Freie Universität Berlin

IMP-IT Verzeichnisdienste

Carsten Schäuble – IT-Dienst MI

Verzeichnisdienste: Ablauf

- Wozu Verzeichnisdienste?
- Welche Verzeichnisdienste gibt es?
- Zugriffsprotokolle?
- Demos von Openldap und Active Directory
- Beispiele von Verzeichnisdiensten
- Verwaltung von Verzeichnisdiensten

Verzeichnisdienste: Definition

- Verzeichnisdienste stellen eine zentrale Sammlung von Daten dar.
- Daten werden hierarchisch gespeichert.
- Zugriffe erfolgen zumeist nach Client-Server-Modell
- Innerhalb eines festen Protokolls
- Es können Daten und Objekte aller Art gespeichert werden, z.B. Telefondaten, Benutzerdaten für Zugangs- und Berechtigungssteuerung usw.
- Prinzipiell können alle Betriebssysteme und Dienste mit derartigem Datenbedarf angegliedert werden.

Verzeichnisdienste: Nutzung

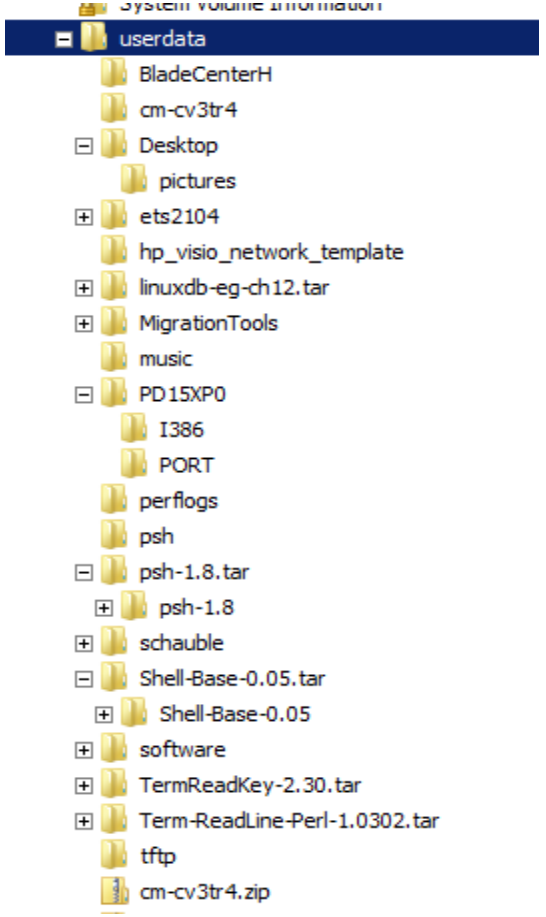
- Authentisierung und Autorisierung von Benutzerdaten unter
  - Windows
  - Unix
  - MacOs
  - Telefonanlagen

Verzeichnisdienste: Nutzung

- Authentisierung und Autorisierung in Applikationen
  - Apache
  - Mailserver z.B. MS Exchange, Lotus Notes
  - Telefonverzeichnisse
  - SAP
  - E-Mail Klient

Verzeichnisdienste: Einfaches Beispiel

- Dateisystem
  - ist hierarchisch über Verzeichnisse und Links
  - speichert Daten in beliebiger Form
  - Ist über Netzwerker-weiterungen voll hierarchisch erweiterbar -z.B. NFS, CIS



Verzeichnisdienste: komplexes Beispiel

- Active Directory (Demo)
  - LDAP
  - Kerberos
  - Komponenten
  - Fremdsystemintegration
  - Referral-Beispiel

Verzeichnisdienste: Beispiel Linux-PAM

- Passwd
- Group
- Automounter
- ➢ Livedemo Poolrechner

Verzeichnisdienste: Datenschutz/-sicherheit

- Gesicherte Datenübertragung bei der Autentisierung
- Übertragung schützenswerter Daten
- ACLs in Verzeichnissen
- Implementierung von Zugriffsmechanismen über Datenstrukturen in Verzeichnissen

LDAP - Überblick

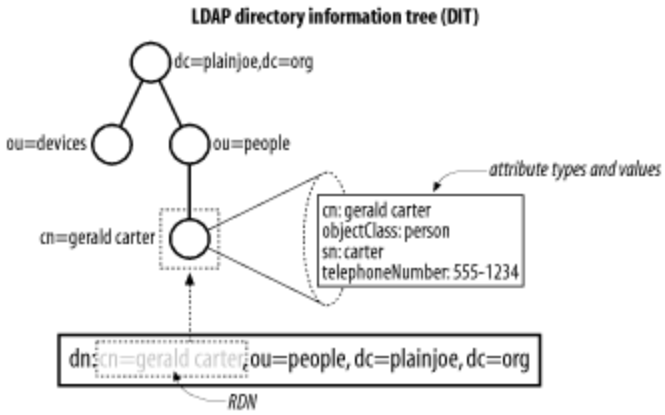
- Lightweight Directory Access Protocol (LDAP)
- Abfrage und Modifikation von Verzeichnisdiensten über IP-Netzwerk
- Client-server-protokoll
- RFC 4511
- Kommunikation erfolgt über Abfragen
- Vereinfachte Version von DAP als Teil von X.500

LDAP - Modelle

- Informationsmodell:
  - Beschreibt Struktur und Daten des Directory Information Trees (DIT).
  - Einträge im DIT werden als ObjektClass modelliert
  - Atrribute dieser ObjektClasses haben definierte Datentypen, Kodierungen und Operatoren

LDAP - Modelle

- Namensmodell:
  - Beschreibt wie Objekte im DIT eindeutig referenziert werden können.
  - Auf jeder Objektebene ist ein Eintrag über ein Attribut eindeutig – relative distinguished name (RDN)
    cn=carsten schauble
  - Objekte haben einen global eindeutigen Pfad (DN)
    cn=carsten schauble, ou=people, dc=fu-berlin, dc=de



LDAP - Modelle

- Funktionales Modell
  - Das LDAP Protokoll selbst.
  - Beschreibt Zugriffe schreibend und lesend im DIT
  - Zugriff ist implementiert über authentisierte Operationen (bindings), Abfragen (searches and reads) und updates (writes).
- Sicherheitsmodell
  - Prüft Identität eines Anfragendes (authentication) und dessen Zugriffsrechte (authorization).
  - Verschiedene Protokollstufen (akt. V3) haben diverse Authentisierungsmethoden implementiert.
  - ACLs sind nicht standardisiert, aber weit verbreitet.

Das LDAP-Transportformat - LDIF

- Klartextformat zum Transport und zur Veränderung von LDAP-Daten.
- Als Ansicht für LDAP-Informationen im Klartextformat besser geeignet als Binärdarstellung
- LDAP Interchange Format (LDIF), definiert in RFC 2849
  - Zusammenstellung von Einträgen, separiert durch Leerzeilen
  - Abbildung von Attribut-Namen zu –Werten
  - Zusammenstellung von direktiven für den Parser zur Anwendung der Informationen
- Import und Änderung von Daten
- Daten müssen dem Schema genügen

LDIF

```
dc=fu-berlin,dc=de:
# LDIF listing fuer dn: dc=fu-berlin,dc=de
dn: dc=fu-berlin,dc=org
objectClass: domain
dc: plainjoe
```

- # Kommentar
- :_ trennt Attribut vom Wert
- Dn Attribut adressiert Eintrag eindeutig

LDIF - Normalisierung

- Entferne alle white spaces ohne escape Sequenz um =
- Entsprechende Zeichen müssen mit dem Excape-Zeichen \ versehen sein
- Alle nicht Escape-Zeichen um das RDN-Join-Zeichen + müssen weg
- Abschließende Leerzeichen müssen weg

aus:

cn=schauble + ou=it, dc=fu-berlin, dc=de

wird:

cn=schauble+ou=it, dc=fu-berlin,dc=de

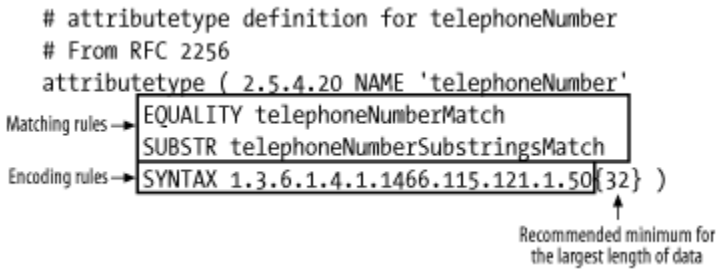
LDIF: Attribute? Classes? Dc?

- Attribute beinhalten Wert(e) mit festen Typen und syntaktischen Regeln
- Attribute können mehrere Werte haben (Liste)

```
# LDIF listing for dn: ou=devices,dc=fu-berlin,dc=de
dn: ou=devices,dc=fu-berlin,dc=de
objectclass: organizationalUnit
ou: devices
telephoneNumber: +49 30 838 75176
telephoneNumber: +49 30 838 75460
description: Container for all network enabled
 devices existing within the fu-berlin.de domain
```

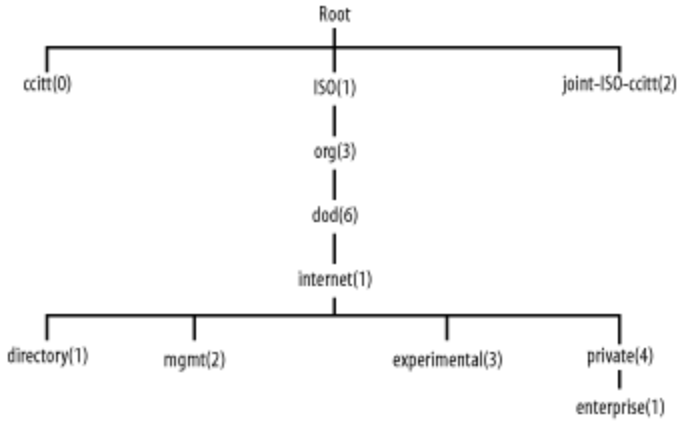
LDIF: Attribute? Classes? Dc?

- Attributsyntax
  - Legt fest in welchem Format Daten gespeichert werden
  - Wie Vergleiche gemacht werden
  - z.B. telephoneNumber
    - A-z, A-Z, 0-9, „, . - ? Usw.



Einschub LDIF: OID

- LDAP nutzt OIDs (ähnlich dem SNMP-Standard)
- OIDs werden durch die IANA unterhalb von mgmt2 vergeben
- Ist eine Zeichenkette bestehend aus Ganzzahlen und Punkten
- OID adressiert eindeutig ein Objekt
- Bezeichnet
  - Attribute,
  - ‚Syntaxen‘,
  - Objekt-Klassen
  - Controls

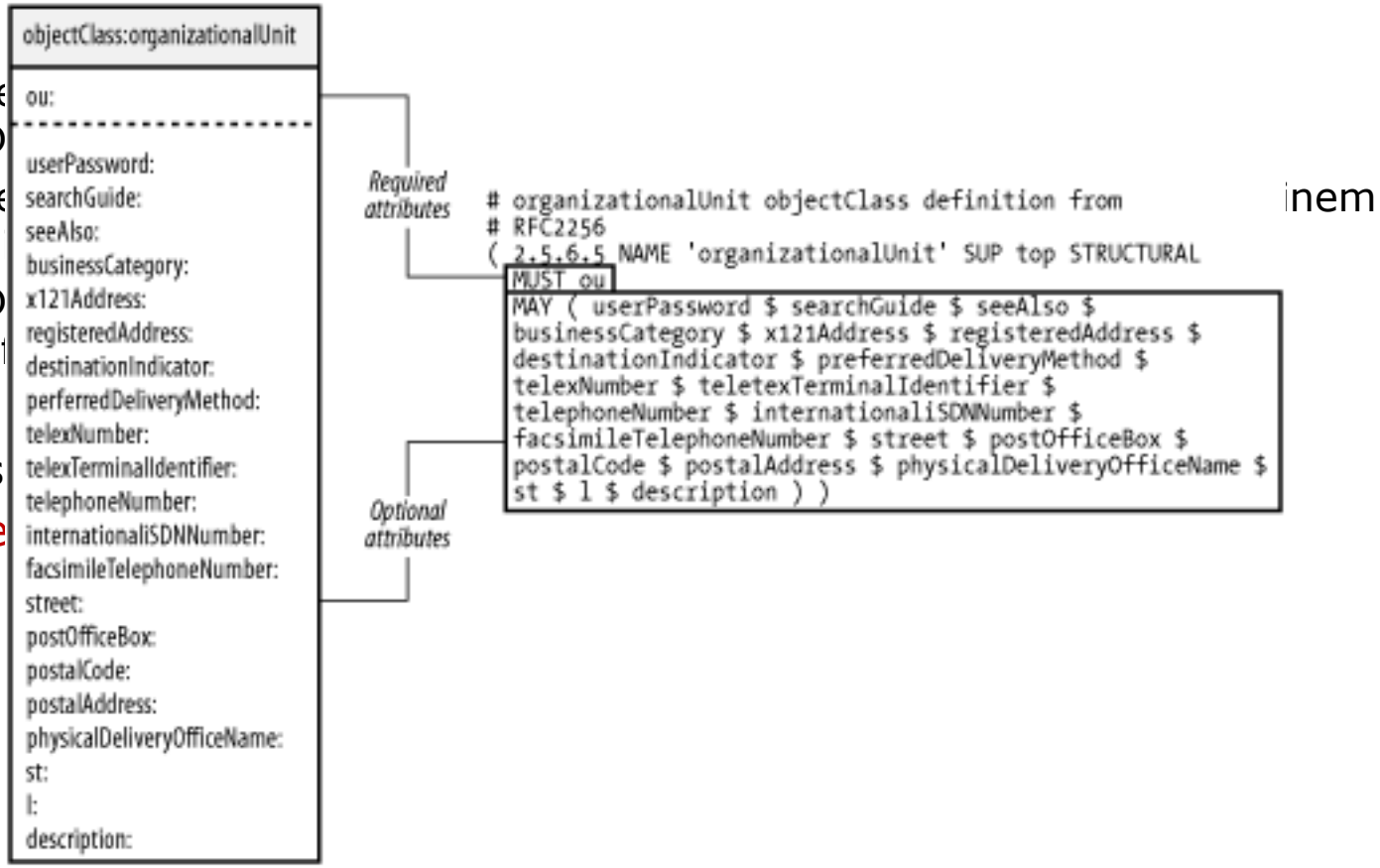


LDIF: objectClasses

- Je
  D
- Je
  E
- D
  P

Beis

obje



inem

LDIF: objectClasses

- ObjectClass besitzt eine OID wie z.B. es auch Attribut Typen, Kodierungen und Vergleichsregeln haben
- MUST gibt Pflichtattribute an,
- MAY definiert optionale Attribute
- SUP definiert das Elternobjekt (parent)
- ObjectClasses können gemeinsame Attribute haben
- Attribute sind ‚flach' definiert.

LDIF: objectClasses Typen

- Structural: Reales Objekt wie person oder organisationalUnit
- Auxiliary: Fügt Charakteristika zu Objekten hinzu. Können nicht eigenständig genutzt werden.
- Abstract: OO, als abgeleitet Klasse etc.
- Typ kann nicht geändert werden

LDIF: DC

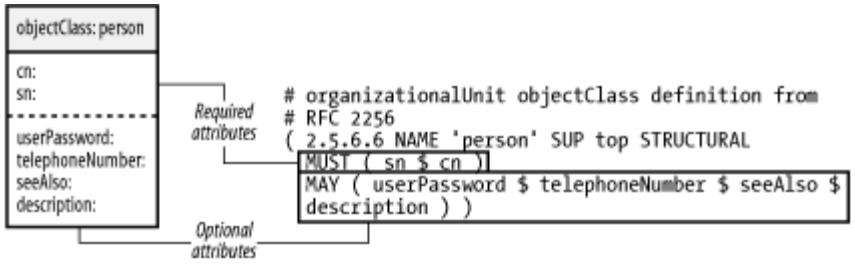
- Original wurde im X.50 Std. der Namensraum durch Geographische und nationale Bereiche aufgespannt.
  Bsp.: X.400 dn: o=fu-berlin, l=berlin, c=germany
- Es gibt aber keine zentrale Möglichkeit, diese Namen zu registrieren!
- RFC2247 bietet die Möglichkeit, den DC auf Basis der DNS-Zone zu bilden -> eindeutig
- Ein DirectoryName (DN) ist der größtmögliche gemeinsame Eintrag, also z.B. dc=fu-berlin, dc=de und bestimmt, ob ein Server für eine Anfrage zuständig ist.
- Ein DomainContext (DC) ist ein Teilobjekt, welches den DN aufspannt
  Bsp.: dn: dc=imp,dc=fu-berlin,dc=de
- Ähnlich dem DNS antwortet ein LDAP-Server nur auf Abfragen unterhalb seines DNs

LDIF: Schema

- Das LDAP-Schema und dessen strukturelle Abkürzungen sind riesig!
  - RFC 3377 and related LDAPv3 standards (http://www.rfc-editor.org/)
  - LDAP Schema Viewer (http://ldap.akbkhome.com/)
  - Object Identifiers Registry (http://www.alvestrand.no/objectid/)
  - Sun Microsystems Product Documentation (http://docs.sun.com)

Authentication

- Direkte Kodierungen: {CRYPT},{MD5}, {SHA},{SSHA}

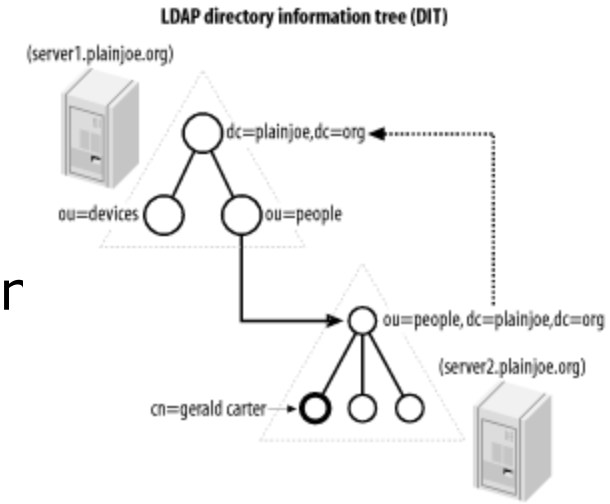


userPassword:
{MD5}Xr4ilOzQ4PCOq3aQ0qbuaQ= =

- Bindungstypen
  - Anonymous Authentication
  - Simple Authentication
  - Simple Authentication over SSL/TLS
  - Simple Authentication and Security Layer (SASL)

Verteilte Verzeichnisse

- Verteilung zur
  - Geschwindigkeitssteigerung
  - Geographischen Lokalisierung
  - Entlang von Zuständigkeitsbereicher
- Setzen von Links




```
# LDIF listing for the entry ou=people,dc=plainjoe,dc=org
dn: ou=people,dc=plainjoe,dc=org
objectClass: referral
ref: ldap://server2.plainjoe.org/ou=people,dc=plainjoe,dc=org
```

Schemabeispiel

- SUN NIS Schema für OpenLDAP

Abfragen

- Bedient sich Postfix Notation (reverse polish notation)
- baseDN: Basis der Abfrage, inkl. Basiskontext wie base, sub oder one
- Beispiel:
  ldapsearch -h ldap.acme.com -p 389 -s sub -D "cn=Directory Manager,o=acme" -W -b "ou=personen,o=acme" "(&(mail=joe*)(c=germany))" mail

Abfragen

- Keine Normalformen: LDAP ist ein Frontend zu einer hierarchischen Datenbanken.
- Es gibt keine Normalform; zum Beispiel können „multivalued attributes“ erlaubt sein.
- Abfragesprache:
  - LDAP unterstützt nur Projektion ohne Erzeugung von errechneten Attributen und Selektion
  - Von den relationalen Operationen werden nur Projektion (Spaltenauswahl), Selektion (Zeilenauswahl), Kreuzprodukt (JOIN), Spaltenumbenennung (Rename, AS) und Aggregation (GROUP BY) unterstützt.
  - Kein Join oder einen Dereferenzierungs-Operator gibt es nicht
  - ein Rename und damit ein Selfjoin existiert nicht; Aggregation wird mit Schleifen im Client auscodiert.
  - LDAP-Abfragesprache keine Algebra, es fehlt die Abgeschlossenheit.
  - Abfrageergebnisse von LDAP-Anfragen sind keine LDAP-Bäume, sondern Knotenmengen, und die LDAP-Abfragesprache ist auf LDAP-Ergebnisse nicht wieder anwendbar, um die Ergebnisse zu verfeinern.

Abfragen

Beispiele:

Server: windc1.fu-berlin.de:3269

Base: DC=fu-berlin,DC=de

BindDn: carsten@FU-BERLIN.DE

Filter:

- (&(&(cn=*)(objectClass=inetOrgPerson))(objectClass=posixAcc

ount))

- sAMAccountName=carsten

ldapsearch -x -W -LLL -D carsten@FU-BERLIN.DE -H ldaps://windc1.fu-berlin.de:3269 -b DC=fu-berlin,DC=de sAMAccountName=carsten

LDAP: Duplication/Replication/Updates

- Die Replikation von Verzeichnisdiensten über den LDAP Standard ist nicht spezifiziert. Jeder Hersteller hat eigene Methoden der Replikation

Replikation von Verzeichnissen

- Replikation
  - Warum?
  - Wann?
  - Volle Synchronisation
  - Differenzsynchronisation …
    - über Log-Files
    - über Seriennummern von Einträgen

Replikation von Verzeichnissen

Wozu Verzeichnisdienstreplikation

- Lastverteilung
  - Applikationsspezifische Verzeichnisse
  - Hohe generelle Abfragelast
  - Große Änderungsrate
- Ausfallsicherheit erhöhen
  - Stromausfall
  - Datenkorruption
  - Redundanzen für Umbauten
- Standortreplikation
  - Ressourcenschonung wie Weitverkehrsnetzanbindungen
- … als Backup

Replikation von Verzeichnissen

- Wann wird repliziert?
  - Bei Änderungen
  - Bei wichtigen Änderungen
  - Zeitgesteuert, z.B. Nachts in Außenstellen
  - Bei Neueinrichtungen

  … oder alles zusammen?

Replikation von Verzeichnissen

- Was sind die Voraussetzungen?
  - Keine Herstellerübergreifenden Standards, daher homogene Softwareausstattung, z.B. openLdap in kontrollierten Versionsständen
  - Gleichheit der Datenschemata
  - Erreichbarkeit der Systeme untereinander

Replikation von Verzeichnissen

- Bekannte Replikationsmechanismen
  - openLdap verwendete den SLURPD, der auf einem Change-Log für inkrementelle Änderungen beruht. Änderungen werden über LDAP-Befehle verteilt. Es gibt Push
  - Seit 2.4 Syncrepl mit RFC 4533 mit Active-Active, Multimastermodel
  - Active Directory nutzt DSN-basierte Replikation im Push und Pull-Verfahren. AD kann sowohl über TCP (RPC-Calls) als auch über SMTP replizieren. SMTP wird bei verteilten Forrests über mehrere Standorte verwendet.

Replikation von Verzeichnissen

- Replikation – Erarbeitung als Tafelbild
  - Object SN = Serial Number
  - uSNCreated
  - uSNChanged
  - Sync-Log-File-

Replikation von Verzeichnissen

Syncrepl …

- Consumer based
- Ist direkt in slapd integriert
- Statusorientierte Replikation – push und pull
- Keine Historie oder Log
- Pull-based: periodisch wird der Provider nach Updates gefragt
- Push-based: Updates werden in Realzeit an Consumer übermittelt
- Status wird mit Synchronisationscookies überwacht
- Replikat kann zu jedem Zeitpunkt aus Backup von Provider oder Consumer erzeugt werden.
- Replikat kann jeder Zeit mit dem Inhalt des Providers abgeglichen werden.

Replikation von Verzeichnissen

Syncrepl …

- Löschen über Session log eines Providers, dass entryUUIDs speichert
- Change Sequence Number (CSN) für LDAP-Objekte
- Es gibt eine maximale CSN im Provider
- The format of a CSN string is: yyyymmddhhmmssz#s#r#c where s is a counter of operations within a timeslice, r is the replica id (normally zero), and c is a counter of modifications within this operation
- Wenn kein contextCSN existiert, werden global welche erzeugt.
- Inkonsistenzen werden durch nachfolgende Syncs behoben
- Keine Transaktionssicherheit

Replikation von Verzeichnissen

Syncrepl …

- Faulheit siegt: OpenLDAP-Replication-Strategies.pdf; PDF, Seiten 17 und 19
- Nachteile von LDAP Sync:
  - Objekt basierend
  - Geänderte und nicht geänderte Objekte werden übertragen
  - Viel Datenverkehr für wenige Änderungen

Replikation von Verzeichnissen

DELTA Syncrepl …

- Basiert auf changelog und syncrepl
- Provider speichert Änderungen
- Consumer prüft das Changelog auf benötigte Einträge
- Replikate mit zu großen Differenzen werden weiterhin durch konventionelles syncrepl synchronisiert

=> UUID und Changelog ⇔ sehr geringe Datenlast während voller oder enger Synchronisation

Replikation von Verzeichnissen

Syncrepl Proxy Mode…

- Comsumer initiiert Verbindungen gegen Proxy
- Provider synchronisiert gegen Proxy
- Sinnvoll bei verdeckten oder nicht zugreifbaren Master-Nodes

Replikation von Verzeichnissen

Replikation in heterogenen Verzeichnisumgebungen

- Fall: Metadatenbank synchronisiert auf ein Active Directory und ein OpenLdap.
  - Wie und was wird synchronisiert?
  - Wer ist für die Synchronisation zuständig?
  - In welche Richtungen wird synchronisiert?

Radius

Remote Authentication Dial In User Service (RADIUS)

- Protokoll für die drei As: AAA = Authentication, Authorization, Accounting
- AAA für Computer und Netzwerkdienste
- Enwickelt von Livingston Enterprises im Jahre 1991.
- Späterer IEEE Standard
- Häufig von ISP verwendet für z.B. Internetzugänge, DSL-Auth, Netzwerkkonfigurationen, E-Mail-Diensten, VPN uvm.
- Beschrieben u.a. in RFC 2865 und RFC 2866

Radius

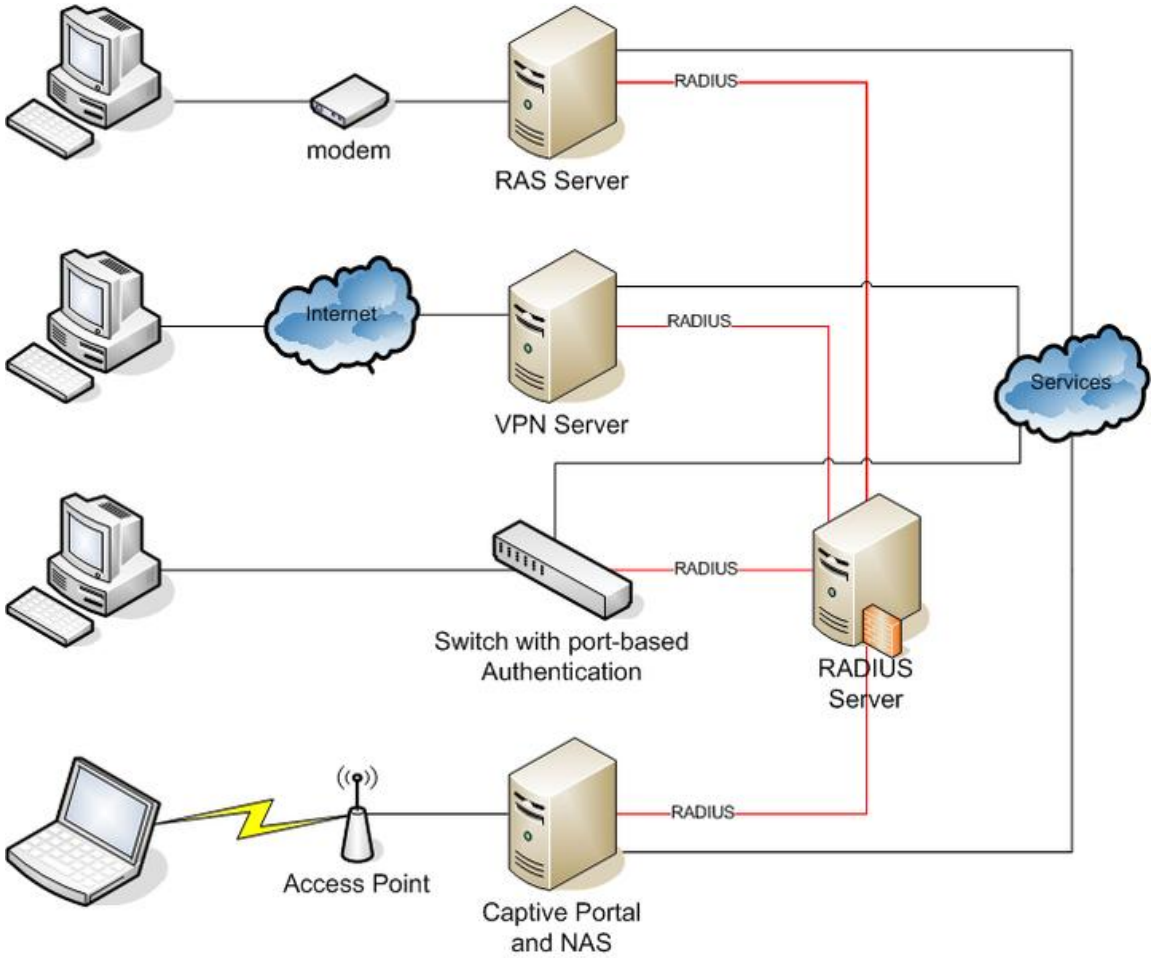
- Client-Server-Protokoll auf Schicht 4
- Verwendet UDP
- Radius-Server werden häufig auf Unix- oder Windows-Servern eingesetzt.
- Integration in Active Directory
- Anschluss an Datenbanken

Radius

Zweck

- Einen Benutzer zu authentisieren bevor er Zugang zu einem Netz/Dienst bekommt
- Die Berechtigungsstufe für authentisierte Benutzer festzulegen
- Die Verbrauchsdaten einer Dienstnutzung erfassen

Radius


modem
RADIUS
RAS Server
Internet
RADIUS
VPN Server
Services
RADIUS
Switch with port-based
Authentication
RADIUS
Server
Access Point
RADIUS
Captive Portal
and NAS

Radius - Authentication and authorization

- Clientensystem sendet einen Request an einen Network Access Server (NAS), um Zugang zu erhalten. Er werden Credentials – Benutzername und Passwort – benötigt
- Dieser Request wird über das Link-Layer-Protokoll übermittelt (z.B. PPP) im Falle von dialup und DSL Providern.
- Der NAS sendet diese Credentials als Radius-Request an den Raiusserver und ggf. zusätzlich Informationen vom NAS-System selbst.
- Der Radius-Server prüft die Informationen anhand bekannter Authentisierungsschemata wie PAP, CHAP und EAP.

Radius - Authentication and authorization

- Nach erfolgter Verifikation antwortet der Radiusserver entweder mit
  - Ablehnung (reject)
  - Challenge: benötigt weitere Informationen wie Pin, Token oder Chipkarte
  - Zustimmung (accept)
- Bei Zustimmung können auch weitere Attribute übermittelt werden wie z.B. IP-Adresse, Telefonnummer, VLAN-ID uvm.
- Moderne Radiusserver können den Login gegen externe Loginsysteme prüfen:
  - SQL-Server
  - Kerberos
  - LDAP
  - Active Directory

Radius - Accounting

- Nach erfolgreichen Login eines Benutzers gegen einen NAS mit Hilfe von Radius kann dieser NAS-Server ein Radius-Paket senden, dass den Namen *Accounting-Start* trägt.
  - Beinhaltet typischerweise Benutzernamen, Netzwerkadresse, Anschlusspunktinformationen und einen Session-Identifier
- Der NAS kann periodische Updates (*interim update*) an den Radiusserver senden.
- Am Ende einer Session sendet das NAS *Accounting Stop* an den Radius-Server

Radius - Session

Beispielausgabe von radwho

zeus:/# radwho

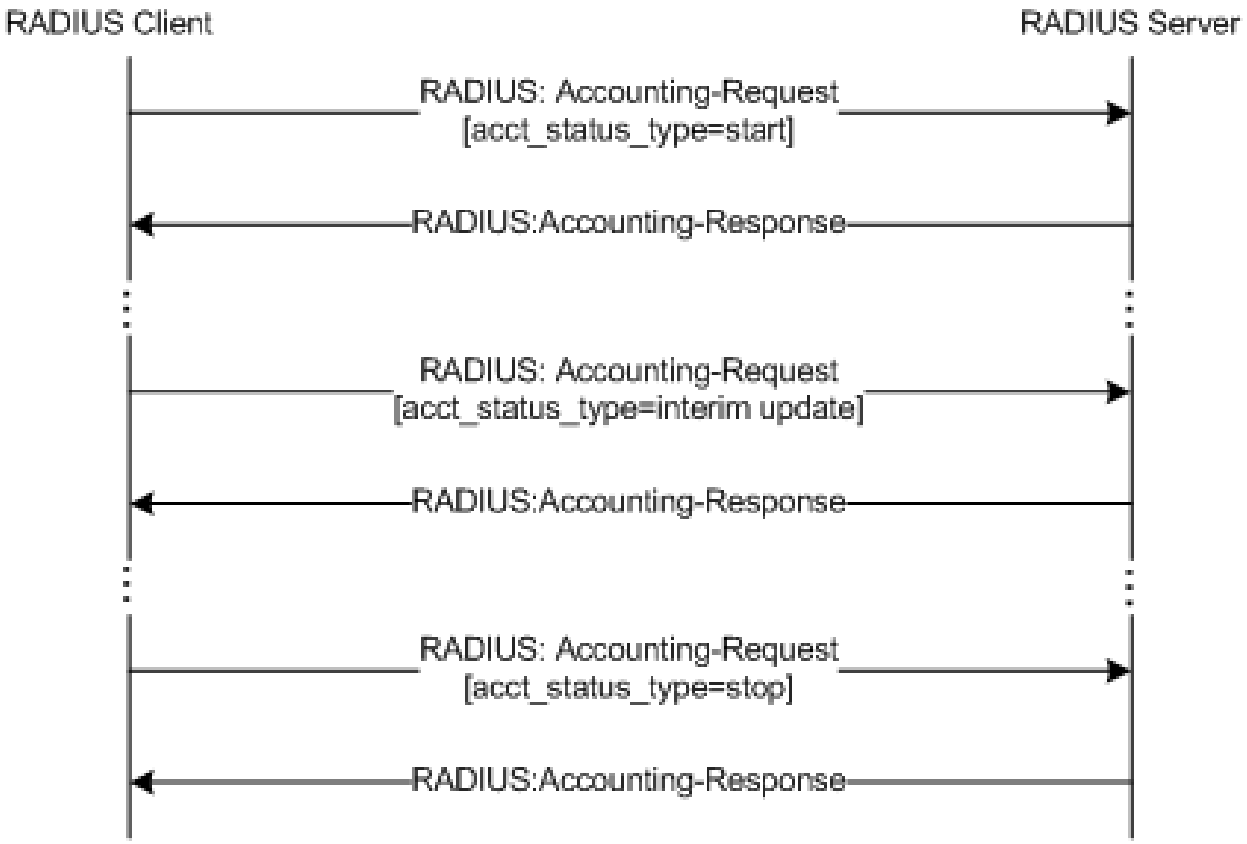
```
Login       Name            What  TTY  When       From       Location
bkunz       bkunz           PPP   S7   Wed 08:1   160.45.11  130.133.48.220
robocup     robocup         PPP   S8   Wed 16:0   160.45.11  130.133.54.96
martni      martni          PPP   S23  Fri 09:5   160.45.11  130.133.51.193
scherfen    scherfen        PPP   S42  Mon 10:4   160.45.11  130.133.52.103
bockmayr    bockmayr        PPP   S46  Tue 10:5   160.45.11  130.133.52.203
preineck    preineck        PPP   S0   Wed 07:3   160.45.11  130.133.48.76
stucki      stucki          PPP   S2   Wed 04:2   160.45.11  130.133.48.22
scharfenbe  scharfenberg    PPP   S1   Tue 15:5   160.45.11  130.133.48.128
akrillo     akrillo         PPP   S3   Wed 07:0   160.45.11  130.133.48.149
ddomazer    ddomazer        PPP   S4   Wed 07:4   160.45.11  130.133.50.26
hochen      hochen          PPP   S5   Tue 13:5   160.45.11  130.133.54.75
```

Radius - Authentication

- Beispieldatensatz für Benutzer schauble für VPN am FB

```
- Tabelle  - ID  - uname   - password – op -        value
"radcheck";39710;"schauble";"Password";"==";„**********"
"radpeply";24464;"schauble";"Framed-IP-Address";"=";"130.133.48.33"
"radpeply";24465;"schauble";"Reply-Message";"=";"Login accepted"
```

Radius

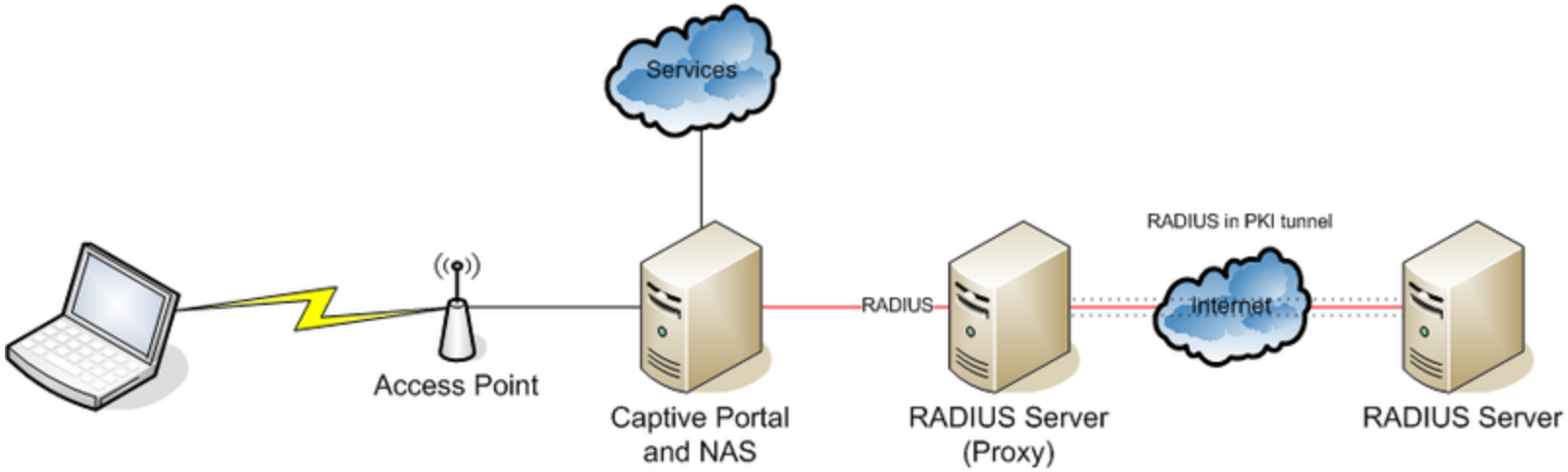

RADIUS Client
RADIUS Server
RADIUS: Accounting-Request
[acct_status_type=start]
RADIUS:Accounting-Response
RADIUS: Accounting-Request
[acct_status_type=interim update]
RADIUS:Accounting-Response
RADIUS: Accounting-Request
[acct_status_type=stop]
RADIUS:Accounting-Response

Radius - Accounting

- Auszug für Benutzer carsten für VPN am FB

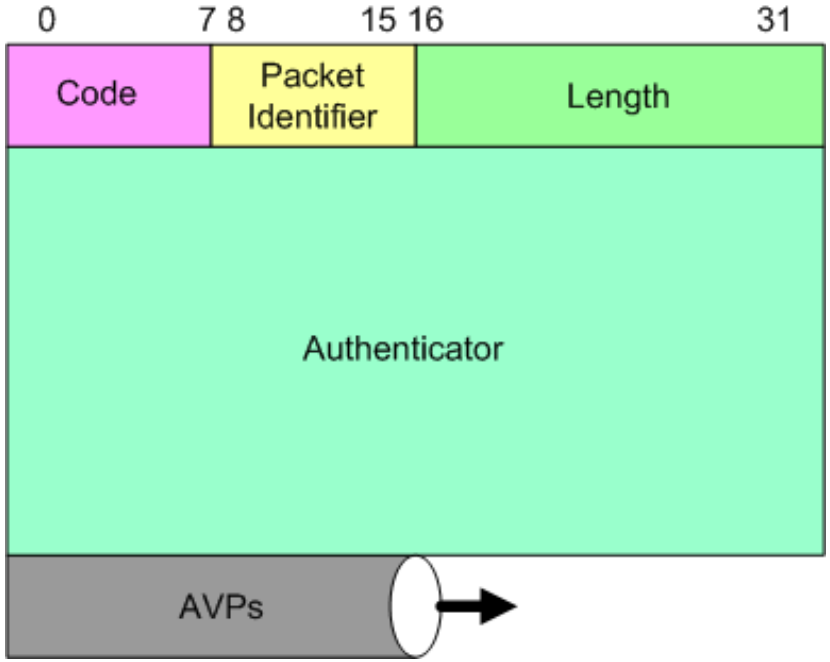
```
Accounting-ID: 164293;
Session-ID: "497CD8B24F1700";
Username: "carsten";
NAS IP Address: "160.45.113.246";
NAS Port ID: 10;
Start: "2009-01-25 22:25:06+01";
Stop: "2009-01-25 22:41:41+01";
Session Time(s): 995;
Bytes IN: 1162177;
Byte OUT: 3009158;
Framed protocol: "PPP";
Framed IP Address: "130.133.48.2”
```

Radius - Roaming



Radius - Paket

- http://en.wikipedia.org/wiki/RADIUS



Radius - Beispiele

Fachbereich Mathematik und Informatik

Aufbau über Metadatenbanken, Radius und Webserver

- VPN-System
- Netzwerkauthentisierung für Switches

Systemkomponenten

- MIID
- Radius-DBs
- Radius-Server
- Portal
- Synchronisationsprogramme
- Monitoring
- Messaging
- Uvm.

Identitätsverwaltung

Identity Management beschäftigt sich mit der Zuordnung von personenbezogenen Daten in Rechneranlagen.

Hierbei werden Anforderungen von Computersystemen, Applikationen, betrieblichen Interessen und Datenschutz verwaltet, korreliert, synchronisiert usw.

Identitätsverwaltung

Kontext

- Im Internet zwischen verschiedenen unabhängigen Dienstanbietern
- In abgeschlossenen Umgebungen wie Banken, Universität, Telekommunikationsanbietern uvm.
- Wird benötigt, um in einer Organisation unterschiedliche Anlagen, Betriebsanforderungen und Betriebsanläufe zu organisieren

Identitätsverwaltung

- Geltungsbereich (innerhalb von Organisationen oder organisationsübergreifend/föderal)
- Lebenszyklus
- Verwaltung und Schutz der Informationen (Attribute) Rollenmanagement über Identitäten
- Verknüpfung der Rollen mit Pflichten, Verantwortungen, Privilegien und Rechten für den Zugriff auf Ressourcen
- Systeme, in denen die Daten gespeichert werden (Verzeichnisse, Datenbanken, etc.)
- Zugansmedien, welche die Daten enthalten (Token, Karten)

Identitätsverwaltung

Wir benötigt um …

- Personenbezogene kontinuierlich und konsistent zu verwalten, bereit zu halten und zu verändern.
- Rechtliche Anforderungen umzusetzen

Anfänglich wurden LDAP-Systeme zur Lösung der multiplen Zugangskorrelationen genutzt.

Später wurden verteilte Datenbanken verwendet.

Identitätsverwaltung

Typen von Identitätsmanagement und – speichern

- Förderales IM
- Dezentrales IM
- Zentrales IM

Abgrenzung zwischen Anlagen- und personenbezogenen Daten

- Welches Datum ist personenbezogen, welches ist ein klares Anlagenmerkmal

Identitätsverwaltung

Implementierungsformen
- LDAP
- Datenbanken
- Metadatenbanken

Mehrwertdienste
- Single Sign On
- Statistik
- Zugangsportale
- Metadaten zur Synchronisation in neue, bislang nicht integrierte Systeme

Identitätsverwaltung

Zentrales Paradigma

- Wer benötigt
- Was
- Wozu
- Wann
- Wie lange?

IT-Systeme müssen mit dem Minimum an Daten auskommen, um zielgerichtet mit Daten zu arbeiten.

Daten wecken Begehrlichkeiten und führen zur zweckentfremdeten Nutzung.

IM in der FU-Berlin

- FUDIS an der ZEDAT als Zentrale Datendrehscheibe – verteiltes und gleichzeitig förderales IM
- Studierendenverwaltung
- Personaldatenbank (SAP)
- Lokale Datenbanken (MIID)
- Dienstedatenbanken (BIOS)

IM in der FU-Berlin

- Zugangsportale
  - Verwaltung von Diensten
- Identity Provider
  - Radius
  - LDAP

IM in …


YOU KNOW, OUR COMPANY COLLECTS DATA ON EVERYONE!
SO, WE KNOW YOUR CREDIT HISTORY...
AND WE KNOW YOUR MEDICAL HISTORY...
AND WE KNOW ALL YOUR IMPORTANT ID NUMBERS...
IN FACT, WE KNOW EVERYTHING ABOUT YOU!
DO YOU KNOW I STOLE MY IDENTITY FROM YOUR COMPANY AND I'M NOT WHO I SAY I AM?

IM in Zahlen

- IM synchronisieren heutzutage über 30 Zielsysteme
- Systeme mit mehr als 30 Mio. Identitäten – US Steuerbehörde ca. 200 Mio. Datensätze
- Datensätze von mehren KB/Identität führen zu Datenbanken von Terrabytegrößen, sowohl verteilt, als auch zentral!

Kerberos (nur V5)

- Ein Autentisierungsprotokoll
- Erlaubt die Identitätsbestätigung über unsichere Netzwerke zweiter Kommunikationspartner
- Free Software vom MIT
- Gegenseitige Autentisierung (mutual auth.)
- Client-Server

Kerberos

Geschützt …

- gegen Abhören (eavesdropping)
- Replay Angriffe

Kerberos

Begriffe

- Key Distribution Center: Kennt Benutzernamen und Passworte
- Admin Server: erlaubt als einzger Server Änderungen
- Service Principal Name: der Username …
- Ticket: Ergebnis einer positiven Authentisierung
- Service: Eine Software, die eine eigene Identität benötigt
- Ticket Forwarding: Transitive Nutzung von Tickets, z.B. für SSH-Hopping
- Key-Tab: privater Schlüssel eines Dienstes/Hosts

Kerberos

Begriffe

- Realm: Administrativer Bereich, Gruppierung für alle Principals. Realm wird immer GROß geschrieben.
- Principal: jedes in Kerberos agierende Objekt hat einen Principal. Ein Principal ist ein eindeutiger Name in einem Realm und von der Struktur her hierarchisch aufgebaut.
  - Benutzer schauble - schauble@FU-BERLIN.DE
  - Host Moskau - host/moskau@imp.fu-berlin.de@UX.IMP.FU-BERLIN.DE
  - Es gibt Service- oder Host-Principals
  - Format:
    username/instance@REALM
    service/fully-qualified-domain-name@REALM

Kerberos

- Kerberos erledigt ausschließlich das erste A von AAA
  - Authentication !!!

Kerberos

Vorteile gegenüber anderen Logins …

- Tickets erlauben single-sign on gegen ebenfalls „kerberisierte“ Dienste – Ticketlebenszeit 8-24h
- Kommunikation nach erster Authentisierung erfolgt ohne weitere Passwörter
- Passwort wird niemals im Klartext übermittelt, sondern immer durch die Key-Tab verschlüsselt und am KDC verifiziert.

Kerberos

KDC …

- Datenbank für SPNs
- Authentication Server
- Ticket Granting Server
- KDCs müssen sich über herstellerspezifische Methoden synchronisieren – kein Standard

Kerberos

Authentication Server

- AS vergibt verschlüsselte Ticket Granting Tickets (TGT) an Klienten, die sich in der REALM einloggen möchten.
- Login erfolgt nicht gegen KDC. KDC verschlüsselt TGT mit Benutzernamenpasswort.
- TGT wird genutzt, um individuelle Service-Tickets zu erzeugen => für jede Kommunikation wird ein eigenes Ticket erzeugt.

Kerberos

Ticket Granting Server (TGS)

- Vergibt individuelle Tickets an clients
- Service Ticket wird erzeugt mit
  - TGT
  - Serviceanforderung

Kerberos

Tickets

- Verschlüsselte Datenstruktur vom KDC mit shared encryption key, der pro Session einzigartig ist.
- Erzeugt Authentisierung und gemeinsames Verschlüsselungstoken für Session.
- Tickets haben Gültigkeit (typ. 8-24h)
- Felder:
  - Benutzer Principal UPN
  - Service SPN
  - Gültigkeitsbereich (Start, Stop)
  - Nutungsbereich (IPs von denen Ticket genutzt werden darf)
  - Session Key

Kerberos

Nachteile

- Lokale Uhren müssen bis auf wenige Sekunden genau synchron sein.
- Es kann nur einen Admin-Server geben
- Single Point auf Failure: Es müssen mehrere KDC installiert werden, um Redundanzen zu erzeugen.
- Admin-Protokoll ist nicht standartisiert

Kerberos

Ticketoptionen und -erweiterungen

- Forwardable Ticket: Tickets können durchgereicht werden und damit von einem Dienst weiterverwendet werden
  - z.B. bei SSH: Das TGT wird genutzt um ein weiteres TGT beim Login zu erzeugen, um lokale Dienste zu nutzen wie die Shell
- Renewable Tickets: können in der Lebenszeit erneuert werden.
- Postdated Tickets: werden erst in der Zukunft gültig – selten genutzt.