP	\\nas.ads.mwn.de\tusp
Zentrale Verwaltung	ZV	\\nas.ads.mwn.de\tuzv
Zentrale Einrichtungen	ZE	\\nas.ads.mwn.de\tuze
Bibliothek	UB	\\nas.ads.mwn.de\tuub

Tabelle 2 Fakultäten und Einrichtungen der TUM und ihre Projektshares

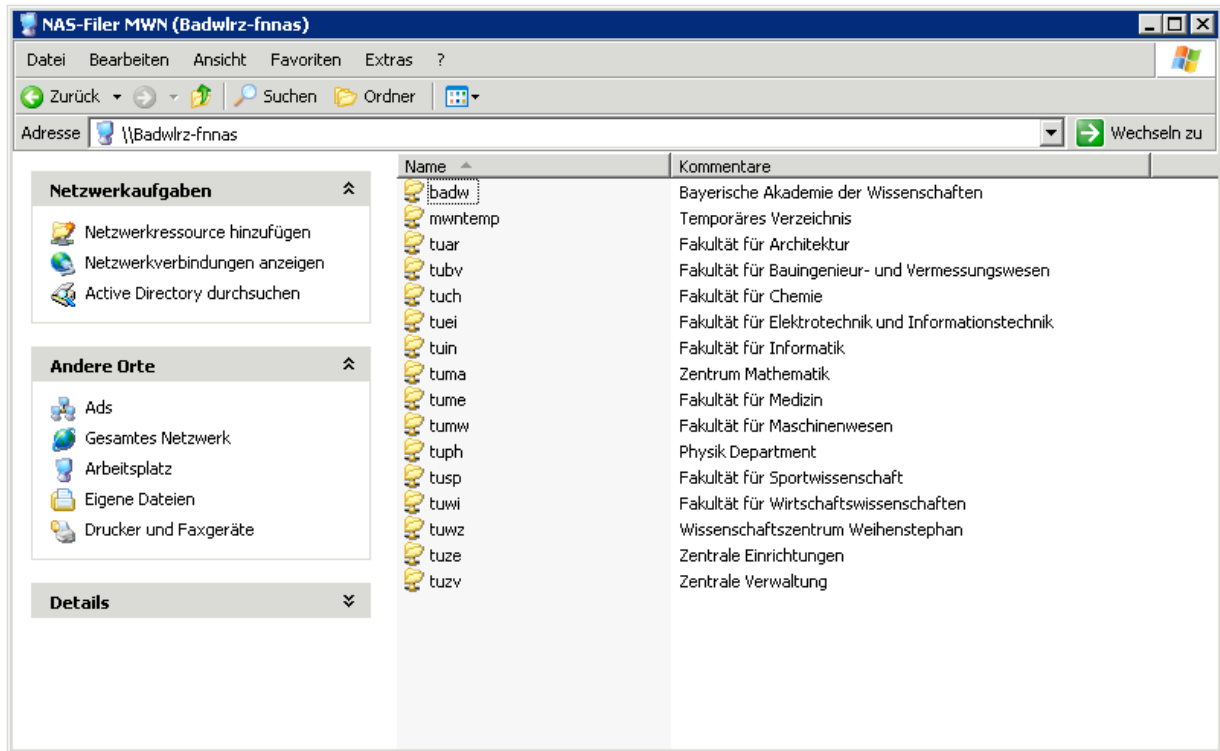


Abbildung 2 Ansicht der Dateiablagen im Windows-Explorer

2.3.2 Dateiablagen innerhalb der Fakultätsbereiche

Um den Speicherplatz einer Fakultät weiter zu unterteilen können für Lehrstühle, Abteilungen oder spezielle Projekte weitere Dateiablagen eingerichtet werden. Diese Entscheidung obliegt dem Information Officer (IO) der Fakultät. Die entsprechenden Dateiablagen werden mit dreistelligen Kürzeln versehen und enthalten ein eigenes Quota sowie einen eigenen CIFS-Share.

Das Standard-Quota für Dateiablagen auf Lehrstuhlebene beträgt 50 GB, kann aber geändert werden. Es wird nur der benutzte Speicherplatz vom Fakultätsspeicherplatz abgezogen, d.h. es kann theoretisch mehr Speicherplatz zugeteilt werden als vorhanden ist – unter der Annahme, dass nicht alles belegt wird („Thin provisioning“).

Beispiel:

Die zentrale Verwaltung (ZV) der TUM hat eine Untereinheit „Zentrale Abteilung 7 – EDV“. Diese erhält das Kürzel „ZA7“ und damit einen eigenen Share „TUZVZA7\$“. Auch kann der innerhalb dieses Bereiches verfügbare Speicherplatz limitiert werden.

Die Dateiablagen innerhalb der Fakultätsbereiche können auf zwei Arten erreicht werden:

- über den Share der Fakultät (\\nas.ads.mwn.de\tuzv in dem Beispiel): hier ist dann „za7“ als Ordner sichtbar
- über den Share der Untereinheit (\\nas.ads.mwn.de\tuzvza7\$)

Abbildung 3 zeigt beide Möglichkeiten in der Ansicht eines Windows-Clients.

Der Sinn der zusätzlichen Shares ist folgender: wenn der Unterbereich ein eigenes Quota bekommt, wäre über den Fakultätsshare nicht sichtbar, wie viel Platz in dem Unterbereich verfügbar ist (CIFS zeigt den Speicherplatz pro Share an). Nutzt man den Share der Untereinheit, dann sind eventuelle Limitierungen zu erkennen. Durch das „\$“-Zeichen am Ende ist der Share der Untereinheit beim Durchsuchen des NAS-Filers nicht sichtbar, so dass die Darstellung übersichtlich bleibt.

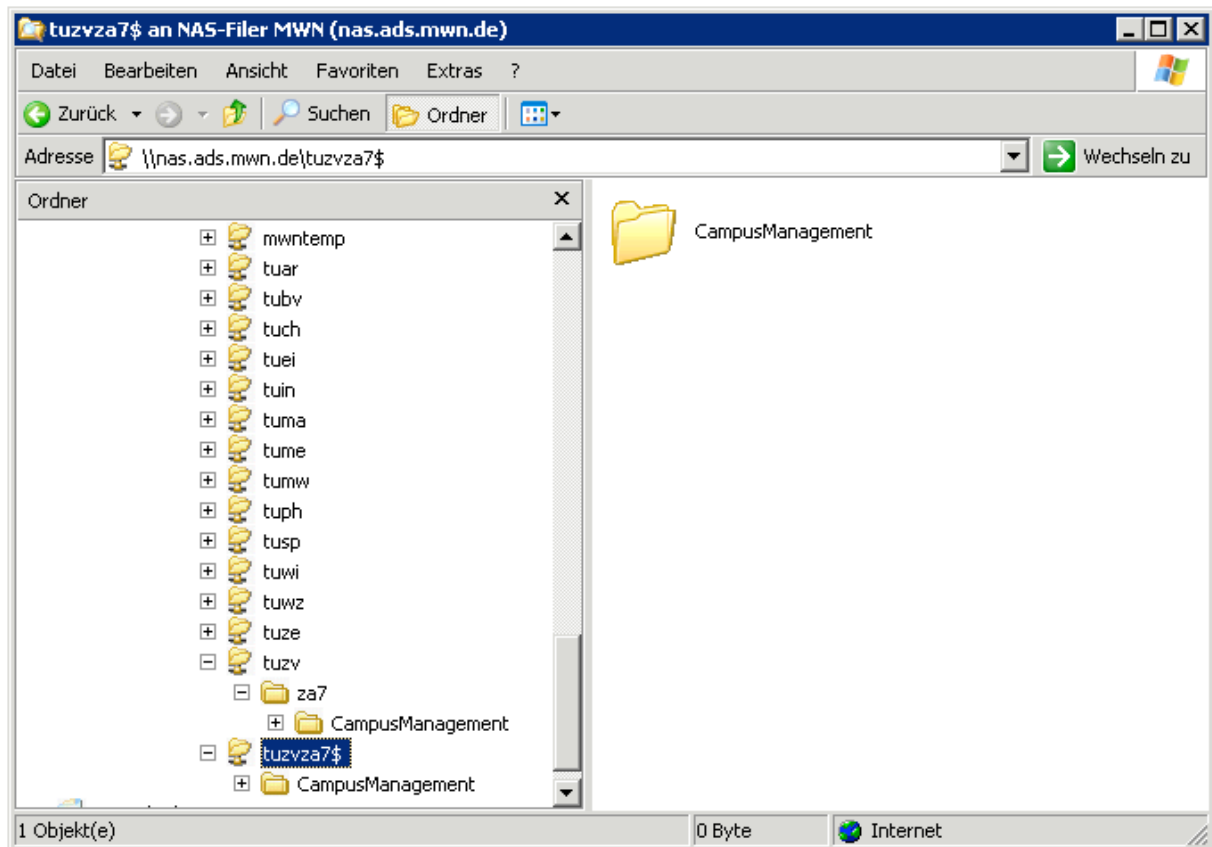


Abbildung 3 Zugriff auf die Shares der Untereinheiten

2.4 Temporäre Dateiablage

Die temporäre Dateiablage hat den Share-Namen [\\nas.ads.mwn.de/mwntemp](https://nas.ads.mwn.de/mwntemp)

Alle Benutzer können jeweils bis zu 5 GB oder 20.000 Dateien in der temporären Dateiablage speichern und beliebig Zugriffsrechte vergeben. Damit können sehr einfach Dokumente ausgetauscht werden ohne einen Projektordner zu benutzen.

Der Inhalt der temporären Ablage wird nach 48 Stunden automatisch gelöscht, so dass hier keine längerfristig benötigten Datei abgelegt werden sollten.

Im Gegensatz zu den anderen Ablagebereichen werden nur die letzten 24h in Snapshots gesichert (6 Snapshots alle 4 Stunden).

3 Zugang zum NAS-Filer mit unterschiedlichen Betriebssystemen

3.1 Windows

Der NAS-Filer unterstützt alle offiziell freigegebenen Windows-Versionen ab Windows XP. Während Windows 2000 und sogar Windows NT sowie Windows 95 ebenfalls funktionieren sollten werden sie vom LRZ nicht mehr unterstützt.

Die Anbindung der Dateiablagen unter Windows hängt davon ab, ob der verwendete Rechner Mitglied der Active Directory-Domäne ads.mwn.de ist.

3.1.1 Windows-Rechner innerhalb der ads.mwn.de-Domäne

Um sich mit einer Dateiablage zu verbinden wählt man aus dem „Extras“-Menü des Windows-Explorers die Option „Netzlaufwerk verbinden...“ (Abb). Im darauffolgenden Dialog (Abb) erscheint eine Liste der noch freien Laufwerksbuchstaben sowie ein Eingabefeld für den „Ordner“. In dieses Eingabefeld muss der Share eingetragen werden, beispielsweise [\\nas.ads.mwn.de\mwntemp](https://nas.ads.mwn.de/mwntemp) für die temporäre Dateiablage oder [\\nas.ads.mwn.de/<kennung>](https://nas.ads.mwn.de/<kennung>) für die persönliche Dateiablage.

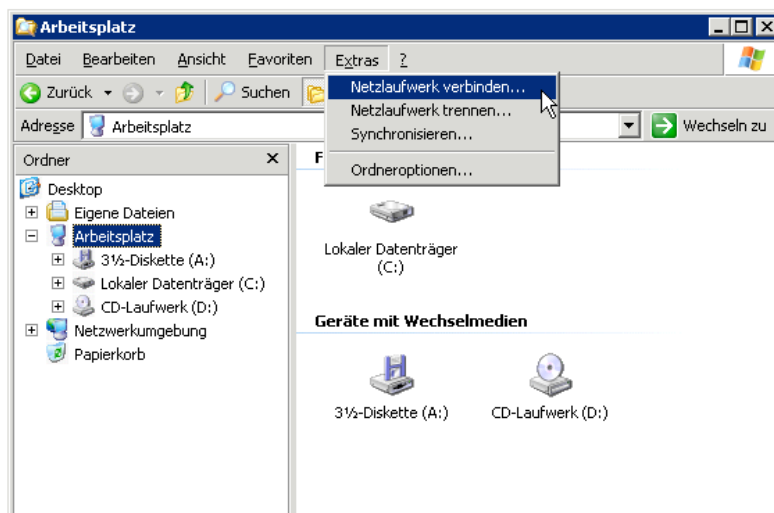


Abbildung 4 Verbinden eines Netzlaufwerks unter Windows

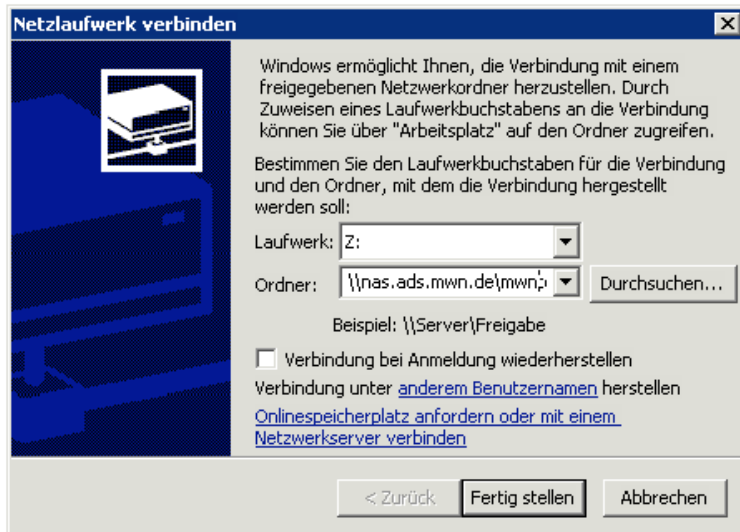


Abbildung 5 Eingabe des Servernamens und der Freigabenamen

Da der Rechner Mitglied der Windows-Domäne ist muss kein Passwort angegeben werden – der Rechner wird den Anmeldenamen sowie die automatisch bereitgestellten Kerberos-Tickets des angemeldeten Benutzers verwenden, um sich mit der Dateiablage zu verbinden und zu authentifizieren.

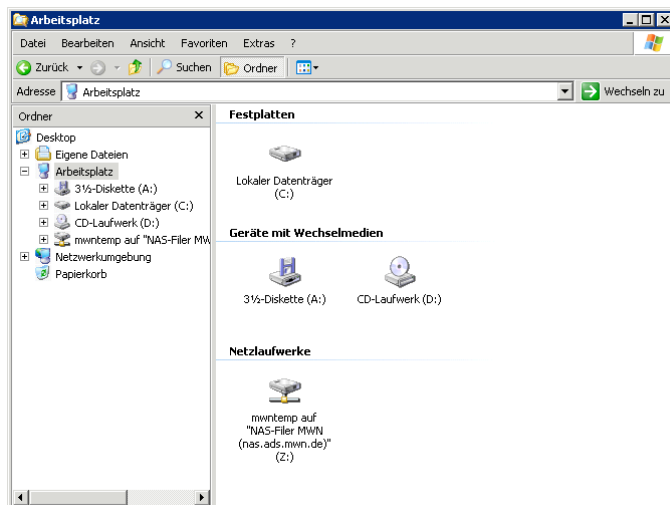


Abbildung 6 Fertig verbundene Dateiablage

3.1.2 Andere Windows-Rechner (nicht in der ads.mwn-Domäne)

Falls ein Windows-Rechner kein Mitglied der Domäne ist muss – zusätzlich zu den oben beschriebenen Schritten – eine Benutzerkennung sowie ein Passwort angegeben werden. Der entsprechende Dialog erscheint automatisch nach dem Anklicken des „Fertig stellen“-Buttons.

Der Benutzername sollte als „ADS\<<Kennung>“ also etwa ADS\ne23mek eingegeben werden. Alternativ kann auch ne23mek@mytum.de verwendet werden – diese Möglichkeit wird jedoch bei Problemen vom Support nicht unterstützt.



Abbildung 7 Windows-Dialog für Benutzername und Kennwort

Das Kennwort entspricht dem MyTUM-Portal-Kennwort.

Auf Wunsch kann das Kennwort auf dem Rechner gespeichert werden, so dass die Verbindung zur Dateiablage automatisch wiederhergestellt werden kann. Diese Möglichkeit sollte man nur auf eigenen Rechnern verwenden.

3.1.3 Trennen der Verbindung zur Dateiablage

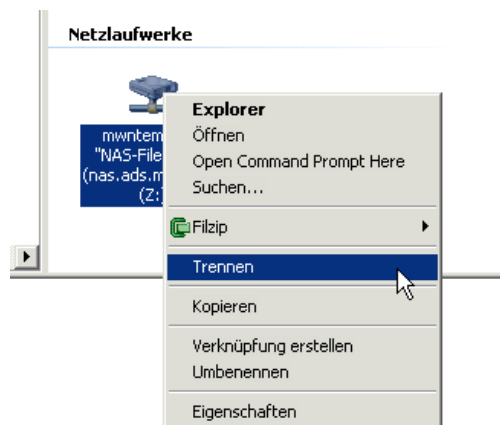


Abbildung 8 Trennen eines Netzlaufwerks

3.1.4 Verbinden der Dateiablagen über die Kommandozeile

Mit Hilfe des **net use** - Kommandozeilenbefehls können die oben beschriebenen Schritte auch in einer Stapelverarbeitungsdatei (auch Batch-Datei genannt) ausgeführt werden.

Beispiel:

```
net use x: \\nas.ads.mwn.de\wintemp
```

Der Benutzername sollte wieder als „ADS\<<Kennung>“ eingegeben werden.

Die genaue Syntax kann mit **net help use** abgerufen werden.

3.2 Linux

Neuere Linux-Kernel der 2.6er Serie verfügen über ein CIFS-Dateisystemmodul. Damit können die Dateiablagen wie folgt gemountet werden:

```
mount -t cifs //nas.ads.mwn.de/<sharename> /mnt/pfad -o username=<lrz-  
kennung>,domain=ADS
```

Beispiel:

```
mount -t cifs //nas.ads.mwn.de/ne23mek /mnt/pfad -o username=ne23mek,domain=ADS
```

Das Passwort muss bei dieser Variante an der Kommandozeile eingegeben werden. Alternativ kann das Passwort auch über eine Umgebungsvariable, aus einer Datei oder einer Pipe heraus gelesen werden (siehe manpage zu mount.cifs).

Wird das mount.cifs und umount.cifs suid-Root gesetzt, können auch Endbenutzer ihre CIFS-Shares selbst mounten. Damit ist es möglich einen automatischen CIFS-Mount der Dateiablagen beim Anmelden an das System umzusetzen. Leider kann die persönliche Dateiablage nicht als Homeverzeichnis unter Linux verwendet werden, da CIFS beispielsweise nicht zwischen Gross- und Kleinschreibung unterscheidet (Linux schon) und keine Softlinks unterstützt werden. Allerdings können übliche Dokumente wie PDF- oder Office-Dateien problemlos gelesen und beschrieben werden.

Als alternative Authentifizierungsmethode bieten Kernel ab 2.6.25 experimentell auch Kerberos an – in diesem Fall kann mit einem gültigen Ticket ohne Passworteingabe auf den Filer zugegriffen werden.

3.2.1 Einstellen von Zugriffsrechten

Die von Linux angezeigten Zugriffsrechte (etwa bei einem ‚ls‘) eines CIFS-Shares sind praktisch bedeutungslos, da die Zugriffskontrolle die ACLs bereits auf dem Server prüft. Das bedeutet konkret, dass jeder Benutzer seine eigene Verbindung unter seiner eigenen Kennung zu einem Share besitzt (und nicht – wie z.B. bei NFS – ein Mountpunkt gemeinsam genutzt wird).

Das Auslesen und Setzen von ACLs unter Linux ist möglich, allerdings recht umständlich. Für diesen Zweck kann das `setcacs` Programm benutzt werden (man `setcacs`). Um `setcacs` zu verwenden ist es übrigens *nicht* notwendig eine Dateifreigabe zu mounten.

3.2.2 Zugriff mit KDE und GNOME

Die beiden beliebten Desktop-Systeme für Linux können die Dateiablagen direkt öffnen.

3.2.2.1 KDE – Konqueror

Um im Konqueror auf die Dateiablagen zuzugreifen muss folgendes in die Adresszeile eingegeben werden:

```
smb://nas.ads.mwn.de/<sharename>
```

Beispiel:

```
smb://nas.ads.mwn.de/ne23mek
```

Nachdem ein Authentifizierungsdialog angezeigt wurde, wird der Benutzername als `ADS\<lrz-kennung>` (z.B. `ADS\ne23mek`) und das MyTUM-Kennwort eingegeben.

3.2.2.2 GNOME und Nautilus

Im Nautilus wird die URL ganz analog angegeben:

```
smb://nas.ads.mwn.de/<sharename>
```

Beispiel:

```
smb://nas.ads.mwn.de/ne23mek
```

Der Nautilus-Logindialog hat drei Felder: in *Benutzername* wird die LRZ-Kennung eingetragen, unter *Domäne* `ADS` und bei *Kennwort* das MyTUM-Kennwort.

3.2.3 Weitere Informationsquellen

- Manpage zu `mount.cifs` und `smbcacs`
- `/usr/src/linux/Documentations/fs/cifs.txt`
- `/usr/src/linux/fs/cifs/CHANGES`
- <http://pserver.samba.org/samba/ftp/cifs-cvs/linux-cifs-client-guide.pdf>

3.3 Mac OS X

Bei Mac OS X kann im Finder die Funktion „Mit Server verbinden...“ (Abbildung 9) aufgerufen werden. Im nachfolgenden Dialog wird die NAS-Filer-Adresse mit einem smb://-Präfix angegeben (siehe Abbildung 10). Schließlich müssen Benutzername und das Kennwort eingegeben werden (Abbildung 11).

Das Passwort kann optional im Mac OS X Schlüsselbund gespeichert werden.

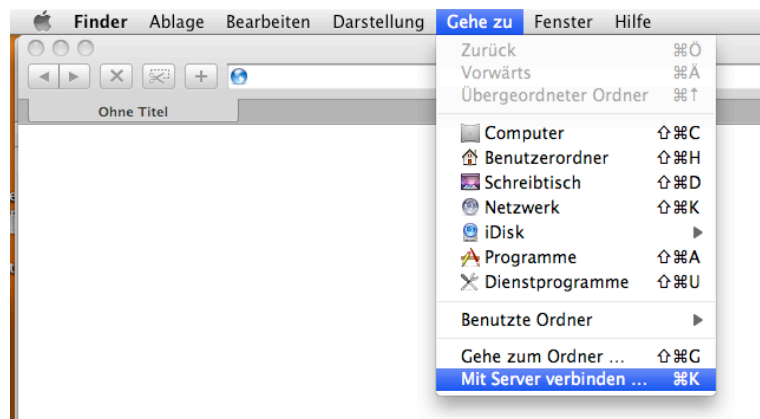


Abbildung 9 Mac OS X: Mit Server verbinden

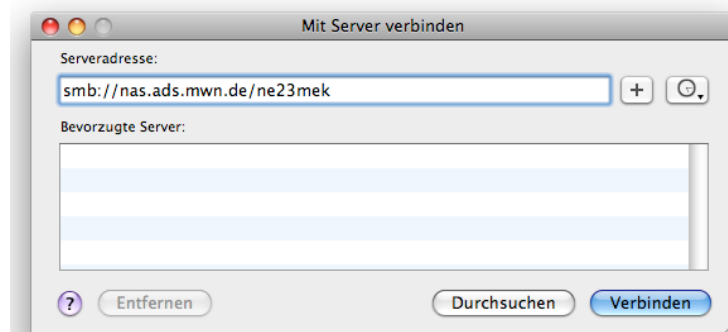


Abbildung 10 Mac OS X: Eingabe des Server- und Freigabensnamens



Abbildung 11 Mac OS X: Eingabe der Benutzererkennung und des Passworts

Mac OS X kann auch Links über CIFS erstellen (diese sind dann jedoch auch nur unter Mac OS X lesbar). Weiterhin unterscheiden Mac-Dateisysteme normalerweise nicht zwischen Groß- und Kleinschreibung, so dass ein weitestgehend transparenter Zugriff auf die Dateiablagen möglich wird.

3.4 Java-CIFS-Client jCIFS

Eine weiterführende Möglichkeit, die Dateiablagen in eigene Anwendungen zu integrieren ist jCIFS, eine Java-Bibliothek, die eine Verbindung zu CIFS-Servern aufbauen kann und einen direkten Zugriff auf die gespeicherten Daten ermöglicht. Damit können recht einfach Anwendungen im Bereich des Dokumentenmanagements erstellt werden. jCIFS benötigt keine gemounteten CIFS-Shares, sondern kommuniziert direkt mit dem Dateiserver.

Kernstück der Bibliothek ist die Klasse `jcifs.smb.SmbFile`, eine Erweiterung von `java.net.URLConnection`. Damit können zum Beispiel Dateien und Verzeichnisse erstellt, geschrieben und gelesen werden.

Weitere Informationen: <http://jcifs.samba.org>

4 Snapshots

Snapshots bieten eine einfache Möglichkeit versehentlich beschädigte oder gelöschte Dateien wiederherzustellen. Jeder Benutzer kann selbst ältere Versionen finden und restaurieren ohne Administratoren fragen zu müssen.

4.1 Einführung

Wie funktionieren Snapshots? Das Speichersystem macht automatisch und regelmäßig Schnapsschüsse („Snapshots“) von allen Dateiablagen. Jeder Snapshot beinhaltet alle Dateien und Verzeichnisse, die in der Dateiablage zum Zeitpunkt der Erstellung vorhanden waren.

Snapshots sind nicht beschreibbar und können nur gelesen werden. Ältere Versionen von Dateien werden nicht auf die Quotas angerechnet.

Es wird stets eine feste Anzahl an Snapshots aufbewahrt: wenn ein neuer Snapshot erstellt wird, löscht der Filer automatisch den ältesten Snapshot des gleichen Typs und rotiert die Nummerierung aller anderen Snapshots. Es gibt drei verschiedene Typen von Snapshots, die alle in Tabelle 3 zusammengefasst sind.

Snapshot-Typ	Zeitplan für die Erstellung und Aufbewahrung
hourly	Alle 4 Stunden um 8, 12, 16 und 20 Uhr Es werden die letzten 14 Snapshots aufbewahrt hourly.0 ist immer der neueste, hourly.13 der älteste Snapshot
daily	Täglich um Mitternacht Es werden die letzten 14 Snapshots aufbewahrt daily.0 ist der neueste („heute um Mitternacht“), daily.13 der älteste Snapshot
weekly	Jede Woche Sonntags um Mitternacht Es werden die letzten 5 Snapshots aufbewahrt weekly.0 ist der neueste („letzten Sonntag um Mitternacht“), weekly.4 der insgesamt älteste Snapshot

Tabelle 3 Zeitplan und Aufbewahrung von Snapshots

Die Wiederherstellung von Daten aus einem Snapshot ist einfach: Die alte Version muss einfach in das aktuelle Verzeichnis kopiert werden. Es ist wichtig daran zu denken, dass eine Datei zum Zeitpunkt der Erstellung in der Dateiablage vorhanden gewesen sein muss, damit sie im Snapshot erhalten bleibt.

Abbildung 12 zeigt unterschiedliche Szenarien, wie Dateien in Snapshots aufbewahrt werden. Der Einfachheit halber werden nur daily-Snapshots angezeigt.

Datei A wurde „vorgestern“ erstellt und zum ersten Mal im Snapshot „daily.1“ festgehalten. Genauso ist es mit Datei B, wobei diese „gestern“ – also zwischen daily.1 und daily.0, gelöscht worden ist. Sie kann jedoch aus dem Snapshot „daily.1“ wiedergeholt werden.

Datei C wurde zwischen den Snapshots daily.1 und daily.0 erstellt und gleich wieder gelöscht. Damit ist sie in keinem der Snapshots vorhanden und kann damit auch nicht mehr

wiederhergestellt werden (in der Realität würde sie vermutlich in einem der alle 4h erstellten „hourly“ Snapshots erhalten bleiben).

Datei D wurde mehrfach editiert und gespeichert. Damit enthält der Snapshot „daily.2“ den Stand von „Gespeichert 0“, daily.1 den von „Gespeichert 1“ aber daily.0 nur den von „Gespeichert 3“. Diese drei Versionen könnten also zurückgeholt werden.

Erstellte Snapshots

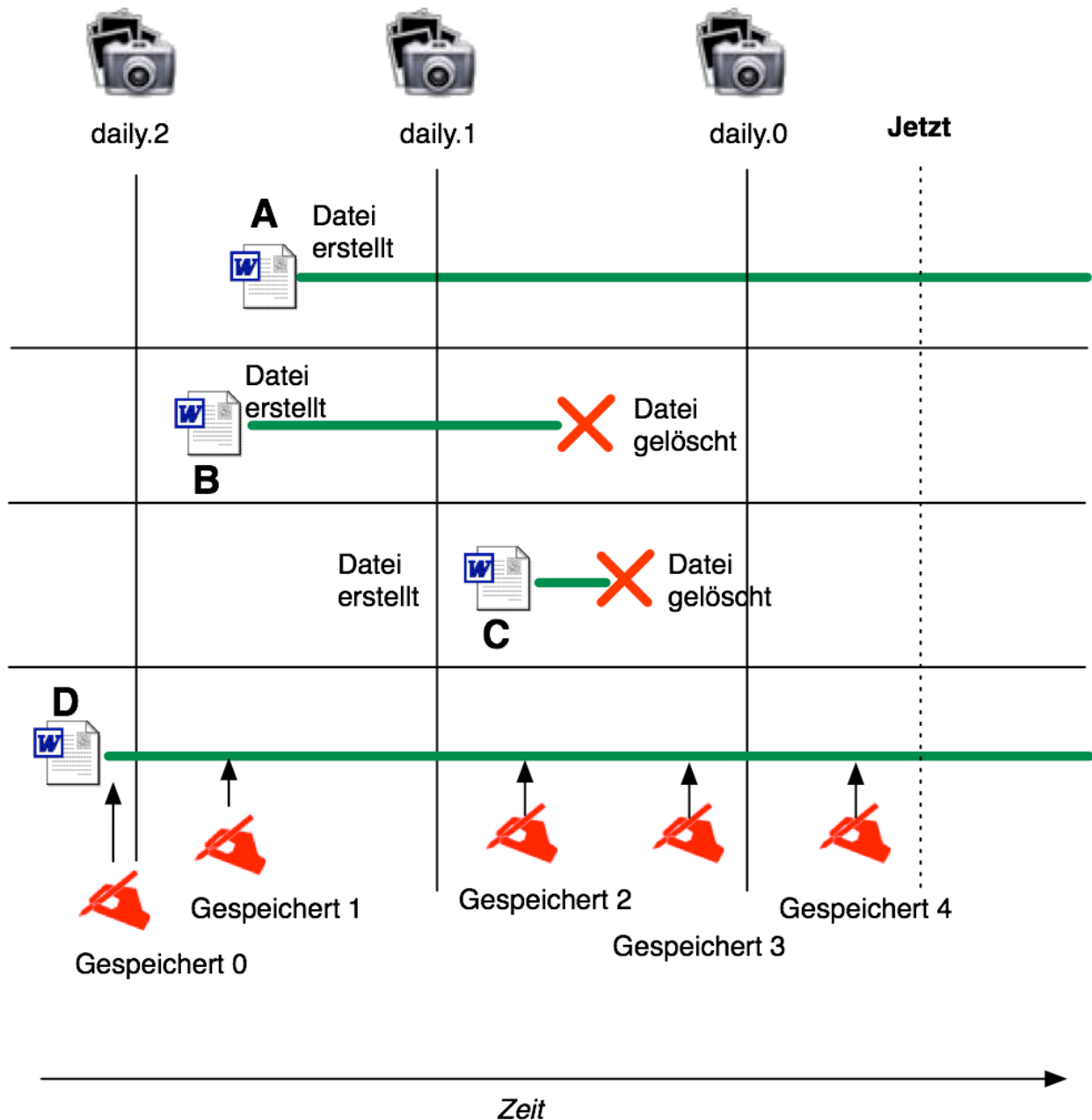


Abbildung 12 Verschiedene Szenarien bei Snapshots

4.2 Zugriff auf Snapshots unter Windows

Windows-Versionen ab Windows XP verfügen über eine integrierte Oberfläche für Snapshots, die über den Eigenschaften-Dialog von Netzlaufwerken, Ordnern und Dateien aufgerufen werden kann (Abbildung 13).

Bei Dateien werden damit automatisch alle verfügbaren, unterschiedlichen Versionen gefunden und angezeigt. Benutzer haben die Möglichkeit die älteren Versionen zu öffnen, eine Kopie zu erstellen oder die aktuelle Version durch die ältere zu ersetzen (Abbildung 14).

Bei einzelnen, gelöschten Dateien ist es wichtig, den dazugehörigen *Ordner* zu öffnen, denn die Datei selbst ist ja nicht mehr da. Im Snapshot des Ordners ist dann auch die Datei zu finden. Die gleiche Vorgehensweise ist nötig, wenn die Datei umbenannt worden ist.

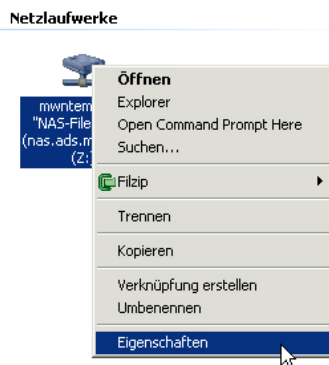


Abbildung 13 Zugang zum „Eigenschaften“-Dialog eines Ordners oder einer Dateiablage

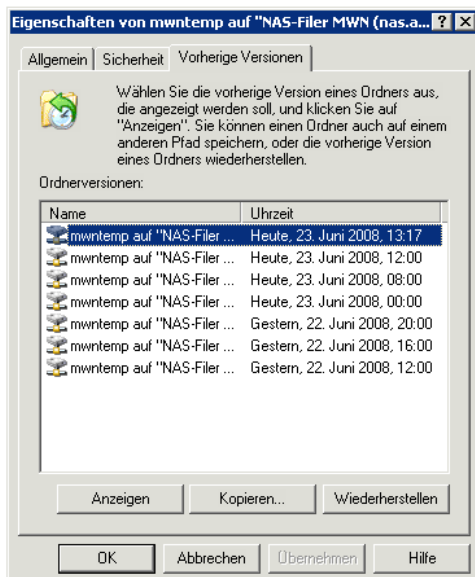


Abbildung 14 Liste verfügbarer Snapshots im „Eigenschaften“-Dialog

Falls man eine ältere Windows-Version nutzt oder direkt in den Snapshots suchen möchte kann man alternativ das versteckte Verzeichnis „~snapshot“ aufrufen (Abbildung 15). In diesem Verzeichnis sind alle verfügbaren Snapshots als Ordner sichtbar und darin befindet sich die gesamte Dateiablage genau so, wie sie zum Zeitpunkt der Erstellung ausgesehen hat.

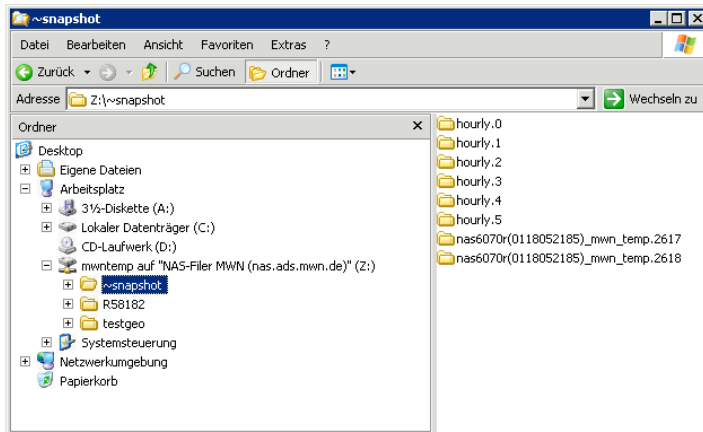


Abbildung 15 Liste von Snapshot-Unterordnern im „~snapshot“-Verzeichnis

4.3 Verwendung mit anderen Betriebssystemen

Unter Linux und Mac OS X können Snapshots nur über das (unsichtbare!) Verzeichnis ~snapshot angezeigt werden.

Bei Linux erfolgt das beispielsweise durch ein „cd ~snapshot“. Auf einem Mac kann – zusätzlich zum Weg über ein Terminal – auch der Finder eingesetzt werden um direkt in den Snapshot-Ordner zu wechseln (siehe Abbildung 16). Dazu wird im Finder „Gehe zu...“/“Gehe zum Ordner..“ ausgewählt.

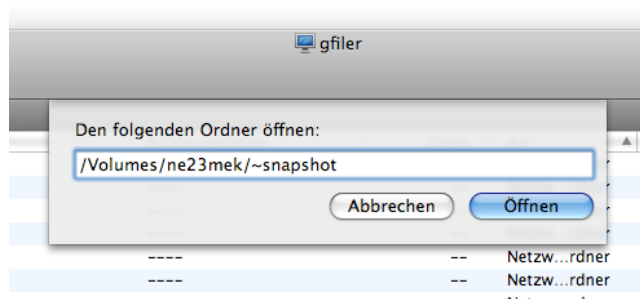


Abbildung 16 Mac OS X: Direkte Navigation zu einem Snapshot-Ordner