

# **Zusammenfassung M127**

Server betreiben

2008-11-12

Emanuel Duss

## Über

Autor Emanuel Duss  
Erstellt 2008-07-22  
Bearbeitet 2008-11-12  
Heute 2008-11-12  
Bearbeitungszeit 23:13:10  
Lehrjahr des Moduls 2. Lehrjahr 2007/2008  
Pfad /  
home/emanuel/Daten/Lehre/Zwischenprüfungen/Zusammenfassungen\_von\_mir/  
M127/M127\_Zusammenfassung.odt

CC-Lizenz



Creative Commons Namensnennung-Keine kommerzielle Nutzung-Weitergabe unter gleichen Bedingungen 2.5 Schweiz

<http://creativecommons.org/licenses/by-nc-sa/2.5/ch/>

Powered by



## Bearbeitungsprotokoll

Datum	Änderung(en)
2008-07-22	Erstellt
2008-09-03	Fertiggestellt

# Inhaltsverzeichnis

<b>1</b>	<b>Ein Server.....</b>	<b>6</b>
1.1	Was braucht alles ein Server?.....	6
1.1.1	Hardware.....	6
1.1.2	Software.....	6
1.1.3	Netzwerk-Hardware.....	6
1.1.4	Wissen.....	6
1.2	Einsatz von Servern.....	7
1.3	Serverarten – Beschreibung.....	7
1.4	Konstanter Betrieb eines Servers.....	8
<b>2</b>	<b>Dateisysteme.....</b>	<b>10</b>
2.1	FAT 12/16/32 File Allocation Table .....	10
2.1.1	NTFS.....	10
2.1.2	HFS.....	11
2.1.3	SMB.....	11
2.1.4	NFS.....	11
2.1.5	HPFS.....	11
2.1.6	ext2-fs.....	11
<b>3</b>	<b>Server einrichten mit einem Script.....</b>	<b>12</b>
3.1	Script für den Server.....	12
<b>4</b>	<b>Netzwerk-Protokolle.....</b>	<b>14</b>
4.1	Nicht routbare Protokolle.....	14
4.2	Routbare Protokolle.....	14
4.2.1	TCP/IP.....	14
<b>5</b>	<b>Das Tool: nslookup.....</b>	<b>15</b>
5.1.1	Ressource-Records (type; ty).....	16
<b>6</b>	<b>Host-File / DNS / WINS / DHCP.....</b>	<b>17</b>
<b>7</b>	<b>DFS.....</b>	<b>18</b>
7.1	Grundfunktion.....	18
7.2	Voraussetzungen.....	18
7.3	FRS (File Replication Service).....	18
7.4	Ausfallsicherheit.....	19
7.5	Verteilen von Daten / Standortübergreifendes DFS.....	19
7.6	Sicherung von Daten.....	19
<b>8</b>	<b>FQDN - Full Qualified Domain Name .....</b>	<b>20</b>
<b>9</b>	<b>Sonstiges.....</b>	<b>21</b>
9.1	Was zeigt der Befehl ipconfig /all?.....	21
9.2	Anderer Befehl für route print?.....	21
9.3	Braucht ein Drucker ein Gateway?.....	22

# Modulbaukasten

© by Genossenschaft I-CH - Informatik Berufsbildung Schweiz

## Modulidentifikation

Modulnummer	127
Titel	Server betreiben
Kompetenz	Server (-Systeme) in einer bestehenden Umgebung betreiben und unterhalten. Dabei Performance, Verfügbarkeits- und Sicherheitsanforderungen überwachen. Dienste, Zugriffs- und Berechtigungsverwaltung administrieren.
Handlungsziele	<ol style="list-style-type: none"> <li>1. Betriebsdokumentation konsultieren und die für den Betrieb definierten Vorgaben beachten.</li> <li>2. Zugriffs- und Berechtigungskonzept für verschiedene Benutzergruppen erstellen, Benutzer auf Grund des erarbeiteten Konzepts administrieren und Betriebsdokumentation ergänzen.</li> <li>3. Für die Serveradministration verfügbare Tools automatisiert und aufgabenorientiert einsetzen. Performance und Verfügbarkeit überwachen.</li> <li>4. Auf Servern neue Betriebssystem-Releases, Updates sowie Korrekturen/ Patches gemäss Vorgabe einspielen und Betriebsdokumentation nachführen.</li> <li>5. Server-Hardware überwachen, unterhalten und Systemupgrades planen.</li> </ol>
Kompetenzfeld	System Management
Objekt	<ul style="list-style-type: none"> <li>• Server mit Print- und File-Services.</li> <li>• Betriebsbereites LAN mit einigen Arbeitsstationen (Clients).</li> </ul>
Niveau	2
Voraussetzungen	<ul style="list-style-type: none"> <li>• Serverdienste in Betrieb nehmen</li> <li>• Vorgaben aus Systemhandbüchern beachten</li> <li>• Umgang mit gesicherten Quellen im Internet (Lieferanten, Hersteller)</li> </ul>
Anzahl Lektionen	40
Anerkennung	Eidg. Fähigkeitszeugnis Informatiker/Informatikerin
Modulversion	1.1
MBK Release	R3
Harmonisiert am	13.06.2005

## Handlungsnotwendige Kenntnisse

Handlungsnotwendige Kenntnisse beschreiben Wissens Elemente, die das Erreichen einzelner Handlungsziele eines Moduls unterstützen. Die Beschreibung dient zur Orientierung und hat empfehlenden Charakter. Die Konkretisierung der Lernziele und des Lernwegs für den Kompetenzerwerb sind Sache der Bildungsanbieter.

Modulnummer	127
Titel	Server betreiben
Kompetenzfeld	System Management
Modulversion	1.1
MBK Release	R3

Handlungsziel	Handlungsnotwendige Kenntnisse
1.	1. Kann für die einzelnen Elemente einer Betriebsdokumentation darlegen, welche Vorgaben für einen geordneten Betrieb enthalten sein müssen.
2.	1. Kennt die Möglichkeiten eines Betriebssystems, die Zugriffsberechtigungen auf Ressourcen festzulegen und kann aufzeigen, welche Auswirkungen diese hinsichtlich Sicherheit und Integrität des Systems haben.
3.	<ol style="list-style-type: none"> <li>1. Kennt Sinn und Zweck einer Reorganisation bei einem File-Server und kann darlegen, welche Auswirkungen eine Reorganisation auf das Speichervolumen und das Zugriffsverhalten hat.</li> <li>2. Kennt grundlegende Kommandobefehle eines Betriebssystems und kann erläutern, welche Wirkungen diese im Betriebssystem auslösen.</li> <li>3. Kennt die Aufgaben, die bei der Administration von Servern anfallen und kann aufzeigen, welche Werkzeuge zur Bearbeitung geeignet sind.</li> </ol>
4.	1. Weiss um die Bedeutung und Wichtigkeit einer vollständigen und fehlerfreien Betriebsdokumentation und kann an Beispielen aufzeigen, wie damit kritische Situationen effizient entgegnet werden kann.
5.	<ol style="list-style-type: none"> <li>1. Kennt die wichtigsten Merkmale der Hardware die beim Upgrade/Update eines Betriebssystems zu überprüfen sind und kann erläutern, welche Konsequenzen sich hinsichtlich Machbarkeit, Ausbau und Performance daraus ableiten lassen.</li> <li>2. Kennt Funktionen zur Überprüfung und Sicherstellung der Integrität von Speichermedien (RAM, HD) und kann erläutern, welche Arten von Fehlern damit verhindert werden können.</li> <li>3. Kennt das Prinzip der redundanten Speicherung der Daten auf verschiedenen Festplatten zur Steigerung der Sicherheit (Redundant Array of Inexpensive Disks, RAID) und kann darlegen, welche Vorkehrungen beim Upgrade solcher Systeme zu beachten sind.</li> <li>4. Kennt Tools zur Überwachung unterbrechungsfreier Stromversorgungen (USV) und kann erläutern, wie mit einer systematischen Überwachung und Pflege solcher Geräte einem Serverausfall vorgebeugt werden kann.</li> </ol>

# 1 Ein Server

## 1.1 Was braucht alles ein Server?

### 1.1.1 Hardware

- USV
  - Zum Schutz des Servers von einem Stromunterbruch
- Nur schwache Grafikkarte
- Einen Switch
- Leistungsfähige Server (IBM, HP)
- Redundanz
  - Netzwerkkarte (NIC)
  - Zwei zu einer Verbinden (Trunk), muss am Switch eingestellt werden
  - Power Supply
  - HDs
  - Lüfter
  - RAM (ECC-RAM: Sicherer)
- CPU
- Raid
  - Raid 0: Striping: Sehr schnell aber keine Redundanz; Daten werden auf 2 HDs aufgeteilt
  - Raid 1: Spiegelung: Sicherer aber nur halb so viel Speicherplatz
  - Raid 5: Min. 3 HDs Dabei wird auf 2 Platten geschrieben und auf der dritten eine Prüfsumme gespeichert. Die Platten wechseln sich dabei immer ab: einmal ist auf der 1. HD die Prüfsumme und dann auf der Zweiten. Dann hat man Geschwindigkeit und Redundanz. Eine HD darf ausfallen. Die Prüfsumme rotiert von Platte zu Platte; ist also nicht immer auf der selben Platte.
- Komponenten sind für 24h/d geplant => Langzeitbetrieb

### 1.1.2 Software

- Betriebssystem
  - Windows-Server / Linux-Server
  - Grafisch Minimal
- Server-Software
  - Dienste (DNS, WINS, DHCP, Fileserver, ...)

### 1.1.3 Netzwerk-Hardware

- Switch (gibt wenig Broadcast gegenüber dem Hub)
  - Gleichzeitig mehrere Geschwindigkeiten
  - Ein Layer-3-Switch kann routen
- Hub
  - Gesamtes Netzwerk wird auf das langsamste Gerät angepasst

### 1.1.4 Wissen

- Sapere aude! - Wage zu wissen! – Immanuel Kant

## 1.2 Einsatz von Servern

- File-Server
  - SMB
- Print-Server
  - Spooling
- Mail-Server
  - Exchange, Domino
- Backup-Server
  - Dedizierter Server macht Sinn (Dediziert = Ausschliesslich, Optimiert für das)
- Datenbank-Server
  - MySQL
- Webserver
  - PHP, Pearl, MySQL
  - Zugriff per FTP
    - Achtung: Passwort wird im Klartext übermittelt (Achtung: Sniffen)
- Active-Directory / Benutzer-Server
  - LDAP
- Applikation-Server
- Terminal-Server
- RAS (Remote Access Service)
- VPN ist Bestandteil von RAS

## 1.3 Serverarten – Beschreibung

### Dateiserver

Sobald der Server für andere Benutzer im Netzwerk Dateien in freigegebenen Ordnern bereitstellt, fungiert er als Dateiserver. Zu konfigurieren sind dazu Freigaben mit den entsprechenden Sicherheitseinstellungen für die Benutzer und Gruppen.

### Druckserver

Die am häufigsten genutzten Dienste eines Servers sind die zur zentralen Bereitstellung und Verwaltung von Druckern. Dieser Dienst ist mit W2k3 Server noch einfacher geworden

### Anwendungsserver

Über die Anwendungsdienste können Server miteinander kommunizieren beziehungsweise spezielle Funktionen als Clients bereitstellen. Sie sind beim W2k3 Server in den Internet Information Services (IIS) verankert.

Für einen normalen Serverbetrieb im Netzwerk, bei dem die zentrale Verwaltung der Benutzerkonten und Ressource (Daten, Drucker, etc.) im Vordergrund steht, sind diese Anwendungsdienste nicht relevant.

### Mailserver

Mit W2k3 Server kann man einen einfachen, aber voll funktionsfähigen Mailserver betreiben.

### Terminalserver

Über den Terminalserver werden Clients virtuelle Windows-Computer zur Verfügung gestellt. Alle Anwendungen und Systemeinstellungen werden am Terminalserver vorgenommen. Die Benutzer greifen auf

diese dann über eine spezifische Clientsoftware zu. Bei einem leistungsfähigen Terminalrechner mit einer schnellen Netzwerkanbindung sind Performance-Unterschiede zu einem lokal arbeitenden Windows kaum noch auszumachen.

## **RAS/VPN Server**

Ein RAS/VPN-Server fungiert heute oft nicht nur im lokalen Netzwerk, sondern soll aus verschiedenen Gründen über eine direkte Datenfernverbindung oder mit Hilfe des Internets als Transportmedium erreichbar sein. Die Remote Access Services (RAS) stellen dazu die benötigten Funktionen bereit.

## **Domänencontroller**

Die Domänencontroller verwalten die Verzeichnisdatenbank der Domäne, in der unter anderem alle Benutzer, Sicherheitsgruppen und Computer erfasst sind ( ▪ Active Directory)

## **DNS-Server**

Das Domain Name System (DNS) dient der Namensauflösung im Internet oder im LAN.

Bei Active Directory wird DNS vorausgesetzt.

IP-Adresse ← → Namen

## **DHCP-Server**

Mithilfe des Dynamic Host Configuration Protocol (DHCP) werden IP-Adressen an Clientcomputer automatisch durch einen zentralen DHCP-Server verteilt.

## **Streaming-Media-Server**

Grundlegende Funktionen für die zentrale Bereitstellung von multimedialen Inhalten im Netzwerk.

## **WINS-Server**

WINS (Windows Internet Name Service) wurde ursprünglich für die Namensauflösung in Windows-Netzwerken entwickelt. Übernimmt eine ähnliche Rolle wie der DNS-Server.

# **1.4 Konstanter Betrieb eines Servers**

Das Eventlog sollte keine Fehler anzeigen. Dann kann man davon ausgehen, dass der Server weiterhin so läuft, wie er ist.

Das Eventlog wird über den Befehl *eventvwr* gestartet.



The screenshot shows the Windows Event Viewer window titled "Ereignisanzeige". The left pane shows a tree view with "Anwendung" selected. The main pane displays a table of 16 events. The table has columns for Typ, Datum, Uhrzeit, Quelle, Kategorie, Ereignis, and Benutzer. The events are sorted by date and time, showing a sequence of events from January 4, 2008, to August 8, 2007.

Typ	Datum	Uhrzeit	Quelle	Kategorie	Ereignis	Benutzer
Information	04.01.2008	09:09:54	LoadPerf	Keine	1000	Nicht
Information	04.01.2008	09:09:54	LoadPerf	Keine	1001	Nicht
Information	04.01.2008	09:05:52	EventSystem	Keine	4625	Nicht
Information	04.01.2008	09:05:52	MSDTC	TM	4193	Nicht
Information	04.01.2008	09:04:24	MsiInstaller	Keine	1005	Admi
Information	04.01.2008	09:04:24	MsiInstaller	Keine	11707	Admi
Information	04.01.2008	09:02:46	LoadPerf	Keine	1000	Nicht
Information	04.01.2008	09:02:45	LoadPerf	Keine	1001	Nicht
Information	04.01.2008	08:58:38	EventSystem	Keine	4625	Nicht
Information	04.01.2008	08:58:35	MSDTC	TM	4193	Nicht
Information	04.01.2008	08:22:22	MsiInstaller	Keine	1005	Admi
Information	04.01.2008	08:21:43	LoadPerf	Keine	1000	Nicht
Information	04.01.2008	08:21:42	LoadPerf	Keine	1001	Nicht
Information	04.01.2008	07:20:06	EventSystem	Keine	4625	Nicht
Information	04.01.2008	07:20:06	MSDTC	TM	4193	Nicht
Information	08.08.2007	13:37:54	LoadPerf	Keine	1000	Nicht
Information	08.08.2007	13:37:53	LoadPerf	Keine	1001	Nicht
Information	08.08.2007	13:33:32	EventSystem	Keine	4625	Nicht
Information	08.08.2007	13:33:31	MSDTC	TM	4193	Nicht
Information	08.08.2007	12:27:48	LoadPerf	Keine	1000	Nicht
Information	08.08.2007	12:27:48	LoadPerf	Keine	1000	Nicht
Information	08.08.2007	12:27:47	LoadPerf	Keine	1000	Nicht

## 2 Dateisysteme<sup>1</sup>

Ein Dateisystem wird benötigt, um mittels beliebiger Datenträger **strukturiert** Dateien und Verzeichnisse **abzulegen**. Lese- und Schreibzugriffe auf das Dateisystem wird mittels **Treiber** umgesetzt. Es gibt weltweit mehr als 100 verschiedene Dateisysteme und Partitionstypen mit jeweils verschiedenen Eigenschaften.

### 2.1 FAT 12/16/32 File Allocation Table

FAT Dateisysteme sind von der Struktur her einfach aufgebaut und enthalten eine zusätzliche Kopie der Dateizuordnungstabelle im ersten MByte auf dem Datenträger. Bei Beschädigung der Haupttabelle kann diese durch die Kopie korrigiert werden, vorausgesetzt das erste MByte ab Sektor 0 wurde nicht gelöscht. Der Zugriff auf FAT Partitionen wird von den meisten Betriebssystemen als Standard unterstützt. Der Einsatz dieses Dateisystem beansprucht nur sehr geringe Ressourcen, zum heutigen Zeitpunkt nachteilig ist der hohe Speicherverschnitt (slack space) der durch eine zu hohe Clustergröße bei der Aufteilung der Dateien entsteht. Dateinamen werden generell in Großbuchstaben abgespeichert, eine Unterscheidung in Groß- oder Kleinschreibung findet unter Windows Betriebssystemen nicht statt. Für das FAT-Dateisystem sind nur wenige Attribute verfügbar. Diese sind **R, H, S, A**: **R**ead-only, **H**idden, **S**ystem und **A**rchive.

Das Dateisystem FAT mit der darauf folgenden 2-stelligen Zahl zeigt die Anzahl der maximal adressierbaren Cluster in Bit an und damit auch die maximale Anzahl von verwaltbaren Dateien. Daraus ergeben sich folgende Angaben:

Merkmale	FAT 12	FAT 16	FAT 32
Max. Dateigröße:	32 MByte	2048 MByte	4096 MByte
Max. Partitionsgröße:	32 MByte	2048 MByte (DOS) // 4096 MByte (NT)	8192 GByte
Max. Anzahl der Dateien:	4096	65536	ca. 4,2 Mio.

#### FAT 12

Kam 1976 erstmals auf 180 KByte **Disketten** zum Einsatz. Die Idee und Grundlagen zu diesem Dateisystem entstanden durch **Tim Patterson**, die Technik wurde 1976 von **Bill Gates aufgekauft**. Für den Dateinamen lassen sich maximal **8 Zeichen**, für die Erweiterung **3 Zeichen** wählen.

#### FAT 32

Ist der Nachfolger von FAT 12 für Festplatten. Diese überarbeitete Version erlaubt jetzt **Partitionsgrößen von bis zu 8 Terabyte**. Allerdings ist in Windows 2000 und **Windows XP** das Formatieren von **mehr als 32 GByte** großen FAT32 Partitionen **nicht direkt möglich**. FAT 32 nutzt gegenüber FAT 16 **kleinere Cluster** was zu einer **besseren Speichernutzung** und **weniger Speicherverschnitt** führt. Dateinamen sind jetzt **nicht mehr auf das 8.3 Schema** beschränkt.

#### 2.1.1 NTFS

**New Technology File System** Dieses Dateisystem wird **seit der ersten Windows NT Version** eingesetzt. Geerbt hat es **Designkonzepte von HPFS**. Die **Verwaltung** findet direkt auf der **Ebene von Sektoren** statt und ermöglicht dadurch **bessere Speicherplatzausnutzung**. Zur Verwaltung der Sektoren und Dateien kommt die **MFT (Master File Table)** zum Einsatz. Es gehört zu den **protokollierenden Dateisystemen** die **jede Änderung protokollieren und überwachen**. **Wird ein Vorgang nicht vollständig beendet, wird der Originalzustand wiederhergestellt**. Mit NTFS lassen sich einzeln **Datei- und Ordner Rechte** einrichten. Die **Partitionsgröße** kann bis zu **2<sup>64</sup> Byte** groß sein, Dateinamen werden mit bis zu **255 Unicode Zeichen**. Es unterstützt eine **transparente Komprimierung** von Dateien und Verzeichnissen und bietet eine

<sup>1</sup> Quelle: [http://www.operating-system.org/betriebssystem/\\_german/w-dateisys.htm](http://www.operating-system.org/betriebssystem/_german/w-dateisys.htm)

Transaktionsverwaltung aller Zugriffen (Indizes). Attribute von gespeicherten Objekten sind **Lesen, Schreiben, Ausführen, Löschen, Berechtigung, Eigentümer und Komprimiert**.

## 2.1.2 HFS

**Hierarchical Filesystem** HFS ist das Standard Dateisystem für **Macintosh** Computer. Es ist der **Nachfolger des MFS** (Macintosh File System) Dateisystem. Eine Partition kann mit bis zu 65.535 Cluster (16-Bit) formatiert werden, die **Clustergröße richtet sich nach der Größe der Partition. Dateinamen** können aus bis zu **31 Zeichen** bestehen, die **maximale Dateigröße beträgt 2 GByte**. Der Nachfolger heisst **HFS+** und zeichnet alle **Zugriffe** auf das Dateisystem **in einem Journal** für höhere Datensicherheit auf. Der **Dateiname** kann jetzt aus bis zu **255 Unicode Zeichen** bestehen. Das Dateisystem kann jetzt mit bis zu 32-Bit Clustern adressiert werden und unterstützt eine maximale **Dateigröße von 8 Exabyte** ( $2^{63}$  byte).

## 2.1.3 SMB

**Server Message Block** Dieses **Netzwerk-Dateisystem bzw. Protokoll** ermöglicht es, auf die exportierten Verzeichnisse eines Rechners mit NetBIOS- und TCP/IP Unterstützung zuzugreifen. Zum Beispiel bietet **Windows** ab der Version **3.11** (Workgroups) diese Funktionalität, wenn ein TCP/IP-Stack installiert ist. Haupteinsatz sind **homogene Windows** Netzwerke aber auch **heterogene Netzwerke**, die sich aus **Unix** oder verwandten Betriebssystemen **und Windows** Computern zusammensetzen.

## 2.1.4 NFS

**Network Filesystem** Sun Microsystems entwickelte dieses Dateisystem um den Dateizugriff über mehrere Computer hinweg zu ermöglichen. Mit diesem **Netzwerk-Dateisystem** können Verzeichnis-Einträge verschiedener Rechner im lokalen Netzwerk ausgetauscht werden. Es ist das **Standard-Dateisystem in Unix Netzwerken** für den Datenzugriff unter den einzelnen Rechnern.

## 2.1.5 HPFS

**High Performance File System** Dieses Dateisystem wurde gemeinsam von **IBM** und **Microsoft** etwa im Jahr 1985 entwickelt. Eingesetzt wurde es zunächst in **OS/2 1.2** und **Microsoft LAN Server**. Die Idee entstand aus den **unzureichenden Fähigkeiten des FAT Dateisystem** für den Einsatz auf Servern und in Netzwerken, wie **fehlende Dateizugriffsrechte**. HPFS besitzt eine deutlich **fortschrittlichere Methode** um die Dateien und Verzeichnisse zu verwalten und die **Fragmentation weitgehend zu vermeiden**. Durch die Anordnung in B-Verzweigungen lassen sich **Objekte schneller auffinden**. Die Objektabelle befindet sich zusätzlich in der **Mitte der Partition** um die **Datensicherheit zu erhöhen** und die **Suchzeit zu minimieren**. Es können sogar **eigene Attribute** wie der Herkunftsort einer Datei definiert werden. 1991 gab Microsoft die Mitarbeit an OS/2 auf, was zum Bruch zwischen IBM und Microsoft führte. Seitdem war Apple Vertriebspartner für OS/2.

## 2.1.6 ext2-fs

**extended filesystem** ext2 ist das erweiterte Dateisystem von Rémy Card. Es kann als das **Standarddateisystem** für das Betriebssystem **Linux** bezeichnet werden. Die **Dateinamen** können bis zu **255 Zeichen** lang sein, die maximale Größe für eine **Partition** liegt mit Kernel 2.2 bei **2 GByte**. Dieses Dateisystem ist so organisiert, dass zu jeder Datei eine **Informationsdatei** (Inode) gehört, in der **F** **ausser dem Dateinamen** vermerkt ist. So werden darin die **Zugriffsrechte, Dateigröße, Position** und die **belegten Dateiblöcke** abgelegt.

Inzwischen wird das ext- Dateisystem mit Verbesserungen im Bereich Design und Leistung in der **Version 3** eingesetzt. (Ext-3: Größe einer Datei 16 GiB–2 TiB; Länge des Dateinamens 255 Byte; Größe des Dateisystems 2 TiB–32 TiB).

## 3 Server einrichten mit einem Script

### 3.1 Script für den Server

Damit wir den Server möglichst schnell einrichten können, erstellen wir alles mit einem Script. Der Vorteil von einem Script ist es, das danach jeder Server genau gleich aussieht.

#### User einrichten

Hinweis: ä = „ // ö = " // ü = ü

Achtung: Kennwortrichtlinien deaktivieren und *gpupdate /force*

Mit net user kann man ganz einfach neue Benutzer erstellen. Diese bekommen das bekannte „just4us“-Passwort.

```
net user ABBM "just4us" /add /expires:never /fullname:"Martina Abbühl"  
/comment:"Zürich" /profilepath:\\zue-srv01\users$\ABBM\Profile /homedir:\\zue-  
srv01\users$\ABBM\Home
```

Das Home-Laufwerk wird automatisch auf den Laufwerksbuchstaben Z:\ gemappt.

#### Globale Groups einfügen!

```
net group GO_Filialleiter /add
```

#### Lokale Groups einfügen!

```
net localgroup LR_Filialleiter /add
```

#### Globele Gruppen zu den Lokalen Gruppen hinzufügen

```
net localgroup LR_Filialleiter GO_Filialleiter /add
```

#### User zu den Globalen Gruppen hinzufügen

```
net group GO_Filialleiter ABBM /add
```

#### Home-Verzeichnis für die Benutzer einfügen

Das Home-Verzeichnis wird im Ordner *D:\Daten\Users\%username%\Home* erstellt.

```
mkdir D:\Daten\Users\ABBM\Home
```

#### Profile-Ordner für die Benutzer erstellen

Das Profil wird im Ordner *D:\Daten\Users\%username%\Profile* erstellt.

```
mkdir D:\Daten\Users\ABBM\Profile
```

#### Berechtigungen erstellen

```
cacls D:\Daten /T /C /G Administrator:F Dom,,nen-Admins:F  
cacls D:\Daten\Users /T /C /G Jeder:R Administrator:F Dom,,nen-Admins:F  
net share users$=D:\Daten\Users /GRANT:Jeder,FULL
```

#### Public-Folder erstellen zum Austauschen von Dateien

Wir erstellen den folgenden Ordner, der für alle freigegeben ist. Dabei haben alle die Vollberechtigung (Gruppe Jeder).

```
mkdir D:\Daten\Public  
cacls D:\Daten\Public /T /C /G Jeder:F  
net share public$=D:\Daten\Public /GRANT:Jeder,FULL
```

## Erstelle Gruppenordner

Auf die Gruppenordner haben nur die bestimmten Gruppen Zugriff.

Hinweis: Wir geben nicht den Ordner einer bestimmten Gruppe frei, sondern der übergeordnete Ordner Groups. Damit gehen wir auf die sichere Seite, wenn jemand in mehreren Gruppen ist. Dann kann man nur den Ordner Groups mappen und der Zugriff ist per NTFS-Berechtigung auf die jeweiligen Unterordner vom Netzwerklaufwerk geregelt.

```
net share groups$=D:\Daten\Groups /GRANT:Jeder,FULL
mkdir D:\Daten\Groups\Filialleiter
cacls D:\Daten\Groups\Filialleiter /T /C /G LR_Filialleiter:F Administrator:F
Dom,,nen-Admins:F
```

## Preislisten-Ordner erstellen und freigeben

In diesem Ordner wird vom Chef eine Preisliste angelegt. Der Filialleiter hat darauf den Vollzugriff. Alle Anderen dürfen aber nur lesen.

```
mkdir D:\Daten\Preislisten
cacls D:\Daten\Preislisten /T /C /G Jeder:R LR_Filialleiter:F Administrator:F
Dom,,nen-Admins:F
net share preislisten$=D:\Daten\Preislisten /GRANT:Jeder,FULL
```

## Berechtigungen für die User auf das Home- und Profile-Verzeichnis

Auf das Home-Verzeichnis hat natürlich nur der User und der Administrator Zugriff.

```
cacls D:\Daten\Users\ABBM /T /C /G ABBM:F Administrator:F Dom,,nen-Admins:F
```

## 4 Netzwerk-Protokolle

### 4.1 Nicht routbare Protokolle

Pro	Kontra
<ul style="list-style-type: none"> <li>● Schnell bei weniger als 30 Geräten</li> <li>● Nur im gleichen Subnetz</li> <li>● Einfache Konfiguration</li> </ul>	<ul style="list-style-type: none"> <li>● Nicht Routbar</li> <li>● Nur für Windows</li> <li>● Nicht für Internetzugriff geeignet</li> </ul>

Beispiele: NetBIOS / NetBEUI

### 4.2 Routbare Protokolle

Pro	Kontra
<ul style="list-style-type: none"> <li>● Geeignet für grosse LANs und WANs</li> <li>● Routbar über Router, Subnetze, Internet</li> <li>● Betriebssystemunabhängig</li> <li>● Heutiges Standardprotokoll</li> </ul>	<ul style="list-style-type: none"> <li>● Zu viel Overhead bei kleinen Netzen</li> <li>● schwierige Konfiguration in grösseren Netzen</li> <li>● Braucht Hilfsmittel wie Host-File, DNS, WINS</li> </ul>

Beispiel: TCP/IP

#### 4.2.1 TCP/IP

- Ipv4 ist heutiger Standard
- Es gibt Adressklassen (Siehe Modul 117)
- Verwendung wenn: Routbar, Internetzugriff und andere Betriebssysteme
- Weitere Theorie siehe Modul 117.

## 5 Das Tool: nslookup

- CLI (Command Line Interface)-Tool um DNS-Einträge abzufragen

### Mailserver auf einem unbekanntem Nameserver abfragen

Mailserver von edulu.ch abfragen	nslookup -type=mx edulu.ch
Nameserver von Google.ch abfragen	nslookup -type=ns google.ch
Mailserver von edulu.ch auf dem Nameserver von Google abfragen	nslookup -type=mx edulu.ch ns1.google.com

### Start of Authority

- Responsible mail address = Verweis auf das Mail vom Admin (wird jedoch nicht direkt eingetragen!)
- Serial = Erstellungsdatum + 2 letzte Zahlen: Änderungen
- Beim DNS hat die TTL eine andere Bedeutung. Die Zahl TTL zeigt an, für welche Zeit (in Sekunden) ein Namenseintrag noch gültig ist. Nach Ablauf dieser Zeit muss die Namensauflösung wiederholt werden. Bei Linux/Unix kann man sich den aktuellen Wert mit den Kommandos 'host' oder 'dig' anzeigen lassen.
- Einstellungen Testen: [www.ipplus.ch](http://www.ipplus.ch) → Tools → DNS

```
nslookup -ty=soa google.ch
Server: s991000.suvanet.ch
Address: 10.99.1.0

Non-authoritative answer:
google.ch
    primary name server = ns1.google.com
    responsible mail addr = dns-admin.google.com
    serial = 2008030700
    refresh = 21600 (6 hours)
    retry = 3600 (1 hour)
    expire = 1209600 (14 days)
    default TTL = 300 (5 mins)

google.ch      nameserver = ns4.google.com
google.ch      nameserver = ns1.google.com
google.ch      nameserver = ns2.google.com
google.ch      nameserver = ns3.google.com
ns1.google.com internet address = 216.239.32.10
ns2.google.com internet address = 216.239.34.10
ns3.google.com internet address = 216.239.36.10
ns4.google.com internet address = 216.239.38.10
```

### Alle Querys anzeigen

```
C:\>nslookup -ty=all teko.ch air.tic.ch
Server: ns1.tic.ch
Address: 193.193.144.12
```

```

DNS request timed out.
  timeout was 2 seconds.
Nicht autorisierte Antwort:
teko.ch text =

      "v=spf1 mx -all"
teko.ch MX preference = 20, mail exchanger = lufw2.teko.ch
teko.ch MX preference = 30, mail exchanger = lufw6.teko.ch
teko.ch MX preference = 40, mail exchanger = lufw7.teko.ch
teko.ch MX preference = 10, mail exchanger = lufw1.teko.ch
teko.ch
      primary name server = lufw1.teko.ch
      responsible mail addr = host-master.teko.ch
      serial = 2008021300
      refresh = 86400 (1 day)
      retry = 7200 (2 hours)
      expire = 604800 (7 days)
      default TTL = 172800 (2 days)
teko.ch nameserver = lufw1.teko.ch
teko.ch nameserver = lufw2.teko.ch
teko.ch nameserver = lufw6.teko.ch

teko.ch nameserver = lufw6.teko.ch
teko.ch nameserver = lufw1.teko.ch
teko.ch nameserver = lufw2.teko.ch
lufw7.teko.ch internet address = 212.59.165.42

```

### 5.1.1 Ressource-Records (type; ty)

SOA	Verwaltungsinfos
A	Adresseintrag (Name → IP) (IPv4)
AAA	Adresseintrag (Name → IP) (IPv6)
NS	Nameserver
CNAME	Canonical Name → Aliasnamen
PTR	Adresseintrag (IP → Name)
MX	MailXChanger – Mailserver
HINFO	Hostinfos (falls gesetzt)
TXT	Kommentare
ALL	(fast) alles (QueryType – aber eigentlich KEIN Ressource Record)



## **6 Host-File / DNS / WINS / DHCP**

Siehe in der Zusammenfassung von M117.

Dort befindet sich auch der DHCP-Relay-Agent!

# 7 DFS

## 7.1 Grundfunktion

Die Grundfunktion von DFS ist es, verschiedene Freigaben auf mehreren Servern zu einer Freigabe zusammenzufassen.

- Client ermittelt durch ActiveDirectory den nächstgelegenen DFS Root-Server. Ist ein DFS Root-Server nicht verfügbar, suchen die Clients einen weiteren.
- DFS leitet die Clients nun zu den DFS-Zielen (Targets), also den Servern mit den entsprechenden Freigaben. Wenn ein solcher Server ausfällt, leitet DFS die Clients zu einem Server, dessen Freigabe als DFS-Target für dieselbe DFS-Verknüpfung konfiguriert ist.

Der Client connectet zum DFS-Server. Dort schaut der Client, wo die eigentliche Freigabe ist, und connectet dann direkt darauf. Es passiert kein Umweg über den DFS-Server. Es muss nicht zwingend eine Windows-Freigabe sein (der Client muss das Protokoll einfach unterstützen).

Wenn ein AD vorhanden ist, erstellt man einen DFS-Domänenstamm.

DFS-Domänenstamm	<a href="#">\\domain.int\stammname</a>
Eigenständiger Stamm	\\computername\stammname

## 7.2 Voraussetzungen

OS	DFS-Client	DFS-Root	DFS-Ziel
W2k3	Ja	Ja	Ja
Windows XP	Ja	Nein	Ja
W2k Server	Ja	Ja	Ja
W2K Professional	Ja	Nein	Ja
Windows NT4 Server	Ja	Ja (kein Domain-Mode)	Ja
Windows NT4 Workstation	Ja	Nein	Ja
Windows 98	Ja (kein Domain Mode)	Nein	Ja

## 7.3 FRS (File Replication Service)

Das funktioniert nur beim **DFS-Domänenstamm** (setzt ActiveDirectory voraus).

Eine DFS-Verknüpfung kann auch auf mehrere Ziele zeigen, die auf verschiedenen Servern liegen. (zwei Ziele)

Wenn eine DFS-Verknüpfung auf 4 Ordner zeigt, möchte man diese 4 Freigaben synchron halten! (Replikationssatz hinzufügen)

Bei Verwendung eines „eigenständigen DFS-Stammes“ (also ohne die Mitarbeit einer Domain) kann man zwar mehrere Ziele definieren, diese jedoch nicht automatisch synchronisieren (das muss dann anders)

gelöst werden.).

## 7.4 Ausfallsicherheit

Sehr wichtig natürlich!!!

Klassischerweise verwendet man Cluster. Doch das DFS kann auch eine preisgünstigere Alternative sein.

DFS ist an zwei Stellen „empfindlich“: am DFS-Root (also die Anlaufstelle der Clients) und die DFS-Zeile (die Freigabe von den Servern).

So macht man es sicherer:

- DFS-Domänenstamm verwenden
- Redundante ActiveDirectory-Domainkontroller. Wenn kein DC vorhanden ist dann finden die Clients überhaupt nichts (/dev/null ☺).
- Redundante DFS-Roots: Wird über die MMC konfiguriert.
- Redundante DFS-Ziele: Mindestens 2 Ziele pro DFS-Verknüpfung. Diese sollten z.B. mit dem File Replication Service synchron gehalten werden.

Die redundanten Maschinen sollten physikalisch getrennt stehen...

## 7.5 Verteilen von Daten / Standortübergreifendes DFS

Damit die Mitarbeiter in Chur nicht über die WAN-Strecke auf den Server in Luzern zugreifen müssen, stellt man in Chur einen Server auf und erstellt eine Freigabe. Diese Freigabe definiert man dann als zusätzliches Ziel. Nun können die Mitarbeiter von Chur auf den Chur-Server zugreifen. Das macht man mit dem Domain Controller, dem DFS-Root und dem FileServer.

→ Man muss Das Datenvolumen beachten, damit die Synchronisation nicht die WAN-Strecke belastet.

## 7.6 Sicherung von Daten

Die verschiedenen Ziele auf den verschiedenen Lokationen werden mit dem FRS synchronisiert. Somit muss man nur an einem Ort einen Tape-Roboter aufstellen.

Sollte der Fileserver auf der Agentur ausfallen, so greifen die Clients auf die Daten im Hauptsitz zu. Ein Störfallkonzept ist also schon integriert ;).

## 8 FQDN - Full Qualified Domain Name

Der vollständige Name einer Domain wird als ihr Fully Qualified Domain Name (FQDN) bezeichnet. Der Domain-Name ist in diesem Fall eine Absolute Adresse.

Der FQDN von `www.wikipedia.de.` ergibt sich durch:

```
3rd-level-label . 2nd-level-label . 1st-level-label . root-label  
www           .   wikipedia       .   de           .
```

Da der Root-Label immer leer ist, wird auf die Darstellung des Punktes zwischen `root-label` und Label der Top Level Domain fast immer verzichtet.

### Subdomain

Als Subdomain bezeichnet man eine Domain, welche in der Hierarchie unterhalb einer anderen liegt. Im allgemeinen Sprachgebrauch sind damit meist Domains in der dritten oder einer weiteren Ebene gemeint. Domains, die direkt unterhalb der Top-Level-Domain liegen, werden umgangssprachlich nicht als Subdomains, sondern als Second-Level-Domain oder nur Domain bezeichnet.

## 9 Sonstiges

### 9.1 Was zeigt der Befehl ipconfig /all?

```
C:\>ipconfig /all

Windows-IP-Konfiguration

    Hostname. . . . . : winxp
    Primäres DNS-Suffix . . . . . :
    Knotentyp . . . . . : Unbekannt
    IP-Routing aktiviert. . . . . : Nein
    WINS-Proxy aktiviert. . . . . : Nein

Ethernetadapter LAN-Verbindung:

    Verbindungsspezifisches DNS-Suffix:
    Beschreibung. . . . . : Intel(R) PRO/100 VE Network
Connection
    Physikalische Adresse . . . . . : 00-0C-F1-D5-4A-D6
    DHCP aktiviert. . . . . : Ja
    Autokonfiguration aktiviert . . . : Ja
    IP-Adresse. . . . . : 10.0.0.104
    Subnetzmaske. . . . . : 255.0.0.0
    Standardgateway . . . . . : 10.0.0.1
    DHCP-Server . . . . . : 10.0.0.1
    DNS-Server. . . . . : 195.186.1.110
    195.186.1.111
    Lease erhalten. . . . . : Donnerstag, 21. Februar 2008
19:52:38
    Lease läuft ab. . . . . : Sonntag, 24. Februar 2008 19:52:38
```

### 9.2 Anderer Befehl für route print?

```
C:\>netstat -r

Routingtabelle
=====
Schnittstellenliste
0x1 ..... MS TCP Loopback interface
0x2 ...00 0c f1 d5 4a d6 ..... Intel(R) PRO/100 VE Network Connection -
Paketplaner-Miniport
=====
=====
Aktive Routen:
    Netzwerkziel      Netzwerkmaske      Gateway      Schnittstelle      Anzahl
    0.0.0.0           0.0.0.0           10.0.0.1    10.0.0.104         20
    10.0.0.0          255.0.0.0         10.0.0.104  10.0.0.104         20
    10.0.0.104       255.255.255.255   127.0.0.1   127.0.0.1          20
    10.255.255.255   255.255.255.255   10.0.0.104  10.0.0.104         20
    127.0.0.0        255.0.0.0         127.0.0.1   127.0.0.1          1
    224.0.0.0        240.0.0.0         10.0.0.104  10.0.0.104         20
    255.255.255.255  255.255.255.255   10.0.0.104  10.0.0.104         1
Standardgateway:      10.0.0.1
=====
Ständige Routen:
```

Keine

```
root@ubuntu:~# netstat -r
Kernel IP Routentabelle
Ziel          Router      Genmask      Flags        MSS  Fenster  irtt  Iface
link-local    *           255.255.0.0  U            0 0      0 eth0
10.0.0.0      *           255.0.0.0   U            0 0      0 eth0
default       10.0.0.1   0.0.0.0     UG           0 0      0 eth0
root@ubuntu:~#
```

### 9.3 Braucht ein Drucker ein Gateway?

Ja! Wenn der Drucker in einem anderen Subnet liegt!

## Stichwortverzeichnis

Anwendungsserver.....	7	Mailserver.....	7
Dateiserver.....	7	netstat.....	21
Dateisysteme1.....	10	nslookup.....	15
DFS.....	18	NTFS.....	10
DFS-Zielen.....	18	4Protokolle.....	14
DHCP.....	17	Nicht routbare.....	14
DHCP-Relay-Agent.....	17	Routbare.....	14
DHCP-Server.....	8	Raid.....	6
DNS.....	17	RAS/VPN Server.....	8
DNS-Server.....	8	Redundanz.....	6
Domänencontroller.....	8	Ressource-Records.....	16
Domänenstamm.....	18	route print.....	21
Drucker.....	22	Script.....	12
Druckserver.....	7	Serverarten.....	7
Eigenständiger Stamm.....	18	Sicherung von Daten.....	19
Einsatz von Servern.....	7	SMB.....	11
Eventlog.....	8	1.1.2Software.....	6
ext2-fs.....	11	Betriebssystem.....	6
FAT.....	10	Start of Authority.....	15
FQDN.....	20	Streaming-Media-Server.....	8
FRS (File Replication Service).....	18	Subdomain.....	20
Gateway.....	22	TCP/IP.....	14
Hardware.....	6	Terminalserver.....	7
Host-File.....	17	WINS.....	17
ipconfig.....	21	WINS-Server.....	8