SCHULNETZ®

QUALIFIZIERUNG
VON SYSTEMBETREUERINNEN
UND SYSTEMBETREUERN

# MICROSOFT-WINDOWS-NETZWERKE
# CLIENT/SERVER

LABORÜBUNGEN

AKADEMIE FÜR LEHRERFORTBILDUNG
UND PERSONALFÜHRUNG DILLINGEN

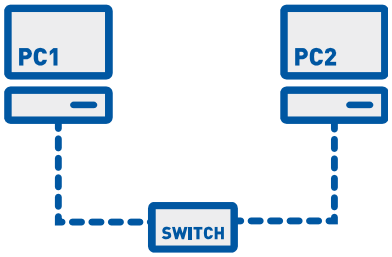
Herausgeber:

Akademie für Lehrerfortbildung und Personalführung
Postfach 1302, 89401 Dillingen
Tel: 09071 53-0

## Inhaltsverzeichnis

# Eingangstest

Für den Eingangstest benötigen Sie zwei Computer mit Windows XP Professional oder Windows 2000. Beide Computer sind miteinander vernetzt. Eine Verbindung mit anderen Geräten, einem Server oder dem Internet ist nicht erforderlich, stört jedoch auch nicht. Zur Konfiguration der beiden Computer benötigen Sie administrative Rechte.

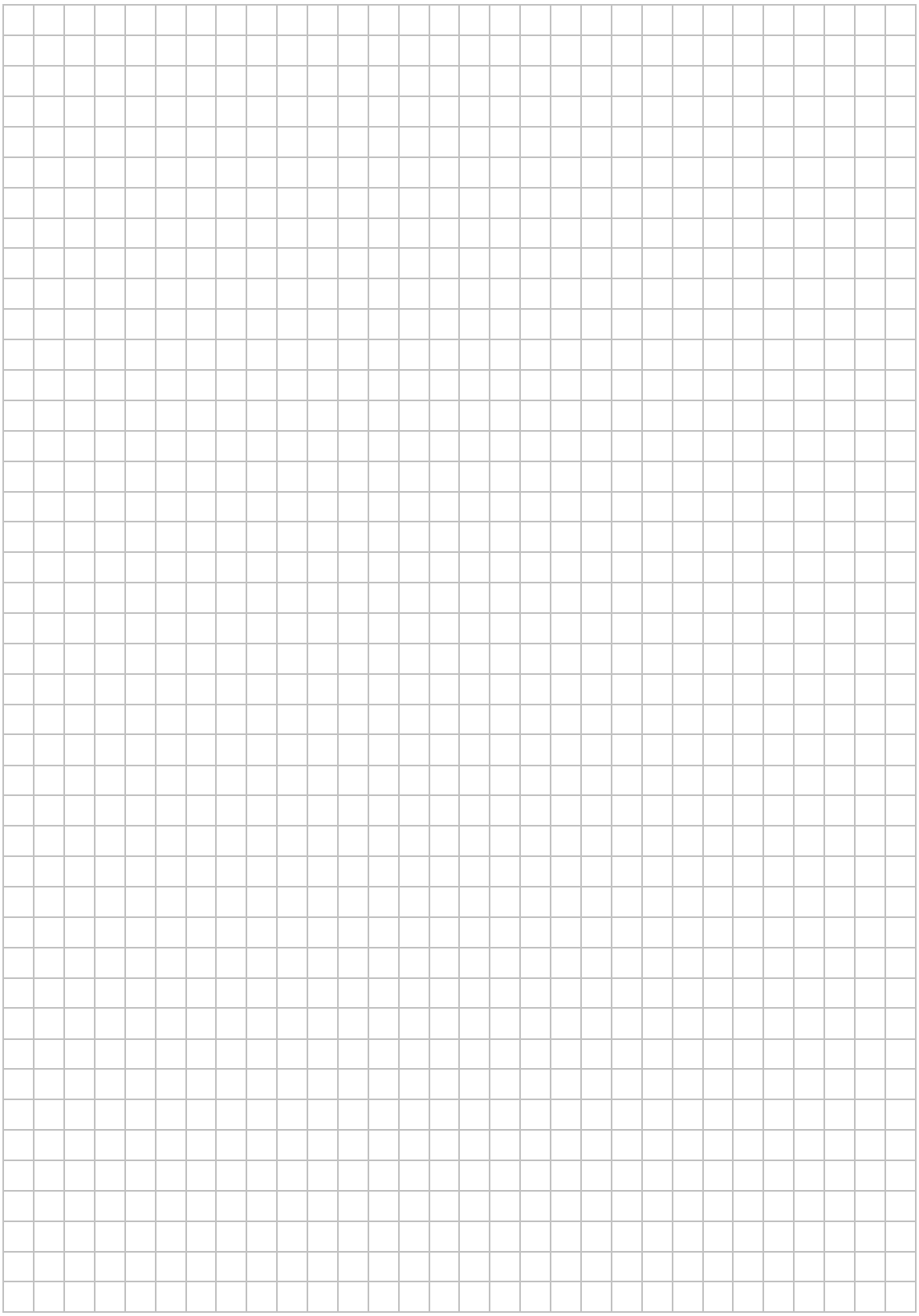



## Aufgaben

1. Konfigurieren Sie beide Computer mit statischen IP-Adressen aus dem Netz 172.20.0.0/16.
2. Testen Sie die Verbindung auf IP-Ebene. Gewährleisten Sie dazu, dass sich beide Computer gegenseitig über einen Ping erreichen können.
3. Ermitteln Sie die MAC-Adressen der beiden Computer.
4. Legen Sie am PC1 die skizzierte Verzeichnisstruktur mit den Ordnern Daten, Austausch und Vorlagen an und geben Sie das Verzeichnis Daten frei. Legen Sie in den Ordnern Austausch und Vorlagen einige Testdokumente ab.


5. Sorgen Sie durch eine geeignete Vergabe der NTFS- und Freigaberechte dafür, dass Sie von PC2 aus auf das Austauschverzeichnis schreibend, auf das Vorlagenverzeichnis jedoch nur lesend zugreifen können.
6. Erstellen Sie ein Systemimage der Systempartition von PC1. Speichern Sie dieses Image auf dem Computer PC2 oder auf einer anderen Partition von PC1.
7. Verändern oder zerstören Sie die Windows-Installation von PC1. Spielen Sie anschließend das vorher erstellte Systemimage wieder zurück.

## Notizen



# Laborübung 01 - Installation von Windows Server 2003

## Szenario

Auf einem Computer wird Windows Server 2003 neu installiert.

## Vorbereitung

- Windows Server 2003 Installations-CD
- Treiber-CD

## Aufgaben

1. Stellen Sie das BIOS so ein, dass der Computer von CD gebootet werden kann. Bootreihenfolge: CD – Festplatte – Diskette
2. Installieren Sie Windows Server 2003 von CD mit folgenden Vorgaben: Systempartition 20 GB, Formatierung mit dem NTFS – Dateisystem.
3. Überprüfen Sie nach der Installation im Gerätemanager die korrekte Installation aller Hardwarekomponenten und installieren Sie bei Bedarf Gerätetreiber nach.
4. Konfigurieren Sie die Netzwerkeinstellungen an Ihrem Computer entsprechend den Erfordernissen (statische IP-Adresse, Gateway, DNS-Server).
5. Überprüfen Sie die Netzwerkfunktionalität mit:
   - *ipconfig /all*
   - *ping* auf das Gateway
   - *ping* auf den DNS-Server
   - *ping* auf www.alp.dillingen.de (Überprüfung der Namensauflösung)
6. Überprüfen Sie in der Ereignisanzeige, ob Warnmeldungen oder Fehler vorliegen und versuchen Sie, die Fehler zu beheben.
7. Erstellen Sie drei weitere Partitionen:
   - Daten (für Austauschverzeichnisse, Images, etc.)
   - Home (Home-Verzeichnisse für die Benutzer, Größe ca. 100 MB pro Benutzer)
   - Profile (Profilverzeichnisse für die Benutzer, Größe ca. 30 MB pro Profil).

## Notizen

## Hinweise

**Gerätemanager**

Startmenü: Systemsteuerung – System – Hardware – Gerätemanager

Kommandozeile: `devmgmt.msc`

**Info über Windows**

Kommandozeile: `winver (winver.exe)`

**Systemkonfigurationsprogramm**

Start – Ausführen: `msconfig`

**Software**

Startmenü: Systemsteuerung – Software (Updates anzeigen)

Kommandozeile: `appwiz.cpl`

**Ereignisanzeige**

Startmenü: Systemsteuerung – Verwaltung – Ereignisanzeige

Kommandozeile: `eventvwr (eventvwr.exe)`

**Informationen zu Fehlermeldungen der Ereignisanzeige**

`http://eventid.net`

`http://microsoft.com/technet/support/ee/ee_advanced.aspx`

**Datenträgerverwaltung**

Arbeitsplatz: Verwalten – Datenträgerverwaltung

**Lizenzmodus nachträglich ändern**

Startmenü: Systemsteuerung – Lizenzierung

**Internet-Explorer – Verstärkte Sicherheitskonfiguration ausschalten**

Startmenü: Systemsteuerung – Software – Windowskomponenten – Verstärkte Sicherheitskonfiguration für Internet-Explorer

## Weiterführende Informationen

### Partitionierung der Festplatte:

Windows Server 2003 wird in einer primären Partition (Basisdatenträger) installiert. Sollen zusätzlich zum Betriebssystem auch Programme auf die Systempartition installiert werden, muss die Größe entsprechend erweitert werden (z. B. 20 GB).

Während der Installation genügt es, nur die Systempartition (NTFS) anzulegen.

### Lizenzierungsart: Pro Server

Bei diesem Lizenzierungsmodell benötigt jede Verbindung zu einem Server eine „CAL“ (Client Access License). Als Verbindungen werden auch Remote-Verbindungen, Drucker-Verbindungen usw. gezählt. In Umgebungen mit nur einem Server kann dieser Lizenzmodus sinnvoll sein. Ein einmaliger Wechsel in den Lizenzmodus "Pro Gerät oder Benutzer" ist möglich.

### Lizenzierungsart: Pro Gerät oder Benutzer

Bei diesem Lizenzierungsmodell benötigt jeder Client oder wahlweise jeder Benutzer eine CAL. Dieses Lizenzierungsmodell eignet sich für Umgebungen mit mehreren Servern. Ein Wechsel in einen anderen Lizenzierungsmodus ist nicht möglich.

### Treiberinstallation am Beispiel einer Fujitsu-Siemens Celsius Workstation

Falls der Netzwerkkartentreiber nicht vorhanden ist, kann dieser über die Treiber-CD nachinstalliert werden.

Aktuelle Treiber findet man auf den Internetseiten des Herstellers:

z. B.: http://www.fujitsu-siemens.de – Support: Seriennummer eingeben oder Gerät auswählen

Spezielle Audio- und Grafikkartentreiber stehen für das Betriebssystem Windows Server 2003 oft nicht zur Verfügung. Es können problemlos die Treiber von Windows XP installiert werden.

### Reihenfolge der Treiberinstallation:

- Aktuelle Version des Chipsatzes installieren.
- Aktuelle Version der Grafikkarte installieren.
- Aktuelle Version der Soundkarte (onboard) installieren.

### Treiber über den Gerätemanager aktualisieren

Eventuell wird im Gerätemanager angezeigt, dass ein Treiber fehlt. Dieser Treiber kann über das Internet aktualisiert werden.

Gerätemanager: Gerät auswählen – Treiber aktualisieren

## Troubleshooting im Netzwerk

| | |
|---|---|
| `ipconfig /all` | Anzeige der IP-Konfiguration des Rechners. |
| `ping alp.dillingen.de` | Überprüft eine Verbindung auf IP-Ebene. |
| `tracert alp.dillingen.de` | Zeigt den tatsächlichen Weg eines IP-Paketes an. |
| `pathping alp.dillingen.de` | Zeigt den tatsächlichen Weg eines IP-Paketes (ab Windows 2000) an. |
| `route print` | Zeigt die Einträge der Routing-Tabelle an. |
| `netstat –r` | Zeigt die Einträge der Routing-Tabelle an. |
| `arp –a` | (address resolution protocol) Liest die Tabelle mit den Zuordnungen von IP-Adressen zu MAC-Adressen im lokalen Netz aus. |
| `arp –d` | Die Einträge in der arp-Tabelle werden gelöscht. |
| `netstat –n` | Bestehende Netzwerkverbindungen werden angezeigt. |
| `nbtstat –c` | Der Cache zur NetBIOS-Namensauflösung wird angezeigt. |

# Laborübung 02 - Systemsicherung des Servers

## Szenario

Der korrekt installierte Windows Server 2003 soll als Image gesichert werden. Auf diese Sicherung kann jederzeit zurückgegriffen werden.

## Vorbereitung/Programme

- Zweite Partition, externe USB-Festplatte oder Fileserver
- Boot-CD mit Imaging-Software (z. B. Drive SnapShot)

## Aufgaben

1. Sichern Sie die Systempartition des Windows Server 2003. Erstellen Sie dazu ein Image der Systempartition auf der Datenpartition (z. B. im Ordner D:\Images).
2. Ändern Sie Einstellungen von Windows oder beschädigen Sie die Systeminstallation (z. B. löschen von C:\ntldr).
3. Übertragen Sie das gespeicherte Image auf die geänderte bzw. beschädigte Systempartition und überzeugen Sie sich, dass Windows Server 2003 ordnungsgemäß wiederhergestellt wurde.

## Notizen

## Hinweise

Mehrere Imaging-Programme erlauben das Sichern der Systempartition aus dem laufenden Windows-Betriebssystem. Für das Zurücksichern des Images ist es jedoch nötig, den Computer von CD oder Diskette zu booten. Einige wenige Imaging-Programme (z. B. Drive SnapShot) ermöglichen das Zurücksichern eines Images beim nächsten Neustart (bei der „normalen“ Startroutine).

# Laborübung 03 - Remoteadministration des Servers

## Szenario

Zur Administration des Servers sollen möglichst komfortable Zugänge und Werkzeuge bereitgestellt werden.

## Aufgaben

### Remote-Administration

1. Ermöglichen Sie am Server die Remotedesktopverbindung und verbinden Sie sich von Ihrem XP-Administrationsrechner aus mit dem Server. Verbinden Sie sich dabei als Administrator.

### Microsoft Management Konsole

2. Stellen Sie mit der Microsoft Management Konsole am Server ein angepasstes Verwaltungswerkzeug bereit, mit dem Sie die Serveradministration durchführen. Binden Sie dabei folgende Snap-Ins ein:
   - DHCP
   - WINS
   - Computerverwaltung des Servers

## Notizen

## Hinweise

### Remotedesktopverbindung aktivieren

| | |
|---|---|
| Arbeitsplatz: | Eigenschaften – Remote – Remotedesktop – Benutzern erlauben eine Remotedesktopverbindung herzustellen |

### Remotezugriff vom Client auf den Server herstellen

| | |
|---|---|
| Startmenü: | Programme – Zubehör – Kommunikation – Remotedesktopverbindung |
| Kommandozeile: | |
| `mstsc` | Microsoft Terminal Server Client |
| `mstsc /admin` | Zugriff auf die Serverkonsole |
| `mstsc /console` | Zugriff auf die Serverkonsole (mit älteren mstsc-Clients) |
| `mstsc /f` | Vollbild-Modus |

### Einrichtung der Microsoft Management Konsole

| | |
|---|---|
| `mmc` | Start der Microsoft Management Konsole |
| Snap-In hinzufügen | Verwaltungswerkzeuge hinzufügen |

## Weiterführende Informationen

### Remotezugriff auf einen Windows-PC

Über das RDP-Protokoll (Remote Desktop Protocol, TCP-Port 3389) kann eine Terminal-Verbindung zu einem Windows-PC hergestellt werden. Bei der Verbindung zu einem Windows XP-Rechner ist nur eine Konsolenverbindung möglich, bei der ggf. ein angemeldeter Benutzer getrennt wird. Zu einem Windows 2003-Server sind gleichzeitig zwei Verbindung und zusätzlich die Konsolenverbindung möglich.

# Laborübung 04 - DHCP und WINS

## Szenario

Der Windows 2003 Server soll als DHCP-Server und WINS-Server arbeiten.

## Aufgaben

1. Installieren Sie, falls noch nicht vorhanden, die Netzwerkdienste DHCP und WINS.
2. Richten Sie den DHCP-Dienst entsprechend den Netzwerkgegebenheiten ein. Sorgen Sie dafür, dass die Clients die eigene IP-Adresse, die IP-Adresse des Standardgateways, des DNS-Servers und des WINS-Servers automatisch über DHCP beziehen. Überprüfen Sie die Funktionsfähigkeit des DHCP-Dienstes am Client.
3. Überprüfen Sie die Konfiguration des WINS-Servers. Stellen Sie fest, welche Clients aktuell den WINS-Server verwenden.

## Notizen

## Hinweise

### Installation von DHCP und WINS

Systemsteuerung: Software – Windows-Komponenten.

### DHCP-Dienst einrichten

Startmenü: Programme – Verwaltung – DHCP

### WINS-Dienst einrichten

Startmenü: Programme – Verwaltung – WINS

## Weiterführende Informationen

## DHCP

DHCP (Dynamic Host Configuration Protocol) ist ein Verfahren, mit dem Computer ihre Netzwerkeinstellungen automatisch zugewiesen bekommen.

Üblicherweise werden folgende Einstellungen mit DHCP übergeben:

- IP-Adresse und Netzwerkmaske
- Gateway
- DNS-Server

Möglich sind noch weitere Zuweisungen, z. B. WINS-Server, Zeitserver, etc.

### DHCP-Kommunikation

| | |
|---|---|
| DHCP-Discover | Der Client sendet eine Anfrage nach einem DHCP-Server. |
| DHCP-Offer | Der DHCP-Server sendet ein Angebot mit Netzwerkeinstellungen. |
| DHCP-Request | Der Client fordert die angebotenen Netzwerkeinstellungen vom DHCP-Server. |
| DHCP-Acknowledge | Der Server bestätigt die Anforderung und Reserviert die IP-Adresse. |

Die DHCP-Kommunikation zwischen Client und Server findet per Broadcast auf den UDP-Ports 67 und 68 statt.

| | |
|---|---|
| `ipconfig` | Anzeige der lokalen IP-Einstellungen |
| `ipconfig /all` | Ausführliche Darstellung |
| `ipconfig /release` | Freigabe der bestehenden IP-Verbindung |
| `ipconfig /renew` | Erneuerung der DHCP-Zuweisung |

**Ablauf der Namensauflösung unter Windows**

Wird ein Computer über einen Namen angesprochen (z. B. ping pc12), muss der Name in eine IP-Adresse aufgelöst werden. Zur Namensauflösung werden folgende Wege der Reihe nach versucht:

- lokaler Hostname
- lokaler DNS-Cache (incl. hosts-Datei)
- Anfrage an den DNS-Server
- lokaler NetBIOS-Cache
- Anfrage an den WINS-Server
- NetBIOS-Broadcast
- lmhosts-Datei

| | |
|---|---|
| `ipconfig /displaydns` | Der DNS-Cache wird angezeigt. |
| `ipconfig /flushdns` | Der DNS-Cache wird geleert. |
| `ipconfig /registerdns` | Erneuert das DHCP-Lease und die Registrierung des Clients beim DNS-Server. |
| `nbtstat -c` | Anzeige des NetBIOS-Cache |
| `nbtstat -n` | Zeigt die lokalen NetBIOS-Namen an |
| `nbtstat -r` | Zeigt eine Statistik an, wie viele Namen über Broadcast bzw. über WINS aufgelöst wurden. |

**NetBIOS/NetBEUI**

| | |
|---|---|
| NetBIOS | Network Basic Input Output System |
| NetBEUI | NetBIOS Extended User Interface |

Der Kommunikationsdienst NetBIOS/NetBEUI wurde 1985 von IBM entwickelt. Er besteht aus drei Teilen:

| | |
|---|---|
| NetBIOS | Schnittstelle für Anwendungen |
| NetBEUI | Transport-Protokoll |
| NDIS | Schnittstelle zur Netzwerkkarte |

Zur Konfiguration von NetBIOS genügen der NetBIOS-Computername und die Arbeitsgruppe. Der NetBIOS-Name darf maximal 15 Zeichen lang sein.

Seit Windows 2000 setzt NetBIOS auf TCP/IP als Transport-Protokoll auf. Um die NetBIOS-Broadcasts zur Namensauflösung zu reduzieren und um die Namensauflösung über Netzwerkgrenzen hinweg zu ermöglichen, wurde WINS eingeführt. NetBIOS wird zunehmend durch DNS abgelöst, einige Dienste verwenden jedoch noch dieses Protokoll. Unter Windows Vista steht dieses Protokoll nicht mehr zur Verfügung.

**WINS**

WINS steht für Windows Internet Name Service und baut auf dem NetBIOS-Dienst auf. Die Clients greifen auf einen WINS-Server zu, um einen Computernamen in eine IP-Adresse aufzulösen.

Wenn ein Windows-Computer gestartet wird, meldet er seinen Namen und IP-Adresse an den WINS-Server. Dieser sammelt die Informationen und gibt sie auf Anfrage an andere Computer heraus. Beim Herunterfahren meldet sich ein Computer wieder bei seinem WINS-Server ab.

Existiert kein WINS-Server, handeln die Computer in der Arbeitsgruppe einen Master Browser aus, der die Informationen der Arbeitsgruppen-Rechner sammelt.

Inkonsistente Zustände können entstehen:

- Nicht allen Mitgliedern der Arbeitsgruppe ist der WINS-Server bekannt.
- Ein Computer wird ausgeschaltet oder vom Netz getrennt, ohne dass er sich beim WINS-Server abmelden konnte.
- Der WINS-Server wird abgeschaltet oder vom Netz getrennt.

WINS verwendet UDP auf Port 137.

**SMB**

Das SMB-Protokoll (Server Message Block) ermöglicht den Zugriff auf Freigaben unter Microsoft Windows. SMB verwendet NetBIOS. Eine Weiterentwicklung von SMB ist CIFS (Common Internet File System), das zur Namensauflösung NetBIOS oder DNS verwendet.

# Laborübung 05 -
# SMB-Zugriff auf einen Windows-Server

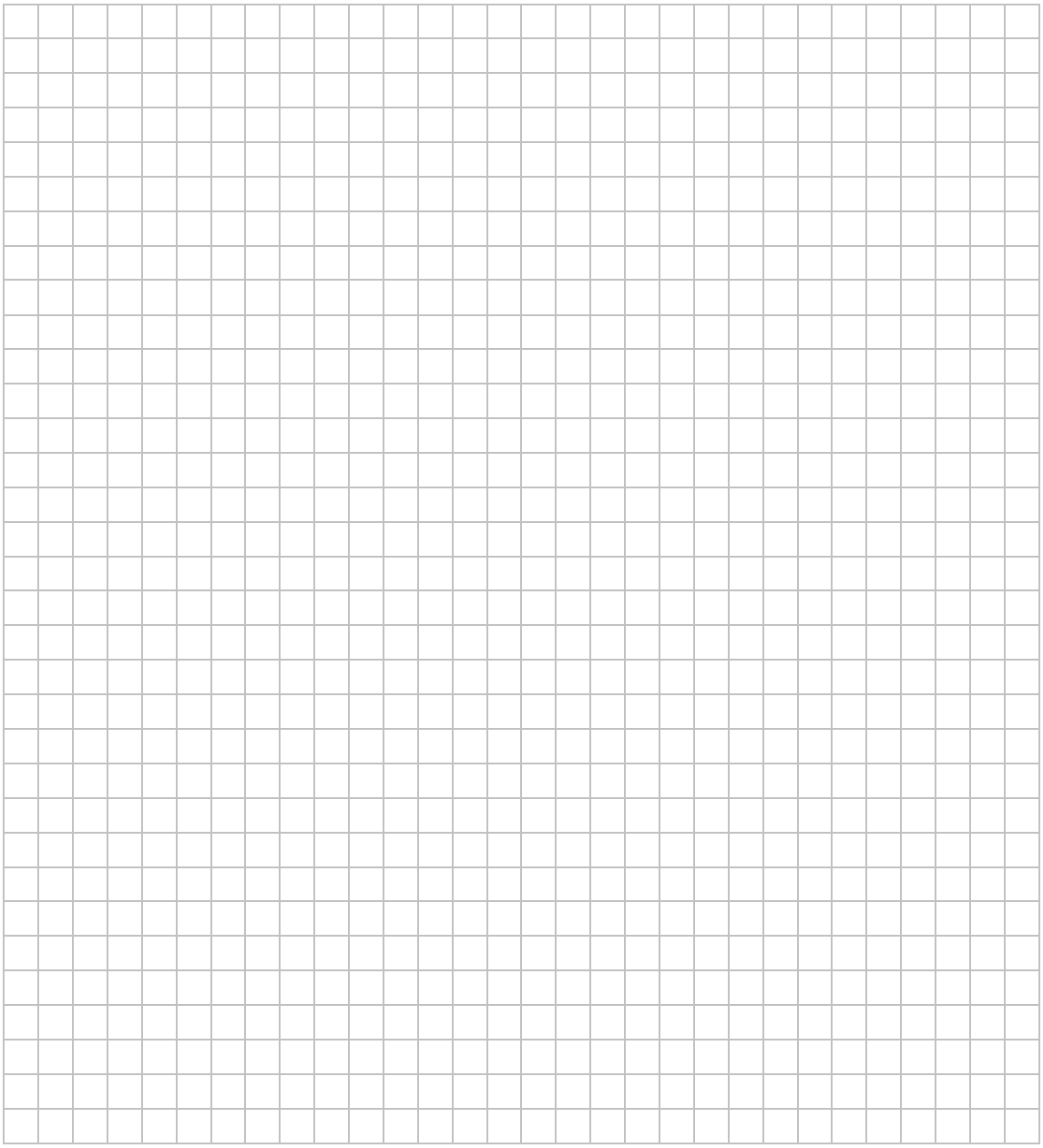
## Szenario

Schüler und Lehrer sollen den Server zur Datenablage und zum Austausch von Dateien nutzen. Im Ordner Austausch sollen alle Benutzer Daten ablegen, austauschen und löschen können. Im Ordner Vorlagen stellen Lehrkräfte den Schülern Unterrichtsmaterial zur Verfügung.


## Aufgaben

1. Legen Sie auf dem Server zwei Gruppen (z. B. Schueler und Lehrer) mit je zwei Benutzerkonten (z. B. s1, s2, l1, l2) an.
2. Erstellen Sie auf dem Server die angegebene Ordnerstruktur und geben Sie den Ordner *Daten* frei.
3. Im Austauschordner sollen die Schüler und Lehrkräfte lesenden und schreibenden Zugriff haben. Im Vorlagenordner können Schüler lesen, Lehrkräfte lesen und schreiben.
4. Greifen Sie vom Arbeitsplatzcomputer mit unterschiedlichen Benutzeraccounts und mit unterschiedlichen Werkzeugen auf die Freigabe am Server zu.
5. Schreiben Sie ein Skript, mit dem Sie sich bei Bedarf am Fileserver anmelden können.
6. Verbinden Sie die Freigabe *Daten* des Fileservers mit einem Laufwerksbuchstaben, so dass bei jedem Neustart des Arbeitsplatzcomputers das Serverlaufwerk verbunden wird.

## Notizen



## Hinweise

**Benutzer- und Gruppenkonten am Fileserver anlegen**

| | |
|---|---|
| Arbeitsplatz: | Verwalten – Lokale Benutzer und Gruppen |

Kommandozeile:

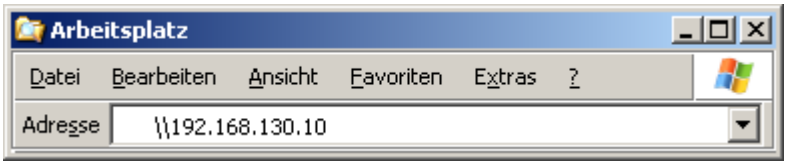
| | |
|---|---|
| `net user s1 12345 /add` | Benutzer s1 mit Passwort 12345 anlegen |
| `net localgroup schueler /add` | Gruppe schueler anlegen |
| `net localgroup schueler s1 /add` | Benutzer s1 zur Gruppe schueler hinzufügen |

### Beispiel für ein Skript zum Anlegen von Benutzern und Gruppen

```
@echo off

REM Benutzer anlegen
net user s1 12345 /add
net user s2 12345 /add

REM Gruppe anlegen
net localgroup schueler /add

REM Benutzer zu einer Gruppe hinzufuegen
net localgroup schueler s1 /add
net localgroup schueler s2 /add
```

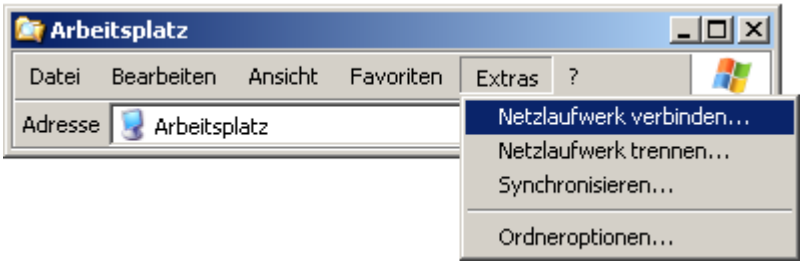
### Zugriff auf Freigaben

Windows-Explorer:




### Netzlaufwerk verbinden

Windows-Explorer:




Kommandozeile:

`net use` *`Laufwerk`*`: \\`*`servername`*`\`*`freigabename`*

`net use x: \\192.168.130.10\Daten`
Die Freigabe wird mit dem Laufwerksbuchstaben x: verbunden.

`net use x: \\192.168.130.10\Daten /user:l1`
Die Freigabe wird mit dem Laufwerksbuchstaben x: verbunden. Zur Authentifizierung wird der Benutzername „l1“ übergeben.

`net use x: \\192.168.130.10\Daten /user:l1 12345`
Die Freigabe wird mit dem Laufwerksbuchstaben x: verbunden. Zur Authentifizierung werden der Benutzername und das Passwort (12345) übergeben.

`net use x: \\192.168.130.10\Daten /persistent:no`
Die Laufwerksverbindung x: wird erstellt und beim Abmelden wieder getrennt.

### SMB-Verbindungen am Fileserver überprüfen

Arbeitsplatz: Verwalten – Freigegebene Ordner – Sitzungen

Kommandozeile: `net session`

### Netzlaufwerk trennen

Windows-Explorer: Extras – Netzlaufwerk trennen

Kommandozeile:

`net use Laufwerk: /delete`

`net use x: /delete` Das Netzlaufwerk x: wird getrennt

`net use *  /delete` Alle Netzlaufwerke werden getrennt

### Zuweisung eines Laufwerksbuchstaben über ein Anmeldeskript (Batch-Datei)

```
@echo off
REM Zuweisen einer Laufwerksverbindung;
REM Vor der Verbindung wird das Laufwerk sicherheitshalber getrennt.

net use x: /delete
net use x: \\192.168.130.10\Daten /persistent:no
```

### Anmeldeskript mit Benutzerabfrage (Batch-Datei)

```
@echo off
REM Zuweisen einer Laufwerksverbindung;

set /P  user="Benutzername: "
net use x: \\192.168.130.10\Daten /user:%user%
```

### Anmeldung über angepasste Tools

Mit einer einfachen Programmier- oder Skriptsprache wird ein kleines Tool erstellt, das den Benutzern eine komfortable Anmeldung erlaubt.

# Laborübung 06 -
# Die Rechtestruktur auf einem Windows-Server

## Szenario

Die angelegte Ordnerstruktur soll gegen versehentliche oder absichtliche Veränderungen geschützt werden.


## Aufgaben

1. Im freigegebenen Ordner *Daten* soll ein Benutzer keine weitere Ordner oder Dateien anlegen können.
2. Überprüfen Sie, ob ein Schüler oder eine Lehrkraft in der Lage ist, das Austauschverzeichnis versehentlich zu löschen und verhindern Sie dies gegebenenfalls.
3. Im Vorlagenordner sollen die Lehrkräfte ihre Daten nur in selbst erstellten Ordnern ablegen können. Die Lehrkräfte sollen sich die Daten gegenseitig nicht überschreiben oder löschen können. Schüler und Lehrer können lesend auf alle Dateien zugreifen.
4. Auf den Ordner Lehreraustausch sollen Schüler keinen Zugriff haben. Sorgen Sie dafür, dass die Schüler diesen Ordner nicht sehen.

## Hinweise

Windows ermöglicht es, NTFS-Rechte sehr differenziert zu vergeben. In den meisten Fällen genügt es jedoch, Leserechte, Lese-/Schreibrechte und Vollzugriff zu unterscheiden.

### Leserecht

Als Leserecht werden die NTFS-Rechte Lesen, Ausführen, Ordnerinhalt auflisten, Lesen zusammengefasst.

### Lese-/Schreibrecht

Beim Lese-/Schreibrecht kommen noch zusätzlich die Rechte Ändern und Schreiben hinzu.

### Vollzugriff

Der Vollzugriff beinhaltet das Lese-/Schreibrecht. Zusätzlich beinhaltet er noch das Recht Rechte zu vergeben und den Besitz von Dateien zu übernehmen.

### Rechteabhängige Anzeige von Ordnern und Dateien

Beim Zugriff auf ein Netzlaufwerk stört es manchmal, wenn Dateien und Ordner angezeigt werden, auf die kein Zugriff besteht. Durch ein Zusatzpaket für den Server (Access-Based Enumeration User Interface, ABEUI.msi) kann dies unterbunden werden.

Suchbegriffe im Internet: ABEUI.msi, download.

## Weiterführende Informationen

### Zusammenspiel zwischen Freigaben und NTFS-Rechten

Um über das SMB- bzw. CIFS-Protokoll auf einen Windows-Server zugreifen zu können, ist eine Freigabe am Windows-Server notwendig. Diese Freigabe ist das Eingangstor zum Server.

Die Freigabe kann mit bestimmten Rechten für verschiedene Benutzer versehen werden (Freigabeberechtigungen). Diese Freigabeberechtigungen stellen die maximalen Rechte dar, die ein Benutzer haben kann, wenn er auf diesem Weg auf den Server zugreift. Durch die NTFS-Rechte können die Rechte eines Benutzers weiter eingeschränkt sein.

Eine gebräuchliche Praxis ist es, Freigaben mit den Freigabeberechtigungen „Jeder – Vollzugriff“ oder „Jeder – Ändern“ zu versehen. Die eigentlichen Beschränkungen für einen Benutzer erfolgen über die NTFS-Rechte (Sicherheitseinstellungen).

# Laborübung 07 - Einrichten eines Domänencontrollers

## Szenario

Ein Windows 2003 Server soll zum Domänencontroller hoch gestuft werden.

## Aufgaben

1. Installieren Sie, falls noch nicht vorhanden, den Netzwerkdienst DNS. über die Systemsteuerung -> Software-> Windows-Komponenten (nur Installation, keine Konfiguration).
2. Richten Sie Ihren Windows 2003 Server unter folgenden Vorgaben als Domänencontroller ein:
   - Erster Domänencontroller des Netzwerkes
   - DNS-Name der Domäne: z. B. alp10.local
   - NetBIOS-Name der Domäne: z. B. ALP10
   - Übernehmen Sie die Standardeinstellungen für die Speicherorte (Datenbank, Protokoll, …)
   - DNS soll automatisch angelegt werden.
3. Geben Sie an, welche Änderungen der Assistent bei der Einrichtung des Domänencontrollers vorgenommen hat. Überprüfen Sie dabei insbesondere
   - die TCP/IP-Netzwerkeinstellungen
   - die lokale Benutzerverwaltung
   - die neu hinzugekommenen Verwaltungsprogramme
4. Überprüfen Sie die Namensauflösung mit nslookup. Testen Sie dabei insbesondere die Namensauflösung und IP-Adressen-Auflösung des Domänencontrollers
5. Vervollständigen Sie die Einträge des DNS-Dienstes: Erstellen Sie eine Reverse-Lookupzone, so dass auch die Auflösung der IP-Adressen in Rechnernamen funktioniert. Überprüfen Sie die Reverse-Namensauflösung mit nslookup.

## Notizen

## Hinweise

### Server zum Domänencontroller hoch stufen

| | |
|---|---|
| `dcpromo` | domain controller promotion |

Der Assistent zum Einrichten des DNS-Servers kann den zu verwaltenden Netzwerkbereich nicht eindeutig erkennen, wenn am Server mehrere Netzwerkkarten aktiv sind oder der Server mit mehreren IP-Adressen arbeitet.

### nslookup (Name Server Lookup)

Mit nslookup kann man einen Nameserver nach der Auflösung eines Namens oder einer IP-Adresse fragen.

`nslookup <aufzulösende Adresse/aufzulösender Name> <DNS-Server>`

Wird der DNS-Server nicht angegeben, so wird der in den Netzwerkeinstellungen angegebenen Nameserver befragt.

| | |
|---|---|
| `nslookup alp.dillingen.de` | Anfrage an den Standard-DNS-Server bezüglich der IP-Adresse von alp.dillingen.de. |
| `nslookup 194.95.207.10` | Anf rage an den Standard-DNS-Server bezüglich des Rechnernamens für die IP-Adresse 194.95.207.10. |
| `nslookup alp.dillingen.de www.dillingen.de` | Anfrage an den DNS-Server www.dillingen.de bezüglich der IP-Adresse von alp.dillingen.de. |

### Antworten von nslookup

| | |
|---|---|
| `Server: hs16p00.alp130.local` | Name des DNS-Servers, der die Anfrage entgegen nimmt. |
| `Adresse: 192.168.130.10` | IP-Adresse des DNS-Servers, der die Anfrage entgegen nimmt. |
| `Nicht autorisierte Antwort:` | Der angefragte DNS-Server hat die Anfrage nicht selbst beantwortet, sondern an einen anderen DNS-Server weitergeleitet. |
| `Name:` www.alp.dillingen.de | Name des angefragten Rechners. |
| `Address(es): 194.95.207.10` | IP-Adresse bzw. IP-Adressen des angefragten Rechners. |
| `Aliases: alp.dillingen.de` | Weitere Namen des angefragten Rechners. |

## Weiterführende Informationen

### Werkzeuge zur Verwaltung von Domänen

- Active Directory-Benutzer und -Computer (dsa.msc):
  Verwaltung der Benutzer und Computer
- Active Directory-Standorte und -Dienste (dssite.msc):
  Verwaltung der Replikation von Verzeichniseinträgen
- Active Directory-Domänen und -Vertrauensstellungen (domain.msc)
  Verwaltung zusammengehöriger Domänen

Die letzten beiden Verwaltungswerkzeuge sind nur in Strukturen mit mehreren Domänen oder mehreren Standorten nötig.

### Sysvol-Freigabe

Die Sysvol-Freigabe ist auf jedem Domänencontroller vorhanden. Der Inhalt dieser Freigabe wird auf allen Domänencontrollern synchron gehalten.

### Netlogon-Freigabe

Die Netlogon-Freigabe ist ein Unterverzeichnis von Sysvol und wird damit auch auf allen Domänencontrollern synchron gehalten. Dieses Verzeichnis eignet sich z. B. um Anmeldeskripte zu hinterlegen.

## Betriebsmasterfunktionen und FSMO-Rollen

Die Active-Directory-Datenbank wird zwischen allen Domänencontrollern einer Domäne synchronisiert. Man erhält dadurch eine gewisse Redundanz und Sicherheit. Bestimmte Funktionen dürfen in einer Domäne jedoch nur einmal vorhanden sein.

Auch in einer Gesamtstruktur mit mehreren Domänen müssen bestimmte Aufgaben (z. B. Benennung von Domänen) von einer einzigen Stelle kontrolliert werden.

Insgesamt gibt es fünf Rollen, die lediglich auf einem Domänencontroller laufen. Diese FSMO-Rollen (Flexible Single Master Operation) oder Betriebsmaster-Funktionen müssen ggf. vor dem Austausch eines Domänencontrollers auf einen anderen Domänencontroller übertragen werden.

### FSMO-Rollen in der Gesamtstruktur

Domänennamen-Master
: Kontrolliert das Hinzufügen, Entfernen oder Umbenennen von Domänen in der Gesamtstruktur.

Schema-Master
: Im Schema sind alle Objekte und Attribute definiert, die im Active-Directory vorkommen können. Jede Active-Directory-Gesamtstruktur hat nur ein Schema. Der Schema-Master kontrolliert Änderungen im Active Directory-Schema.

**FSMO-Rollen in einer Domäne**

| | |
|---|---|
| PDC-Emulator | In Domänen mit NT4 Backup-Domänencontrollern (BDCs) fungiert der PDC-Emulator als Primary Domain-Controller. Darüber hinaus ist er für die Aktualisierung von Kennwortänderungen, für die Durchsetzung von Gruppenrichtlinien und für die Zeitsynchronisation erforderlich. |
| RID-Master | In einer Domäne ist jedem AD-Objekt eine eindeutige SID (Security-ID) zugeordnet, die aus der Domänen-ID und einer relativen ID (RID) besteht. Die RIDs werden den Domänencontrollern in Blöcken von ca. 500 Stück zur Verfügung gestellt. Ein Domänencontroller kann nur so lange neue Objekte anlegen bis alle RIDs verbraucht sind. |
| Infrastrukturmaster | Der Infrastrukturmaster verwaltet den Globalen Katalog (Suchindex über alle ADs in der Gesamtstruktur). Er ist für die Aktualisierung von Verweisen von Objekten innerhalb der Domäne und zu Objekten in anderen Domänen verantwortlich. In Strukturen mit nur einer Domäne spielt der Infrastrukturmaster praktisch keine Rolle. |

## DNS (Domain Name System)

Das DNS ist ein hierarchisch aufgebauter Namensraum für Internetadressen.

**Domäne bzw. DNS-Domäne**

Ein zusammenhängender Teilbereich des DNS-Namensraumes z. B. alp.dillingen.de

**Domäne bzw. Windows-Domäne**

Lokaler Sicherheitsbereich mit zentraler Verwaltung

**FQDN (Full Qualified Domain Name)**

Vollständiger Name einer Domäne oder eines Computers im DNS-Namensraum z. B. alp.dillingen.de oder server1.alp.dillingen.de.

**Zone bzw. DNS-Zone**

Ein zusammengehöriger Bereich des DNS-Baumes, der von einem Nameserver verwaltet wird. Eine Zone ist ein administrativer Bereich, der mehrere Domänen enthalten kann. Üblicherweise ist eine Zone mit einer Domäne identisch.

**DNS-Server**

Ein Computer, auf dem der DNS-Serverdienst läuft. Ein DNS-Server verwaltet eine oder mehrere Zonen und löst DNS-Abfragen auf.

**Nameserver**

Ein DNS-Server für eine bestimmte Zone.

**Autorisierender Nameserver**

Ein Nameserver, der die Befugnis zum Auflösen von DNS-Namen für eine bestimmte Zone hat. Jeder Computer in dieser Zone (für den eine DNS-Namensauflösung erfolgen soll) muss diesem Nameserver bekannt sein. Jede Zone hat mindestens einen autorisierenden Nameserver.

**Forward-Lookupzone**

Die Forward-Lookupzone stellt die Zuordnung zwischen einem Domänennamen und der IP-Adresse her.

**Reverse-Lookupzonen**

Eine Reverse-Lookupzone verwaltet die Informationen, die zum Auflösen von IP-Adressen in DNS-Namen nötig sind.

Um die Auflösung von IP-Adressen zu ermöglichen, verwendet man die fiktive Domäne Die IP-Netze sind Subdomänen dieser fiktiven Domäne, also z. B. 130.168.192.in-addr-arpa für das Netzwerk 192.168.130.0/24.

Die umgekehrte Namensauflösung kann von einigen Diensten (z. B. Mail-Servern) gefordert werden, um zu überprüfen, mit welchem Server diese kommunizieren. Für den Betrieb von Windows-Netzen oder für Active-Directory ist sie nicht erforderlich.

**Ressourceneinträge (Ressource Record, RR)**

Ein Eintrag in der DNS-Datenbank wird als Ressourceneintrag bezeichnet.

Beispiele:

| | |
|---|---|
| Host-Eintrag (A-Record): | Auflösung eines DNS-Namens in eine IP-Adresse. |
| Alias-Eintrag (CNAME-Record): | Alias-Name eines Computers |
| Nameserver-Eintrag (NS-Record): | Liste der Nameserver, die schreibend auf eine Zone zugreifen dürfen. |
| Start-of-Authority-Eintrag (SOA): | Markiert den Beginn einer Zone. |
| Service-Eintrag (SRV-Record) | Service-Eintrag des Domain-Controllers, damit die Dienste erreicht werden können (z. B. Globaler Katalog, Gruppenrichtlinien, Anmeldung in der Domäne). |
| Zeiger-Eintrag (PTR-Record) | Auflösung von IP-Adressen in Namen. |

**DNS-Resolver**

Ein Dienst, der auf den Client-Computern ausgeführt wird, um DNS-Namen aufzulösen bzw. DNS-Server abzufragen.

**hosts-Datei**

Die hosts-Datei ist eine Textdatei auf einem Client zur manuellen Zuordnung von Hostnamen zu IP-Adressen. Unter Windows XP befindet sich die Datei im Verzeichnis Windows\system32\drivers\etc.

**DNS-Namensauflösung unter Windows**

Wird ein Computer über einen Namen angesprochen (z. B. ping pc12), muss der Name in eine IP-Adresse aufgelöst werden. Zur DNS-Namensauflösung werden der Reihe nach folgende Wege versucht:

- lokaler Hostname
- lokaler DNS-Cache (incl. hosts-Datei)
- Anfrage an den DNS-Server

Ist die DNS-Namensauflösung nicht erfolgreich, wird versucht, über den NetBIOS-Dienst den Namen aufzulösen (siehe NetBIOS/WINS).

| | |
|---|---|
| `ipconfig /displaydns` | Anzeige des DNS-Cache. |
| `ipconfig /flushdns` | Leert den DNS-Cache. |
| `ipconfig /registerdns` | Erneuert das DHCP-Lease und die Registrierung des Clients beim DNS-Server. |

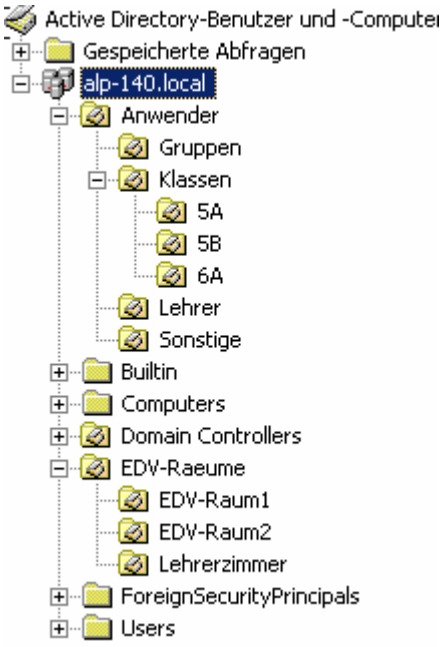
# Laborübung 08 - Einrichten einer Domänenstruktur

## Szenario

Die vorhandene Schulstruktur wird in der Domänenstruktur abgebildet.

## Aufgaben

1. Richten Sie eine Domänenstruktur nach folgendem Muster ein.




2. Verschieben Sie die bisher angelegten Benutzer in die entsprechenden Organisationseinheiten.
3. Nehmen Sie die Clients in die Domäne auf und verschieben Sie diese ggf. in die entsprechende Organisationseinheit.
4. Melden Sie sich an einem Client als Domänenbenutzer an und greifen Sie auf eine Freigabe am Server zu.
5. Legen Sie einen neuen Benutzer an und vergeben Sie ihm ein gültiges Passwort nach den geltenden Komplexitätsrichtlinien.
6. Ändern Sie die Sicherheitsrichtlinie für Domänen so ab, dass auch kurze und einfache Kennwörter erlaubt sind.

## Hinweise

**Client in die Domäne aufnehmen**

| | |
|---|---|
| Arbeitsplatz: | Eigenschaften – Computername – Ändern |

**Einfache Kennwörter**

| | |
|---|---|
| Sicherheitsrichtlinie für Domänen: | Sicherheitseinstellungen – Kontorichtlinien |

**Anwendung der Kennwortrichtlinie**

| | |
|---|---|
| `gpupdate` | Bewirkt, dass eine Richtlinie sofort und nicht erst nach der nächsten planmäßigen Aktualisierung wirkt. |

## Notizen

# Weiterführende Informationen

## Das Active Directory

Das Active Directory ist eine Datenbank in der Informationen über Benutzer, Gruppen und Computer gespeichert werden. Diese sogenannten Objekte werden in Organisationseinheiten (Organizational Unit, OU) zusammengefasst und verwaltet.

### Standardcontainer im Active Directory

| | |
|---|---|
| Builtin | Vom System vordefinierte Gruppen. Diese können weder gelöscht noch umbenannt oder verschoben werden. |
| Computers | Computer, die neu in die Domäne aufgenommen werden. |
| Domain Controllers | Alle Domänencontroller der Domäne |
| Foreign Security Principals | SIDs (Security-IDs) aus anderen Domänen, zu denen eine Vertrauensstellung existiert. |
| Users | Benutzer und Gruppen, die automatisch angelegt werden. |

Mit Ausnahme der Domain Controllers sind die Standardcontainer nicht als Organisatorische Einheiten (OUs) definiert. Deshalb stehen für diese Container bestimmte Funktionen (z. B. Gruppenrichtlinien) nicht zur Verfügung.

## Sicherheitsrichtlinien

Für jeden Windows-PC existieren lokale Sicherheitsrichtlinien, die auch als Gruppenrichtlinien bezeichnet werden. Sind die Windows-PC Mitglied einer Domäne, dann wirken zusätzlich die Domänenrichtlinien. Für Domänencontroller gelten außerdem die Domänencontrollerrichtlinien, die üblicherweise sehr restriktiv sind.

### Lokale Richtlinien (gpedit.msc)

Seit Windows 2000 befindet sich auf jedem Computer mit installiertem Windows ein lokales Gruppenrichtlinienobjekt, das über gpedit.msc aufgerufen wird.

### Die Standard-Domänenrichtlinie

Die Standard-Domänenrichtlinie (Default Domain Policy) ist mit der Domäne verknüpft und wirkt über die Richtlinienvererbung auf alle Benutzer und Computer in der Domäne.

### Die Standard-Domänencontrollerrichtlinie

Die Standard-Domänencontrollerrichtlinie (Default Domain Controller Policy) ist mit der Domänencontroller-Organisationseinheit verknüpft, in der standardmäßig die Computerkonten für Domänencontroller gespeichert sind.

**Komplexitätsrichtlinien für Passwörter**

Wenn die Komplexitätsrichtlinien aktiviert sind, muss ein Passwort aus mindestens sieben Zeichen aus drei verschiedenen Kategorien verwendet werden: Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen.

# Laborübung 09 - Gruppenrichtlinien

## Szenario

Im EDV-Raum soll die Administration der Clients zentral erfolgen. Einigen Benutzern soll eine eingeschränkte Umgebung präsentiert werden.

## Aufgaben

1. Installieren Sie die Gruppenrichtlinien-Verwaltungskonsole „gpmc“ auf dem Server.
2. Erstellen Sie eine Richtlinie, die es verbietet, die Systemsteuerung aufzurufen. Ordnen Sie diese Richtlinie der Organisationseinheit „Klassen“ zu, in der sich alle Schüler befinden. Testen Sie die Funktionalität der Gruppenrichtlinie.
3. Entfernen Sie bei den Eigenschaften eines Ordners oder einer Datei die Registerkarte „Sicherheit“.
4. Blenden Sie für die Schüler die Netzwerkumgebung im Windows-Explorer aus.
5. Erzwingen Sie für alle Benutzer das „Klassische Startmenü“.

## Hinweise

### Gruppenrichtlinien-Verwaltungskonsole

Suchbegriffe im Internet: gpmc.msi, download.

### Systemsteuerung verbieten

Benutzerkonfiguration – Administrative Vorlagen – Systemsteuerung

### Registerkarte Sicherheit entfernen

Benutzerkonfiguration – Administrative Vorlagen – Windows-Komponenten – Windows-Explorer – „Registerkarte Sicherheit entfernen“

### Klassisches Startmenü erzwingen

Benutzerkonfiguration – Administrative Vorlagen – Startmenü und Taskleiste „Klassisches Startmenü erzwingen“

### Netzwerkumgebung ausblenden

Benutzerkonfiguration – Administrative Vorlagen – Windows Komponenten – Windows-Explorer „Benachbarte Computer“ nicht unter Netzwerkumgebung anzeigen

Benutzerkonfiguration – Administrative Vorlagen – Windows Komponenten – Windows-Explorer – Symbol „Gesamtes Netzwerk“ nicht in „Netzwerkumgebung“ anzeigen

Benutzerkonfiguration – Administrative Vorlagen – Desktop – Desktopsymbol „Netzwerkumgebung“ ausblenden

### Aktualisierung der Gruppenrichtlinien

Gruppenrichtlinien werden automatisch ca. alle 90 Minuten vom Client aktualisiert. Mit dem Befehl gpupdate (am Client) können die Richtlinien sofort aktualisiert werden. Einige Richtlinien wirken erst nach einem Neustart des Computers oder nach dem erneuten Anmelden des Benutzers.

| | |
|---|---|
| `gpupdate` | Das Gruppenrichtlinienmodul am Client liest neue oder veränderte Richtlinien ein (Group Policy Update). |
| `gpupdate /force` | Erzwingt, dass alle Gruppenrichtlinien neu gelesen und angewandt werden. |
| `secedit /refreshpolicy` | Group Policy Update bei Windows 2000 |

## Weiterführende Informationen

### Gruppenrichtlinien

Gruppenrichtlinien sind ein Werkzeug, um in einer Active-Directory Domäne Systemeigenschaften, Sicherheitseinstellungen oder Profileigenschaften zu definieren.

In Domänenstrukturen sind diese Richtlinien hierarchisch geordnet. Gruppenrichtlinien werden auf Organisationseinheiten vergeben und wirken auf alle Benutzer und Computer in dieser Organisationseinheit.

### Voraussetzungen:

Windows 2000 Domänencontroller (oder Nachfolger)
Clients mit Windows 2000, XP, Vista (in die Domäne eingebunden)
DNS-Server mit SRV-Unterstützung (Service-Records)

### Systemrichtlinien

Als Vorläufer der Gruppenrichtlinien gelten die Systemrichtlinien oder Policies von Windows NT 4, die z. B. mit poledit.exe erzeugt werden. Befindet sich in der Netlogon-Freigabe des Domänencontrollers eine Datei config.pol bzw. ntconfig.pol, wird diese beim Anmelden von einem Windows 95/98/ME bzw. NT-Client ausgelesen und ausgeführt. Damit können jedoch nur Richtlinien gesetzt werden, die prinzipiell auch vom Benutzer selbst gesetzt werden können.

### Speicherort der Gruppenrichtlinien

Gruppenrichtlinien werden auf dem Domänencontroller im freigegebenen Verzeichnis SYSVOL unter <Domäne>\Policies gespeichert.

### Hierarchie der Gruppenrichtlinien

Die Verarbeitung der lokalen Sicherheitseinstellungen und der Gruppenrichtlinienobjekte in der Domäne erfolgen in einer bestimmten Reihenfolge:

- Lokales Gruppenrichtlinienobjekt
- Domänen-Gruppenrichtlinienobjekte
- Gruppenrichtlinienobjekte der Organisationseinheit, von der übergeordneten zur untergeordneten Organisationseinheit.

Wird eine Richtlinie in mehreren Ebenen mit unterschiedlichen Einstellungen aktiviert, dann setzt sich die zuletzt abgearbeitete Richtlinie (OU-Richtlinie) durch.

### Ausnahmen der Hierarchie

- Eine Richtlinie kann erzwungen werden und wird damit nicht mehr durch eine nachgeordnete Richtlinie überschrieben.
- Bestimmte Richtlinien wirken nur, wenn sie auf Domänenebene vergeben werden (z. B. Kennwortrichtlinien).

### Kontrolle der Gruppenrichtlinien

| | |
|---|---|
| Am Client: | rsop.msc (Resultant Set of Policies) |
| | gpresult.exe |
| Am Server: | Gruppenrichtlinienverwaltung – Gruppenrichtlinienmodellierung Simulation eines Szenarios anhand der Zugehörigkeit eines Computers oder Benutzers zu einer Organisationseinheit (OU). |
| | Gruppenrichtlinienverwaltung – Gruppenrichtlinienergebnisse Darstellung der tatsächlich auf einen Computer oder Benutzer wirkenden Gruppenrichtlinien. |

## Weitere Beispiele für Gruppenrichtlinien

### Einfache Kennwörter

Sicherheitsrichtlinie für Domänen – Sicherheitseinstellungen – Kontorichtlinien

### Zwischengespeicherte Profile löschen

Computerkonfiguration – Administrative Vorlagen – System – Benutzerprofile
„Zwischengespeicherte Kopien von servergespeicherten Profilen löschen“

**Willkommenseite unterdrücken**

Computerkonfiguration – Administrative Vorlagen – System – Anmeldung
„Willkommensseite für erste Schritte bei der Anmeldung nicht anzeigen“

**Nur zugelassene Anwendungen ausführen**

Benutzerkonfiguration – Administrative Vorlagen – System

**Nachrichtendienst (net send) unterbinden**

Computerkonfiguration – Windows-Einstellungen – Systemdienst – Nachrichtendienst

**Beim Anmelden auf Netzwerk warten**

Unter Windows XP wird der Windows-Explorer vor dem Netzwerk geladen. Desktop-einstellungen, die mit Gruppenrichtlinien festgelegt wurden, können daher nicht übernommen werden. Der Computer arbeitet mit den "Cached Logon Credentials". Auch die Softwareverteilung gelingt nur mit der Einstellung:

Computerkonfiguration – Administrative Vorlagen – System – Anmeldung
"Beim Neustart des Computers und bei der Anmeldung immer auf das Netzwerk warten".

**„Netzlaufwerk verbinden“ aus dem Windows-Explorer entfernen**

Benutzerkonfiguration – Administrative Vorlagen – Windows Komponenten – Windows-Explorer – Optionen „Netzlaufwerk verbinden und Netzlaufwerk trennen“ entfernen.

**Zugriff auf Systemsteuerungselemente regeln**

Benutzerkonfiguration – Administrative Vorlagen – Systemsteuerung – Nur angegebene Systemsteuerungssymbole anzeigen „Angegebene Systemsteuerungselemente ausblenden“

| | |
|---|---|
| Appwiz.cpl: | Software |
| Desk.cpl: | Anzeigeeigenschaften |
| Main.cpl: | Mauseinstellungen |

**Regelmäßige Änderung des Computerkennworts verhindern**

Standardmäßig ändert ein Computer ca. alle 30 Tage das Kennwort mit dem er sich beim Domänencontroller authentifiziert. Dies kann zu Problemen führen, wenn der Computer mit einem Festplattenschutz arbeitet oder ein vorheriges Image zurück gespielt wird.

Computerkonfiguration – Lokale Richtlinie – Sicherheitsoptionen – „Domänenmitglied: Änderungen von Computerkennwörtern deaktivieren“

# Laborübung 10 - Servergespeicherte Profile

## Szenario

Jede Lehrkraft soll an jedem Computer der Domäne ihre persönlichen Desktop-Einstellungen (Hintergrund, Verknüpfungen usw.) und ihre persönlichen Windows-Explorer-Einstellungen vorfinden und diese entsprechend ihren Vorstellungen abändern dürfen. Es werden dazu servergespeicherte Profile verwendet.

## Aufgaben

1. Erstellen Sie auf der Partition, auf der die Profile abgelegt werden einen Ordner z. B. „Profile“ und geben Sie diesen frei. Übernehmen Sie die unten angegebene Ordnerstruktur.


2. Sorgen Sie dafür, dass jede Lehrkraft unterhalb des Ordners „Lehrer“ berechtigt ist, den Profilordner anzulegen.
3. Weisen Sie der Lehrkraft den jeweils passenden Profilpfad zu und melden Sie sich an einem Client als diese Person an und wieder ab. Überprüfen Sie, ob das Profil auf den Server geschrieben wurde. Zeigen Sie, dass Sie als Administrator standardmäßig keinen Zugriff auf dieses Profil haben.
4. Sorgen Sie über eine entsprechende Gruppenrichtlinie dafür, dass bei zukünftig angelegten Profilen die Administratoren nicht ausgesperrt bleiben.

## Weiterführende Aufgabe

Wenn Sie die Rechte in der Profilfreigabe auf den Standardeinstellungen belassen haben, besteht für alle Benutzer die Möglichkeit, die Profilfreigabe als weitere Datenablage zu missbrauchen.

5. Ändern Sie die NTFS-Rechte des Profilordners bzw. der Unterordner so ab, dass Benutzer neue Profile erstellen können, aber unberechtigte Zugriffe möglichst ausgeschlossen sind.

## Hinweise

### Profilpfad festlegen

Der Profilpfad wird im Active Directory beim jeweiligen Benutzer eingetragen.
\\server\freigabe\Ordnerstruktur\%username%

### Administrativer Zugriff auf Profile

Über eine Computergruppenrichtlinie kann dem Administrator Einblick in neu angelegte Profilordner der Benutzer gewährt werden.
Computerkonfiguration – Administrative Vorlagen – System – Benutzerprofile – „Sicherheitsgruppe Administratoren zu servergespeicherten Profilen hinzufügen“.

## Weiterführende Informationen

### Default User-Profil

Hat ein Benutzer noch kein eigenes Profil, wird das „Default User“-Profil als Vorlage genommen.

### NTFS-Berechtigungen für den Profilordner

Der Profilordner des Benutzers für das servergespeicherte Profil wird automatisch bei der Anmeldung des Benutzers angelegt, wenn im Benutzerprofil ein Profilpfad angegeben wurde. Für diesen Vorgang braucht der Benutzer zusätzlich zu den Leserechten die Berechtigung einen Ordner zu erstellen.

Minimale Berechtigungen der Benutzer für den Profilordner, damit neue Profile angelegt werden können:

Übernehmen für: „Nur in diesem Ordner“
☑ Ordner durchsuchen
☑ Ordner auflisten
☑ Attribute lesen
☑ Erweiterte Attribute lesen
☑ Ordner erstellen
☑ Berechtigungen lesen

# Laborübung 11 - Erstellen eines Standardprofils

## Szenario

Die Schüler sollen ein verbindliches Standardprofil erhalten, das Sie als Systembetreuer entsprechend den Erfordernissen angepasst haben. Die Lehrkräfte erhalten beim ersten Anmelden an der Domäne dieses Standardprofil als Vorlage und können es jedoch für ihre Zwecke anpassen.

## Aufgaben

1. Erstellen Sie ein Musterprofil für Lehrkräfte und Schüler an einem Desktop-Computer (administrative Rechte) nach folgenden Vorgaben:
   - Passen Sie Startmenü, Taskleiste und Desktop so an, dass diese der klassischen Windows-Ansicht entsprechen.
   - Passen Sie die Anzeige im Windows-Explorer so an, dass alle Dateien sowie die Dateierweiterungen angezeigt werden und dass die Dateien und Ordner immer in der Detailansicht erscheinen.
2. Kopieren Sie dieses Profil für die Lehrkräfte in den Ordner „Default User“ auf der Netlogon-Freigabe und für die Schüler in eine Freigabe auf der Partition „Profile“. Sichern Sie das Schülerprofil gegen Änderungen (verbindliches Profil, Schreibschutz).
3. Weisen Sie den Lehrkräften und Schülern den jeweils passenden Profilpfad zu.
4. Melden Sie sich als Lehrkraft in der Domäne an und kontrollieren Sie, ob Sie das richtige Profil bekommen. Ändern Sie als Lehrkraft Einstellungen an Ihrem Profil und überprüfen Sie, ob die Änderungen dauerhaft gespeichert werden.
5. Melden Sie sich als Schüler in der Domäne an und kontrollieren Sie, ob Sie das richtige Profil bekommen haben. Ändern Sie als Schüler Einstellungen an Ihrem Profil und überprüfen Sie, ob die Änderungen dauerhaft gespeichert werden.

## Notizen

## Hinweise

### Eigenschaften von Taskleiste und Startmenü

Startmenü: Start – Eigenschaften

### Ordneroptionen

Windows-Explorer: Extras – Ordneroptionen – Ansicht

### Kopieren von Profilen

Die Erstellung des Profils, das als Vorlage dient, so wie auch der Kopiervorgang sollten mit administrativen Rechten durchgeführt werden.

Arbeitsplatz: Eigenschaften – Erweitert – Benutzerprofile – Einstellungen – Kopieren nach

Benutzer ändern – "Jeder"

Die Berechtigungen für „Jeder“ können anschließend gegebenenfalls auf Leserechte reduziert werden.

### Default User in der Freigabe Netlogon

Existiert in der Netlogon-Freigabe ein „Default User“-Profil, so wird dieses als zukünftig als Vorlage verwendet. Das Profil muss den Namen „Default User“ haben. Nachträgliche Änderungen beim Namen oder bei Berechtigungen können dazu führen, dass das Profil nicht verwendet wird.

Im „Default User“-Profil sollte der Ordner "Eigene Dateien" gelöscht werden. Gegebenenfalls können noch weitere Ordner gelöscht werden (z. B. Anwendungsdaten, Cookies, Lokale Einstellungen).

### Verbindliche Profile

Es gibt verschiedene Möglichkeiten ein verbindliches servergespeichertes Profil zu erstellen:

Windows-Explorer: Umbenennen der Datei NTUSER.DAT in NTUSER.MAN (mandatory, verbindlich)

Gruppenrichtlinie: Computer – Administrative Vorlagen – System – Benutzerprofile: „Propagierung von Änderungen an servergespeicherten Profilen auf den Server verhindern“

Bei einem verbindlichen Profil genügt es, wenn der Benutzer Leserechte hat.

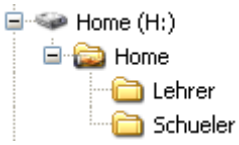
# Laborübung 12 - Das persönliche Homeverzeichnis

## Szenario

Jeder Schüler und jede Lehrkraft soll eine persönliche Datenablage im Netzwerk zur Verfügung haben und dieses im Windows-Explorer stets als verbundenes (gemapptes) Laufwerk vorfinden.

## Aufgaben

1. Erstellen Sie eine Freigabe *Home* auf der Homepartition und legen Sie die Unterordner *Lehrer* und *Schueler* an.




2. Weisen Sie jedem Schüler und jeder Lehrkraft im entsprechenden Benutzerprofil ein Homeverzeichnis (Basisverzeichnis) zu.
3. Vergeben Sie die NTFS-Rechte so, dass Schüler keinen Zugriff auf andere Homeverzeichnisse haben. Lehrer sollen Einblick in die Homeverzeichnisse aller Schüler haben.
4. Beschränken Sie den verfügbaren Speicherplatz eines Schülers in seinem Homeverzeichnis auf 10 MB und testen Sie die Wirkungsweise dieser Einstellung.
5. Sorgen Sie dafür, dass beim Speichern unter *Eigene Dateien* das Homeverzeichnis der Benutzer verwendet wird.
6. Überprüfen Sie, ob die „Eigenen Dateien“ als Offline-Dateien zur Verfügung gestellt werden. Verhindern Sie ggf. die Verwendung von Offlinedateien.

## Notizen

## Hinweise

### Basisverzeichnis im Benutzerprofil zuweisen

Im Profil des Benutzers wird der Pfad zum Homeverzeichnis einem Laufwerksbuchstaben zugeordnet. Das Homeverzeichnis wird dadurch automatisch angelegt und bei der nächsten Anmeldung des Benutzers mit dem Laufwerksbuchstaben verknüpft. Die Rechte des Benutzers werden vom System automatisch so gesetzt, dass dieser Vollzugriff hat.

Basisordner:

```
h:    \\server\Freigabe\Ordner\%username%
```

### Kontingentverwaltung (Quota)

Laufwerk: Eigenschaften – Kontingent

### Eigene Dateien umleiten

Die „Eigenen Dateien“ sind im Benutzerprofil gespeichert. Bei einem servergespeicherten Profil sollten die „Eigenen Dateien“ auf das Homeverzeichnis des Benutzers umgeleitet werden.

Gruppenrichtlinie: Benutzerkonfiguration – Windows-Einstellungen – Ordnerumleitung

Damit die Gruppenrichtlinie für die Ordnerumleitung erfolgreich wirken kann, muss für die Freigabeberechtigung Vollzugriff gewährt werden.

### Offlinedateien ausschalten

Gruppenrichtlinie: Benutzerkonfiguration – Administrative Vorlagen – Netzwerk – Offlinedateien:

- „Benutzerkonfiguration von Offlinedateien nicht zulassen“
- „Offline verfügbar machen entfernen“
- „Verwendung von Offlinedateiordnern verhindern“
- „Umgeleitete Ordner nicht automatisch offline verfügbar machen“

## Weiterführende Informationen

### Offlinedateien und Ordnerumleitung „Eigene Dateien“

Offlinedateien sind eine Technologie, bei der Serverlaufwerke lokal zwischengespeichert werden, damit Benutzer Zugriff auf ihre Daten haben, wenn das Netzwerk nicht verfügbar ist (mobile Benutzer). Arbeitet der Benutzer im Netzwerk, werden beim An- und Abmelden die Daten synchronisiert. Die Synchronisation kann unter Umständen sehr lange dauern. In Verbindung mit der Ordnerumleitung für „Eigene Dateien“ ist der Offline-Zugriff nicht erwünscht; durch die Ordnerumleitung soll die Synchronisation gerade verhindert werden.

# Laborübung 13 - Arbeiten mit Gruppen

## Szenario

In der Gruppe Schuelerzeitung sind diejenigen Schülerinnen, Schüler und Lehrkräfte zusammengefasst, die die Schülerzeitung gestalten. Diese erhalten ein gemeinsames Arbeitsverzeichnis und später gegebenenfalls noch weitere Rechte (z. B. Ausdrucken am Farbdrucker der Schule).

In der Gruppe Lokale_Admins sind die Betreuer der Arbeitsstationen zusammengefasst. Diese haben administrative Rechte an den Clients, jedoch nicht am Server. Einschränkende Gruppenrichtlinien sollen für diese Gruppe nicht gelten.

## Aufgaben

1. Erstellen Sie eine lokale Gruppe Austausch und geben Sie dieser Gruppe die notwendigen Rechte für das Austauschverzeichnis.
2. Ordnen Sie der lokalen Gruppe Austausch die globalen Personengruppen Lehrer und Schueler zu.
3. Zur Gruppe Schülerzeitung sollen alle Lehrer und einige Schüler gehören, die ein gemeinsames Verzeichnis nutzen. Erstellen Sie dafür eine geeignete Struktur.

## Weiterführende Aufgaben

4. Erstellen Sie die Gruppe Lokale_Admins (globale Gruppe) und fügen Sie der Gruppe einige Lehrer oder Schüler als Mitglieder hinzu.
5. Sorgen Sie durch eine Gruppenrichtlinie oder durch Einstellungen an jedem Client dafür, dass die Mitglieder der Gruppe Lokale_Admins administrative Rechte am Client haben.
6. Sorgen Sie dafür, dass einschränkende Gruppenrichtlinien (z. B. Ausblenden der Systemsteuerung) für die Gruppe Lokale_Admins nicht gelten.

## Notizen

## Hinweise

### Domänenfunktionsebene heraufstufen

Einige Gruppenfunktionalitäten sind erst verfügbar, nachdem die Domänenfunktionsebene auf „Windows 2000-pur“ oder „Windows Server 2003“ heraufgestuft wurde (z. B Verschachtelung von Gruppen, universelle Gruppen, Konvertieren von Gruppen)

Active Directory-Benutzer und -Computer – Domäne auswählen – Domänenfunktionsebene heraufstufen – „Windows 2000 pur“ oder „Windows Server 2003“

### Einzelne Benutzer zu lokalen Administratoren machen

Sinnvoll ist es, die Benutzer in einer globalen Gruppe (Lokale_Admins) zusammenzufassen.

| | |
|---|---|
| Möglichkeit 1: | An jedem Client wird die Gruppe Lokale_Admins zur Gruppe Administratoren hinzugefügt. |
| Möglichkeit 2: | Die Gruppe Lokale_Admins wird über eine Gruppenrichtlinie bei allen Clients zur Gruppe Administratoren hinzugefügt:<br>Computerkonfiguration – Windows Einstellungen – Sicherheitseinstellungen – Eingeschränkte Gruppen – Gruppen hinzufügen – Diese Gruppe ist Mitglied von Administratoren |

### Sicherheitsfilterung für eine Gruppenrichtlinie

Standardmäßig gilt eine Gruppenrichtlinie für alle Benutzer und Computer (authentifizierte Benutzer). Für jede Gruppenrichtlinie lässt sich jedoch festlegen, für welche Benutzer und Computer innerhalb der zugeordneten OU die Einstellungen gelten sollen (Gruppenrichtlinie auswählen: Bereich – Sicherheitsfilterung).

### Gruppenmitgliedschaft

Die Mitgliedschaft in einer Gruppe wird nur bei der Anmeldung überprüft. Werden Personen einer Gruppe hinzugefügt oder aus einer Gruppe entfernt, müssen diese sich neu anmelden, damit die Änderungen wirksam werden.

# Weiterführende Informationen

## Das Gruppenkonzept eines Windows-Servers

### Sicherheitsgruppe - Verteilergruppe

Sicherheitsgruppen sind dazu da, um Zugriffsrechte zu setzen. Bei der Anmeldung eines Benutzers wird überprüft, in welchen Sicherheitsgruppen dieser Benutzer Mitglied ist.

Verteilergruppen haben die Funktion einer Mailingliste (E-Mail-Verteiler) bei Exchange. Zugriffsrechte können darüber nicht gesetzt werden.

### Universelle Gruppen

Universelle Gruppen sind nur in größeren Strukturen mit mehreren Domänen von Bedeutung. Sie können Mitglieder aus anderen Domänen haben. Voraussetzung für den Einsatz ist die Hochstufung der Gesamtstrukturfunktionsebene auf „Windows 2000-pur“ oder „Windows Server 2003“ (AD Domänen- und Vertrauensstellungen - Gesamtstrukturfunktionsebene heraufstufen)

### Globale Gruppen

In globalen Gruppen sollen Personen zusammengefasst werden. (Personen sind global in einer Domäne definiert.)

### Lokale Gruppen

In lokalen Gruppen werden Berechtigungen für bestimmte Aufgaben oder Ressourcen (z. B. NTFS-Rechte, Druckerberechtigungen) definiert. (Ressourcen sind lokal an ein Gerät gebunden.)

### Verschachtelung der Gruppen

Die globalen Gruppen sind nach Personengruppen oder Abteilungen benannt (Lehrer, Schueler, Buchhalter, Abteilungsleiter, …).

Die lokalen Gruppen sind nach Aufgaben benannt (Pflege der Webseiten, Einsicht in die Kundendaten, Pflege der Schülerdatei, Nutzung des Farbdruckers, Nutzung des Internets, …).

Indem eine globale Gruppe Mitglied einer lokalen Gruppe wird, erhalten die Personen in der globalen Gruppe die entsprechenden Rechte auf Ressourcen.

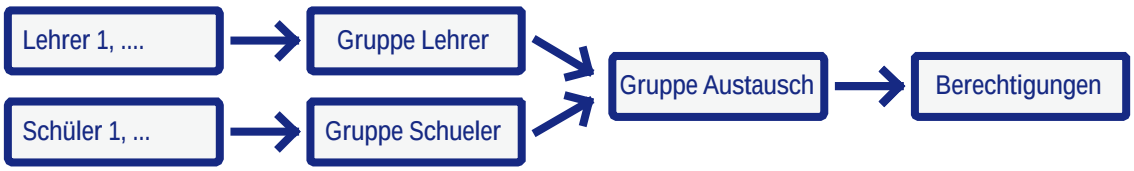
**Einfaches Gruppenkonzept**


**Erweitertes Gruppenkonzept**


Bei komplexen Berechtigungsstrukturen bringt das erweiterte Gruppenkonzept Vorteile

**Beispiel**

In einem Austauschordner sollen komplexe Berechtigungen gelten (z. B. jeder Benutzer darf nur von ihm selbst erstellte Inhalte bearbeiten oder löschen). Es wird eine lokale Gruppe Austausch erstellt, der die Berechtigungen für den Austauschordner zugewiesen werden. Jede globale Gruppe (Personengruppe), die Mitglied in der lokalen Gruppe Austausch ist, erhält automatisch die notwendigen Berechtigungen. Auch wenn neue Personengruppen aufgenommen werden müssen, muss man sich keine weiteren Gedanken über die Dateirechte machen.




In kleinen überschaubaren Strukturen erscheint die Unterteilung (lokale Gruppen, globale Gruppen, universelle Gruppen) übertrieben. Hier genügt ein einfaches Gruppenkonzept, z. B. nur globale Gruppen zu definieren und diesen direkt die Rechte auf Ressourcen zuzuweisen.

# Laborübung 14 - Anmeldeskripte

## Szenario

Jedem Schüler und jeder Lehrkraft soll über ein Anmeldeskript eine komfortable Umgebung bereitgestellt werden. Alle Netzlaufwerke sollen über Laufwerksbuchstaben angesprochen und Drucker sollen den Benutzern automatisch zugewiesen werden.

## Aufgaben

1. Erstellen Sie ein Anmeldeskript, so dass die Benutzer alle für sie interessanten Freigaben am Server über Laufwerksbuchstaben ansprechen können.
2. Die Mitglieder der Gruppe Schuelerzeitung sollen ein eigenes Projektverzeichnis bekommen, das über den Laufwerksbuchstaben S: angesprochen wird.
3. Variieren Sie die Zuweisung des Anmeldeskripts
   - über das Benutzerprofil
   - über eine Gruppenrichtlinie

## Notizen

## Hinweise

### Verbinden einer Freigabe mit einem Laufwerk

`net use` *`Laufwerk`*`: \\`*`server`*`\`*`freigabe`*

```
net use x: \\192.168.130.10\Daten
```

```
net use x: \\Server\Daten
```

### Zuweisung eines Login-Skriptes im Benutzerprofil

Damit das erstellte Login-Skript vom System verwendet wird, muss es in der Netlogon-Freigabe gespeichert sein. Im Profil des Benutzers wird lediglich der Dateiname des Skriptes eingetragen, da das System automatisch auf die Netlogon-Freigabe zugreift. Es können folgende Dateitypen verwendet werden: .bat, .cmd, .vbs, .com oder .exe.

### Zuweisung eines Login-Skriptes über Gruppenrichtlinien

Gruppenrichtlinie: Benutzerkonfiguration – Windows-Einstellungen – Skripts – Anmelden – Dateien anzeigen – Hinzufügen

Windows schlägt als Speicherort für Anmeldeskripte, die über Gruppenrichtlinien zugewiesen werden, das Gruppenrichtlinienverzeichnis vor. Damit wird das Skript zusammen mit der Gruppenrichtlinie gespeichert. Nachteilig daran ist, dass die Skripte nicht alle zentral an einer Stelle liegen. Alternativ kann deshalb auch der Netlogon-Pfad des Anmeldeservers angegeben werden: %Logonserver%\netlogon\<Skript>

### Anmeldeskript sichtbar ausführen

In der Testphase ist es sinnvoll, das Anmeldeskript sichtbar ausführen zu lassen.

Gruppenrichtlinie: Benutzerkonfiguration – Administrative Vorlagen – System – Skripts:

- Anmeldeskript gleichzeitig ausführen
- Anmeldeskript sichtbar ausführen

## Weiterführende Informationen

### Reihenfolge beim Abarbeiten von Login-Skripten

1. Login-Skripte über Gruppenrichtlinien
2. Laufwerksverbindungen auf lokaler Ebene
3. Login-Skript, dessen Pfad im Active-Directory-Profil des Benutzers hinterlegt ist.

### Anmeldeskripte

Anmeldeskripte oder Loginskripte sind neben den Gruppenrichtlinien ein zentrales Steuerungselement, um Benutzern eine spezifische Umgebung bereitzustellen.

Skripte können in folgenden Situationen ausgeführt werden:

- Beim Starten oder Herunterfahren eines Computers
- Beim Anmelden oder Abmelden eines Benutzers

## Beispiele für Anmeldeskripte

### Zuweisung eines Laufwerksbuchstabens

```
@echo off
REM Zuweisen einer Laufwerksverbindung;
REM Vor der Verbindung wird das Laufwerk sicherheitshalber getrennt.

net use x: /delete 2>nul
net use x: %logonserver%\Daten /persistent:no
```

### Zuweisung eines Laufwerks in Abhängigkeit der Gruppenmitgliedschaft

#### ifmember

Das Programm *ifmember.exe* aus dem Windows-Ressource Kit (rktools) gibt als Errorlevel die Anzahl der Gruppen aus, in denen der jeweilige Benutzer Mitglied ist. Wird die Datei *ifmember.exe* in die Netlogon-Freigabe kopiert, ist sie von jedem Rechner aus aufrufbar.

`ifmember Gruppe1 Gruppe2 Gruppe3 ….`

| | |
|---|---|
| `ifmember Gruppe` | gibt errorlevel 1 zurück, wenn der Benutzer Mitglied der Gruppe ist, sonst errorlevel 0 |

**Variante A:**

```
@echo off
REM Zuweisen einer Laufwerksverbindung
REM in Abhängigkeit der Gruppenmitgliedschaft

%logonserver%\netlogon\ifmember.exe G_Schuelerzeitung
if errorlevel 1 (
   net use s: /delete
   net use s: %logonserver%\Schuelerzeitung /persistent:no
)
```

**Variante B:**

```
@echo off
REM Zuweisen einer Laufwerksverbindung
REM in Abhängigkeit der Gruppenmitgliedschaft

%logonserver%\netlogon\ifmember.exe G_Schuelerzeitung
if not errorlevel 1 goto label_1
   net use s: /delete
   net use s: %logonserver%\Schuelerzeitung /persistent:no
:label_1
```

# Laborübung 15 - Drucken im Netzwerk

## Szenario

Jeder EDV-Raum ist mit einem Drucker ausgestattet. Die Computer sollen so konfiguriert werden, dass die Benutzer automatisch den Drucker im jeweiligen Raum als Standarddrucker zur Verfügung haben.

Für die Nutzung eines Druckers am Client gibt es grundsätzlich verschiedene Ansätze:

- Installation des Netzwerkdruckers als lokaler Drucker am Muster-Client. Der Muster-Client wird geklont.
- Ein am Server installierter Netzwerkdrucker wird freigegeben. Am Muster-Client wird der Drucker als Netzwerkdrucker eingebunden. Der Muster-Client wird geklont.
- Ein am Server installierter Netzwerkdrucker wird freigegeben. Über ein Anmeldeskript wird der Drucker dem jeweiligen Benutzer zugewiesen.

## Aufgabe

1. Testen Sie die verschiedenen Ansätze zum Einrichten eines Druckers und diskutieren Sie jeweils die Vor- und Nachteile.

## Notizen

## Hinweise

### Installation eines Netzwerkdruckers am Client (Lokaler Drucker)

Start - Einstellungen – Drucker und Faxgeräte – Drucker hinzufügen:
lokalen Drucker installieren (TCP/IP-Port)

### Installation und Freigabe eines Netzwerkdruckers am Server

Start - Einstellungen – Drucker und Faxgeräte – Drucker hinzufügen:
lokalen Drucker installieren (TCP/IP-Port) – Freigabe

### Zugriff eines Clients auf eine Druckerfreigabe

Windows-Explorer: Auswahl der Druckerfreigabe – Verbinden

### Zugriff auf eine Druckerfreigabe über ein Anmeldeskript

```
rundll32 printui.dll,PrintUIEntry /in /n \\Server\Freigabename
```

### Hilfe zur Syntax und Informationen zum Befehl printui.dll

```
rundll32 printui.dll,PrintUIEntry /?
```

## Notizen

## Weiterführende Informationen

### Zuweisen eines freigegebenen Druckers in Abhängigkeit des Computernamens

Wurden die Computernamen entsprechend den Räumen benannt z. B. HS16P01, HS16P02, ..., so können diese Angaben genutzt werden, um Drucker raumbezogen zuzuweisen.

```
REM Zuweisen eines freigegebenen Druckers
REM in Abhängigkeit der ersten 4 Zeichen des Computernamens.
REM Der neu zugewiesene Drucker wird als Standard definiert.

if /i %computername:~0,4%==HS16 (
   rundll32 printui.dll,PrintUIEntry /in /n \\server\HP
   rundll32 printui.dll,PrintUIEntry /y  /n \\server\HP
)
```

### Zuweisen eines freigegebenen Druckers in Abhängigkeit der OU

Liegen die Computer im Active-Directory in OUs, die nach den Computerräumen benannt sind, lassen sich damit die Drucker raumbezogen zuweisen. Zur Abfrage dient das Programm dsquery.exe, das dazu in die Netlogon-Freigabe kopiert wird.

```
REM Zuweisen eines freigegebenen Druckers in Abhängigkeit des Raumes
REM Der neu zugewiesene Drucker wird als Standarddrucker definiert.

\\server\netlogon\dsquery computer -name %computername% | find "EDV_1" > nul
if not errorlevel 1 (
   echo "Computer ist in Raum EDV_1"
   rundll32 printui.dll,PrintUIEntry /in /n \\server\HP
   rundll32 printui.dll,PrintUIEntry /y  /n \\server\HP
)

\\server\netlogon\dsquery computer -name %computername% | find "EDV_2" > nul
if not errorlevel 1 (
   echo "Computer ist in Raum EDV_2"
   rundll32 printui.dll,PrintUIEntry /in /n \\server\HP
   rundll32 printui.dll,PrintUIEntry /y  /n \\server\HP
)
```

### Errorlevel

Jedes Kommando gibt einen Errorlevel zurück, der in Skripten oder Batch-Programmen mit *%errorlevel%* oder mit *if errorlevel zahl* abgefragt werden kann.

| | |
|---|---|
| `if errorlevel 0` | gibt immer true zurück, wenn der errorlevel >= 0 ist. |
| `if errorlevel 1` | gibt immer true zurück, wenn der errorlevel >= 1 ist. |
| `if errorlevel 2` | gibt immer true zurück, wenn der errorlevel >= 2 ist. |

### Zuweisen eines freigegebenen Druckers mit einer Computerrichtlinie

### Der Loopback-Verarbeitungsmodus bei Gruppenrichtlinien

- Bei der Anmeldung an einem Terminalservers sollen für einen Benutzer restriktivere Einstellungen gelten, wie bei der Anmeldung an einem normalen Client.
- Die Druckerzuweisung ist prinzipiell nur für den Benutzer möglich, sie soll jedoch eigentlich nach Computern erfolgen.

In beiden Fällen sollen benutzerbezogene Einstellungen in Abhängigkeit von einem Computer vergeben werden, an dem der Benutzer angemeldet ist.

Im Loopback-Verarbeitungsmodus kann eine Benutzerrichtlinie an ein Computerobjekt gebunden werden. Die Richtlinie wirkt nur dann, wenn der Benutzer am jeweiligen Computer angemeldet ist. Der Loopback-Verarbeitungsmodus erzeugt dabei eine Schleife, die den Client bei der Benutzeranmeldung dazu veranlasst, auch die Computerobjekte auszuwerten.

| | |
|---|---|
| Gruppenrichtlinie: | Computerkonfiguration – Administrative Vorlagen – System – Gruppenrichtlinien: „Loopbackverarbeitungsmodus für Benutzergruppenrichtlinie“ |

Der Loopback-Verarbeitungsmodus kennt zwei Einstellungen:

| | |
|---|---|
| Zusammenführen: | Die Benutzerrichtlinien des Computerobjekts werden mit den Richtlinien des Benutzerobjekts zusammengeführt. Die Benutzerrichtlinien des Computerobjekts haben im Zweifelsfall Vorrang. |
| Ersetzen: | Die Benutzereinstellungen des Benutzerobjekts werden ignoriert. |

# Ergänzende Übungen

# Erweiterung der AD-Struktur mit Skripten

Um mehrere Benutzer gleichzeitig anzulegen und die administrative Verwaltung zu vereinfachen, werden Skripte eingesetzt.

### Anlegen einer Organisationseinheit

```
dsadd ou "Vollständiger Name der OU"
dsadd ou "ou=Verwaltung,dc=alp,dc=local"
```

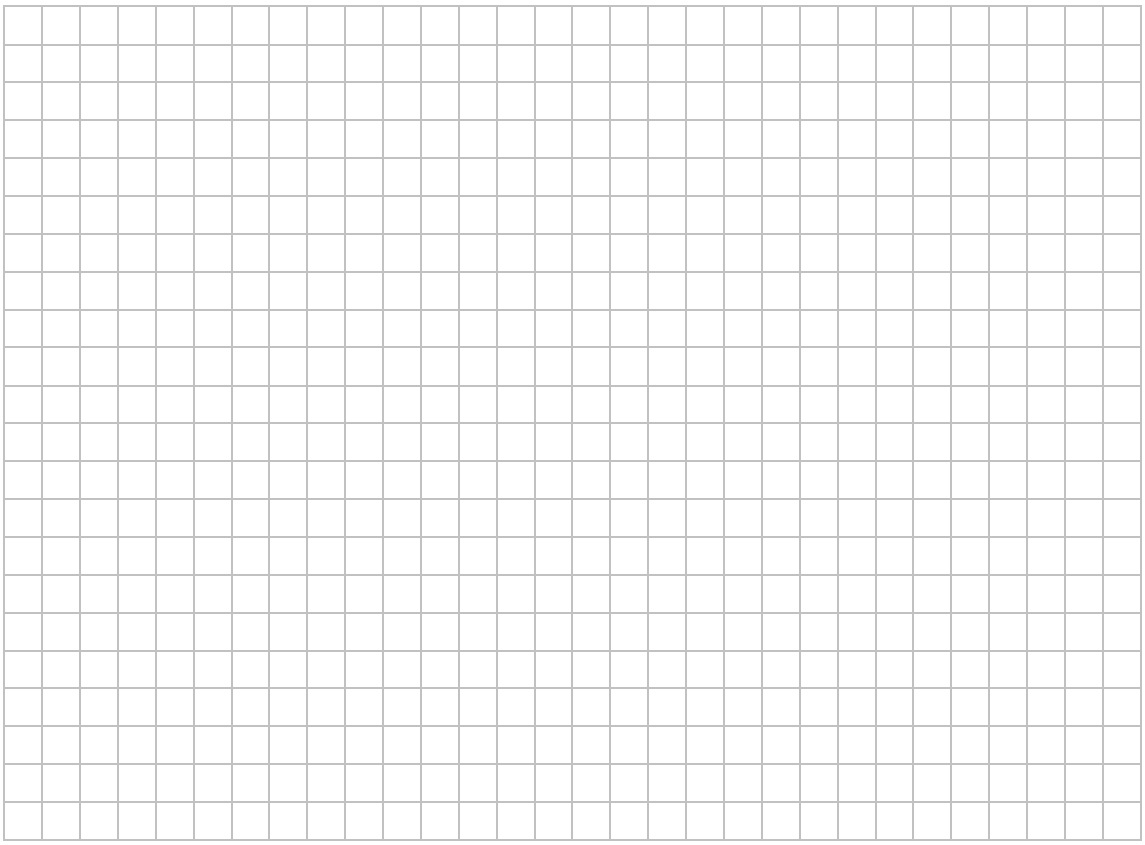
### Anlegen eines Benutzers

```
dsadd user "Vollständiger Name" -samid Anzeigename -pwd Passwort
dsadd user "CN=Chef,ou=Verwaltung,dc=alp,dc=local" -samid Chef -pwd 12345
```

### Anlegen einer Gruppe

```
dsadd group "Vollständiger Name der Gruppe"
dsadd group "CN=Direktorat,ou=Verwaltung,dc=alp,dc=local"
```

## Notizen



## Beispiel für ein Installationsskript

Im nachfolgenden Skript wird die AD-Struktur mit allen OUs, Gruppen und Benutzern angelegt. Danach wird die Dateistruktur angelegt, ein Verzeichnis wird freigeben und die Ordner werden mit Berechtigungen versehen.

```
@echo off

set dc1=alp130
set dc2=local

dsadd ou "ou=Verwaltung,dc=%dc1%,dc=%dc2%"
dsadd ou "ou=Direktorat,ou=Verwaltung,dc=%dc1%,dc=%dc2%"
dsadd ou "ou=Sekretariat,ou=Verwaltung,dc=%dc1%,dc=%dc2%"
dsadd ou "ou=Gruppen,ou=Verwaltung,dc=%dc1%,dc=%dc2%"

dsadd user "CN=Chef,ou=Direktorat,ou=Verwaltung,dc=%dc1%,dc=%dc2%"
        -samid Chef -pwd 12345 -mustchpwd yes -disabled no

dsadd user "CN=Sekretaerin1,ou=Sekretariat,ou=Verwaltung,dc=%dc1%,dc=%dc2%"
        -samid Sekretaerin1 -pwd 12345
dsadd user "CN=Sekretaerin2,ou=Sekretariat,ou=Verwaltung,dc=%dc1%,dc=%dc2%"
        -samid Sekretaerin2 -pwd 12345

dsadd group "CN=Direktorat,ou=Gruppen,ou=Verwaltung,dc=%dc1%,dc=%dc2%"
dsadd group "CN=Sekretariat,ou=Gruppen,ou=Verwaltung,dc=%dc1%,dc=%dc2%"
dsadd group "CN=Jahresbericht,ou=Gruppen,ou=Verwaltung,dc=%dc1%,dc=%dc2%"

dsmod group "CN=Sekretariat,ou=Gruppen,ou=Verwaltung,dc=%dc1%,dc=%dc2%"
    -addmbr "CN=Sekretaerin1,ou=Sekretariat,ou=Verwaltung,dc=%dc1%,dc=%dc2%"
dsmod group "CN=Sekretariat,ou=Gruppen,ou=Verwaltung,dc=%dc1%,dc=%dc2%"
    -addmbr "CN=Sekretaerin2,ou=Sekretariat,ou=Verwaltung,dc=%dc1%,dc=%dc2%"

md d:\Verwaltung
md d:\Verwaltung\Direktorat
md d:\Verwaltung\Sekretariat

net share Verwaltung /DELETE
net share Verwaltung=d:\Verwaltung /GRANT:jeder,full

cacls d:\Verwaltung /g Administratoren:F Sekretariat:W Direktorat:R <
d:\ja.txt
cacls d:\Verwaltung\Direktorat /g Administratoren:F Direktorat:W <
d:\ja.txt
cacls d:\Verwaltung\Sekretariat /g Administratoren:F Direktorat:R Sekreta-
riat:W
      < d:\ja.txt
```

Die Datei ja.txt enthält nur das Zeichen j und bestätigt damit die ja/nein-Abfrage.

# Softwareverteilung über Gruppenrichtlinien

Steht für eine Software ein MSI-Paket (Microsoft Software Installation) zur Verfügung, so kann die Software innerhalb der Domäne verteilt werden. Das MSI-Paket muss über eine Freigabe zur Verfügung gestellt werden.

## Zuweisung eines MSI-Paketes über Gruppenrichtlinien

Gruppenrichtlinie: Computer- oder Benutzerkonfiguration – Softwareeinstellungen – Softwareinstallation

MSI-Paket über den Netzwerkpfad auswählen (kein lokaler Pfad).

### Erweiterte Einstellungen:

„Anwendung deinstallieren, wenn sie außerhalb des Verwaltungsbereichs liegt."

Wird der Anwender oder der Computer aus der Zuständigkeit der Gruppenrichtlinie entfernt, so wird die Software deinstalliert.

### Beim Neustart auf das Netzwerk warten

Die Softwareverteilung gelingt nur, wenn vor dem Start des Installationsvorganges das Netzwerk zur Verfügung steht.

Gruppenrichtlinie: Computerkonfiguration – Administrative Vorlagen – System – Anmeldung: „Beim Neustart des Computers und bei der Anmeldung immer auf das Netzwerk warten".

### Änderungen

mst-files (Transform-Dateien) unterstützen die Anpassung der Softwarepakete, z. B. dass die Lizenzvereinbarung nicht bei jeder Neuinstallation des Programms aufs Neue akzeptiert werden muss.

### Aktualisierungen

msp-files (Microsoft Patches) sind Service-Packs für MSI-Pakete.

### Mit erhöhten Rechten installieren

Bei der Zuweisung eines MSI-Paketes für eine bestimmte Benutzerkonfiguration kann es erforderlich sein, dem MSI-Paket zur Installation erhöhte Rechte zuzuweisen, da die normalen Benutzerrechte nicht ausreichen.

Gruppenrichtlinie: Benutzerkonfiguration – Administrative Vorlagen – Windows-Komponenten – Windows Installer: „Immer mit erhöhten Rechten installieren"

## MSI-Pakete erstellen

Das Erstellen von MSI-Paketen kann sehr aufwändig werden.

### Lizenzpflichtige Werkzeuge

WinInstall (http://www.scalable.com)

Wise Installation Studio (http://www.wise.com)

### Lizenzfreie Werkzeuge

WinInstall LE (http://www.scalable.com/WinINSTALL_LE.aspx)

http://www.appdeploy.com/

### Grundsätzliches Vorgehen beim Erstellen eines MSI-Paketes

- WinInstall LE auf einer „sauberen“ Arbeitsstation installieren
- WinInstall LE ausführen und „Vorher Schnappschuss erstellen“
- Installation der gewünschten Software
- WinInstall LE ausführen und „Nachher Schnappschuss erstellen“

Einige Softwareprodukte (z. B. Acrobat Reader, Java Runtime Environment) bringen fertige MSI-Pakete mit, verbergen diese jedoch hinter einem Installer. Wenn der Installer die MSI-Dateien in einem temporären Verzeichnis entpackt hat, kann man die MSI-Dateien kopieren, bevor sie vom Installer wieder gelöscht werden.

Für den Acrobat Reader gibt es fertige MSI-Pakete unter
ftp://ftp.adobe.com/pub/adobe/reader/win/8.x/8.1

### Bearbeiten von MSI-Paketen

Microsoft bietet mit dem Programm orca.exe ein allgemeines Werkzeug zum Bearbeiten von MSI-Paketen. Es ist im Windows SDK (Software Development Kit) für Server 2003 enthalten.

http://www.microsoft.com/msdownload/platformsdk/sdkupdate/psdk-full.htm

Daneben sind für einige Softwareprodukte (z. B. Acrobat Reader) spezielle und leichter bedienbare Werkzeuge zur Bearbeitung von MSI-Paketen erhältlich.

# Microsoft-Management-Konsole am Client

## Szenario

Die Administration mehrerer Server soll von einem Client aus über die Microsoft-Management-Konsole ermöglicht werden.

## Aufgabe

1. Richten Sie an einem Client die Microsoft-Management-Konsole mit allen notwendigen Snap-Ins ein, so dass Sie den Server administrieren können.

## Hinweise

### Einrichtung der Microsoft-Management-Konsole

| | |
|---|---|
| `mmc` | Start der Microsoft-Management-Konsole |
| Snap-In hinzufügen | Verwaltungswerkzeuge hinzufügen |

### Management-Konsole am Client

Beim Einrichten der Management-Konsole am Server stehen die notwendigen Snap-Ins zur Auswahl. Beim Einrichten der Management-Konsole an einem Client müssen ggf. einige Snap-Ins nachinstalliert werden.

### Adminpak am Client installieren

In der Management-Konsole am Client sind nicht alle Verwaltungswerkzeuge (Snap-Ins) für den Server vorinstalliert. Durch die Installation eines Administrationspaketes (adminpak.msi) stehen auch die Snap-Ins zur Verwaltung des Domänencontrollers zur Verfügung (z. B. Active Directory Benutzer und Computer). Das zur jeweiligen Serverversion gehörige Adminpak enthält die passenden Verwaltungswerkzeuge. Eine vorbereitetes Installationspaket liegt auf dem Server unter:

C:\Windows\System32\adminpak.msi

### Gruppenrichtlinienverwaltungskonsole am Client installieren

Die Gruppenrichtlinienverwaltungskonsole (gpmc.msi) ist innerhalb der Microsoft-Management-Konsole erst verfügbar, nachdem sie lokal installiert wurde. Gegebenenfalls ist am Client vorher Framework 1.1 (.NET framework 1.1) zu installieren.

# Administrative und versteckte Freigaben

### Zugriff auf administrative Freigaben

Alle Festplattenlaufwerke sind standardmäßig mit einer administrativen Freigabe versehen (C$, D$, …). Das Windows-Verzeichnis ist standardmäßig mit der administrativen Freigaben ADMIN$ verbunden. Der Zugriff auf die administrativen Freigaben kann nur durch einen Eingriff in die Registry dauerhaft unterbunden werden.

| | |
|---|---|
| `\\Server\C$` | Zugriff auf ein Laufwerk |
| `\\Server\ADMIN$` | Zugriff auf das Windows-Verzeichnis |

### Anlegen versteckter Freigaben

Versteckte Freigaben sind Freigaben, die in der Netzwerkumgebung nicht angezeigt werden. Der Benutzer muss den Freigabenamen kennen, um darauf zuzugreifen. Versteckte Freigaben unterscheiden sich beim Anlegen von normalen Freigaben nur dadurch, dass am Ende des Freigabenamens das $-Zeichen angehängt wird.

# Remotezugriffe auf die Clients

Herunterfahren der Clients vom Administrationsrechner aus

## Aufgaben

1. Erstellen Sie ein Skript, das alle Computer eines Computerraumes herunterfährt.
2. Überprüfen Sie, welche Rechte ein Lehrer benötigt, damit er das Skript ausführen kann.

| | |
|---|---|
| `shutdown –s –m \\Computer` | Herunterfahren eines entfernten Computers |
| `shutdown –a` | Abbrechen des Shutdown-Befehls |
| `shutdown –i` | Grafische Bedienoberfläche zum Shutdown-Befehl |

# Zeitsynchronisation

In einer Windows-Domäne wird die korrekte Uhrzeit automatisch vom Domänencontroller auf die Clients übertragen. Wird trotz richtiger Zeitzone eine falsche Uhrzeit angezeigt, dann ist am Domänencontroller eventuell ein falscher oder nicht funktionierender Zeitserver eingetragen.

## Aufgaben

1. Überprüfen Sie am Server die korrekte Zeitzone und die Uhrzeit.
2. Stellen Sie fest, welcher Internet-Zeitserver zur Zeitsynchronisation verwendet wird.
3. Stellen Sie am Domänencontroller den Zeitserver ptbtime1.ptb.de als Standard-Zeitserver ein und synchronisieren Sie die Uhrzeit mit diesem Server.

## Notizen

## Hinweise

| | |
|---|---|
| `w32tm /tz` | Anzeige der aktuellen Zeitzone |
| `net time /querysntp` | Zeigt den aktuell eingestellten Zeitserver an. |
| `w32tm /config /manualpeerlist:ptbtime1.ptb.de /syncfromflags:manual` | Festlegen des zu verwendenden Zeitservers |
| `w32tm /config /update` | Benachrichtigt den Zeitdienst, dass sich die Konfiguration geändert hat. |
| `w32tm /resync` | Synchronisiert die Uhrzeit mit dem Zeitserver |

## Weiterführende Informationen

Die Clients synchronisieren ihre Uhrzeit bei der Anmeldung an den Domänencontroller automatisch. Weichen die Uhrzeiten zu sehr voneinander ab, ist eventuell eine Anmeldung am Domänencontroller nicht möglich.

In größeren Strukturen, mit mehreren Domänencontrollern oder Domänen ist die Hierarchie wie die Uhrzeit synchronisiert wird, festgelegt. Üblicherweise synchronisiert sich der erste Domänencontroller mit einer externen Zeitquelle und wirkt als Zeitgeber für die anderen Domänencontroller und Clients.

Festlegen des Zeitservers entsprechend der Domänenhierarchie:

```
w32tm /config /syncfromflags:domhier
```

Anfragen an eine Zeitquelle können im symmetrischen Modus oder im Client-Modus gesendet werden. Im symmetrischen Modus agiert der anfragende Computer als gleichberechtigter Partner und handelt mit dem angefragten Zeitserver eine gemeinsame Zeit aus. Von externen Zeitservern wird dies im Allgemeinen nicht akzeptiert. Im Client-Modus übernimmt der anfragende Computer die vom Zeitserver erhaltene Zeit.

Anfragen im symmetrischen Modus:

```
w32tm /config /manualpeerlist:<server>,0x1 /syncfromflags:manual
```

Anfragen in Client-Modus:

```
w32tm /config /manualpeerlist:<server>,0x8 /syncfromflags:manual
```

| | |
|---|---|
| `net stop w32time` | Beendet den Zeitserverdienst |
| `net start w32time` | Startet den Zeitserverdienst |
| `w32tm /monitor` | Anzeige des Zeitservers in der Domäne und der externen Zeitquelle |
| NTP | Network Time Protocol |
| SNTP | Simple Network Time Protocol |

Anfragen an den Zeitserver werden über den UDP-Port 123 gesendet. Dieser darf nicht durch eine Firewall blockiert sein.

# Datensicherung

## Szenario

An einem Server sind alle sicherungsrelevanten Benutzerdaten im Ordner *Daten* abgelegt. Dieser Ordner soll regelmäßig und automatisiert gesichert werden.

## Aufgaben

1. Schreiben Sie ein Skript, das den Ordner *Daten* im Ordner *Backup_Daten* sichert. Achten Sie darauf, dass die NTFS-Berechtigungen mit gesichert werden.
2. Geben Sie den Ordner *Backup_Daten* lesend frei, so dass alle Benutzer (mit entsprechenden Berechtigungen) auf die gesicherten Daten zugreifen können.
3. Automatisieren Sie die Datensicherung mit dem Windows-Taskplaner, so dass der Datenordner automatisch einmal am Tag (in der Testphase alle 2 Minuten) gesichert wird.
4. Definieren Sie einen Ihrer Arbeitsplatzrechner als Backupserver und schreiben Sie ein Skript, das den Ordner *Daten* des Servers über das Netzwerk auf dem Backupserver sichert. Automatisieren Sie diese Datensicherung.
5. Entwerfen Sie ein Sicherungskonzept für Ihre Schule.
   - Was wird gesichert?
   - Wie häufig wird gesichert? (Tagesbackup, Wochenbackup, Archivierung, …)
   - Wohin wird gesichert? (zweite Festplatte, Backupserver, USB-Platte, …)

## Hinweise

### Datensicherung mit robocopy

Die Kommandozeilen-Tool *robocopy.exe* ist im Ressource-Kit (rktools) von Microsoft enthalten und kann vom Microsoft-Server herunter geladen werden. Suchbegriffe in einer Suchmaschine: tktools, robocopy, download. Eine ausführliche Dokumentation findet man in der Datei robocopy.doc.

`robocopy <Quelle> <Ziel> <Optionen>` Syntax von robocopy

`robocopy <Quelle> <Ziel> /MIR` Das Ziel wird mit der Quelle synchronisiert.

`robocopy <Quelle> <Ziel> /MIR /COPYALL`
NTFS-Berechtigungen werden mitkopiert.

Die /Mir-Option (Mirror) ist mit Vorsicht zu behandeln, da in der Quelle nicht mehr vorhandene Dateien im Zielverzeichnis automatisch gelöscht werden.

Für das Quell- und Zielverzeichnis können auch Netzwerkpfade angegeben werden:

```
robocopy D:\Daten \\server\freigabe\Backup_Daten /MIR
```

Der Befehl kopiert den Inhalt von D:\Daten auf den Server in den Ordner *Backup_Daten*. Dort werden veraltete Daten ersetzt, fehlende ergänzt und überzählige Dateien und Ordner gelöscht.

### Beispielskript für eine Datensicherung auf einen Backupserver

In einer Logdatei wird protokolliert, ob die Datensicherung erfolgreich war. Damit ist das Skript auch für eine automatische Datensicherung (nachts) geeignet.

```
@ECHO OFF

set Logfile=D:\logfile.log
set Quelle=D:\Daten\
set Ziel=\\BackupServer\Freigabe\Backup_Daten\

echo.                                                  >> %Logfile%
echo.                                                  >> %Logfile%
echo ------------------------------------------------  >> %Logfile%
echo Datensicherung: %computername%, %date% %time%  >> %Logfile%
echo.                                                  >> %Logfile%

robocopy %Quelle% %Ziel% /R:3 /W:3 /MIR /TEE /LOG+:%Logfile% /NDL

pause
exit
```

### Beispiel für eine Datensicherung auf einen USB-Stick

Bei der Sicherung auf einen USB-Stick ist es wichtig vor der Sicherung zu überprüfen, ob die Laufwerke existieren. Auf eine Logdatei wird verzichtet, da Fehler sofort erkannt werden.

```
@ECHO OFF

set Quelle=D:\Daten\
set Ziel=G:\Backup_Daten\

IF NOT EXIST %Quelle% color CF & echo %Quelle% existiert nicht & goto Fehler
IF NOT EXIST %Ziel%   color CF & echo %Ziel% existiert nicht & goto Fehler

robocopy %Quelle% %Ziel% /R:3 /W:3 /MIR /NDL

pause
exit

:Fehler
pause
exit
```

### Automatisieren eines Skriptes mit dem Taskplaner von Windows

Den Taskplaner von Windows findet man unter Programme – Zubehör – Systemprogramme – Geplante Tasks. Vor dem Automatisieren muss das Skript so weit getestet werden, dass es ohne Benutzereingriffe läuft.

## Weiterführende Informationen

Zur Datensicherung stellen externe Festplatten, NAS-Systeme (Network-Attached-Storage), eine redundante Verteilung der Daten auf mehrere Server oder Backup-Server sinnvolle Möglichkeiten dar. Die regelmäßige Datensicherung sollte automatisiert und ohne Benutzereingriffe erfolgen. Nur so ist gewährleistet, dass sie auch durchgeführt wird. Bandlaufwerke sollten zur Datensicherung auch aus diesen Gründen nicht mehr beschafft werden. Bei der Datenarchivierung muss vor allem auf die Langlebigkeit der verwendeten Technik und der Medien geachtet werden. Dafür eignen sich vor allem CD-Brenner oder DVD-RAM-Brenner.

## Gründe für eine Datensicherung

**Dateien werden versehentlich gelöscht oder überschrieben.**

Gründe sind üblicherweise, dass man ein Dokument unter einem anderen Namen abspeichert oder ein Dokument bearbeitet und Teile davon löscht oder zerstört. Auch manche Programme können durch unvorhergesehene Umstände die von ihnen bearbeiteten Dateien in einem unbrauchbaren Zustand zurücklassen.

**Das gesamte Datenverzeichnis ist nicht mehr zugänglich.**

Gründe können defekte Festplatten, ein kaputter PC, ein abhanden gekommenes Notebook oder auch das versehentliche Neuformatieren der Datenpartition im Rahmen eines Updates sein.

**Es muss auf einen früheren Datenbestand zurückgegriffen werden.**

Für manche Daten gibt es eine Aufbewahrungspflicht, um gegebenenfalls für einen bestimmten zurückliegenden Zeitpunkt recherchieren zu können. Daneben kommt es vor, dass ein Dokument vermisst wird, das früher einmal existiert hat.

## Lösungsansätze zur Datensicherung

Gegen das versehentliche Löschen oder Überschreiben der Daten hilft es, wenn man regelmäßig eine Sicherungskopie aller Daten in einem anderen Verzeichnis (z. B. Backup_Daten) anlegt. Liegen die Daten auf einem Server, ist es sinnvoll, wenn die Datensicherung in der Nacht automatisch durchgeführt wird. Den Benutzern wird für dieses Verzeichnis „Backup_Daten“ der lesende Zugriff freigegeben. Damit ist möglich, dass diese auf den Stand ihrer Daten vom Vortag zurückgreifen können. An einem Einzelplatz-PC sollte ein Sicherungsskript zumindest soweit vorbereitet sein, dass es auf „Knopfdruck“ ohne weitere Benutzereingriffe abläuft.

Sind die gesamten Daten eines PC oder eines Servers nicht mehr zugänglich, so muss auf eine externe Datensicherung zurückgegriffen werden. In einer Serverumgebung sollte auch dieser Vorgang automatisiert (in der Nacht) ablaufen. In größeren Umgebungen bietet sich dazu z. B. ein eigener Backupserver an, der nur die Aufgabe hat, eine Datensicherung aller Server vorrätig zu halten. In kleineren Verwaltungsumgebungen eignet sich dafür auch ein Arbeitsplatz-PC mit einer großen Festplatte, der nachts oder in der Mittagspause als Backupserver eingesetzt wird.

Eine weitere einfache Möglichkeit der Datensicherung bieten externe USB-Festplatten oder bei kleineren Datenmengen auch USB-Sticks. Per USB angeschlossene Geräte eignen sich nur bedingt für eine vollkommen automatisierte Datensicherung. Manche externe Festplatten wachen nicht mehr von alleine auf, wenn sie sich im Ruhezustand befinden. Ein Skript zur Datensicherung, das automatisch abläuft, muss dies berücksichtigen und zumindest dafür sorgen, dass keine Fehler passieren, wenn eine externe USB-Festplatte nicht bereit ist. Im Anschluss an die Sicherung wird die externe Festplatte an einem sicheren Ort aufbewahrt.

Die Datenarchivierung erfolgt anlassbezogen zum Abschluss eines Schuljahres oder eines Projektes. Die Daten werden dazu themenbezogen auf CD gebrannt und aufbewahrt. CDs sind für eine längere Aufbewahrung besser geeignet als DVDs. Ebenfalls geeignet wären DVD-RAMs, diese können jedoch von vielen DVD-Laufwerken nicht gelesen werden.

**Beispielszenario zur Datensicherung eines Servers**

An einem Server sind alle Benutzerdaten im Verzeichnis D:\Daten abgelegt. Dieses Verzeichnis soll gesichert werden.

1. In der Nacht wird eine lokale Kopie der Daten angefertigt, die den Benutzern lesend freigegeben wird.
2. Eine weitere tägliche Kopie der Daten wird auf einem Backupserver abgelegt. Dort werden ggf. zusätzlich Wochen- oder Monatskopien abgelegt.
3. Auf einer externen Festplatte wird einmal pro Monat der Datenbestand gesichert. Dazu kommen abwechselnd mehrere externe Festplatten zum Einsatz, die in einem Safe aufbewahrt werden.
4. Zur Datenarchivierung werden wichtige Daten einmal pro Jahr auf CD gebrannt und gesichert aufbewahrt. Dazu werden mehrere Sicherungssätze angefertigt, die getrennt aufbewahrt werden.

**Beispielszenario zur Datensicherung eines privaten Notebooks**

An einem privaten Notebook sollen alle relevanten Daten in einem Verzeichnis D:\Backup_Notebook_Daten und zusätzlich auf einem USB-Stick gesichert werden. Wenn sich das Notebook im „Heimnetzwerk“ befindet, werden die Daten auf einen Server übertragen.

1. Es wird ein Skript bereitgestellt, das alle relevanten Daten (auch E-Mail-Ordner, Favoriten, persönliche Kontakte, …) auf „Knopfdruck“ in das Verzeichnis D:\Backup_Notebook_Daten kopiert.
2. Es wird ein weiteres Skript bereitgestellt, um das Verzeichnis D:\Backup_Notebook_Daten auf einem USB-Datenträger abzulegen. Dabei wird automatisch überprüft, ob der richtige USB-Datenträger eingelegt ist.
3. Es wird ein weiteres Skript bereitgestellt, um das Verzeichnis D:\Backup_Notebook_Daten im „Heimnetzwerk“ auf den Server zu sichern. Dabei wird automatisch überprüft, ob das Heimnetzwerk erreichbar ist.