Zusammenfassung M159

Directoryservices konfigurieren und in Betrieb nehmen

Emanuel Duss

2011-11-28

Informationen

Autor	Emanuel Duss
Erstellt am	2009-09-01
Bearbeitet am	2011-11-28
Erstellt mit	OpenOffice.org auf Ubuntu Linux

Lizenz

Bearbeitungsprotokoll

Datum	Version	Änderung
2009-09-01	0.1	Erstellt
2009-10-01	0.2	Release 1; LDAP
2009-11-02	0.3	Release 2 für Prüfung
2010-03-01	0.4	Release 3 für Prüfung (Themen vgl. Schluss)
2010-05-15	1	Final

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1 LDAP

1.1 X.500 Standard

Um Active Directory zu verstehen, muss man zuerst den als Basis dienenden X.500-Standard verstehen. Der X.500-Standard beschreibt ein globaler Verzeichnisdienst, der hierarchisch aufgebaut ist. X.500 ist ein offener Standard und somit existieren keine klaren Vorgaben über die zu speichernden Informationen.

Es werden lediglich die Verwendung von Objekten und Verbindungen beschrieben. Ein Objekt kann einer oder mehreren Objektklassen angehören. Die Objekte besitzen Attribute, welche Informationen zum Objekt liefern. Alle Objekte eines Verzeichnisses werden in einer Directory Information Base (DIB) zusammengefasst. Die in der DIB vorhandenen Informationen werden in einer Baumstruktur abgelegt (DIT – Directory Information Tree).

Jedes Objekt verfügt über einen eindeutigen Bezeichner (Distinguished Name, DN), der sich aus einem relativen Bezeichner (Relative Distinguished Name, RDN) und dem jeweiligen Objektpfad im Verzeichnisbaum der sogenannten Gesmtstruktur (Forest) zusammensetzt.

Kommuniziert wird über das ISO/OSI-Modell. Der Client ist der Verzeichnis-Benutzer-Agent (Directory User Agent, DUA) und der Server der Verzeichnis-System-Agent (Directory System Agent, DSA). Der Benutzer (DUA) verwendet das Directory Access Protocol (DAP) als Abfragesprache um mit dem Server (DSA) zu kommunizieren. Die einzelnen DSA kommunizieren untereinander mit dem Directory System Protocol (DSP). Die Informationen werden über das Directory Operational Binding Management Protocol (DOP) verbreitet. Die Replikation geschieht durch das Directory Information Shadowing Protocol (DISP) um die Ausfallsicherheit und die Reaktionszeit zu erhöhen.

Microsoft Active Directory ist weitgehend an den X.500-Standard angelehnt. Der DSA dient als Domänenkontroller. Zur Abfrage wird eine abgewandelte Version von DAP genutzt – LDAP.

1.2 LDAP / Verzeichnisdienst

Ein Verzeichnisdienst ist vergleichbar mit einem Telefonbuch. Dort sind Objekte der Netzwerkressourcen mit Informationen verknüpft. Objekte sind zum Beispiel Benutzer, Drucker, Shares und Datenbanken. Die Informationen könnten der Name des Objekts oder der Standort sein. Somit erleichtert der Verzeichnidienst die zentrale Verwaltung aller Netzwerkobjekte. Alle Informationen werden an einem Ort gesammelt und gepflegt. Im Active Directory hat jedes Objekt eine eindeutige GUID (Globally Unique Identifier), welche eine Länge von 128 Bit hat und beim erstellen des Objekts zugeteilt wird.

Was die Sicherheit betrifft: Den Objekten können Berechtigungen vergeben werden. Alle Personen sehen z.B. Die Email-Adresse, doch nur Hagbard Celine sieht den Fnordfucktor (ein normales Feld von einem Benutzer) der einzelnen Personen. In der Zugriffliste jedes Objekts ist beschrieben, wer welche Berechtigung hat.

1.3 Lightweight Directory Access Protocol (LDAP)

LDAP ist das Zugriffsprotokoll in einer AD-Umgebung. Alle Aktionen von Clients oder Servern mit dem AD (z.B. Login, Suchabfragen, Kommunikation zwischen DC) werden über LDAP vollzogen.

Mit LDAP können textorientierte Abfragen direkt über den TCP/IP-Stack gemacht werden. LDAPv2 wurde im RFC 1478 und später im RFC 1777 definiert. LDAPv3 ist im RFC 2251 definiert. Die meisten Implementierungen von Verzeichnisdiensten unterstützen beide Standards.

1.4 LDAP-Architektur

LDAP ist das Zugriffsprotokoll für X.500-basierte Verzeichnisdienste. Gegenüber DAP bietet es mit AD die folgenden Verbesserungen: LDAP benutzt TCP/IP, das Funktionsmodell ist vereinfacht, um selten gebrauchte Funktionen erleichtert worden, es werden normale Zeichenketten zur Darstellung statt eine komplizierte Syntax verwendet.

Ein LDAP-Client kann Handlungen wie Suchen oder Löschen eines Objektes an den Server übermitteln.

Verbindung

Der Client initiiert die Kommunikation zum Server über IP-Adresse und **TCP-Port 389**. Die Authentifizierung ist entweder anonym oder mit einem Username und Passwort. Die Verbindung kann auch verschlüsselt werden.

Dann greift der Client auf den Server zu. Am häufigsten sind Suchvorgänge. Es gibt aber auch Hinzufügen, Löschen, Ändern oder Umbenennen.

1.5 LDAP-Modelle

LDAP-Modelle repräsentieren die Dienste, wie sie über den Server bereitgestellt und vom Client gesehen werden.

- Informationsmodell: Strukturbeschreibung der Information, die im Verzeichnis gespeichert werden
- Namensmodell: Beschreibt, wie die Informationen im Namensraum aufgebaut und organisiert sind
- Funktionsmodell: Beschreibt, welche Operationen an den Informationen vollzogen werden können (Löschen, etc...)
- Sicherheitsmodell: Beschreibt wie der Zugriff auf die Informationen geschützt wird.

1.5.1 Funktionsmodell

Dieses Modell beschreibt die Operationen, die Sie auf den Daten ausführen können

Abfrage Operationen

- Suchen nach Einträgen, die den Suchkriterien genügen; Vergleichen eines Eintrags
- Search, read, compare

Update Operationen

- Modifizieren eines Eintrags; modifizieren des ausgezeichneten Namens; Hinzufügen eines neuen Eintrags; Löschen eines Eintrags
- Add, delete, modifiy, modifiy DN (rename)

Authentifizierungs & Kontrolloperationen

- Bind - Authentifizieren
- unbind - Abmelden
- abandom - Anfrage abbrechen

LDAPv3 Erweiterungen (exop - extended operations)

- LDAP control - kann Verhalten bestehender Operationen abändern
- SASL für Authentifizierung

1.5.2 Informationsmodell

Informationsmodell beschreibt was in ein Verzeichnis abgelegt werden kann Im Schema werden die Definitionen von Objekt-Klassen und Attributen festgelegt.

Die einzelnen Elemente des Schemas tragen eine OID (Objekt-Identifier). Die OID sind weltweit eindeutig festgelegt. Zur Realisierung von Schemaerweiterungen können bei der IANA OID-Bereiche zur Firmen internen Verwendung beantragt werden.

Klassentypen

- abstrakte Klassen (dienen der Vererbung an strukturelle Klassen oder Hilfsklassen. Die Klasse "top" ist eine abstrakte Klasse.)
- strukturelle Klassen (davon können im DIT konkrete Objekte angelegt werden. (inetOrg-Person ist eine konkrete Klasse. Davon können konkrete Objekte im LDAP-DIT von openLDAP oder Active Directory angelegt werden. Vergl. z.B den Technet Artikel "Erstellen einer InetOrgPerson.)

Definitionen für Klassen oder Attribute

- jedes Attribut beschreibt eine besondere Eigenschaft des Objektes
- Syntax der erlaubten Einträge - - wie müssen Values ausschauen
- Regeln für Vergleich von Values (z.B. ignoriere Gross-/Kleinschreibung)
- Auflistung der Vererbungs-Abfolge (für Klassen)
- Auflistung der der MUST und MAY Attribute (für Klassen)
- Regeln für Sortierungen (z.B. lexigraphisch, nummerisch)
- Unterscheidung in zwei Klassen
- user attributes - “normale” Daten durch Nutzer gepflegt
- operational attributes - werden automatisch gepflegt z.B. modfiyTimeStamp

Value(s)

- die eigentlich zu speichernden Daten

Getrennte Datenhaltung

Das Informationsmodell wird in zwei Bereiche geteilt

- Anwendungsdaten
  - die eigentlich zu speichernden Daten mit eindeutiger Identifizierung
  - diese werden zwischen Server und Client ausgetauscht
  - Online: über LDAP
  - Offline: über LDIF ASCII-Text-Schnittstelle mit Import-/Export Tools
- Schemadaten
  - die formelle Beschreibung der möglichen Objekte mit ihren Attributen
  - sind am Server hinterlegt (OpenLDAP: Textfiles geparst beim Serverstart)
  - eingehende Anwendungsdaten werden gegen Schema geprüft
  - Client kann sich bei Server über hinterlegte Schema informieren (teilweise Zukunft)

1.5.3 Namensmodell

- Namensmodell beschreibt wie Daten angeordnet und angesprochen werden
- Das Namensmodell von LDAP ist hierarchisch aufgebaut.
- Die Daten werden im DIT (Directory Information Tree) eingespeichert.
- Der DIT ist eine Datenstruktur, die auf Suchoperationen optimiert ist.
- Das Einfügen von Daten ist hingegen zeitaufwendiger, da dazu Verknüpfungen im DIT zu lösen und neu zu bilden sind, was einen gewissen Aufwand bedeutet.
- Suchoperation auf den Daten im LDAP-DIT kommen weitaus häufiger vor als Add-, Modify- oder Delete-Operationen.
- jedes Objekt ist über seinen DN (distinguished name) eindeutig identifiziert
- durch Zerlegung des DN kann es in einen Baum eingeordnet werden

1.5.4 Sicherheitsmodell

Dieses Model beschreibt wie ein Verzeichnis geschützt werden kann

Integrity (Integrität)

Es muss sichergestellt sein, dass die Informationen, die der Empfänger erhält, auch die unveränderten Informationen sind, die der Sender verschickt hat.

Die übertragenen Daten (inkl. Authentifizierungsdaten) können mit Verschlüsselungsverfahren geschützt werden.

Dazu wurde LDAP V3 um den Standard SASL (Simple Authentication and Security Layer) ergänzt.

Als hauptsächliches Verschlüsselungs-verfahren wird SSL (Secure Socket Layer) eingesetzt.

Confidentiality (Vertraulichkeit)

Die Informationen, die versendet werden, dürfen für Aussenstehende nicht zu lesen sein (Verschlüsselung der Daten).

Authorization (Autorisierung)

Es muss sichergestellt sein, dass der Nutzer ausschliesslich das machen kann, wozu er berechtigt ist. Dafür ist es notwendig, eine Benutzerkennung einzurichten, die den Nutzer mit Rechten (z.B. lesen, schreiben, löschen) versieht. Die Festlegung von Berechtigungen erfolgt in der Konfigurations-Datei <slapd.conf>. Es ist auch anonymer Zugriff möglich.

1.6 Der Namenskontext

Alle Objekte in LDAP / Active Directory werden über eindeutige Namen Distinguished Names (Dns) angesprochen. Der Aufbau ist an den X.500-Standard angelehnt.

Jedes Objekt besteht aus einem oder mehreren Attributen. Jedes Attribut besteht aus einem Typ und einem Wert. Die Definition welches Attribut zu welchem Objekt gehört, wird in der Objekt-Klasse beschrieben.

AD ist hierarchisch aufgebaut und besteht aus zwei Arten von Objekten: Container-Objekte und Leaf-Objekte. Container-Objekte können weitere Objekte enthalten. Leaf-Objekte hingegen nicht.

Container	Objekt, das andere enthalten kann (z. B. Organisationseinheit)
Leaf	Objekt, das an einer Endposition des DIT steht (z. B. Benutzer)
Attribute	In der Definition einer Klasse wird definiert für welche Objekte welche Attribute mit Werten belegt sein müssen oder können. Können in Objekten gespeichert werden. Je nach Schemadefinition können nur ein Wert oder mehrere Werte gespeichert werden.
Schema	Definiert die Objektklassen, Attribute

Werte

- Der Wert kann zwingend oder optional sein
- Es sind einen oder mehrere Werte möglich
- Werte können eine Syntax haben (z. B. Für ein Datum)
- Matching-Rules für Suchoperationen

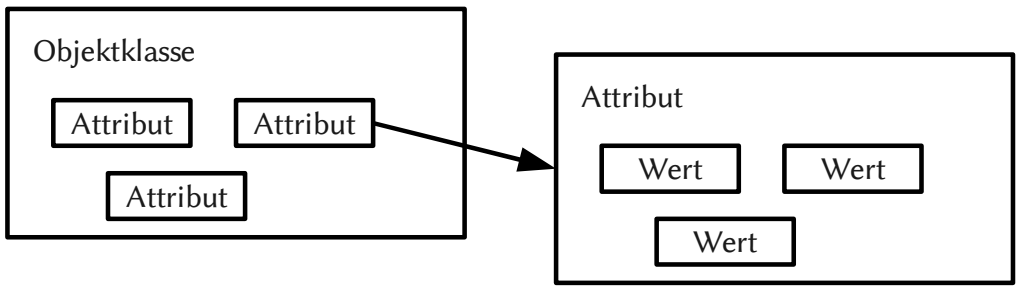


Abbildung 1: Objekte, Attribute und Werte

1.6.1 Distinguished Name (DN)

Gesamter Pfad zu einem Objekt im DIT.

```
CN=cwest,OU=Autoren,DC=CertPro,DC=de
```

CN=cwest beschreibt in dem Beispiel ein Objekt im Container OU=Autoren der Domäne DC=CertPro, die sich wiederum unterhalb der Domäne DC=de befindet.

CN = Common Name; OU = Organizational Unit; DC = Domain Component

1.6.2 Relative Distinguished Name (RDN)

Teil der DN, der das Objekt relativ zu seinem Namenskontext beschreibt. Er stellt die eigentliche Objektbezeichnung dar, ohne die Angabe des gesamten Namenspfades (-Kontextes). RDN werden häufig bei Suchabfragen nach Objekten in AD verwendet. Beispiel: CN=cwest.

1.6.3 LDAP-URL

Aufbau: LDAP://servername_oder_IP-Adresse/DN_des_Objekts

```
LDAP://dc1.CertPro.de/CN=cwest,CN=users,DC=certpro,DC=de
```

1.6.4 User Principal Name (UPN)

Steht jedem Benutzer-Objekt zur Verfügung. Aufbau nach RFC 822: UPN-Präfix (Benutzername)@UPN-Suffix (Domänenname). Beispiel: cwest@certpro.de.

Das UPN-Präfix muss eindeutig sein und ist mit dem Benutzeranmeldenamen unter Windows kompatibel. Das UPN-Suffix ist entspricht meist dem Domänennamen. Da der Aufbau wie bei einer Email-Adresse ist, ist der wird oft dasselbe dafür verwendet.

1.7 Aufbau eines LDAP Directory Information Trees

Es gibt zwei Typen von Objekten:

- Container, welcher weitere Container enthalten kann (z.B. Organisationseinheit)
- Leaves / Endknoten, welcher weitere Leaves enthalten kann, aber keine Objekte (z.B. Computer, Benutzer)

Alle Einträge werden in einer Baumstruktur angelegt, welche sich DIT nennt. Der DIT kann auf mehrere Server verteilt werden. Die Server müssen sich jedoch verlinken, damit alle Informationen im Verzeichnis gefunden werden können. Der oberste Eintrag, den ein Server besitzt, wird auch als Suffix oder Naming Context bezeichnet.

1.8 Verzeichnis vs. Datenbank

Verzeichnis

- Funktionen gehen weit über herkömmliche relationale Datenbanken hinaus
- Informationen werden öfter abgerufen als geändert
- AD benutzt das LDAP-Protokoll zum Zugriff (Einfach & schlank; optimiert für Lesezugriffe)
- Hierarchischer Aufbau

Datenbank

- Vermehrt werden aktualisierte Daten geschrieben
- Datenbank mittels standardisierten, komplexen SQL-Abfragen
- Aufbau ist relational

1.9 LDAP Informationsmodell / Namensmodell

Der Aufbau der Objekte (besteht aus Attributen) und der Wertebereich der Attribute wird im LDAP-Schema festgelegt. Es bestehen auch Objekthierarchien.

Alle Einträge werden in einer Baumstruktur angeordnet, die sich Directory Information Tree (DIT) nennt.

Die Anordnung basiert auf eindeutigen DNs der Objekte. Das ist ein eindeutig definierter Name (Distinguished Name, DN), welcher sich aus einer Reihe von relativ definierten Namen (Relative Distinguished Name, RDN) zusammensetzt. Beispiel:

```
dn: cn=eris,dc=discordia,dc=org
```

1.9.1 Attributtypen

Hier sind wichtige Attributstypen, welche case-insensitive sind!

- dc Domain Component Name der Domänenbestandteile
- cn Common Name Objektname
- c country Ländername
- st StateOrProvinceName Name eines Bundeslandes / Kanton
- l LocalityName Name einer Stadt
- o OrganisationName Name einer Organisation
- ou OrganisationalUnit Name der Organisationseinzeit
- uid UserID UserID

1.10 Hierarchie von Klassen für Benutzerobjekte

Folgendes könnte ein LDAP-Datensatz für Eris, die Göttin der Verwirrung darstellen. Folgendes Beispiel soll jedoch nicht verwirren, sondern aufklären, so wie es Immanuel Kant seinerzeit getan hat.

Die jeweiligen Attribute sind in der Schemadatei definiert und somit nicht ganz au der Luft gegriffen.

Objektklassen definieren

```
objectClass: top Oberste Klasse
(Wurzel)
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
```

Attribute der Klasse person

```
sn: Bond
cn: James Bond
telephoneNumber: 020 7930 9007
userPassword: {crypt}geheim
description: Agent 007
```

Attribute der Klasse organizationalPerson

```
ou: MI6
title: Commander
street: The Enquiries Desk
postOfficeBox: 3255
st: CT
postalCode: SW1P 1AE
facsimileTelephoneNumber: 020 7930 9000
```

Attribute der Klasse inetOrgPerson

```
departmentNumber: 00
employeeType: permanent
givenName: James
initials: JB
jpegPhoto: james.jpg
audio: james.wav
homePhone: 020 7930 9007
pager: Opening the toy cabinet
preferredLanguage: English
userCertificate: certs/jb_cert.pem
```

1.11 LDIF-Datei

LDIF ist ein Akronym für LDAP Data Interchange Format und ist im RFC 2849 definiert.

1.11.1 Aufbau des DIT

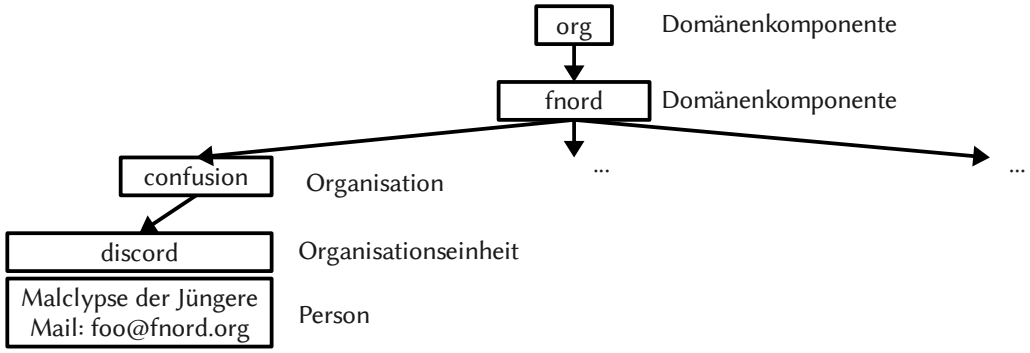


Abbildung 2: DIT

1.11.2 LDIF-Datei

Organisation „confusion“

```
dn: dc=fnord, dc=org
objectclass: dcObject
objectclass: organization
o: confusion
dc=helpnet
l: Atlantis
postalcode: 2305
streetadress: Snafuberg 1337
```

Organisationseinheit „discord“

```
dn: ou=discord, o=confusion, dc=fnord, dc=org
objectclass: organizationalunit
ou: discord
description: verwirrung
telephonenumber: 555-2305-1337-42
```

Person „Malclypse der Jüngere“

```
dn: cn=Malclypse der Jüngere, ou=discord, o=confusion, dc=fnord, dc=org
objectclass: person
objectclass: organizationalperson
objectclass: inetorgperson
cn: Malclypse der Jüngere
sn: der Jüngere
mail: foo@fnord.org
```

Optional:

```
uid: Malclypse
l: Fnordhausen
postalcode: 420523
streetadress: Tarantellastrasse 23
telephonenumber: 040-7654321
facsimiletelephonenumber: 040-7654321
```

2 Active Directory Infrastruktur[1]

2.1 AD vs. P2P

AD	P2P (Kein AD)
Vorteile von Active Directory • Einfachere Administration • Zentrale Verwaltung von Usern und Computer • Sicherheit: Gruppenrichtlinien und Passwortrichtlinien • Benutzeranwendbarkeit: Suchen von AD-Objekten • Ressourcen- und Zugriffssteuerung (ACL) • (Dynamisches DNS) Nachteile von AD • Hard- und Software-Aufwand	Vorteile von P2P • Kostengünstig • Unkomplizierter und schneller Aufbau Nachteile von P2P • Geräte- und Verzeichnisfreigaben für jeden PC lokal einrichten • Sicherheit: Nur wenig Zugriffs- und Datensicherheit • Je nach OS nicht stabil / belastbar • Eingeschränkte Zugriffssteuerung

Tabelle 1: AD vs. P2P

2.2 AD-Architektur

In Active Directory sind DN-Zonen nach dem X.500-Standard integriert. Verwendet wird LDAPv2 bzw. LDAPv3.

Mit Active Directory kann man ein Verzeichnisdienst betreiben. Dieser Verzeichnisdienst wird entweder von einem oder von mehreren Domänencontrollern im Multi-Master-Betrieb ausgeführt. Dabei handelt es sich um Sonderfunktionen, die nur von einem einzigen Domänencontroller ausgeführt werden können. Diese sind in Masterrollen unterteilt.

Beim erstellen einer Domäne entsteht automatisch eine OU „Domain Controllers“ und darin sind alle DC enthalten.

AD DS (Active Directory Domain Services) ist die Implementierung des Microsoft Verzeichnisdienstes, welches aus mehreren Komponenten besteht. Diese Komponenten vereinen DNS, X.500-Namenskonvention und LDAP. LDAP ist das primäre Zugriffsprotokoll der AC DS. Die erste Version kam mit Windows 2000 Server. Ein Konkurrent war Novell Directory Services, der sich jedoch nicht durchsetzen konnte.

1 Quelle: Active Directory für Windows Server 2008; Addison-Wesley; ISBN: 978-3-8273-2740-6; Ab Seite 98

2.3 Leistungen von Active Directory

Mit Active Directory kann man eine zentrale Verwaltung und Ausführung von folgenden Punkten erreichen.

2.3.1 Authentifizierung mit Kerberos

Mit Kerberos kann man sich in einem Netzwerk authentifizieren. Die Authentifizierung übernimmt eine vertrauenswürdige dritte Partei, der Kerberos-Server. Kerberos unterstützt auch Single Sign-on.

Der Client meldet sich am Kerberos-Server (auch Key Distribution Center, KDC) an und fordert ein Ticket Granting Ticket (TGT) an. Zum Anmelden braucht der Benutzer ein Passwort oder eine SmartCard. Das Ticket kann auch gleich bei der Benutzeranmeldung angefordert werden. Mit dem TGT kann der Client weitere Tickets für Dienste anfordern, ohne noch einmal ein Passwort einzugeben. Es ist möglich mit dem Session-Key die Daten zu verschlüsseln.

Das vom Kerberos-Server angeforderte Ticket kann jetzt an weitere Server weitergegeben werden, um sich zu authentifizieren.

2.3.2 Autorisierung / Berechtigungen

Mit Hilfe vom Active Directory können Berechtigungen auf freigegebene Ressourcen vergeben werden, wie z.B. ACL, Sicherheitsgruppen, Services oder Tickets.

2.3.3 Durchsetzen von Gruppenrichtlinien

Im Active Directory können wir Gruppen definieren. Diese Gruppen werden OUs genannt. In eine Gruppe können User und Computer enthalten sein.

Diesen Gruppen kann man Benutzerrechte, Konfigurationen und Richtlinien zuweisen.

2.4 Logische Strukturierung

Eris' diskordische Geheiminformation zur Prüfung (vielleicht klappt's):

Zu jedem AD-Standort gehört ein eigenes Subnetz... (wenn diese Frage an der Prüfung kommt: bitte 'Heil Eris' rufen (Inf 4B))!

Domänenstruktur (Tree)

Teilbereich einer Gesamtstruktur des AD DS. Einzelne oder mehrere, über Vertrauensstellungen zusammenhängende Domänen, die einem bestimmten Namensraum entsprechen. Einen gemeinsamen, hierarchischer LDAP/DNS-Namespace ab 2nd level. z.B. subdom1.example.org

Domänengesamtstruktur (Forest)

Logische Grenze einer AD DS Infrastruktur.

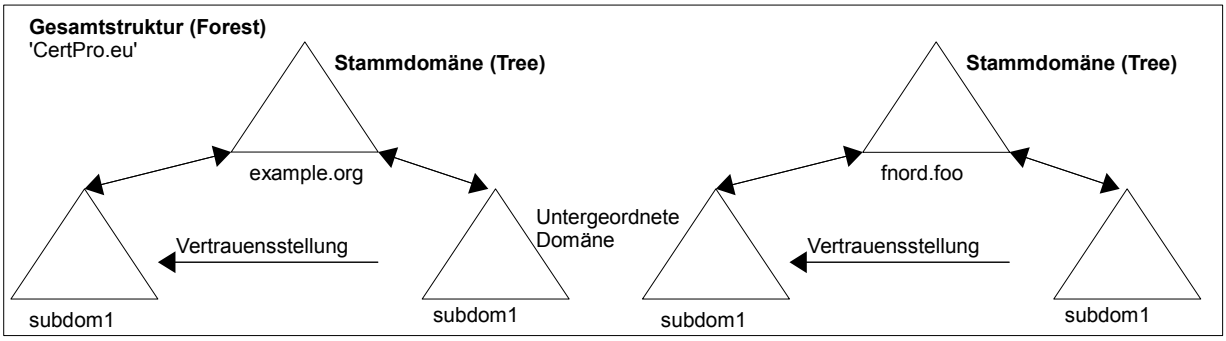


Abbildung 3: Gesamtstruktur

2.5 Globaler Katalogserver (Global Catalog, GC)

Der globale Katalogserver ist zuständig für die Suche nach Objekten im Verzeichnis. Um eine Suche im AD schneller abzuwickeln, benutzt das AD den globalen Katalogserver. Informationen aus anderen Domänen werden automatisch repliziert. Nützlich bei mehr als 100 User pro Standort.

Der globale Katalog ist eine Verzeichnisdatenbank, die von Anwendungen und Clients zum Suchen eines beliebigen Objekts in einer Gesamtstruktur abgefragt werden kann. Jedes Objekt im AD wird in den globalen Katalog repliziert.

Zweck

Im globalen Katalogserver werden alle LDAP-DIT Objekte der Domänengesamtstruktur. (= alle Active Direcotry Objekte) gespeichert.

Dabei werden die am *häufigsten* nachgefragten Attribute ebenfalls auf dem Katalogserver gespeichert. Welche das sind, ist im *Schema definiert.*

Standorte der globalen Katalogserver

Der erste globale Katalogserver wird automatisch auf dem Domänencontroller einer AD-Gesamtstruktur eingerichtet. Weitere Katalogserver sollten grundsätzlich an jedem Standort eingerichtet werden, der über einen DC verfügt (+ jede Exchange-Domäne ??? :D). Aber nicht bei stark eingeschränkter Bandbreite. Auf dem DC, die als Infrastrukturmaster genutzt werden sollte kein Katalogserver eingerichtet werden.

Vorteil eines globalen Katalogservers

- Schnellere Suche in der Gesamtstruktur, weil GCs kommen in jeder Domäne vor und haben Infos von allen AD-LDAP-Objekten, aller Domänen der Gesamtstruktur.
- Gesamtstrukturweite Benutzeranmeldung ohne Rückgriff auf Stammdomäne des Users möglich. Weil sonst könnten sich die User nicht mehr anmelden, da bei der Anmeldung die Gruppenzugehörigkeit ermittelt wird.

Verbindung

Die Verbindung zum Katalogserver geschieht über den Port 3268 auf TCP.

2.6 Betriebsmasterrollen

AD unterstützt Multimasterreplikation von Verzeichnisdaten. Das heisst, jeder DC kann Verzeichnisänderungen akzeptieren und diese Änderungen auf alle anderen DCs replizieren.

2.6.1 Übersicht über die Betriebsmasterrollen

Betriebsmasterrolle	Für was soll das gut sein?	Wo?
Schemamaster	Überwacht und aktualisiert alle Aktualisierungen und Änderungen am Schema. („Hosten“ des Schemas). Details siehe unten...	Forest
DNS-Master	Steuert das Hinzufügen und Entfernen aus der Gesamtstruktur.	Forest
RID-Master	Weist jedem der verschiedenen DCs in der Gesamtstruktur Sequenzen relativer Ids zu. Nur ein DC fungiert in jeder Domäne in der Gesamtstruktur als RID-Master.	Tree
PDC-Emulator	Funkiert als primärer DC, wenn die Domäne ältere Clients aus dem Zeitraum vor AD oder Windows NT-Sicherungsdomänencontroller enthält. Er verarbeitet Konnwortänderungen von Clients und repliziert Aktualisierungen auf die Sicherungsdomänencontroller.	Tree
Infrastrukturmaster	Aktualisiert die Verweise von Gruppen auf Benutzer, wenn Mitglieder von Gruppen umbenannt oder geändert werden.	Tree
Domänennamenmaster	Der Domänencontroller mit der Funktion des Domänennamenmasters steuert das Hinzufügen oder Entfernen von Domänen in der Gesamtstruktur.	Forest

Tabelle 2: Betriebsmasterrollen

Gesamtstruktur: Forest; Stammdomäne: Tree

Schemamaster

Eine konkrete Ausprägung des Active Directory Schemas bildet die Basis für den Einzel- und Mehrfachdomänen-Betrieb. Die Betriebsmasterrolle 'Schema Master' übernimmt das „Hosten“ des Schemas. Der Schemamaster steht auf dem ersten DC in der Domänen-Gesamtstruktur.

Das Schema wird z.B. durch den Exchange Server 2008 oder den Communication Server verändert. Um das Snap-In für das AD zu aktivieren, muss man mit 'regsrv32 schmmgmt.dll' die genannte DLL registrieren. (Frag mich jetzt nicht wieso; ich sehe den Sinn auch nicht... ^^)

2.6.2 Weitere Infos

- http://technet.microsoft.com/de-de/library/cc773108%28WS.10%29.aspx
- http://openbook.galileocomputing.de/microsoft_netzwerk/microsoft_netzwerk_23_000.htm
- http://www.microsoft.com/germany/technet/prodtechnol/windowsserver/technologies/fea

tured/ad/active-directory-betriebshandbuch-05.mspx

3 DNS

3.1 Bevor es DNS gab

3.1.1 Hosts-File (Veranschaulichung: Hosts im IP-Cache)

Wir erstellen einen neuen Eintrag im Hosts-File. Dann leeren wir den IP-Cache und lassen diesen anschliessend anzeigen.

```
C:\>echo 192.0.32.10    example.org >> c:\windows\system32\drivers\etc\hosts
C:\>ipconfig /flushdns
[...]
C:\>ipconfig /displaydns
[...]
         example.org
         ----------------------------------------
[...]
         (Host-)A-Eintrag. . : 192.0.32.10

         10.32.0.192.in-addr.arpa
         ----------------------------------------
[...]
         PTR-Eintrag . . . . . : example.org
[...]
```

Die IP-Adressen vom hosts-File werden also im IP-Cache angezeigt. So ist auch 127.0.0.1 im DNS-Cache enthalten, da dieser Eintrag ebenfalls in der Hosts-Datei eingetragen ist.

3.1.2 NetBIOS Namensauflösung

NetBIOS ist eine serverlose, broadcastbasierte Namensauflösung der NetBIOS-Namen zu IP-Adressen. NetBIOS-Namen sind die Namen der PCs.

1. Ping foobar
2. Broadcast: „Wer hat NetBIOS-Namen 'foobar'?“
3. foobar sendet seine IP-Addr
4. PC01 trägt Zuordnung foobar mit IP-Adresse in NetBIOS-Cache ein.

```
C:\>nbtstat -c
[...]
    Keine Namen im Cache
C:\>ping foobar
Ping foobar [10.11.3.158] mit 32 Bytes Daten:
[...]
C:\>nbtstat -c
[...]
                  NetBIOS-Remotecache-Namentabelle
        Name               Typ         Hostadresse     Dauer [Sek.]
    ------------------------------------------------------------
    FOOBAR          <00>  EINDEUTIG       10.11.3.158         597
C:\>
```

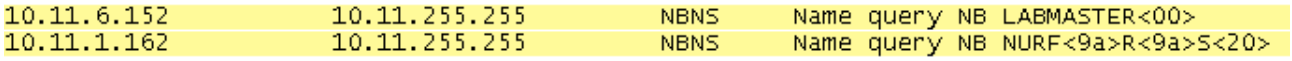


Abbildung 4: NetBIOS Wireshark Capture

- NBNS verursacht deutlichen Overhead (hohe unnötige Netzwerklast)!
- AD basiert für die internen Dienste vollständig auf DNS (kein NetBIOS)!
- Kann verzichtet werden: im Prinzip ja, aber es muss getestet werden (eventuell hat es noch Anwendungen, die nur mit NetBIOS funktionieren.)

3.1.3 WINS: Serverbasierte NBDS

WINS erstellt anhand der NetBios-Broadcast eine Datenbank, mit den Zuordnungen IP-Adresse und Name.

Knotentyp:Defniniert die Namensauflösungsstrategie für eine Netzwerk-Client.

Knotentypen[2]

Die einzelnen Rechner, die auch Konten oder Nodes genannt werden können zur Namensauflösung auf unterschiedliche Arten konfiguriert werden. Der sogenannte Knotentyp legt fest, auf welche Art die Namensauflösung bei der jeweiligen Maschine erfolgt. Die Einstellungen erfolgen in der Regel automatisch, können jedoch in der Registry (unter dem Schlüssel ...NodeType) editiert werden oder dem Client in der DHCP Konfiguration übergeben werden.

b-Knoten	p-Knoten
Die Namensauflösung erfolgt allein über Broadcasts. Dieser Knotentyp wird automatisch eingestellt, falls sich kein WINS Server im Netzwerk befindet. Der Registry-Schlüssel wird hierfür auf den Wert 1 eingestellt.	Der Name wird mit Hilfe einer Point-to-Point Verbindung zu einem WINS Server aufgelöst. Dieser Typ wird automatisch eingestellt, wenn mindestens ein WINS Server im Netzwerksegment vorhanden ist.
m-Knoten	**h-Knoten**
Diese Einstellung kombiniert den B- und den P-Knoten mit der Defaulteinstellung der Namensauflösung per Broadcast. Falls der Name so nicht aufgelöst werden kann, wird eine Auflösung per WINS Server versucht. Der Registryeintrag muss hierfür auf 4 gesetzt werden.	Beim h-Knoten (Hybrid-Knoten) erfolgt auch eine kombinierte Auflösung der Rechnernamen. Allerdings ist hier die Defaulteinstellung die WINS Auflösung. Der Schlüssel in der Registry wird hier auf 8 gesetzt. Der h-Knotentyp wird auf einer Maschine automatisch als Default eingestellt, wenn in den Netzwerkeinstellungen ein WINS-Server angegeben wird.

Tabelle 3: Knotentypen

2 Quelle: http://www.admins-tipps.de/Microsoft/Windows_NT/Die_WINS_Knotentypen.htm

3.2 DNS-Namensauflösung

3.2.1 Anycast-Adressierung der Root-Server

Es gibt 13 DNS-Root-Server. Dies sind aber mehr als 13 physische Hosts. Ein Root-DNS-Server kann aus mehreren Hosts bestehen. Dies nennt man „verteilt“. Diese Hosts werden über anycast adressiert.

Anycast ist eine Adressierungsmethode, in der eine Gruppe von Computern angesprochen wird. Der mit der kürzesten Route (der mit der kürzesten Metrik) antwortet.

Welcher Root-Server verwendet wird, wird anhand der Routing Tabelle auf den Routern im Internet entschieden. Diese schauen auf die geographische oder strukturelle Lage eines Resolvers.

Neue Route hinzufügen

Host-Route: Weg zum Ziel über mehrere Punkte in einem Netzwerk (Windows)

```
route add $ZIELNETZWERK mask $ZIELNETZMASKE $GATEWAY
```

Beispiel:

```
route add 172.16.23.0 mask 255.255.255.0 10.0.0.1
```

Unter Linux

```
route add -net 172.16.23.0 netmask 255.255.255.0 gw 10.0.0.7
```

Wenn man mehrere Routen angibt, die zu einem Ziel führen, entscheiden die Kosten, die man mit Metrik angeben kann.

3.2.2 Die Root-Server (Domain '.')

```
C:\>nslookup
> set type=ns
> .
[...]
A.ROOT-SERVERS.NET      internet address = 198.41.0.4
B.ROOT-SERVERS.NET      internet address = 192.228.79.201
[...]
```

Die Root-Server nehmen keine rekursiven Anfragen entgegen. Sie können nur die Nameserver der nächsten DNS-Zonen ausgeben. Dies wird wegen der Auslastung der Root-Server so gemacht.

3.2.3 Vorgang

1. Ping www.switch.ch
2. DNS-Client-Software (Resolver):
    1. Zuerst wird /etc/hosts gefragt (und in den DNS-Cache eingetragen)
    2. danach den DNS-Cache
    3. dann den DNS-Server

3.2.4 Arten

- Forward-Lookup: Auflösen von Hostnamen in IP-Adressen (Auf dem DNS-Server wird hierfür ein A-Record erstellt).
- Reverse-Lookup: Auflösen einer IP-Adresse in einen Hostnamen (Auf dem DNS-Server wird hierfür ein PTR-Record erstellt).

3.3 Namserver-Typen

3.3.1 Caching Only DNS-Server

- Für keine Zone authorisierend (besitzt keine Zonendateien)
  - Ausser für interne Domain „localhost“
- Nimmt rekursive Queries von den Clients entgegen
- Löst Anfragen von den Clients iterativ auf (--> Verfügt über Root-Hints)
- Speichert aufgelöste Anfragen (bis Gültigkeitsdauer abgelaufen ist)
- Beantwortet erneute Anfragen nach gecachten Einträgen mit dem Vermerk „nicht authorisierend“
- Im LAN kann der DNS-Server keine Anfragen für Computer im LAN beantworten, da er diese nicht kennt (keine Zone dafür; P2P-Netzwerk). Für diesen Zweck kann man NetBIOS nutzen.

3.3.2 Forwarding Nameserver

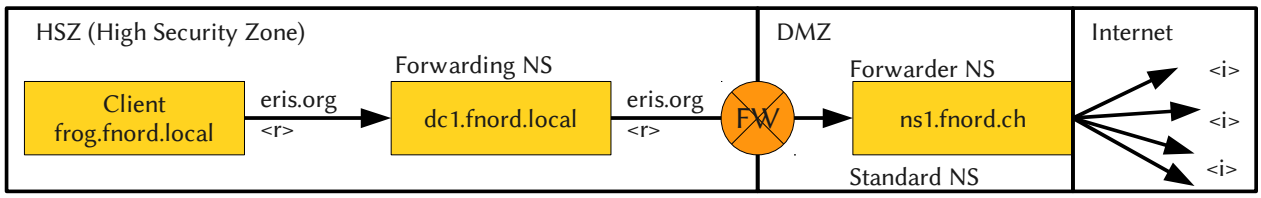


Abbildung 5: Forwarding Nameserver

r = rekursive Queries | i = iterative Queries (Dies ist im DNS-Paket Query-Flag festgelegt!)

Die Domäne .local benötigt keine Delegierung von oben, da diese nirgends registriert ist.

Der Forwarding Nameserver benötigt keine Root-Hints. Root-Hints sind A-Records auf die Root-DNS-Server. Der Forwarder NS benötigt diese jedoch zwingend, damit er weiss, wo er die Queries (jeweils iterativ) hinschicken muss.

Die Domäne ns1.fnord.ch muss bei der Domäne .ch (Organisation SWITCH) delegiert werden.

Vorteile

- Reduktion des DNS-Traffic aus / in die HSZ
- Der DNS-Server legt die abgefragten Einträge im Cache ab.
- Straffe Firewallregeln für DNS aus / in HSZ (Port 53 nur zwischen dc1 und ns1; Client dürfen nicht Port 53 nutzen!)
- Weniger Belastete DCs in der HSZ, da diese nicht auf die Root-Einträge zugreifen müssen.

Bind 9 Konfiguration Forwarding NS

```
options {
      forwarders {ipaddr_NS1, ipaddr_NS2;};
      forward only;
}
```

Forwarders: Welche DNS-Server abgefragt werden sollen

Foward only: keine iterative Abfrage

3.4 DNS-Zonen

Durch das Delegieren von Unterbereichen des DNS-.Trees in neue Zonen wir der administrative Aufwand für die Verantwortlichen der darüber liegenden Zonen verringert. Gäbe es die Zonendelegierung nicht, müsste der Administrator der Root-Zone „.“ alle DNS-Einträge der gesamten Welt, dem Universum und dem ganzen Rest alleine pflegen. Auch die Zonendateien werden kleiner was der Übertragung einer ganzen Zone zu gute kommt.

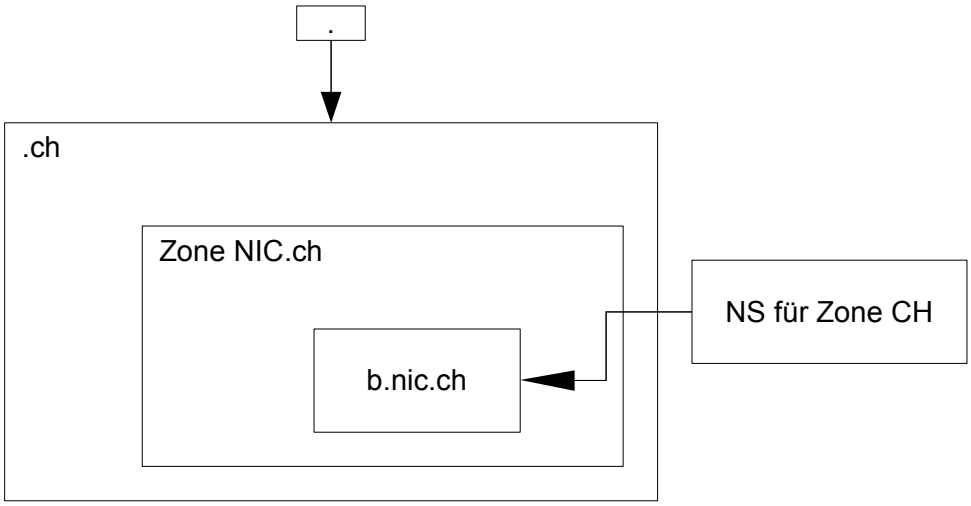
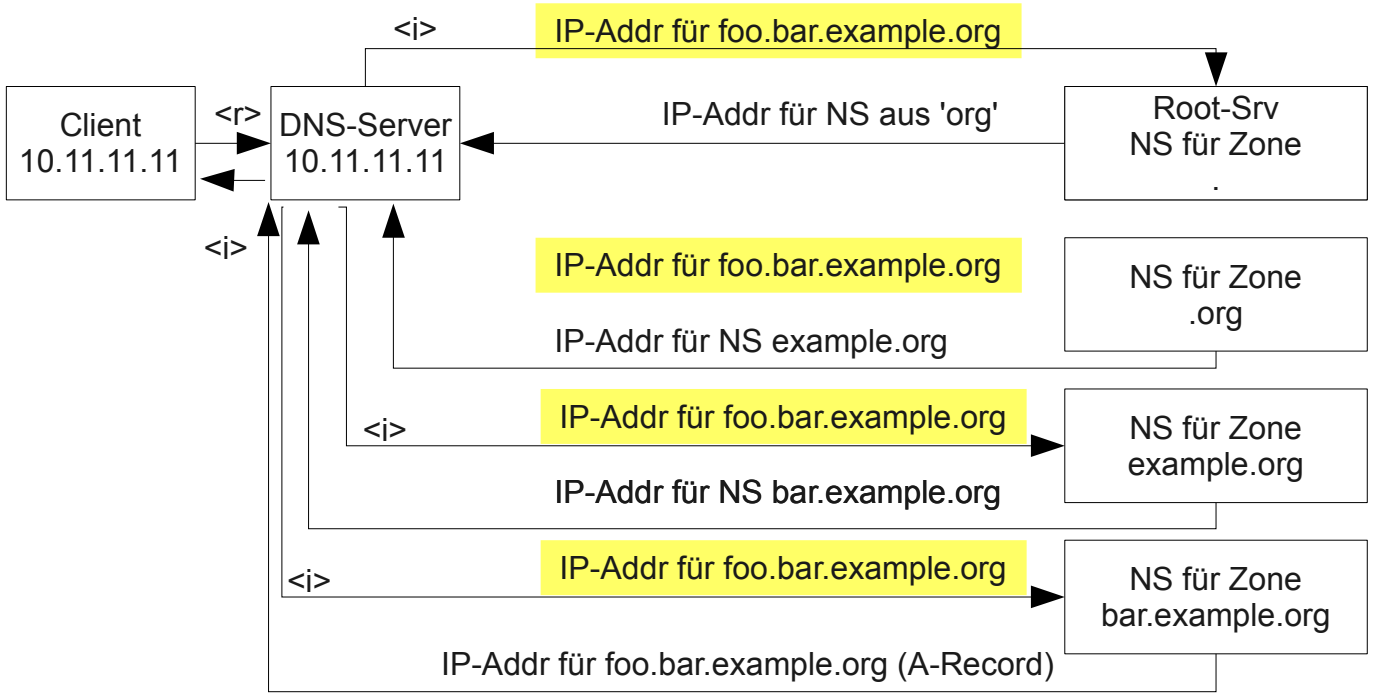


Abbildung 6: DNS-Zonen

b.nic.ch kann die Zone als Master oder Slave hosten. Zonenfiles für Forward + Reverse Lookup-Zone.

Falls eine DNS-Zone auf einem DC als „Active Directory integrierte DNS Zone“ betrieben ist, ist die Unterscheidung Master/Slave hinfällig (-> Multimaster-Betrieb). (LAP-Frage! Vgl. ^^). Einspeicherung der RR im LDAP-DIT!!!

3.5 Prozess der Namensauflösung – rekursive und iterative Queries



<r> rekursive DNS-Abfrage Ziel = Vollständige Auflösung
<i> Iterative Anfrage Ziel = bestmögliche Antwort, typisch ist NS der nächst tieferen Zone

Abbildung 7: Namensauflösung

3.6 Vorteile der AD integrierten DNS-Zonen

Vorteile einer AD integrierten DNS-Zone gegenüber einer Standard-DNS-Zone:

- Multimaster-Betrieb für DNS: RR können auf jedem DC geupdatet werden -> Kein Master / Slave Betrieb der autorisierenden DNS-Server
- Replikation der RR mit AD-Replikation, da die RR wie andere AD-Objekte im LDAP-DIT gespeichert werden
- DDNS-Fähigkeit (ab W2k3-DHCP-Server) (Jedoch auch mit Bind möglich!)

3.7 Dynamisches DNS

Dynamisches DNS (DDNS) kann in Windows-Umgebungen eingesetzt werden. Änderungen an den IP-Adressen, die der Client per DHCP zugewiesen bekommt, werden automatisch in die Zonendatei geschrieben.

- Der DHCP-Client schreibt den A-Record in das Forward-Lookup-File
- Der DHCP-Server schreibt den PTR-Record in das Reverse-Lookup-File

Läuft der DHCP-Eintrag ab, entfernt der DHCP-Server beide Einträge.

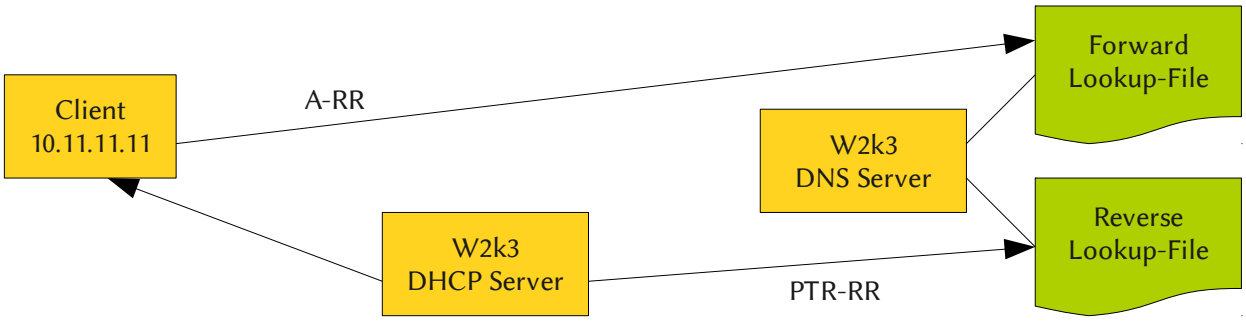


Abbildung 8: DDNS

1. Der DHCP-Server vergibt den Client eine IP-Adresse
2. Die IP-Adresse, die der DHCP-Server vergibt, wird als PTR-Record im Reverse Lookup-File vom DNS-Server eingetragen
3. Der Name / FQDN vom Client wird im Forward Lookup-File vom DNS-Server eingetragen.

3.8 Ressource-Record Types

RR	Beschreibung	F / R
A	Host-Eintrag	F
MX	Mailserver	F
SRV	Active Directory Service Komponente (z.B. Für LDAP-Server, Global Catalog-Server, Kerberos-Server)	F
PTR	ip-addr zu FQDN	R
SOA	Administrations-Angaben zu Zonendatei z.B. Gültigkeitsdauer der gecachten RR	F UND R !!!
NS	Eintrag zur Aufführung eines Nameservers	F UND R !!!

Tabelle 4: Ressource-Record Types

F / R = Forward- (F) oder Reverse-Lookup (R) Zonendatei

Wichtige SRV-RR

In einer AD-Umgebung sind folgende Dienste mit dem Ressource-Record-Type SRV gebräuchlich:

- _ldap: LDAP-Server
- _kerberos: Kerberos
- _kpasswd: Kerberos-Kennwortänderung
- _gc: Globaler Katalogserver

SOA-Zone

Beispiel:

```
example.com. IN SOA master.example.com. hostmaster.example.com.  2007061501 3600
1800 604800 1800
```

Name	der Zone
IN	Zonenklasse (meist IN für Internet)
SOA	Kürzel für *Start Of Authority*
Primary	Primary Master für diese Zone, hat in der Praxis nur geringe Bedeutung • er definiert, an wen dynamische Updates gesendet werden sollen (siehe Dynamisches Update) • er gibt an, an wen keine Notifies gesendet werden (siehe Zonentransfer)
Mail-Adresse	des Verantwortlichen für diese Zone. (Das „@“ wird durch „`.`“ ersetzt. Punkte vor dem „@“ werden durch „`\.`“ ersetzt.)
Seriennummer	wird bei jeder Änderung inkrementiert (vorzugsweise JJJJMMDDVV dient als Hinweis, wann die Zone zuletzt aktualisiert wurde)

Refresh	Sekundenabstand, in dem die Slaves anfragen, ob sich etwas geändert hat (lt. Ripe-203 86400 (24 Stunden))
Retry	Sekundenabstand, in denen ein Slave wiederholt, falls sein Master nicht antwortet (lt. Ripe-203 7200 (2 Stunden))
Expire	wenn der Master auf einen Zonentransfer-Request nicht reagiert, deaktiviert ein Slave nach dieser Zeitspanne in Sekunden die Zone (lt. Ripe-203 3600000 (1000 Stunden))
TTL	negativ-Caching-TTL (lt. Ripe-203 172800 (2 Tage)) (siehe DNS-Caching)

3.9 Zonendelegierung und Glue Records

- Zonen werden delegiert, um den Verantwortungsbereich der DNS-Administratoren einzugrenzen
- Um die Serverlast auf den Root-Servern einzugrenzen

3.9.1 Beispiel

Folgendermassen geschieht die Delegierung der Domain sbb.ch:

- . (Root) (Zonen-Delegierung) --> .ch --> .sbb --> alle Computer der SBB

Organisation der Zonendelegierung für sbb.ch

- Im Forward-Lookup-Zonen-File für Zone .ch sind zwei Einträge erforderlich
  - den Host ns1.sbb.ch als NS für sbb.ch definieren
  - Bekanntgabe der IP-Adresse des NS (Glue-Record)

Forward-Zonendatei auf dem .ch-Nameserver

```
; Zonenfile von ch.
$ORIGIN sbb.ch                ;alle folgenden Einträge sind für sbb.ch gültig
@ IN NS ns1.sbb.ch            ;Nameserver von SBB
@ IN NS ns2.sbb.ch            ; ''
ns1 IN A 194.150.245.3        ;Glue-Record (geleimt, immer gültig ^^)
ns2 IN A 194.150.245.4        ;Glue-Record (geleimt, immer gültig ^^)
```

3.10 Reverse-Lookup

Mit Reverse DNS-Abfragen kann man IP-Adressen in Hostnamen umwandeln. Dazu verwendet man die PTR-Records und die Domain 'in-addr.arpa'.

3.10.1 Die in-addr.arpa-Zone

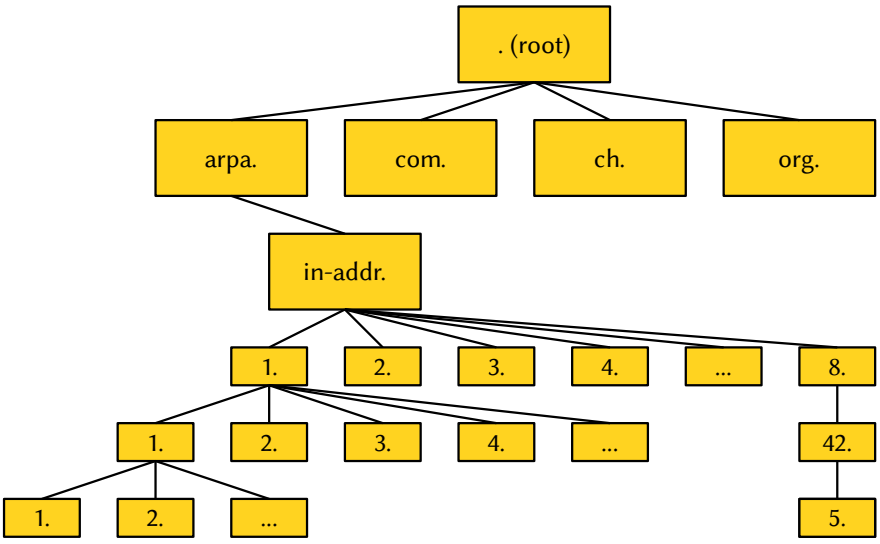


Abbildung 9: Domain 'in-addr.arpa'

3.10.2 Ablauf

Wir haben die IP-Adresse

- Client fragt Nameserver nach dem PTR-Record zur IP-Adresse (23.5.42.8)
- Der Nameserver ändert die IP-Adresse in eine FQDN. Dafür wird die IP-Adresse rückwärts geschrieben (8.42.5.23.in-addr.arpa).
- Der Nameserver fragt jetzt die Zone in-addr.arpa, wer zuständig ist für die Zone 23.in-addr.arpa. So geht er iterativ alle Nameserver durch. Wie bei einer normalen iterativen DNS-Abfrage.

3.11 DNS-Zonentransfer

Der SOA-RR gibt im TTL-Feld an, wie lange die RR gültig sind (typisch 12h).

Der Slave-Zonen-DNS-Server fordert die SOA des Master-DNS-Server an. Der Slave vergleicht die Serial Number mit der Serial Number der eigenen SOA. Wenn die Master Serialnumber grösser ist, dann geschieht ein Zonentransfer:

- AXFR: Übertragung der vollständigen Zone (TCP)
- IXFR: Inkrementelle Zonenübertragung (nur die geänderten RR) (TCP)

- NOTIFY-Methode: Der Master Server meldet nach jedem Update der Zonendatei den NS-RR eingetragenen DNS-Servern die neue Serial-Number. Die Slaves können dann per AXFR oder IXFR die Zonendatei übertragen.
- Server-Hol-Methode: Der Server sieht anhand des SOA-Records, ob es eine Änderung gab.

Die Zonenübertragung läuft über TCP. Das ist beim Erstellen von Firewall-Regeln wichtig.

```
c:\tmp>nslookup
> set type=axfr
> server ns1.eris.org
Standardserver:  ns1.eris.org
Address:  23.5.42.3
> ls -d eris.org
[ns1.eris.org]
 eris.org.   SOA    eris.org hostmaster.eris.org. (2010040517 10800 3600 604800
86400)
 eris.org.   NS     ns1.eris.org
 eris.org.   NS     ns2.eris.org
 eris.org    A      85.124.23.250
 eris.org.   MX     10   mail.eris.org
 mail        A      23.5.42.4
 ns1         A      23.5.42.3
 ns2         A      23.5.42.4
[...]
```

3.12 Typisches DNS-Konzept

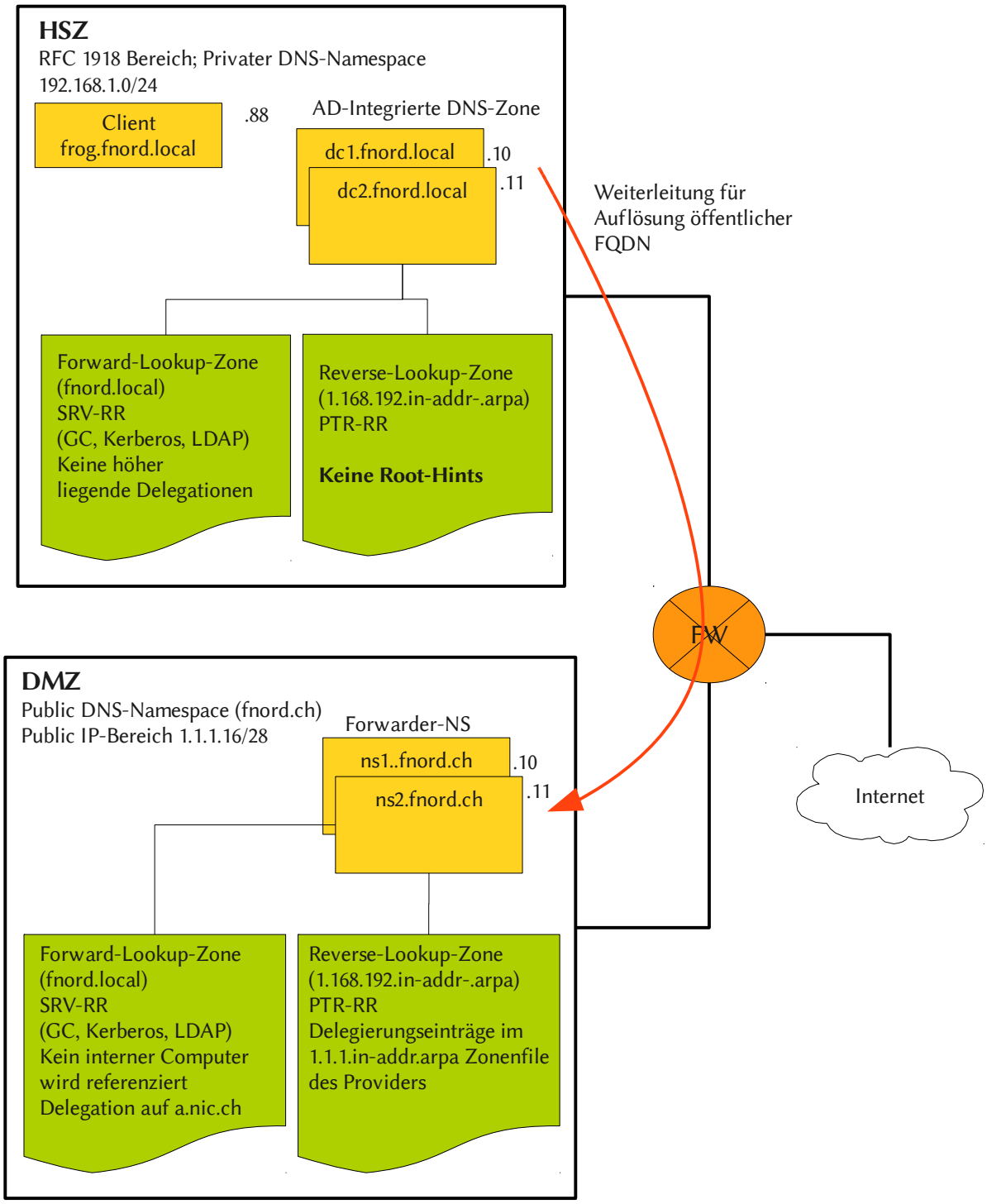


Abbildung 10: DNS-Konzept

4 AD Rechte und Berechtigungen

4.1 Unterscheidung zwischen Rechten und Berechtigung

Englisch: Rights and Premissions

Rechte: Diese bekomme ich um etwas zu machen:

Berechtigung: Auf eine Ressource

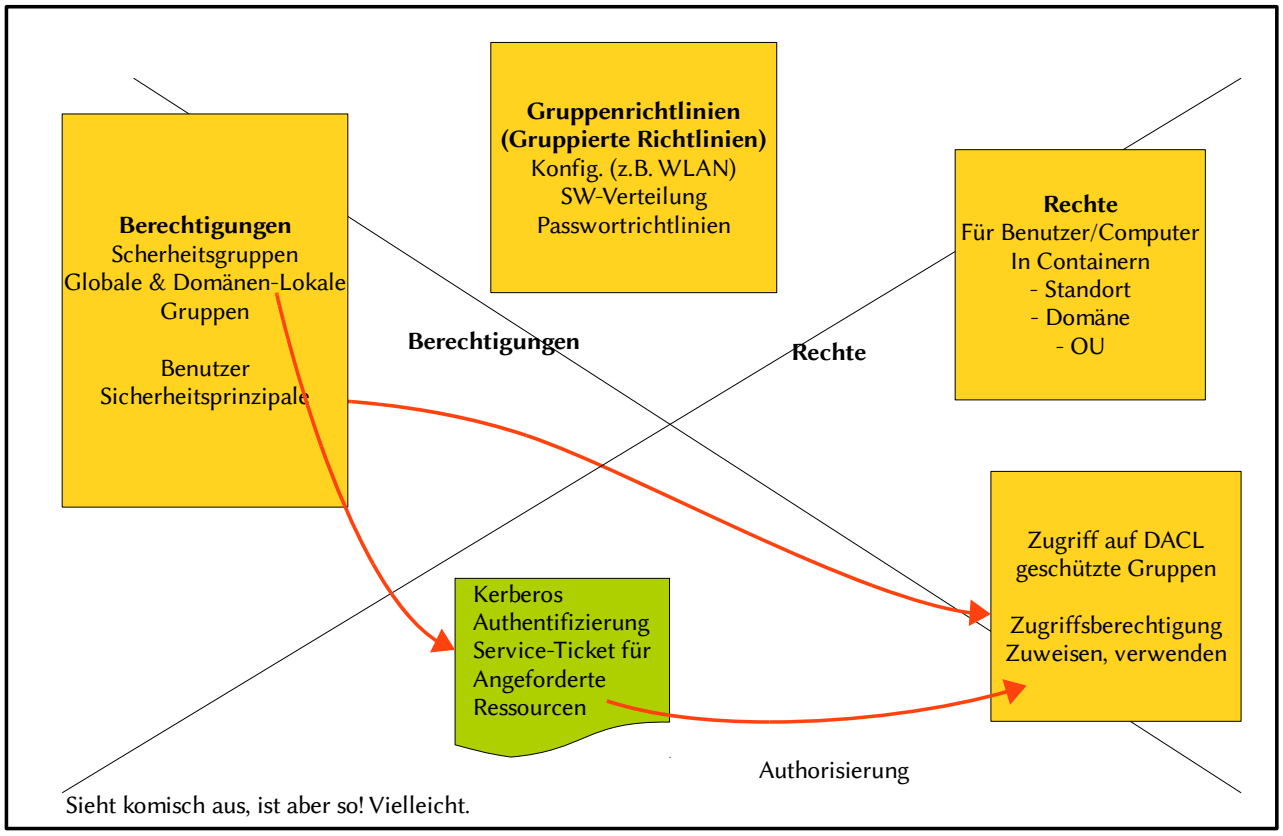


Abbildung 11: Rechte und Berechtigung

Sicherheitstoken: Enthält Sicherheitskennung und Sicherheitsgruppen; wird von Kerberos übergeben

- Sicherheitsrichtlinien werden mit Group Policies (GPOs) erstellt.
- Diese können auf LDAP-Containerobjekte angewandt werden (OUs, Domänen und Standorte).
- Diese Container enthalten wiederum Objekte, die so genannten Leaves (Computer und Benuzter (Nicht Gruppen!!!)).

4.2 Elemente der Ressourcen-Zugriffsverwaltung

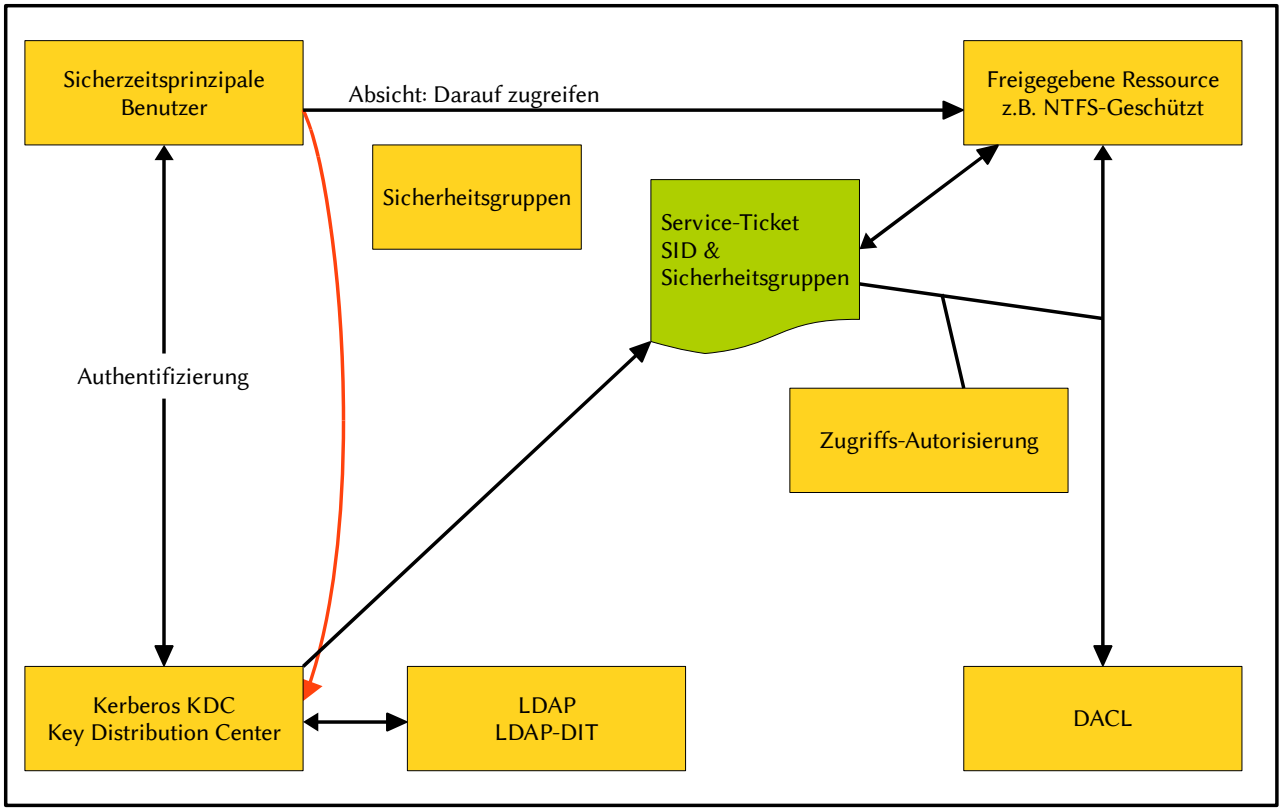


Abbildung 12: Elemente der Zugriffsverwaltung

Sicherheitsprinzipale: Identität von Benutzern oder Computern in den Domänen des ADS; Eindeutig durch SID (Security Identifier)

4.3 Zugriffskontrolllisten

- **ACL**: Access Control List
  Liste von Einträgen mit denen der Zugriff auf Ressourcen geregelt werden kann.
- **DACL**: Discretionary Access Control List
  Zugriffskontrolle beim Ressourcenzugriff (eigentliche Zugriffssteuerung)
- **SACL**: Security Access Control List
  Zur Definition zur Überwachungsaufträgen auf Ressourcen (Steuerung der Überwachung des Zugriffs auf Ressourcen)

4.4 AD-Steuerung des Ressourcen-Zugriffs

Diese zweistufige Zuweisung vom Berechtigungen wird von Microsoft empfohlen und gilt für die LAP als Standard. Alles andere was trotzdem funktionieren würde ist falsch und nicht gültig und kann direkt den Hasen gegeben werden! Seite 220 bis 221 im Buch ist dies beschrieben.

4.4.1 Übersicht

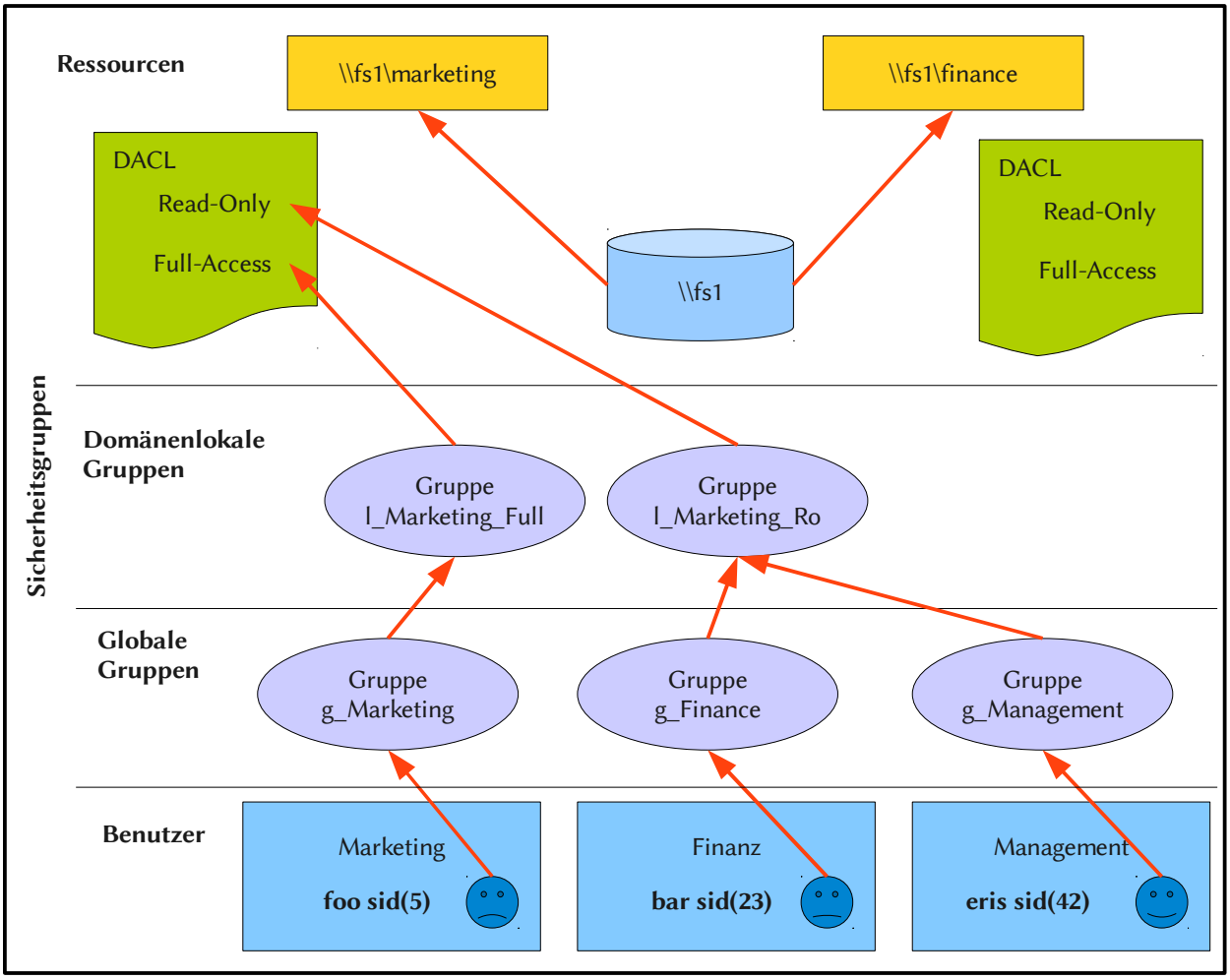


Abbildung 13: Ressourcen-Zugriff

4.4.2 Vorteile

- Flexibilität
- Minimierung der DACL

4.4.3 Beschreibung und was möglich ist

- Benutzeraccounts werden immer (!) in Globale Gruppen gelegt.
- Globale Gruppen dienen nur dem Zweck Personen zu ordnen und sortieren
- Mehrere Globale Gruppen können verschachtelt werden.
- Globale Gruppen werden in Domänenlokale Gruppen zugeordnet.
- Domänenlokale Gruppen lassen sich nicht verschachteln. (Containmenttechnik)
- Einzelne Ressourcen erhalten ihre Berechtigung immer (!) via Domänenlokale Gruppen.

- Für jede Berechtigungsart (Readonly, Full) gibt es eine eigene Domänenlokale Gruppe! Demnach gibt es eine Domänenlokale Gruppe für Readonly und eine Domänenlokale Gruppe für Full.
- Domänenlokale Gruppen können nicht in Lokale Gruppen gelegt werden.
- DL Gruppen sind zur Berechtigungsvergabe auf Shares für globale Gruppen, das kann auch nur für ein Projekt geben, wo am Anfang vielleicht nur ein Benutzer ist.

4.5 Gruppenrichtlinien

Autoamtisch OU Domain Controllers mit allen Dcs.

Strukturierung AD:

- OU_Infrastrukturserver
  - Radiusserver
  - Fileserver
  - Printserver
- Domain
- Standorte

4.5.1 Was sind GPOs?

- Dem Client werden GPOs gesetz anhand Funktion, Standort, Gruppenmitgliedschaft.
- Benutzer erhält egal wo er sich im AD anmeldet seine GPOs

4.5.2 Auf was werden diese gesetzt?

GPOs kann man auf Standorte, Domänen, Organisationseinheiten (OU) linken

Wenn keine GPO vorhanden, dann wird die lokale GPO verwendet.

Abarbeitungsreihenfolge der Richtlinien für Benutzer und Computer

1. Lokale GPO
2. Standort (Site)
3. Domänen GPO
4. Organization Unit GPO
5. Benutzer

Richtlinien werden addiert oder wenn unterschiedlich überschrieben von oben nach aben!

Bei widersprüchlichen GPOs wird diese näher am Benutzer genommen.

4.5.3 Vererbung

- Richtlinien werden vererbt wenn sie aktiviert, nicht aktiviert sind

- nicht konfigurierte werden nicht vererbt

4.5.4 Inhalt GPO

- Computerkonfiguration: PC-Konfig. wird bei jedem Start angewendet
- Benutzerkonfiguration: Je Benutzer am PC
    - Softwareeinstellungen
    - Windows-Einstellungen
        - Skripte
        - Sicherheitseinstellungen
    - Administrative Vorlagen

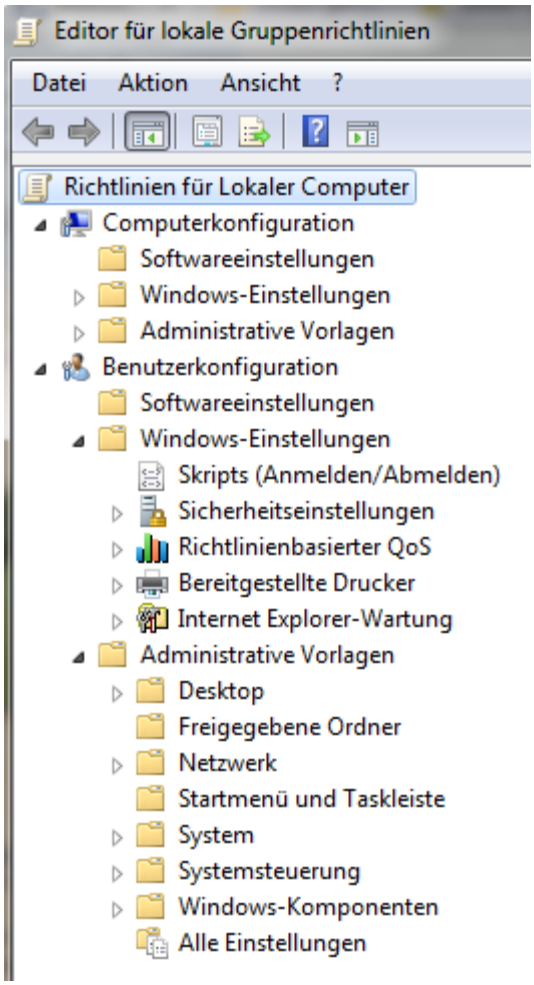


Abbildung 14: Gruppenrichtlinien

Softwareeinstellungen

Erstellung, Konfiguration neuer Pakete für Softwareverteilung

Windowseinstellungen

Knoten	Beschreibung
Skripte	Ab- und Anmelden von Users; Hoch- und Herunterfahren von PCs
Sicherheitseinstellungen	Kontorichtlinien etc. detaillierte Einstellungen für User, PCs
Internet Explorer	Alle IE Einstellungen (Proxy etc.)
Remote-Installationsdienste	Einstellungen für Remote ~
Ordnerumleitung	Eigene Dateien etc. verschieben z.B.

Administrative Vorlagen

HKEY_LOCAL_MACHINE und HKEY_CURRENT_USER Registry Einstellungen werden hier konfiguriert. Können manuell nachinstalliert werden z.B. für Office 2007.

Dazu zählen:

- Windows Komponenten (MSN, IE, Installer)
- System
- Netzwerk (LAN, DFÜ)
- Drucker
- Startmenü, Taksleite
- Desktop (Hintergrund, Bildschirmschoner)
- Systemsteuerung

4.5.5 Abarbeitung der GPO für Benutzer und Computer

Sobald RPC-Dienst (Remote Procedure Call) gestartet ist, werden Computerkonfigurations GPOs abgearbeitet

Nach Benutzerauthentifizierung wird Profil geladen, Abarbeitung GPO

Lokal-> Standort -> Domäne -> OU

Danach kommen die Login-Skripte

Das ist standardmässig so, Ausnahmen sind möglich mit folgenden Optionen

Kein Vorrang	Durchsetzung wird erzwungen mit dieser Option haben zwei GPOs diese Option wird wieder das näher am Benutzer genommen
Deaktiviert	GPO wird an jeweiligem Container nicht durchgesetzt
Loopback	Computerkonfiguration hat Vorrang vor der Benutzerkonfiguration

Weitere Informationen

- http://emanuelduss.ch
  Weitere Zusammenfassungen, Dokumentationen und Dokumente von mir
- http://inf.ifrag.ch
  Das Forum der Informatiklernenden
- http://www.zytrax.com/books/dns/
  Englisches DNS Buch

Glossar

Begriff	Definition
~	„Die Tilde steht für viele Verzeichnisse“ - Zitat BBZWITS-Lehrer
ACL	Access Control List
AD	Active Directory
AD DS	Active Directory Domain Services
CN	Common Name
DAP	Directory Access Protocol; Abfragesprache
DC	Domain Component
DIB	Directory Information Base; Alle Objekte eines Verzeichnisses
DISP	Directory Information Shadowing Protocol; Protokoll zur Replikation von Informationen
DIT	Directory Information Tree; In der DIB vorhandene Informationen
DN	Distinguished Name; Eindeutiger Bezeichner eines Objekts
DNS	Domain Name Services; Dienst zur Namensauflösung
DOP	Directory Operational Binding Management Protocol; Protokoll zur Verberitung von Informationen
DSA	Directory System Agent; Verzeichnis-Server
DSP	Directory System Protocol; Kommunikationsprotokoll zwischen X.500-Servern
DUA	Directory User Agent; Verzeichnis-Client (Verzeichnis-Benutzer-Agent)
Forest	Domänengesamtstruktur
Forest	Gesamtstruktur
KDC	Key Distribution Center; Stellt TGT-Tickets aus
Kerberos	Authentifizierungsprotokoll
LDAP	Lightweight Directory Access Protocol
NDS	Novell Directory Services; Verzeichnisdienst von Novell
OU	Organizational Unit
RDN	Relative Distinguished Name; Relativen Bezeichner; in DN enthalten
SID	Security Identifier
TGT	Ticket Granting Ticket; Ticket zum Nachweisen einer Authentifizierung
Tree	Domänenstruktur
UPN	User Principal Name
X.500	Standard für den Entwurf eines globalen Verzeichnisdienstes

Stichwortverzeichnis