

EM AG

# Server & Dienste

Betriebsdokumentation einer Systemumgebung

Mirio Eggmann  
Februar & März 2015

# Inhaltsverzeichnis

Abbildungsverzeichnis.....	2
Tabellenverzeichnis.....	3
Server Grundlagen.....	4
Hardware und Software .....	4
Installation und Konfiguration .....	5
Updates .....	9
Energieeffizienz.....	9
Netzplan.....	10
Backup.....	11
RAID.....	13
Server Dienste.....	15
AD DS .....	15
Print-Server.....	18
Routing .....	18
IIS.....	19
DNS.....	21
DHCP .....	23
FSRM.....	25
GPO.....	26
Ressourcenverwaltung.....	28
Shares.....	28
IGDLA.....	29
Benutzerprofile .....	30
Reorganisation / Migration.....	31
Netzwerktools.....	31
Scripting.....	33
PowerShell.....	33
Servertool.....	34
Eventlog auswerten (Event Viewer -> eventvwr).....	34
Remotedesktop (mstsc.exe).....	34
Computermanagement.....	34
Performance Monitor (Perfmon.exe).....	34
Registry .....	35
MMC .....	35
RSAT-Tools.....	35
Netzsicherheit.....	36
Schwachstellen .....	36
Virenschutz.....	36
Passwort .....	36
Administrator / root Konto.....	37
Benutzer Authentifizierung .....	37

## Abbildungsverzeichnis

Abbildung 1 Netzplan.....	10
Abbildung 2 Voll Backup.....	11
Abbildung 3 Differenzielles Backup .....	11
Abbildung 4 Inkrementelles Backup.....	11
Abbildung 5 RAID 0.....	13
Abbildung 6 RAID 1.....	13
Abbildung 7 RAID 5.....	13
Abbildung 8 RAID 6.....	14
Abbildung 9 RAID 10.....	14
Abbildung 10 Pool.....	14
Abbildung 11 Enhanced Security Configuration.....	15
Abbildung 12 Ordnerstruktur.....	17
Abbildung 13 OU (Organisation Unit) .....	17
Abbildung 14 Print Share .....	18
Abbildung 15 Routing Weg.....	18
Abbildung 16 DHCP Verlauf .....	23
Abbildung 17 FSRM - Quotas.....	25
Abbildung 18 FSRM - File Screening.....	25
Abbildung 19 FSRM - Storage Report.....	25
Abbildung 20 GPO Laufwerk-verbinden Einstellungen / Item-level targeting / Laufwerke.....	27
Abbildung 21 IGDLA.....	29
Abbildung 22 Benutzerprofile.....	31
Abbildung 23 Reorganisation .....	31
Abbildung 24 MMC .....	35

# Tabellenverzeichnis

Tabelle 1 Hardware und Software - Allgemein .....	4
Tabelle 2 Hardware und Software - Server mit GUI.....	4
Tabelle 3 Hardware und Software - Server ohne GUI (Core).....	4
Tabelle 4 Hardware und Software – PC .....	4
Tabelle 5 Hardware und Software – Webserver.....	4
Tabelle 6 Konfiguration - GUI Server.....	5
Tabelle 7 Konfiguration - CORE Server.....	6
Tabelle 8 Konfiguration - Windows 7 Client.....	7
Tabelle 9 Konfiguration - Debian.....	8
Tabelle 10 Updates.....	9
Tabelle 11 AD DS - Einstellungen.....	15
Tabelle 12 Benutzer - Ausbildner.....	16
Tabelle 13 Benutzer - Lernende .....	16
Tabelle 14 Print Server Einstellungen.....	18
Tabelle 15 Installations Logbuch.....	19
Tabelle 16 DNS Reverse Lookup Zone - Records .....	21
Tabelle 17 DNS Forward Lookup Zone - Records.....	22
Tabelle 18 Forward Lookup Zonen.....	22
Tabelle 19 Reverse Lookup Zonen.....	22
Tabelle 20 Listening Interfaces / Forwarding .....	22
Tabelle 21 DHCP Begriffe .....	23
Tabelle 22 DHCP Einstellungen.....	24
Tabelle 23 FSRM Begriffe.....	25
Tabelle 24 NTFS Berechtigung.....	28
Tabelle 25 Beispiel Berechtigungen .....	28
Tabelle 26 IGDLA Matrix.....	30
Tabelle 27 Netzwerkdienste.....	32
Tabelle 28 PowerShell.....	33

# Server Grundlagen

## Hardware und Software

Alle PC's und Server laufen auf virtuellen Maschinen und teilen sich somit die Ressourcen eines DELL Laptops, wie die CPU Leistung, RAM etc.

### Allgemein

Hardware	Software
1x Switch - ZyXEL GS1920-48	1x Oracle VM VirtualBox Manager

Tabelle 1 Hardware und Software - Allgemein

### Server mit GUI

Hardware	Software
1x RAM 2GB (Virtuell)	1x Windows Server 2012R2
1x CPU – Intel Core i7-4600M	1x UnThreat Virenschutz
1x HDD – 45GB (Virtuell)	1x PDF Creator
1x Grafikkarte –AMD Radeon HD 8790M	
2x NIC – Intel PRO/1000 MT Desktop	

Tabelle 2 Hardware und Software - Server mit GUI

### Server ohne GUI (Core)

Hardware	Software
1x RAM 1GB (Virtuell)	1x Windows Server 2012R2
1x CPU – Intel Core i7-4600M	1x UnThreat Virenschutz
1x HDD – 25GB (Virtuell)	
1x Grafikkarte –AMD Radeon HD 8790M	
1x NIC – Intel PRO/1000 MT Desktop	

Tabelle 3 Hardware und Software - Server ohne GUI (Core)

### PC

Hardware	Software
1x RAM 512MB (Virtuell)	1x Windows 7 Enterprise 32bit
1x CPU – Intel Core i7-4600M	1x UnThreat Virenschutz
1x HDD – 25GB (Virtuell)	
1x Grafikkarte –AMD Radeon HD 8790M	
1x NIC – Intel PRO/1000 MT Desktop	

Tabelle 4 Hardware und Software – PC

### Webserver

Hardware	Software
1x RAM 512MB (Virtuell)	1x Debian 7.7
1x CPU – Intel Core i7-4600M	
1x HDD – 2GB (Virtuell)	
1x Grafikkarte –AMD Radeon HD 8790M	
1x NIC – Intel PRO/1000 MT Desktop	

Tabelle 5 Hardware und Software – Webserver

## Installation und Konfiguration

### GUI Server

Ich habe beim GUI Server zwei Netzwerkkarten eingebaut und zwar eine als NAT Interface um auf das Internet zu kommen und die andere als Internes Netzwerk, damit er als eine Art Router spielen kann. Weiter hat dieser Server 2GB Ram und eine 45GB HDD und eine 5GB HDD und auch noch ein paar Disks zum testen von den verschiedenen RAID Formen. Als Betriebssystem wurde Windows Server 2012R2 64bit eingesetzt.

Der GUI Server wurde mit den Standardeinstellungen installiert. Weiter wurde dieser Server als Domain Controller gewählt. Es wurde noch die Hide Protection und das Ausblenden der Endungen von Dateien deaktiviert. IPv6 wurde deaktiviert, weil es in diesem Netzwerk nicht von Nutzen ist.

Hostname:	SRV-BEGGMM-GUI
Domain/Workgroup:	MeineFirma.local
IP:	Internes Netzwerk: 192.168.1.10 NAT: 10.0.2.15
Subnetz:	255.255.255.0
Netzadresse:	192.168.1.0
DNS-Server:	127.0.0.1
Standard-Gateway:	192.168.1.10
Zeitzone:	(UTC+01:00) Amsterdam, Berlin, Bern...
Sprache:	Englisch
Tastaturlayout:	Deutsch (Schweiz)
Update:	Manuell
Dienste:	DNS, AD DS, FSRM, DHCP, DC, GPO, Print Server, IIS, Routing, Backup
Produkt ID:	BEFCC8B5-4380-4FAC-9084-11895C4CB4DF
Betriebssystem:	Windows Server 2012 R2 GUI
Virenschutz:	UnThreat Virenschutz
Partitionen:	<b>Disk 0: 45GB</b> -System Reserved 350MB NTFS - System -(C:) 35GB NTFS – Betriebssystem -(E:) 5GB NTFS – Groupdata -(F:) 5GB NTFS - Userdata <b>Disk 1: 5GB</b> -(D:) 5GB NTFS – Printer <b>Disk 2-7:10GB (Testzwecke RAID)</b>
Lokale Administrator:	Login: Administrator Passwort: Welcome\$15

Tabelle 6 Konfiguration - GUI Server

## Core Server

Der GUI Server besitzt nur eine Netzwerkkarte und zwar eine „Internes Netzwerk“ NIC. Der Core Server besitzt nur 1 GB Ram, weil er ohne GUI betrieben wird. Speicher hat dieser auch nur 25GB, weil er als 2. Server dient. Als Betriebssystem wurde Windows Server 2012R2 64bit verwendet.

Beim Core Server wurde die Installation zuerst mit einem GUI gemacht, damit dies später ohne Probleme installiert und deinstalliert werden kann. Direkt nachdem die Grundeinstellungen vorgenommen wurden, habe ich das GUI wieder deinstalliert

*Command: Uninstall-WindowsFeature Server-Gui-Shell*

und die Einstellungen über Powershell vorgenommen. Im Powershell wurde IPv6 deaktiviert.

*Command: sconfig (in Powershell)*

Hostname:	SRV-BEGGMM-CORE
Domain/Workgroup:	MeineFirma.local
IP:	Internes Netzwerk: 192.168.1.11
Subnetz:	255.255.255.0
Netzadresse:	192.168.1.0
DNS-Server:	192.168.1.10
Standard-Gateway:	192.168.1.10
Zeitzone:	(UTC+01:00) Amsterdam, Berlin, Bern...
Sprache:	Englisch
Tastaturlayout:	Deutsch (Schweiz)
Update:	Manuell
Dienste:	DHCP, DNS
Produkt ID:	00252-70000-00000-AA535
Betriebssystem:	Windows Server 2012 R2 Core
Virenschutz:	UnThreat Virenschutz
Partitionen	Disk 0: 25GB -System Reserved 350MB NTFS – System -(C:) 25GB NTFS - System
Lokale Administrator:	Login: Administrator Passwort: Welcome\$15

Tabelle 7 Konfiguration - CORE Server

## Windows Client

Der Windows 7 Client wurde mit der minimal Anforderung von 512MB Ram installiert. Daher wurde auch nur eine 32bit Version eingesetzt. Weiter besitzt dieser PC nur eine NIC mit dem Standard Internes Netzwerk. Bei den Adaptereinstellungen wurde IPv6 deaktiviert und die Einstellungen der IP und des DNS Server etc. wurden manuell vergeben.

Hostname:	BEGGMM-PC
Domain/Workgroup:	MeineFirma.local
IP:	Internes Netzwerk: 192.168.1.101 (Reservation DHCP)
Subnetz:	DHCP
Netzadresse:	DHCP
DNS-Server:	DHCP
Standard-Gateway:	DHCP
Zeitzone:	(UTC+01:00) Amsterdam, Berlin, Bern...
Sprache:	Deutsch
Tastaturlayout:	Deutsch (Schweiz)
Update:	Manuell
Dienste:	-
Produkt ID:	00392-918-5000002-85125
Betriebssystem:	Windows 7 Enterprise 32bit
Virenschutz:	UnThreat Virenschutz
Partitionen	<b>Datenträger 0: 25GB</b> -System reserviert 100MB NTFS – System -(C:) 25GB NTFS - Betriebssystem
Lokale Administrator:	Login: Beggmm Passwort: Welcome\$15

Tabelle 8 Konfiguration - Windows 7 Client

## Debian Webserver

Der Debian Webserver besitzt nur 512MB RAM, weil nur eine Webseite auf dieser Maschiene läuft. Es wurde ein opensource Debian 7.7 installiert.

Hostname:	BEGGMM-PC
Domain/Workgroup:	MeineFirma.local
IP:	Internes Netzwerk: 192.168.1.15 (Reservation DHCP)
Subnetz:	DHCP
Netzadresse:	DHCP
DNS-Server:	DHCP
Standard-Gateway:	DHCP
Zeitzone:	(UTC+01:00) Amsterdam, Berlin, Bern...
Sprache:	Deutsch
Tastaturlayout:	Deutsch (Schweiz)
Update:	Manuell
Dienste:	Apache2
Produkt ID:	-
Betriebssystem:	Debian 7.7
Virenschutz:	-
Partitionen	<b>Datenträger 0: 2GB</b> - Betriebssystem
Lokale Administrator:	Login: root Passwort: Welcome\$15

Tabelle 9 Konfiguration - Debian

## Updates

Host	Letzte Updates
SRV-BEGGMM-GUI	19.12.2014
SRV-BEGGMM-CORE	19.12.2014
BEGGMM-PC	22.12.2014

Tabelle 10 Updates

Das automatische Updaten der Server und des PC's wurde deaktiviert um allfällige Inkompatibilitäten zu verhindern. Daher muss dies der System Admin manuell durchführen, wenn er sicher ist, dass das Update voll kompatibel ist.

## Energieeffizienz

Die Energieeffizienz ist bei den beiden Servern sehr hoch, weil sie beide über einen Laptop laufen, welcher nicht viel Strom braucht. Daher ist aber auch die Leistung ein wenig beschränkt.

### Formel für den Strompreis in CHF pro x Stunden

$$\frac{\text{Anzahl Watt}}{\text{Wirkungsgrad}} * \frac{\text{Anzahl h}}{1000} * \text{Energiekosten(CHF)/kWh}$$

### Ausrechnung Energieeffizienz Laptop

$$\frac{90}{0.65} * \frac{1}{1000} * 0.22 = 0.03 \text{ Rappen pro Stunde}$$

## USV

Dieser Server besitzt eine Art USV (Unterbrechungsfreie Stromversorgung) und zwar eine Laptopbatterie, welche die beiden Server 2 Stunden aufrecht halten kann.

### Offline USV

Diese Modelle leiten den Strom im Normalbetrieb direkt an den Ausgang weiter. Bei einem Ausfall kann es zu einer Verzögerung von bis zu 10ms geben bis es einsetzt.

### Netzinteraktive USV

Die Umschaltung bei einem Ausfall dauert nur ca. 2-4ms. Weiter schützt es auch vor Unterspannung und Überspannung.

### Online USV

Schaltet ohne Verzögerung ein und schützt vor Überspannung, Unterspannung, Schwankungen der Frequenz und vor Oberschwingungen.

Zuhause würde ich mich persönlich für eine Offline USV entscheiden, weil ein NAS die paar ms sicher Aushält, weiter ist dies auch viel billiger. In einem Betrieb würde ich aber eine Online USV einsetzen, denn dort darf so etwas nicht passieren und die anderen Features sind sicher auch noch von Vorteil.

Beschreibung zu USV und Auswahl: [Link zum Dokument](#)

Excel Dokument: [Link zum Dokument](#)

# Netzplan

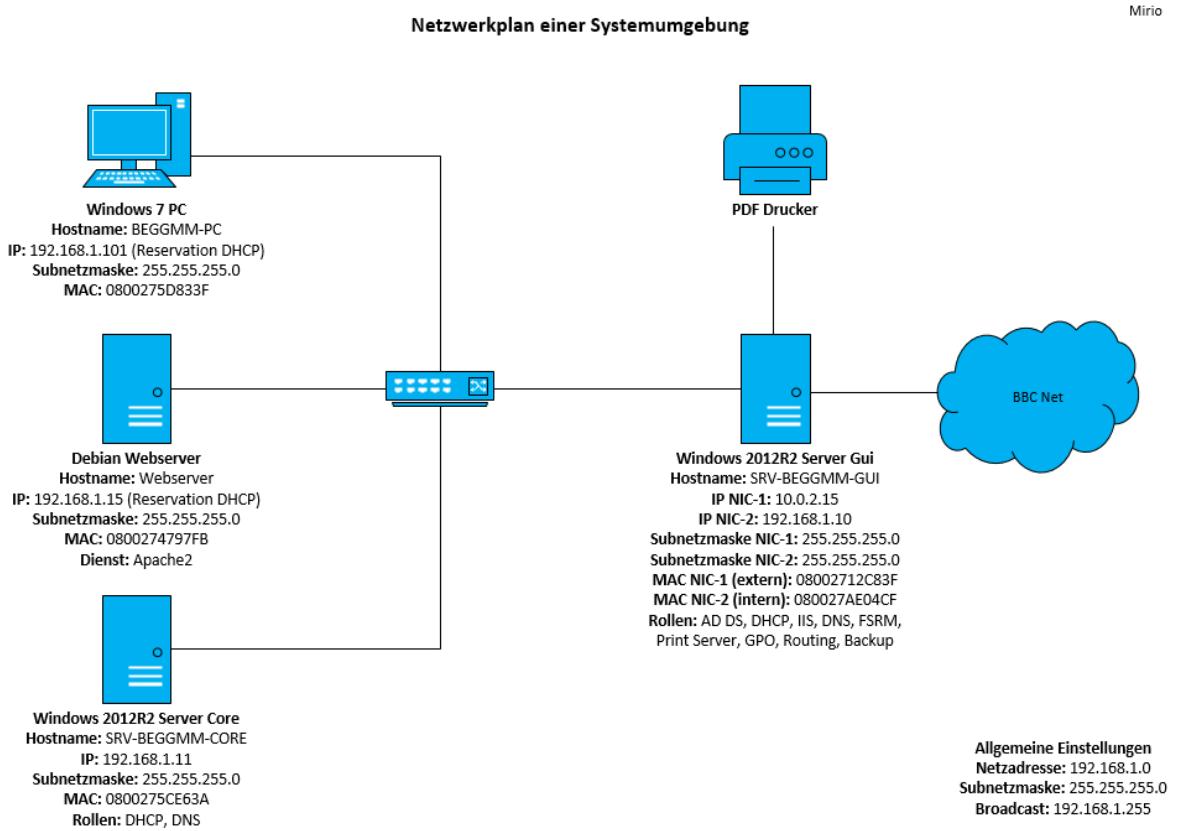


Abbildung 1 Netzplan

## Backup

Datensicherungen werden erstellt, damit man bei einem Ausfall nicht alle Daten einfach verliert.

### Voll Backup

Es gibt 2 unterschiedliche vollständige Backups und zwar die Vollsicherung, welche Daten wie Laufwerke, Partitionen, bestimmte Dateiformate sichert und die Abbildsicherung, die ein 1:1 Abbild vom Datenträger macht (Programme, Betriebssystem)



Abbildung 2 Voll Backup

- + Einfache Wiederherstellung
- Benötigt sehr viel Platz!

### Differenzielles Backup

Bei dieser Backup Methode wird nur einmal ein Fullbackup gemacht (es können auch mehrere) und danach werden beim nächsten Backup nur die Änderungen gespeichert. Beim nächsten werden die Änderungen vom letzten Mal + die neuen Änderungen gespeichert. Dies geht dann immer so weiter und um ein Backup wiederherzustellen benötigt man das letzte Fullbackup + den letzten Differenz Punkt.

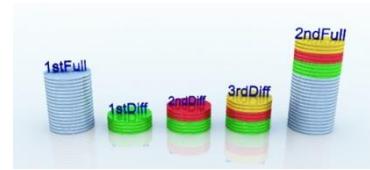


Abbildung 3 Differenzielles Backup

- + Weniger Platzbedarf als Full-Backup
- Mehr Platzbedarf als Incremental

### Inkrementelles-Backup

Diese Version von Datensicherung benötigt im Vergleich zu den anderen sehr wenig Platz, denn es muss nur einmal ein ganzer Sicherungspunkt gemacht werden und danach werden bei jedem Backup nur noch die Änderungen gespeichert und nicht noch die alten Änderungen. Um das Backup wiederherzustellen benötigt man jedoch jeden einzelnen Sicherungspunkt.



Abbildung 4 Inkrementelles Backup

- + Benötigt wenig Speicherplatz
- Restore benötigt alle Backups zurück bis zum letzten Fullbackup!

## Disaster Recovery

Ein Disaster Recovery wird erstellt, damit man im schlimmsten Fall (Naturkatastrophe etc.) sein System trotzdem wiederherstellen kann. Dies sollte wie auch das Backup extern gemacht werden.

### Disaster Verhindern:

- System Überwachen
- Backup machen
- Serverhardware verwenden
- Raid erstellen
- Redundanz von wichtigen Systemen
- Mehrere Standorte
- SLA's definieren

Man sollte eine Planungskommission einrichten und eine Risikoanalyse durchführen. Weiter sollte man Prioritäten festlegen und ein Recovery Konzept bestimmen. Eine Datensammlung könnte auch noch durchgeführt werden und von Vorteil ist noch eine Anleitung oder ein Handbuch zu schreiben. Man sollte Testkriterien – und Vorgehensweisen entwickeln und den Recovery-Plan durchspielen. Den Plan genehmigen und abnehmen lassen.

## Planung

- Recovery Plan erstellen
- Inventar erstellen
- Die Prioritäten für das System / die Dienste definieren
- Systemhandbücher erstellen und aktuell halten
- Das gesamte Konzept auch mal testen
- Ein Dokument erstellen und verfügbar ablegen

Falls ein Disaster Auftritt sollte man Ruhe bewahren und genau nach dem Konzept vorgehen.

## Speichermedien

- Externe Festplatten
- USB Stick
- Cloud
- NAS
- Shares
- Magnetband
- CD / DVD / Blueray
- RDX Cartidges

## Einstellungen auf dem Windowsserver

Zuerst muss man auf dem Windows Server ein Feature hinzufügen und zwar Windows Server Backup. Danach kann man dies über diesen Namen öffnen.

Unter *Windows Backup -> Local Backup -> Backup Schedule* wurde ein Backup Plan eingerichtet, welcher jeden Tag um 1 Uhr in der Nacht (als Testzwecke um 10 Uhr am Morgen) eine Sicherung vom Laufwerk F: (mit dem UserProfiles/Homes) auf ein externes NAS ( vVolume als Testzweck) macht.

Ein Backup kann Wiederhergestellt werden, indem man unter *Windows Backup -> Action -> Recover* geht und dort das gewünschte Backup wählt.

### Commands:

*wbadmin start backup -> Backup erstellen starten*  
*wbadmin get status*

## RAID

Ein RAID ermöglicht ein Ausfallsicheres System und schnelle Geschwindigkeiten, jedoch bedeutet dies nicht, dass dadurch ein Backup gemacht wird, denn wenn etwas auf einer Platte gelöscht wird, wird dies auch auf den anderen Platten übernommen.

### RAID Versionen

#### Software-RAID

Beim Software RAID wird es von einer Software auf dem lokalen System verwaltet

- + Günstig
- Langsam
- Je nach System schwer wiederherzustellen

#### Hardware-RAID

Dieses RAID wird von spezieller Hardware verwaltet. Entweder man nimmt die günstigere Version welche OnBoard ist oder man kauft eine Erweiterungskarte, die entsprechend viel kosten kann.

- + Schnell
- + Unabhängig vom System
- Teuer

### RAID 0 (Striping / Simple)

Die Daten werden falls Sie nicht zu klein sind auf mehreren Festplatten gespeichert. Jedoch besteht keine Redundanz und wenn eine Platte aussteigt sind diese Daten verloren.

- + Geschwindigkeit
- Ausfallsicherheit

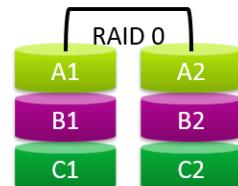


Abbildung 5 RAID 0

### RAID 1 (Mirroring)

Beim RAID 1 werden die Daten Redundant auf mehreren Platten gespeichert. Somit ist nur die Hälfte des gesamten Speichers verfügbar.

- + Ausfallsicherheit
- Geschwindigkeit
- Verlust von Datenvolumen

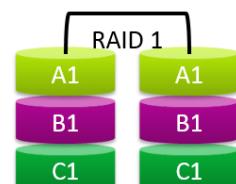


Abbildung 6 RAID 1

### RAID 5 (Parity)

Die Daten werden wie bei RAID 1 auf mehreren Platten gespeichert, jedoch verliert man nur eine Platte und dies ist möglich durch eine sogenannte **Parity**, welche es ermöglicht die Daten wieder zu berechnen.

- + Geschwindigkeit
- + Ausfallsicherheit
- + Geringstmöglicher Volumenverlust
- Es darf nur eine Platte pro Mal ausfallen

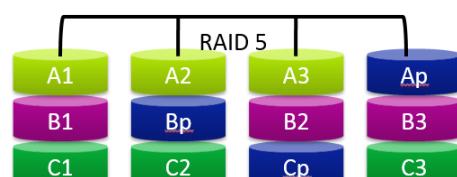


Abbildung 7 RAID 5

## RAID 6

RAID 6 ist eine Erweiterung des RAID 5 und dies ermöglicht, dass eine Platte mehr ausfallen kann, weil es eine Platte mehr mit dem Paritätsbit besitzt.

- + Geschwindigkeit
- + Ausfallsicherheit
- + Geringer Volumenverlust

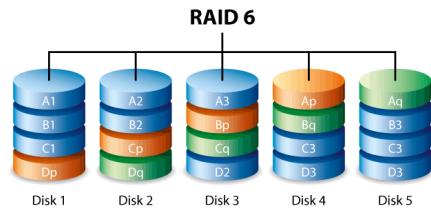


Abbildung 8 RAID 6

## RAID 10

Ein RAID 10 ist eine Kombination zwischen dem RAID 0 und dem RAID 1 es ist eine sogenannte Mischform. Es ermöglicht einen schnellen Datenzugriff und eine grosse Sicherheit, der Verlust vom Datenvolumen ist aber sehr hoch.

- + Geschwindigkeit
- + Ausfallsicherheit
- Verlust von Datenvolumen

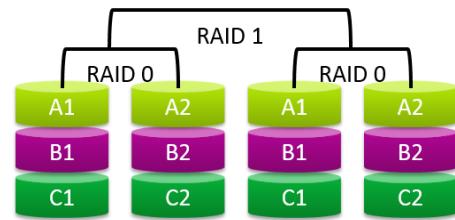


Abbildung 9 RAID 10

## Begriffe:

- GBT: GUID Partition Table (kleinere Platten)
- MBR: Master Boot Record (große Platten)

## Datenträgerverwaltung

### Storage Pool

Ein storage Pool kann verwendet werden um diverse Festplatten mit unterschiedlichen Größen zusammen zu fassen. Der Speichertyp spielt auch keine Rolle.

### Virtual Disk

Man kann Virtuelle Platten erstellen, entweder

**Thin:** Dynamische Festplatte, sie wächst mit oder

**Fixed:** Fest, die Größe der Festplatte ist vorgegeben

### Disks

Übersicht der verschiedenen Disks (vDisk und Normal)

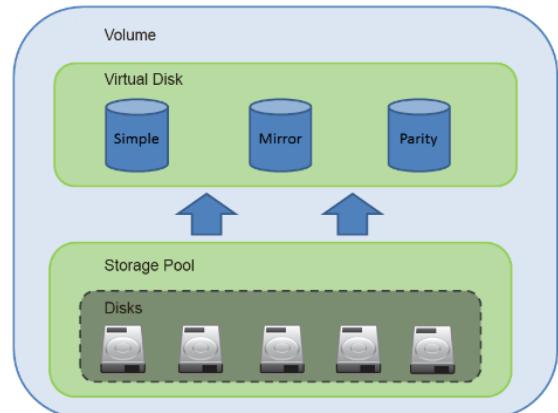


Abbildung 10 Pool

### Volumes

Mit diesem Schritt erstellt man das eigentliche Volume, wie z.B. Laufwerk E:\.

### Server Einstellungen

Vom Volumen E:\ wird jeden Tag um 14:45 Uhr eine Shadow Copy gemacht. Weiter wird auch nach jedem Auftrag ein Sicherungspunkt erstellt, damit ich später dorthin zurückkehren kann. Zu Beginn habe ich vom frisch aufgesetzten Server einen Klon erstellt, damit ich im schlimmsten Fall darauf zurückgreifen kann. Ein spezielles RAID wurde nur zu Testzwecken installiert.

# Server Dienste

## AD DS

### Installation

Vor der AD Installation muss dem Server eine feste IP gegeben und der Hostname passend angegeben werden. Weiter sollte eine Time Zone festgelegt werden und die Enhanced Security Konfiguration ausgeschaltet werden. Nach der Installation der AD DS Rolle (DNS auch, weil dies von AD DS benötigt wird) muss ein Domain Controller promotet (SRV-BEGGMM-GUI) werden und ein „new Forest“ angelegt werden und darunter eine neue Domäne erstellt werden in meinem Fall: MeineFirma.local. Zuletzt muss auch noch ein Restore Passwort definiert werden (in diesem Fall: Welcome\$15).

**Time Zone:** (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

### Enhanced Security Konfiguration

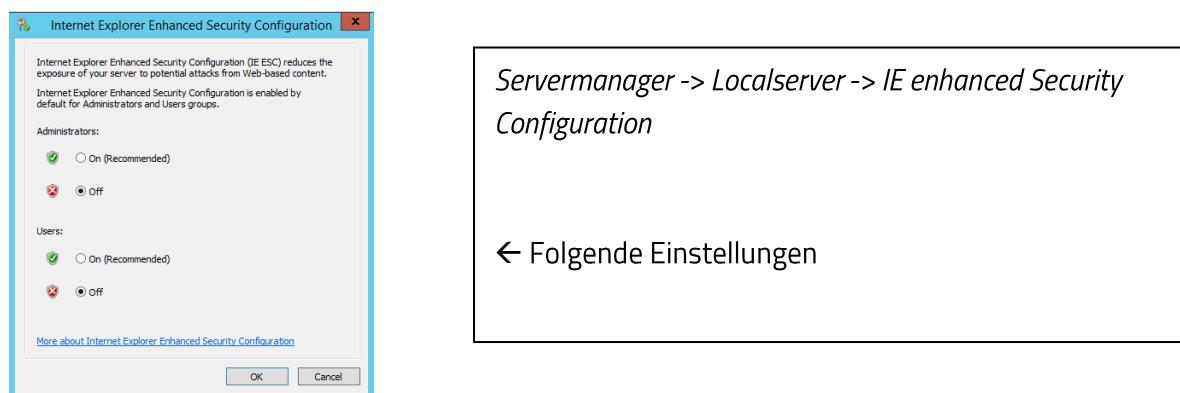


Abbildung 11 Enhanced Security Configuration

### Konfiguration Server

New Forest:	MeineFirma.local
Restore Passwort:	Welcome\$15
NetBIOS:	MEINEFIRMA
<b>Pfade:</b>	
Database	C:\Windows\NTDS
Log files	C:\Windows\NTDS
SYSVOL	C:\Windows\SYSVOL

Tabelle 11 AD DS - Einstellungen

### Objekte

#### Computer

Die Computer benötigt man um diverse Rechte an Computern an verschiedenen Stellen zu vergeben. z.B. das die Benutzer von Gäste PC's aus keinen Zugriff auch die Shares haben. Allgemein benötigt es dieses Objekt, weil man sonst nicht auf die Domäne zugreifen kann.

Bei den Computern sind nur der Core Server, der Webserver und der Windows Client zu sehen.

## **Benutzer und Passwörter**

Benutzer können im AD angelegt werden um Servergespeicherte Profile zu erstellen und um diese zentral zu Verwalten und Berechtigen. Unter Properties kann noch eingestellt werden, dass er sich nur zu einer gewissen Zeit anmelden kann, sein Konto gesperrt ist, das er sein Passwort ändern/nicht ändern/ändern muss oder an welchen PC's er sich einloggen kann. Es können auch noch Passwortrichtlinien in den GPO's eingerichtet werden und UserHomes vergeben werden.

Ausbildner:

Benutzer	Voller Name	Passwort
test	Test	Welcome\$15
test2	Test	Welcome\$15

Tabelle 12 Benutzer - Ausbildner

Lernende:

Benutzer	Voller Name	Passwort
test3	test	Welcome\$15
test4	test	Welcome\$15
...	...	...
test16	test	Welcome\$15

Tabelle 13 Benutzer - Lernende

## **Gruppen**

Ich habe mit 2 Arten von Gruppen gearbeitet und zwar mit globalen Gruppen und mit lokalen Gruppen. Die Shares wurden mit Read & Modify versehen, damit die Berechtigungen ohne Probleme mit NTFS gemacht werden können. Diese Share Berechtigung wurde für die authentifizierten Users gemacht.

### **Globale Gruppen:**

Die globalen Gruppen beinhalten die diversen Users, in diesem Fall in einer globalen Gruppe die Informatik Lernenden und eine andere mit den Informatik Ausbildern. Weiter hat es auch noch für jedes Team eine globale Gruppe. Dies ermöglicht, dass jedes Jahr die Lernenden einfach zu wechseln, ohne immer die gesamte Ordnerstruktur mit NTFS Berechtigungen zu ändern.

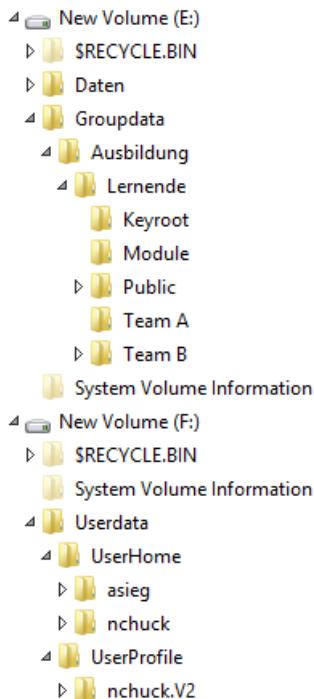
### **Lokale Gruppen:**

Für jeden Ordner in der Ordnerstruktur wurden lokale Gruppen angelegt. Diese dienen dazu, dass dort die globalen Gruppen mit NTFS Berechtigungen berechtigt werden können. Diese lokalen Gruppen besitzen meistens mehrere lokale Gruppen von der gleichen Sorte, mit dem einzigen Unterschied, dass es entweder r (read) oder rwxm (read & write & execute & modify) ist. Dies ist, damit später nur noch die Benutzer in die entsprechenden globalen Gruppen verschoben werden müssen um ihnen Rechte zu geben oder die globalen Gruppen bewegen werden müssen.

## **Domain Controller**

Der DC verwaltet die Domäne und ist der „Chef“ der verschiedenen Server. Er ist ein Server zur zentralen Authentifizierung und Autorisierung von Computern und Benutzern in einem Netzwerk. Es können mehrere DC's festgelegt werden, dies macht aber in den meisten Fällen keinen Sinn.

## Shares/Ordnerstruktur



Die Ordnerstruktur dient dazu verschiedene Ressourcen Zielgerecht freizugeben. Sie können mit Shareberechtigungen und NTFS Berechtigungen versehen werden.

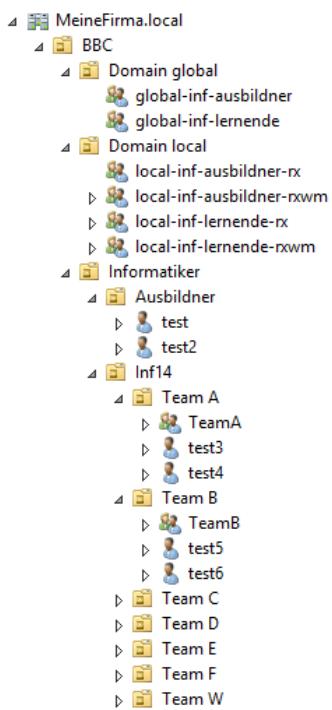
**Die Ordnerstruktur wurde folgendermassen aufgebaut:**

Es wurde ein Volume erstellt für die Allgemeinen Daten von den diversen Teams und ein zweites Volume für das UserHome und das UserProfile. Die Verzeichnisse vom Volume E: wurden mit globalen und lokalen Gruppen berechtigt.

Die Ordner vom Volume F: wurden nur mit dem entsprechendem User versehen, damit er auch ein wenig Privatsphäre besitzt.

Abbildung 12 Ordnerstruktur

## OU (Organisation Unit)



OU dienen der Struktur (der besseren Übersicht) von einer Domäne. Dadurch können dann spezifische Gruppen oder Benutzer oder Computer z.B. mit GPO's versehen werden.

**Dies stellt den Aufbau meiner OU's dar:**

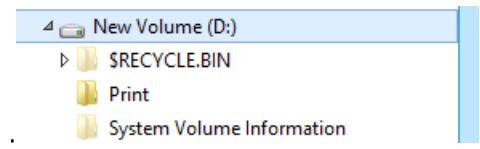
Zuoberst ist zuerst mein Forest. Danach folgt ein Hautordner mit dem Namen BBC und dieser beinhaltet den ganzen Aufbau. Darauf folgen der Ordner mit den globalen Gruppen und unten dran die lokalen Gruppen.

Im Ordner Informatik befinden sich die Ausbildner und auch die verschiedenen Teams von 2014.

Abbildung 13 OU (Organisation Unit)

## Print-Server

Als Printer wurde auf dem SRV-BEGGMM-GUI PDF-Creator installiert. PDF-Creator dient als Standard Printer für den Windows Client. Um diesen zu verwalten wurde die Print Management Rolle installiert. Es wäre auch möglich das ganze über GPO zu machen, siehe GPO. Der freigegebene Drucker wurde mit NTFS Berechtigungen berechtigt. Der Drucker druckt Standardweise in Schwarz & Weiss und wurde über diese Rolle freigegeben. Gespeichert werden die gedruckten Sachen als PDF unter dem Volumen D:\Print



Name	PDFCreator
Treiber	PDFCreator Windows x64 & x86
Freigabe	\\\SRV-BEGGMM-GUI\PDFCreator
Berechtigung	<b>Authenticated Users:</b> Print, Manage Documents <b>Administrator:</b> Print, Management this printer, Manage documents

Abbildung 14 Print Share

Tabelle 14 Print Server Einstellungen

## Routing

Die Rolle „Routing und Remote Access“ wird verwendet um einen Server als Router zu verwenden. Um diese Rolle zu installieren, wird auch noch die IIS Rolle benötigt. Die Rolle wurde nur als NAT installiert und nicht als VPN. Dies wurde gemacht, weil die Clients nur Internet benötigen. Dieser Dienst wurde auf dem GUI Server installiert. Weiter wurden noch die DHCP Server Einstellungen geändert und zwar der Router, welcher auf 192.168.1.10. geändert wurde. Überall wurden die Netzwerkadapter auf LAN gestellt aussert beim GUI Server wurde WAN und LAN eingesetzt

### Routing über zweiten Server

Um den GUI Server ein wenig zu entlasten habe ich beim 2. Versuch die Rooting Rolle noch auf de Core Server installiert. Dazu habe ich zuerst die Rolle vom GUI Server gelöscht und danach habe ich im DHCP Dienst den Router auf die IP vom Core Server geschaltet (192.168.1.11). Beim Server wurde der Standard Gateway auch noch auf 192.168.1.11 gestellt.

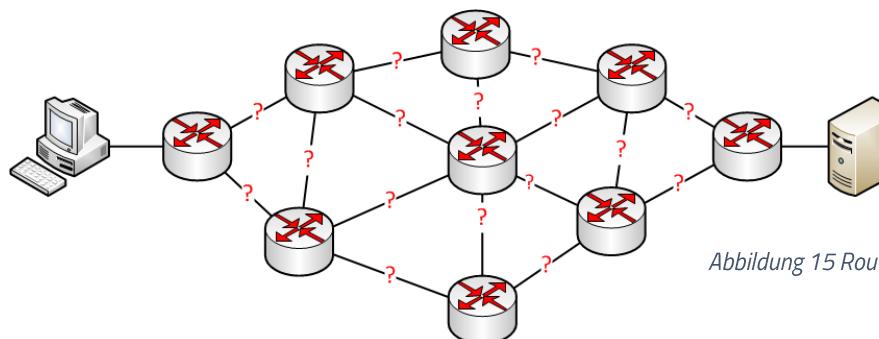


Abbildung 15 Routing Weg

Auf diesem Bild sieht man, wie ein Computer seinen Weg zu einem anderen Aufbau (anderes Netzwerk), er wählt immer den kürzesten.

## IIS

### Installations Logbuch

Aufgabe	Einstellung
Betriebssystem:	Linux, Debian (32 bit)
ISO:	debian-7.7.0-i386-netinst.iso
Speichergrösse (RAM):	512MB
Festplatte:	2GB, Festplatte erzeugen (VDI, dynamisch alloziert)
Zeigergerät:	PS/2-Maus
USB:	Deaktiviert
Audio:	Deaktiviert
Netzwerk:	Internes Netzwerk
MAC Adresse:	0800274797FB
IP:	DHCP (MAC Reservation 192.168.1.15)
Hostname:	webserver
Erreichbar unter:	webserver.meinefirma.local
Intranetseite erreichbar:	http://intranet1.meinefirma.local
Webseite erreichbar:	http://www.meinefirma.local
Sprache:	Deutsch – Schweiz
Land:	Europa/Schweiz
Debian-Archiv-Spiegelserver:	ftp.ch.debian.org
HTTP-Proxy:	-
Locale:	de_CH.UTF-8 UTF-8
Keymap/Keyboard:	Schweizerdeutsch
Software:	Standard-Systemwerkzeuge
Group Boot Loader:	Ja

Tabelle 15 Installations Logbuch

### Testen direkt auf dem Debian Server

- `wget http://localhost` Webseite testen auf dem Webserver
- `cat index.html` Html Datei anschauen
- `apache2ctl -M`: Überprüfen ob das PHP Modul geladen wurde.
- `apache2ctl configtest`: Konfigurationsdateien vor dem Neustart überprüfen
- `apache2ctl restart`: Konfigurationen durch Neustart übernehmen
- `a2ensite meinefirma.local`: Erstellt einen symlink in sites-enabled damit die site angezeigt wird und aktiv ist.
- `apachectl -k graceful`: Unterbrechungsfreier Neustart
- `apachectl -k restart`: Neustarten
- `ifconfig`: Netzwerkeinstellungen überprüfen

### Über einen anderen Client testen

- `webserver.meinefirma.local`: Webseite aufrufen in einem Browser
- `ping webserver.meinefirma.local`: Testen ob die DNS Einstellungen stimmen und ob er erreichbar ist.

### Konfigurationsbeschrieb:

## Installierte Programme

apt-get install apache2

apt-get install php5

## Netzwerk Einstellungen auf DHCP eingestellt

nano /etc/network/interfaces

#internesnetzwerk

allow-hotplug eth0

iface eth0 inet dhcp

ifconfig eth0 up andere ifconfig NAME down

## Grundeinstellungen für die eigene Webseite vorgenommen

cp /etc/apache2/sites-available/default /etc/apache2/sites-available/meinefirmalocal

cd /var/www/

mkdir meinefirmalocal

cp index.html meinefirmalocal/

## Index.html unter /var/www/meinefirmalocal angepasst:

```
<VirtualHost *:80>
    ServerAdmin webmaster@meinefirma.local
    DocumentRoot /var/www/meinefirmalocal
    ServerName meinefirma.local
    ServerAlias meinefirma.local *.meinefirma.local
    <Directory />
        Options FollowSymLinks
        AllowOverride None
    </Directory>
    <Directory /var/www/meinefirmalocal/>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride None
        Order allow,deny
        allow from all
    </Directory>
    ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
    <Directory "/usr/lib/cgi-bin">
        AllowOverride None
        Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
        Order allow,deny
        Allow from all
    </Directory>
    ErrorLog ${APACHE_LOG_DIR}/error.log
    # Possible values include: debug, info, notice, warn, error,
crit,
    # alert, emerg.
    LogLevel warn
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

## DNS

Der Zweck von DNS ist eine IP in einen Namen aufzulösen oder umgekehrt. Dies erfolgt durch Anfragen, welche von anderen Geräten gestellt werden. Normalerweise erfolgt dies meistens über einen DNS Server vom Provider in unserem Netzwerk haben wir aber einen eigenen DNS Server konfiguriert, welcher die internen Aufgaben übernimmt. Sonstige Anfragen werden an den DNS Server von Google gesendet.

Die Tabelle von DNS ist hierarchisch aufgebaut. Der oberste Punkt ist der Root. Die nächste Ebene heisst Top Level Domain, kurz TLD. Dort befinden sich alle Endungen der Webseiten. Zum Beispiel .de .org .local. Weiter unten gibt es dann noch mehrere Ebenen und alle zusammen ergeben dann den „Fully Qualified Domain Name“ oder kurz FQDN z.B. **intranet.meinefirma.local**.

Es gibt verschiedene Arten von Zonen. Die Forward Lookup Zone wandelt Namen in eine IP und beinhaltet eine MSDCS Zone, welche vorhanden sein muss und jeder Domain Controller darin eingetragen sein muss. Weiter ist eine Reverse Lookup Zone vorhanden, welche eine IP in einen Namen umwandelt.

In diesen zwei Zonen können wiederum 3 neue Zonen erstellt werden: Eine Primary Zone, welche eine Kopie von einer Zone macht und direkt auf dem Server aktualisiert werden kann, eine Secondary Zone, die eine Kopie von einer Zone auf einem anderen Server macht und somit hilft die Performace auf dem ersten Server zu erhöhen und die Fehlerrate zu verhindern. Eine Stub Zone dient dazu Anfragen weiterzuleiten, denn diese Zone selbst ist nicht autorisiert Anfragen aufzulösen. Sie dient sozusagen als Forwarder.

Unter SOA kann die Seriennummer und die Refresh interval, retry interval, expires after, minimum default TTL eingestellt werden und der primary Server festgelegt werden. Weiter kann die zuständige Person definiert werden.

Ein Client ruft zuerst sein Hosts file auf (dort kann auch viel manipuliert werden), danach schaut er in den Cache, später beim DNS Server, wenn dieser nicht bescheid weiss fragt er den Forwarder (ISP) und dieser gibt es dann dem entsprechenden Root Server weiter.

### Commands:

**Nslookup:** Um Hostnamen in IP's umzuwandeln oder umgekehrt.

**Ipconfig:** Allgemeine Infos anzeigen

**Ipconfig /flushdns:** DNS Cache leeren

**Ipconfig /displaydns:** DNS Cache anzeigen

**Ping -a:** Um zu testen ob der Hostname und die IP-Adresse angezeigt wird.

**nslookup ls [gewünschte Zone]:** Der Client kann die Zonen Einträge anschauen(Zonenfreigabe)

Records: Reverse Lookup Zone	
PTR Records	Ordnet einer gegebenen IP-Adresse einen oder mehrere Hostnamen zu. Sie stellen damit gewissermaßen das Gegenstück zur klassischen Zuordnung einer oder mehrerer IP-Adresse(n) zu einem gegebenen Hostname per A- oder AAAA Resource Record dar.
Alias (CNAME) records	Alternativen Namen für einen Host (Alias)

Tabelle 16 DNS Reverse Lookup Zone - Records

Records: Forward Lookup Zone	
Host (A) records	Mit einem A Resource Record wird einem DNS-Namen eine IPv4-Adresse zugeordnet. Sie werden auch für die Angabe von Subnetzmasken zu Rückwärtsauflösung verwendet.
Alias (CNAME) records	Alternativen Namen für einen Host (Alias)
Service (SRV) records	Kann zeigen, welche IP-basierenden Dienste in einer Domain angeboten werden.
Mail Exchanger ( MX) records	Der MX Resource Record einer Domain ist ein Eintrag im DNS, welcher sich ausschliesslich auf den Dienst E-Mail (SMTP) bezieht. Sagt aus unter welchem FQDN der Mail-Server zu einer Domäne erreichbar ist.
Start of authority (SOA) records	Wichtiger Bestandteil einer Zonendatei im DNS. Es Enthält wichtige Angaben zur Verwaltung der Zone, insbesondere zum Zonentransfer.
Name server (NS) records	Ein Datensatz eines DNS Servers mit den 2 Funktionen: <ul style="list-style-type: none"> <li>o Er definiert, welche Nameserver für diese Zone offiziell zuständig sind, oder</li> <li>o er verkettet Zonen zu einem Zonen-Baum (Delegation).</li> </ul>

Tabelle 17 DNS Forward Lookup Zone - Records

#### MSDCS:

MSDCS wird benötigt, weil diverse Dienste auf DNS basieren, wie z.B. AD DS und somit Zugriff auf diese Zone benötigen. Dadurch kann der DNS Server Informationen im AD DS speichern.

#### Einstellungen:

Es wurde so eingestellt, damit nur die IP 192.168.1.100 (Client), 192.168.1.11 (Core), 192.168.1.15 (Webserver) und der GUI Server selbst 192.168.1.10 DNS anfragen stellen können. Weiter wurde ein Zonen Transfer aktiviert, damit der Client auf MeineFirma.local Zone Zugriff hat.

Forward Lookup Zone: MeineFirma.local ergänzte Records	
Zone:	MeineFirma.local
	_msdcs.MeineFirma.local
A-Record:	srvweb01 – 192.168.1.10
A-Record:	webserver – 192.168.1.15
CNAME-Record:	Intranet – webserver.meinefirma.local
CNAME-Record:	www – srvweb01.meinefirma.local

Tabelle 18 Forward Lookup Zonen

Reverse Lookup Zone: MeineFirma.local ergänzte Records	
Zone:	1.168.192.in-addr.arpa
PTR-Record:	15.1.168.192.in-addr.arpa - webserver
PTR-Record:	10.1.168.192.in-addr.arpa – srvweb01

Tabelle 19 Reverse Lookup Zonen

Listening Interfaces	192.168.1.10
Forwarding	192.168.1.10 8.8.8.8 (Google)

Tabelle 20 Listening Interfaces / Forwarding

## DHCP

DHCP steht für „Dynamic Host Configuration Protocol“ und ermöglicht die Zuweisung der Netzwerkkonfiguration an Clients über einen Server. Dies ermöglicht Geräte leichter einzubinden. Der DHCP Server muss berechtigt werden, damit es den DNS Server benutzen darf.

Begriffe	Beschreibung
Scope	Für jedes Subnetz wird ein Scope definiert und dort werden die Einstellungen für das gesamte Subnetz eingestellt.
Adresspool	Dieser Pool definiert, wie gross der Bereich der verfügbaren IP-Adressen im Subnetz ist.
Range (Exclusion Range)	Die Exclusion Range kann definiert werden, damit der DHCP Server in diesem IP-Bereich keine IP's vergibt. Wenn in
Leasetime	Die Mietdauer, wie lange ein Client die IP-Adresse behalten darf, bis er wieder eine neue Adresse braucht. In der Hälfte der Lease Zeit fragt der Client noch einmal nach, ob es immer noch ok ist.
Reservierung	Die Reservierung erfolgt über eine Mac-Adresse und dient dazu einem Gerät immer die selbe IP Adresse zu vergeben, obwohl sie dynamisch ist.
Autorisierung	Der DHCP-Server muss autorisiert werden, damit er mit dem DNS-Server zusammen arbeiten kann und IP Adressen vergeben darf.
Relay Agent	Dieser leitet DHCP-Meldungen zwischen DHCP-Clients und DHCP-Server in verschiedenen IP-Netzwerken weiter.
Failover	Ein Failover kann auf gemacht werden, damit wenn ein Server ausfällt, dass der 2. das Vergeben der IP's weiter machen kann.

Tabelle 21 DHCP Begriffe

### Commands:

`ipconfig /all`: Alle Netzwerkeinstellungen anzeigen

`ipconfig /release`: Die IP Adresse vom DHCP Server wieder freigeben

`ipconfig /renew`: Die Einstellungen erneuern

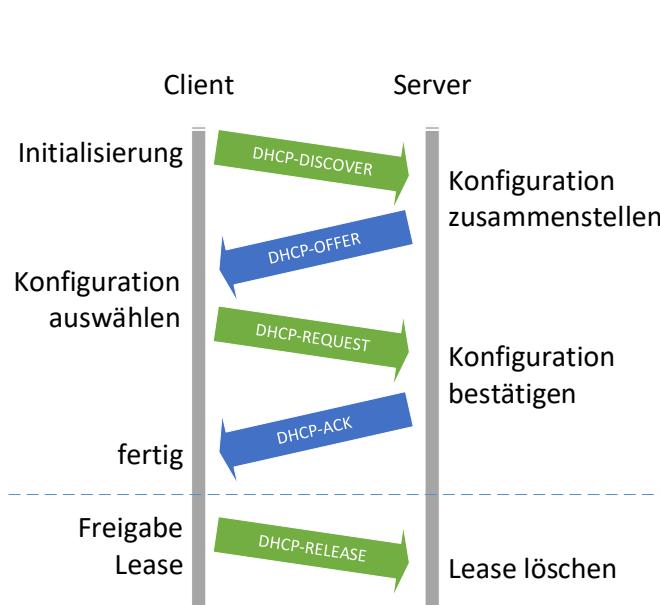


Abbildung 16 DHCP Verlauf

**DHCP-Discover:** Der Client sucht über Broadcast nach einem DHCP Server..

**DHCP-Offer:** Ein Server meldet sich zurück und bietet seine Dienste über Unicast an.

**DHCP-Request:** Der Client fordert eine vorgegebene IP an.

**DHCP-Ack:** Der Server bestätigt, dass die Einstellungen übernommen wurden.

**DHCP-Release:** Der Client gibt die IP wieder frei.

**DHCP-Nack:** Der Server hat die Anfrage abgelehnt.

Die DHCP Rolle wurde auf dem GUI Server installiert und auf dem Core Server wurde ein Failover eingerichtet. Es wurde folgendermassen konfiguriert:

Aufgabe	Einstellung
Name:	Scope01
IP Bereich:	192.168.1.100-192.168.1.120
Exclusion:	192.168.1.100-192.168.1.120
Lease Duration:	1 min (nur zum Testen) sonst 8 Tage
Default Gateway:	192.168.1.10
Parent domain:	MeineFirma.local
DNS IP Adresse	192.168.1.10 8.8.8.8
Scope Options:	Router, Time Server, DNS Server, DNS Domain Name
Reservation	Name: BEGGMM-PC IP: 192.168.1.101 MAC: 08-00-27-5d-83-3f Supported types: Both
	Name: webserver IP : 192.168.1.15 MAC : 08-00-27-47-97-FB Supported types : Both

Tabelle 22 DHCP Einstellungen

Damit die Reservation auf dem Client muss er die IP dynamisch beziehen und danach sollte noch *ipconfig /release und renew* ausgeführt werden.

## FSRM

FSRM steht für „File Ressource Management“ und ist auch direkt die entsprechende Rolle, welche benötigt wird.

Quotas Management	Mit den Quotas kann man diverse Speichereinschränkungen festlegen. Dazu erstellt man ein Template (eine Art Schablone) mit einem entsprechenden Namen, definiert eine Limite des Volumens und man kann eine Meldung definieren, falls dies Limite überschritten wird oder wenn der Benutzer schon nahe an der Limite ist. Diese Quotas können dann auf die entsprechenden Ordner gesetzt werden.
File Screening Management	Mit dem kann man festlegen, welche Dateien in einem Ordner sein dürfen und welche nicht. z.B. in einem Musik Ordner ist es nicht unbedingt Sinnvoll Dateien wie .docx zu beinhalten. In „FileGroups“ kann man die entsprechenden Dateiendungen zulassen oder nicht zulassen. In den File Screening Templates kann man danach noch definieren, was mit den verbotenen Dateien geschehen soll.
Storage Reports	Dies dient dazu Benutzer zu informieren, wenn sie z.B. ihre Quota beinahe erreicht haben oder wenn sie zu grosse Dateien hochgeladen haben. Der Admin kann definieren wie häufig der entsprechende Ordner kontrolliert werden soll und ob er eine Mail bekommen will, falls eine solche Meldung erscheint.

Tabelle 23 FSRM Begriffe

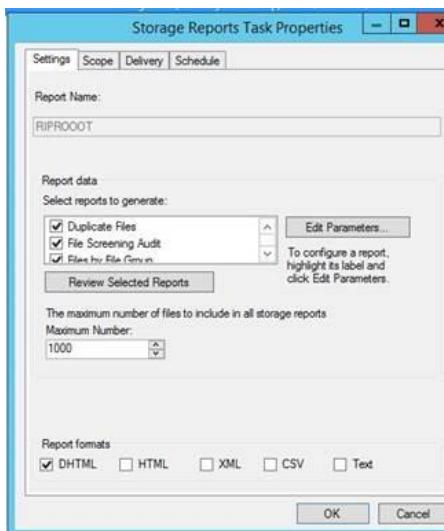


Abbildung 19 FSRM - Storage Report

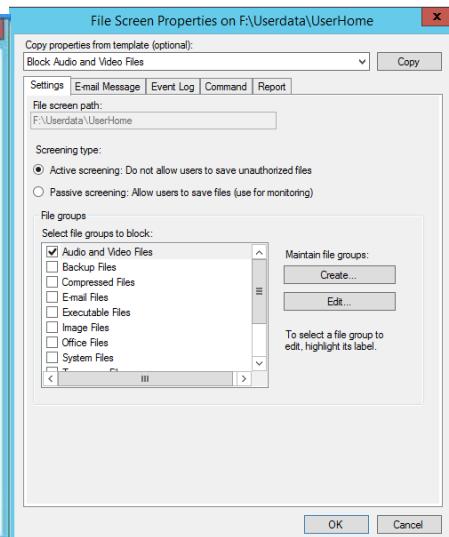


Abbildung 18 FSRM - File Screening

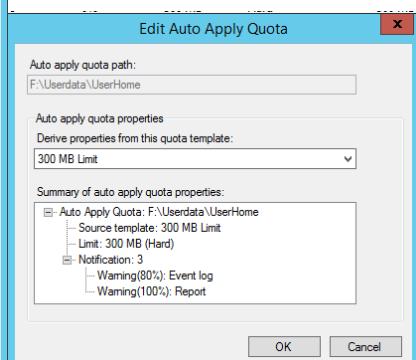


Abbildung 17 FSRM - Quotas

## GPO

GPO steht für „Group Policy Object“ und ist nützlich um diverse Richtlinien von Gruppen, Benutzer, PC's usw. zu konfigurieren, wie z.B. einen Standard Drucker festlegen oder nur Shares einzubinden, welche die Benutzer dazu berechtigt sind diese zu nutzen. Es ist eine Sammlung spezifischer Gruppenrichtlinieneinstellungen.

### Default GPO

- Die Default Domain Policy dient dazu allgemeine GPO Einstellungen für die gesamte Domäne vorzunehmen, wie z.B. die Passwortrichtlinien.
- Die Default Domain Controller Policy wird für die Domain Controller genutzt, z.B. um zu definieren, wer sich bei den Domain Controller einloggen darf.

### Speicherort der GPO's

GPO's werden unter: *Domains -> MeineFirma.local -> Group Policy Objects* gespeichert und können anschliessend verlinkt werden.

Die GPO's sind auf dem Server mit einer Unique ID im Ordner SYSVOL abgelegt. Der genaue Pfad ist: *C:\Windows\SYSVOL\domain\Policies*. Dieser Ordner ist freigegeben und von dort beziehen die Clients ihre GPO Einstellungen.

### Erstellen und zuweisen

Um GPO's zu erstellen oder zuzuweisen benutzt man das Tool Group Policies Management (GPM):

- Erstellen und verknüpfen: *Rechtsklick auf eine gewünschte OU -> Create a GPO..., and Link it...*
- Erstellen: *Rechtsklick auf das OU Group Policy Objects -> New*
- Verknüpfen: *Rechtsklick auf ein gewünschtes OU -> Link an Existing GPO*

### GPO Update

- Computer-Einstellungen werden beim Start übernommen.
- User-Einstellungen werden bei der Anmeldung übernommen.
- CMD: *gpupdate /force*
- Powershell: *invoke-gpupdate*

### Passwort Richtlinien ändern

*Server Manager -> Tools -> GPO -> (Rechtsklick Edit auf „Default Domain Policy“) -> Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Account Policies -> Passwort Policies*

### Drucker

Pfad der Einstellungen: *Drucker-verbinden ->Edit->User Configuration->Preferences->Control Panel Settings-> Printers*

### Screen Saver

Pfad: *User Configuration -> Policies -> Administrative -> Control Panel -> Personalization-> Screen saver timeout*

### Restricted Group

Pfad: *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Restricted Groups*

## Laufwerke automatisch verbinden

Diese GPO wird auf OU's mit Usern angewendet.

The screenshot shows two windows side-by-side. On the left is the 'M: Properties' dialog box under the 'General' tab. It has fields for 'Action' (Create), 'Location' (\\\192.168.1.10\Sharename), 'Reconnect' (checked), 'Label as' (Sharename), 'Drive Letter' (M), and 'Connect as (optional)' fields for User name, Password, and Confirm password. Below are 'Hide/Show' options for the drive. At the bottom are 'OK', 'Cancel', 'Apply', and 'Help' buttons. On the right is a GPO targeting rule titled 'the user is a member of the security group MEINEFIRMA\local-management-rxwm OR the user is a member of the security group MEINEFIRMA\local-management-rx'. It lists six items with their order, action, path, and reconnect status:

Name	Order	Action	Path	Reconnect
M:	1	Create	\\\192.168.1.10\Management	Yes
N:	2	Create	\\\192.168.1.10\Marketing	Yes
O:	6	Create	\\\192.168.1.10\Produktion	Yes
P:	3	Create	\\\192.168.1.10\Public	Yes
Q:	4	Create	\\\192.168.1.10\Entwicklung	Yes
U:	5	Create	\\\192.168.1.10\Buchhaltung	Yes

Abbildung 20 GPO Laufwerk-verbinden Einstellungen / Item-level targeting / Laufwerke

Aufpassen mit OR (in einer der beiden Gruppen) oder AND (in beiden Gruppen sein müssen)!

Pfad der Einstellungen: *GPO->Edit->User Configuration->Preferences-> Windows Settings -> Drive Maps*

## Client Services

Pfad: *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> System Services*

## Background ändern

Man muss darauf achten, dass der Share für alle zugänglich ist! (z.B. \\\192.168.1.10\SYSVOL\bild.jpg)

Pfad: *User Configuration -> Policies -> Administrative -> Desktop -> Desktop -> Desktop Wallpaper*

## Admin auf Benutzerprofile Zugriff

*Computer Configuration -> Administrative -> System -> User Profiles -> Add the...*

Die HTML Dateien wurden unter dem Verzeichnis „[GPO Einstellungen](#)“ abgelegt.

# Ressourcenverwaltung

## Shares

Bei Shares sollte die Vererbung ausgeschaltet werden, weil man dort andere lokale Gruppen einfügt und keine Einstellungen von oben übernehmen sollte. Es sollte nach dem IGDLA Konzept vorgegangen werden und zwar mehrere lokale Gruppen erstellen für z.B. die gleiche Abteilung, mit dem einzigen Unterschied, dass die eine Gruppe rx (Lesen & Ausführen) und die andere rxwm (Lesen & Ausführen & Modifizieren & Schreiben) hat. Somit muss man später nur noch die globalen Gruppen bei den entsprechenden lokalen einbinden. Standard Users und Create Owner können in beinahe allen Fällen herausgelöscht werden.

### NTFS Berechtigungen:

Person(en)	Berechtigung		
	Full control	rxwm	rx
SYSTEM	x		
Administrator	x		
Lokal-XXXX-rx			x
Lokal-XXXX-rxwm		x	

Tabelle 24 NTFS Berechtigung

### Mehr Sicherheit:

Es besteht auch die Möglichkeit sogenannte Administrative Shares zu machen. Diese werden mit einem \$ beim erstellen ergänzt z.B. userhomes\$ und können somit bei normalem Gebrauch nicht gesehen werden, natürlich sind diese durch den Einsatz von Tools trotzdem sichtbar. Diese dienen dazu für mehr Sicherheit zu sorgen, denn nicht jeder benötigt Zugriff, z.B. auf die Userhomes.

Unter: *Windows Server Manager -> File and Storage Services -> Shares -> SHARENAME -> Properties -> Settings -> Enable access-based enumeration* kann zusätzlich noch eingestellt werden, dass man nur die Shares sieht, auf welche man auch Zugriff hat.

### Beispiel Public

Inheritance wurde ausgeschaltet und der Share wurde mit Authenticated Users (change) und dem SYSTEM (full control) ausgestattet. Der Share wurde nicht versteckt.

### NTFS Berechtigungen:

Person(en)	Berechtigung		
	Full control	rxwm	rx
Sharename: Public			
SYSTEM	x		
Administrator	x		
Lokal-Public-rx			x
Lokal-Public-rxwm		x	

Tabelle 25 Beispiel Berechtigungen

## IGDLA

IGDLA befasst sich mit der Vergabe von Rechten für Ressourcen mit lokalen und globalen Gruppen. Dies wurde weiter oben schon angewendet bei dem AD DS. Dieses Verfahren wird eingesetzt, damit später der Aufwand nicht gross ist um neue Benutzer hinzuzufügen oder zu löschen.

### Globale Gruppen und lokale Gruppen und Ressourcen

Bei IGDLA werden globale Gruppen in lokalen Gruppen abgelegt, dies ist der Fall, weil lokale Gruppen nicht in andere lokale Gruppen geschossen werden können.. Die lokalen Gruppen werden wiederum bei den entsprechenden Ressourcen (Ordner/Shares) berechtigt. Dies ermöglicht eine Grundstruktur durch die lokalen Gruppen und später müssen nur noch die globalen Gruppen in die entsprechenden lokalen geschmissen werden, diese besitzen meistens ein rx (lesen) und ein rxwm (lesen & schreiben).

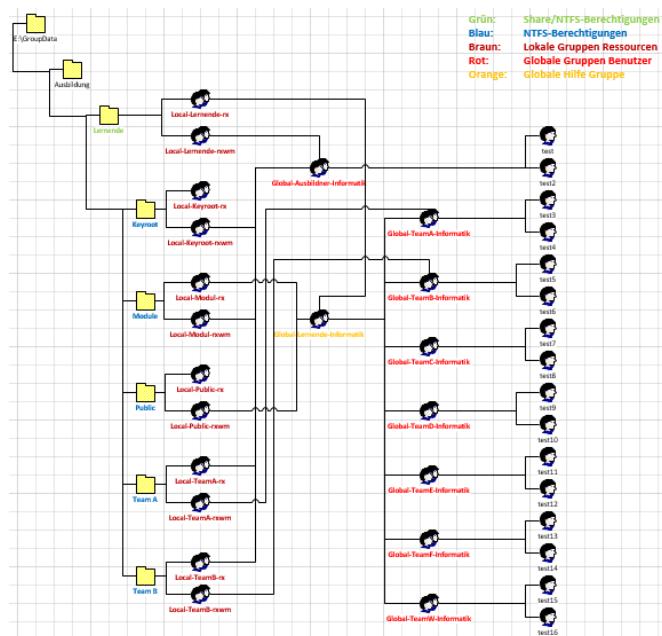


Abbildung 21 IGDLA

Ressource	Gruppen	Global-Ausbildner-Informatik	Global-Lernende-Elektronik	Global-TeamA-Informatik	Global-TeamB-Informatik
E:\GroupData\Ausbildung\Lernende - (Lernende\$)	Local-Lernende-rx		R,X - (C)		
E:\GroupData\Ausbildung\Lernende\Keyroot	Local-Lernende-rxwm Local-Keyroot-rx		R,X,W,M -(C)		
E:\GroupData\Ausbildung\Lernende\Modul	Local-Keyroot-rxwm Local-Module-rx		R,X,W,M	R,X	
E:\GroupData\Ausbildung\Lernende\Public	Local-Module-rxwm		R,X,W,M		
E:\GroupData\Ausbildung\Lernende\Team A	Local-Public-rx Local-Public-rxwm Local-TeamA-rx		R,X,W,M	R,X,W,M	
E:\GroupData\Ausbildung\Lernende\Team B	Local-TeamA-rxwm Local-TeamB-rx Local-TeamB-rxwm		R,X,W,M	R,X	R,X,W,M

## Benutzerprofile

### Servergespeicherte Profile

Es gibt verschiedene Arten von Benutzerprofilen, eine Art ist das Servergespeicherte Profil. Sie sind ein sehr hilfreiches Mittel, um sämtliche Einstellungen zentral zu speichern. Der Einsatz lohnt sich aber nicht immer, weil es voraussetzt, dass immer ein Server läuft, auf welchem diese Profile gespeichert sind. Es ist auch möglich, dass die Daten trotzdem noch lokal auf dem PC gespeichert werden, und wenn man sich wieder verbindet werden sie auf dem Server abgeglichen. Für diese Profile ist ein kleiner Server und ein Active Directory nötig.

Ein Servergespeichertes Profil kann im AD DS unter dem gewünschten Benutzer -> Properties -> Profile eingebunden werden, dort kann man den Pfad vom Userhome auf dem Share eingeben, dies sieht dann etwa so aus: \\192.168.1.10\userprofile\$\%username%

Weiter kann auch noch ein Homelaufwerk erstellt werden, dies unter dem selben Pfad, wie das Profil un dies würde dann so aussehen: \\192.168.1.10\userhome\$\%username%.

- + Der Benutzer kann sich auf jedem PC einloggen, welcher mit der Domäne verbunden ist und hat immer seine Daten.
- + Konfiguration kann zentral verwaltet werden.
- + Jedes Profil muss nur einmal angelegt werden.
- + Berechtigungen müssen nur einmal gesetzt werden.
- Es muss immer ein Server laufen, damit man auf diese Profile zugreifen kann.

### Share / NTFS Berechtigungen

Um ein gutes Berechtigungskonzept aufzubauen benötigt man ein Grundwissen vom Benutzen von Berechtigungen. Bei den Shareberechtigungen muss beinahe immer Read & Modify gegeben werden, weil es sonst Probleme geben kann mit den NTFS Permissions. Bei den Share Berechtigungen kann man SYSTEM, Administrator und Authenticated Users hineintun. Bei den NTFS-Berechtigungen sollten lokale Gruppen eingefügt werden nach dem Prinzip von IGDLA. Weiter muss auch dort SYSTEM und Administrator drin bleiben. Dies kann allerdings nur angewendet werden, wenn die Benutzer alle in einer Domäne sind.

### GPO Account Richtlinien:

Unter Account Policies können Passwort Richtlinien, Account lockout und Kerberos Einstellungen vorgenommen werden. Der Link um dort hin zu gelangen:

*Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Account Policies*

### GPO Profile

Unter den Userprofiles kann man einstellen, dass der Administrator Zugriff auf die Benutzerprofile hat.: *Computer Configuration/ Policies /Administrative Templates/ System /Userprofile*

### Beispiel Benutzer:

User profile	
Profile path:	\\\192.168.1.10\userprofile\\$\\hans
Logon script:	
Home folder	
<input checked="" type="radio"/> Local path:	\\\192.168.1.10\userhome\\$\\hans
<input type="radio"/> Connect:	
To:	

		Geschäftsleitung	Entwicklung	Produktion	Administration	Verkauf
Ressource	Gruppen	Glo-geschaeft	Glo-entwicklung	Glo-produktion	Glo-administration	Glo-verkauf
H:\Abteilung	Loc-rx-Abteilung		R,X,(R)	R,X,(R)	R,X,(R)	R,X,(R)
	Loc-rxwm-Abteilung	R,X,W,M,(C)				
H:\Abteilung\Ent_Pro	Loc-rx-Ent_Pro					
	Loc-rxwm-Ent_Pro	R,X,W,M	R,X,W,M	R,X,W,M		
H:\Abteilung\Entwicklung	Loc-rx-Entw			R,X		
	Loc-rxwm-Entw	R,X,W,M	R,X,W,M			
H:\Abteilung\Produktion	Loc-rx-Produkt		R,X			
	Loc-rxwm-Produkt	R,X,W,M		R,X,W,M		
H:\Abteilung\Admin_Ver	Loc-rx-Adm_Ver					
	Loc-rxwm-Adm_Ver	R,X,W,M			R,X,W,M	R,X,W,M
H:\Abteilung\Administration	Loc-rx-Adminis					R,X
	Loc-rxwm-Adminis	R,X,W,M			R,X,W,M	
H:\Abteilung\Verkauf	Loc-rx-Verkauf				R,X	
	Loc-rxwm-Verkauf	R,X,W,M				R,X,W,M
H:\Abteilung\Public	Loc-rx-Public					
	Loc-rxwm-Public	R,X,W,M				

Abbildung 23 Reorganisation

Abbildung 22 Benutzerprofile

## Reorganisation / Migration

Damit später ein anderer Informatiker das Berechtigungskonzept übernehmen kann, benötigt er einige Vorgaben, dazu eignet sich z.B. ein solches Diagramm (es wurde nach dem IGDLA Konzept aufgebaut):

R --> Read (NTFS-Berechtigung)

X --> Execute (NTFS-Berechtigung)

W --> Write (NTFS-Berechtigung)

M --> Modify (NTFS-Berechtigung)

(R) --> Read (Share-Berechtigungen)

(C) --> Change (Share-Berechtigungen)

## Netzwerktools

Ping	Anpingen eines Gerätes / Webseite
-a	Mit DNS Einstellungen
Ipconfig	Ausgeben von: IP-Adresse, Subnetzmaske, Standard-Gateway
-all	Zusätzlich: Hostname, DNS-Server, NetBIOS, WINS
-flushdns	DNS Cache leeren
-displaydns	DNS Cache anzeigen
-release	Adapter freigeben
-renew	IP Adressen für die Adapter
-?	Hilfe Optionen
Nslookup	IP Adresse in einen Hostnamen umwandeln oder umgekehrt
Netstat	Netzwerkstatistiken anzeigen

-an	Wenn Computer empfangsbereit ist und Adressen nur in nummerischer Form
Route	Man kann Routen erstellen / löschen und ansehen
-print	Zeigt die aktuellen Routen an
Tracert	Dieses Programm ermittelt über welche Route das Paket nimmt zum Ziel
Wireshark	Netzwerkverkehr untersuchen

Tabelle 27 Netzwerkdienste

# Scripting

## PowerShell

### GUI installieren / deinstallieren

- Install-WindowsFeature Server-Gui-Shell
- Uninstall-WindowsFeature Server-Gui-Shell

### Gerät herunterfahren

- Shutdown -r -t 0

### Feature installieren

- Install-WindowsFeature FEATURENAME

### Server Konfiguration

- Sconfig

### Einzelne Benutzer / OU / Gruppen erstellen oder löschen

Aufgabe	Code
ACC hinzufügen	New-ADUser –Name VORNAME –Displayname „NAME“ –GivenName VORNAME –Surname NACHNAME –Path „PFAD AD“
OU hinzufügen	New-ADOrganizationalUnit NAME
Gruppe hinzufügen	New-ADGroup GRUPPENNAME –Path „PFAD OU“ –GroupScope [Lokal/Global] –GroupCategory [Security]
ACC Passwort setzen	Set-ADAccountPassword ACCNAME
ACC aktivieren	Enable-ADAccount ACCNAME
ACC in Gruppe	Add-ADGroupMember GRUPPENNAME ACCNAME
ACC löschen	Remove-ADUser ACCNAME
Gruppe löschen	Remove-ADGroup NAME
OU löschen	Remove-ADOrganizationalUnit NAME

Tabelle 28 PowerShell

### Mehrere Benutzer mit CSV einbinden

Import-Csv c:\CSVNAME.csv | New-ADUser –organization "{MeineFirma}"

### Script zum einbinden von mehreren Benutzern

```
Import-Module ActiveDirectory
$Users = Import-Csv -Delimiter ";" -Path "PFAD_ZUM_CSV"
foreach ($User in $Users) {
    $OU = "OU=Entwicklung,OU=Users,OU=switzerland,OU=europe,OU=meinefirma,DC=meinefirma,DC=local"
    $Passwort = $User.Passwort
    $VollerName = $User.Name + " " + $User.Nachname
    $Vorname = $User.Name
    $Nachname = $User.Nachname
    $Kürzel = $Nachname.Substring(0,4).ToLower() + $Vorname.Substring(0,1).ToLower()
    New-ADUser -Name $VollerName -SamAccountName $Kürzel -UserPrincipalName $Kürzel@meinefirma.local -DisplayName $VollerName -GivenName $Vorname -Surname $Nachname -AccountPassword (ConvertTo-SecureString $Passwort -AsPlainText -Force) -Enabled $true -Path $OU
}
```

## Servertool

### Eventlog auswerten (Event Viewer -> eventvwr)

Im Event Viewer können diverse Informationen, Errors und Warnungen ausgelesen werden, welche vom System gemeldet wurden. Unter anderem kann man darin z.B. auch sehen wann z.B. etwas im Performance Monitor gestartet wurde und auch wieder gestoppt wurde. Meldungen, wie z.B. der freie Speicher ist unter 50 % können auch ausgegeben werden, wenn diese zuvor z.B. im Performance Monitor definiert wurden.

#### Verwendung:

- Sogenannte Logs (Infos, Warnungen, Errors) auslesen

### Remotedesktop (mstsc.exe)

Um Remotedesktop zu nutzen muss die Firewall deaktiviert werden oder eine Regel eingeführt werden, da sonst dieser Dienst nicht genutzt werden kann. Um sich einzuloggen ist es am besten den Administrator zu nutzen, damit man volle Rechte hat.

#### Verwendung:

- Dieser Dienst ist sehr praktisch um einen Server von extern zu verwalten, damit man nicht immer in den Keller gehen muss um den Server zu konfigurieren.
- Weiter ist es auch sehr nützlich um Leuten von extern bei Problemen zu helfen.

## Computermanagement

Unter Computer Management können Systemprogramme (Ereignisanzeige, Geräte Manager, Freigegebene Ordner, Leistungsdaten und Warnungen, Lokale Benutzer und Gruppen), Speicher (Wechselmedien, Defragmentierung, Datenträgerverwaltung) und Dienste und Anwendungen (Dienste, WMI-Steuerung, Indexdienst.) verwaltet und genutzt werden.

#### Verwendung:

- Laufwerksbuchstaben vergeben
- Festplatte einbinden
- ...

### Performance Monitor (Perfmon.exe)

Dieses Tool ermöglicht das analysieren eines Servers und kann helfen Probleme zu beheben. Um zu testen wie es aussehen würde, kann man cpustress.exe installieren. Dies ermöglicht den CPU mit unnötigen Sachen zu Überlasten.

#### Verwendung:

- CPU Auslastung überwachen
- RAM Auslastung überwachen
- Warnen, falls der Freie Speicherplatz zu klein wird (z.B. unter 50%)

## Registry

Dies ist die Windows-Registrierungsdatenbank und ist seit der Windows NT Version verfügbar. In dieser Konfigurationsdatenbank werden Informationen von Windows und anderen Programmen gespeichert. Sie dient dazu das System zu verwalten.

- HKEY\_CURRENT\_USER  
Dort findet man Infos zu dem aktuellen User, wie Wallpaper, etc.
- HKEY\_LOCAL\_MACHINE  
Hier findet man alle Infos zum Client selber.
- HKEY\_CURRENT\_CONFIG  
Hier sind die Konfigurationen des aktuellen Users gespeichert.
- Etc...

## Verwendung:

- IPV6 deaktivieren
- Numlock aktivieren / deaktivieren

## MMC

Die Microsoft Management Console kann über *Windows + r -> mmc* geöffnet werden. Danach kann über *File -> Add Snap-in -> Die benötigten Dienste hinzufügen*.

## Verwendung:

- Dies ist praktisch um die benötigten Dienste im Überblick zu haben und alles über ein Fenster erreichbar ist.

## Beispiel Konsole mit dem Namen KonsoleSerververwaltung:

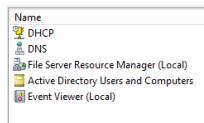


Abbildung 24 MMC

## RSAT-Tools

Die RSAT-Tools dienen dazu einen Server von einem anderen Standort aus zu verwalten. Anders als bei Remotedesktop werden die Tools lokal auf dem Client gespeichert. Nach der Installation können die Tools über *Start -> Alle Programme -> Verwaltung* geöffnet werden.

Dazu muss man von der Windows Seite diese Dateien herunterladen:

<http://www.microsoft.com/de-de/download/details.aspx?id=7887>

Für 32 Bit-Systeme: x86fre\_GRMRSAT\_MSU.msu

Für 64 Bit-Systeme: amd64fre\_GRMRSATX\_MSU.msu

## Verwendung:

- Server von extern Verwalten

# Netzsicherheit

## Schwachstellen

- 1. Schwachstelle Administrator

Eine Schwachstelle von meinem virtuellen Netz ist, dass eine Person, welche das Administratorkennwort kennt erpresst werden könnte. Dies hätte verherende Folgen, weil der Administrator alles verändern kann. Verhindern kann man dies nur indem man ein sicheres Kennwort nimmt und es niemandem weiter sagt. Weiter sollte dieser Administrator keine strafrechtlichen Anschuldigungen besitzen.

- 2. Schwachstelle DHCP Dienst / Ethernet Steckplatz

Ein weiteres Problem könnte sein, dass sich jemand Zugang ins Netzwerk verschafft, indem er sich mit einem Ethernet Kabel an einem freien Stecker einklinkt. Beim DHCP Dienst könnte es auch ein Problem geben, weil es zu viele freie IP's hat. Um zu verhindern, dass es zu grosse folgen hat, sollten freie Steckplätze nicht zu offen plaziert sein und wenn es wirklich sicher sein soll, sollte eine MAC-Filterung aktiviert werden, welche nur Leute drauf lässt, welche im Router oder so eingetragen sind. Auch dies ist nicht vollkommen sicher und man sollte z.B. die Shares nur für authentifizierte User freigeben. Der DHCP Bereich sollte, wenn es wirklich sicher sein soll, nur sehr wenige automatisch vergeben werden und die anderen sollten excluded sein und mit einer Reservation vergeben werden. Somit ist die Sicherheit schon nicht schlecht und es kann damit gearbeitet werden.

- 3. Schwachstelle Virenschutz

Eine letzte Schwachstelle ist, dass man keinen Virenschutz installiert hat und sich somit Viren einschleichen können. Es sollte ein gut bewerteter gratis Virenschutz oder noch besser einen Virenschutz, welchen man bezahlen muss bezogen werden. Auf meiner VM ist z.B. UnThreat installiert und dies ist ein ziemlich guter Gratisvirenschutz.

## Virenschutz

Wie vorhin schon erwähnt habe ich auf meinen beiden Servern und auf dem Windows Client einen Virenschutz installiert. Ich habe mich für den UnThreat Virenschutz entschieden, weil mir dieser gerade zur Verfügung stand. Dies ist ein gratis Virenschutz, welcher ziemlich gut gegen Viren schützt. Wenn es ein wenig sicherer sein sollte, würde ich Kaspersky nehmen, weil dieser eine gute Bewertung hat und ich gute Erfahrungen damit gemacht habe, aber ein wenig kostet.

## Passwort

Ich kann die Benutzer auffordern ihre Passwörter beim ersten Login zu ändern oder ich könnte machen, dass die Benutzer ihre Passwörter gar nicht ändern könnten. Weiter ist es auch möglich einzustellen, dass die Benutzer ihre Passwörter alle X Tage ändern müssen. Die Komplexität vom Passwort kann ich als Administrator auch vorgeben. Wenn ein Benutzer sein Passwort vergessen hat kann ich dies auch wieder zu einem Standard Passwort ändern und ihm somit aus der „patsche“ helfen.

## [Administrator / root Konto](#)

Dies sollte nicht für jeden Benutzer zur Verfügung stehen, weil man sonst nicht zurückverfolgen kann, wer z.B. Mist auf dem Server gebaut hat. Dies kann schwere Folgen für den Admin haben, weil er die Fehler der Benutzer ausbügeln muss. Weiter könnten die Benutzer auch wichtige Daten klauen und diese für teures Geld verkaufen.

Ein Administrator sollte sich auch nicht ohne weiteres auf jedem PC anmelden können, weil wenn er z.B. vergisst sich abzumelden, könnte sich ein Benutzer wie oben erwähnt Eingriff in das System verschaffen.

Als Administrator kann ich mein Passwort schützen, indem ich ein langes und komplexes Kennwort nehme mit Sonderzeichen etc. und mich nur auf „sicheren“ PC anmelden.

## [Root Rechte](#)

Bei Linux gibt es eine sogenannte Sudoers Datei und dort drin werden auch Berechtigungen gespeichert. Ausgeführt können Dateien als Admin mit dem Command „sudo“.

In der Windows Umgebung können Dateien mit Rechtsklick -> als Administrator ausführen im Admin Modus geöffnet werden.

## [Benutzer Authentifizierung](#)

Meistens dienen der Authentifizierung ein Passwort und der dazugehörige Benutzername.

z.B. Kerberos