



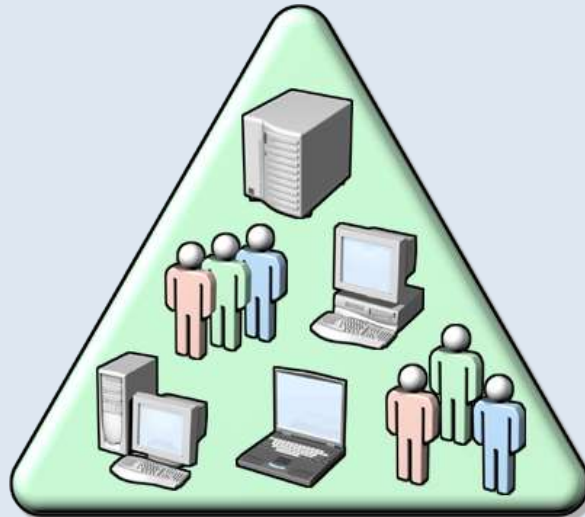
Active Directory

- Einführung
- Betriebsmaster
- Weitere Begriffe
- Installation
- Kerberos / DNS
- Sites & Replikation
- RODC
- Best Practice
- AD-Konten
- Policies / GPOs
- Dynamic Access Control
- Vertrauensstellungen
- AD wiederherstellen
- PSO
- Weiteres

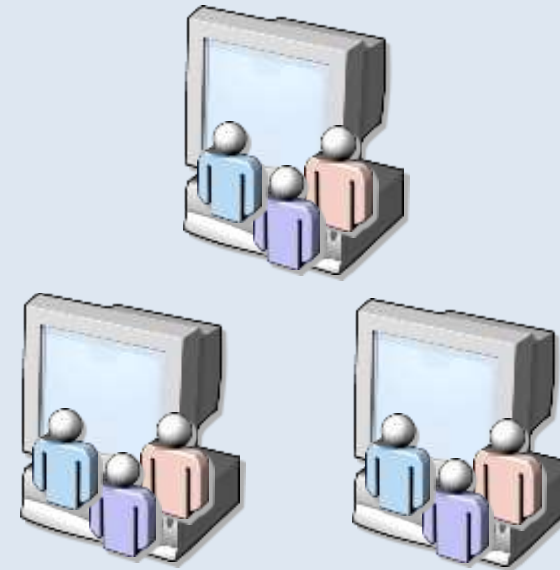
EINFÜHRUNG

Ein Verzeichnisdienst ist sowohl die Verzeichnisinformationsquelle als auch der Dienst, der die Informationen verfügbar und nutzbar macht

Zentrale Verwaltung



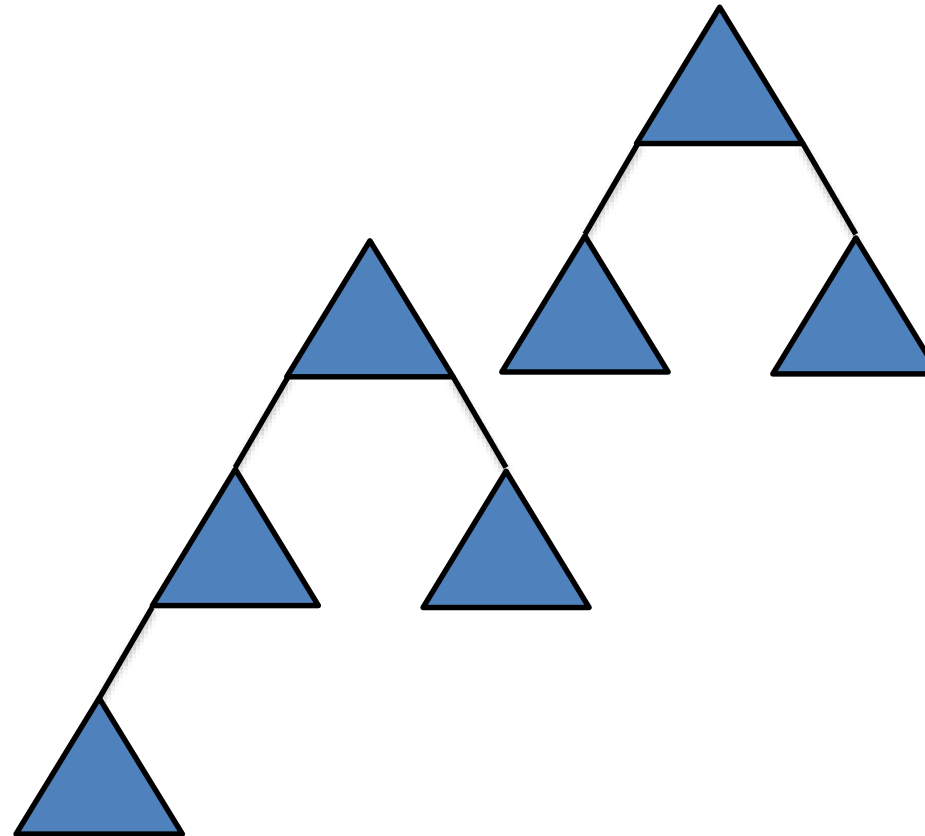
Verstreute Verwaltung



- Verzeichnisdienst von Microsoft
- Speichert Objekte wie z.B.
 - Computer
 - Benutzer
 - Gruppen
- Speichert Berechtigungen
- Hauptkomponenten
 - LDAP (Lightweight Directory Access Protocol)
 - Kerberos
 - DNS

- Stützt sich auf eine Datenbank
 - Jet-System
 - relational
 - transaktionsorientiert
 - ntds.dit
 - Hierarchisch gegliedert
 - Schema als „Bauplan“
 - Klassen
 - Attribute
 - Benötigt min. einen Domänencontroller
- | | |
|------------------|------------|
| • Attribute | • Klassen |
| • objectSID | • User |
| • sAMAccountName | • Group |
| • location | • Computer |
| • manager | • Site |
| • department | |

- Struktur
- Begriffe:
 - Gesamtstruktur (*Forest*)
 - Struktur (*Tree*)
 - Domäne (*Domain/Leaf*)
 - Standort (*Site*)



Domänen sind logische Verzeichniskomponenten, die zur Gruppierung und Verwaltung der AD DS-Objekte in einer Organisation verwendet werden

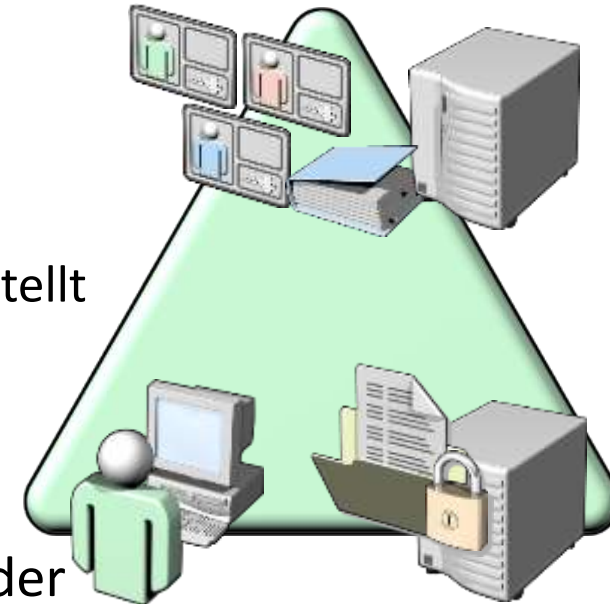


Woodgrove
Bank.com

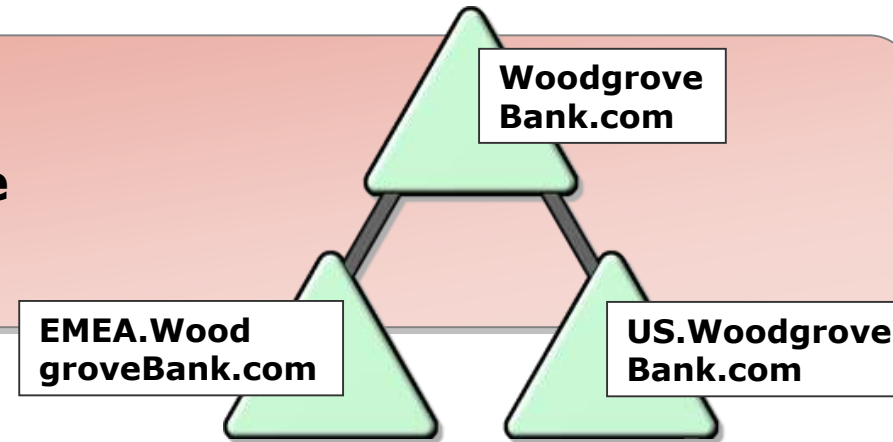
Domänen sind:

- Eine administrative Grenze zur Anwendung von Richtlinien auf Objektgruppen
- Eine Replikationsgrenze für die Replikation von Daten bei Domänencontrollern
- Eine Authentifizierungs- und Autorisierungsgrenze, die die Möglichkeit bietet, den Zugriff auf Ressourcen zu beschränken

- Besteht aus einem oder mehreren Domänencontrollern
- Alle Domänencontroller replizieren den Domänennamenskontext (Domain NC).
 - Die Domäne stellt den Kontext dar, innerhalb dessen Benutzer, Gruppen, Computer usw. erstellt werden.
 - "Replikationsgrenze"
- Vertrauenswürdige Identitätsquelle: Jeder Domänencontroller kann jede Anmeldung in der Domäne authentifizieren.
- Die Domäne ist der *maximale* Bereich (Grenze) für bestimmte Verwaltungsrichtlinien.
 - Kennwort
 - Sperrung



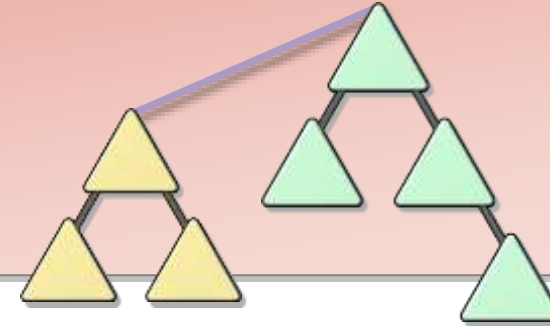
Eine Domänenstruktur ist eine aus Domänen bestehende Hierarchie in den AD DS



Alle Domänen in der Domänenstruktur:

- **Verfügen über einen zusammenhängenden Namespace mit der übergeordneten Domäne**
- **Können zusätzliche, dem Namespace hinzugefügte untergeordnete Domänen haben**
- **Haben eine bidirektionale transitive Vertrauensstellung mit anderen Domänen in der Struktur**

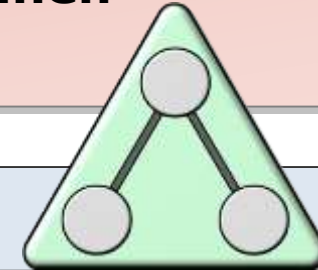
Eine Gesamtstruktur ist eine Sammlung aus einer oder mehreren Domänenstrukturen



Gesamtstrukturen:

- **Haben das gleiche Schema**
- **Haben die gleiche Konfigurationspartition**
- **Haben den gleichen globalen Katalog, um Suchläufe zu ermöglichen**
- **Aktivieren Vertrauensstellungen zwischen allen Domänen in der Gesamtstruktur**
- **Haben die gleiche Organisations-Admins- und Schema-Admins-Gruppe**

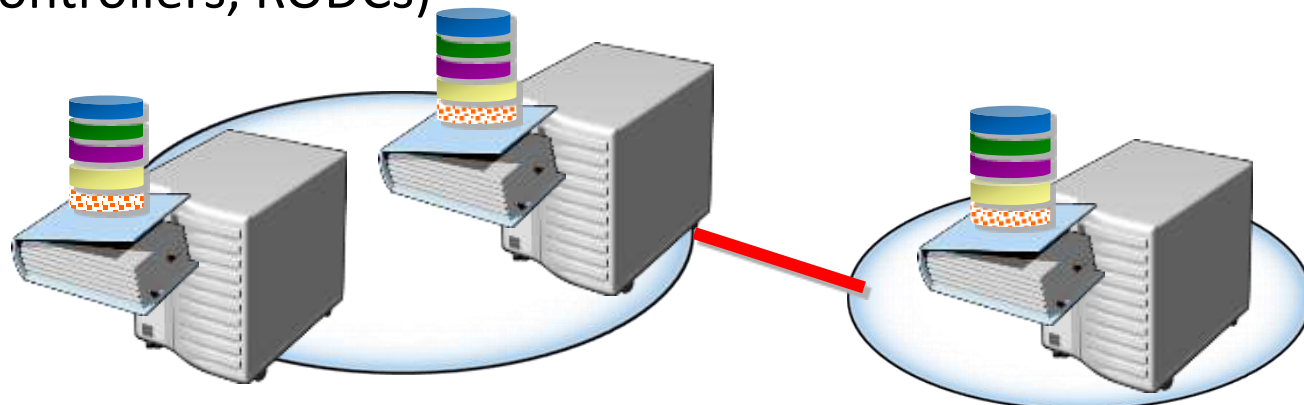
OEs (OUs) sind Active Directory-Container, die Benutzer, Gruppen, Computer und andere OEs enthalten können



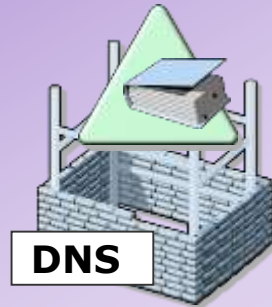
OUs werden verwendet:

- **Zum hierarchischen und logischen Darstellen Ihres Unternehmens**
- **Zum Verwalten einer Sammlung von Objekten auf konsistente Art und Weise**
- **Zum Delegieren von Berechtigungen für die Verwaltung von Objektgruppen**
- **Zum Anwenden von Richtlinien**

- Server, die die AD DS-Rolle ausführen
 - Hosten die Active Directory-Datenbank (**NTDS.DIT**) und **SYSVOL**
 - Zwischen Domänencontrollern repliziert
 - Kerberos-KDC-Dienst (Key Distribution Center, Schlüsselverteilungscenter): Authentifizierung
 - Andere Active Directory-Dienste
- Bewährte Methoden
 - Verfügbar: mindestens zwei in einer Domäne
 - Sicher: Server Core, schreibgeschützte Domänencontroller (Read-Only Domain Controllers, RODCs)



- **AD DS erfordert eine DNS-Infrastruktur**

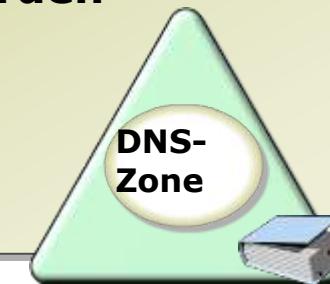


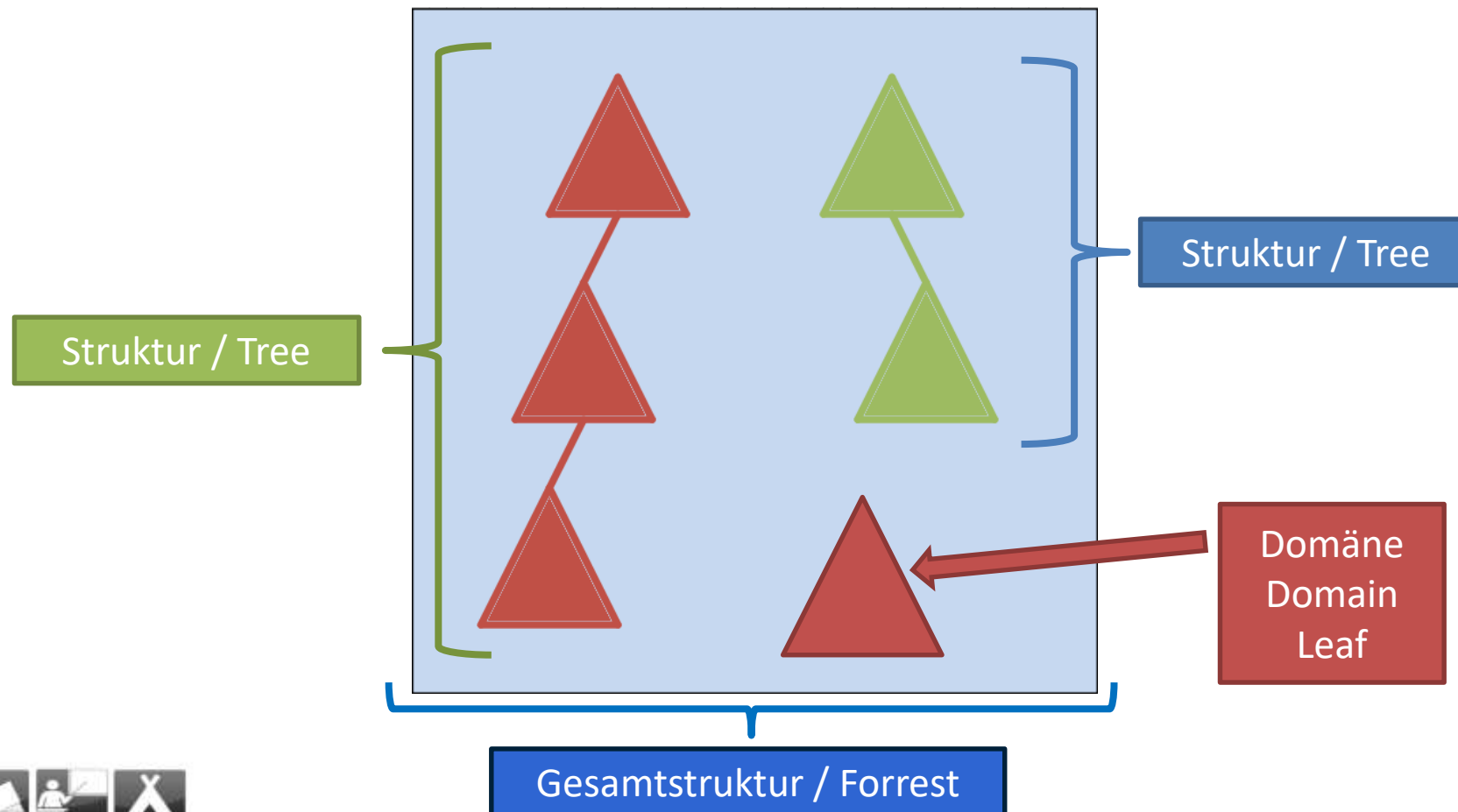
- **AD DS-Domännennamen müssen DNS-Domännennamen sein**



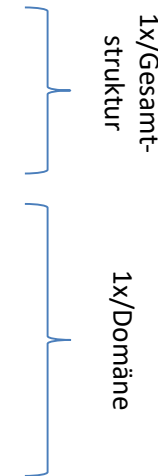
- **AD DS-Domänencontrollerdatensätze müssen im DNS registriert sein, damit andere Domänencontroller und Clientcomputer die Domänencontroller finden können**

- **DNS-Zonen können in AD DS als integrierte Active Directory-Zonen gespeichert werden**

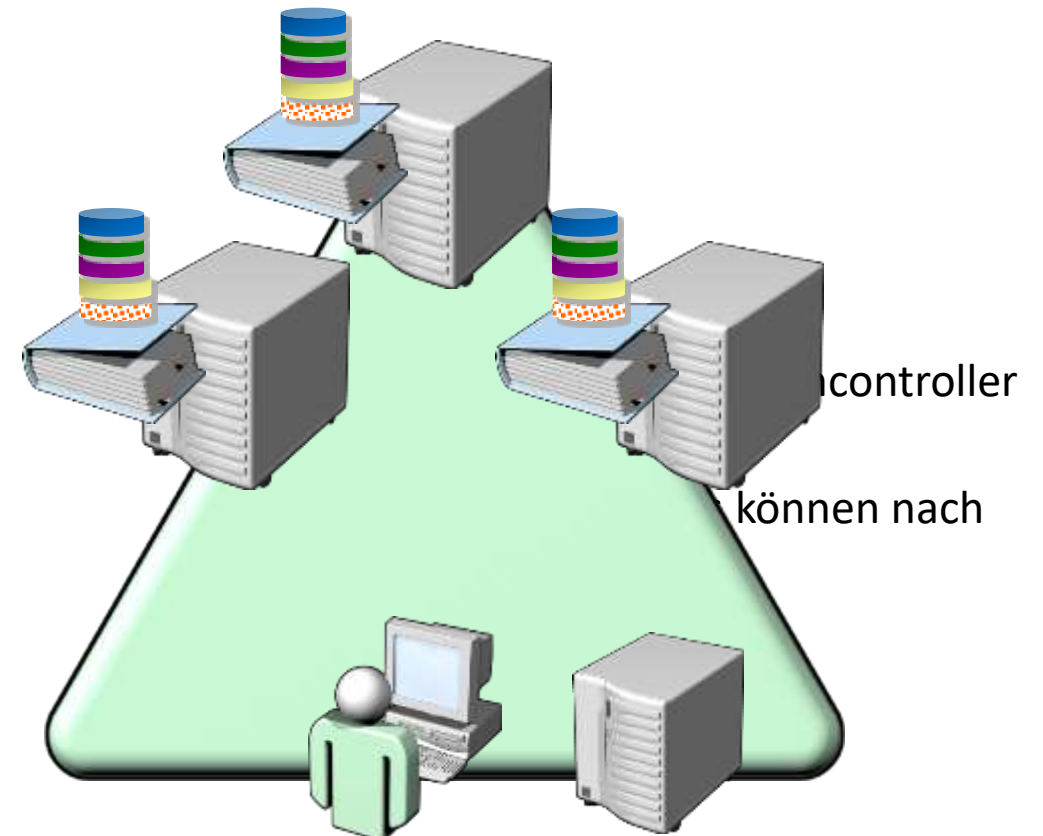




- Funktionsebenen
 - Domänenfunktionsebene
 - Gesamtstrukturfunktionsebene
- Betriebsmaster (FSMO)
 - Schema-Master (Schema-Änderungen)
 - Domain-Name-Master (Namensraum b. neuen Domänen)
 - Infrastruktur-Master (domänenübergreifend)
 - RID-Master (SID-Generierung)
 - PDC-Emulator (Kennwortänderungen, Zeit, ...)



- Domänenfunktionsebenen
- Gesamtstrukturfunktionsebenen
- Neue Funktionen erfordern, dass *Domänencontroller* auf einer bestimmten Windows-Version ausgeführt werden.
 - Windows Server 2003
 - Windows Server 2008
 - Windows Server 2008 R2
 - Windows Server 2012
- Funktionsebene kann nicht heraufgestuft
frühere Windows-Versionen ausführen
- Domänencontroller mit früheren Versionen
dem Heraufstufen
der Funktionsebene nicht
hinzugefügt werden.



BETRIEBSMASTER / FSMO-ROLLEN

- Anwendung und Verwaltung der GPO
 - Kennwortänderungen
 - Externe Vertrauensstellungen
 - Zeitserver
-
- `dsquery server -hasfsmo pdc`
 - `PS: Get-ADDomain | select PDCEmulator`

- RID: Relative Identifiers
- SID neuer Objekte werden aus Domänen-Kennung und RID erstellt
- RID-Master weist DCs RID-Pools zu
- Anfänglich: 500 RID pro DC; bei 250 wird nachgefordert
- RID nicht verfügbar? Keine neuen Objekte!
- `dsquery server -hasfsmo rid`
- PS: `Get-ADDomain | select RIDMaster`

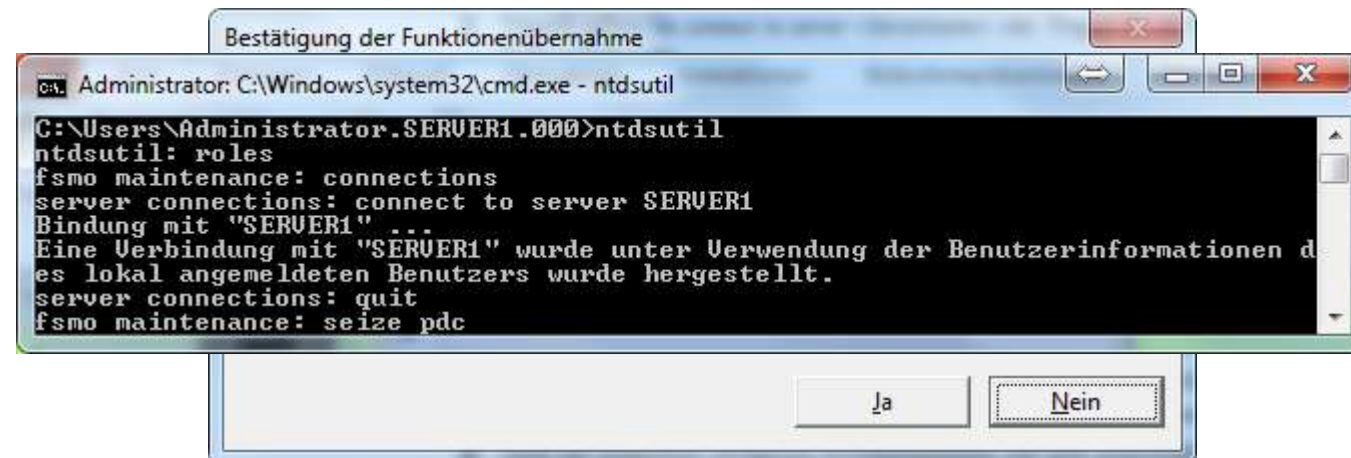
- Bei nur einer Domäne: unwichtig
 - Berechtigungen von Usern anderer Domänen innerhalb der Gesamtstruktur
 - Dient als *Cache*, damit nicht alle Domänen abgefragt werden müssen
-
- `dsquery server -hasfsmo infr`
 - `Get-ADDomain | select InfrastructureMaster`

- Schema = Struktur des Verzeichnisses
 - Schema ist erweiterbar (z.B. für Exchange)
 - Zuständig: Schemamaster
 - Ausfall nicht kritisch, solange keine Änderungen erfolgen sollen
-
- `dsquery server -hasfsmo schema`
 - PS: `Get-ADForest | select SchemaMaster`

- Verwaltet Domänen und Strukturen innerhalb der Gesamtstruktur
 - Nötig für Erstellung neuer Domänen
 - Sonst keine Aufgabe
-
- `dsquery server -hasfsmo name`
 - PS: `Get-ADForest | select DomainNamingMaster`

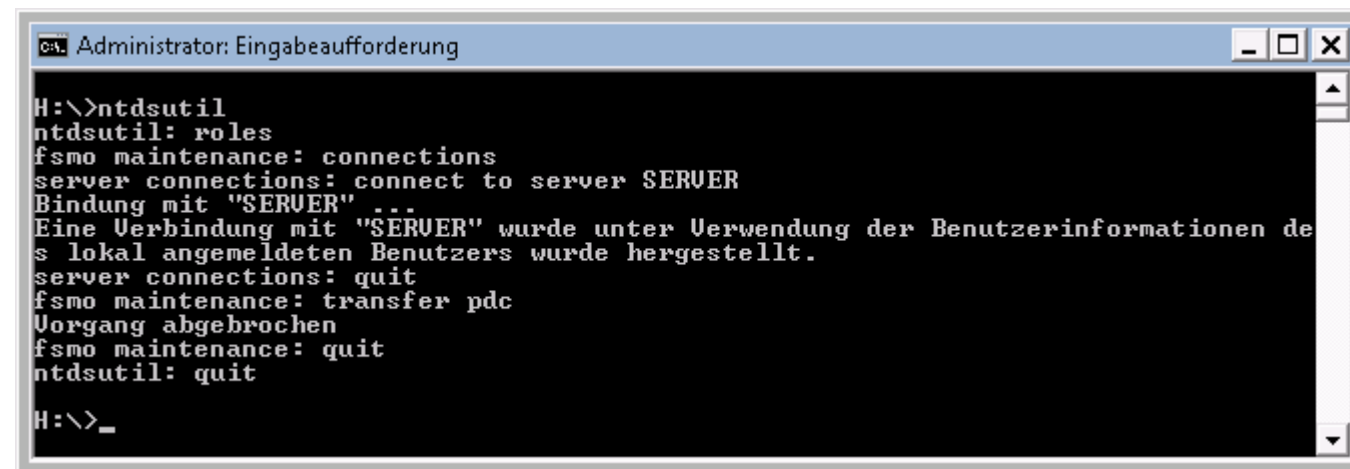
- Ab 2 Domänen: Infrastrukturmater und GC trennen
 - Domänennamenmaster und Schemamaster zusammen mit GC
 - PDC-Emulator und RID-Master gemeinsam auf einen DC mit GC
-
- `netdom query fsmo`
 - PS: `Get-ADForest | select SchemaMaster, DomainNamingMaster`
 - PS: `Get-ADDomain | select PDCEmulator, RIDMaster, InfrastructureMaster`

- Optimal: Sauber übertragen
- Bei dauerhaftem Ausfall: Übernahme der Rollen möglich
- Wichtig: Defekte Maschine nie wieder an's Netz!



- NTDSUTIL starten

- ROLES -> "*fsmo maintenance*„
- CONNECTIONS
- Connect to Server <Servername>
- Quit -> „*fsmo maintenance*“
- Transfer schema master
- Transfer domain naming master (gilt bis einschließlich Windows Server 2003!)
- Transfer naming master (gilt ab Windows Server 2008!)
- Transfer RID master
- Transfer PDC
- Transfer infrastructure master
- Quit
- Quit



```
H:\>ntdsutil
ntdsutil: roles
fsmo maintenance: connections
server connections: connect to server SERVER
Bindung mit "SERVER" ...
Eine Verbindung mit "SERVER" wurde unter Verwendung der Benutzerinformationen de
s lokal angemeldeten Benutzers wurde hergestellt.
server connections: quit
fsmo maintenance: transfer pdc
Vorgang abgebrochen
fsmo maintenance: quit
ntdsutil: quit
H:\>_
```

- Transferring Command syntax:

```
Move-ADDirectoryServerOperationMasterRole  
-Identity "Target-DC" -  
OperationMasterRole PDCEmulator
```

OR

```
Move-ADDirectoryServerOperationMasterRole  
-Identity "Target-DC" -OperationMasterRole 0
```

Seizing Command syntax:

```
Move-ADDirectoryServerOperationMasterRole  
-Identity "Target-DC"  
-OperationMasterRole PDCEmulator -Force
```

OR

```
Move-ADDirectoryServerOperationMasterRole  
-Identity "Target-DC" -OperationMasterRole 0  
-Force
```

- Rollen-Namen / Nummern:

Role Name	Number
PDCEmulator	0
RIDMaster	1
InfrastructureMaster	2
SchemaMaster	3
DomainNamingMaster	4

WEITERE BEGRIFFE UND ZUSAMMENHÄNGE

- Multi-Master-Replikation
- Globaler Katalog (GC)
- Read-Only-DC
- Container & Organisationseinheit (OU)
- AD-Standorte (Sites)

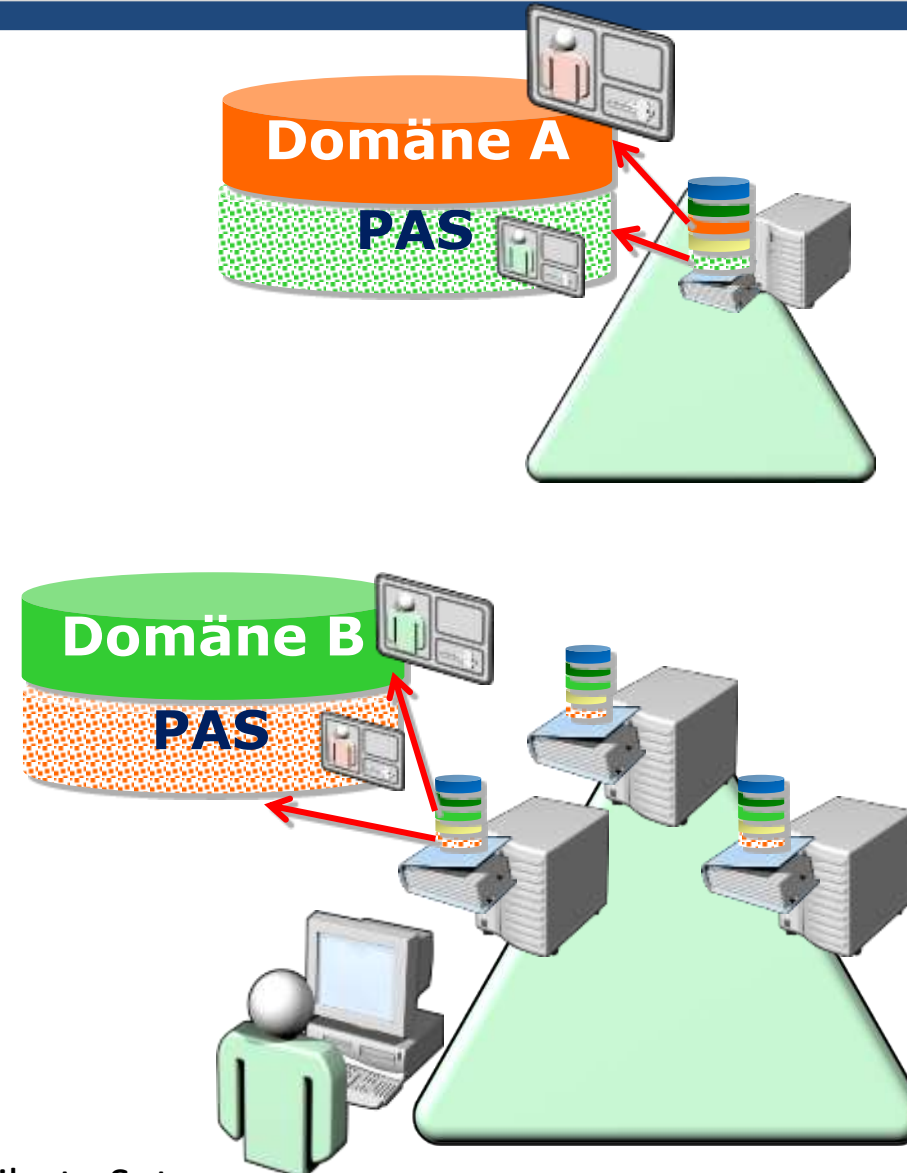
Globale Katalogserver sind Domänencontroller, in denen auch eine Kopie des globalen Katalogs gespeichert wird



Der globale Katalog:

- **Enthält eine Kopie aller AD DS-Objekte einer Gesamtstruktur, die nur einige der Attribute für jedes Objekt in der Gesamtstruktur enthält**
- **Verbessert die Effizienz von Objektsuchläufen, indem unnötige Verweise auf Domänencontrollern vermieden werden**
- **Ist erforderlich für Benutzer, die sich bei einer Domäne anmelden**

- Teilattributsatz oder globaler Katalog
- Enthält alle Objekte in allen Domänen in der Gesamtstruktur
- Enthält nur ausgewählte Attribute
- Eine Art Index
- Kann von jeder Domäne aus durchsucht werden
- Sehr wichtig für viele Anwendungen



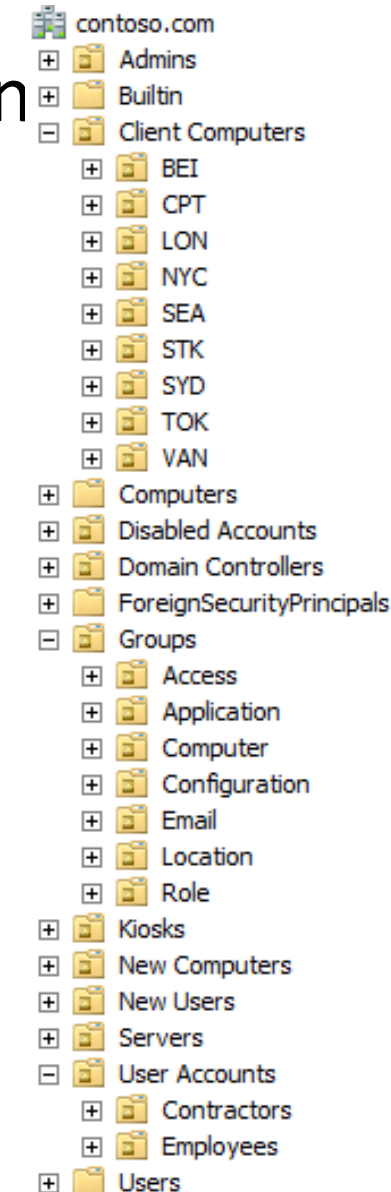
PAS: Partial Attribute Set

- Kann parallel auf mehreren DCs laufen
- Enthält Index aller Domänen
- Min. 1x pro Standort, besser mehr
- Mehr GC = Mehr Replikationen = Traffic
- Kein GC verfügbar => Keine Anmeldung möglich!

- Werden zur logischen und physischen Organisation genutzt
- Lassen sich „schachteln“
- Ous u.a. für Policies (GPO)

funktion

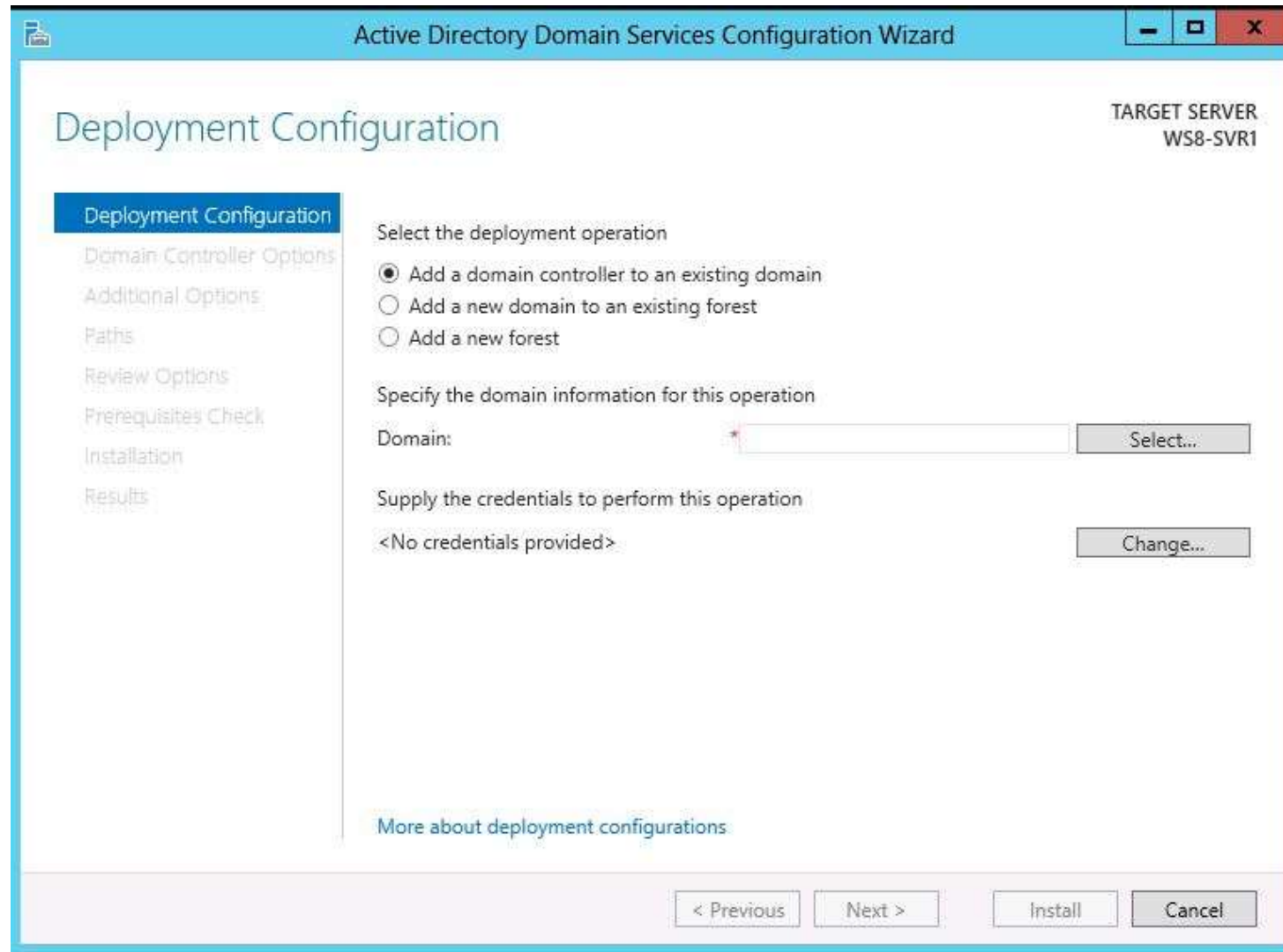
Verwaltung im



- Zeitdifferenz (Server/Clients) ungünstig
 - Kennwörter werden nicht übertragen
 - Kerberos arbeitet mit Tickets
- PDC-Emulator verteilt Zeit
- `w32tm /config /syncfromflags:manual
/manualpeerlist:ptbtime1.ptb.de /update
/reliable:YES`
- `w32tm /resync`

INSTALLATION AD / DC

- Bestehende Domäne evtl. anpassen (ADPrep)
 - `adprep /forestprep`
 - `adprep /domainprep /gpprep`
 - Adprep.exe auf DVD:\Support\Adprep
 - Auf Schemamaster ausführen!
 - Alternativ während Promotions-Prozess durch neuen Servermanager
- IP-Adresse und DNS
- Rolle hinzufügen
 - Seit Server 2012 kein `dcpromo` mehr!



Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
WS8-SVR1

Deployment Configuration

Domain Controller Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select the deployment operation

- ☒ Add a domain controller to an existing domain
- ☐ Add a new domain to an existing forest
- ☐ Add a new forest

Specify the domain information for this operation

Domain:

Supply the credentials to perform this operation

<No credentials provided>

[More about deployment configurations](#)

< Previous Next > Install Cancel

- Hostname & IP-Adressen
- Rolle „AD DS“ über Servermanager hinzufügen
- „Server zum Domänencontroller
heraufstufen“
- Neue Gesamtstruktur erstellen
- Namen frei wählen nach Schema
`präfix.suffix`
- Weitere Server der Domäne hinzufügen

- `dcpromo /unattend:"D:\answerfile.txt"`

[DCINSTALL]

UserName=<The administrative account in the domain of the new domain controller>

UserDomain=<The name of the domain of the new domain controller>

Password=<The password for the UserName account>

SiteName=<The name of the AD DS site in which this domain controller will reside>

This site must be created in advance in the Dssites.msc snap-in.

ReplicaOrNewDomain=replica

ReplicaDomainDNSName=<The fully qualified domain name (FQDN) of the domain in which you want to add an additional domain controller>

DatabasePath="<The path of a folder on a local volume>"

LogPath="<The path of a folder on a local volume>"

SYSVOLPath="<The path of a folder on a local volume>"

InstallDNS=yes

ConfirmGC=yes

SafeModeAdminPassword=<The password for an offline administrator account>

RebootOnCompletion=yes

- Kann parallel auf mehreren DCs laufen
- Enthält Index aller Domänen
- Min. 1x pro Standort, besser mehr
- Mehr GC = Mehr Replikationen = Traffic
- Kein GC verfügbar => Keine Anmeldung möglich!

- Installieren Sie die AD DS auf SRV1 und SRV2
- Verschieben Sie den Infrastruktur-Master von SRV1 auf SRV2
- Aktivieren (oder deaktivieren) Sie den GlobalCatalog auf SRV2



- Kennwörter nicht übertragen
- Authentifizierung läuft über *Tickets*
- Ticket wird bei Anmeldung am PC und damit AD ausgestellt
- Dienste prüfen nur noch Gültigkeit des Tickets
 - „Ticket Granting Ticket“ (TGT)
 - Session Key zur Verschlüsselung (symmetrisch)

AD-STANDORTE UND -REPLIKATION

- Was sind Standorte?
- Default-First-Site-Name
- Intra-Site / Inter-Site
- Standorte verwalten

⇒ Testsysteme

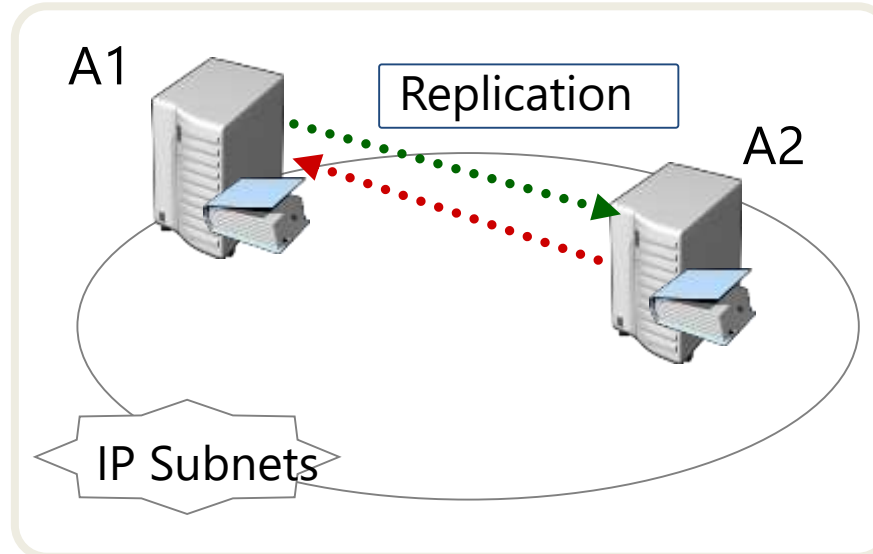
⇒ Subnets

⇒ Standorte

⇒ Standortverknüpfung

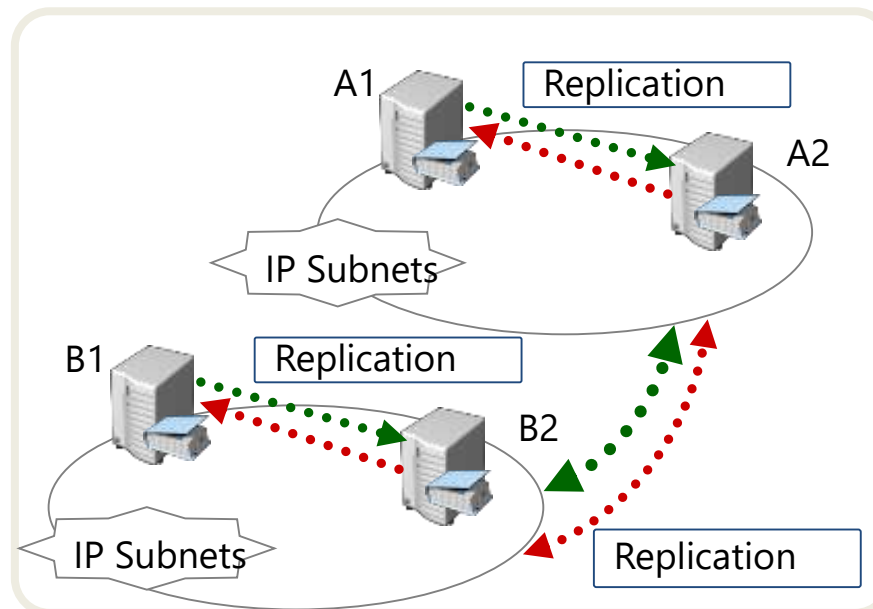
⇒ DefaultIPSiteLink

⇒ Zeitplan / Kosten



Replication within sites:

- Assumes fast, cheap and highly reliable network links
- Does not compress traffic
- Uses a change notification mechanism

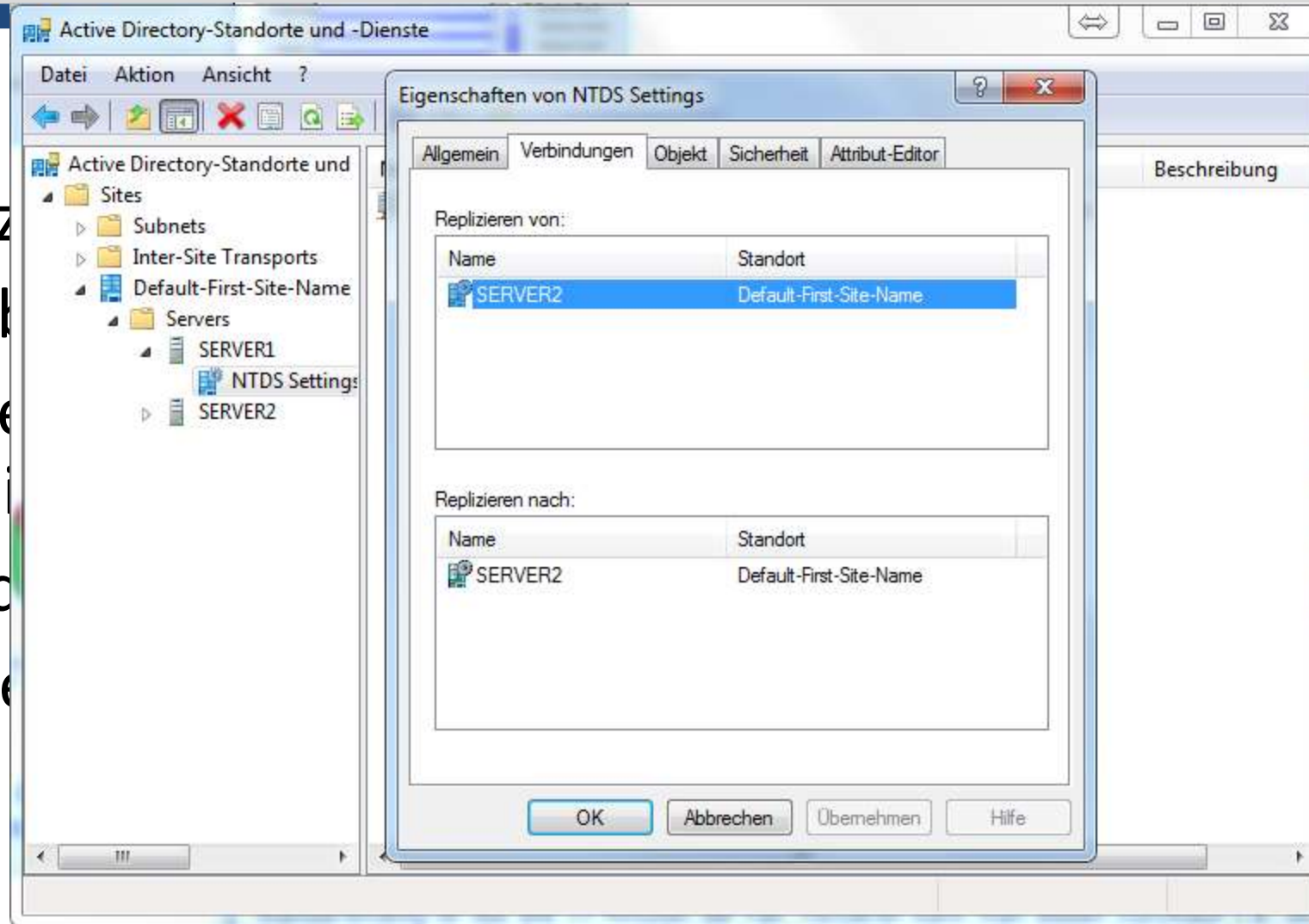


Replication between sites:

- Assumes higher cost, limited bandwidth and unreliable network links
- Ability to compress replication between sites
- Occurs on a configured schedule

- Bridgeheadserver ist für Replikation zu anderen Standorten „Anlaufstelle“
- Wird automatisch bestimmt (Server mit niedrigster `objectGUID`)
- Kann manuell verändert werden
- Bei mehreren Domänen in GS: BGH zusammen mit GC!

- Default:
 - GC repliz
 - Kann in k
 - Am selbe
 - 15min b
 - „Dringend
- ⇒ Testsystem



mäne

orten:

- **Neue PowerShell-Cmdlets:**

- `New-ADReplicationSite / Get-...`
- `New-ADReplicationSiteLink / Get-...`
- `New-ADReplicationSiteLinkBridge / Get-...`
- `New-ADReplicationSubnet / Get-...`
- `Get-ADReplicationConnection`
- `Get-ADReplicationFailure`
- `Get-ADReplicationPartnerMetadata`
- ...

- RepAdmin.exe examples
 - **repadmin /showrepl** Lon-dc1.adatum.com
 - **repadmin /showconn** Lon-dc1 adatum.com
 - **repadmin /showobjmeta** Lon-dc1 "cn=Linda Miller,ou=..."
 - **repadmin /kcc**
 - **repadmin /replicate** Tor-dc1 Lon-dc1 dc=adatum,dc=com
 - **repadmin /syncall** Lon-dc1.adatum.com **/A /e**
- DCDiag /test:*testName*
 - **FrsEvent** or **DFSREvent**
 - **Intersite**
 - **KccEvent**
 - **Replications**
 - **Topology**

- SYSVOL-Ordner wird zwischen DCs repliziert
- Enthält z.B. Skripte und GPOs
 - File Replication Service (Server 2003 und älter)
 - Distributed File System (ab Server 2008)
- Um von FRS auf DFS umzustellen:
 - Funktionsebene min. Server 2008
 - dfsrmig.exe

- Richten Sie 2 AD-Sites samt Subnetzen ein
- Legen Sie einen Inter-Site-Link an
- Verschieben Sie SRV2 zu einem der neuen Standorte



READ-ONLY DC

- Keine Änderungen
- Leitet Änderungen an reguläre DCs weiter
- RODC speichert keine / nur festgelegte Kennwörter zwischen
- Schützt bei Diebstahl / Kompromitierung
- Einen Domänen-Server zum RODC heraufstufen
- Replikations-Richtlinien steuern (Am RODC-Objekt oder am Benutzer)
- Anzeige, welche Kennwörter gespeichert sind („Erweitert“)

NYC-RODC Properties

General Operating System Member Of Delegation

Password Replication Policy Location Managed By Dial-in

This is a Read-only Domain Controller (RODC). An RODC stores users and computers passwords according to the policy below. Only passwords for accounts that are in the Allow groups and not in the Deny groups can be replicated to the RODC.

Groups, users and computers:

Name	Active Directory Dom...	Setting
Account Operators	Adatum.com/Builtin	Deny
Administrators	Adatum.com/Builtin	Deny
Allowed RODC Password Repli...	Adatum.com/Users	Allow
Backup Operators	Adatum.com/Builtin	Deny
Denied RODC Password Repli...	Adatum.com/Users	Deny
Server Operators	Adatum.com/Builtin	Deny

< ||| >

Advanced... Add... Remove

OK Cancel Apply Help

- Installieren Sie einen RODC auf SRV3
- Machen Sie sich mit den diversen Einstellungen vertraut



BEST PRACTICE

- Bestandteil des Server-Managers
- Die meisten Rollen haben eigenen Best Practice Analyzer

- min. 2 DC
- min. 1 GC
- Statische Adressen an DCs sinnvoll
- DNS

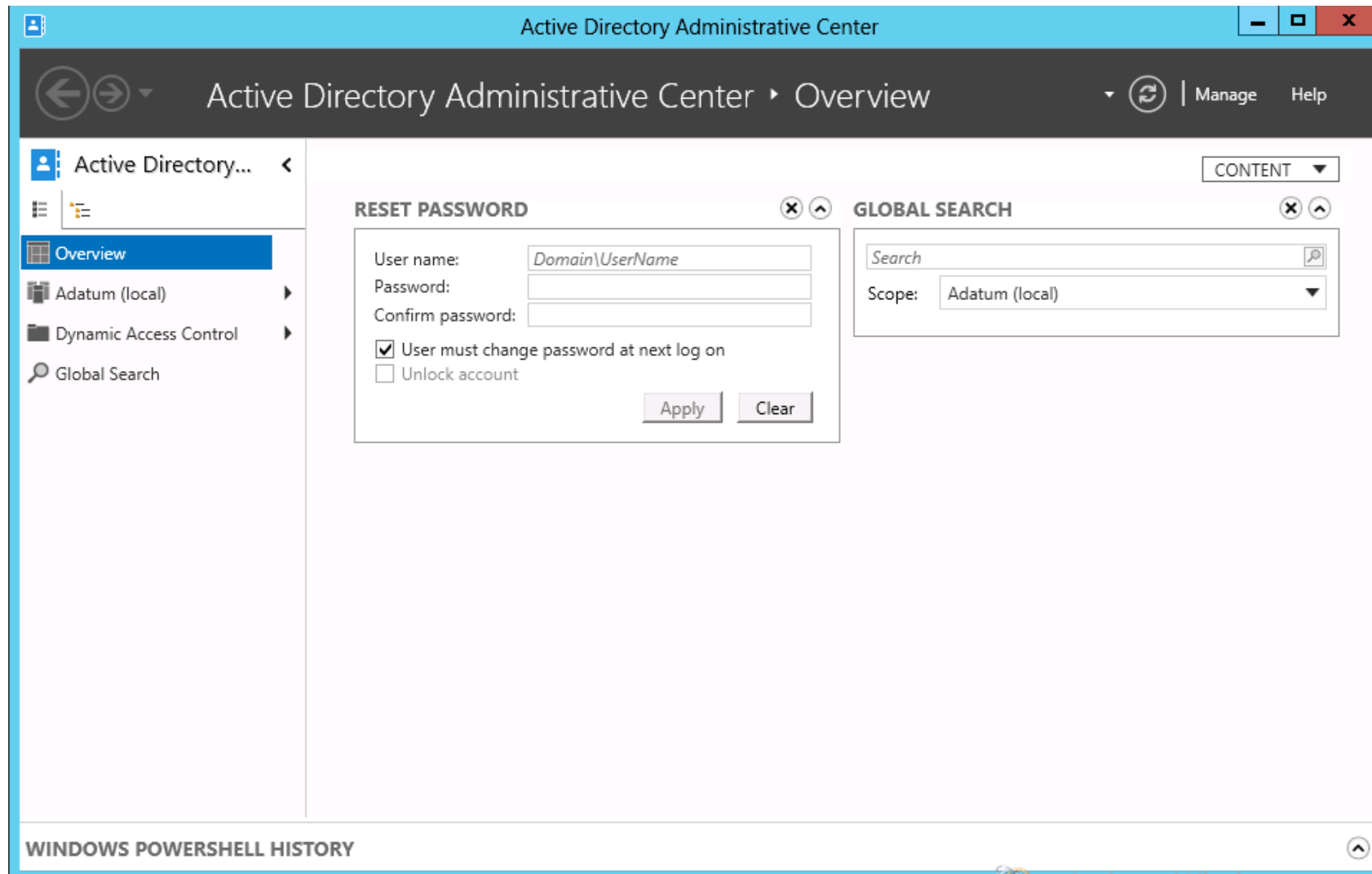
- AD und Hyper-V in gemeinsamer Parent-Partition
- AD und SQL Server auf einem Host

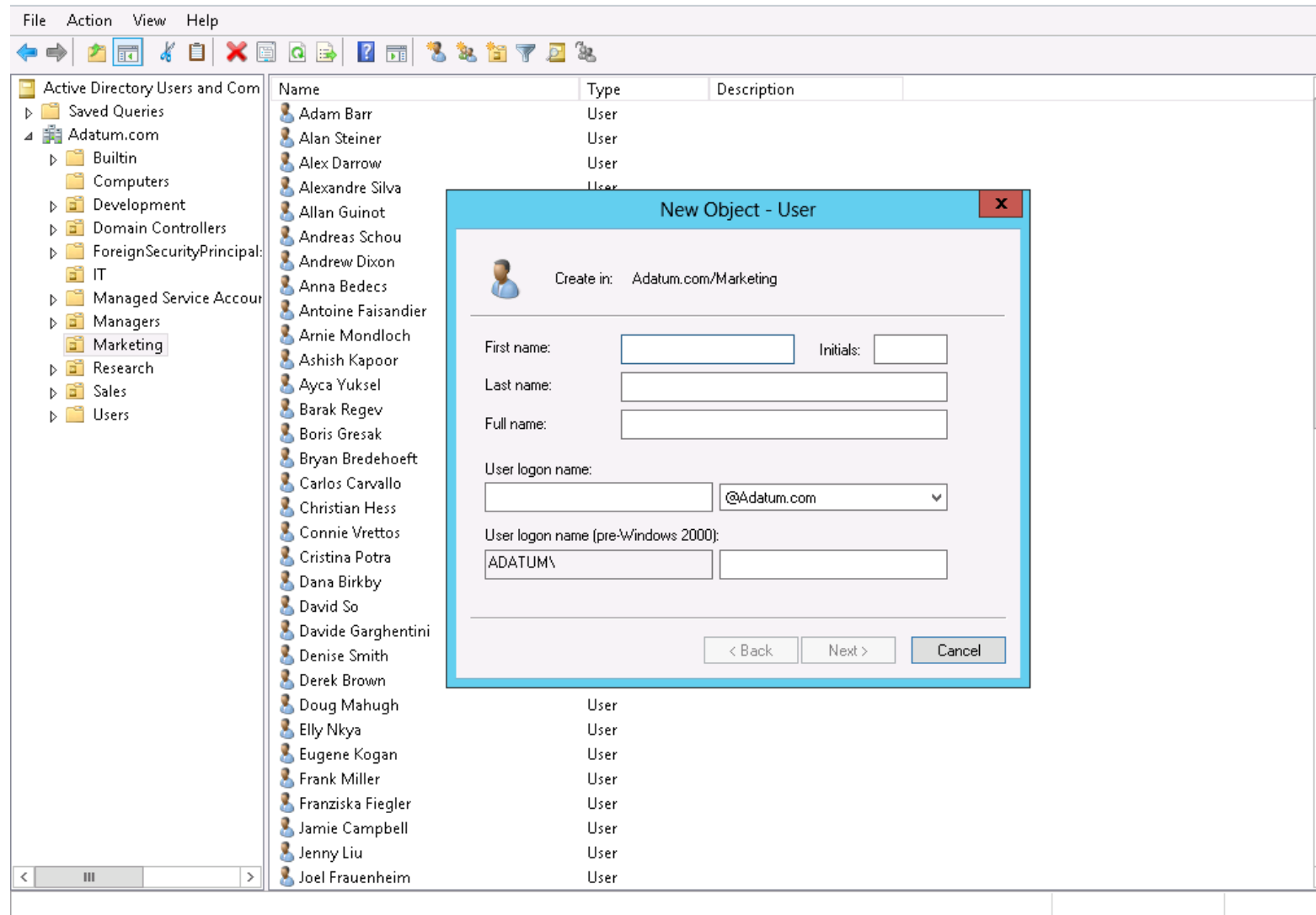
- Benutzen Sie den Best Practice Analyzer im Server Manager
- Machen Sie sich mit den Ergebnissen und Empfehlungen vertraut



AD-KONTEN UND -OBJEKTE

- Benutzer, Gruppen und Computer
- SID
- Container und OUs
- Delegation





- Für Servergespeicherte Profile: Profilpfad am AD-Konto eintragen
(mit %username%) → wird mitkopiert!
- Alternativ: Per PS-Skript
- Standardprofil: Referenz-Profil erstellen und nach
„\\SERVER\Netlogon\Default User.V2“ kopieren
(wird verwendet, wenn User kein servergespeichertes und kein lokales Profil hat)

Adam Barr Properties

Published Certificates	Member Of	Password Replication	Dial-in	Object
Security	Environment	Sessions	Remote control	
Remote Desktop Services Profile		COM+	Attribute Editor	
General	Address	Account	Profile	Telephones
Organization				

User profile

Profile path:

Logon script:

Home folder

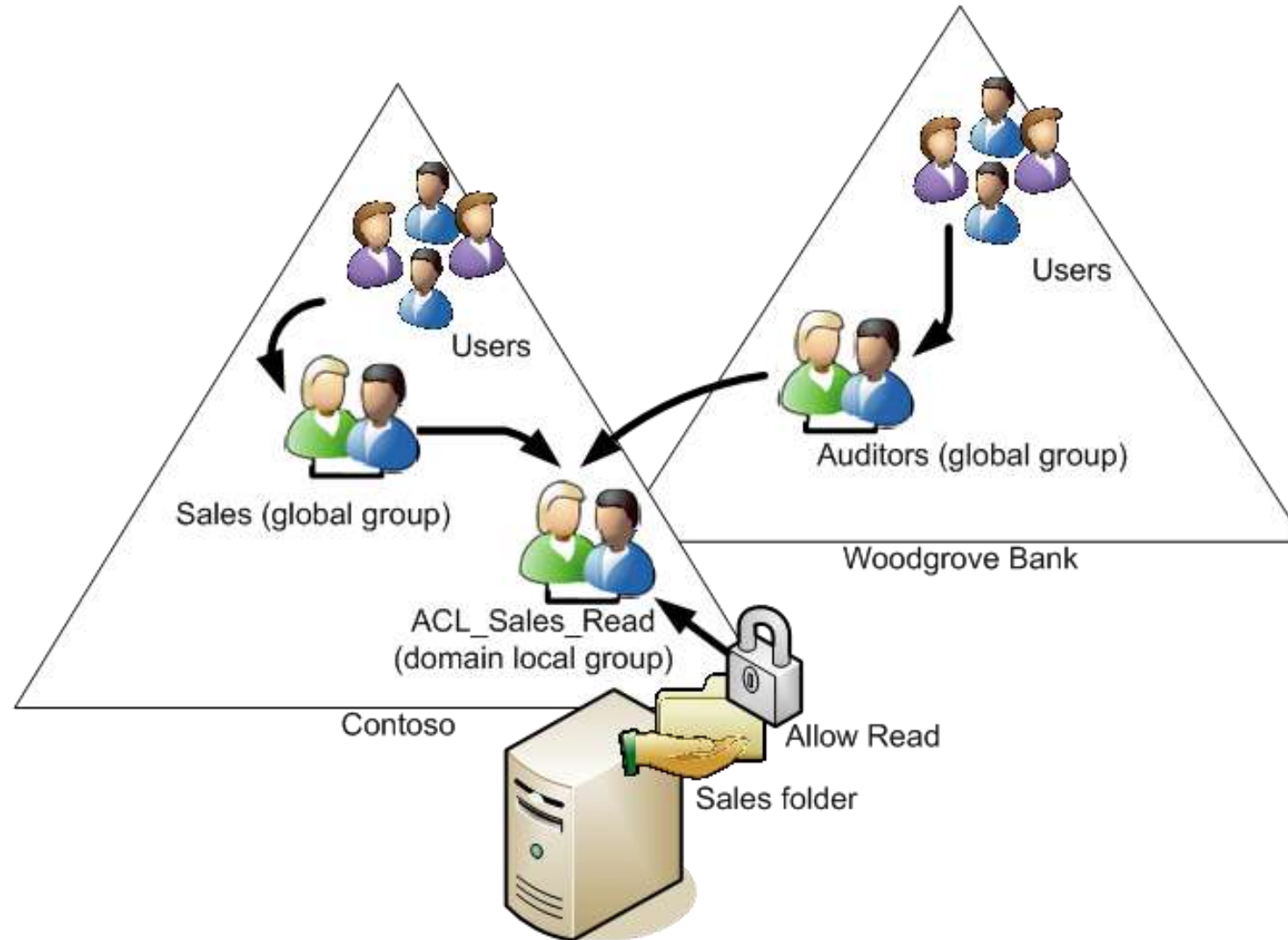
☐ Local path:

☒ Connect: H: To:

OK Cancel Apply Help

- Distribution groups / Verteilungsgruppen
 - Used only with email applications
 - Not security-enabled (no SID); cannot be given permissions
- Security groups / Sicherheitsgruppen
 - Security principal with an SID; can be given permissions
 - Can also be email-enabled





Group scope	Members from same domain	Members from domain in same forest	Members from trusted external domain	Can be assigned permissions to resources
Local	U, C, GG, DLG, UG and local users	U, C, GG, UG	U, C, GG	On the local computer only
Domain Local	U, C, GG, DLG, UG	U, C, GG, UG	U, C, GG	Anywhere in the domain
Universal	U, C, GG, UG	U, C, GG, UG	N/A	Anywhere in the forest
Global	U, C, GG	N/A	N/A	Anywhere in the domain or a trusted domain

U User
C Computer
GG Global Group
DLG Domain Local Group
UG Universal Group

- ADSI-Edit öffnen (z.B. via mmc)
- `Configuration / cn=Display Specifiers, cn=Configuration, dc=DOMAIN, dc=SUFFIX`
- Deutsch: 407
- Englisch: 409
- `cn=user-Display` öffnen, Attribut-Editor
- `createDialog` bearbeiten, z.B. `„%<sn>, %<givenName>“`

- Kennwörter werden (falls nötig) automatisch vom AD geändert
- Unterliegen nicht den Kennwortrichtlinien der Domäne
- `new-ADServiceAccount „Accountname“ -Enable $true`
- Konto mit Computerkonto verknüpfen

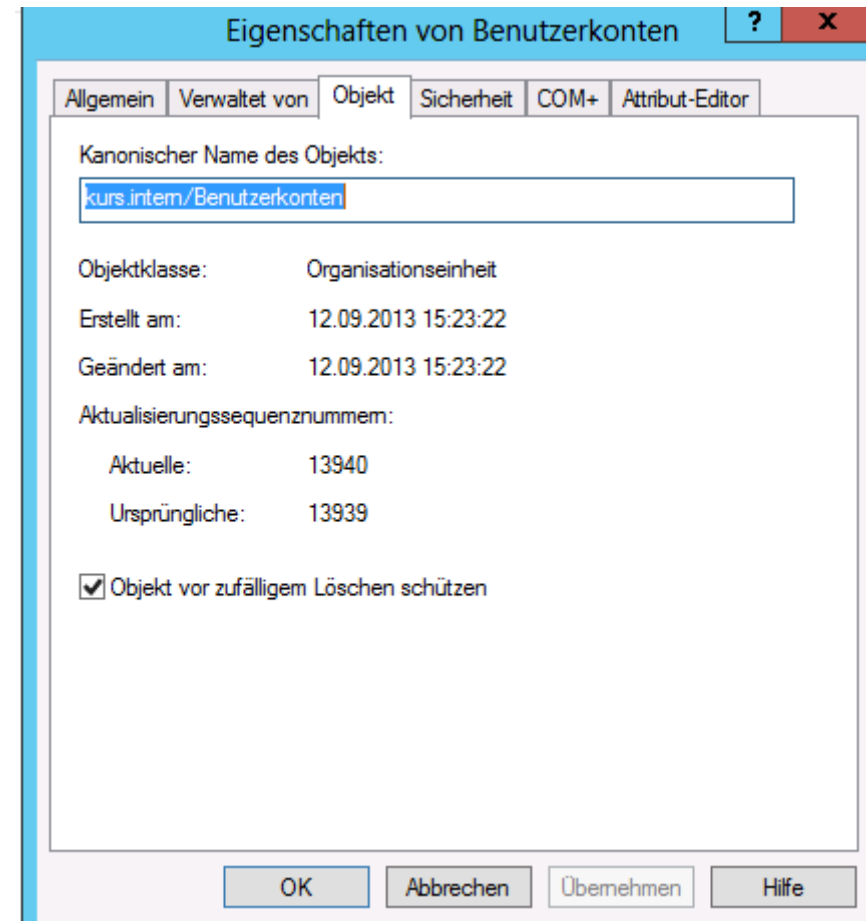
```
Add-ADComputerServiceAccount -Identity  
<Zielcomputer> -ServiceAccount <Erstelltes  
Dienstkonto>
```

- Auf Anwendungsserver:

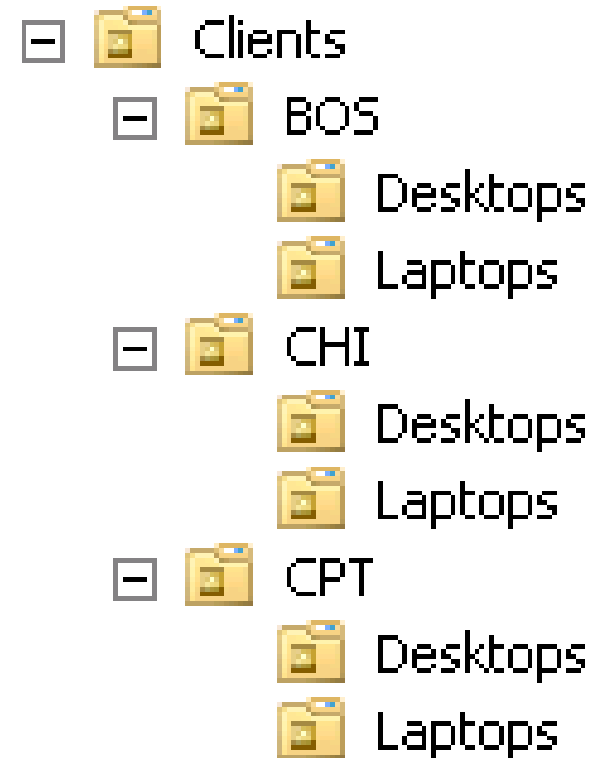
```
Install-ADServiceAccount "Name des Accounts"
```

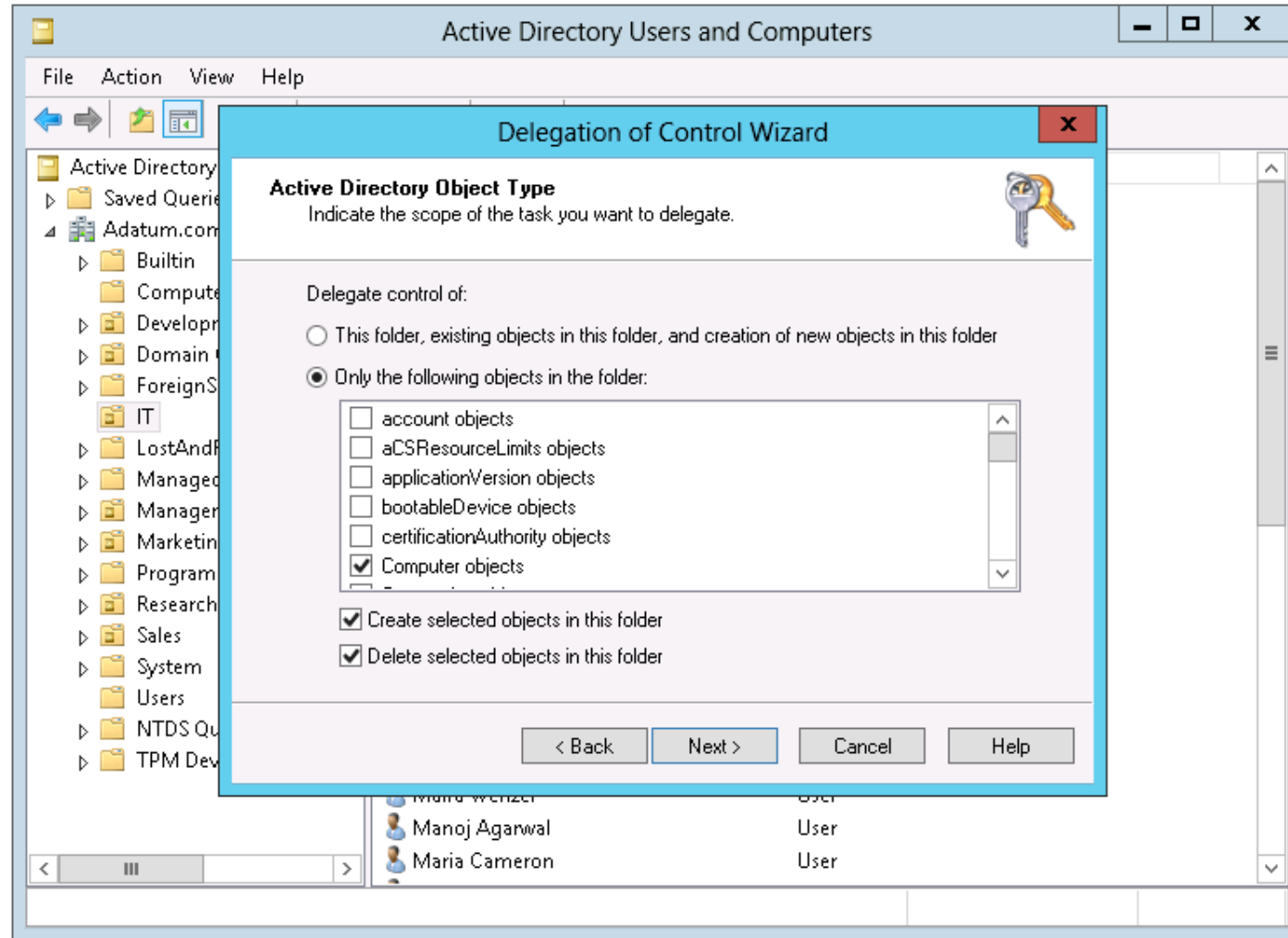

- Können nun an mehrere Computer-Konten innerhalb der selben Domäne gebunden werden
- Voraussetzung:
 - Server 2012 DC
 - gMSA auf Server 2012 genutzt
- Bedienung wie für reguläre MSA

- Standardmäßig angekreuzt bei OUs
- Ansicht/Erweiterte Features



- Computer- und Benutzerkonten in eigene Ous
- Sinnvolle Gliederung (z.B. nach Standort, Abteilung, ...)





- Computers have accounts
 - sAMAccountName and password
 - Used to create a secure channel between the computer and a domain controller
- Scenarios where a secure channel can be broken
 - Reinstalling a computer, even with same name, generates a new SID and password
 - Restoring a computer from an old backup, or rolling back a computer to an old snapshot
 - Computer and domain disagree about what the password is

- Do not simply remove a computer from the domain and rejoin
 - Creates new account: new SID, lost group memberships
- Options for resetting the secure channel
 - Active Directory Users and Computers
 - DSMod
 - NetDom
 - NLTest
 - Windows PowerShell

- Wenn Computer aus Domäne entfernt wird, bleibt Computerkonto in Domäne (deaktiviert)
 - Wenn PC nicht sauber aus Domäne entfernt wurde
 - `dsquery computer -stalepwd xx`
- Computer-PW alle 30 Tage geändert!
- `dsquery computer -stalepwd 70 | dsrm -noprompt -c`

- Deaktivierte Computerkonten:
- `Search-ADAccount -AccountDisabled -ComputersOnly`
- Alle Computer, die X Tage nicht angemeldet waren:
- `Search-ADAccount -AccountInactive -Timespan X -ComputersOnly | Sort-Object | FT Name -A`

- Domänen-Beitritt, ohne, dass AD bzw. DC erreichbar ist
 - `djoin /provision /domain DOMAIN.INTERN /machine COMPUTERNAME /savefile FILE.djoin`
 - FILE.djoin auf Client übertragen
 - `djoin /requestodj /loadfile FILE.djoin /windowspath C:\Windows /localOS`

- Schauen Sie sich das AD Verwaltungscenter an
- Erzeugen Sie eine OU
- Legen Sie ein paar Benutzerkonten im AD an
- Gruppieren Sie diese mit Hilfe einer Sicherheitsgruppe
- Delegieren Sie dieser Gruppe Rechte auf die OU

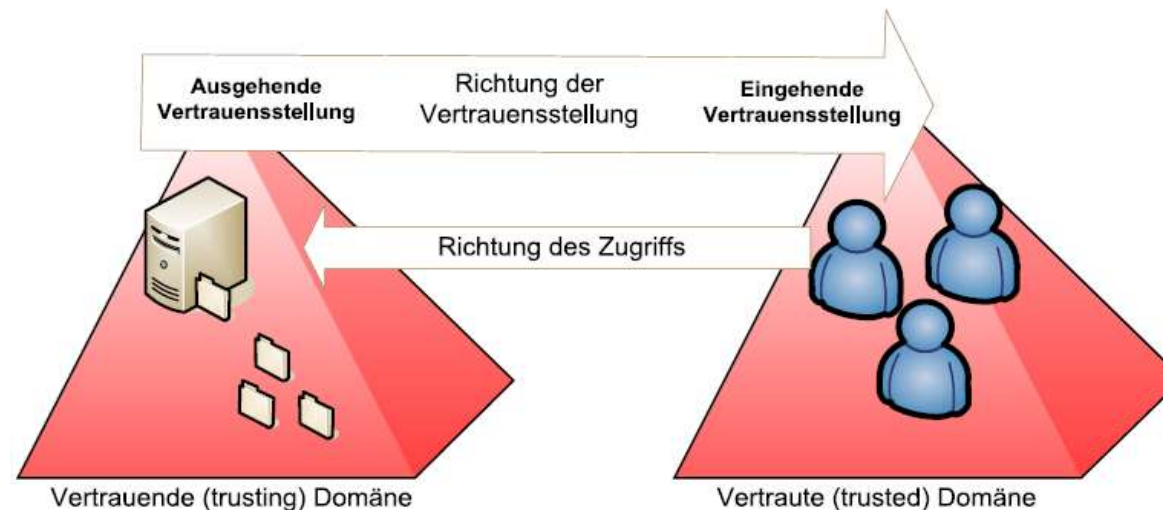


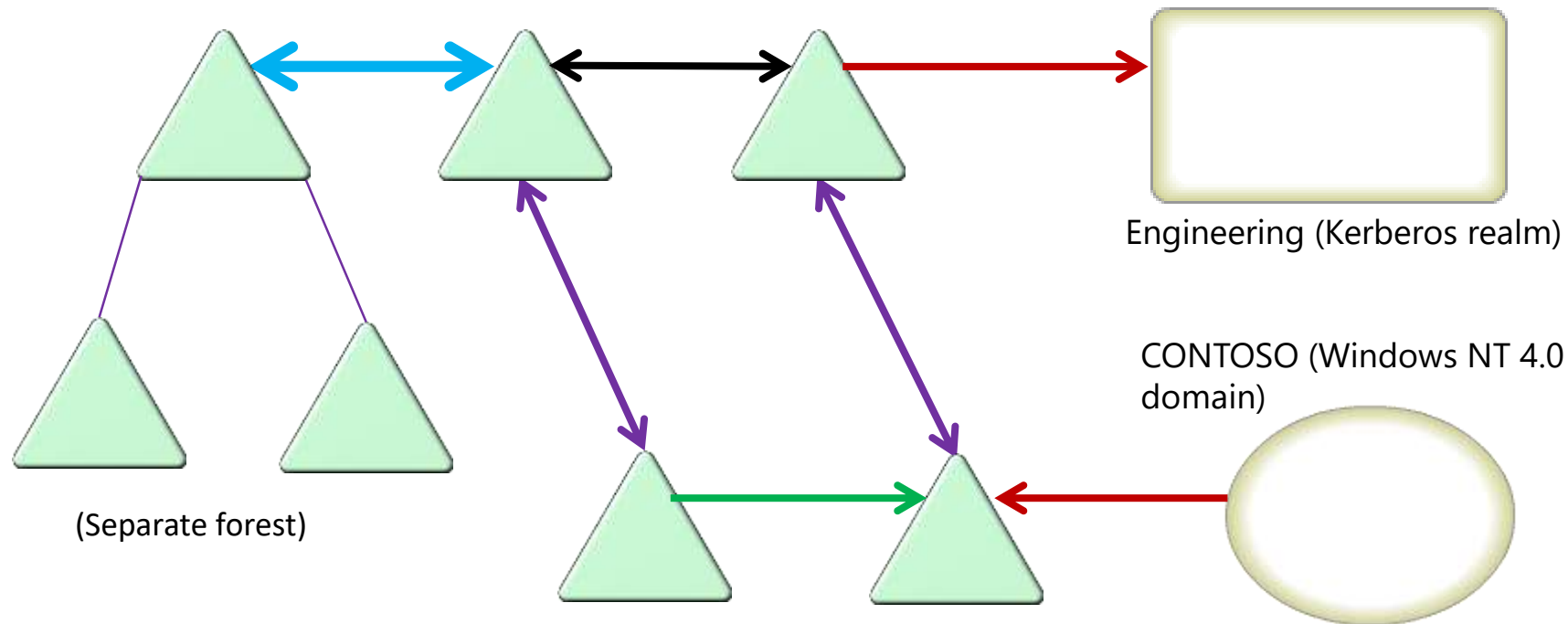
- Bedarf Planung!
- Irreversibel
- Neue Attribute: Vorher prüfen, ob OID frei; bei Bedarf registrieren (ISO)
- `regsvr32 schmmgmt.dll`
- mmc-Snapin „Active Directory-Schema“

VERTRAUENSSTELLUNGEN

- Innerhalb GS: Automatisch zwischen allen Domänen (transitiv)
- Zusätzlich zu anderen Domänen möglich
 - bidirektional
 - unidirektional

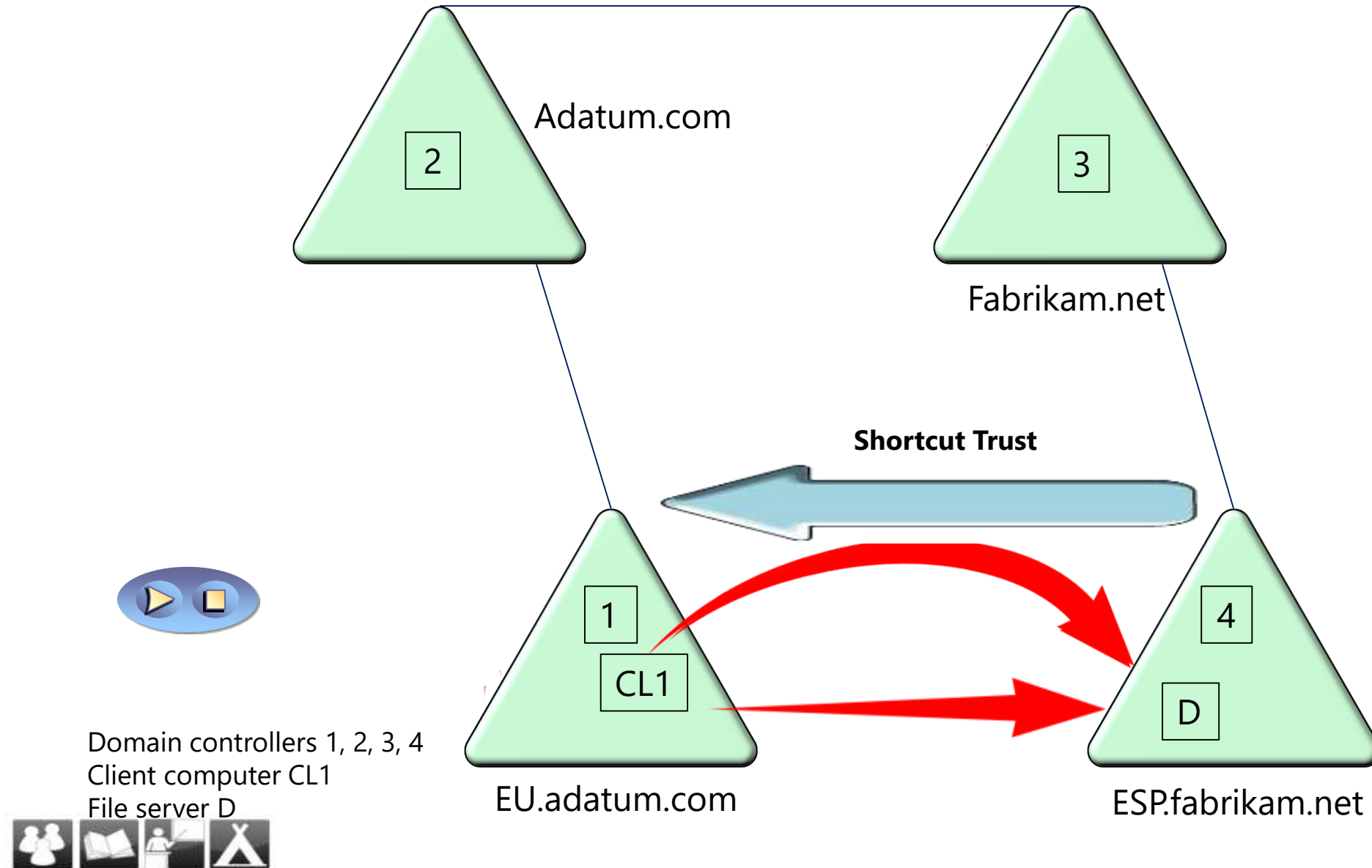
⇒ Testsysteme





Trust type	Transitive?	Color
Parent-child	Yes	Purple
Tree root	Yes	Black
External (domain or Kerberos realm)	No	Red
Shortcut	No	Green
Forest (complete or selective)	Yes	Blue





- Anmeldung am Netzwerk/PC über VPN
 - VPN-Verbindung muss bereits existieren
 - Am Anmeldebildschirm Button unten rechts:



- Muss als Rollendienst mit dem RD-Sitzungshost installiert werden
- Aufruf über <https://SERVER/RDWeb> bzw.
- <https://RDFARM/RDWeb>

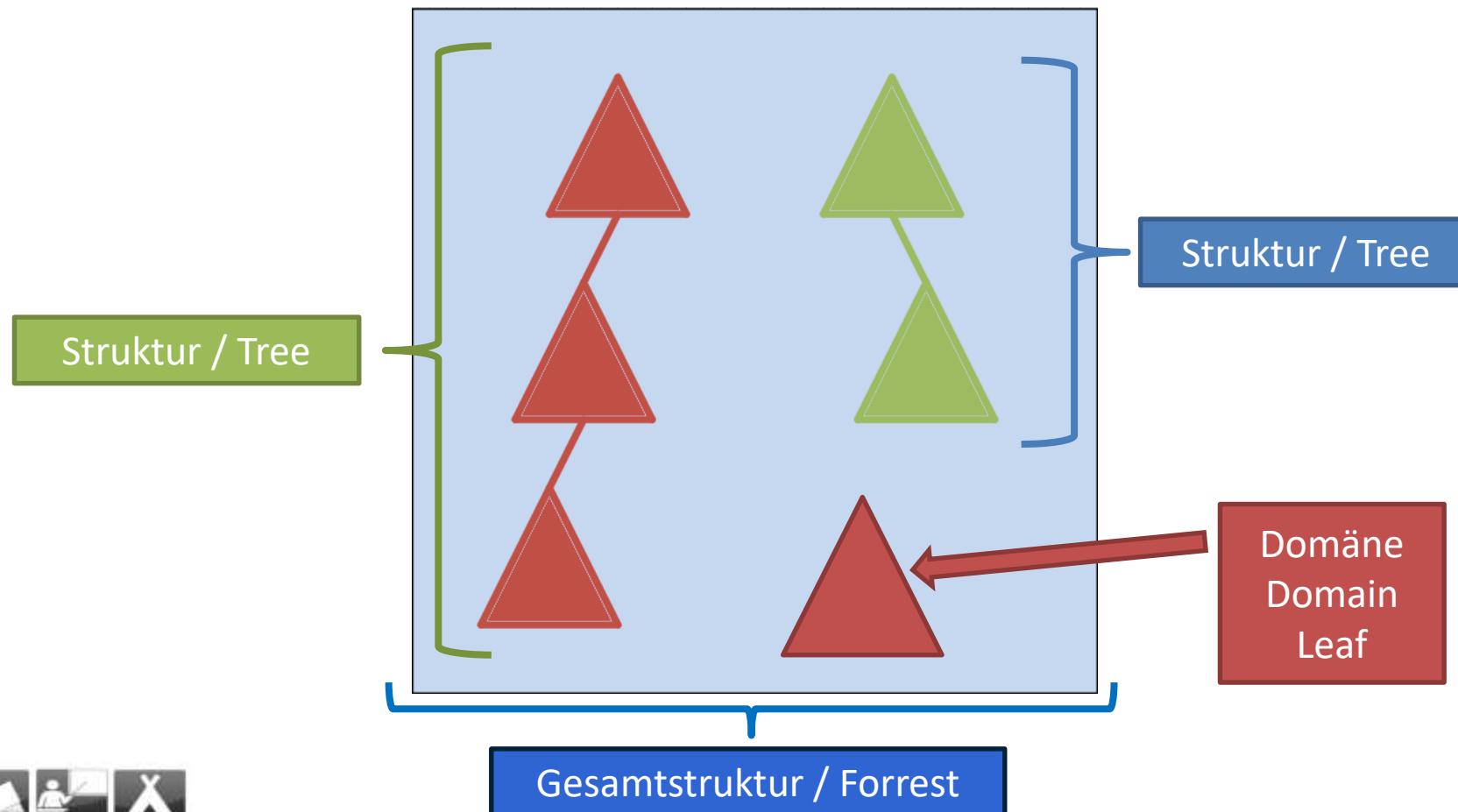
PASSWORD SETTING OBJECTS

- Bisher: Für 2 Kennworteinstellungs-Sätze 2 Domänen notwendig
- PSO kann mit Benutzer oder Gruppen (global!) verknüpft werden
- `New-ADFineGrainedPasswordPolicy -Name "NAME" -Precedence 20 -ComplexityEnabled $true -Description "DESC" -Displayname "DFN" -LockoutDuration "0.00:15:00" -LockoutObservationWindow "0.00:15:00" -LockoutThreshold 15 -MaxPasswordAge "60.00:00:00" -MinPasswordAge "5.00:00:00" -MinPasswordLength 8 -PasswordHistoryCount 10 -ReversibleEncryptionEnabled $false`

- `Add-ADFineGrainedPasswordPolicySubject <NAME> <USER/GRP>`
- `Set-ADFineGrainedPasswordPolicy "CN=<PSO-NAME>,CN=Password Settings Container,CN=System,DC=Domäne,DC=de" -Precedence 15 -MinPasswordLength 12`
- `Get-ADFineGrainedPasswordPolicy -Filter { Name -Like "*" }`
- `Get-ADUserResultantPasswordPolicy <Benutzer>`
- `Get-ADFineGrainedPasswordPolicySubject <Name der PSO>`
- `Remove-ADFineGrainedPasswordPolicySubject <Name der PSO> -Subjects <Benutzer/Gruppen> -Confirm:$False`
- `Remove-ADFineGrainedPasswordPolicy <Name der PSO> -Confirm:$False`
- **NEU: PSO über Active Directory Verwaltungszentrum**

⇒ Demo / Übung

WIEDERHOLUNG 1. TAG

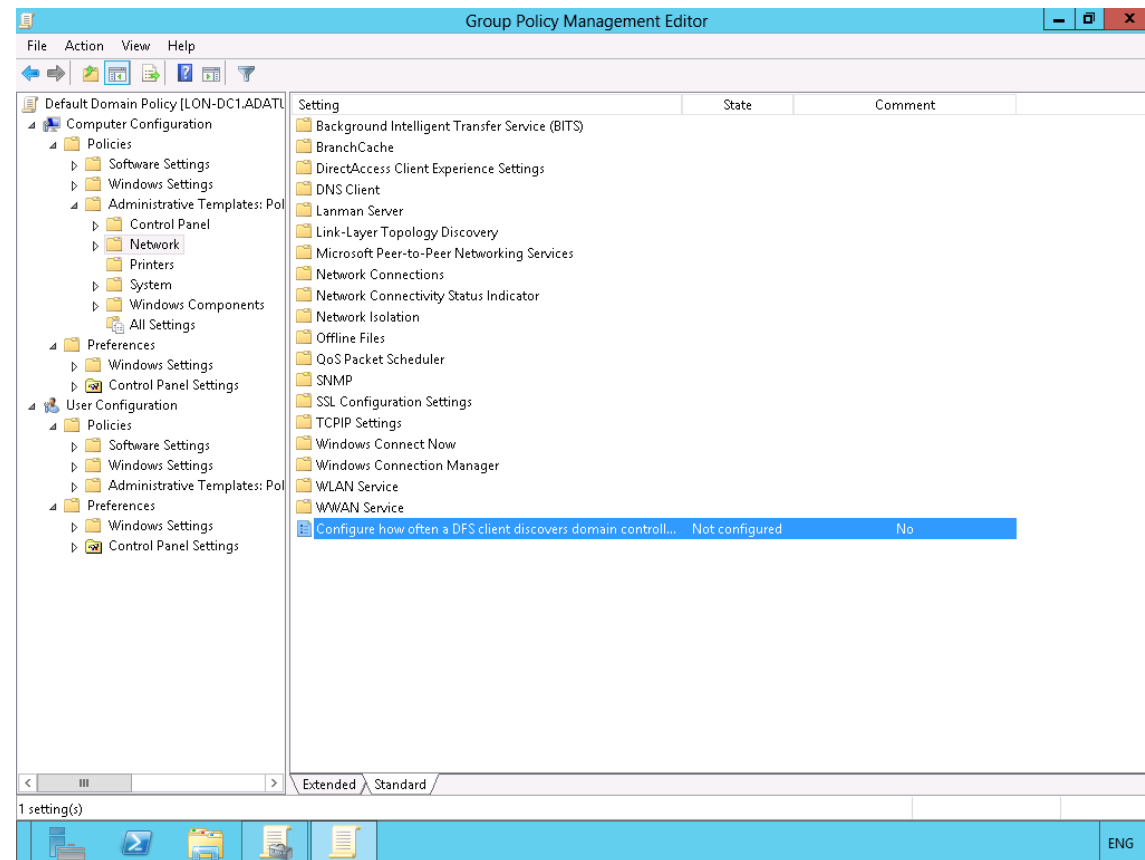


- Wo liegt der Unterschied zwischen einem Container und einer OU?
- Was sind Funktionsebenen und welche Zusammenhänge existieren dabei?
- Was ist das „Schema“?
- Wie lässt sich ein Server 2012 zum Domänencontroller heraufstufen?

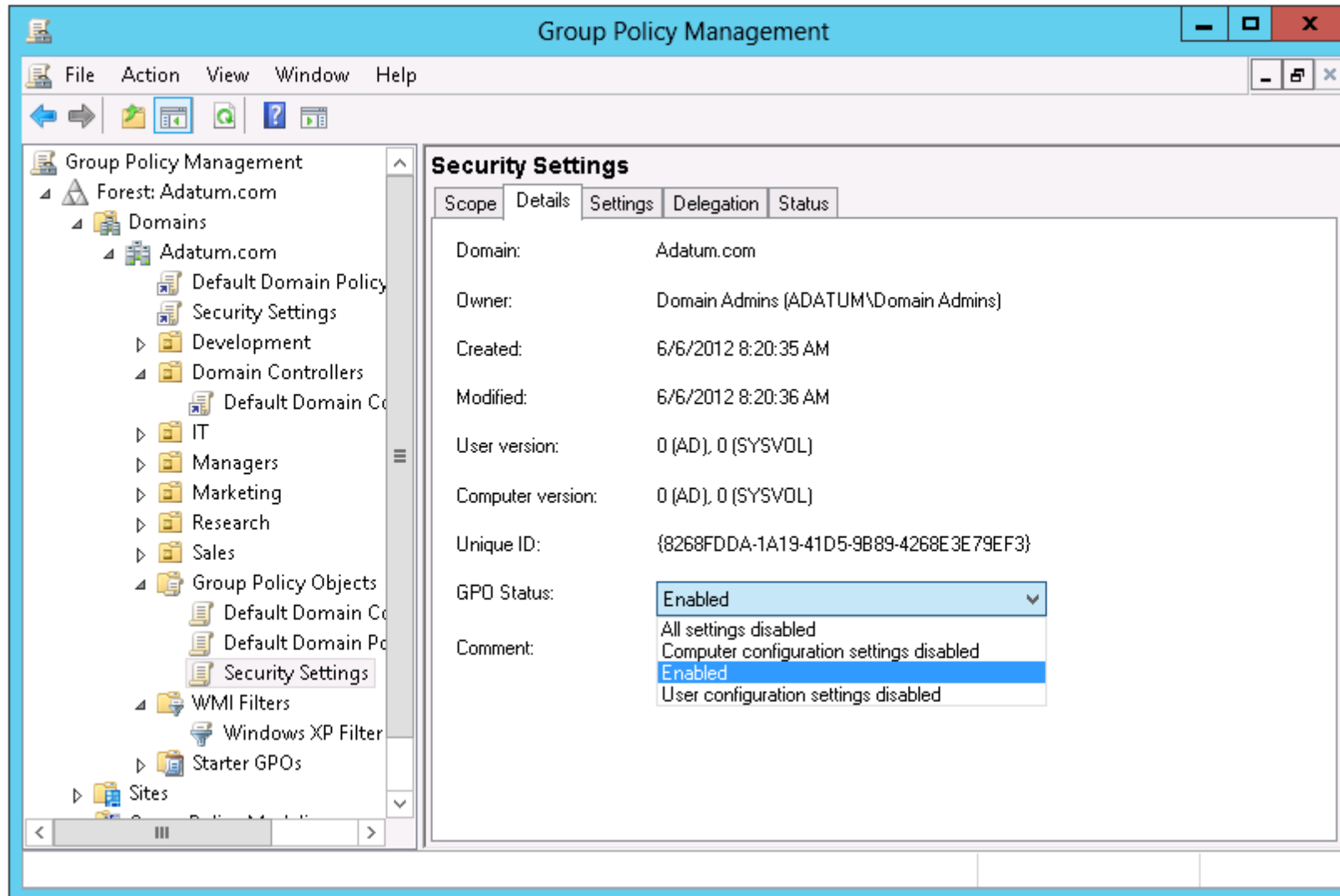
- Welche *FSMO-Rollen* gibt es und wie sind diese verteilt?
- Wie kann man die Rollen an andere Server übertragen? (2 Arten)
- Was sind AD-Sites und wie werden diese eingesetzt?
- Was ist ein Bridgehead-Server?
- Was ist *TGT*?
- Welche Besonderheiten besitzt der *RODC* und wo wird er beispielsweise eingesetzt?

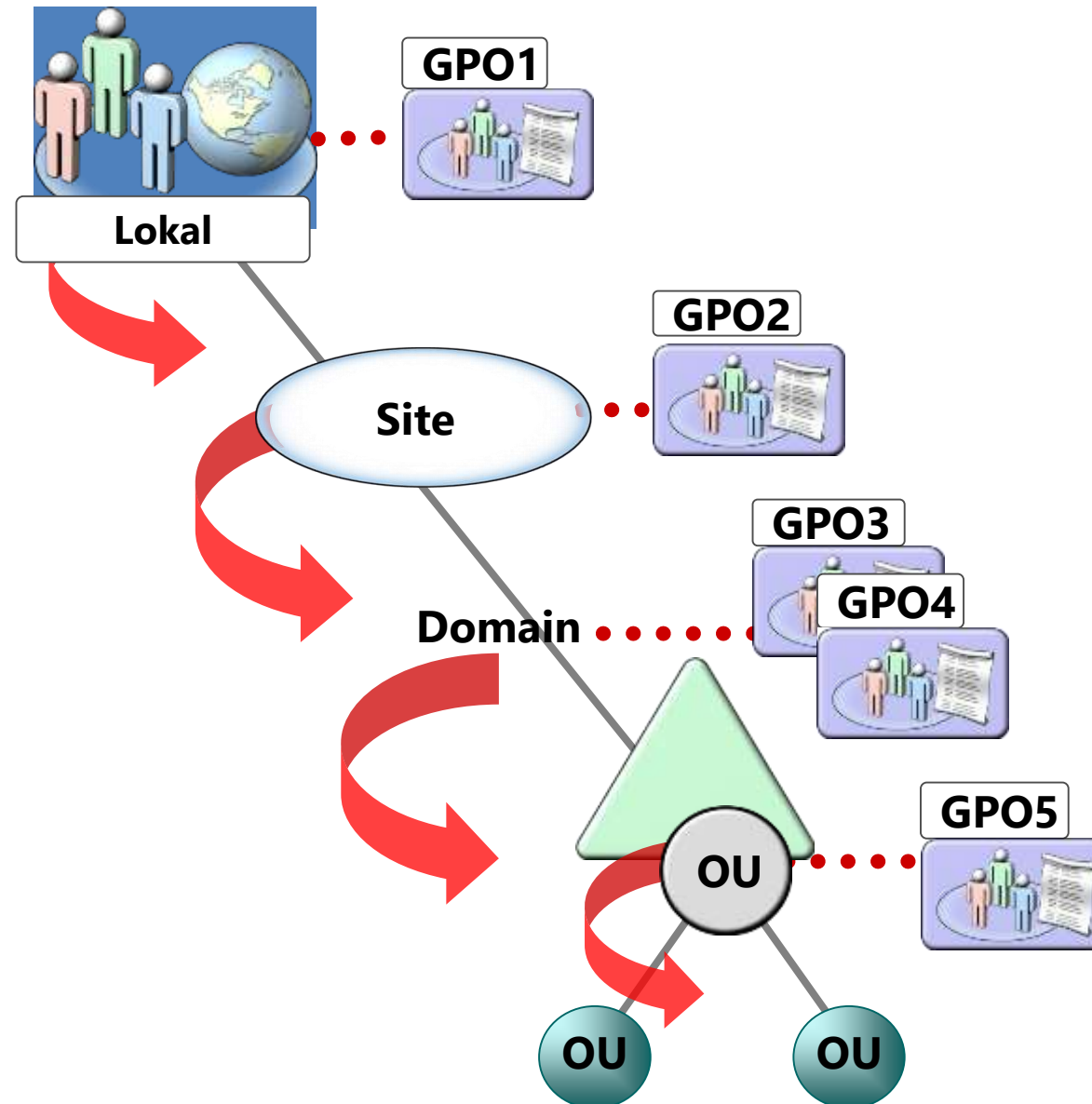
POLICIES / GPO

- Zentrales Verwalten von
 - Einstellungen
 - Sicherheitsrichtlinien
 - Anwendungen
 - ...
- für
 - Computer
 - Benutzer

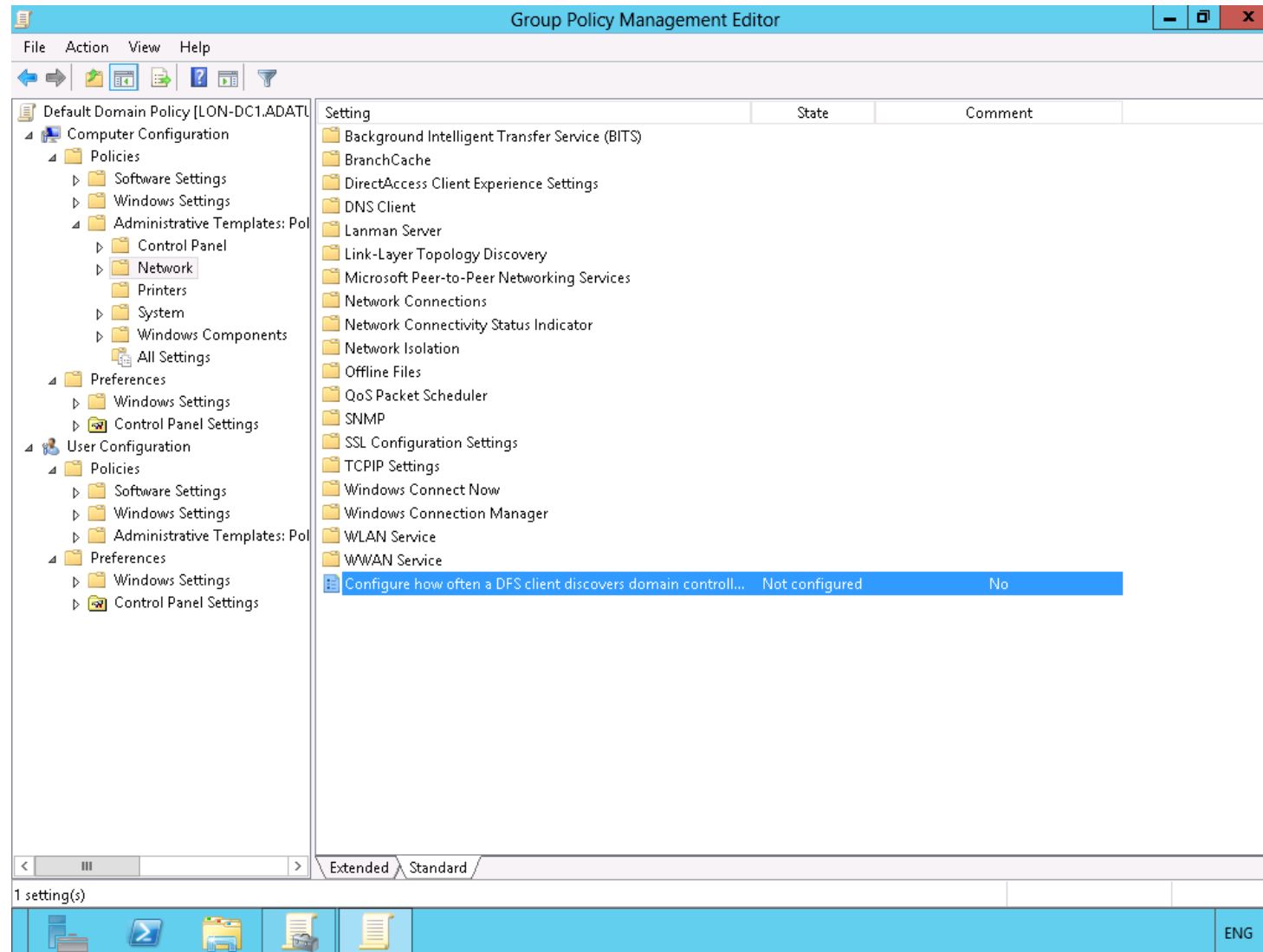


- Benutzer-GPO / Computer-GPO
 - Objektstatus beschleunigt Abarbeitung
- Benutzung
 - Richtlinien vs. Einstellungen
- Abarbeitungsreihenfolge:
 - Local
 - Site
 - Domain
 - OU in die Tiefe
- Neu: Invoke-GPUUpdate
 - ⇒ z.B. `Get-ADComputer | Invoke-GPUUpdate`

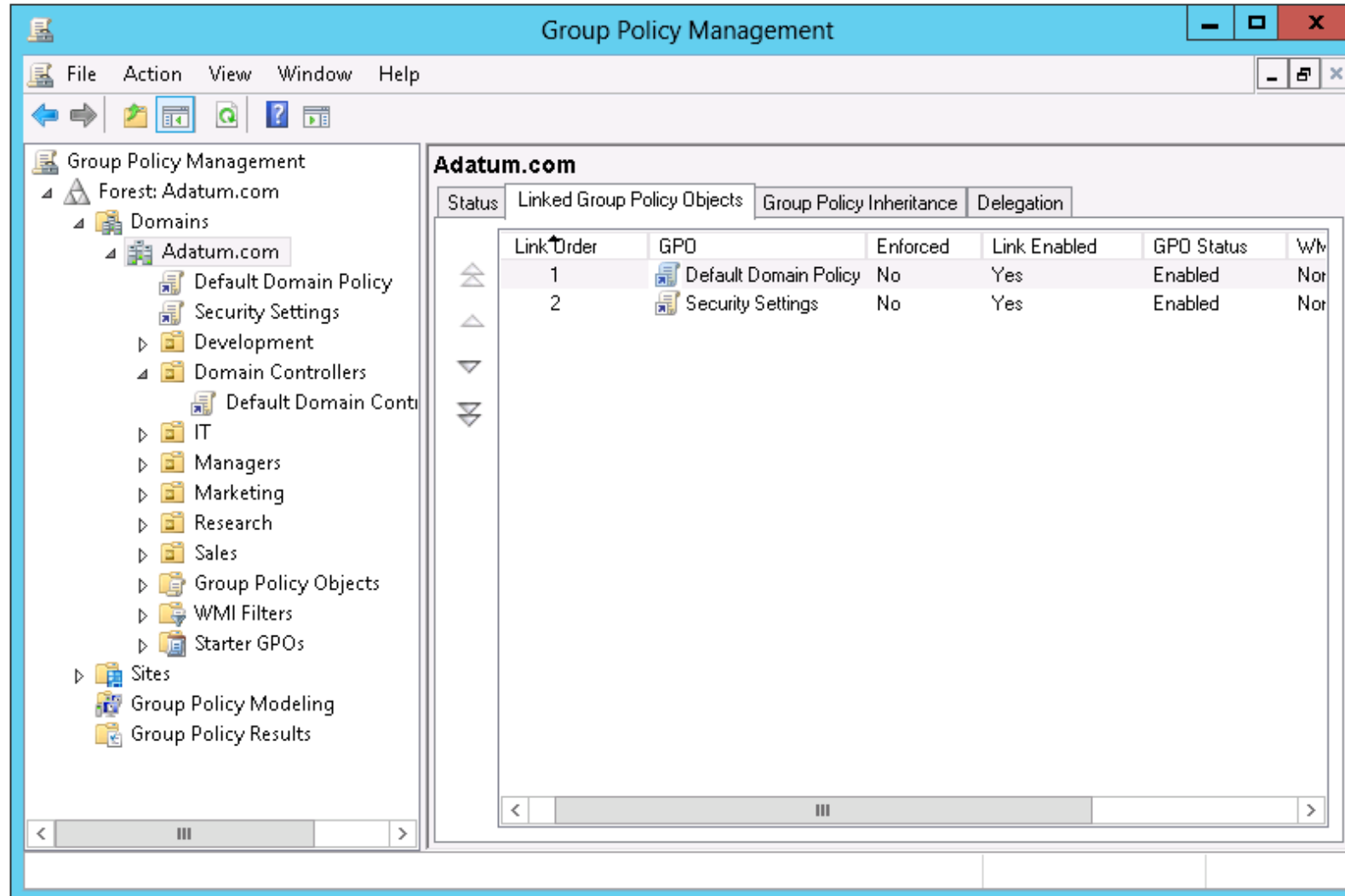




- Vererbung / Vererbung deaktivieren
- Erzwingen
- Verknüpfungsreihenfolge

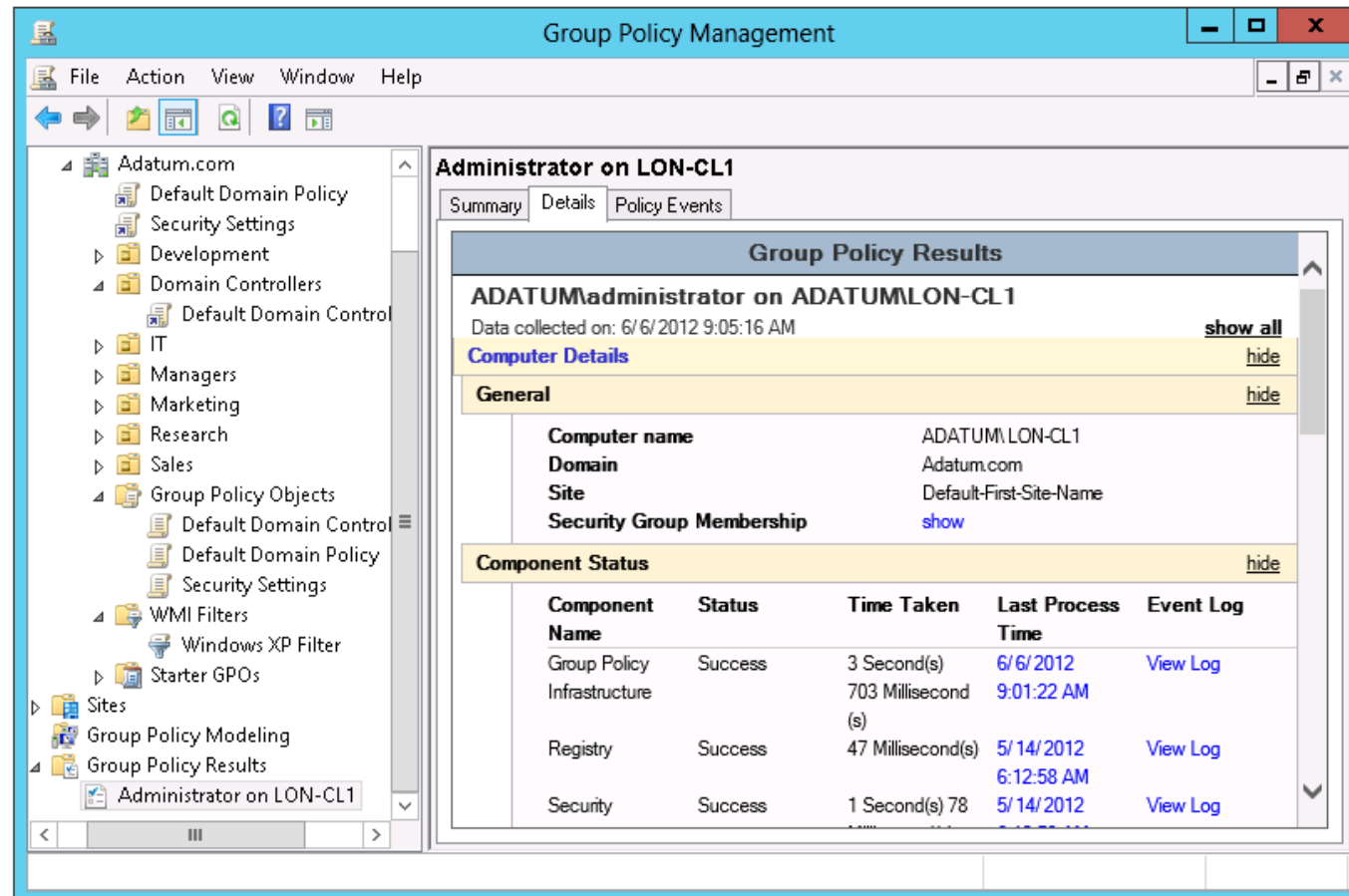


Setting	State	Comment
Background Intelligent Transfer Service (BITS)		
BranchCache		
DirectAccess Client Experience Settings		
DNS Client		
Lanman Server		
Link-Layer Topology Discovery		
Microsoft Peer-to-Peer Networking Services		
Network Connections		
Network Connectivity Status Indicator		
Network Isolation		
Offline Files		
QoS Packet Scheduler		
SNMP		
SSL Configuration Settings		
TCPIP Settings		
Windows Connect Now		
Windows Connection Manager		
WLAN Service		
WWAN Service		
Configure how often a DFS client discovers domain controll...	Not configured	No



Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI
1	Default Domain Policy	No	Yes	Enabled	Not
2	Security Settings	No	Yes	Enabled	Not

- Gruppenrichtlinienergebnisse
- Gruppenrichtlinienmodellierung



The screenshot displays the Group Policy Management console. The left pane shows the hierarchy: Adatum.com > Group Policy Objects > Administrator on LON-CL1. The right pane shows the 'Group Policy Results' for this GPO on the computer ADATUM\administrator on ADATUM\LON-CL1, with data collected on 6/6/2012 at 9:05:16 AM. The results are categorized into 'Computer Details' and 'Component Status'.

Group Policy Results

ADATUM\administrator on ADATUM\LON-CL1
Data collected on: 6/6/2012 9:05:16 AM [show all](#)

Computer Details [hide](#)

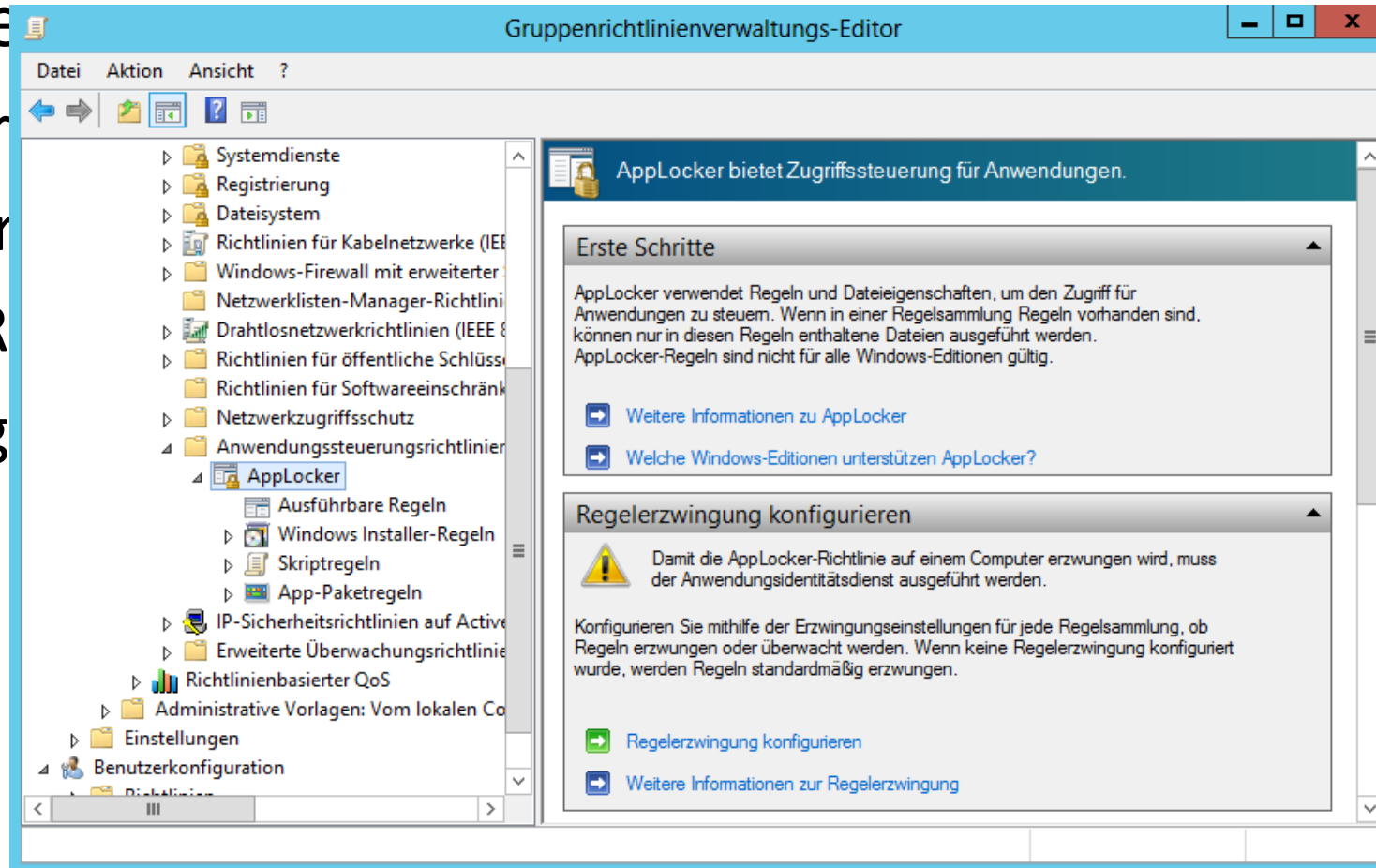
General [hide](#)

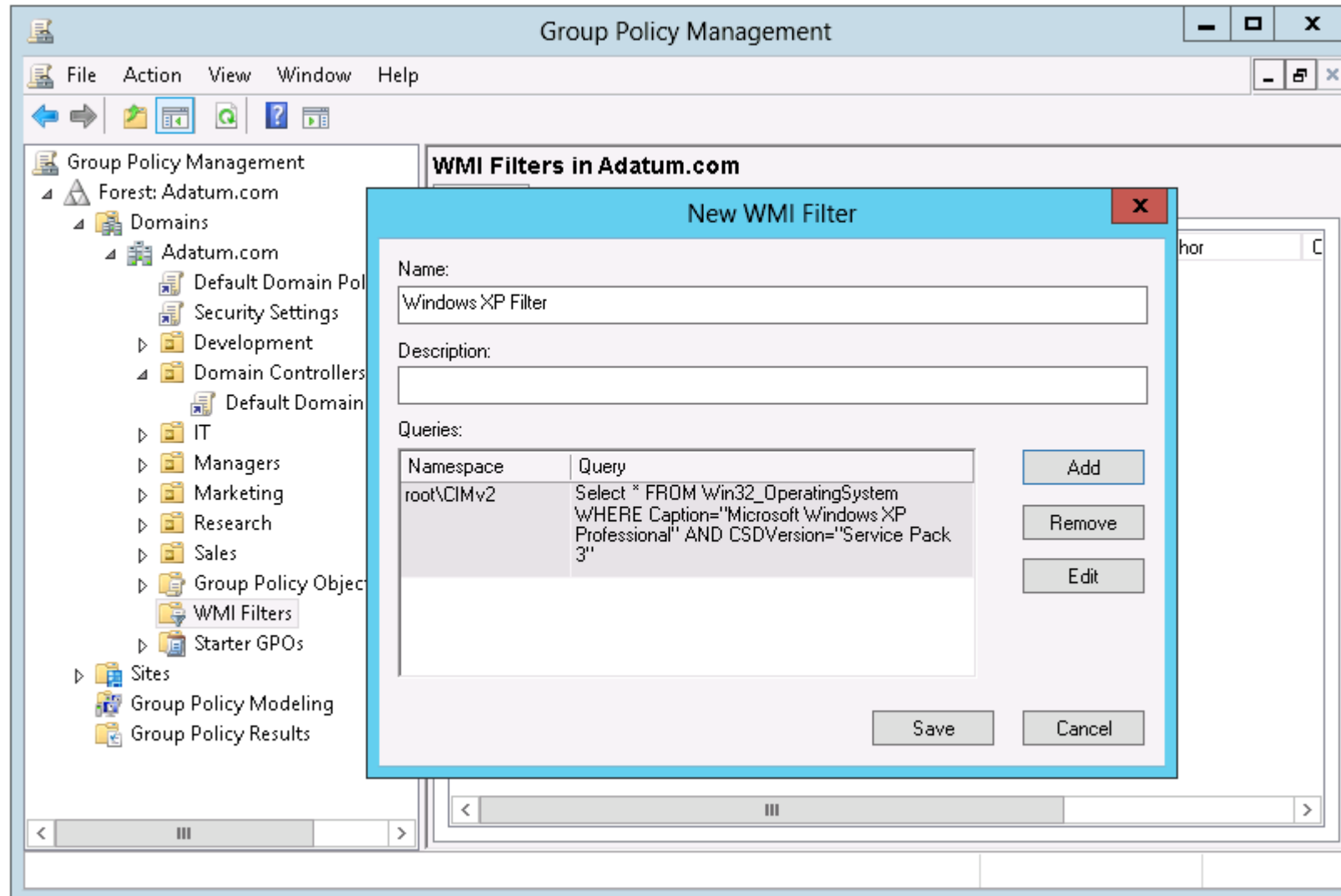
Computer name: ADATUM\LON-CL1
Domain: Adatum.com
Site: Default-First-Site-Name
Security Group Membership: [show](#)

Component Status [hide](#)

Component Name	Status	Time Taken	Last Process Time	Event Log
Group Policy Infrastructure	Success	3 Second(s) 703 Millisecond(s)	6/6/2012 9:01:22 AM	View Log
Registry	Success	47 Millisecond(s)	5/14/2012 6:12:58 AM	View Log
Security	Success	1 Second(s) 78	5/14/2012	View Log

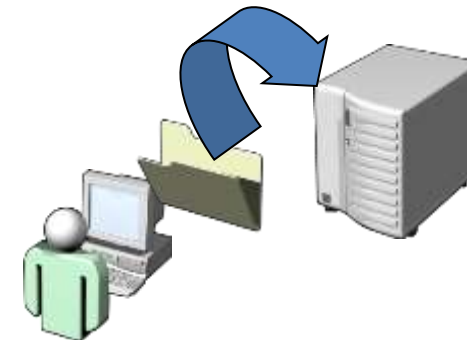
- AppLocker
 - Ausführung
 - Installer
 - Script-R
 - Erzwing

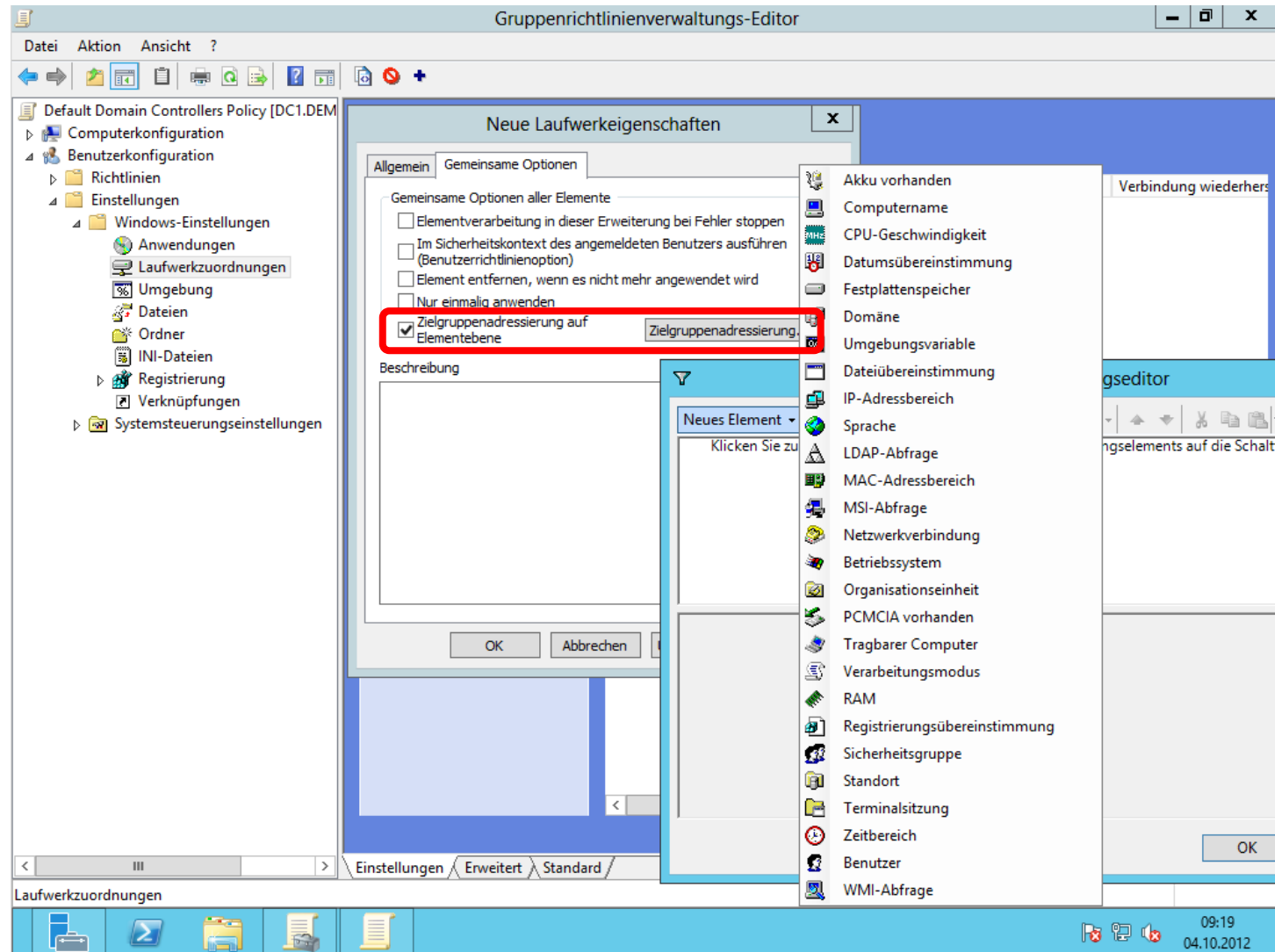




Folgende Ordner können in Windows Vista, Windows 7 und Windows 8 umgeleitet werden:

- Desktop
- Start Menu
- Documents
- Pictures
- AppData\Roaming
- Contacts
- Downloads
- Favorites
- Saved Games
- Searches
- Links
- Music
- Videos





- Machen Sie sich vertraut mit:
 - Gruppenrichtlinienverwaltung
 - Möglichkeiten der Richtlinien
 - Möglichkeiten der Einstellungen
 - Vererbung
 - Verknüpfungsreihenfolge
 - Gruppenrichtlinienmodellierung
 - Gruppenrichtlinienergebnisse



KLONEN EINES DOMÄNENCONTROLLERS

- Voraussetzungen:
 - Klon-Quelle läuft unter Server 2012
 - Klon-Quelle ist nicht PDC-Emulator
 - PDC-Emulator ist online
 - Klon-Quelle ist Mitglied der AD-Gruppe „Klonbare Domänencontroller“
 - Klon-Ziel wird NACH Klon-Quelle gestartet

⇒ Clonen eines virtuellen DCs

- Klon-Quelle in Gruppe „Klonbare Domänencontroller“ aufnehmen
- %WINDIR%\System32\SampleDCCloneConfig.xml als %WINDIR%\NTDS\DCCloneConfig.xml
- Get-ADDCCloneExcludedApplicationList => %WINDIR%\NTDS\CustomDCCloneAllowList.xml
- Quelle herunterfahren
- HDD duplizieren
- Quelle und danach Ziel mit neuen



- Übung:
 - SRV4 zum DC heraufstufen
 - Klonen vorbereiten
 - SRV4 als DC auf neuen SRV4-Klon klonen



⇒Hyper-V-Replica

⇒Asynchrone Replikation einer virtuellen Maschine mit zweitem Hyper-V-3.0-Server

⇒Storage-Migration

⇒Verschieben der VHD eines virtuellen Servers (im laufenden Betrieb) (evtl. direkt auf UNC-Pfad)

⇒PowerShell Modul

⇒Get-Command -Module Hyper-V

⇒Get-Command -Module Hyper-V | Select -Unique Noun |
Sort Noun

⇒Dynamic Memory / Smart Paging

AD WIEDERHERSTELLEN

- Nicht autorisierende Wiederherstellung
 - Ein DC defekt, AD auf anderen DC(s) intakt
- Primäre Wiederherstellung des gesamten AD
 - Nur ein DC vorhanden oder alle DCs verloren
- Autorisierende Wiederherstellung des gesamten AD
 - Systemcrash o.ä. hat gesamtes AD beschädigt, Änderungen wurden an alle DC repliziert
- Autorisierende Wiederherstellung eines Teils des AD
 - OU o.ä. gelöscht, bereits repliziert

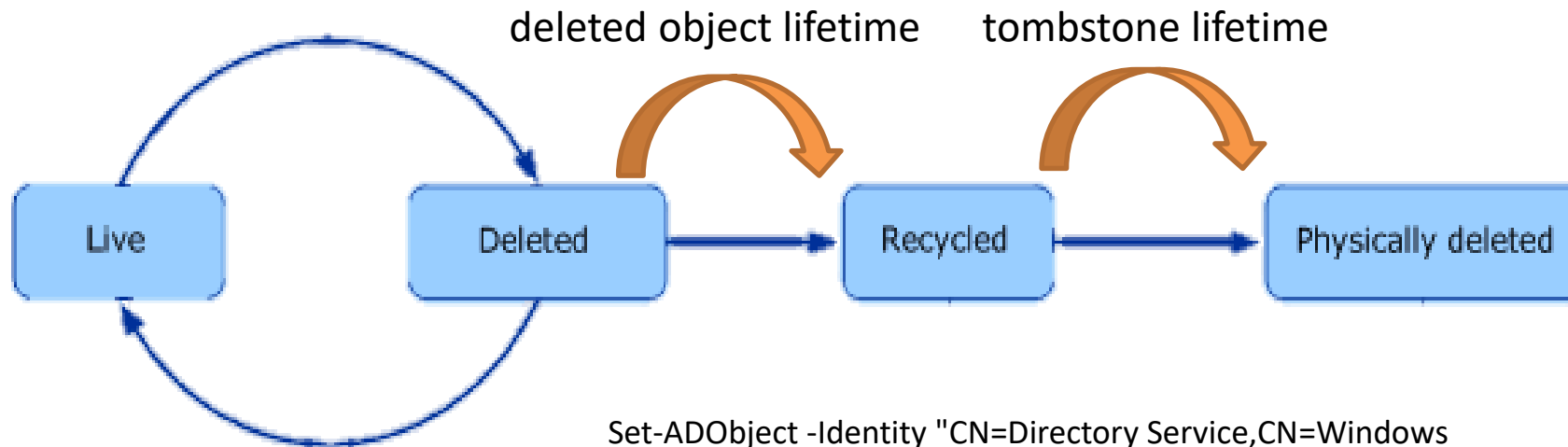
- DC herunterfahren
- Mit erweiterten Optionen starten (F8) -> Verzeichnisdienstwiederherstellung
- Aus Windows Server Sicherung Systemstatus wiederherstellen (in urspgl. Ordner)
- Fertig!
- Änderungen seit Backup werden von anderen DCs repliziert

- DC herunterfahren
- Mit erweiterten Optionen starten (F8) -> Verzeichnisdienstwiederherstellung
- Aus Windows Server Sicherung Systemstatus wiederherstellen (in urspgl. Ordner)
 - Dabei auswählen „Wiederhergestellte Daten in replizierten Datensätzen als primäre Daten für Replikate markieren“
- Fertig!

- Nicht autorisierende Wiederherstellung ohne Neustart ausführen
- NTDSUTIL.exe starten
 - authoritative restore ...
 - ... DATABASE
 - ... SUBTREE *SUBTREE_DN*
 - quit
- Neustart

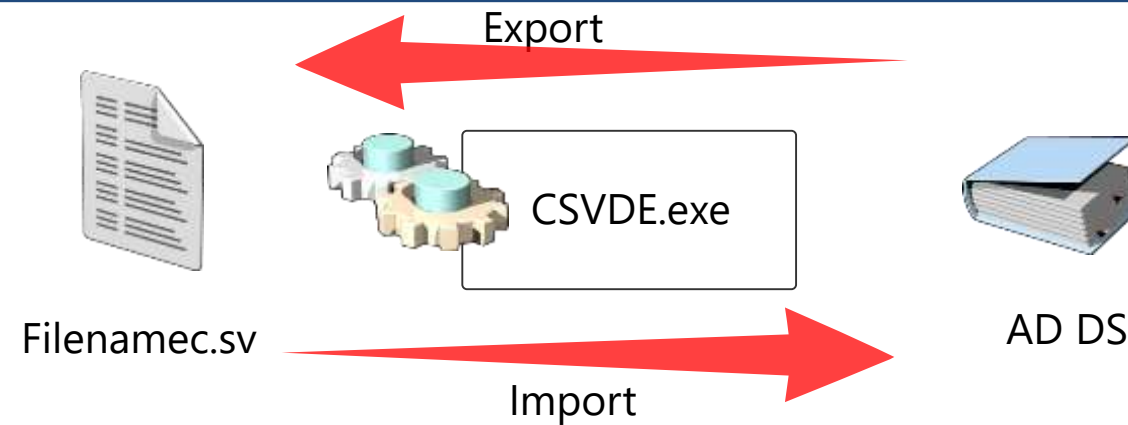
- Server 2008 R2 Domänen-Funktionsebene notwendig
- Lässt sich nicht rückgängig machen!
- Powershell:
 - `Enable-ADOptionalFeature „Recycle Bin Feature“ -Scope ForestOrConfigurationSet -Target „DOMAIN.INTERN“`
- Wiederherstellung:
 - `Get-ADObject -Filter {sAMAccountName -eq „TUSER“} -IncludeDeletedObjects | Restore-ADObject`
- NEU: Über ADAC!

- tombstone lifetime: **tombstoneLifetime** Attribut
 - Standard: NULL -> Bedeutet 60 Tage (hard-coded)
- deleted object lifetime: **msDS-deletedObjectLifetime** Attribut
 - Standard: NULL -> tombstoneLifetime -> 60 Tage



```
Set-ADObject -Identity "CN=Directory Service,CN=Windows  
NT,CN=Services,CN=Configuration,DC=Fabrikam,DC=COM" -  
Partition "CN=Configuration,DC=Fabrikam,DC=COM" -Replace  
@{tombstoneLifetime='210'}
```

- csvde.exe
 - Sichern: `csvde -f output.csv`
 - Wiederherstellen: `csvde -i -f input.csv`
- Windows Server Sicherung (Systemstatus)
- Alternative: ntds.dit und Logs offline sichern
- Besser: Server-Sicherung oder Dritthersteller-Tools



Use CSVDE to export objects to a .csv file:

- -f filename
- -d RootDN
- -p SearchScope
- -r Filter
- -l ListOfAttributes

Use CSVDE to create objects from a .csv file:

```
Csvde -i -f filename -k
```

- Aktivieren Sie den AD-Papierkorb
- Stellen Sie mit dessen Hilfe ein gelöschttes Konto wieder her
- Legen Sie ein AD-Snapshot an und mounten Sie diesen, um darauf zuzugreifen



WEITERES

- z.B. bei Fusion von Unternehmen
- `Netdom move computer /D:Ziel-Domäne
[/OU:Ziel-OU] [/DU:AD-User /PD:AD-Pass]
[/UO:Benutzer /PO:Pass] [/Reboot]`

- Wird bei `dcpromo` festgelegt
- gerät leicht in Vergessenheit
- `NTDSUTIL "set dsrm password" "sync from domain account NAME" q q`

```
C:\Users\Administrator>NTDSUTIL "set dsrm password" "sync from domain account Administrator" q q
NTDSUTIL: set dsrm password
DSRM-Administratorkennwort zurücksetzen: sync from domain account Administrator
Das Kennwort wurde erfolgreich synchronisiert.
DSRM-Administratorkennwort zurücksetzen: q
NTDSUTIL: q
```

- Geschieht nur einmalig und für den lokalen DC!

- Nach
 - Größerer Löschaktion
 - Deaktivierung eines GC
- `net stop ntds /y`

```
C:\Users\Administrator>ntdsutil
ntdsutil: activate instance ntds
Aktive Instanz wurde auf "ntds" festgelegt.
ntdsutil: files
file maintenance: compact to c:\ntds_neu.dit
Defragmentierungsmodus wird initialisiert...
    Quelldatenbank: C:\Windows\NTDS\ntds.dit
    Zieldatenbank: c:\ntds_neu.dit\ntds.dit

          Defragmentation  Status (% complete)
0      10      20      30      40      50      60      70      80      90      100
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
.....

Es empfiehlt sich, umgehend eine Sicherung dieser Datenbank
vorzunehmen. Durch Wiederherstellen einer Sicherung, die vor der
Defragmentierung erstellt wurde, wird die Datenbank wieder in den Zustand verset
zt,
in dem sie sich zum Zeitpunkt der Sicherung befand.

Die Komprimierung war erfolgreich. Sie müssen:
    "c:\ntds_neu.dit\ntds.dit" "C:\Windows\NTDS\ntds.dit" kopieren
und die folgenden Protokolldateien löschen:
del C:\Windows\NTDS\*.log
```

- Offiziell nicht für 64Bit supportet!
- x64-Version herunterladen und in %windir% kopieren
- `regsvr32 acctinfo2.dll`
- **ADSI-Editor** (CN=user-Display, CN=407, CN=DisplaySpecifiers, CN=Configuration, DC=Domäne, DC=TLD)
- CN=user-display / adminPropertyPages
- Wert „2, {5969F63F-CACF-40bf-8891-CA580EB589E9}“ hinzufügen
- Neuer Reiter am User im AD

Wieviele Computer darf ein Benutzer zur Domäne hinzufügen?

- **Wer? GPO:** Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\
Zuweisen von Benutzerrechten\Hinzufügen von Arbeitsstationen zur Domäne
 - Standard: Authentifizierte Benutzer
- **Default: 10 Clients**
 - Kann mittels ADSI-Editor verändert werden!
(Standardmäßiger Namenskontext/Rechtsklick auf Domäne/ms-DS-MachineAccountQuota)

- Damit wird DC auch in der (funktionstüchtigen) Domäne entfernt
- `ntdsutil`
 - `metadata cleanup`
 - `connections`
 - `connect to server SERVER`
 - `quit`
 - `select operation target`
 - `select domain DOMAIN`
 - `select site SITE`
 - `select server DC-NUMMER (list server in site)`
 - `quit`
 - `remove selected server`
 - `quit`

- Wenn DC FSMO-Rollen hatte erfolgen entsprechende Meldungen zur Übernahme
- DC-Objekt muss noch aus *Active Directory-Standorte und – Dienste* gelöscht werden
- DNS-Daten löschen
 - CleanUp seit 2008 auch über GUI

POWERSHELL FÜR ACTIVEDIRECTORY

- Modul laden:

- Import-Module ActiveDirectory

- Beispiel:

```
foreach ($computer in (get-adcomputer -  
filter * -searchbase  
"cn=computers,dc=mydomain,dc=local").name)  
{ $name = "\\\" + $computer; shutdown -m $name -s -  
f -t 0 }
```

- Nützlich: Quest PowerShell Commands (ActiveRoles Management)

Cmdlet	Description
New-ADUser	Creates user accounts
Set-ADUser	Modifies properties of user accounts
Remove-ADUser	Deletes user accounts
Set-ADAccountPassword	Resets the password of a user account
Set-ADAccountExpiration	Modifies the expiration date of a user account
Unlock-ADAccount	Unlocks a user account after it has become locked after too many incorrect login attempts
Enable-ADAccount	Enables a user account
Disable-ADAccount	Disables a user account

```
New-ADUser "Joe Healy" -AccountPassword (Read-Host -AsSecureString "Enter password") -Department IT
```


Cmdlet	Description
New-ADGroup	Creates new groups.
Set-ADGroup	Modifies properties of groups.
Get-ADGroup	Displays properties of groups.
Remove-ADGroup	Deletes groups.
Add-ADGroupMember	Adds members to groups.
Get-ADGroupMember	Displays membership of groups.
Remove-ADGroupMember	Removes members from groups.
Add-ADPrincipalGroupMembership	Adds group membership to objects.
Get-ADPrincipalGroupMembership	Displays group membership of objects.
Remove-ADPrincipalGroupMembership	Removes group membership from an object.

```
New-ADGroup -Name "CustomerManagement" -Path  
"ou=managers,dc=adatum,dc=com" -GroupScope Global -  
GroupCategory Security
```

```
Add-ADGroupMember CustomerManagement -Members "Joe Healy"
```

Using Windows PowerShell Cmdlets to Manage Computer Accounts

Cmdlet	Description
New-ADComputer	Creates new computer accounts
Set-ADComputer	Modifies properties of computer accounts
Get-ADComputer	Displays properties of computer accounts
Remove-ADComputer	Deletes computer accounts
Test-ComputerSecureChannel	Verifies or repairs the trust relationship between a computer and the domain
Reset-ComputerMachinePassword	Resets the password for a computer account
Cmdlet	Description

```
New-ADComputer -Name LON-SVR8 -Path  
"ou=marketing,dc=adatum,dc=com -Enabled $true
```

```
Test-ComputerSecureChannel -Repair
```



Cmdlet	Description
New-ADOrganizationalUnit	Creates organizational units
Set-ADOrganizationalUnit	Modifies properties of organizational units
Get-ADOrganizationalUnit	Views properties of organizational units
Remove-ADOrganizationalUnit	Deletes organizational units
New-ADOrganizationalUnit	Creates organizational units
Set-ADOrganizationalUnit	Modifies properties of organizational units
Get-ADOrganizationalUnit	Views properties of organizational units

```
New-ADOrganizationalUnit -Name Sales -Path  
"ou=marketing,dc=adatum,dc=com" -  
ProtectedFromAccidentalDeletion $true
```

Parameter	Description
SearchBase	Defines the AD DS path to begin searching.
SearchScope	Defines at what level below the SearchBase a search should be performed.
ResultSetSize	Defines how many objects to return in response to a query.
Properties	Defines which object properties to return and display.

Operator	Description
-eq	Equal to
-ne	Not equal to
-lt	Less than
-le	Less than or equal to
-gt	Greater than
-ge	Greater than or equal to
-like	Uses wildcards for pattern matching

- Use the pipeline operator (|) to pass a list of objects to a cmdlet for further processing

```
Get-ADUser -Filter 'company -eq "$null"' | Set-ADUser -  
Company "A. Datum"
```

```
Get-ADUser -Filter 'lastlogondate -lt "January 1, 2012"' |  
Disable-ADAccount
```

```
Get-Content C:\users.txt | Disable-ADAccount
```