

# Server und Netzwerk – Konfiguration

## **Dokumentenmanagement**

Datum: 19. September 2003

Version: 1.1

Autor: AAC Communications / info@card.ch

Dateiname: Netzwerkdokumentation.pdf

# Inhaltsverzeichnis

## 1 Verzeichnisstruktur

1.1	Installationsort.....	Seite 3
1.2	Festplatten und Partitionen eines Servers.....	Seite 3
1.3	Partition C:.....	Seite 3
1.4	Partition D:.....	Seite 4

## 2 Login

2.1	logon.cmd.....	Seite 5
-----	----------------	---------

## 3 Netzwerkaufbau

3.1	Standart Netzwerkaufbau.....	Seite 6
3.2	IP und DNS Konfiguration des Servers.....	Seite 7
3.3	IP und DNS Konfiguration der Clients via DHCP.....	Seite 7

4	Zugriffsrecht der User.....	Seite 7
---	-----------------------------	---------

5	Virenschutz.....	Seite 8
---	------------------	---------

## 6 Datensicherung

6.1	NT Backup.....	Seite 8
6.2	Backup-Ablauf.....	Seite 8
6.3	Beispiel einer Kontroll-Liste:.....	Seite 9

7	Scripts.....	Seite 10
---	--------------	----------

## 8 Netzwerktopologie

8.1	NT Backup.....	Seite 11
8.2	Backup-Ablauf.....	Seite 12

# 1 Verzeichnisstruktur

## 1.1 Installationsort

Software-Pakete für den Server selbst, werden auf die c:-Partition entweder nach c:\Apps oder nach c:\Programme geladen. Software-Pakete für Benutzer müssen auf die d:-Partition nach d:\Apps geladen und so zur Verfügung gestellt werden.

Sämtliche Log Files des Servers, z.B. die Protokoll Dateien von Active Directory, werden unter d:\data\logs gespeichert.

## 1.2 Festplatten und Partitionen eines Servers

Der Server wird gemäss nachfolgender Tabelle konfiguriert.

Um eine grundlegende Sicherheit der Daten zu gewährleisten verwenden wir Raid Systeme. Mit diesen Systemen kann ein höheres Mass an Datensicherheit gewährleistet werden als es mit einzelnen Festplatte mögliche wäre.

### Gross –RAID

Festplatte	Grösse	RAID-Typ	Partitionen	Zweck / Inhalt
Harddisk 1	18.2 GB	RAID 1	C:	System-Laufwerk enthält Windows Betriebssystem, Infrastruktur-Programme
Harddisk 2	18.2 GB		Grösse: 18.2 GB	
Harddisk 3	36.4 GB	RAID 5	D:	Daten-Laufwerk Persönliche und Firmen Daten
Harddisk 4	36.4 GB		Grösse: 68 GB	
Harddisk 5	36.4 GB			

## 1.3 Partition c:

Im c:-Laufwerk befinden sich das Windows-System, Server - eigene Applikationen und Administrations-Werkzeuge.

Pfad	Zweck	Freigabe/Recht	Sicherheitsrecht
c:\	Root-Verzeichnis	c\$ / -	admin:FC, users:FC
c:\	Weiter div. Hersteller Tools		admin:FC, users:FC
c:\apps	für Server-Software		admin:FC, users:FC
C:\dokumente und einstellungen	Lokale Userprofile des Servers		admin:FC, users:FC
c:\programme	Standard-Windows-Programme		admin:FC, users:FC
c:\util	Administrations-Werkzeuge		admin:FC, users:FC
c:\winnt	Betriebssystem-Pfad	Admin\$ / -	admin:FC, users:FC

## 1.4 Partition d:

Hier befinden sich die Applikationen, sowie deren Installations- und Logdateien. Ausserdem werden sämtliche Daten auf die Partition d geschrieben.

In der Profiles\$-Freigabe befinden sich die Profildaten aller Benutzer, die sich an diesem Server anmelden wollen, und in der Netlogon Freigabe die Logon-Datei für die Laufwerk-Zuweisung. Siehe nachfolgende Tabelle.

Pfad	Zweck	Freigabe/Recht	Sicherheitsrecht	Laufwerk
D:\apps	Installationsverzeichnis der Netzwerksoftware		Admin:FC, users:FC	
D:\apps\<programm>	Installationsverzeichnis der einzelnen Programme	<Programm>\$ Admin: FC, Users: FC	Admin: FC Users: FC	Je nach Anwendung
D:\data	Datenverzeichnis auf dem Server		Admin: FC Users: FC	
D:\data\apps-data	Daten von Netzwerksoftware. z.B. Twixtel	apps-data\$ Admin: FC, Users: R	Admin: FC Users: FC	
D:\data\global	Globale Daten und Vorlagen	global\$ Admin: FC, Users: R	Admin: FC Users: FC	X
D:\data\groups\	Gemeinsame Dateiablage der Abteilungen / Firmen	groups\$ Admin: FC, Users: R	Admin: FC Users: FC	
D:\data\groups\<gid>	Verzeichnis der einzelnen Firmen / Abteilungen	Admin: FC, Users: R	Admin :FC Users: R	G
D:\data\logs	Logdateien des Servers		Admin: FC	
D:\data\profiles	Profile der User	profiles\$ Admin FC, Users: FC	Admin: FC Users: FC	
D:\data\remote	Installations Files z.B. Office	remote\$ Admin FC, Users: R	Admin: FC Users: FC	
D:\data\sysvol	Domain Ordner	Sysvol Admin: FC, Users: R	Admin: FC Users: R	
D:\data\sysvol\sysvol\muster1.de\scripts	Weiterer Domain – Ordner. Zugriffspfad für Logon Scripts	Netlogon Admin: FC, Users: R	Admin: FC Users: R	
D:\data\Temp	Ordner für temporären Datenaustausch	temp\$ Admin: FC, Users: FC	Admin: FC Users: FC	
D:\data\users	Persönliche Dateien der User	users\$ Admin: FC, User: FC	Admin: FC Users: FC	
D:\data\users\<pid>	Persönlicher Ordner des Users <pid>	Admins:FC, <pid>: FC	Admin: FC <pid>: FC	H

Oft genutzte Installationen ( Office, Twixtel, Druckertreiber etc. ) befinden sich im data\remote Verzeichnis.

Über den Ordner data\global werden Anleitungen, Vorlagen usw. dem User zur Verfügung gestellt.

Der Ordner data\temp dient dem Datenaustausch zwischen den Usern und wird regelmässig mit einer Routine jedes Wochenende geleert.

Damit ein Benutzer mit über fest zugewiesenen Laufwerken (mapped Drives) auf seine Daten zugreifen kann, werden einem Benutzer beim Anmelden folgende Laufwerksbuchstaben fest zugewiesen:

Freigabe	Pfad	Zweck	Laufwerk
groups\$\<gruppe>	d:\data\groups\	Gemeinsame Datenablage für Abteilungen	G:
Users\$\<pid>	d:\data\users\<PID>	persönliches Datenverzeichnis eines Benützers	H:
temp\$	d:\data\temp	temporärer Datenaustausch unter den Abteilungen	T:
gobal\$	d:\data\global	Globale Daten und Vorlagen	X:

Die Zuweisung dieser Laufwerke erfolgt während des Anmeldens eines Benützers.

## 2 Login

Damit die verbunden Laufwerke jedes Users und seiner Gruppe nicht bei jedem Neustart von Hand wiederhergestellt werden müssen verwenden wir so genannte Loginscripts.

Mit diese Scripts haben wir die Möglichkeit eine Reihe von Befehlen schon beim Systemstart bzw. der Anmeldung auszuführen.

Damit wird uns die Möglichkeit gegeben das ein User auch an einer anderen Workstation nicht auf sein gewohntes Arbeitsumfeld ( persönliche Daten, Gruppen- bzw. Abteilungsdaten usw. ) verzichten muss.

Im Verlauf Beschreibe ich den wichtigsten Scripts logon.cmd

### 2.1 logon.cmd

Das Loginscript liegt im Verzeichnis d:\data\sysvol\sysvol\muster1\scripts auf den Domain Controllern. Es wird über den Share NETLOGON durch Windows 2000 automatisch aufgerufen. Ausserdem befindet sich die Datei ifmember.exe ebenfalls dort.

```
echo OFF
REM _____
REM
REM File:      Logon.cmd
REM Version:   1
REM Date:      19.08.2003
REM Author:    AAC Communications
REM
REM Login Script Start in den Gruppenrichtlinien
REM _____

net use h: \\muster-server-2k3\users$\%username% /persistent:no
net use k: \\muster-server-2k3\apps$\europa3000 /persistent:no
net use t: \\muster-server-2k3\temp$ /persistent:no
net use x: \\muster-server-2k3\global$ /persistent:no

rem Abfrage Gruppe MUSTER

\\muster-server-2k3\netlogon\ifmember MUSTER
if errorlevel 1 goto log_muster

rem Sprung zu :log_muster

rem Abfrage Gruppe Muster2

\\muster-server-2k3\netlogon\ifmember muster2
if errorlevel 1 goto log_muster2

goto END

rem Login Gruppe MUSTER
:log_muster

net use l: \\muster-server-2k3\europa_kunden
```

```
net use m: \\muster-server-2k3\daten /persistent:no

rem Abfrage ob user00. Wenn erfolgreich Sprung zu user00
if /i %username%==user00 goto user00
if /i %username% neq user00 goto rest

goto END

rem Spezial User00
:user00
net use g: \\muster-server-2k3\groups$ /persistent:no

goto END

rem alles anderen user
:rest

net use g: \\muster-server-2k3\groups$\muster_com /persistent:no

goto END

rem Login Gruppe Muster2
:log_muster2

net use g: \\muster-server-2k3\groups$\muster2 /persistent:no
goto END

:END
```

Funktionsweise:

Als erstes Prüft der Script ob der User in Gruppe MUSTER oder Muster2 ist. Wenn er in der Gruppe MUSTER sein sollte springt er zu log\_muster und fährt dort weiter. Sollte er aber nicht in der Gruppe MUSTER sein sondern nur in der Gruppe Muster2 so springt der Script zu :log\_muster2.

## 3 Netzwerkaufbau

### 3.1 Standart Netzwerkaufbau

Um eine Einheit bei unseren Kunden zu erreichen vergeben wir die IP Adressen anhand eines Schemas. dieses Schema sieht wie folgt aus.

Maschinen - Typ	IP - Pool
Server ( statisch )	192.168.x.002 - 192.168.x.029
Printserver ( statisch )	192.168.x.030 - 192.168.x.045
Gateway ( statisch )	192.168.x.046 - 192.168.x.050
Client Rechner ( statisch oder dynamisch )	192.168.x.051 - 192.168.x.249
Support – Bereich	192.168.x.250 - 192.168.x.254

## 3.2 IP und DNS Konfiguration des Servers

Da der muster-server-2k3 sowie Domain-Kontroller wie auch ein DNS Server ist benötigen wir in der Netzwerkkonfiguration keine weiteren DNS Server.

Er leitet DNS Anfragen, die er nicht beantworten kann ( aus der Datenbank oder dem Cache ), an die im DNS Server vorkonfigurierten Adressen weiter.

Das Netzwerk im Server sieht folgendermassen aus:

### 1. Netzwerkkarte ( Trust Zone = inneres Netz )

IP - Adresse	= 192.168.1.2
Subnetz	= 255.255.255.0
DNS Weiterleitung	= 81.221.250.10 ( dns1.green.ch ) im DNS Server definiert. 195.186.1.111 ( dns2.bluewin.ch )

## 3.3 IP und DNS Konfiguration der Clients via DHCP

Wegen des wesentlich einfacheren Handlings bekommen die Clientrechner die IP-Adresse und weitere Daten per DHCP-Server vom muster-server-2k3 zugeteilt.

Der Pool beginnt mit 192.168.1.51 und endet bei 192.168.1.249. Das heisst es ist möglich max. 249 Clients einzubinden.

DNS Server und Gateway werden wie folgt verteilt.

### Standard Client Konfiguration

Subnet	= 255.255.255.0
Gateway	= 192.168.1.x
DNS Server	= 192.168.1.2

## 4 Zugriffsrecht der User

Wie schon weiter oben beschrieben Beschränken wir den Zugang zu den einzelnen Freigaben ( nur der User darf auf sein Verzeichnis zugreifen usw. )

Ausserdem Vergeben wie je nach User verschiedene Sicherheitslevel.

Je nach Level kann er einige Einstellungen im Windows nicht ändern.

Alle User bekommen die Normalen Domain-Benutzer Rechte.

Sie können Ihren PC ihren persönlichen wünschen Anpassen, Stossen aber bei Softwareinstallationen oder ähnlichen Dingen schnell an ihre Grenzen.

Diese Massnahmen sollen keine Schikane sein. Sie dienen in erster Linie dem Schutz des Users.

## 5 Virenschutz

Alle Server und Clients müssen mit einem aktuellen Anti-Viren-Programm geschützt sein.

Auf den Server läuft der Norman Antivirus welcher sich selbstständig via Internet aktualisiert.

Dies geschieht im Normalfall 1 mal am Tag. Ausserdem stellt er den Clients die aktuellsten Virus Definitionen und Programmupdates via Netzwerk zur Verfügung. Diese überprüfen stündlich den Server und aktualisieren sich wenn nötig.

Der Norman Antivirus wird ins Verzeichnis d:\apps\norman installiert. Damit die Clients aktualisiert werden können, wird der Ordner mit norman\$ freigegeben.

## 6 Datensicherung

Trotz des oben erwähnten Raid Verfahrens müssen Ihre Daten täglich gesichert werden. Aufgrund von Geschwindigkeit und Grösse der zu sichernden Daten haben sich hier AIT Laufwerke bewährt.

Des Weiteren sollte darauf geachtet werden das sich immer ein Sicherungssatz ausser Haus befindet damit im Falle eines Unglücks (z.B. Feuer im Gebäude) diese Daten auch noch vorhanden wären.

### 6.1 NT Backup

Die Datensicherung mit dem NT Backup auf Band erfolgt täglich Montag bis Freitag um 21.00 Uhr.

Wird ein Standardserver neu installiert, kann es vorkommen dass das Laufwerk vom NT Backup nicht erkannt wird. In diesem Fall muss erst der Dienst Wechselmedien aktiviert und auf automatisch starten gestellt werden.

Wir führen bei den täglichen Backups immer ein komplettes Backup des Datenlaufwerks ( Laufwerk D ) durch. Einmal im Monat wird ein Komplettbackup des Servers durchgeführt und das Tape ausser Haus gelagert.

In den meisten Fällen reicht eine geschedulte Backuplösung mit dem NT Backup.

Da man aber damit keine Disaster Recovery anfertigen kann, wird in den Fällen wo es nötig ist Backup Exec von Veritas eingesetzt.

### 6.2 Backup-Ablauf

Der Backupverantwortlicher, dessen Aufgabe es ist täglich die Bänder anhand des Planes zu wechseln und das Backup zu kontrollieren, muss bei Unstimmigkeiten sofort Meldung zu machen.

Eine normale Backupwoche sieht wie folgt aus.

Montag:	Band Freitag entnehmen Log kontrollieren einlegen Band Montag	Donnerstag:	Band Mittwoch entnehmen Log kontrollieren einlegen Band Donnerstag
Dienstag:	Band Montag entnehmen Log kontrollieren einlegen Band Dienstag	Freitag:	Band Donnerstag entnehmen Log kontrollieren einlegen Band Freitag
Mittwoch:	Band Dienstag entnehmen Log kontrollieren einlegen Band Mittwoch		

Am letzten Freitag im Monat sieht das ganze etwas anders aus.

Nach der Entnahme des Donnerstag Bandes wird als erstes das Reinigungsband eingelegt.

Nachdem dies wieder ausgeworfen wurde, wird das Monatsband eingelegt. Nach dem Backup wird dieses Band wieder Ausserhaus gelagert und normal gemäss Kontrollliste weitergemacht.

### 6.3 Beispiel einer Kontroll-Liste

Diese oder eine ähnliche Liste sollte im Serverraum zur Kontrolle hängen.

<b>Montag:</b>	neue Kontroll-Liste ausdrucken und aufhängen Band Freitag entnommen Log kontrolliert Band Montag eingelegt	
	Alles kontrolliert und ok. Datum / Visum	_____
<b>Dienstag:</b>	Band Montag entnehmen Log kontrolliert Band Dienstag eingelegt	
	Alles kontrolliert und ok. Datum / Visum	_____
<b>Mittwoch:</b>	Dienstag entnehmen Log kontrolliert Band Mittwoch eingelegt	
	Alles kontrolliert und ok. Datum / Visum	_____
<b>Donnerstag:</b>	Band Mittwoch entnehmen  Log kontrolliert Band Donnerstag eingelegt	
	Alles kontrolliert und ok. Datum / Visum	_____
<b>Freitag:</b>	Band Donnerstag entnehmen Monatsbackup Log kontrolliert Band Freitag eingelegt	Ja / Nein
	Alles kontrolliert und ok. Datum / Visum	_____

## 7 Scripts

Ein weiter Script der automatisch ausgeführt wird ist dieser. Er leert das Temp Verzeichnisses.

```
@echo OFF
REM _____
REM
REM File:      deltmp.cmd
REM Version:   1
REM Date:     11.05.2003
REM Author:   AAC Communications
REM
REM _____
```

```
Echo J | rd d:\data\temp /s
```

```
md d:\data\temp
```

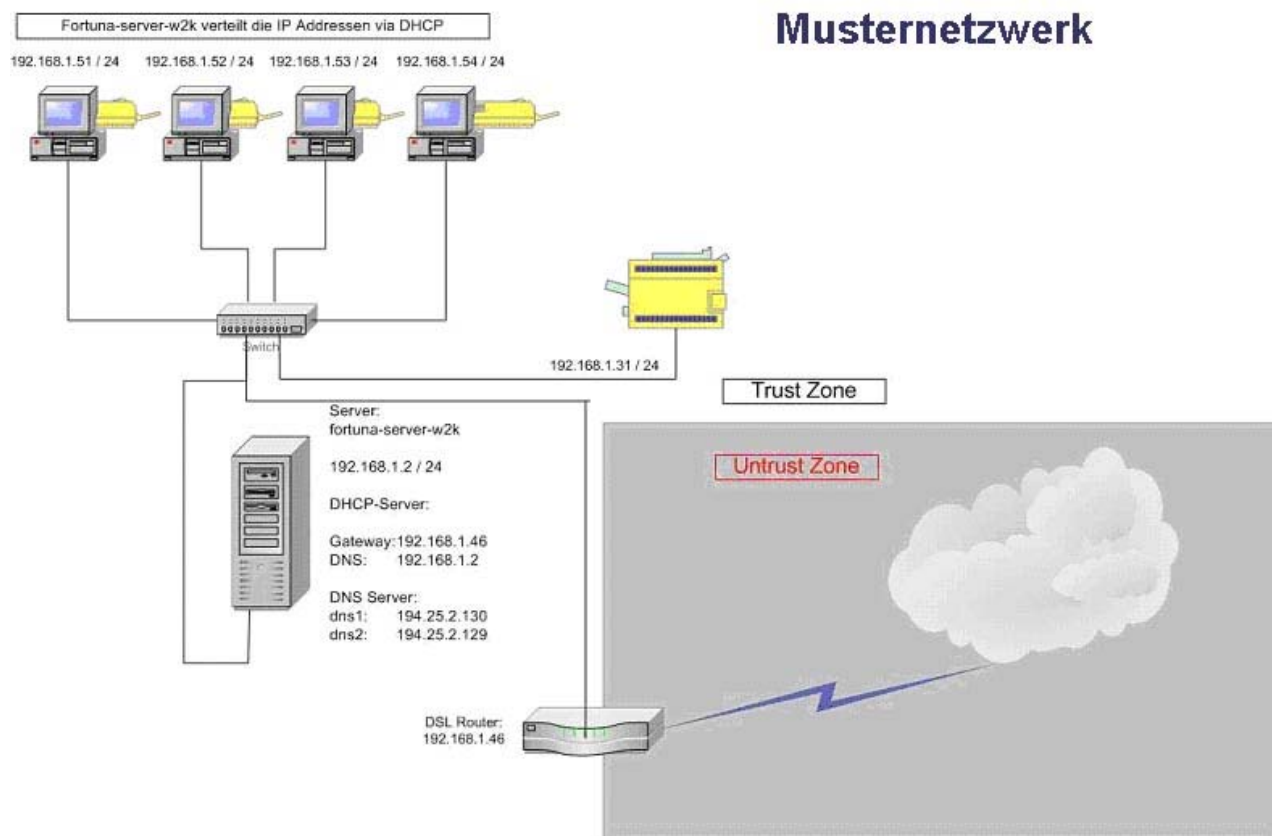
Funktionsweise:

Dieser Script wird über den Scheduler wöchentlich einmal aufgerufen.

Erst löscht er das Verzeichnis d:\data\temp mit dem kompletten Inhalt ( das echo J | bewirkt das jede abfrage mit j beantwortet wird ) und erstellt ihn dann wieder.

## 8 Netzwerktopologie

### 8.1 Netzwerktopologie ohne Firewall



## 8.2 Netzwerktopologie mit Firewall

