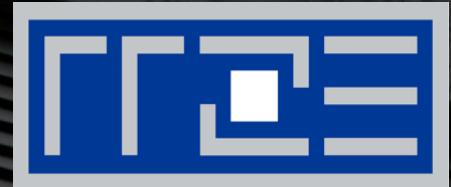


# REGIONALES RECHENZENTRUM ERLANGEN [RRZE]



## MS Active Directory

Systemausbildung – Grundlagen und Aspekte von  
Betriebssystemen und System-nahen Diensten, 01.06.2016  
Sebastian Schmitt, RRZE

# Agenda

- Einführung
- Hauptkomponenten
- Aufbau
- Replikation
- Gruppenrichtlinien
- Blick in die FAUAD

# Einführung

Windows NT – Primary Domain Controller (PDC)

Windows 2000 erscheint

- Microsoft führt das Active Directory ein
- Verzeichnisdienst ↔ Infrastruktur-Dienst
  - Ersetzt lokale SAM (Security Account Manager)  
[Benutzernamen, Gruppen, Passwörter]
  - Zentraler Verzeichnisdienst für alle Objekte  
[User, Drucker, Computerobjekte etc.]
  - Hierarchisch gegliedert

# Was ist ein Verzeichnisdienst

- Eigenschaften:
  - hierarchisch
  - objektorientiert
  - Zuordnung: Eigenschaften ↔ Objekten
- Datenbank (AD)
  - Jet Blue DB – hierarchisch, verteilt, skalierbar
- Anwendung:
  - Authentifizierung
  - zentrale Benutzerverwaltung



# HAUPTKOMPONENTEN ACTIVE DIRECTORY



- LDAP
- Kerberos
- CIFS
- DNS

# Was ist LDAP?

- **Lightweight Directory Access Protocol**
- Protokollstandard zur Abfrage und Modifikation von Informationen eines Verzeichnisdienstes (Directory)
- Leichtgewichtige Implementierung des DAP-Protokolls (X.500)
- Aktuelle Version LDAP v3 in RFC 2251 spezifiziert
- Oberbegriff für Implementierungen und Technologien, die eine LDAP-Schnittstelle anbieten

Quelle: Benutzerverwaltung – LDAP, Andrei Galea 20.5.2015

# LDAP für den Verzeichnisdienst

- Informationen über Benutzer und Gruppenzugehörigkeit
  - Lokale SAM-Ablöse
  - Speichert Objekte
    - › Benutzer
    - › Gruppen
    - › Drucker
    - › Computer
    - › Gruppenrichtlinien
    - › ...

# Warum LDAP?

- Hohe Interoperabilität
  - Zugriff mittels einheitlichem LDAP-Protokoll, ermöglicht (theoretische) Unabhängigkeit von zugrundeliegender Datenhaltung
  - Spezifikation von Datenstrukturen in Schemata erhöht die Nutzbarkeit der gespeicherten Daten durch verschiedenste Client-Anwendungen
    - › Authentifizierung → Samba, PAM, Radius, ...
    - › E-Mail Verzeichnis → Thunderbird, Outlook, ...
- Hierarchische Datenhaltung/-zugriff

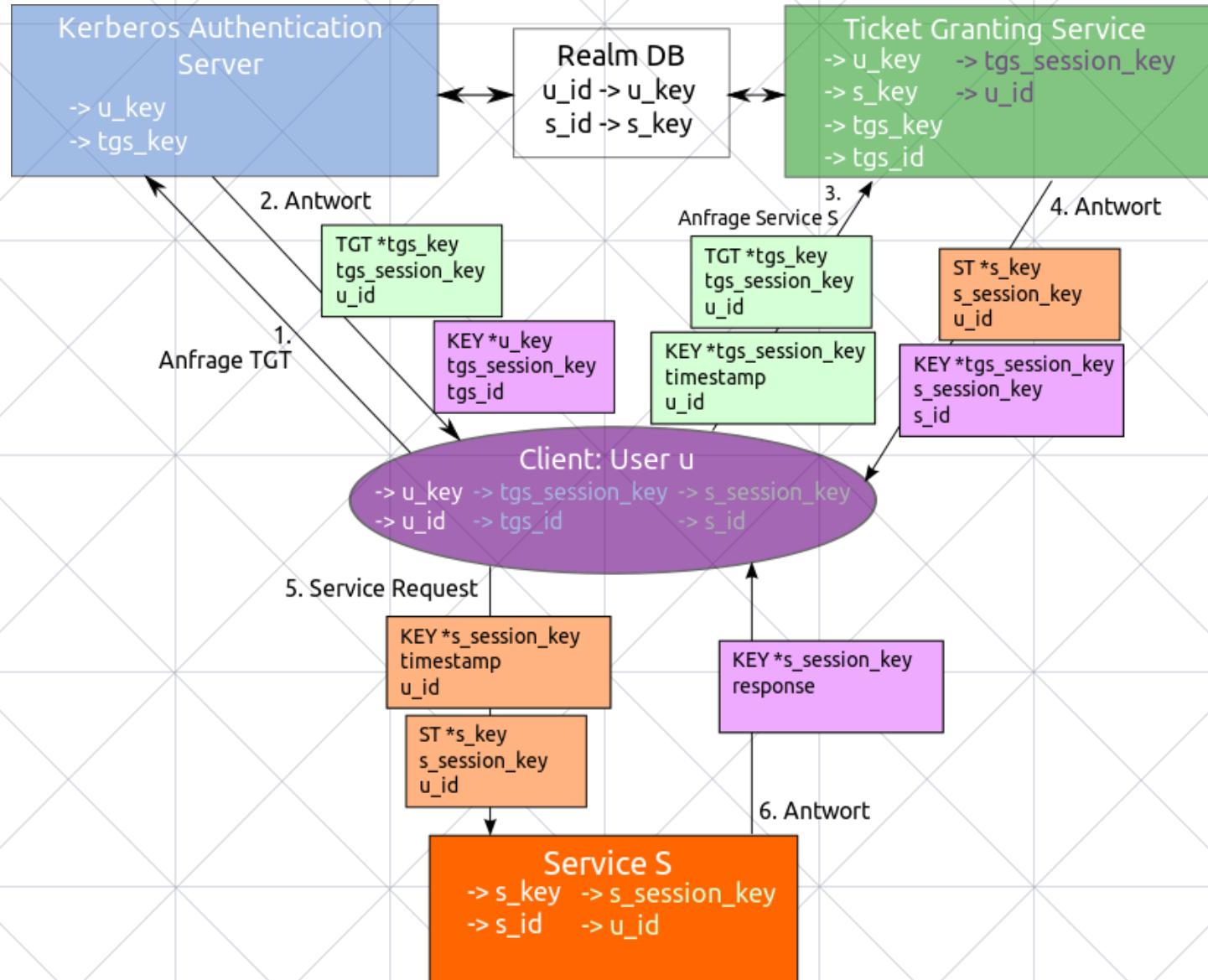
Quelle: Benutzerverwaltung – LDAP, Andrei Galea 20.5.2015

# Kerberos

- Protokoll zur Authentifizierung von Benutzern
  - Benutzer erhält nach Authentifizierung ein sog. Ticket Granting Ticket (TGT)
  - Mit gültigem TGT kann er Diensttickets erhalten
- Nur einmal Passwort eingeben (TGT erhalten) um dann Zugriff auf verschiedene Dienste (Diensttickets) zu erhalten

# Kerberos - Funktionsweise

- 3 Parteien
  - Client
  - Dienst-Server
  - Kerberos-Server, Ticket-Granting Server
- Authentifizierung Client ↔ Server
- Session Key
  - Client ↔ Kerberos-Server ↔ Server (Dienst)



Quelle: [http://de.wikipedia.org/wiki/Datei:Kerberos\\_german.svg#/media/File:Kerberos\\_german.svg](http://de.wikipedia.org/wiki/Datei:Kerberos_german.svg#/media/File:Kerberos_german.svg)

- Common Internet File System
  - erweiterte Version von Server Message Block (SMB)
  - Ablage von Dateien im Netzwerk
  - Nutzt DNS (SRV-Records) zum Auffinden von Dateien
- ... Zugriff von außerhalb der FAU nur via VPN möglich...

# DNS

- Domain Name System
- Active Directory benötigt „eigenes“ DNS (vorher NetBIOS – WINS)
- DNS muss SRV-Ressourceneinträge (SRV-Records) unterstützen
- Muss nicht unbedingt ein Microsoft DNS sein

# DNS-Einträge

\_msdcs.test.fau.de. IN NS test1.uni-erlangen.de.  
IN NS test2.uni-erlangen.de.

\_sites.test.fau.de. IN NS test1.uni-erlangen.de.  
IN NS test2.uni-erlangen.de.

\_tcp.test.fau.de. IN NS test1.uni-erlangen.de.  
IN NS test2.uni-erlangen.de.

\_udp.test.fau.de. IN NS test1.uni-erlangen.de.  
IN NS test2.uni-erlangen.de.

# DNS-Einträge

DomainDNSZones.test.fau.de.

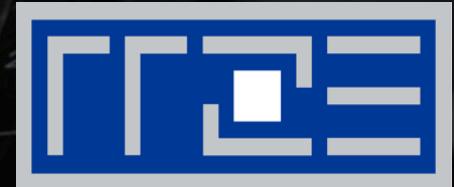
IN NS test1.uni-erlangen.de.  
IN NS test2.uni-erlangen.de.

ForestDNSZones.test.fau.de.

IN NS test1.uni-erlangen.de.  
IN NS test2.uni-erlangen.de.



# AUFBAU ACTIVE DIRECTORY



- Bestandteile
- Datenbank
- Objekte
- Hierarchie

# Aufbau – Bestandteile

- Schema definiert
  - Objekttypen
  - Klassen
  - Attribute
- Konfiguration
  - Struktur „AD-Wald“ und seine „Bäume“
- Domain
  - Informationen, die sie selbst und die in ihr erstellten Objekte beschreiben

# Aufbau – Datenbank

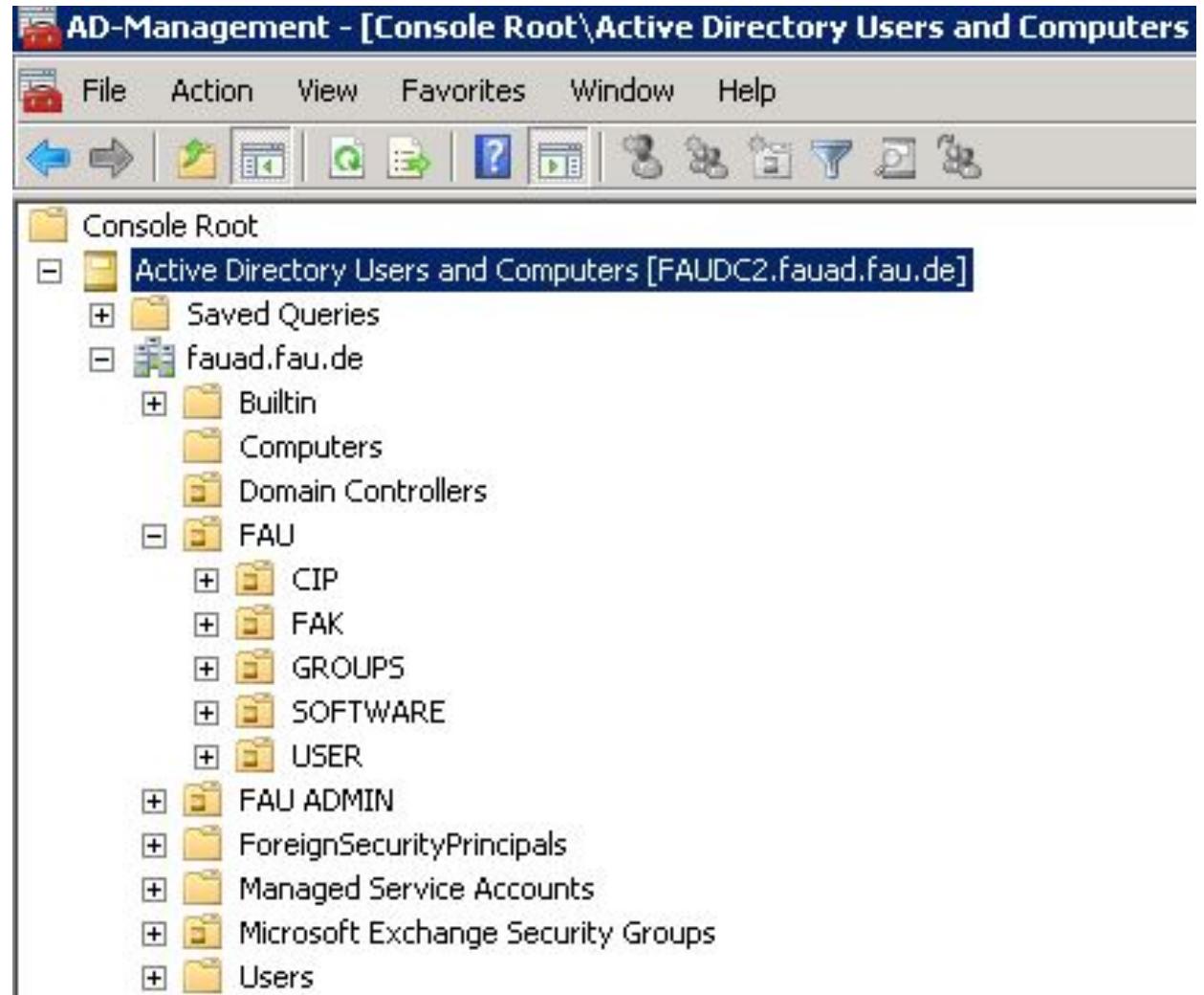
- Jet-DB
  - Relational
  - Transaktionsorientiert
  - Begrenzt auf 16 TB (2 Milliarden Objekte pro DC)
- 3 Haupttabellen
  - schema table (Schema)
  - link table (Objekt-Struktur)
  - data table (Daten)

# Aufbau – Objekte

- Konten
  - Benutzer
  - Gruppen
  - Computer
- Ressourcen
  - Gruppenrichtlinien
  - Dateifreigaben
  - Druckerfreigaben

# Aufbau – Objekte

- Hierarchische Gliederung in Organisationseinheiten (OU = Organisational Unit)
- Eigenschaften von OUs können vererbt werden
- Vgl. Aufbau LDAP-Baum



# Aufbau – Hierarchie

- Wald (forest) – Gesamtstruktur
  - Ansammlung aller Objekte, deren Attribute, Regeln und Container in dem Verzeichnis abgelegt werden
  - Verwaltet einen oder mehrere „Bäume“
- Baum (tree)
  - Verwaltet einen oder mehrere Domains
- Domain
  - Beinhaltet Konten und Ressourcen

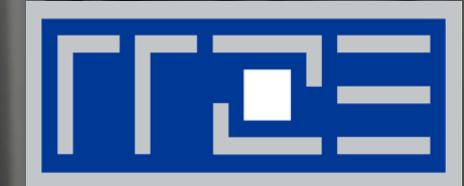
# Aufbau – Hierarchie

- Organisationseinheiten (OU = Organisational Unit)
- Standorte
  - Räumliche Gliederung
  - IP-Subnetze
    - › LAN
    - › WAN
  - Kontrolle des Netzwerkverkehrs

→ Planung sehr wichtig !



# REPLIKATION ACTIVE DIRECTORY



- Multi-Master-Replikation
- FSMO-Rollen

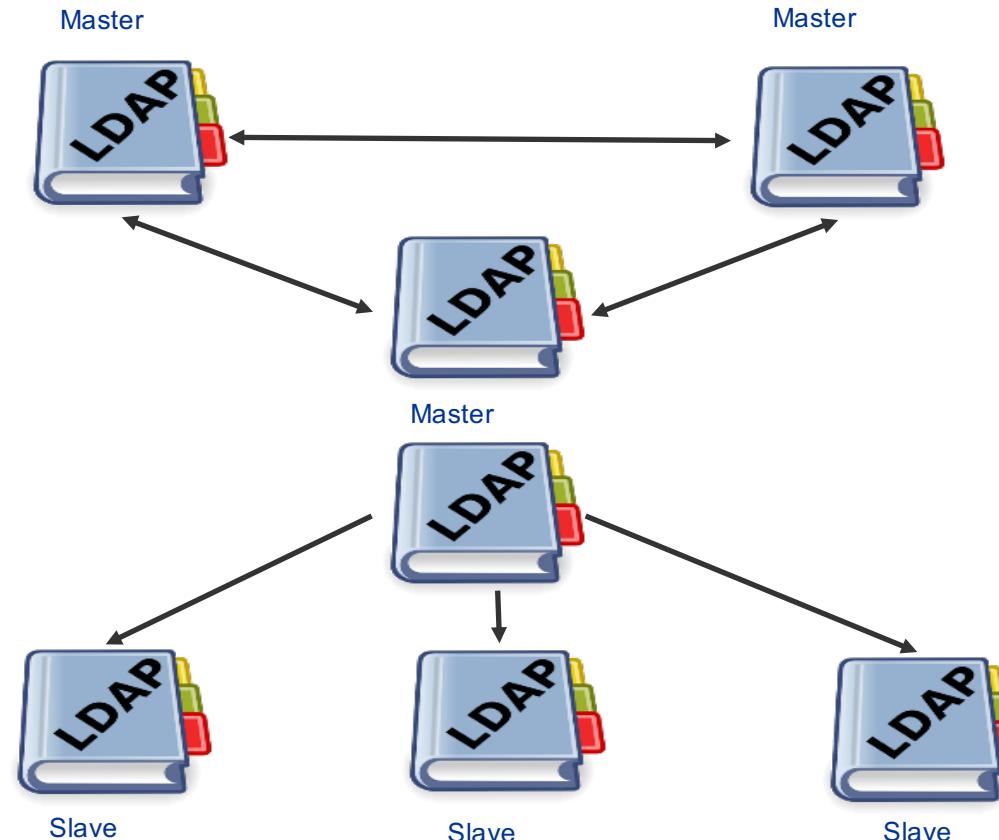
# Replikation

- Vorteile: Lastenverteilung und Ausfallsicherheit

- Typen:

- Multimaster

- Master-Slave:



Quelle: Benutzerverwaltung – LDAP, Andrei Galea 20.5.2015

# Multi-Master-Replikation

- Änderungen werden an alle Domain Controller (DC) verteilt
  - Konfliktbehandlung
    - DC der als letztes Daten geschrieben hat, gewinnt
    - Im Vorfeld Prüfungen zur Konfliktvermeidung implementiert
    - Manche Anfragen nur von einem DC zu beantworten
- Flexible Single Master Operation (FSMO)

# FSMO – Schema Master

- 1x pro Wald (forrest)
- Schema Master zuständig für Schema-Updates  
LDAP://cn=schema,cn=configuration,dc=<domain>
- Schema-Updates werden vom Schema Master an alle DCs repliziert

# FSMO – Domain Naming Master

- 1x pro Wald (forrest)
- Domain Naming Master zuständig für Domain Namenskontext  
LDAP://cn=Partitions,cn=configuration,dc=<domain>
- Domain Naming Master einziger DC, über den Domains hinzugefügt oder entfernt werden können.

# FSMO – RID Master

- 1x pro Domain
- Verwalter von IDs innerhalb einer Domain
- Jedes Objekt erhält eine eindeutige ID  
unique Security ID (SID):  
$$\text{SID} = \text{Domain SID} + \text{relative Objekt ID (RID)}$$
- Zuständig wenn Objekte über Domaingrenzen hinweg verschoben werden

# FSMO – PDC Emulator

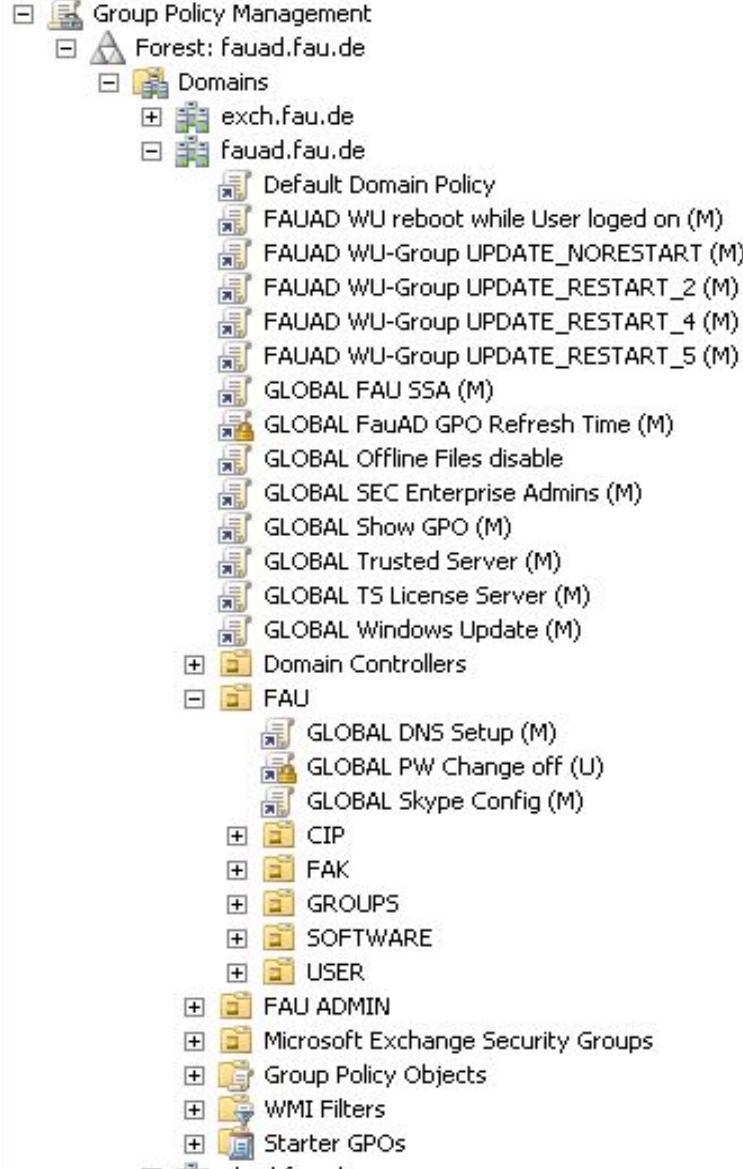
- 1x pro Domain
- „Hüter der Zeit“ – wichtig für Kerberos
- Zuständig für Passwörter
  - Änderungen
  - Logging
  - Account-Lock
- Abwärtskompatibilität zu Windows NT 4.0

# FSMO – Infrastructure Master

- 1x pro Domain
- Zuständig für Inter-Domain-Kommunikation
- **Global Catalog**
  - Such-Cache zum Auffinden aller Objekte in einer Domain oder eines Forrests
  - Wird durch Multi-Master-Replikation aktualisiert

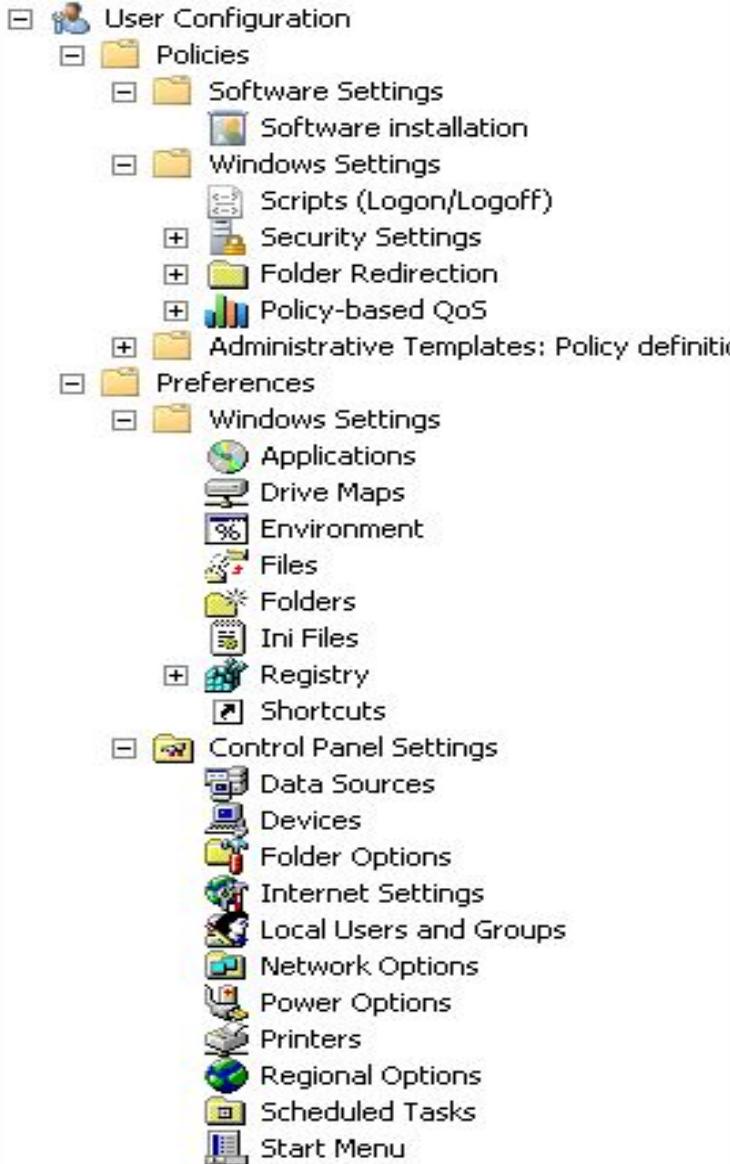
# GRUPPENRICHTLINIEN ACTIVE DIRECTORY

- Benutzer
- Maschine



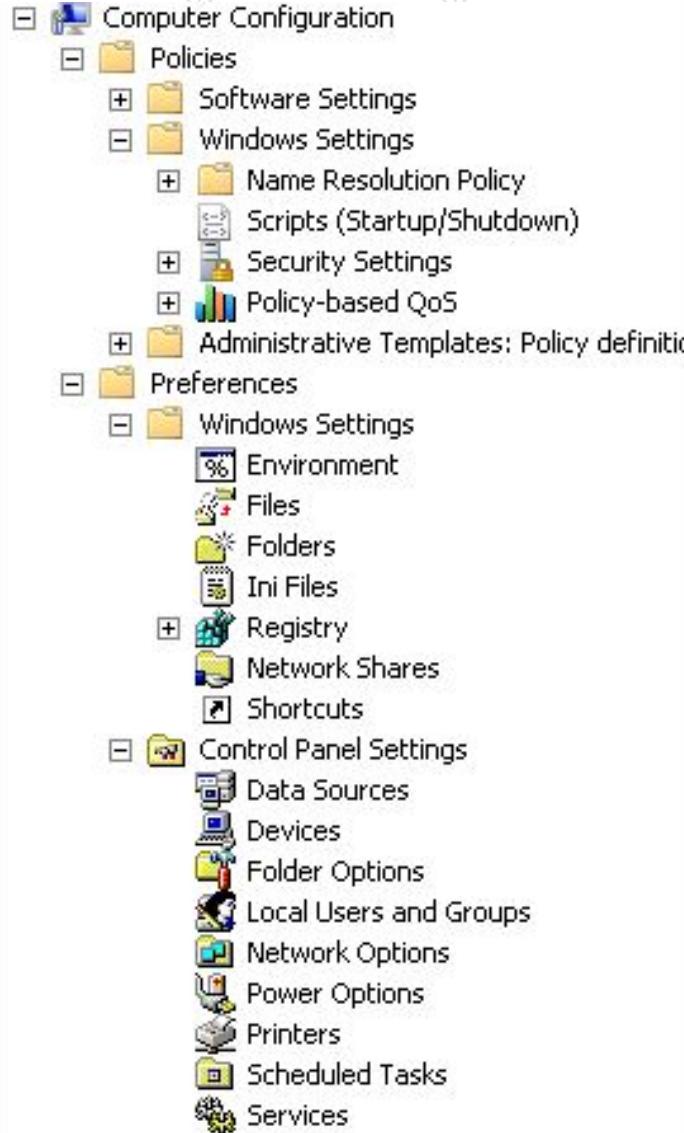
# Gruppenrichtlinien Group Policy Object (GPO)

- Zentrale Verteilung von Konfigurationen für
  - Benutzer
  - Computer
- Wirken hierarchisch  
„Je näher am Objekt, desto wirksamer“
- Erweiterbar durch ADM/ADMX-Vorlagen



# Gruppenrichtlinie Benutzer

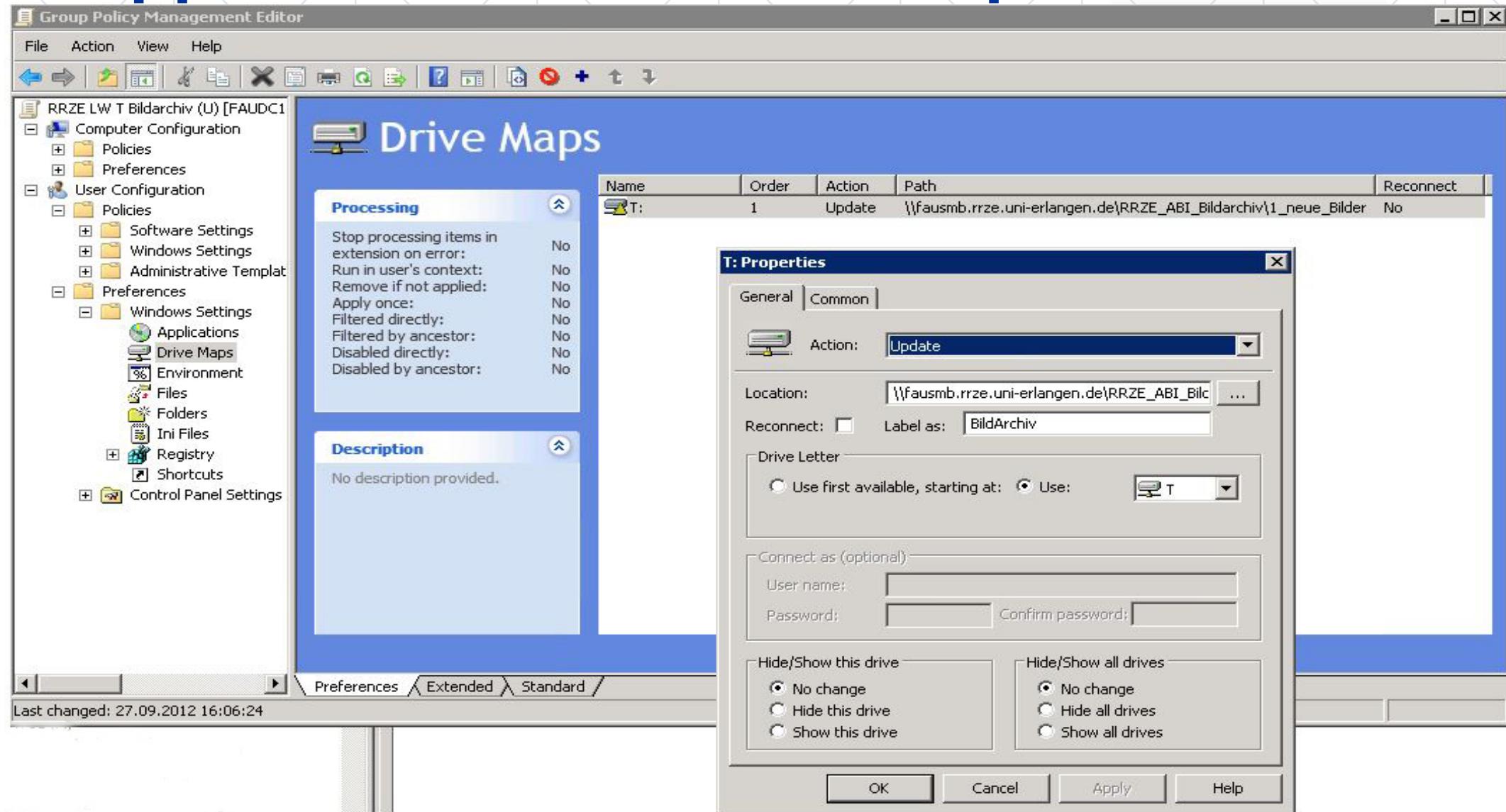
- Zentrale Benutzerkonfiguration
  - Einstellungen benutzerbezogen
    - Systemsteuerung
    - Drucker
    - Laufwerke
    - Registry-Einträge
    - Programmkonfigurationen  
(Word, Excel, Outlook etc.)
  - Skripte  
Anmeldung/Abmeldung



# Gruppenrichtlinie Computer

- Zentrale Computerkonfiguration
  - Einstellungen computerbezogen
    - › Systemsteuerung
    - › Drucker
    - › Laufwerke
    - › Registry-Einträge
    - › Programmkonfigurationen  
(Word, Excel, Outlook etc.)
  - Skripte  
starten/beenden

# Gruppenrichtlinien – ein Beispiel



# Gruppenrichtlinien – hinter den Kulissen

- XML-Dateien, die repliziert werden

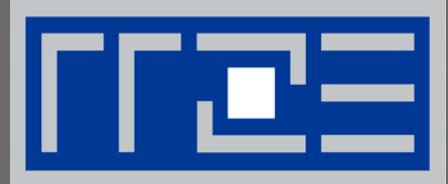
Name	Date modified
Group Policy	26.05.2015 15:12
Machine	26.05.2015 15:12
User	26.05.2015 15:12
GPT	26.05.2015 15:12

Name	Date modified
Applications	26.05.2015 15:12
Documents & Settings	26.05.2015 15:12
Preferences	26.05.2015 15:12
Scripts	26.05.2015 15:12

```
1  <?xml version="1.0" encoding="utf-8"?>
2  <Drives clsid="{8FDDCC1A-0C3C-43cd-A6B4-71A6DF20DA8C}">
3  <Drive clsid="{935D1B74-9CB8-4e3c-9914-7DD559B7A417}"
4   name="T:" status="T:" image="2" changed="2012-09-27 14:06:24"
5   uid="{8E788164-C1B2-4762-B911-811C55129A13}">
6
7   <Properties action="U" thisDrive="NOCHANGE" allDrives="NOCHANGE"
8     userName="" path="\fausmb.rrze.uni-erlangen.de\RRZE_ABI_Bildarchiv\1_neue_Bilder"
9     label="BildArchiv" persistent="0" useLetter="1" letter="T"/>
10
11 </Drive>
12 </Drives>
```

# BLICK IN DIE FAUAD

Live-Demo

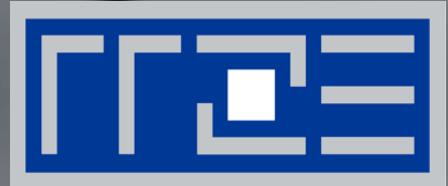


# Fehlersuche – Hilfe zur Selbsthilfe

- Active Directory nutzt viele Dienste
  - Entsprechende Ports an der Firewall, Router offen?
- Active Directory arbeitet mit Kerberos
  - Passt die Uhrzeit, Zeitzone?
- Active Directory arbeitet mit DNS
  - Stimmen die DNS-Einträge, -Server, -Auflösung?
- Was steht in den Logfiles?



# ORGANISATORISCHES



- Die Vorträge im Überblick
- Andere Vortragsreihen des RRZE
- Ablageorte Vortragsfolien
- RRZE-Veranstaltungskalender / Mailingliste abonnieren
- Themenvorschläge & Anregungen

# Weitere Vorträge zur „Systemausbildung“

20.04.2016 – Geschichte der Betriebssysteme

27.04.2016 – Unixoide Betriebssysteme (Unix, Linux, OS X)

04.05.2016 – Benutzerverwaltung: LDAP

11.05.2016 – Windows-Betriebssysteme

**01.06.2016 – Benutzerverwaltung: MS Active Directory**

08.06.2016 – Storage / Filesysteme

15.06.2016 – Virtualisierung

22.06.2016 – Backup / Archiv

29.06.2016 – Systemüberwachung, Monitoring

06.07.2016 – High Performance Computing

13.07.2016 – IT-Sicherheit

Immer mittwochs  
(ab 14 c.t.),  
Raum 2.049 im  
RRZE

# Andere Vortragsreihen des RRZE

## Campustreffen

- immer donnerstags ab 15 Uhr c.t.
- vermittelt Informationen zu den Dienstleistungen des RRZE
- befasst sich mit neuer Hard- & Software, Update-Verfahren sowie Lizenzfragen
- ermöglicht den Erfahrungsaustausch mit Spezialisten

## Netzwerkausbildung „Praxis der Datenkommunikation“

- immer mittwochs in den Wintersemestern, ab 14 Uhr c.t.
- Vorlesungsreihe, die in die Grundlagen der Netztechnik einführt
- stellt die zahlreichen aktuellen Entwicklungen auf dem Gebiet der (universitären) Kommunikationssysteme dar

# Vortragsfolien

Die Vortragsfolien werden nach der Veranstaltung auf der Webseite des RRZE abgelegt:

<http://www.rrze.fau.de/news/systemausbildung.shtml>

# RRZE-Veranstaltungskalender & Mailinglisten

- Kalender abonnieren oder bookmarken
  - Alle Infos hierzu stehen auf der Webseite des RRZE unter:  
<http://www.rrze.fau.de/news/kalender.shtml>
- Mailingliste abonnieren
  - Wöchentliche Terminhinweise werden zusätzlich an die Mailingliste [RRZE-Aktuelles](#) gesendet.
  - Auch diese Liste kann man abonnieren:  
<https://lists.fau.de/mailman/listinfo/rrze-aktuelles>

# Themenvorschläge & Anregungen

Themenvorschläge und Anregungen nehmen wir gerne entgegen!

Bitte schreiben Sie uns einfach eine E-Mail an:

[rrze-zentrale@fau.de](mailto:rrze-zentrale@fau.de) (Betreff: Systemausbildung)

# REGIONALES RECHENZENTRUM ERLANGEN [RRZE]



## Vielen Dank für Ihre Aufmerksamkeit!

Regionales RechenZentrum Erlangen [RRZE]

Martensstraße 1, 91058 Erlangen

<http://www.rrze.fau.de>