# eDirectory

- Allgemeines
- Aufbau
- Objekttypen und deren Eigenschaften
- Kontext
- Partitionen und Replikationen
- Zeitsynchronisation
- Namensgebung

# eDirectory – Allgemeines

- NDS als Netware Directory Services im Jahr 1994 mit Netware 4 als Nachfolger des Bindery-Systems eingeführt.
- Später auf Novell Directory Services umbenannt, da auch auf WindowsNT/2000 und Unix-System lauffähig
- Heute oft als e-Directory bezeichnet

# Aufbau

- Baumartig mit drei Klassen von Objekten
  - Rootobject (Wurzel des Baumes; bezeichnet mit dem Pseudonamen [Root])
  - Containerobjects (C, O und OU)
  - Leafobjects (Blattobjekte, CN)

# Rootobject

- Einmalig in einem Tree
- Der Name des Trees ist mit diesem Objekt verbunden
- Alle Eigenschaften für den gesamten Tree sind mit diesem Objekt verbunden (z.B.: B-Recht für [Public])

# Containerobjects

- Nur Containerobjekte können weitere Objekte beinhalten
- Containerobjekte haben auch Eigenschaften für alle Objekte darin
- C Countryobject
- O Organisation Object
- OU Organizational Unit Object

# Countryobject

- Countryobjects können nur in [Root] existieren
- Namen müssen die international üblichen Namen (ISO 3166-1) der Länder entsprechen
- Countryobjects können nur Objekte des Types O beinhalten.

# Organisationobject

- Organisationobjects können in [Root] oder in Objekten des Typs C existieren
- Organisationobjects können OU- oder Leafobjects beinhalten
- Die Namen entsprechen üblicherweise den Firmennamen

# Organizational Unit Object

- Diese Objekte können in Objekten der Typen O oder OU existieren.
- In diesen Objekten können weitere OU oder Leafobjekte untergebracht sein.
- Die Namen können frei gewählt werden, sollten aber „sprechend“ sein.

# Leafobjects

- Blatt- oder Endobjekte stellen die eigentlichen Elemente des Netzwerkes dar.
- Je nach Art des Objektes sind hier verschiedene Eigenschaften möglich (z.B.: Drucker hat einen Standort, Benutzer?)

# Leafobjekttypen

- Einige Standardtypen:
  - AFP-Server
  - Alias
  - User (Benutzer)
  - Workstation (Computer)
  - Volume (Datenträger)
  - Group (Gruppe)
  - Server
  - Profile (Profil)

# Leafobjekttypen 2

- Einige Standardtypen:
  - Directory (Verzeichniszuordnung)
  - Role (Organisatorische Funktion)
  - License (Lizenz)
  - Application (Anwendungsprogramm)
  - Printer (Drucker)
  - Printserver (Druckserver)
  - Queue (Warteschlange)
  - NDPS-Broker (NDPS-Vermittler)

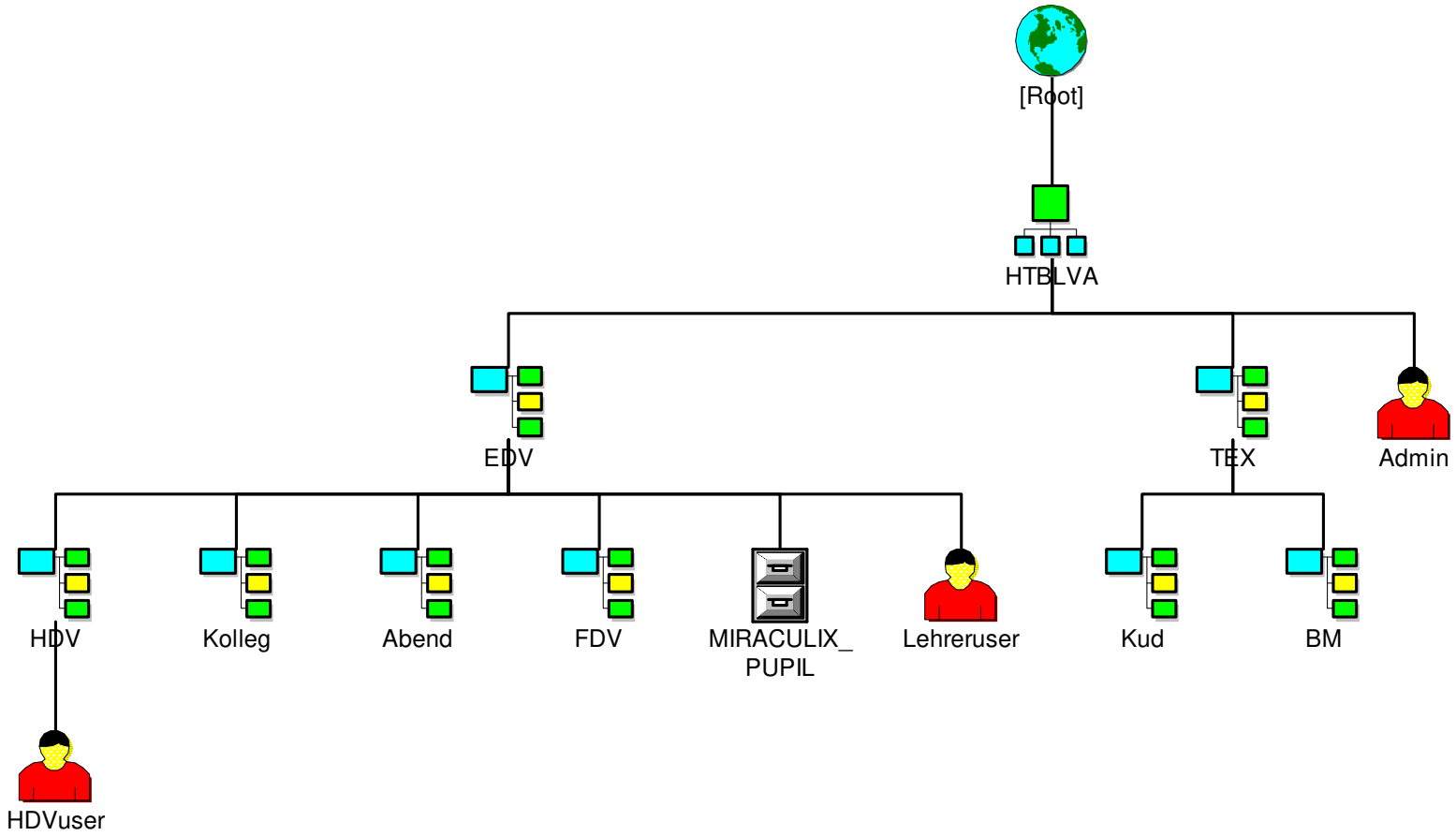
# Leafobjekttypen 3

- Neben den Standardtypen sind noch beliebige Erweiterungen möglich:
  - fw1 User
  - Bagger
  - Kran
  - Flugzeug
  - ...

# Kontext

- Um ein Objekt korrekt zu beschreiben muß der DN verwendet werden.
- Der Kontext ist jener Teil des DN, der zum CN hinzugefügt werden muß.
- Ein „Default Context“ (Standard Kontext) spart die Angabe des Kontexts für Objekte in diesem Kontext.

# Beispiel


[Root]
HTBLVA
EDV
TEX
Admin
HDV
Kolleg
Abend
FDV
MIRACULIX_
PUPIL
Lehreruser
Kud
BM
HDVuser

# Beispiel (1)

- Kein Countryobject
- Ein Organisationobject names HTBLVA
- Viele OU-Objects
- Viele Leafobjects von denen nur drei Benutzer und ein Volume eingezeichnet ist.

# Beispiel (2)

- Der Name des Benutzers Admin:
  - <treename>/cn=admin.o=htblva oder kurz
  - <treename>/admin.htblva
- Der RDN des Benutzers Admin
  - im Kontext HTBLVA: cn=admin
  - im Kontext [Root]: cn=admin.ou=htblva
  - im Kontext Kolleg.EDV.HTBLVA: admin..

# Beispiel (3)

- DN des Objektes MIRACULIX_PUPIL:
  - MIRACULIX_PUPIL.EDV.HTBLVA
- RDN des Objektes:
  - Kontext EDV.HTBLVA: MIRACULIX_PUPIL
  - Kontext HDV.EDV.HTBLVA: MIRACULIX_PUPIL.
  - Kontext HTBLVA: MIRACULIX_PUPIL.EDV

# Eigenschaften

- Jedes Objekt im eDirectory hat Eigenschaften (Properties)
- Containereigenschaften beziehen sich oft auf alle Objekte im Container
- Mögliche Eigenschaften im Schema beschrieben
- Eigenschaften können optional oder mandatory sein

# Eigenschaften von Organisations

- Name
- Login Script
- Rechte

# Eigenschaften von Volumes

- Name
- Host Server
- Host Volume
- Version

# Eigenschaften von Benutzern

- First Name, Last Name, Full Name
- UserID (Login Name)
- Key Material
- e-Mail-Address
- Title, Telephone Number, Address
- Home Directory Volume, Home Directory Path

# Eigenschaften von Benutzern 2

- Account Ablaufdatum
- Password Parameter
- Gruppenmitgliedschaften
- Beschränkung gleichzeitiger Verbindungen
- Last Login
- …

# Eigenschaften von Gruppen

- Name
- Description
- Members
- Rights to Files and Directories
- …

# Partitionen

- Ein NDS-Baum kann in mehrere Partitionen aufgeteilt werden
- Ein Aufteilung hat nur dann Sinn, wenn mehrere Server vorhanden sind
- Von jeder Partition existieren standard-mäßig 2 Kopien (Replikationen)

# Replikationen

- Replikationen sind Kopien aller Daten einer Partition
- Automatische Erstellung
- Manuelle Erstellung

# Replikationstypen

- Masterreplikation (Masterreplica)
- [Gefilterte] Schreiben/Lese-Replikation ([Filtered] Read-Write-Replica)
- [Gefilterte] Nur-Lese-Replikation ([Filtered] Readonly-Replica)
- Linkreplikationen (Subordinate Reference Replica)

# Zeitsynchronisation

- Damit mehrere Server korrekt mit e-Directory arbeiten können muß(!) eine einheitliche Zeit im System herrschen
- Alle Server haben daher intern UTC (gleich GMT = MEZ-1Stunde/2Stunden)
- Zusätzlich wird die lokale Zeit für die Anzeige verwendet (aus UTC gebildet).

# Zeitservertypen

- SINGLE REFERENCE
- REFERENCE
- PRIMARY
- SECONDARY

# SINGLE REFERENCE

- Die Uhrzeit dieses Server wird als Referenz für das Netzwerk verwendet.
- Daneben nur SECONDARY Timeserver sinnvoll.
- Die Uhrzeit wird auch Clients bzw. auf Wunsch auch per NTP zur Verfügung gestellt.

# REFERENCE

- Referenzzeitserver, der allerdings mit anderen Zeitservern die Netzwerkzeit abstimmt (seine eigene Zeit aber nicht daran anpaßt).
- Daneben sind SECONDARY und PRIMARY Timeserver möglich.
- Die Uhrzeit wird auch Clients bzw. auf Wunsch auch per NTP zur Verfügung gestellt.

# PRIMARY

- Zeitserver, der mit anderen Zeitservern (PRIMARY oder REFERENCE) die Netzwerkzeit abstimmt.
- Daneben sind SECONDARY, PRIMARY und REFERENCE Timeserver möglich.
- Die Uhrzeit wird auch Clients bzw. auf Wunsch auch per NTP zur Verfügung gestellt.

# SECONDARY

- Zeitserver, der selbst seine Uhrzeit von anderen Zeitservern (PRIMARY, SINGLE REFERENCE oder REFERENCE) bekommt.
- Die Uhrzeit wird auch Clients bzw. auf Wunsch auch per NTP zur Verfügung gestellt.

# Namensgebung

- In eDirectory-Namen sollten folgende Zeichen nicht verwendet werden

  . [,] + =

- Möglich sind aber auch diese mit dem \ (=Fluchtsymbol) davor
- 47 Zeichen maximale Länge für Namen, die SAP (Service Advertising) benötigen
- Richtlinien für Namensgebung sinnvoll

# Richtlinien Namensgebung

- Damit später der Baum durchsucht werden kann.
- Genaue Beschreibung der Namensbildung
- Genaue Beschreibung der Schreibweise und der Trennzeichen
- Strikte Einhaltung (!)

# Beispiele Namensgebung

- Login Name
  - Erster Buchstabe Vorname
  - Familienname (hhabicht)
- Telefonnummer
  - Internationale Schreibweise (+49 89 5475)
- Full Name
  - Vorname Zuname (Hugo Habicht)