SCHULNETZ®

QUALIFIZIERUNG
VON SYSTEMBETREUERINNEN
UND SYSTEMBETREUERN

MICROSOFT-WINDOWS-NETZWERKE
CLIENT/SERVER

LABORÜBUNGEN

AKADEMIE FÜR LEHRERFORTBILDUNG
UND PERSONALFÜHRUNG DILLINGEN

IMPRESSUM

Herausgeber:	Akademie für Lehrerfortbildung und Personalführung Kardinal-von-Waldburg-Str. 6-7 89407 Dillingen
Autoren:	Redaktionsgruppe bayerischer Systembetreuer Georg Schlagbauer, Barbara Maier, Akademie Dillingen
URL:	http://alp.dillingen.de/schulnetz
Mail:	schlagbauer@alp.dillingen.de
Stand:	Mai 2016

Inhaltsverzeichnis

Laborübung 01 - INSTALLATION VON WINDOWS SERVER 2012 R2

Szenario

Auf einem Computer wird Windows Server 2012 neu installiert.

Vorbereitung

- Windows Server 2012 Installations-DVD oder Installations-Stick
- ggf. Treiber-CD für die verwendeten Computer bzw. Internetzugang

Aufgaben

1. Überprüfen Sie im BIOS, ob Ihre Hardware Virtualisierungstechnologie unterstützt.
2. Installieren Sie Windows Server 2012 R2 von einem Installationsmedium. Folgende Installations-Varianten stehen zur Verfügung:
   a) Klassische Installation:
   Der Windows Server wird auf einem physikalischen PC installiert (Systempartition ca. 50 GB; der restliche Festplattenplatz kann später eingerichtet werden).
   b) Installation mit Hyper-V:
   Zunächst wird ein Host-System (Windows Server 2012) mit der Rolle Hyper-V auf einem physikalischen PC installiert (Systempartition ca. 50 GB; der restliche Festplattenplatz kann später eingerichtet werden). Der eigentliche Windows Server 2012 wird als virtuelle Maschine auf diesem Hostsystem installiert (siehe Laborübung 2).
3. Überprüfen Sie, ob Updates zur Verfügung stehen und installieren Sie diese (gegebenenfalls am Host-System und in der virtuellen Maschine). Stellen Sie am Hyper-V-Host-System den Update-Mechanismus auf manuell ein.
4. Überprüfen Sie im Gerätemanager die korrekte Installation aller Hardwarekomponenten und installieren Sie bei Bedarf Gerätetreiber nach.
5. Konfigurieren Sie die Netzwerkeinstellungen an Ihrem Computer entsprechend den Erfordernissen (statische IP-Adresse, Gateway, DNS-Server).

6. 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)
7. Überprüfen Sie in der Ereignisanzeige, ob Warnmeldungen oder Fehler vorliegen und versuchen Sie, die Fehler zu beheben.

Notizen

Hinweise

Virtualisierungseinstellungen im BIOS

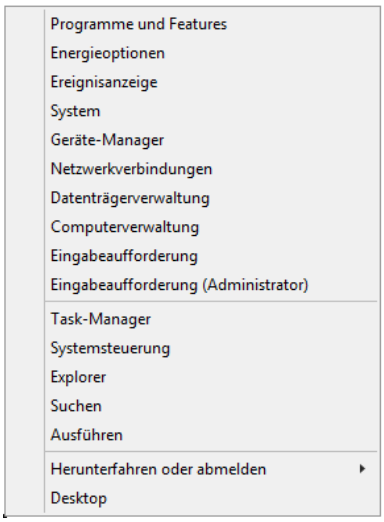
BIOS-Setup – (Security) – Virtualization

Verwaltungswerkzeuge unter Windows Server 2012

Schnellzugriff (`Win+x` oder Rechtsklick auf Startkachel)

Ressourcenmonitor (`resmon.exe`)

Informationen zu Fehlermeldungen der Ereignisanzeige: http://eventid.net



Server Manager – Lokaler Server

- Windows Updates
- Netzwerkkarte konfigurieren

Notizen

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.
`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`	Löscht die Einträge in der arp-Tabelle.
`netstat –n`	Bestehende Netzwerkverbindungen werden angezeigt.
`nbtstat –c`	Der Cache zur NetBIOS-Namensauflösung wird angezeigt.

Notizen

Laborübung 02 - UMGANG MIT HYPER-V

Szenario

Ein Windows Server 2012 R2 soll als virtuelle Maschine unter Hyper-V auf dem Host-System installiert werden. Auf die Laborübung kann verzichtet werden, wenn entschieden wurde, den Server physikalisch zu installieren.

Aufgaben

1. Fügen Sie dem System die Rolle Hyper-V zu.
2. Wählen Sie sinnvolle Vorgaben für die Speicherorte der virtuellen Festplatten und Computer.
3. Erstellen Sie einen virtuellen Switch mit einer Verbindung zum externen Netzwerk.
4. Installieren Sie Windows Server 2012 R2 in einer neuen virtuellen Maschine.

Notizen

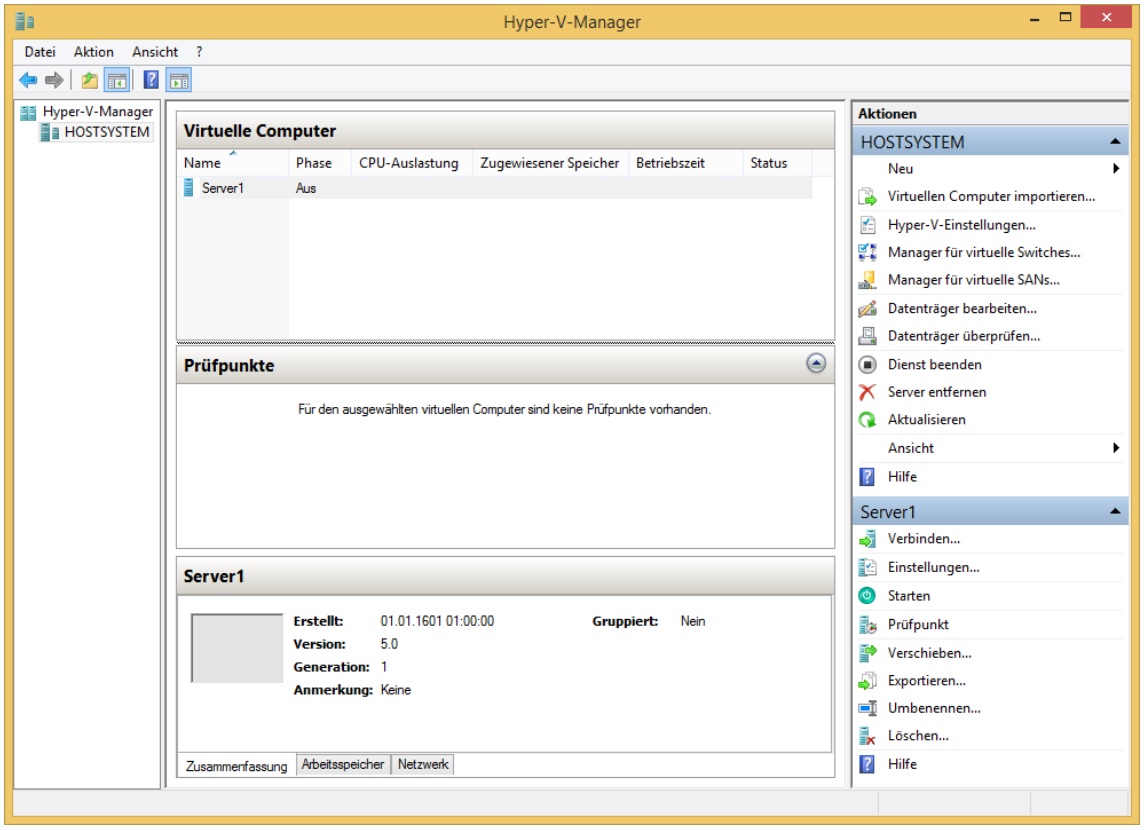
Hinweise

Hyper-V-Rolle hinzufügen

Server-Manager – Verwalten – Rollen und Features hinzufügen

Hyper-V-Manager

Server-Manager – Tools – Hyper-V-Manager



Speicherorte der virtuellen Festplatten und Computer

Standardmäßig sind die Speicherorte im Profil des Benutzers festgelegt. Dies sollte bei einer Serverinstallation geändert werden, z.B.

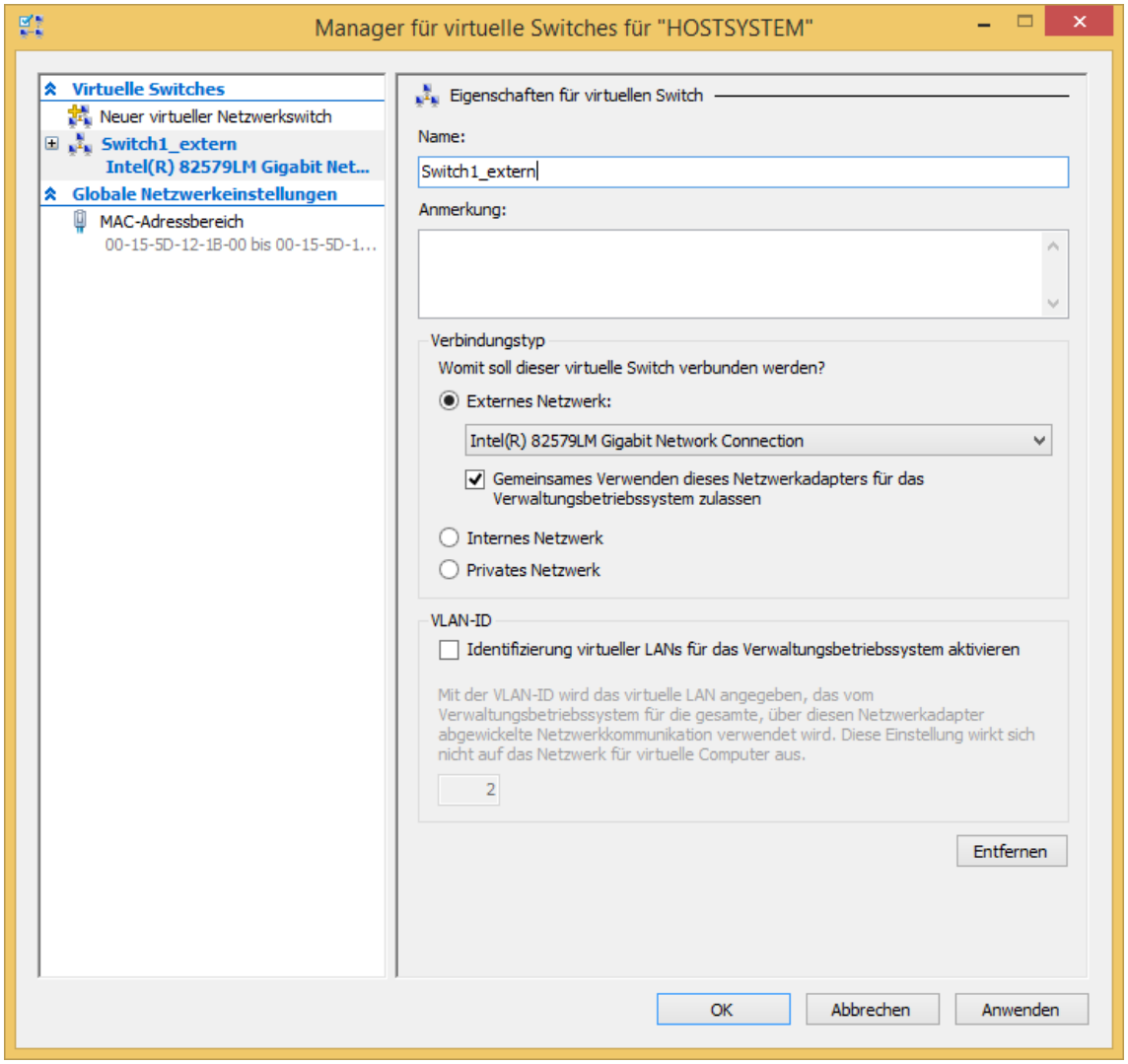
Speicherort für virtuelle Festplatten: D:\Hyper-V\VHDs

Speicherort für virtuelle Computer: D:\Hyper-V

Es empfiehlt sich, die virtuellen Maschinen auf einer eigenen Partition zu betreiben.

Manager für virtuelle Switche

Die Netzwerkkarten der virtuellen Computer werden mit einem virtuellen Switch verbunden. Soll der virtuelle Computer wie ein realer Computer in das Netz eingebunden werden, muss der virtuelle Switch mit der physikalischen Netzwerkkarte verbunden werden.



Notizen

Laborübung 03 - REMOTEADMINISTRATION DES SERVERS

Szenario

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

Aufgaben

1. Konfigurieren Sie Ihren Server:
   - Windows-Updates
   - Netzwerkeinstellungen (statische IP-Adresse)
   - Sinnvoller Computername (max. 15 Zeichen)
   - Internet-Explorer – Verstärkte Sicherheitskonfiguration ein-/ausschalten

Remote-Administration

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

Systemsicherung

3. Erstellen Sie ein Backup Ihrer Server 2012-Grundinstallation.

Hinweise

Netzwerkstandorte

Der Netzwerkstandort bestimmt die Firewall-Regeln. Die Remotedesktopverbindung ist standardmäßig nur innerhalb eines privaten Netzwerks möglich.

Netzwerkstandort ändern über die lokale Sicherheitsrichtlinie

Lokale Sicherheitsrichtlinie (`secpol.msc`) – Netzwerklisten-Manager-Richtlinien – Netzwerk – Netzwerkadresse

Netzwerkstandort ändern mit der Powershell

```
PS C:\> Get-NetConnectionProfile


Name             : Netzwerk
InterfaceAlias   : Ethernet
InterfaceIndex   : 4
NetworkCategory  : Public
IPv4Connectivity : Internet
IPv6Connectivity : NoTraffic


PS C:\>Set-NetConnectionProfile -InterfaceIndex 4 -NetworkCategory private
```

Remotedesktopverbindung in der Firewall öffnen

Falls der Netzwerkstandort „Öffentliches Netzwerk“ ist, muss die Remotedesktopverbindung in der eingehenden Firewall-Regel erlaubt werden.

Remotedesktopverbindung aktivieren

Server-Manager – Lokaler Server – Remotedesktop

Remotezugriff vom Client auf den Server herstellen

Remotedesktopverbindung (`mstsc` – Microsoft Terminal Server Client)

Remotezugriff auf einen Windows-PC

Über das RDP-Protokoll (Remote Desktop Protocol, TCP- und ab Version 8.0 auch UDP-Port 3389) kann eine Terminal-Verbindung zu einem Windows-PC hergestellt werden. Bei der Verbindung zu einem Windows-Rechner ist nur eine Konsolenverbindung möglich, bei der ggf. ein angemeldeter Benutzer getrennt wird. Zu einem Windows-Server sind gleichzeitig zwei Verbindungen mit unterschiedlichen Benutzer-Accounts möglich.

Laborübung 04 - DOMAINCONTROLLER, DNS, DHCP

Szenario

Der Windows Server 2012 soll als Domaincontroller, DNS- und DHCP-Server arbeiten.

Aufgaben

1. Diskutieren Sie, für welche Aufgaben ein Domänencontroller erforderlich ist.
2. Installieren Sie, falls noch nicht vorhanden, die Serverrollen Domänencontroller (Active Directory Domänendienste), DNS und DHCP (ggf. zuvor Prüfpunkt erstellen).
3. Richten Sie Ihren Windows Server 2012 unter folgenden Vorgaben als Domänencontroller ein:
   - Neue Gesamtstruktur
   - 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
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 gegebenenfalls eine Reverse-Lookupzone, so dass auch die Auflösung der IP-Adressen in Rechnernamen funktioniert. Überprüfen Sie die Reverse-Namensauflösung mit nslookup.
6. Richten Sie den DHCP-Dienst entsprechend den Netzwerkgegebenheiten ein. Sorgen Sie dafür, dass die Clients die eigene IP-Adresse, die IP-Adresse des Standardgateways und des DNS-Servers automatisch über DHCP beziehen. Überprüfen Sie die Funktionsfähigkeit des DHCP-Dienstes am Client.

Hinweise

Diskussionspapier

	Lösungen	DC erforderlich
Dateiaustausch über das Netzwerk		
Jeder Benutzer hat ein eigenes Homeverzeichnis		
Benutzerverwaltung		
DNS (Namensauflösung)		
DHCP		
Windows-Client (Installation)		
Windows-Client (Softwareverteilung)		
Windows-Client (Servergespeicherte Profile)		
Windows-Client (Schutz vor Änderungen)		

Rollen und Features hinzufügen

Server-Manager – Verwalten – Rollen und Features hinzufügen

Wahl des Domänennamens

Die Endung .local wird im Internet nicht verwendet und kann deshalb keine Kollisionen mit bestehenden Domänen verursachen. Wenn die Schule über einen öffentlichen Domänennamen (z.B. mittelschule-dillingen.de) verfügt, kann es sinnvoll sein, statt .local einen Subdomänen-Namen (z.B. schulnetz.mittelschule-dillingen.de) zu verwenden.

Nachteile der Endung .local

- Es kann kein vertrauenswürdiges SSL-Zertifikat erworben werden.
- Ein lokaler Exchange-Server verwendet standardmäßig Benutzer@Domänennamen als Antwortadresse. Emails an diese Adressen (z.B. user@mittelschule-dillingen.local) können nicht zugestellt werden.

Einrichten einer Reverse-Lookupzone

Reverse-Lookupzonen sind in einem lokalen Netzwerk nicht notwendig. Die Auflösung einer IP-Adresse in einen Namen ist z.B. beim Betrieb eines öffentlichen Mail-Servers notwendig.

Server-Manager – Tools – DNS – Reverse Lookupzone – Neue Zone

DHCP konfigurieren

Server-Manager – Tools – DHCP – Neuen Bereich anlegen

nslookup (Name Server Lookup)

Mit nslookup kann ein Nameserver nach der Auflösung eines Namens oder einer IP-Adresse angefragt werden.

```
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`	Anfrage 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 autorisierende 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.

`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.

DHCP (Dynamic Host Configuration Protocol)

DHCP 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 (Dies muss zwingend der Domänencontroller bzw. der für die Domäne zuständige DNS-Server sein.)

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

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 (Resource 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. Bei Windowssystemen befindet sich die Datei im Verzeichnis Windows\system32\drivers\etc.

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

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.

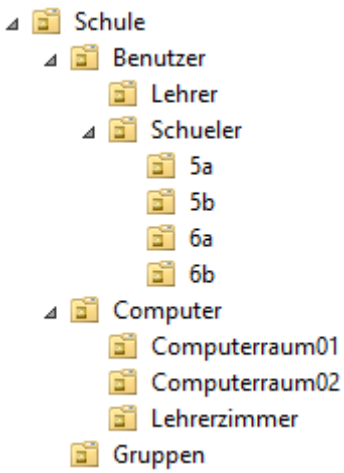
Laborübung 05 - EINRICHTEN EINER ACTIVE-DIRECTORY-STRUKTUR

Szenario

Die vorhandene Schulstruktur soll in der Domäne abgebildet werden.

Aufgaben

1. Richten Sie eine AD-Struktur für Ihre Schule 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. Legen Sie einen neuen Benutzer an und vergeben Sie ihm ein gültiges Passwort nach den geltenden Komplexitätsrichtlinien.

Hinweise

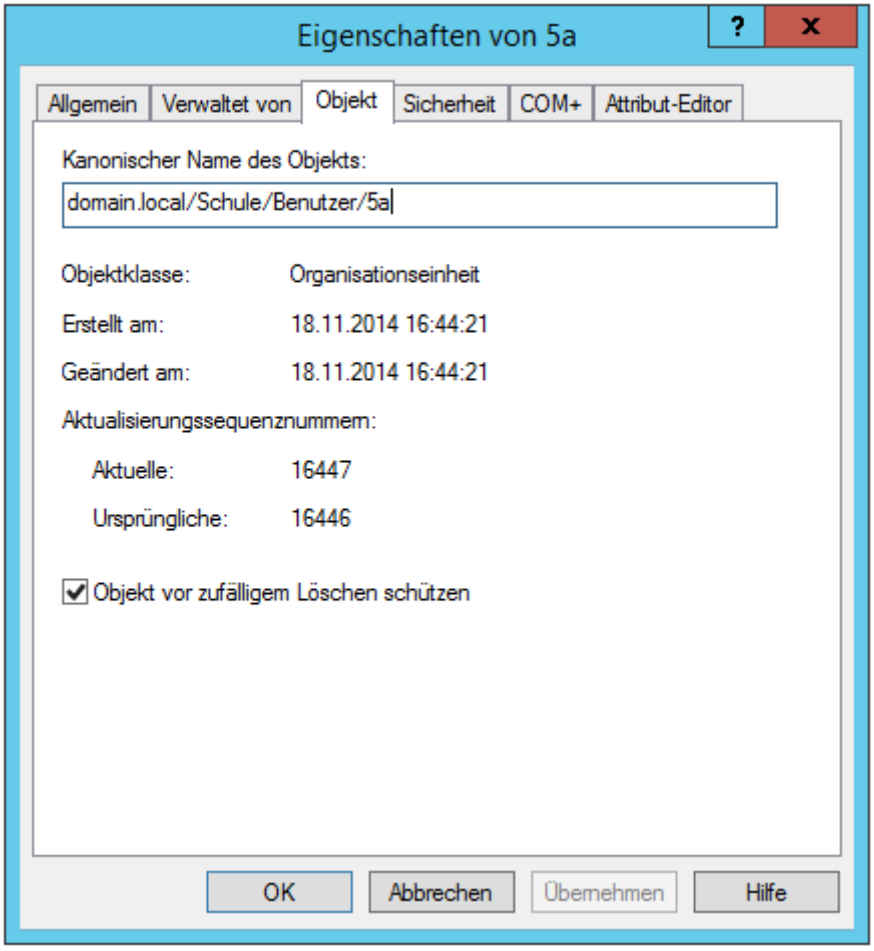
Im Active Directory (Verzeichnisdienst) sind die Rollen und Berechtigungen aller Benutzer und Computer abgebildet. Die spätere Administration wird erleichtert, wenn die Struktur im Active Directory der realen Schulstruktur entspricht.

Client in die Domäne aufnehmen

Computer:	Eigenschaften – Computername – Ändern
Windows-Taste + Pause:	Eigenschaften – Computername – Ändern

OU-Einträge löschen oder verschieben

Beim Anlegen einer Organisationseinheit wird diese standardmäßig vor versehentlichem Löschen geschützt. Soll diese OU nachträglich gelöscht oder verschoben werden, muss bei den Eigenschaften der OU in der Registerkarte Objekt der entsprechende Eintrag deaktiviert werden. Falls die Registerkarte Objekt nicht sichtbar ist, kann diese durch Aktivierung „Erweiterte Features“ im Menüpunkt „Ansicht“ angezeigt werden.



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.
Managed Service Accounts	Verwaltet z.B. Exchange- oder SQL-Dienstkonten.
Foreign Security Principals	SIDs (Security-IDs) aus anderen Domänen, zu denen eine Vertrauensstellung existiert.
Users	Benutzer und Gruppen, die automatisch angelegt werden.

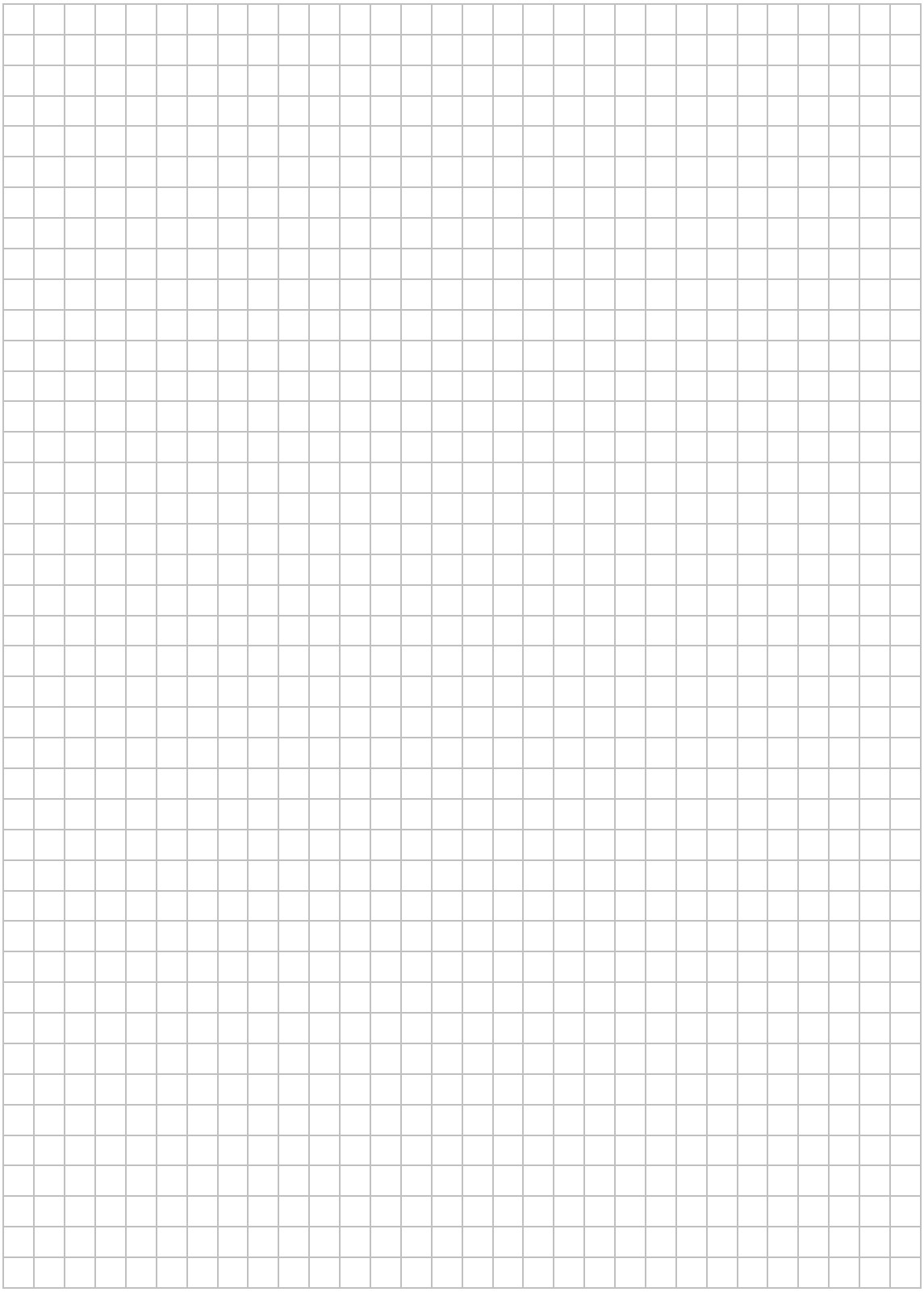
Mit Ausnahme der Domain Controllers sind die Standardcontainer nicht als Organisatorische Einheiten (OUs) definiert. Deshalb stehen für diese Container bestimmte Funktionen (z. B. Gruppenrichtlinien) nicht zur Verfügung.

Komplexitätsrichtlinien für Passwörter

Wenn die Komplexitätsrichtlinien aktiviert sind, muss ein Passwort mindestens sieben Zeichen aus drei verschiedenen Kategorien haben:

Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen.

Notizen



Laborübung 06 - GRUPPENRICHTLINIEN

Szenario

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

Aufgaben

1. Ändern Sie die Kennwortrichtlinie für Domänen so ab, dass auch kurze und einfache Kennwörter erlaubt sind.
2. Erstellen Sie eine Gruppenrichtlinie, die es verbietet, die Systemsteuerung aufzurufen. Lehrkräfte sollen von der Richtlinie nicht betroffen sein. Testen Sie die Funktionalität der Gruppenrichtlinie.
3. Der Zugriff der Schüler auf das Internet soll über einen Proxy erfolgen. Sorgen Sie dafür, dass der Proxy über eine Gruppenrichtlinie in den Internet-Explorer eingetragen wird.

Hinweise

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.

Einfache Kennwörter

Default Domain Policy

Gruppenrichtlinie: Computerkonfiguration – Richtlinien – Windows-Einstellungen – Sicherheitseinstellungen – Kontorichtlinien – Kennwortrichtlinien

Systemsteuerung verbieten

Gruppenrichtlinie: Benutzerkonfiguration – Richtlinien – Administrative Vorlagen – Systemsteuerung

Aktualisierung der Gruppenrichtlinien

Gruppenrichtlinien werden automatisch alle 90 – 120 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.

Weiterführende Informationen

Gruppenrichtlinien

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

Gruppenrichtlinien werden auf Organisationseinheiten vergeben und wirken auf alle Benutzer und Computer in dieser Organisationseinheit.

Hierarchie der Gruppenrichtlinien

In Domänenstrukturen sind Gruppenrichtlinien hierarchisch geordnet. Die Verarbeitung erfolgt in einer bestimmten Reihenfolge:

- Lokale Sicherheitseinstellungen und lokale Gruppenrichtlinien
- Domänen-Gruppenrichtlinien

- Gruppenrichtlinien 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 kann damit nicht mehr durch eine nachgeordnete Richtlinie überschrieben werden.
- Bestimmte Richtlinien wirken nur, wenn sie auf Domänenebene (Default Domain Policy) vergeben werden (z. B. Kennwortrichtlinien).

Speicherort der Gruppenrichtlinien

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

Kontrolle der Gruppenrichtlinien

Am Client:	rsop.msc (Resultant Set of Policies, Richtlinienergebnissatz)
	gpresult.exe /r
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

Letzten Anmeldenamen nicht anzeigen

Gruppenrichtlinie: Computerkonfiguration – Richtlinien – Windows-Einstellungen – Sicherheitseinstellungen – Lokale Richtlinien – Sicherheitsoptionen – „Interaktive Anmeldung: Letzten Benutzernamen nicht anzeigen“

Zwischengespeicherte Profile löschen

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

Beim Anmelden auf Netzwerk warten

Unter Windows wird der Windows-Explorer vor dem Netzwerk geladen. Desktopeinstellungen, 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:

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

Zugriff auf Systemsteuerungselemente regeln

Gruppenrichtlinie: Benutzerkonfiguration – Richtlinien – 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.

Gruppenrichtlinie: Computerkonfiguration – Richtlinien – Windows-Einstellungen – Sicherheitseinstellungen – Lokale Richtlinien – Sicherheitsoptionen – „Domänenmitglied: Änderungen von Computerkennwörtern deaktivieren“

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. Das heißt, benutzerbezogene Einstellungen sollen 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.

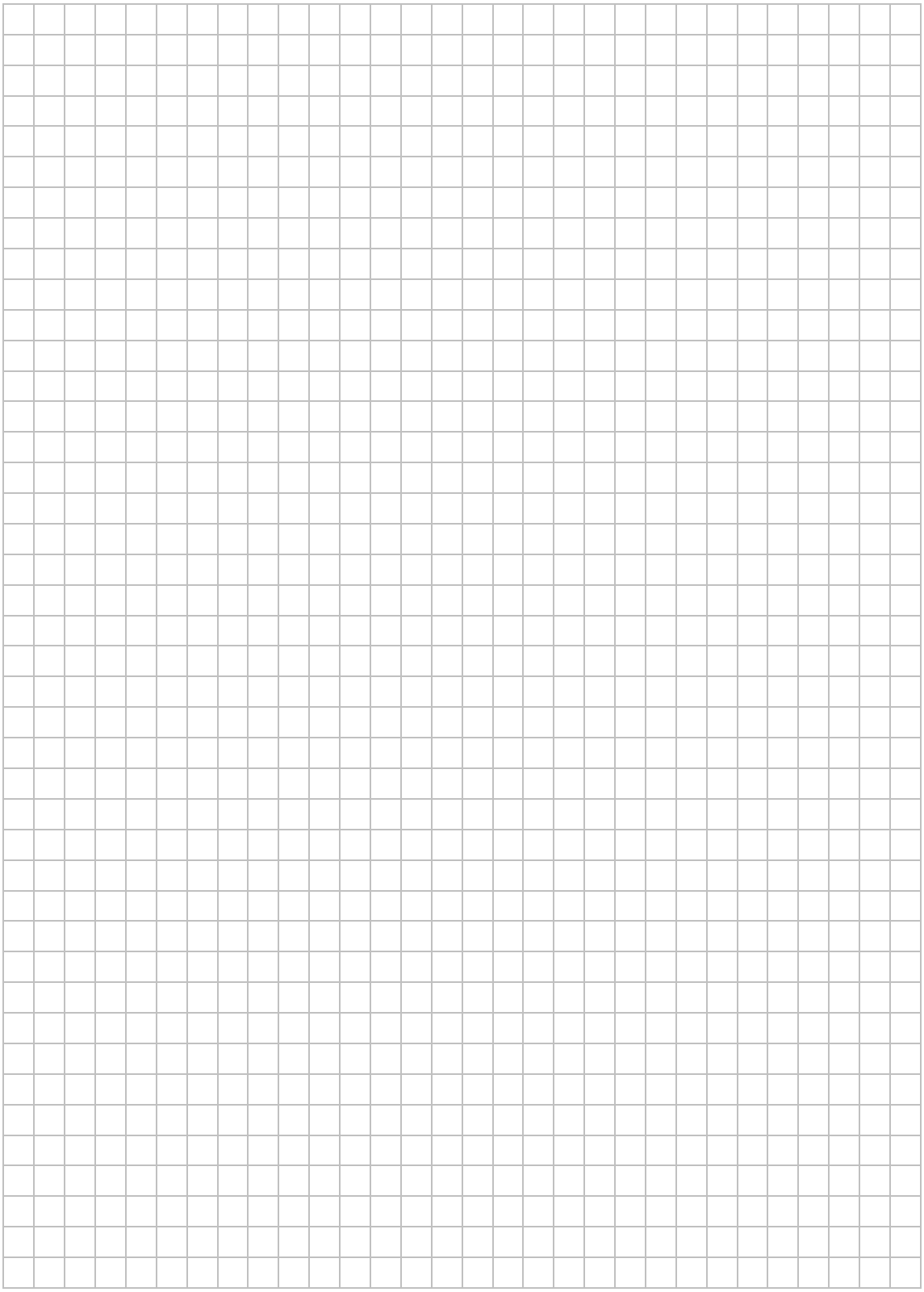
Gruppenrichtlinie: Computerkonfiguration – Richtlinien – Administrative Vorlagen – System – Gruppenrichtlinie – „Loopbackverarbeitungsmodus für Benutzergruppenrichtlinie konfigurieren“

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.

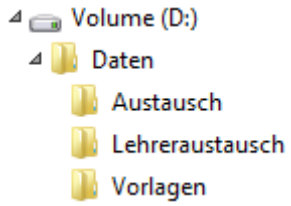
Notizen



Laborübung 07 - SMB-ZUGRIFF UND NTFS-RECHTE BEIM 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 an und ordnen Sie die Benutzer s1, s2, l1, l2 diesen Gruppen zu.
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. Die Freigabe soll über einen Laufwerksbuchstaben angesprochen werden.

Weiterführende Aufgaben

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

6. Im freigegebenen Ordner *Daten* soll ein Benutzer keine weitere Ordner oder Dateien anlegen können.
7. Überprüfen Sie, ob ein Schüler oder eine Lehrkraft in der Lage ist, das Austauschverzeichnis versehentlich zu löschen und verhindern Sie dies gegebenenfalls.
8. 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.
9. 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.

Ordner ohne Berechtigungen ausblenden

Server-Manager – Datei-/Speicherdienste – Freigaben - <Freigabe>-Eigenschaften – Einstellungen – Zugriffsbasierte Aufzählung aktivieren

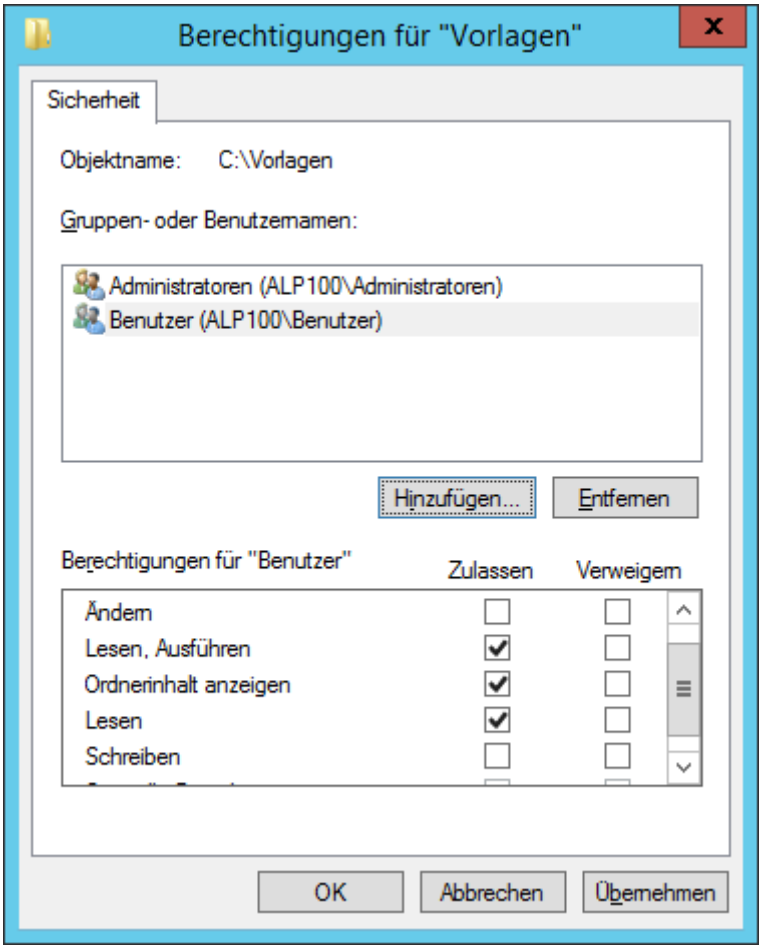
Gruppenrichtlinie zur Laufwerkszuordnung

Gruppenrichtlinie: Benutzerkonfiguration – Einstellungen – Windows-Einstellungen – Laufwerkszuordnungen

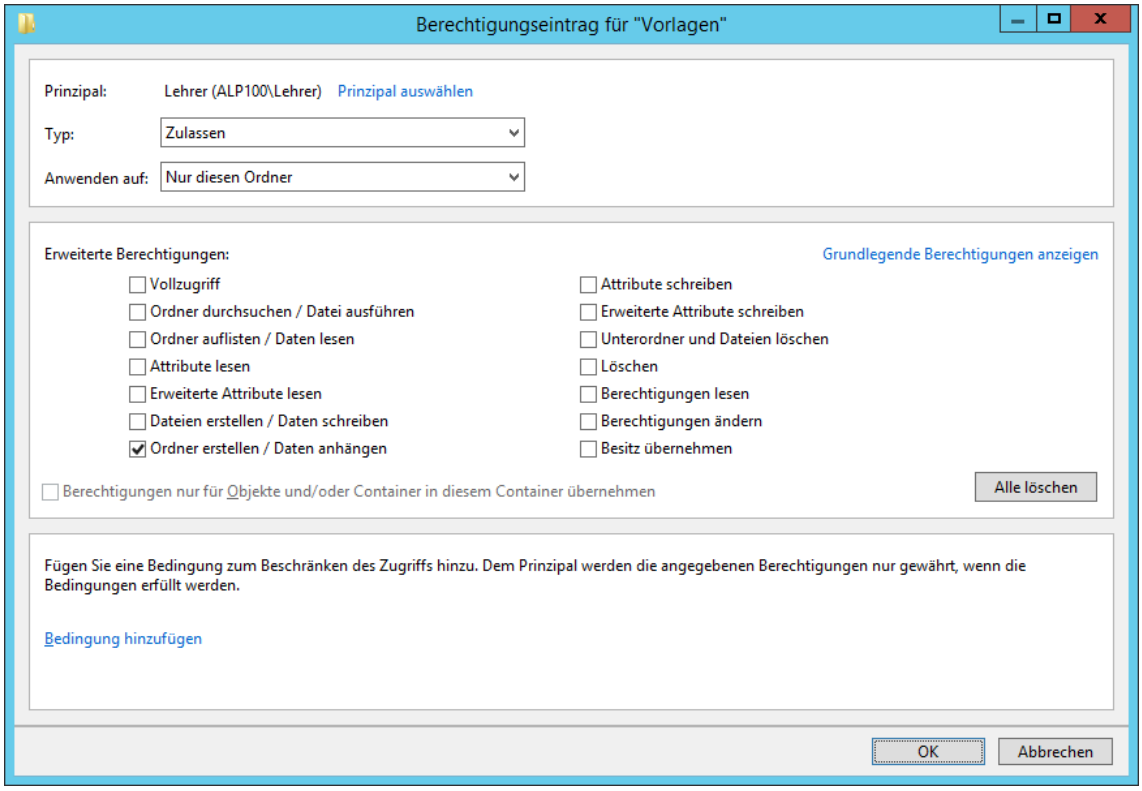
Beispiel für die Vergabe von NTFS-Rechten

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.

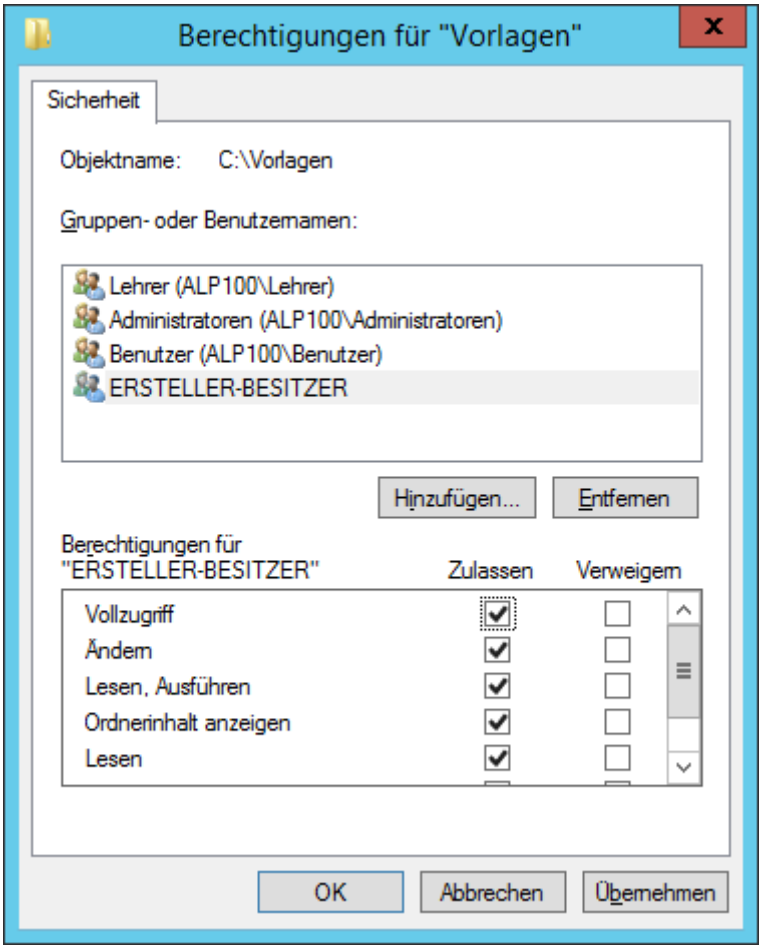
Im ersten Schritt wird für den Ordner Vorlagen die Vererbung unterbrochen und überflüssige Berechtigungen entfernt. Die Gruppe der Administratoren erhält weiterhin Vollzugriff. Die Gruppe der Benutzer erhält Leserechte. Alle Lehrer und Schüler sind in der Gruppe Benutzer enthalten.



Im zweiten Schritt wird der Gruppe Lehrer die Berechtigung gegeben, im Ordner Vorlagen Ordner zu erstellen. Damit können Lehrkräfte Ordner anlegen; sie können den Ordner jedoch nicht umbenennen und auch keine Dateien in diesen Ordner ablegen.



Im dritten Schritt wird der Gruppe „Ersteller-Besitzer“ Vollzugriff gegeben. Hat ein Lehrer einen Ordner angelegt, ist er „Ersteller-Besitzer“ dieses Ordners und hat damit Vollzugriff. Alle anderen Benutzer haben durch die Vererbung Leserechte.



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).

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.

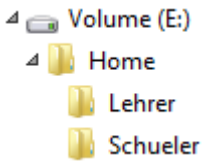
Laborübung 08 - DAS PERSÖNLICHE HOMEVERZEICHNIS

Szenario

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

Aufgaben

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



2. Weisen Sie jedem Schüler und jeder Lehrkraft im dazugehörigen 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. Sorgen Sie dafür, dass beim Speichern unter Dokumente das Homeverzeichnis der Benutzer verwendet wird.

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%
```

Ordner Dokumente umleiten

Der Ordner „Dokumente“ ist im Benutzerprofil gespeichert. Damit Dokumente standardmäßig auf dem Server gespeichert werden, sollte der Ordner „Dokumente“ in das Homeverzeichnis des Benutzers umgeleitet werden.

Gruppenrichtlinie: Benutzerkonfiguration – Richtlinien – Windows-Einstellungen – Ordnerumleitung

Soll der Administrator Zugriff auf den Ordner „Dokumente“ erhalten, dürfen dem Benutzer keine exklusiven Zugriffsrechte gewährt werden.

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

Die Ordnerumleitungen für Bilder, Videos und Musik können so festgelegt werden, dass sie dem Ordner „Dokumente“ folgen.

Laborübung 09 - SERVERGESPEICHERTE PROFILE

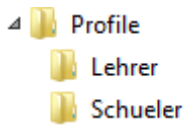
Szenario

Jede Lehrkraft soll an jedem Computer der Domäne ihre persönlichen Desktop-Einstellungen und ihre persönlichen Windows-Explorer-Einstellungen vorfinden und diese entsprechend ihren Vorstellungen abändern dürfen.

Die Schüler bekommen ein einheitliches verbindliches Standardprofil.

Aufgaben

1. Erstellen Sie einen Ordner z. B. „Profile“ und geben Sie diesen frei. Übernehmen Sie die unten angegebene Ordnerstruktur.



2. Weisen Sie der Lehrkraft den jeweils passenden Profilpfad zu. Überprüfen Sie, ob das Profil auf den Server geschrieben wurde. Zeigen Sie, dass Sie als Administrator standardmäßig keinen Zugriff auf dieses Profil haben.
3. Sorgen Sie über eine entsprechende Gruppenrichtlinie dafür, dass bei zukünftig angelegten Profilen die Administratoren nicht ausgesperrt bleiben.
4. Erstellen für alle Schüler ein einheitliches verbindliches Standardprofil, das diese nicht mehr verändern können.

Weiterführende Aufgaben

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%
```

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 die Berechtigung einen Ordner zu erstellen.

Administrativer Zugriff auf Profile

Über eine Computergruppenrichtlinie kann dem Administrator Einblick in neu angelegte Profilordner der Benutzer gewährt werden.

Gruppenrichtlinie: Computerkonfiguration – Richtlinien – Administrative Vorlagen – System – Benutzerprofile – „Sicherheitsgruppe Administratoren zu servergespeicherten Profilen hinzufügen“.

Default User-Profil

Hat ein Benutzer noch kein eigenes Profil, wird das „Default User“-Profil des lokalen Computers an dem sich der Benutzer zum ersten Mal anmeldet als Vorlage genommen.

Verbindliches Standardprofil

Der einfachste Weg, für alle Schüler ein einheitliches verbindliches Standardprofil zu erstellen, geht wie folgt:

1. Für einen beliebigen Schüler wird ein servergespeichertes Profil angelegt.
   `\\DC\Profile\Schueler\Standard`
2. Im Profil wird die Datei NTUSER.DAT in NTUSER.MAN (mandatory, verbindlich) umbenannt.
3. Dem betreffenden Schüler werden die Vollzugriffsrechte für das Profil entzogen und dafür für alle Schüler Leserechte gesetzt.
4. Der Profilpfad wird bei allen Schülern (im Active Directory) eingetragen.

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

Weiterführende Informationen

Einschränkungen bei der Nutzung servergespeicherter Profile

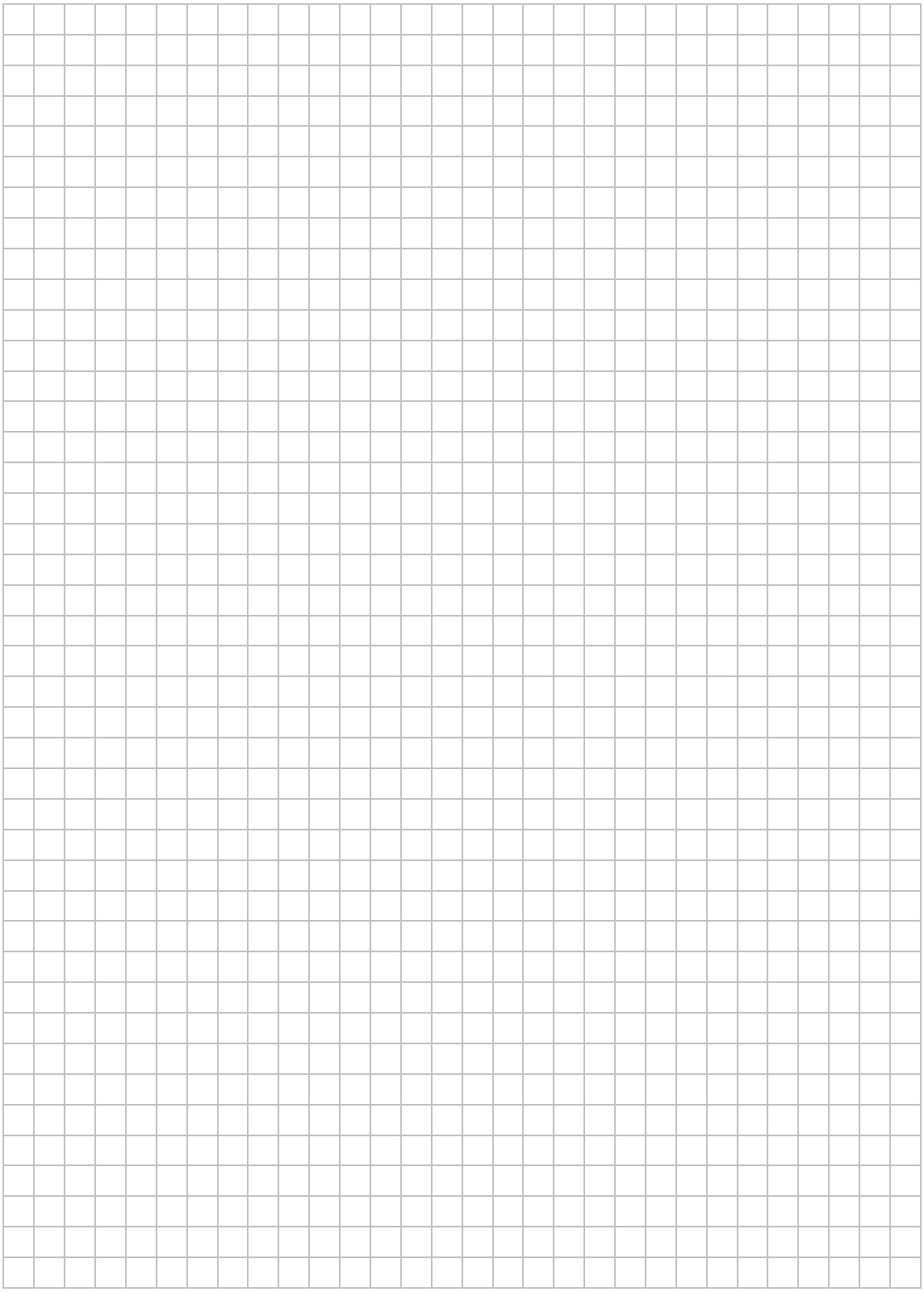
Werden in einer Domänenstruktur unterschiedliche Client-Systeme (Windows 7, 8, 8.1, 10) verwendet, können servergespeicherte Profile Probleme bereiten. Ebenso problematisch können Clients sein, auf denen unterschiedliche Versionen der Anwendungsprogramme laufen. Viele moderne Programme (Apps) nehmen auf servergespeicherte Profile keine Rücksicht.

Große servergespeicherte Profile verlängern die Anmelde- und Abmeldezeit.

Defekte Profile können nicht repariert, sondern nur gelöscht werden.

Notizen

Notizen



Laborübung 10 - 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 – Richtlinien – 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 – Richtlinien – 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 – Richtlinien – Administrative Vorlagen – Windows-Komponenten – Windows Installer: „Immer mit erhöhten Rechten installieren“

MSI-Pakete erstellen

Das Erstellen von MSI-Paketen kann sehr aufwändig werden. Die meisten Werkzeuge (MSI-Generator) dazu sind kostenpflichtig.

Grundsätzliches Vorgehen beim Erstellen eines MSI-Paketes

- MSI-Generator auf einer „sauberen“ Arbeitsstation installieren.
- „Vorher Schnappschuss“ der Arbeitsstation erstellen.
- Die gewünschte Software installieren.
- „Nachher Schnappschuss“ erstellen.

MSI-Pakete besorgen

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.

Acrobat Reader: ftp://ftp.adobe.com/pub/adobe/reader/win

Firefox: http://www.frontmotion.com/

Laborübung 11 - DRUCKEN IM NETZWERK

Szenario

Jeder Computerraum verfügt über einen eigenen Drucker. Die Benutzer sollen die Drucker im jeweiligen Raum nutzen können.

Aufgaben

1. Die Benutzer sollen automatisch den Drucker im jeweiligen Raum als Standarddrucker zur Verfügung haben.

Hinweise auf Installationskonzepte für das Drucken

Lokale Installation am Client

Am einfachsten ist es, wenn alle Drucker lokal auf den Clients installiert sind. Die Benutzer wählen je nach Standort den richtigen Drucker aus.

In der Praxis kann dies so funktionieren, dass im Image alle Drucker aller Räume installiert sind. Als Standard-Drucker ist ein pdf-Drucker ausgewählt. Durch die Netzwerkinfrastruktur (VLANs, Firewall) wird verhindert, dass Drucker anderer Räume angesprochen werden.

Installation eines Netzwerkdruckers am Client (Lokaler Drucker)

Systemsteuerung – Geräte und Drucker – Drucker hinzufügen – Lokalen Drucker oder Netzwerkdrucker mit manuellen Einstellungen hinzufügen

Drucken über eine Freigabe eines Servers

Der Drucker wird am Server installiert und freigegeben. Die Clients greifen über die Freigabe am Server auf den Drucker zu. Bei diesem Verfahren kann der Server die Druckertreiber für die Clients bereitstellen.

Installation und Freigabe eines Netzwerkdruckers am Server

Systemsteuerung – Geräte und Drucker – Drucker hinzufügen – IP Adresse – Treiber wählen – Freigabename festlegen – im Verzeichnis auflisten

Zuweisen eines Druckers am Client

1. Durch den angemeldeten Benutzer (Rechtsklick auf die Freigabe)
2. Durch Gruppenrichtlinien
3. Durch Anmeldeskripte

Druckerzuweisung durch Gruppenrichtlinien

Mit Gruppenrichtlinien können Drucker sowohl benutzer- als auch computerabhängig zugewiesen werden. Empfohlen werden dabei Druckertreiber vom Typ 4.

Drucker nach Raumzugehörigkeit zuweisen

Neue Rolle am DC:	Installieren der Rolle „Druck- und Dokumentendienste“
Druckverwaltung:	Server – Treiberpakete hinzufügen
Druckverwaltung:	Drucker – neuen Drucker hinzufügen, freigeben
Gruppenrichtlinie:	Erstellen einer Gruppenrichtlinie zur Verteilung der Drucker und Zuweisen dieser Richtlinie auf die betreffenden OUs
Drucker rechte Maus:	„Mit Gruppenrichtlinie bereitstellen“, zuvor erstellte Gruppenrichtlinie auswählen

Druckerzuweisung per Computerrichtlinie

Gruppenrichtlinie:	Computerkonfiguration – Einstellungen – Systemsteuerungseinstellungen – Drucker Neu – TCP/IP Drucker

Druckerzuweisung per Benutzerrichtlinie

Gruppenrichtlinie: Benutzerkonfiguration – Einstellungen – Systemsteuerungseinstellungen – Drucker Neu – freigegebener Drucker

Druckerinstallation soll ohne administrativen Eingriff erfolgen (Point and Print)

Bei Windows 7 verhindert diese Richtlinie, dass bei den Clients evtl. eine Warnung oder eine Eingabeaufforderung mit erhöhten Rechten erscheint, um den Drucker zu installieren.

Gruppenrichtlinie: Computerkonfiguration – Richtlinien – Administrative Vorlagen – Drucker – „Point-and-Print-Einschränkungen“ – deaktivieren

Druckerzuweisung über Anmeldeskripte

Zugriff auf eine Druckerfreigabe über ein Anmeldeskript

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

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 IP-Adresse

```
REM Zuweisen eines freigegebenen Druckers
REM in Abhängigkeit der ersten 3 Bytes der IP-Adresse des Client-PCs.
REM Der neu zugewiesene Drucker wird als Standard definiert.
```

```
REM IP-Adresse ermitteln und zerlegen (IP enthält die ganze Adresse,
REM IPb1 bis IPb4 die einzelnen Bytes)

for /f "skip=1 tokens=2 delims=[]" %%* in ('ping.exe -n 1 -4 %computer-
name%') Do (set "IP=%%*")
for /f "tokens=1,2,3,4 delims=." %%a in ("%IP%") do set IPb1=%%a&set
IPb2=%%b&set IPb3=%%c&set IPb4=%%d

IF %IPb1%==10 (
  IF %IPb2%==0  (
    IF %IPb3%==200 (
      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 (
```

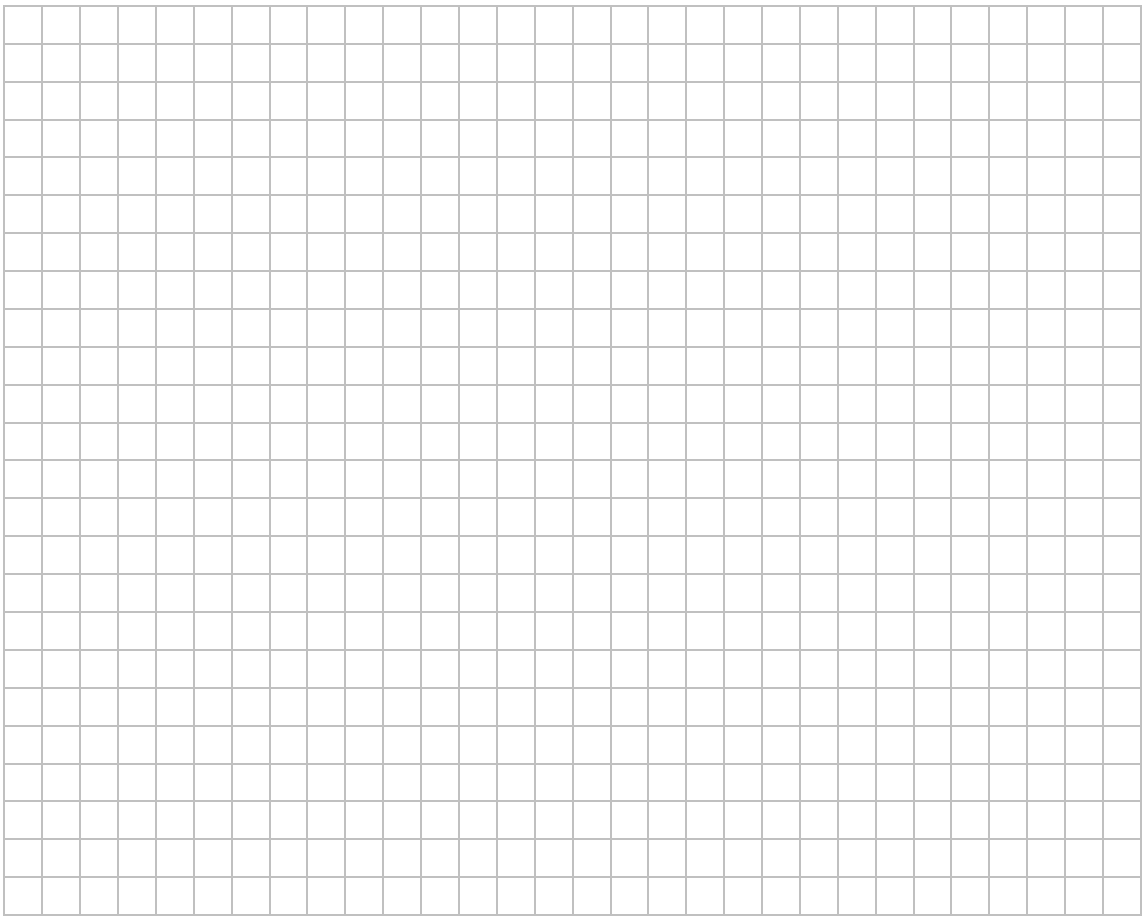
```
   echo "Computer ist in Raum EDV_2"
   rundll32 printui.dll,PrintUIEntry /in /n \\server\HP
   rundll32 printui.dll,PrintUIEntry /y  /n \\server\HP
)
```

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.

Notizen



Notizen

Laborübung 12 - 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

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 – Richtlinien – 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 – Richtlinien – 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

Variante A:

```
@echo off
REM Zuweisen einer Laufwerksverbindung
REM in Abhängigkeit der Gruppenmitgliedschaft
net user /DOMAIN %username% | find „G_Schuelerzeitung“
if not errorlevel = 1 (
   net use s: %logonserver%\Schuelerzeitung /persistent:no
)
```

Variante B:

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

net user /DOMAIN %username% | find „G_Schuelerzeitung“
if errorlevel 1 goto next1
   net use s: /delete
   net use s: %logonserver%\Schuelerzeitung /persistent:no
:next1
```

ERGÄNZENDE ÜBUNGEN

UPDATE EINES DOMÄNENCONTROLLERS

Szenario

Ein bestehender Domänencontroller z.B. auf Basis von Server 2003 oder 2008, soll auf einen Domänencontroller auf Basis von Server 2012 R2 upgedatet werden.

Ein bestehender Domänencontroller soll auf eine neue Hardware umgezogen und ggf. virtualisiert werden.

Update eines Domänencontrollers

Nicht empfohlene Vorgehensweise: Sukzessive Migration von Server 2003 auf Server 2008, Server 2008 R2, Server 2012, Server 2012 R2.

Gründe:

- Migration von 32-Bit-Versionen auf 64-Bit-Versionen nicht möglich
- Veraltete Hardware bleibt bestehen
- Jeder Migrationsschritt kann scheitern (Backup notwendig)

Empfohlene Vorgehensweise:

Ein zweiter Domänencontroller mit aktuellem Serverbetriebssystem wird in die bestehende Domäne als weiterer Domänencontroller aufgenommen. Anschließend wird der bisherige DC zu einem normalen Server herabgestuft. Die FSMO-Rollen werden automatisch auf den neuen DC übertragen. Der neue Domänencontroller ist gleichzeitig auch der neue DNS-Server. Dies muss den Clients bzw. dem DHCP-Server mitgeteilt werden.

Dienste und Speicherbereiche, die auf dem ehemaligen DC noch aktiv sind (z. B. DHCP, Druckdienste, Dateifreigaben, Homeverzeichnisse, Profile, etc.) müssen manuell verschoben werden. Anschließend kann der herabgestufte Server aus der Domäne genommen und abgeschaltet werden.

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 of 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

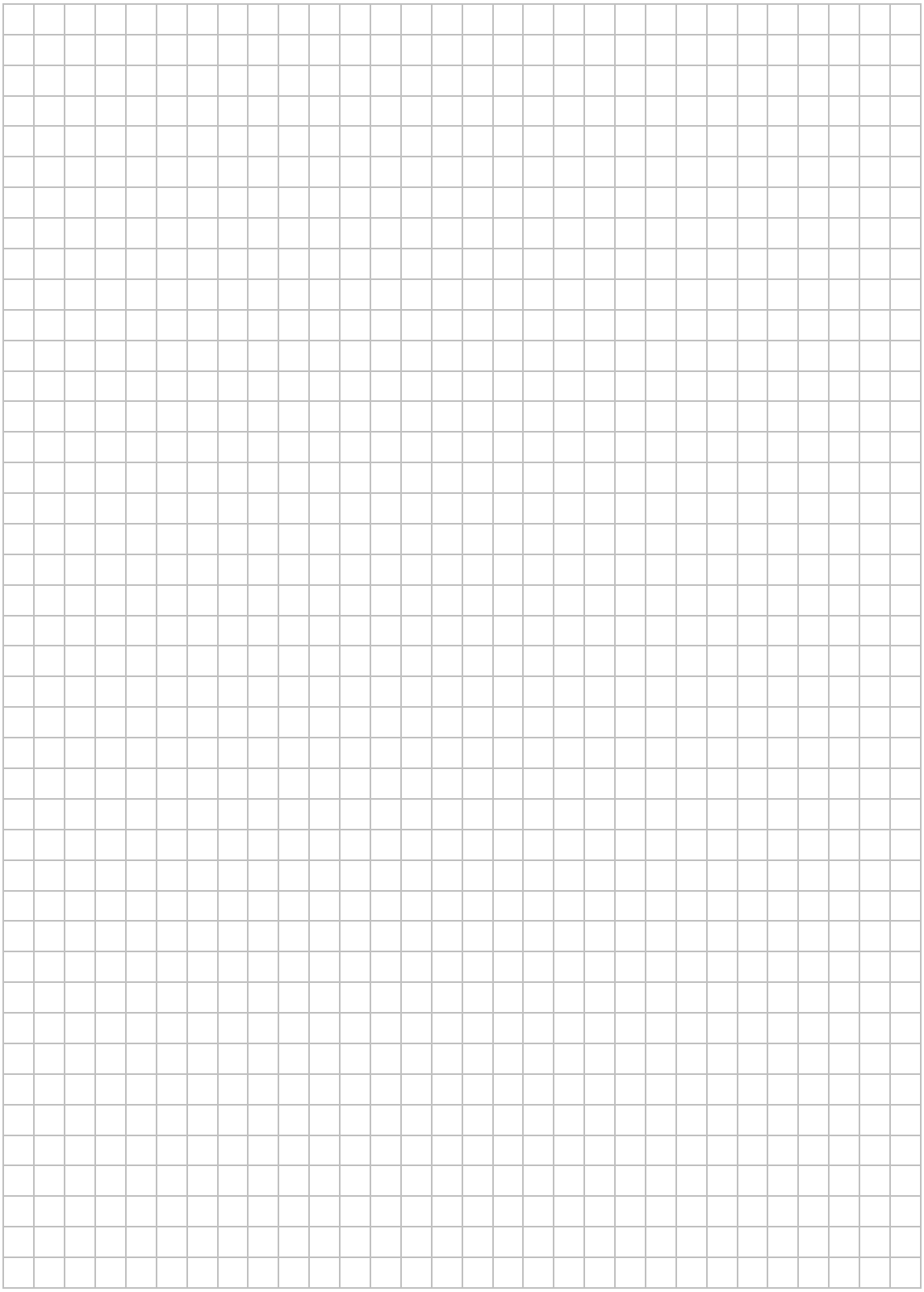
PDC-Emulator
: In Domänen mit NT4 Backup-Domänencontrollern (BDCs) fungiert der PDC-Emulator als Primary Domain-Controller. Darüber hinaus ist er für die Aktualisierung von Kennwortänderungen, für die Durchsetzung von Gruppenrichtlinien und für die Zeitsynchronisation erforderlich.

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.
`netdom query fsmo`	Zeigt an, auf welchen Servern die Betriebsmasterrollen aktiviert sind.

Notizen

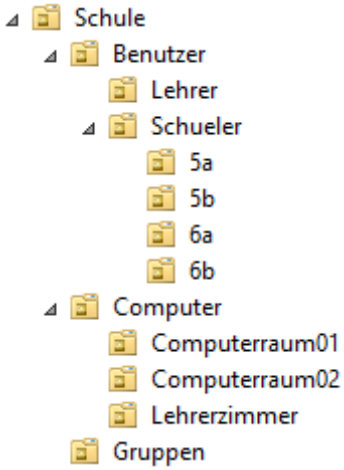
Notizen



AUTOMATISIERTES ANLEGEN VON BENUTZERN

Szenario

Aus der Schülerdatei soll eine Schülerliste exportiert und im Active Directory eingelesen werden. Accounts, die noch nicht existieren, sollen neu angelegt werden, bereits existierende Accounts sollen gegebenenfalls in die richtige Klasse verschoben werden.



Für neue Accounts soll zudem ein Homeverzeichnis angelegt werden.

Einrichten der AD-Struktur mit Skripten

Die AD-Struktur lässt sich gut auf Kommandozeile bearbeiten. Zum Einsatz kommen dabei die Kommandozeilenbefehle dsadd, dsmove, dsquery, etc. Eine Hilfe dazu erhält man mit

```
dsadd /?
```

Anlegen einer Organisationseinheit

```
dsadd ou "Vollständiger Name der OU"
```

```
dsadd ou "ou=5a,ou=Schueler,ou=Benutzer,ou=Schule,dc=alp,dc=local"
```

Anlegen einer Gruppe

```
dsadd group "Vollständiger Name der Gruppe"
```

```
dsadd group "CN=Schueler,ou=Gruppen,ou=Schule,dc=alp,dc=local"
```

Anlegen eines Benutzers

```
dsadd user "Vollständiger Name" <Optionen>
dsadd user "cn=hans,ou=5a,ou=Schueler,ou=Benutzer,ou=Schule,dc=alp,dc=local"
```

Folgende Optionen werden häufig gesetzt:

`-samid hans`	security account manager, Benutzer-ID
`-upn hans`	user prinzipal name, Anmeldename
`-display hans`	Anzeigename
`-pwd 12345`	Passwort
`-mustchpwd no`	must change password
`-canchpwd yes`	can change password
`-pwdneverexpires yes`	password never expires
`-disabled no`	Benutzer nicht deaktiviert
`-hmdrv x:`	Homeverzeichnis
`-hmdir "\\DC\Home\Schueler\hans"`	
`-profile \\DC\Profile\Schueler\hans`	
`-loscr Anmeldeskript.bat`	Anmeldeskript
`-memberof "cn=Schueler,ou=Gruppen,ou=Schule,dc=alp,dc=local"`	
	Es können auch mehrere Gruppen angegeben werden.
`-q`	quiet; es werden nur Fehlermeldungen angezeigt.

Skript zum Anlegen eines Schülers

Die nachfolgende Batchdatei erzeugt einen Schüleraccount in der angegebenen Klasse. Der Schüler erhält ein Homeverzeichnis und Vollzugriff für sein Homeverzeichnis. Falls der Schüleraccount bereits existiert, wir der Schüler ggf. in die richtige Klasse verschoben.

Aufruf

```
erzeuge_Schueler.bat name klasse passwort
erzeuge_Schueler.bat hans 5a 12345
```

Batchdatei erzeuge_Schueler.bat

```
@echo off
rem Erstellen eines Schueleraccounts bzw.
rem Verschieben eines Schuelers in die richtige Klasse
rem Aufruf: erzeuge_Schueler.bat name klasse passwort

set domain=dc=alp,dc=local
set ouSchueler=ou=Schueler,ou=Benutzer,ou=Schule,%dom%
set ouGruppen=ou=Gruppen,ou=Schule,%dom%
set homedir=\\DC\Home\Schueler

rem Anlegen falls der Benutzer nicht existiert

dsquery user -name %1 | find "Schule"
if errorlevel 1 (
dsadd user "CN=%1,OU=%2,%ouSchueler%" ^
   -upn %1 -samid %1 -display %1 ^
   -pwd %3 ^
   -hmdrv x: ^
   -hmdir "%homedir%\%1" ^
   -mustchpwd no -canchpwd yes ^
   -reversiblepwd no -pwdneverexpires yes ^
   -memberof "cn=Schueler,%ouGruppen%" ^
   -disabled no

   md %homedir%\%1
   icacls %homedir%\%1 /grant "%1:(CI)(OI)F"
)

rem Verschieben des Benutzers

for /f %%i in ('dsquery user -name %1') do set cnuser=%%i
dsmove %cnuser% -newparent "OU=%2,%ouSchueler%"
```

Hinweis:

Die Befehle dsadd und dsmove sind üblicherweise sehr lang und müssen in einer Zeile stehen. Auf der Kommandozeile kann mit dem Zeichen ^ ein Befehl über mehrere Zeilen eingegeben werden.

Schülerliste

Textdatei Schuelerliste.txt

HansFeil 5a 12345
KlaraMeier 5a 12345
PeterMix 5a 12345

Die Textdatei Schuelerliste.txt besteht aus den Schülernamen, der Klasse und dem Passwort. Diese Datei wird im Wesentlichen aus dem Schulverwaltungsprogramm generiert, muss aber danach eventuell noch angepasst werden (Anmeldenamen erzeugen, Umlaute entfernen, etc.). Diese Anpassung kann auch automatisiert (z. B. Excel, Perl, Batch-Datei, etc) erfolgen.

Folgende Befehle können beim Generieren der Anmeldenamen hilfreich sein:

Ersetzen von Umlauten

```
set v=Günther
set v=%v:ü=ue%
echo %v%                ergibt:    Guenther
```

Kürzen von Anmeldenamen

```
set v=Guenther
set v=%v:~0,4%
echo %v%                ergibt:    Guen
```

Zusammensetzen von Namen

```
set v=Guen
set n=Baumann
set g=%n%%v%
echo %g%                ergibt:    BaumannGuen
```

Skript zum Anlegen aller Schüler

Das nachfolgende Skript erzeuge_alle_Schueler.bat arbeitet die Textdatei Schuelerliste.txt ab und ruft für jede Zeile das Skript erzeuge_Schueler.bat auf.

Batchdatei erzeuge_alle_Schueler.bat

```
@echo off
for /f "tokens=1,2,3 delims=,; "  %%a in (Schuelerliste.txt) do ^
call erzeuge_Schueler.bat %%a %%b %%c
```

Notizen

Notizen

ZEITSYNCHRONISATION

In einer Windows-Domäne wird die korrekte Uhrzeit automatisch vom Domänencontroller (Domänencontroller mit der FSMO-Rolle PDC-Emulator) auf die Clients übertragen.

Normalerweise sollten an den Zeiteinstellungen keine Änderungen notwendig sein. Bei Problemen, die auf eine abweichende Zeit innerhalb der Domäne zurückzuführen sind, kann folgendes überprüft werden:

- Sind alle Clients und Server in der gleichen Zeitzone?
- Ist die Hardware-Uhr bei den Clients in Ordnung oder kommt es regelmäßig zu Problemen, wenn die Clients längere Zeit nicht in Betrieb waren?
- Ist am Domänencontroller ein funktionierender Zeitserver eingetragen?

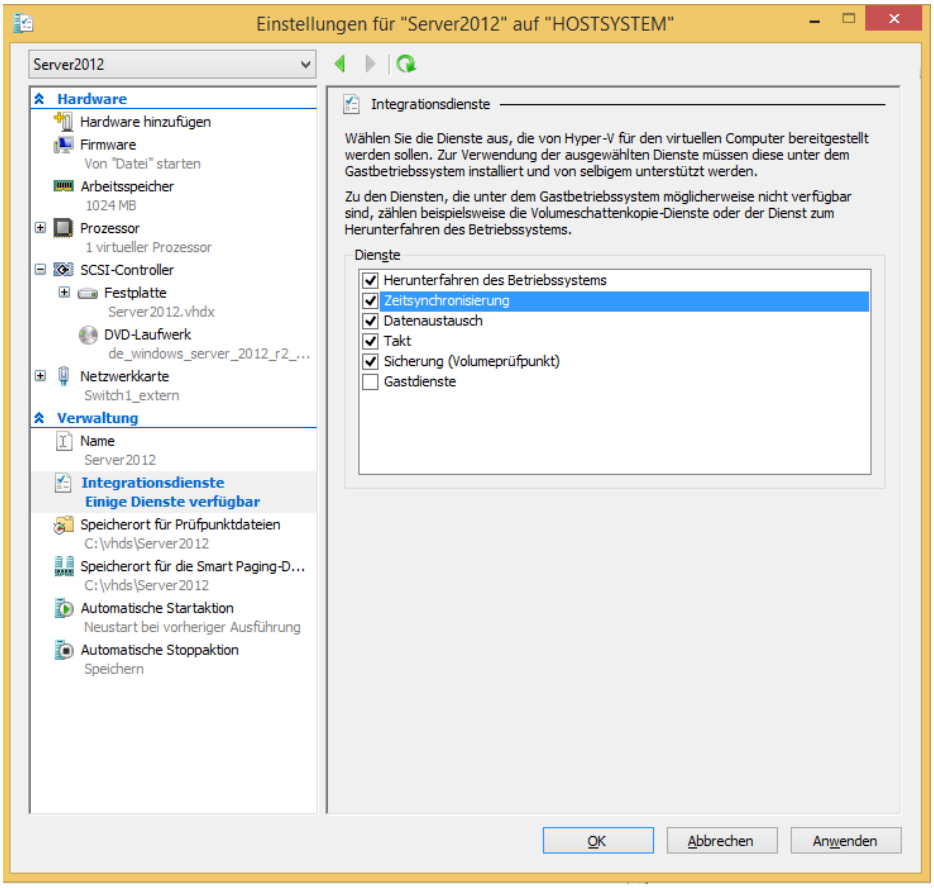
Aufgaben

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 gegebenenfalls am Domänencontroller den Zeitserver ptbtime2.ptb.de als Standard-Zeitserver ein.

Hinweise

Virtualisierte Umgebungen

Läuft der Domänencontroller in einer virtualisierten Umgebung (z. B. Hyper-V), dann wird üblicherweise die Zeit des Host-PC übernommen.



Überprüfung des Zeitserverdienstes

`w32tm /tz`	Zeigt die aktuelle Zeitzone an.
`w32tm /query /source`	Zeigt den aktuell genutzten Zeitserver an.
`w32tm /config /manualpeerlist:ptbtime2.ptb.de /syncfromflags:manual`	Legt den Zeitserver fest, der zukünftig verwendet werden soll.
`w32tm /config /update`	Die Konfigurationsänderung wird angewandt.
`w32tm /resync`	Synchronisiert die Uhrzeit mit dem Zeitserver
`net stop w32time`	Der Zeitserverdienst wird beendet.
`net start w32time`	Der Zeitserverdienst wird gestartet.
`w32tm /monitor`	Anzeige des Zeitservers in der Domäne und der externen Zeitquelle

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.

Festlegung 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.

Anfrage im symmetrischen Modus:

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

Anfrage im Client-Modus:

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

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.

Notizen