

Grundlagen: Standards für AD

- zur Verwendung
für das Informatikmodul I 59:
„Directory Services konfigurieren und
in Betrieb nehmen“
- Informatiker, Fachrichtung **Systemtechnik**,
5. Semester
- D. Jenny, daniel.jenny@gbssg.ch,
058-228 26 57, 0043-5574-731 34,
076-450 37 70

Grundlagen: Standards für AD

Eigenschaften Verzeichnisdienst:

- **Skalierbar**: Auch grössere Datenmengen sollten in die Verzeichnisse aufgenommen werden können.
- **Erweiterbar**: Zusätzliche Objekttypen und Inhaltsstrukturen sollten eingefügt werden können.
- **Verfügbar**: Jeder Benutzer muss ständig auf die für ihn relevanten und laufend aktualisierten Daten zugreifen können.
- **Performant**: Der Zugriff auf die benötigten Daten sollte schnell und zuverlässig funktionieren.
- **Sicher**: Es muss gewährleistet sein, dass der Zugriff auf die Informationen nur durch berechtigte Personen erfolgen kann.

[Quelle: «Microsoft Windows Server 2008», Herdt]

R

Grundlagen: Standards für AD

Übersicht:

- X.500: enthält Schema, Domänenmodell, ...
- DNS
- Lightweight Directory Access Protocol (LDAP):
 - Industriestandard von IETF
 - Zugriff von Fremdsystemen auf AD
 - Siehe späteres Kapitel

Grundlagen: Standards für AD

Übersicht:

- **X.500 mit Schema und Domänenmodell**
- DNS
- Lightweight Directory Access Protocol (LDAP):
 - Industriestandard von IETF
 - Zugriff von Fremdsystemen auf AD
 - Siehe späteres Kapitel

X.500 Standard

Eigenschaften:

- bildet die konzeptionelle Grundlage des AD
- Eigenschaften eines Verzeichnisdienstes:
 - Dezentraler Aufbau, "keine Zentrale"
 - Suchmöglichkeit über ganze Struktur
 - Einheitlicher Namenskontext, jedes Objekt hat seinen einzigartigen Platz im Baum
 - Daten sind aufgrund vorgegebener Struktur (Schema) abgelegt; Struktur ist erweiterbar;

X.500 Standard

siehe
Attribut-
Editor

Namensbildung bei Objekten mit DN/RDN:

- Jedes Objekt verfügt über einen eindeutigen Distinguished Name (DN), der sich über alle Ebenen zusammensetzt:
 - DN: KantonSG
 \ GBS
 \ Informatik
 \ Jenny
 - Relative Distinguished Name (RDN) ist der Name in *einer* Ebene, z.B. Informatik

DN

RDN

X.500 Standard

Schema

- Das Schema regelt:
 - Vergabe des DN in festgelegter Struktur:
Kanton SG – GBS – Informatik – Jenny
 - Beschaffenheit der Objektklassen (User):
 - zwingende/optionale Attribute
 - Objektkl. können vererben (Spezial-User)
 - Eigenschaften der Attribute (Vorname, Modellbezeichnung): "Feldlänge", "Feldtyp"

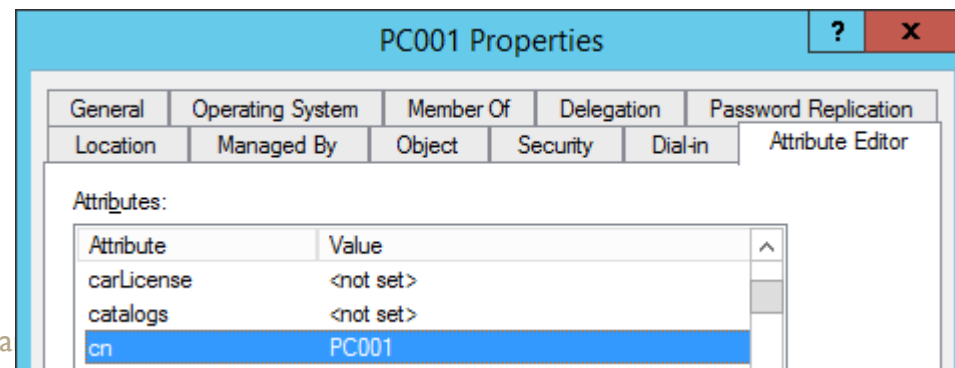
siehe
Schema-
Editor

X.500 Standard

nach-
machen

Attribut-Editor:

- Server-Manager | Tools | AD Users and Computers:
 - in der Domäne neuen Computer «PC001» anlegen
 - View | Advanced Features
 - Rechtsklick auf «PC001» | Properties | Attribute Editor



X.500 Standard

nach-
machen

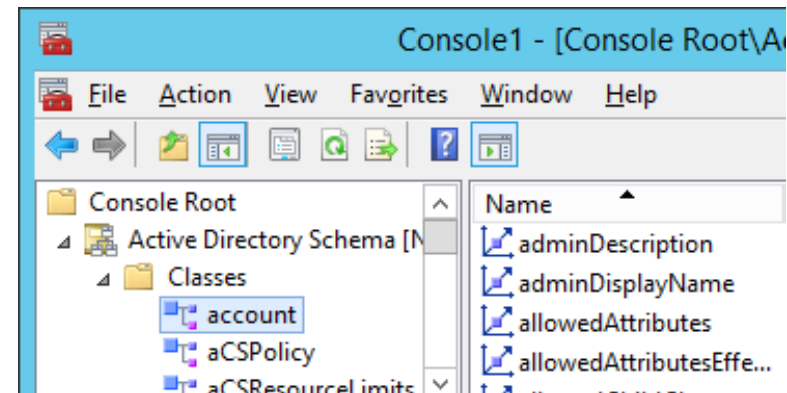
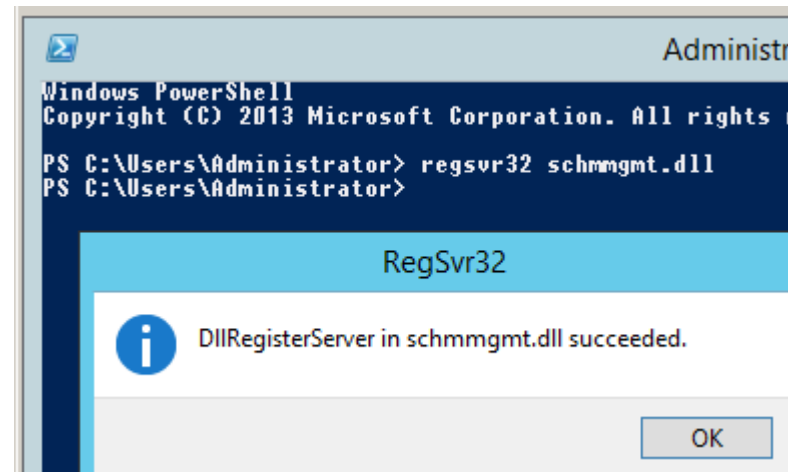
Schema-Editor:

- Der AD-Schema-Editor wird als MMC-Snap-In erst dann ersichtlich, wenn folgender Befehl in der Konsole ausgeführt wurde:

```
regsvr32 schmmgmt.dll
```

- Editor aus der Konsole öffnen:

```
mmc | File  
| Add Snap-in...  
| AD Schema  
| Add >
```



X.500 Standard

Könnte das Schema geändert werden?

- Ja, aber in der Regel vermeidet man Änderungen am Schema.
- Änderungen können nötig werden, wenn neue Software installiert wird.
Es ist allerdings ein Ausweg möglich: Die neue Software erhält ein vorhandenes, aber nicht benutztes Feld zur Benutzung.
- Beachten Sie: In der Regel verfügt eine Kundeninstallationen nur über ein einziges Schema.

X.500 Standard

nach-
vollziehen

Objekt «demopc» im Attribut-Editor:

Organisations-einheit (Built In)

Objektklasse

Objekt-Bezeichnung

Attribut-bezeichn.

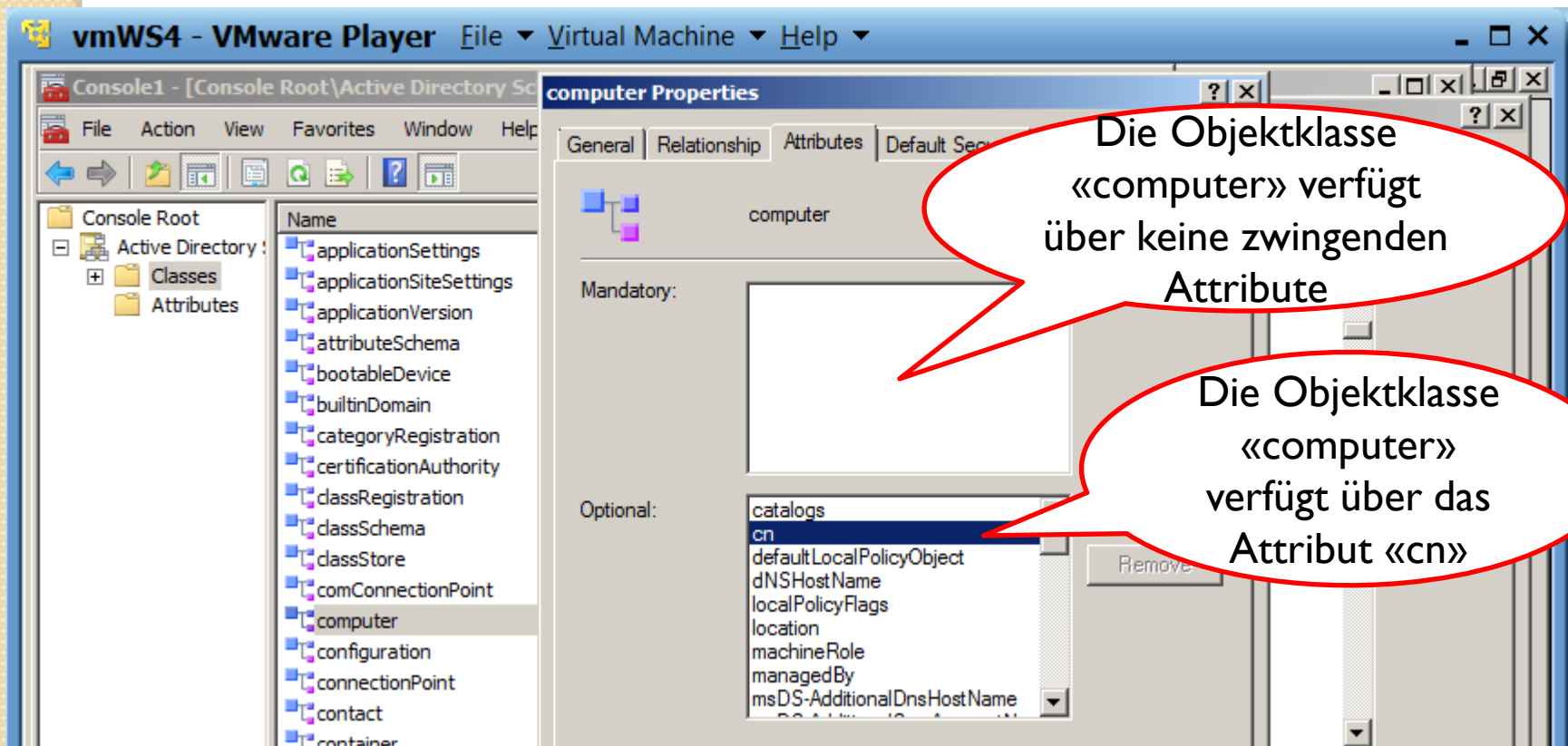
Attributwert

Attribute	Value
c	<not set>
carLicense	<not set>
catalogs	<not set>
cn	demopc
co	<not set>
coPage	0
com	<not set>
com	<not set>
com	<not set>
com	<not set>
com	0
com	<not set>
com	<not set>
com	<not set>
department	<not set>

X.500 Standard

nach-
vollziehen

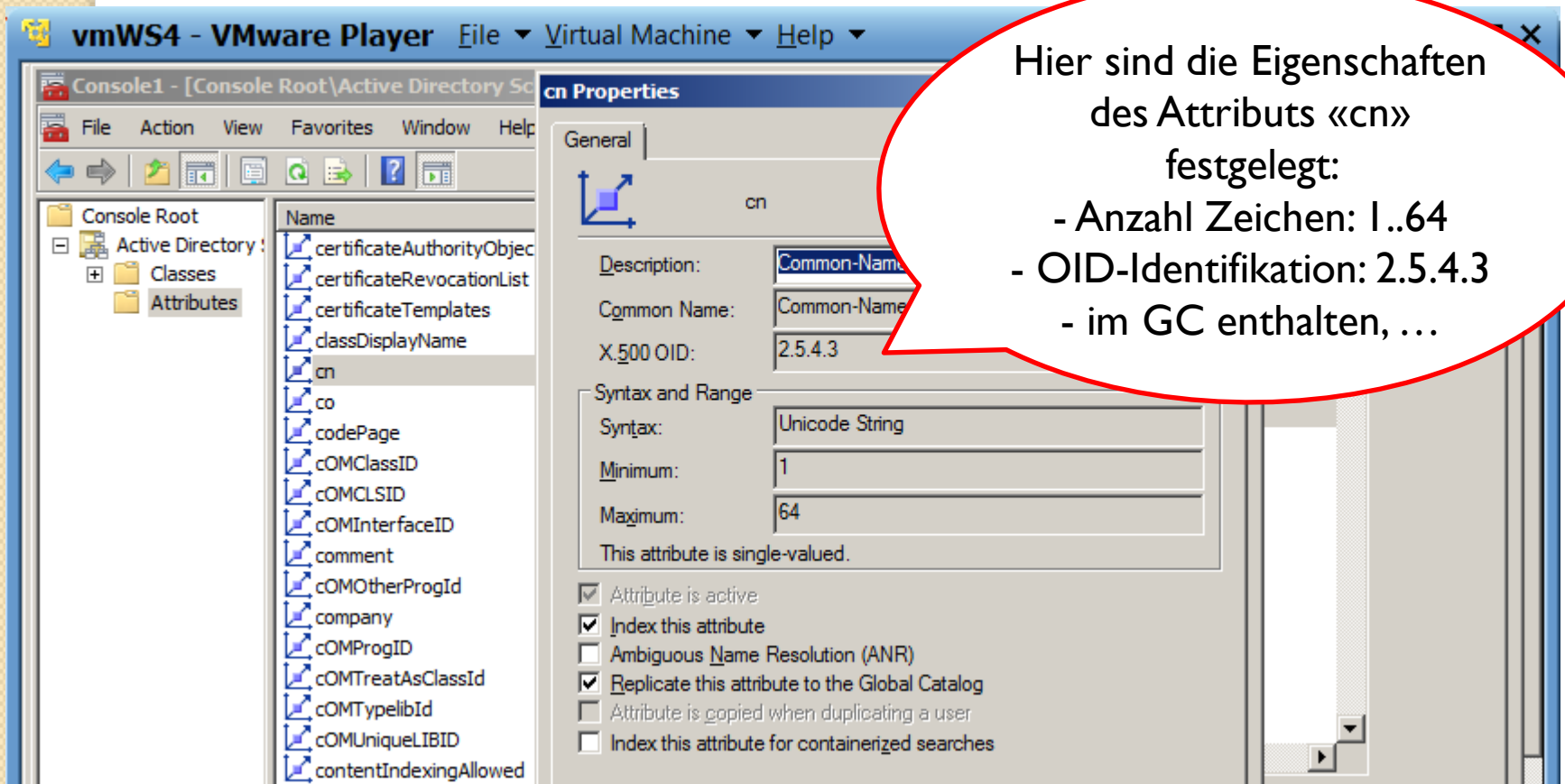
Objektklasse «computer» im Schemaeditor:



X.500 Standard

nach-
vollziehen

Attribut «cn» im Schemaeditor:



The screenshot shows the 'vmWS4 - VMware Player' window with the 'Active Directory Schema Editor' open. The 'cn Properties' dialog box is displayed, showing the following details:

- Name:** cn
- Description:** Common-Name
- Common Name:** Common-Name
- X.500 OID:** 2.5.4.3
- Syntax and Range:**
 - Syntax:** Unicode String
 - Minimum:** 1
 - Maximum:** 64
- This attribute is single-valued.**
- Attribute is active:** ☒
- Index this attribute:** ☒
- Ambiguous Name Resolution (ANR):** ☐
- Replicate this attribute to the Global Catalog:** ☒
- Attribute is copied when duplicating a user:** ☐
- Index this attribute for containerized searches:** ☐

A red speech bubble points to the dialog box with the following text:

Hier sind die Eigenschaften des Attributs «cn» festgelegt:

- Anzahl Zeichen: 1..64
- OID-Identifikation: 2.5.4.3
- im GC enthalten, ...

X.500 Standard

nach-
vollziehen

Attribute...

- ...definieren die Eigenschaften der Felder der Klassen, wie
 - Byte
 - numerisch
 - Unicode-Zeichenfolge
 - Gross-/Kleinschreibung beachten
 - Zeit
 - SID
 - Adresse

X.500 Standard

nach-
vollziehen

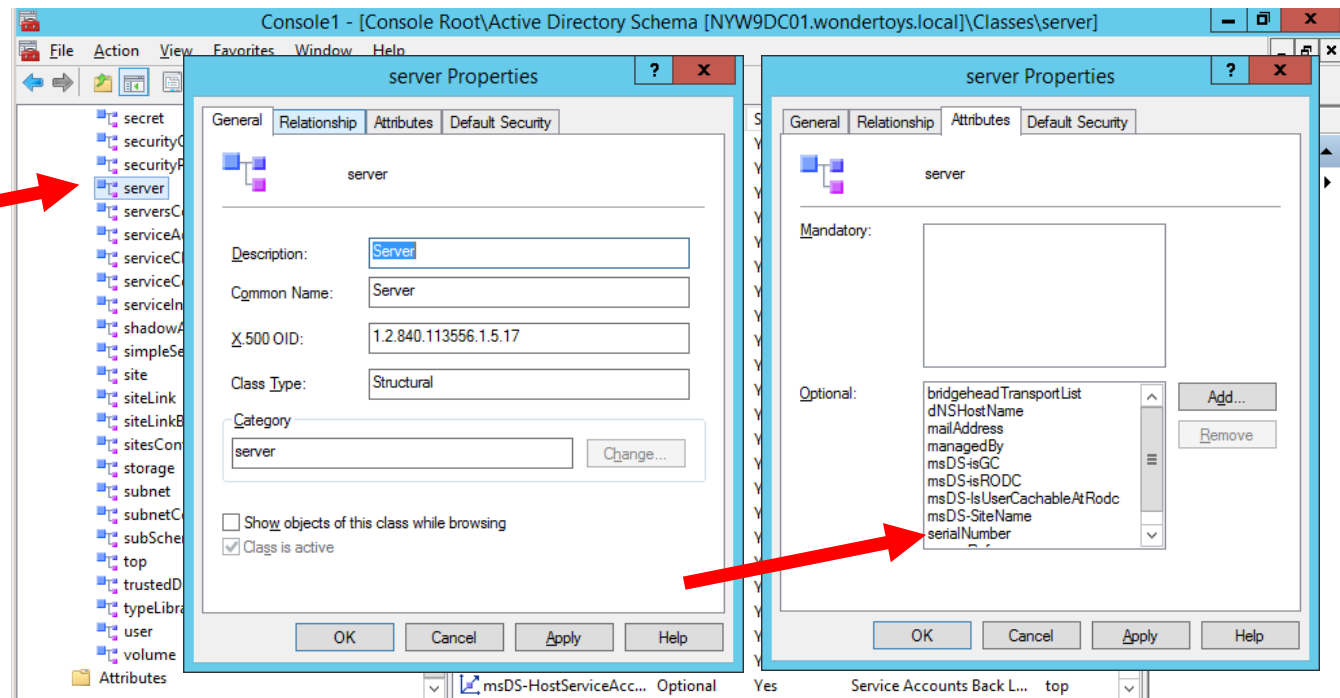
Klassen...

- ...definieren Eigenschaften der Objekte, wie
 - Computer
 - Benutzer
 - Örtlichkeit, wie Standort
 - Gruppe
 - Drucker-Warteschlange

X.500 Standard

nach-
vollziehen

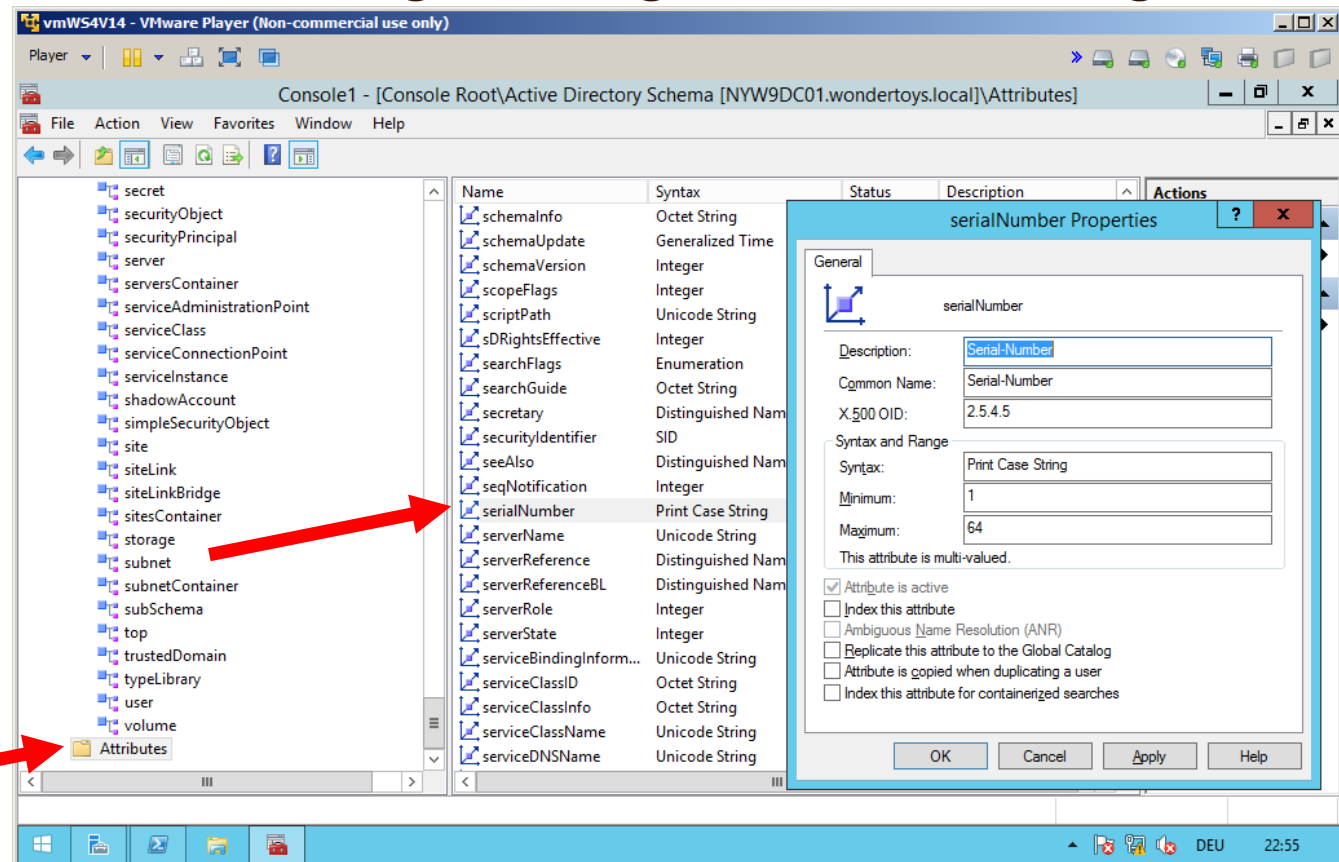
Weiteres Beispiel: Die Objektklasse «server» besteht u.a. aus dem Attribut «serialNumber», ...



X.500 Standard

nach-
vollziehen

... das über folgende Eigenschaften verfügt:



X.500 Standard

Was ist eine OID?

- Dies ist ein Object Identifier (OID) und wird in Normen, wie X.500 und SNMP, verwendet.

[Quelle: <https://msdn.microsoft.com/en-us/library/ms677614%28v=vs.85%29.aspx>]

- Beispiel für «user class»: 1.2.840.1.13556.1.5.9:

Wert	Bedeutung
1	ISO
2	ANSI
840	USA
1.13556	Microsoft
1	Active Directory
5	Classes
9	user class

X.500 Standard

Wo werden OIDs im Schema eingesetzt?

- Objektklassen und Attribute werden durch eine OIDs identifiziert.
(Zum Unterschied: Objekte erhalten eine SID)

X.500 Standard

3.2 X.500 Standard – Umsetzung im AD

- X.500 verwendet Single-Master-Replikation: ein Primary (mit Original) und mehrere Secondary (verfügen über Kopie). Änderungen sind nur im Primary möglich. → Modell begrenzt
- AD verwendet Multi-Master-Replikation: mehrere Master verwalten das Original → Konfliktsituationen müssen geregelt werden. (Aber: Sensible Vorgänge, wie die FSMO-Rollen, sind ohne Multi-Master-Replikation.)

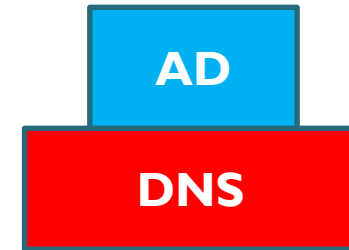
R

Grundlagen: Standards für AD

Übersicht:

- X.500 mit Schema und Domänenmodell
- **DNS**
- Lightweight Directory Access Protocol (LDAP):
 - Industriestandard von IETF
 - Zugriff von Fremdsystemen auf AD
 - Siehe späteres Kapitel

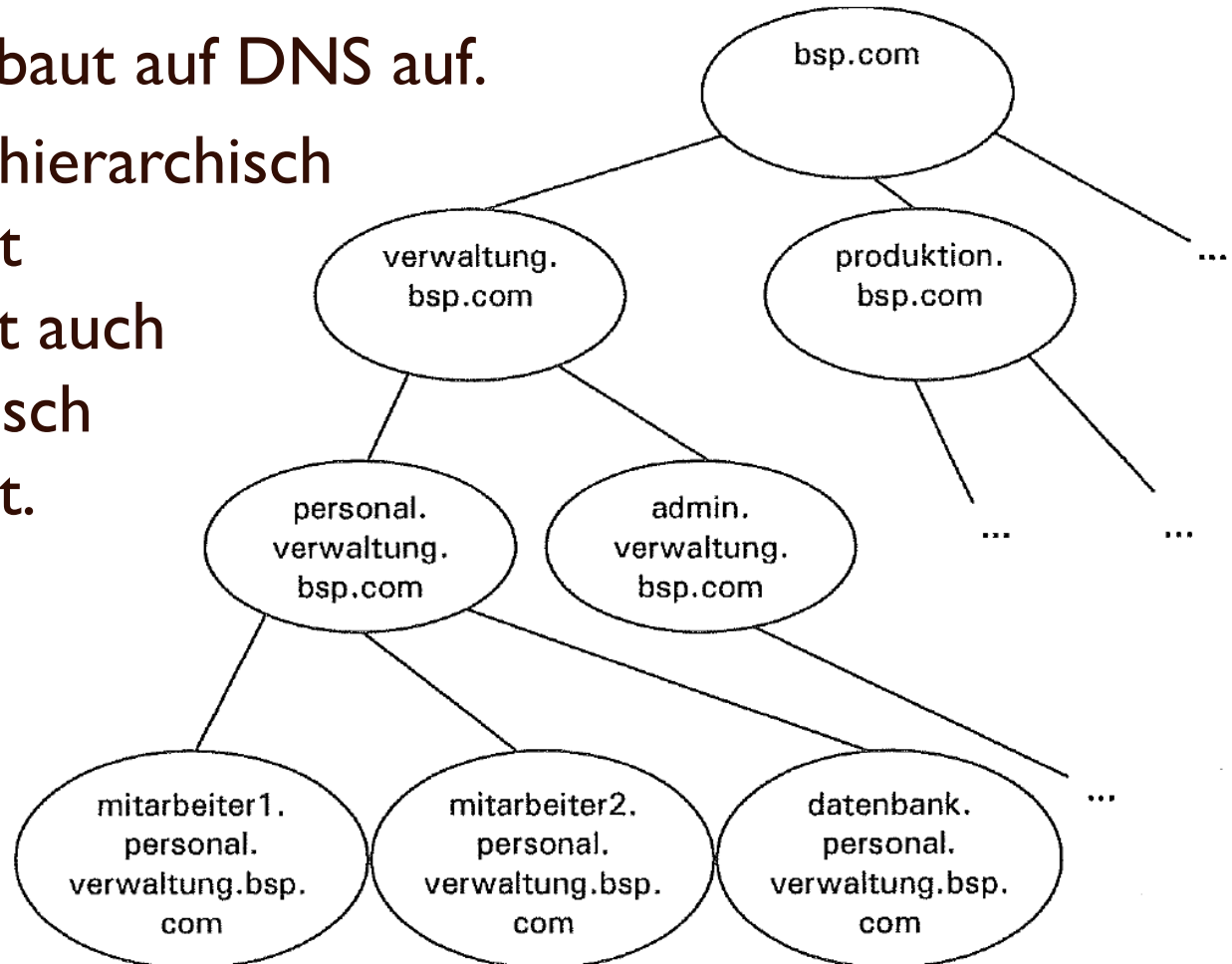
DNS



Das AD baut auf DNS auf.

DNS ist hierarchisch
aufgebaut

→ AD ist auch
hierarchisch
aufgebaut.



DNS

DNS-Eigenschaften:

- basiert auf TCP/IP-Protokoll
- Eine DNS-Domäne, z.B. «nesa-sg.ch», ist eine Verwaltungseinheit, die andere DNS-Subdomänen enthalten kann, z.B. «gbs».
→ Der Fully Qualified Domain Name (FQDN) lautet dann: «gbs.nesa-sg.ch»
- Die DNS-Domäne kann Mitglied einer übergeordneten DNS-Domäne sein: Die Domäne «nesa-sg.ch» ist ein Teil der «ch»-Domäne.

DNS

nach-
machen

Zonen sind «unsere» Domänen:

- Eine **Zone** ist der Teilbereich einer DNS-Domäne, der **von unserem eigenen DNS-Server verwaltet** wird.
- Zonen auf DNS-Server einsehen: Server-Manager | Tools | DNS | Forward Lookup Zones | Zonename auswählen | Kontextmenü | Properties | General | Type:
 - Primary mit Store... → AD integrated
 - Primary ohne Store... → DNS traditionell
 - Secondary → DNS traditionell

DNS

Zonentypen:

1. Primäre Zone: enthält das "Original" der Zonendaten (Webserver-Name, -IP)
2. Sekundäre Zone:
 - enthält eine "Kopie"
 - Der Secondary fragt periodisch beim Primary nach, ob sich die Zone verändert hat. Falls ja, verlangt der Secondary die Übertragung der ganzen Zone.

DNS

3. Zonen können im AD integriert werden:
 - Im AD kann eine DNS-Zone anstelle Single-Master als Multimaster verwaltet werden (i. G. zu: Das DNS verlangt Single-Master):
 - Damit können mehrere DNS-Server die Zone ändern. Wegen der Replikation wird die Änderung auf die anderen übertragen.
 - Diese Zone heisst «AD integrierte Zone».
 - Empfehlenswerte Lösung bei AD

DNS

Servertypen:

- Primary/Secondary-DNS-Server:
DNS verlangt im Internet mind. 2 DNS-Server pro Domäne, d.h. 1 Primary und mind. 1 Second.
- Der gleiche Server kann für die Zonen A, B und C ein Primary und für X, Y und Z Secondary sein.
- DNS-Server mit AD sind in der Regel nur im internen Netz zu finden. Diese DNS-Server können Zonen als Primäre Zone, Sekundäre Zone oder AD integrierte Zone verwalten.

DNS

Bedingte Weiterleitung:

- Bedingte W.: Für die aufgeführten Domänen ist hinterlegt, an welchen DNS-Server die Anfrage weitergeleitet werden soll:
Suche nach Domäne X → statische Weiterleitung an DNS-Server Y (IP wird hinterlegt)
- DNS-Manager | im linken Fenster den Server anklicken | im rechten Fenster erscheint «Conditional Forwarders»
| Kontextmenü «New ...»

nach-
machen

DNS

Unbedingte Weiterleitung:

- Kann eine Anfrage nicht anhand **eigener** Zonen oder des Caches beantwortet werden, wird sie an den angegebenen DNS-Server weitergeleitet. Dies ist in der Regel der DNS-Server des ISP.
- DNS-Manager | im linken Fenster den Server anklicken | Properties | Forwarders: Hier kann eine IP-Adresse angegeben werden.

nach-
machen

DNS

Caching unterstützt die Namensauflösung: Ein aufgelöstes Paar Name/IP wird für eine gewisse Zeit zwischengespeichert.

- Server-Caching: in der Regel aktiv
- Caching-Only-DNS-Server: Server ohne Zone; dient der Zwischenspeicherung (Bsp. Schule); macht nur unbedingte Weiterleitung;
- Client-Caching: Resolver des Clients merkt sich die letzten DNS-Anfragen und deren Ergebnisse:
`ipconfig /displaydns`

nach-
machen

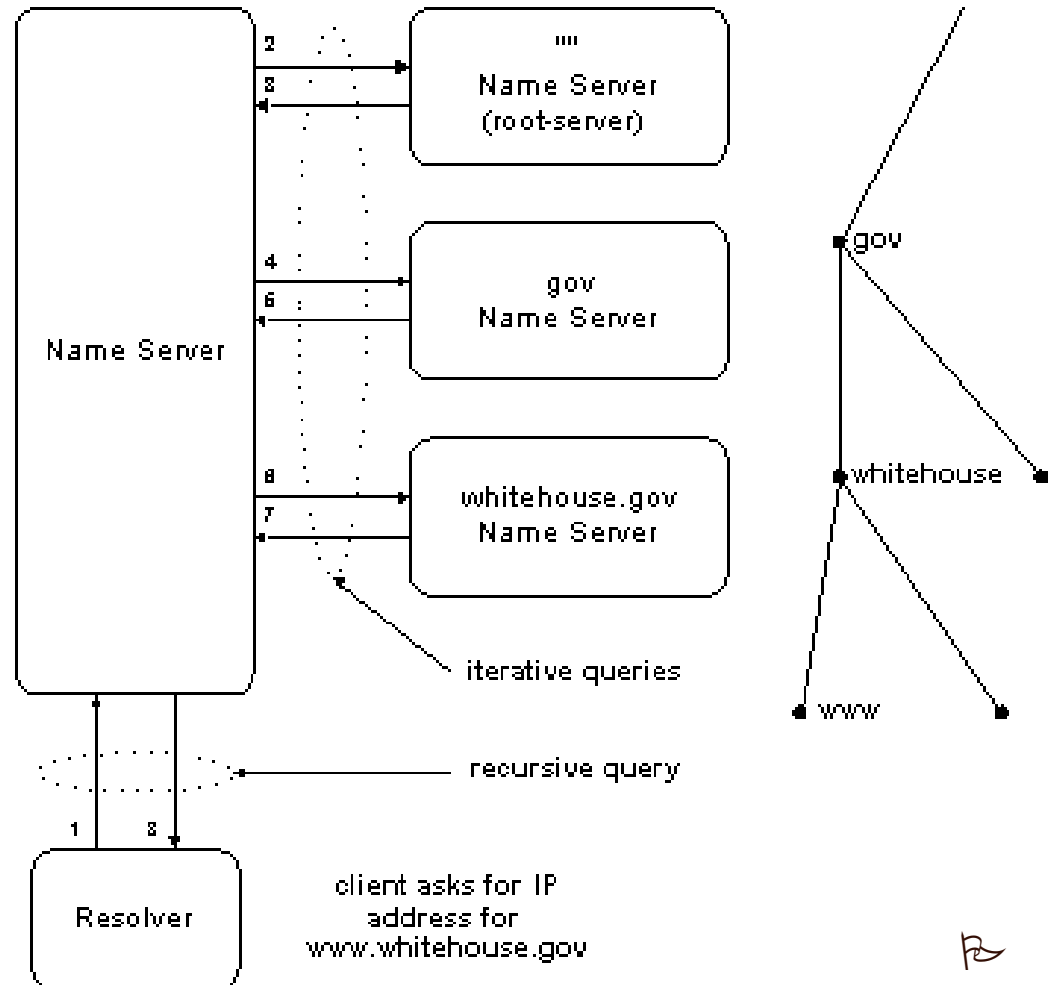
DNS

Schritte der Namensauflösung: 1/2

- rekursive Ermittlung: Der angefragte DNS-Server (des ISP) führt die Suche zu Ende und gibt das **vollständige** Resultat dem DNS-Client zurück.
- iterative Ermittlung: Der (vom DNS des ISP) angefragte DNS-Server gibt nur das zurück, was er weiss. Der DNS-Server (des ISP) weiss nun mehr, aber noch nicht alles. Somit muss er in einem **nächsten Schritt** den nächsten DNS-Server anfragen.

DNS

Schritte der Namens- auflösung: 2/2



Bildquelle:
<http://www.it-zeugs.de/images/image006.gif>

Grundlagen: Standards für AD

Übersicht:

- X.500 mit Schema und Domänenmodell
- DNS
- **Leightweight Directory Access Protocol (LDAP):**
 - Industriestandard von IETF
 - Zugriff von Fremdsystemen auf AD
 - Siehe späteres Kapitel

RR

Grundlagen: Domäne u. Standort

- zur Verwendung für das Informatikmodul I 59: „Directory Services konfigurieren und in Betrieb nehmen“
- Informatiker, Fachrichtung **Systemtechnik**, 5. Semester
- D. Jenny, daniel.jenny@gbssg.ch,
058-228 26 57, 0043-5574-731 34,
076-450 37 70

Grundlagen: Domäne u. Standort

Überblick:

- Domänenmodell
- Domänenstruktur (tree)
- Gesamtstruktur (forest)
- Standort (site)

Grundlagen: Domäne u. Standort

Überblick:

- **Domänenmodell**
- Domänenstruktur (tree)
- Gesamtstruktur (forest)
- Standort (site)

Domänenmodell

Eigenschaften Domänen 1/3:

- Arbeitsgruppen \Leftrightarrow Domäne:
 - A.G. enthalten gleichberechtigte PCs.
 - Domänen weisen den Ordnern die spezifischen Rechte für Gruppen/User zentral zu.
- Weitere Domänen können bei Bedarf hinzugefügt werden.
- **Empfehlung: So wenig Domänen wie möglich!**



Domänenmodell

Eigenschaften Domänen 2/3:

- Für die meisten Fälle wird 1 Domäne geplant.
- Nur in folgenden Fällen muss mehr als 1 Domäne vorgesehen werden:

- eigene Sicherheitszone
- autonome Verwaltung
- Gewünschter Schutz des Schemas, indem in Stamm-Domäne keine IT-Objekte vorhanden sind → Niemand aus «bsp.ch» kann Schema ändern.

Ohne Objekte
schutz.schema

bsp.ch



Site



Organizational Unit

Bildquelle: <http://conceptdraw.com/examples/computer-security>



Domänenmodell

Eigenschaften Domänen 3/3:

- Domänengrenzen sind Sicherheitsgrenzen:
 - Der Admin der übergeordneten Domäne hat nicht automatisch alle Rechte.
 - Die Objekte (z. B. Server, Clients, Benutzer) werden wegen dem gemeinsamen Namenskontext schnell gefunden.
- Einer Benutzergruppe können domänenübergreifende Berechtigungen für Verwaltungsaufgaben auf Objekte erteilt werden.

Domänenmodell

Eigenschaften Domänenkontrollen (DC):

- Ohne DC gibt es keine Domäne.
- Warum mehr als 1 DC? → Vermeiden des Single Point of Failure und Leistungsbedarf
- **Empfehlung: Mind. 2 DCs pro Domäne.**
- wenn mehrere DCs: Jeder DC schreibt auf AD, Synchronisierung mit Multi-Master Replikation
- Jeder DC enthält alle Objekte **aller** Domänen.
Ausnahme: Read Only DC (RODC):
Nicht alle Objekte werden repliziert.



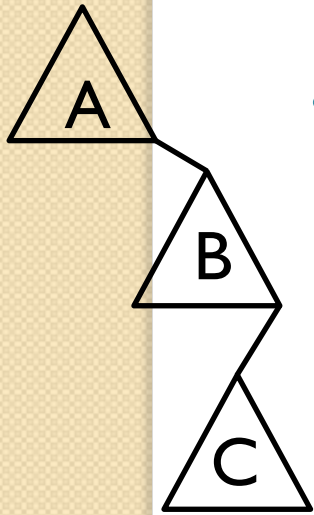
bsp.ch



bsp.ch

Domänenmodell

Vertrauensstellung zwischen unter- und übergeordneten Domänen:



- Die Vertrauensstellung wird standardmässig wie folgt eingerichtet:
 - implizit, d.h. automatisch
 - bidirektional, d.h. in beide Richtungen
 - transitiv, d.h. wenn $A \rightarrow B$ vertraut und $B \rightarrow C$ vertraut, \Rightarrow dann vertraut auch $A \rightarrow C$ (Der Datenzugriff erfolgt in Gegenrichtung zur Vertrauensrichtung.)

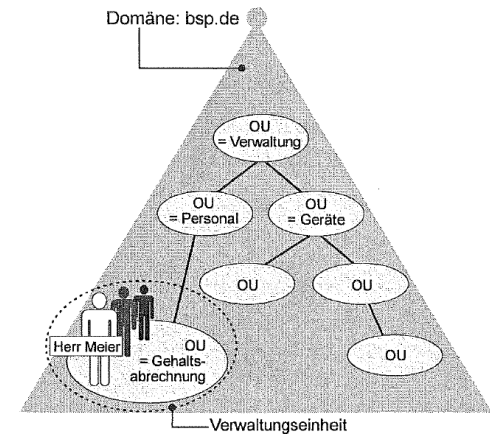
Domänenmodell

Regeln für Domännennamen:

- Jede Domäne verfügt über einen FQDN-Namen:
 - Beispiel: «verwaltung.gbssg.ch»
- NetBIOS-Namen können beim Anmelden oder bei der Suche auch verwendet werden:
 - Beispiel: «verwaltung»

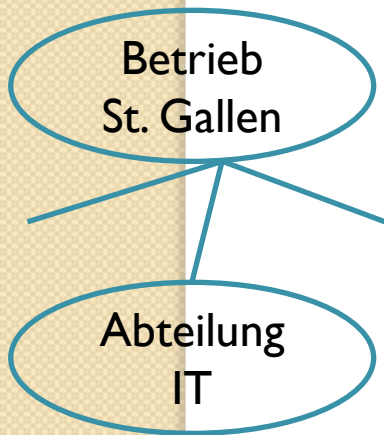
nach-
machen

Domänenmodell



Organisational Unit (OU) 1/2:

- OUs bieten beliebige Unterteilung in einer Domäne für eigene Unternehmen, Abteilungen
- OU kann Benutzer, Drucker usw. enthalten.
- Strukturierungsmöglichkeiten:
 - Abbilden der Firmenstruktur durch OUs
 - Zuweisen von Verwaltungstätigkeiten an andere Personen durch Admin
 - Gruppenrichtlinien: auf OU anwenden
 - Sichtbarkeit: nur Benutzer mit Leseberechtigung für OU sehen OU-Inhalt



Domänenmodell

Organisational Unit (OU) 2/2:

- Server-Manager | Tools | AD Users and Computers:
 - Domäne wählen | Kontextmenü | New | Organizational Unit | Name der OU erfassen
 - Soll OU wieder gelöscht werden:
 - View | Advanced Features einschalten
 - Kontextmenü der OU | Properties | Object | Protect object ... deaktivieren

nach-
machen

Grundlagen: Domäne u. Standort

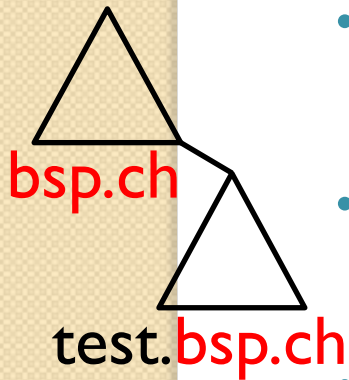
Überblick:

- Domänenmodell
- **Domänenstruktur (tree)**
- Gesamtstruktur (forest)
- Standort (site)

Domänenstruktur (tree)

Domänenstruktur (Tree, Domänenbaum):

- kontinuierlicher Namenskontext: **bsp.ch**, **test.bsp.ch**, **produktion.bsp.ch**
- DC mit Global Catalog (GC) enthält wichtige Informationen aller Objekte.
- Das Schema ist für alle gleich. Es gibt nur eine Stamm-Domäne. So wenig Domänen wie möglich!



Grundlagen: Domäne u. Standort

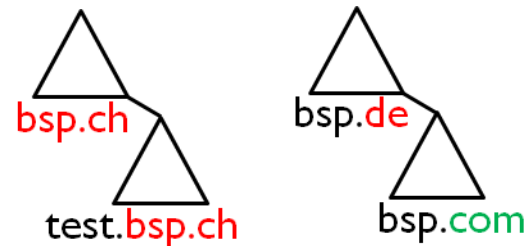
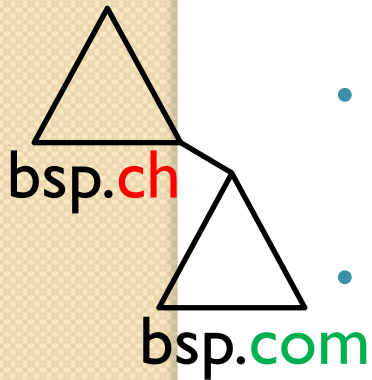
Überblick:

- Domänenmodell
- Domänenstruktur (tree)
- **Gesamtstruktur (forest)**
- Standort (site)

Gesamtstruktur (forest)

Gesamtstruktur (Forest, Domänenwald):

- Verbindung von mehreren Domänenstrukturen → unterschiedliche Namensräume werden verbunden: bsp.ch + bsp.com.
- DC mit GC enthält wichtige Informationen aller Objekte.
- Das Schema ist für alle gleich. Es gibt nur eine Stamm-Domäne. So wenig Domänen wie möglich!
- kein Unterschied für AD:



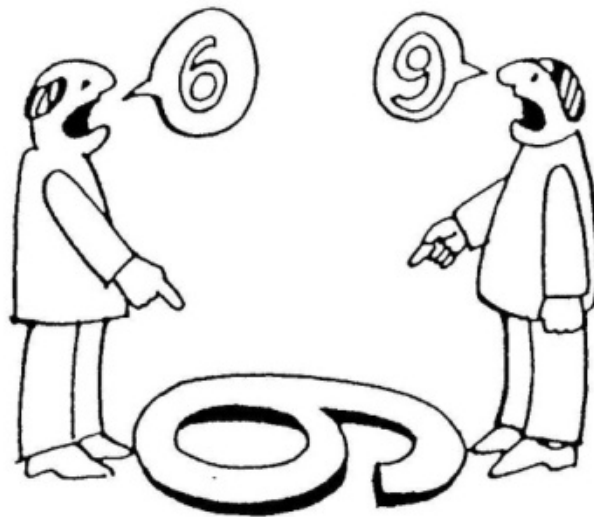
Grundlagen: Domäne u. Standort

Überblick:

- Domänenmodell
- Domänenstruktur (tree)
- Gesamtstruktur (forest)
- **Standort (site)**

Standort (site)

Wir wissen, dass die Realität je nach Sichtweise unterschiedlich wahrgenommen werden kann:



[Bildquelle: <http://www.psychoweb.net/erich/angebot/kommunikation/index.php>]



[Bildquelle: <http://www.caritas-linz.at/aktuell/news/news/artikel/1036/735/>]

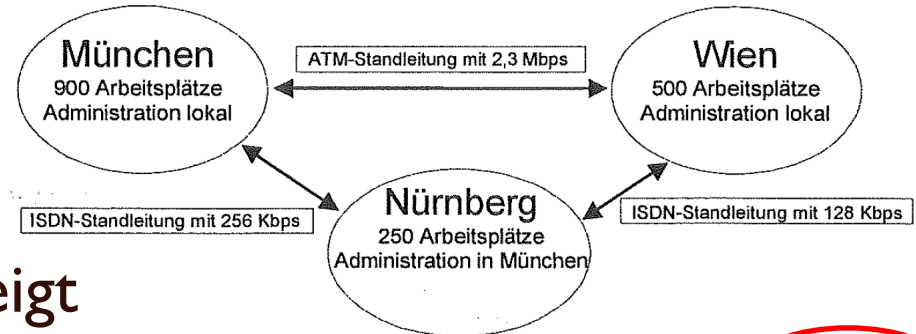
Standort (site)

unterschiedliche Sichtweisen:

- logische Sicht → Domänen:
 - Der Aufbau wirkt sich auf die Namensgebung und auf die Benutzer aus.
 - Aufgabe: Rechte/GPO/... werden zugeteilt.
- physische Sicht → Standorte:
 - Lösung ist für Benutzer unsichtbar.
 - Aufgabe: Replikation wird optimiert

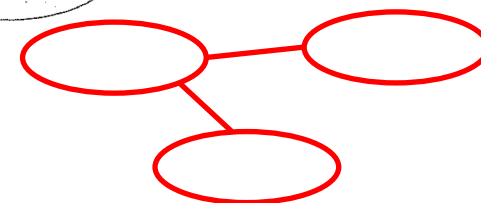
Standort (site)

Redundanz vorhanden → gut



Eigenschaften:

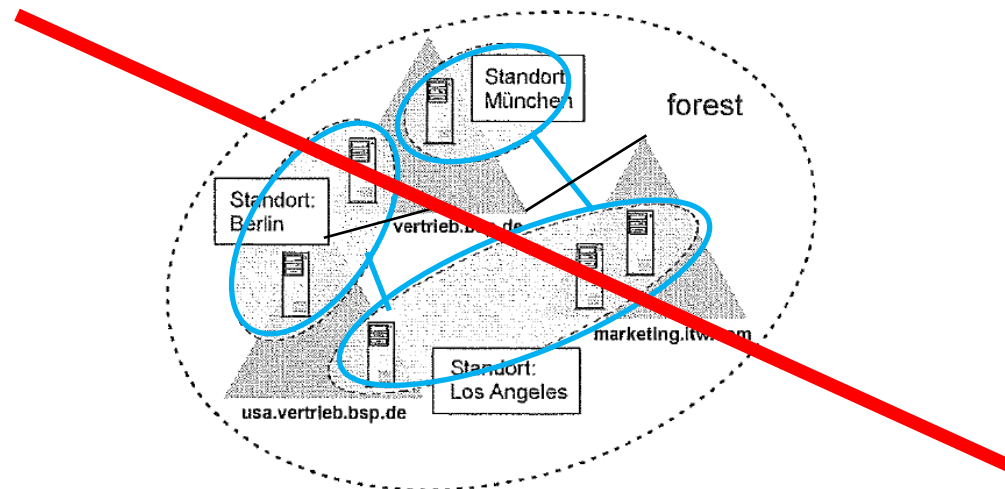
- physische Sicht zeigt Standorte als **Ellipsen** und WAN-Strecken als **Striche**.
- Replikation: **Keine Redundanz vorhanden → kritisch**
 - innerhalb eines S.: schnell, häufig, automat.
 - zwischen den S.: langsam und selten
- Jeder S. hat ein eigenes IP-Subnetz. → Die S. müssen mit Routern verbunden werden.
- Redundante Strecken sind erwünscht.



Standort (site)

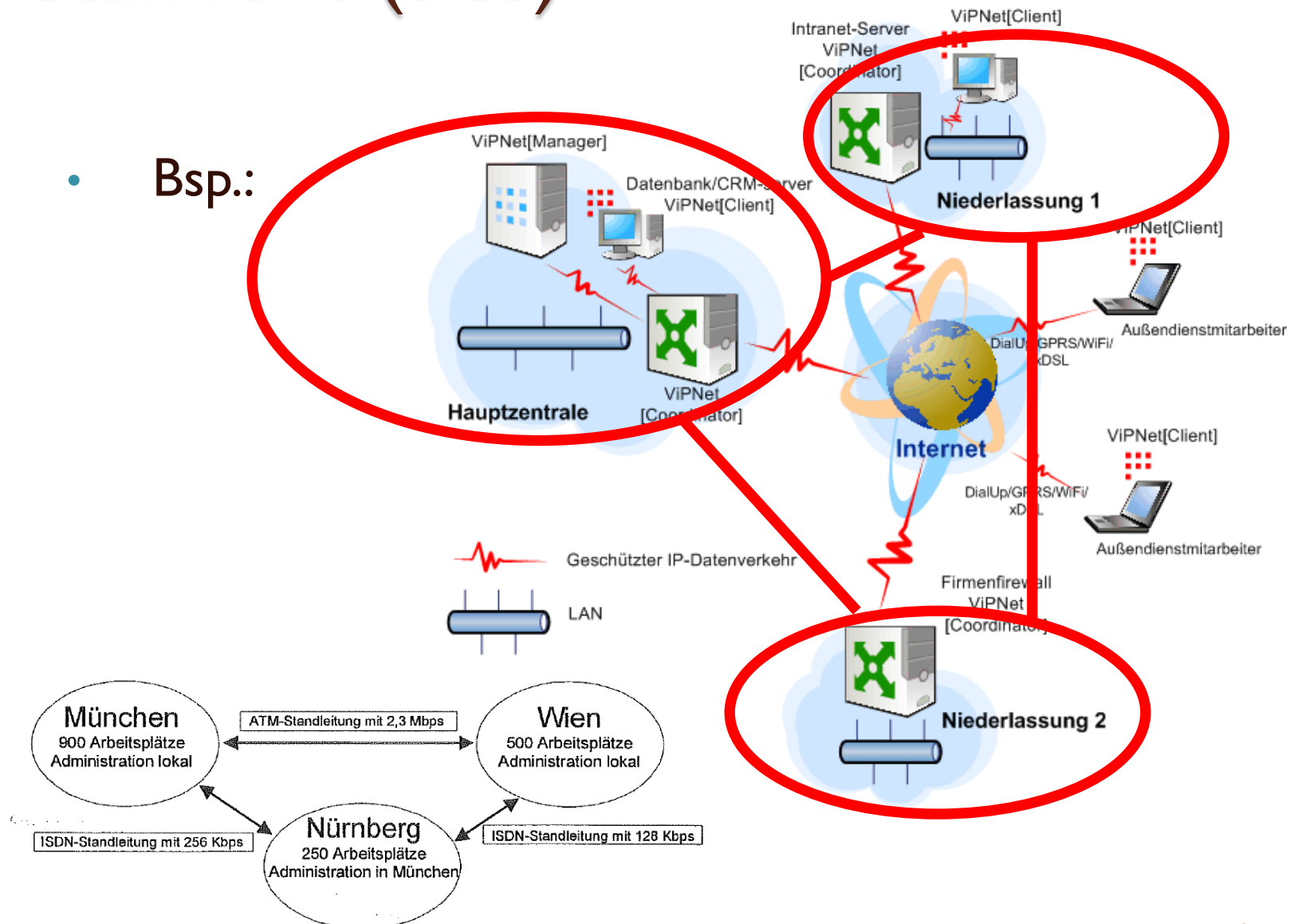
Kombinierte Zeichnung mit Domänen und Standorten?

- Darstellungen mit logischer **und** physischer Sicht wirken unübersichtlich und sind deshalb zu meiden → 2 separate Skizzen nötig:



Standort (site)

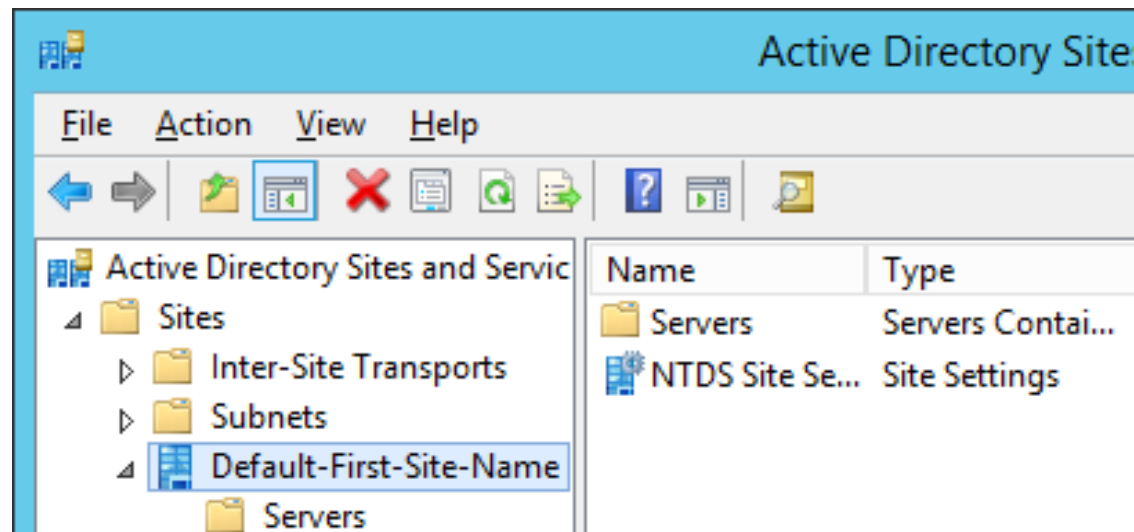
• Bsp.:



Standort (site)

Standort einrichten:

- Server-Manager | Tools | AD Sites and Services:
- «Default-First-Site-Name» ist ein Standort.



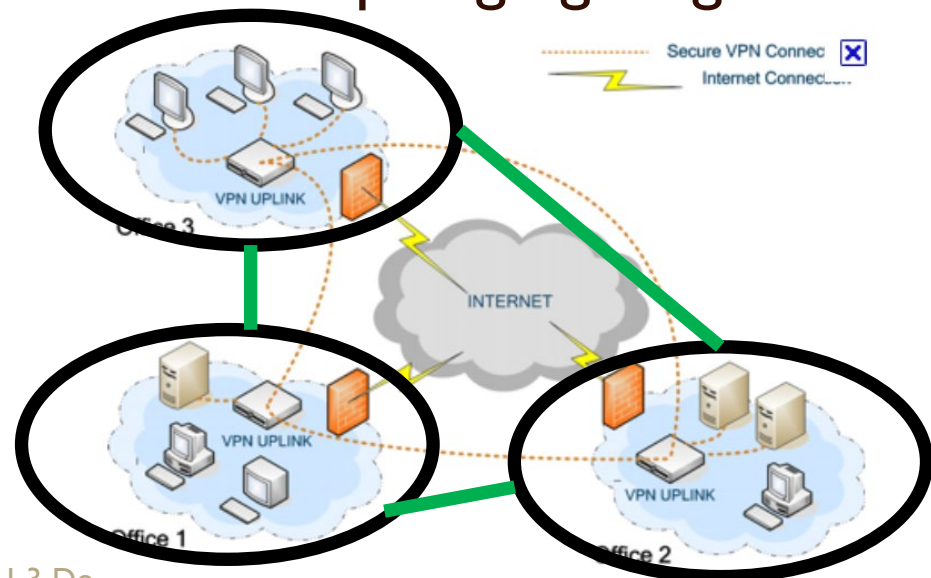
- weitere Standorte über Kontextmenü möglich

Standort (site)

Server-Manager | Tools | AD Sites and Services | Sites
| Inter-Site Transport | IP | DEFAULTIPSITELINK:

nach-
vollziehen

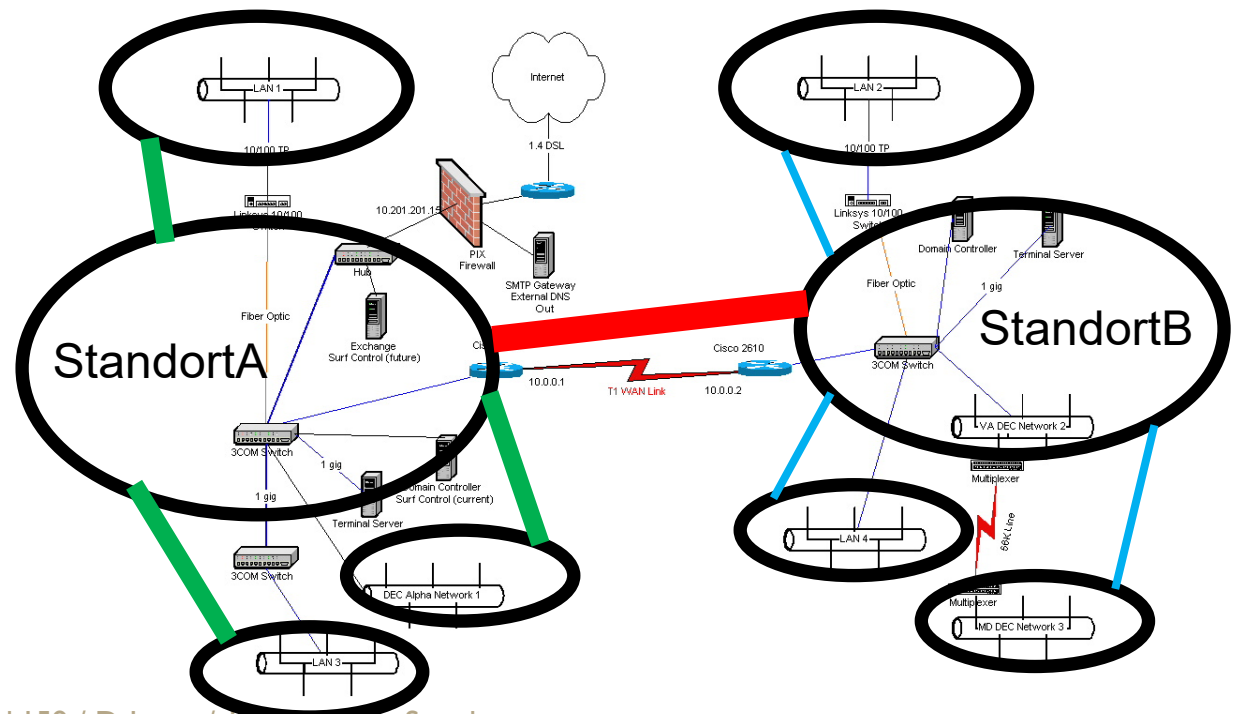
- 3 Standorte mit gleichwertigen, d. h. gleich schnellen Verbindungen
→ Eine «Standortverknüpfung» genügt:



Standort (site)

8 Standorte mit **ungleichen** Verbindungen:

- Die Verbindungen sind unterschiedlich schnell.
→ Es sind 3 «Standortverknüpfungen» nötig:

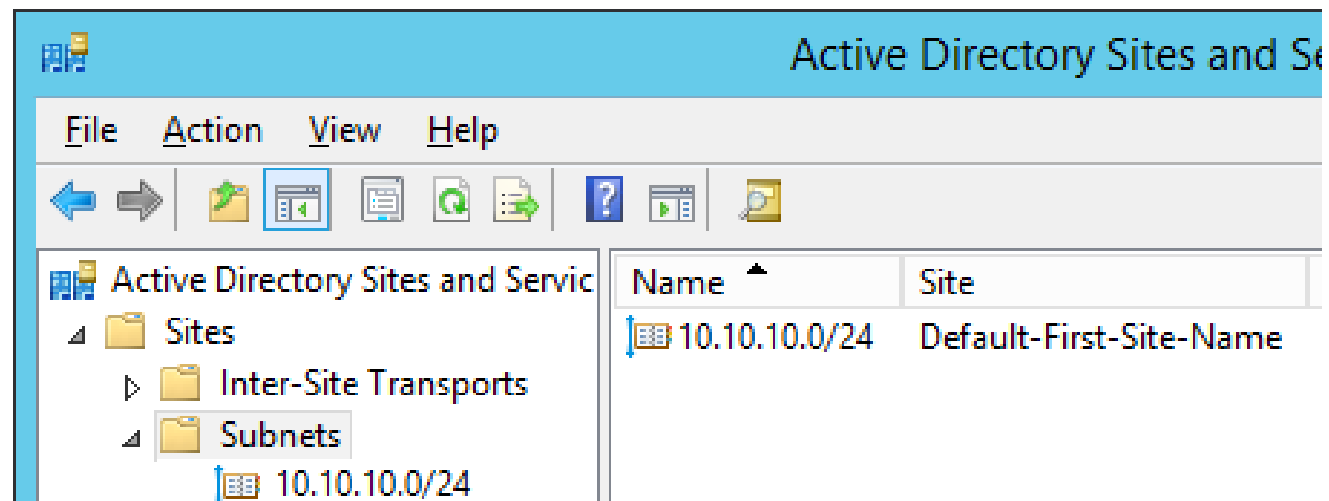


Standort (site)

Jeder Standort (Default-First-Site-Name) hat sein eigenes Subnetz (10.10.10.0/24):

- Server-Manager | Tools | AD Sites and Services | Sites | Subnets:

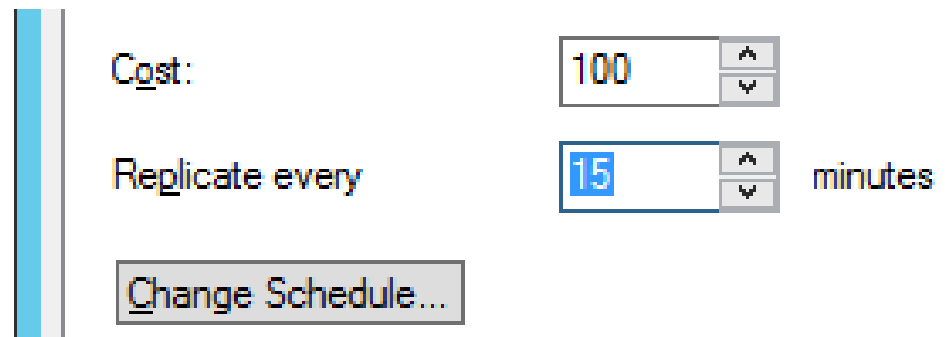
nach-
vollziehen



Standort (site)

Die Replikation zwischen den Standorten findet nicht dauernd statt. Nach einer erfolgten Replikation wird eine Pause von mind. 15 Minuten eingelegt:

- Server-Manager | Tools | AD Sites and Services
| Sites | Inter-Site Transport | IP
| DEFAULTIPSITELINK | Kontextmeü
| Properties:



Cost: 100

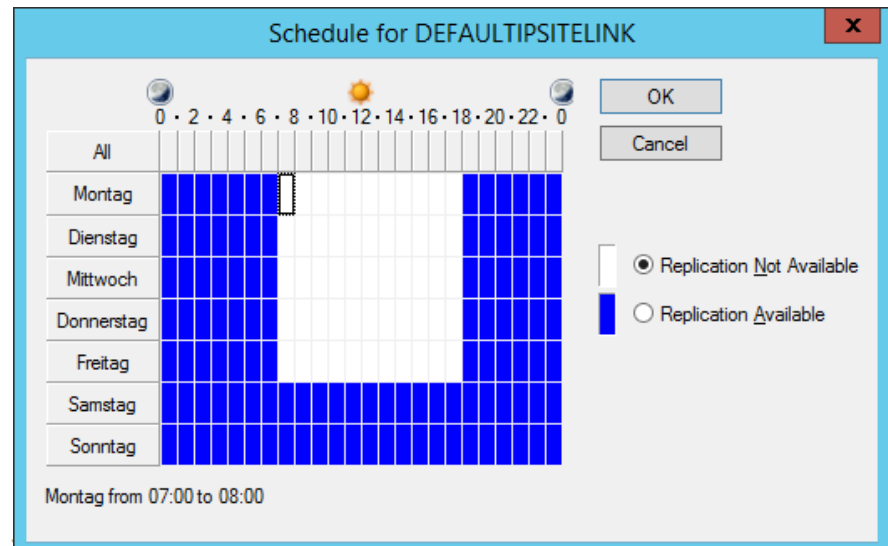
Replicate every 15 minutes

Change Schedule...

Standort (site)

Für jede Standortverknüpfung können die Replikationsfenster festgelegt werden:

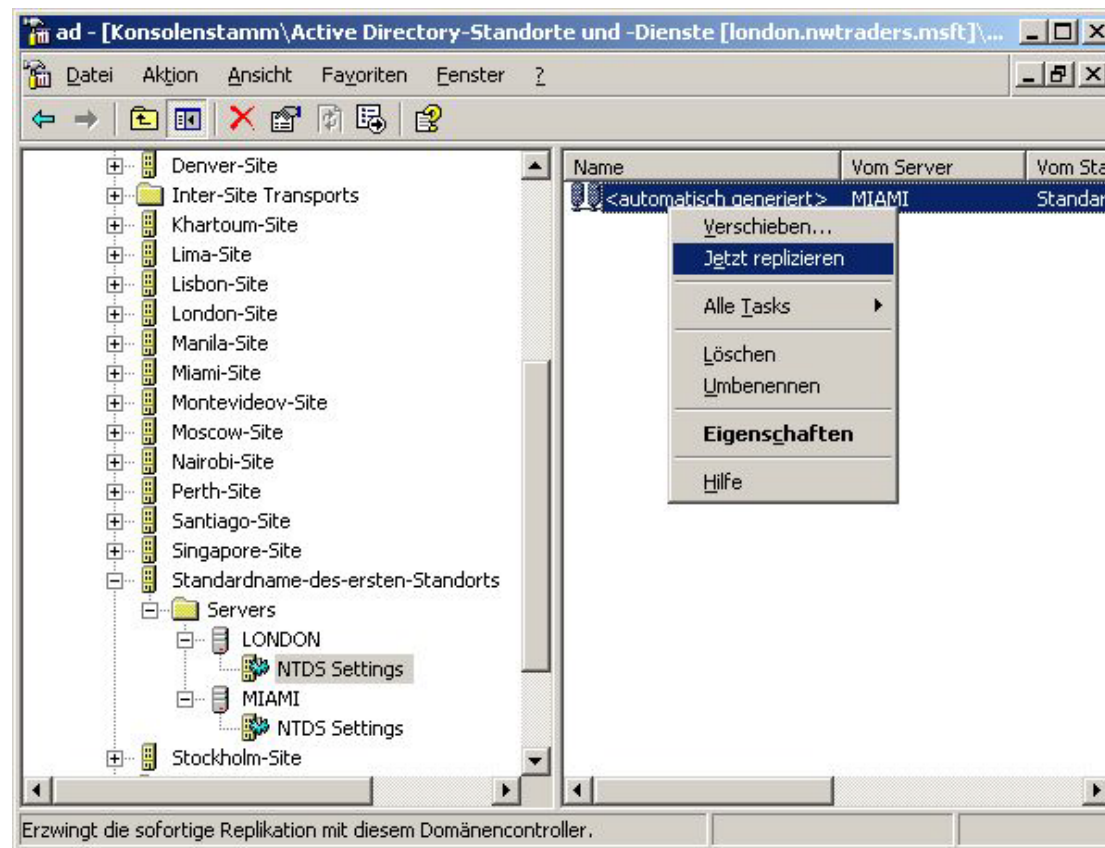
- Server-Manager | Tools | AD Sites and Services
| Sites | Inter-Site Transport | IP
| DEFAULTIPSITELINK | Kontextmeü
| Properties
| General
| «Change
Schedule...»



Standort (site)

(Erst praktisch
nachvollziehbar,
wenn 2 Standorte
vorhanden sind.)

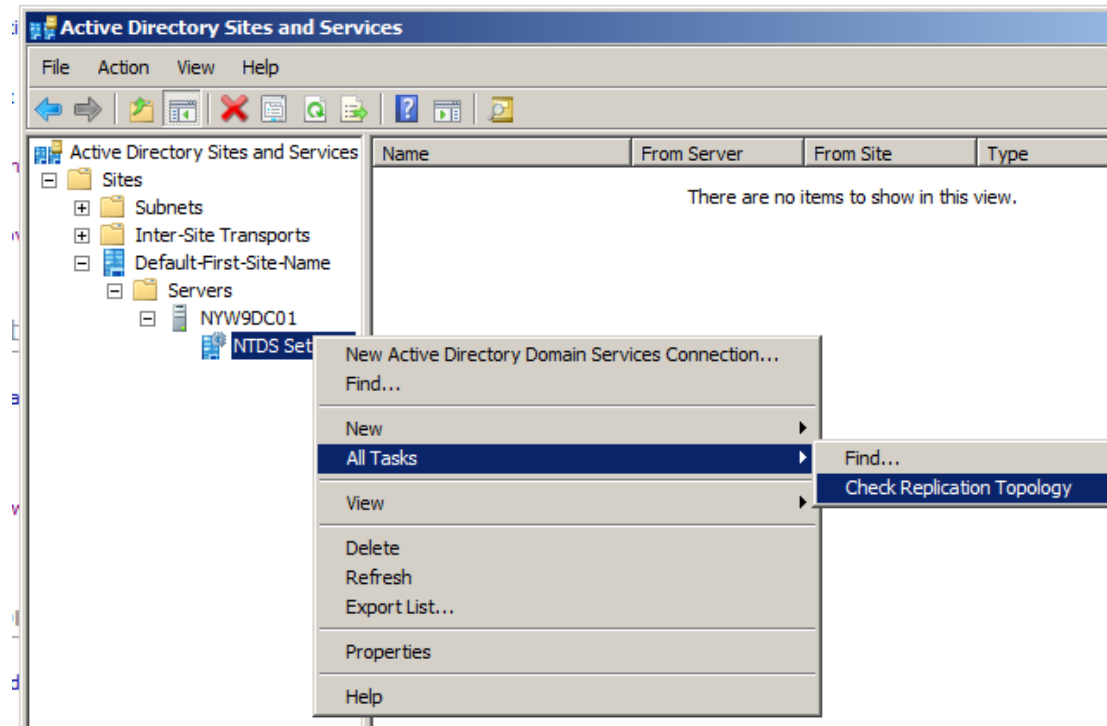
Replikation manuell anstossen:



Bildquelle:
<http://www.mcse-certification.de/archive/s/121-Replikation-mit-dem-Domänen-Controller-erzwingen.html>

Standort (site)

- Replikationstopologie überprüfen:



- Replikation überwachen: RepAdmin.exe

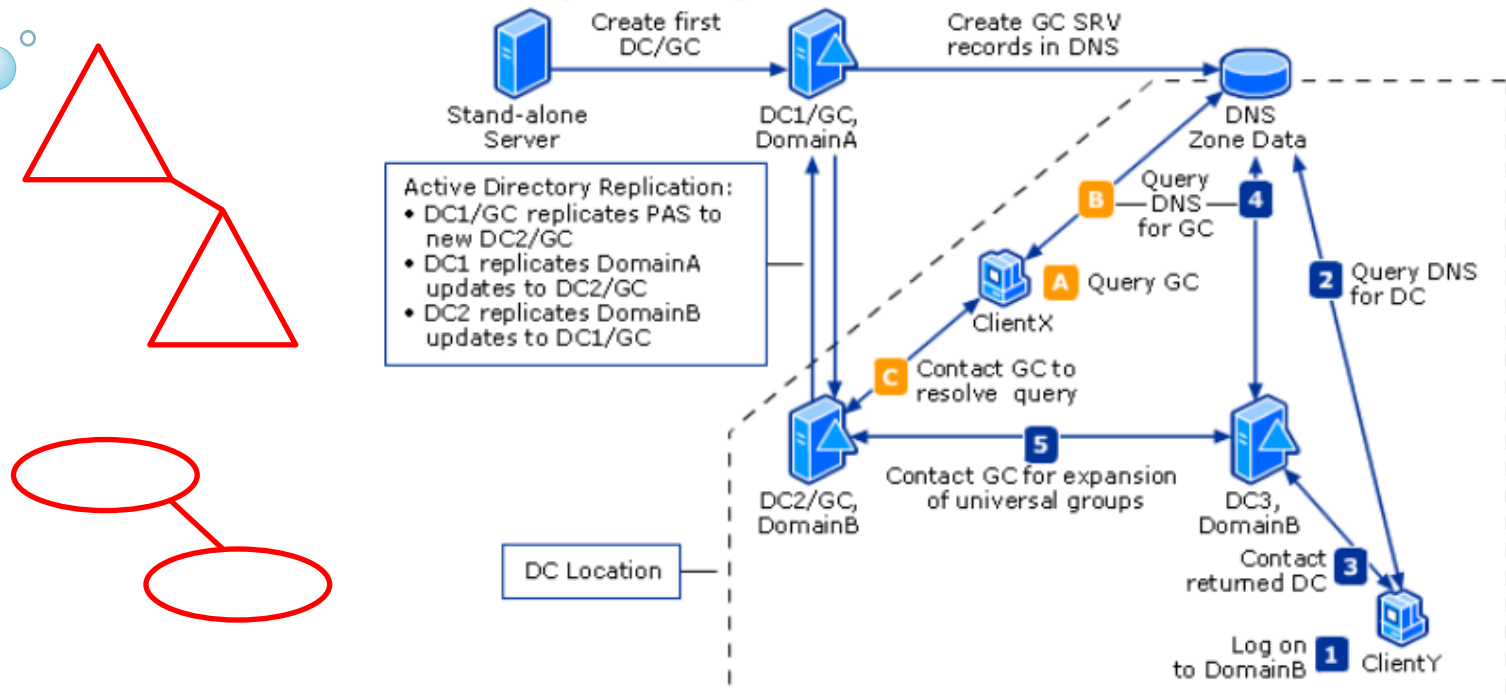
Standort (site)

nach-
vollziehen

Global Catalog: NTDS Settings | Kontextmenü | Properties | General: Checkbox GC ersichtlich

- Meldet sich ein Client an, wird seine Anfrage von DC zu DC weitergeroutet, bis sie bei einem DC landet, der über einen GC verfügt, siehe nächste Folie.
- Ein GC ist immer ein DC.
- Alle DCs dürfen GC enthalten.
- **Empfehlung: Pro Standort mind. 1 DC, am besten mit GC**

Standort (site)



- Client meldet sich beim nächsten GC an:
 - A through C: (A) ClientX wants to send a query to the global catalog. ClientX prompts (B) a DNS query to locate the closest global catalog server, and then (C) the client contacts the returned global catalog server DC2 to resolve the query.
 - I through 5: (I) ClientY wants to log on to the domain, which prompts (2) a DNS query for the closest domain controllers. (3) ClientY contacts the returned domain controller DC3 for authentication. (4) DC3 queries DNS to find the closest global catalog server and then (5) contacts the returned global catalog server DC2 to retrieve the universal groups for the user.

Standort (site)

weitere Details zu Domänen und Standorten
siehe Lehrmittel, Datei

«galileocomputing_windows_server_2012r2.zip»:

- insbesondere Kap. 8.2 in Datei
«8.2_PlanungUndDesignAD 2012 R2.pdf»

Grundlagen: Entwurf AD

- zur Verwendung für das Informatikmodul I 59: „Directory Services konfigurieren und in Betrieb nehmen“
- Informatiker, Fachrichtung **Systemtechnik**, 5. Semester
- D. Jenny, daniel.jenny@gbssg.ch,
058-228 26 57, 0043-5574-731 34,
076-450 37 70

Grundlagen: Entwurf AD

Überblick:

- Einfaches Directoryservice-Konzept
- Details zum Entwurf

Grundlagen: Entwurf AD

Überblick:

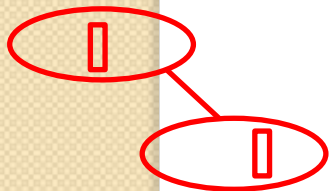
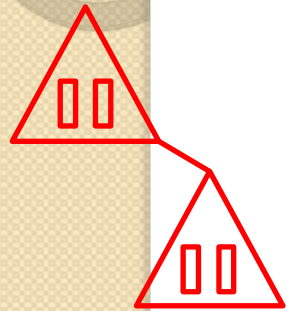
- **Einfaches Directoryservice-Konzept**
- Details zum Entwurf

Einfaches Directoryservice-Konzept

- logische Sicht:
 - Faustregel: 1 Domäne; weitere Domänen nur:
 - bei Schemaschutz
 - bei «autonome», «eigenständige» Verwalt.
 - bei «eigener» Sicherheitsbereich
 - 2 DCs pro Domäne (Herstellerempfehl.)
- physische Sicht:
 - bei üblicher WAN-Verbind.: 1 DC/Standort
 - bei Hochgeschw.-Verb.: 1 DC für alle so zusammengeschlossenen Standorte

Einfaches Directoryservice-Konzept

- logische Sicht:
 - 2 DCs pro Domäne (Herstellerempfehl.)
 - Merkregel:
Domäne → **D**ouble → pro **D**omäne: 2 DCs
- physische Sicht:
 - bei üblicher WAN-Verbind.: 1 DC/Standort
 - Merkregel:
Standort → **S**ingle → pro **S**tandort: 1 DC



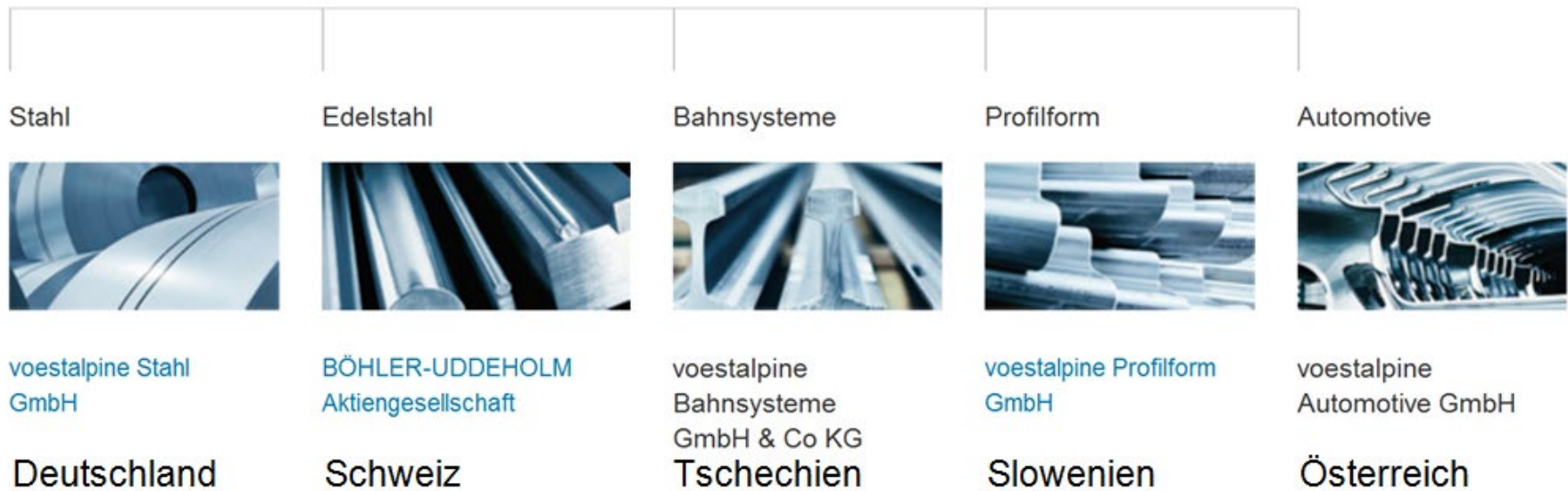
Einfaches Directoryservice-Konzept

- Lösen Sie 2 Fallbeispiele, alleine oder zu zweit
- Gesucht:
 - logische Sicht mit Mindestanzahl DC
 - physische Sicht mit Mindestanzahl DC
 - Mindestanzahl DC insgesamt
 - kostengünstigste Minimalvariante
 - Bezeichnung der Domänen und Standorte

Einfaches Directoryservice-Konzept

Fallbeispiel 1, 1/2:

voestalpine AG



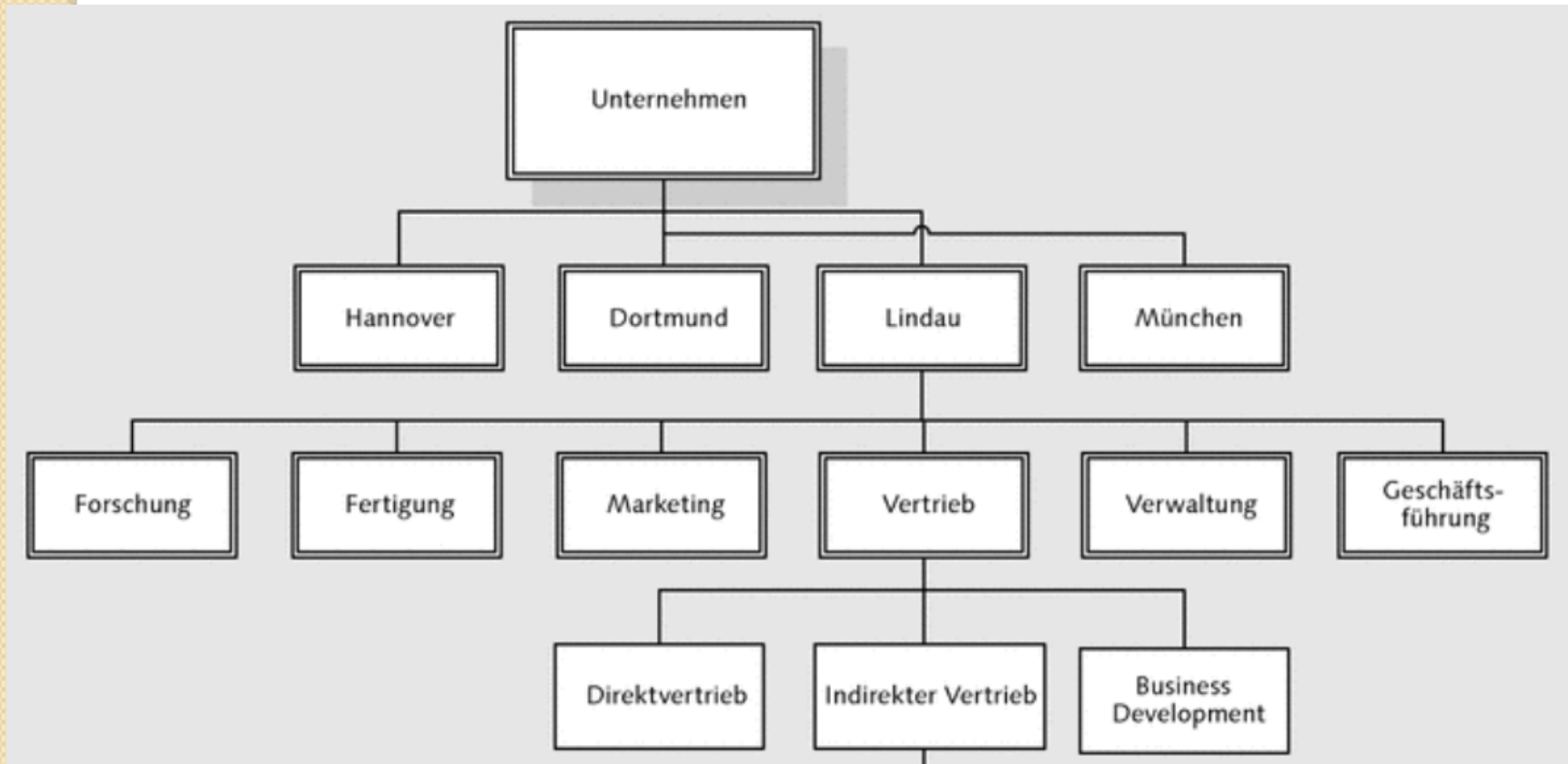
Einfaches Directoryservice-Konzept

Fallbeispiel 1, 2/2:

- Die voestalpine-Betriebe Stahl, Edelstahl, Bahnsysteme, Profilform und Automotive befinden sich gemäss Abbildung an den 5 Niederlassungen D, CH, CZ, SLO und A.
- Es sind spezielle Vorkehrungen für die Sicherheit des Schemas zu treffen.
- Die anderen 4 Niederlassungen sind nur mit dem Hauptsitz Österreich verbunden.
- Hochgeschwindigkeits-WAN-Strecken

Einfaches Directoryservice-Konzept

Fallbeispiel 2, I/2:



Einfaches Directoryservice-Konzept

Fallbeispiel 2, 2/2:

- Die abgebildeten 4 Niederlassungen Hannover, Dortmund, Lindau und München sind vollvermascht.
- München erhält einen eigenen Sicherheitsbereich und verwaltet sich autonom.
- Es kommen kostengünstige WAN-Strecken zum Einsatz.
- Lindau ist der Hauptsitz und beschäftigt 1000 Mitarbeiter, die anderen weniger als 100.