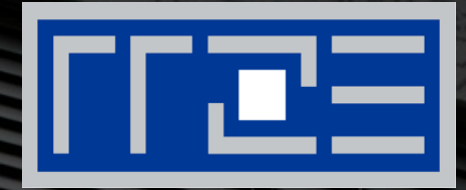


# REGIONALES RECHENZENTRUM ERLANGEN [RRZE]



## MS Active Directory

Systemausbildung – Benutzerverwaltung FAUAD,  
07.07.2021 Sebastian Schmitt, RRZE

# Agenda

- Einführung → Zukunft?
- Hauptkomponenten
- Aufbau
- Replikation
- Gruppenrichtlinien
- Sicherheit / Security
- 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

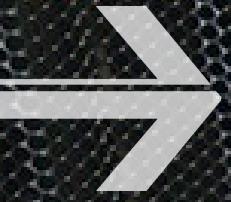
# Zukunft?

## Microsoft goes cloud

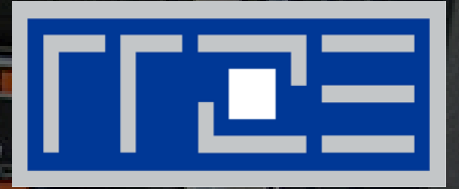
- Azure Active Directory
  - Flache Struktur
  - Keine OU-Struktur
  - Nur Gruppen
- Windows Installation via Autopilot
- Microsoft InTunes

# Was ist ein Verzeichnisdienst

- Eigenschaften:
  - Zuordnung: Eigenschaften  $\Leftrightarrow$  Objekten
  - objektorientiert
  - hierarchisch
- Datenbank (AD)
  - Jet Blue DB – hierarchisch, relational, verteilt, skalierbar
- Anwendung:
  - Authentifizierung
  - zentrale Benutzer- und Ressourcenverwaltung



# HAUPTKOMPONENTEN ACTIVE DIRECTORY



- LDAP
- Kerberos
- CIFS
- DNS





# Was ist LDAP?

- **L**ightweight **D**irectory **A**ccess **P**rotocol
- Protokollstandard zur Abfrage und Modifikation von Informationen eines Verzeichnisdienstes (Directory)
- leichtgewichtige Implementierung des DAP-Protokolls (X.500)
- Aktuelle Version LDAP v3 in RFC 4511 (2006) 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 Protokoll (LDAP), 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

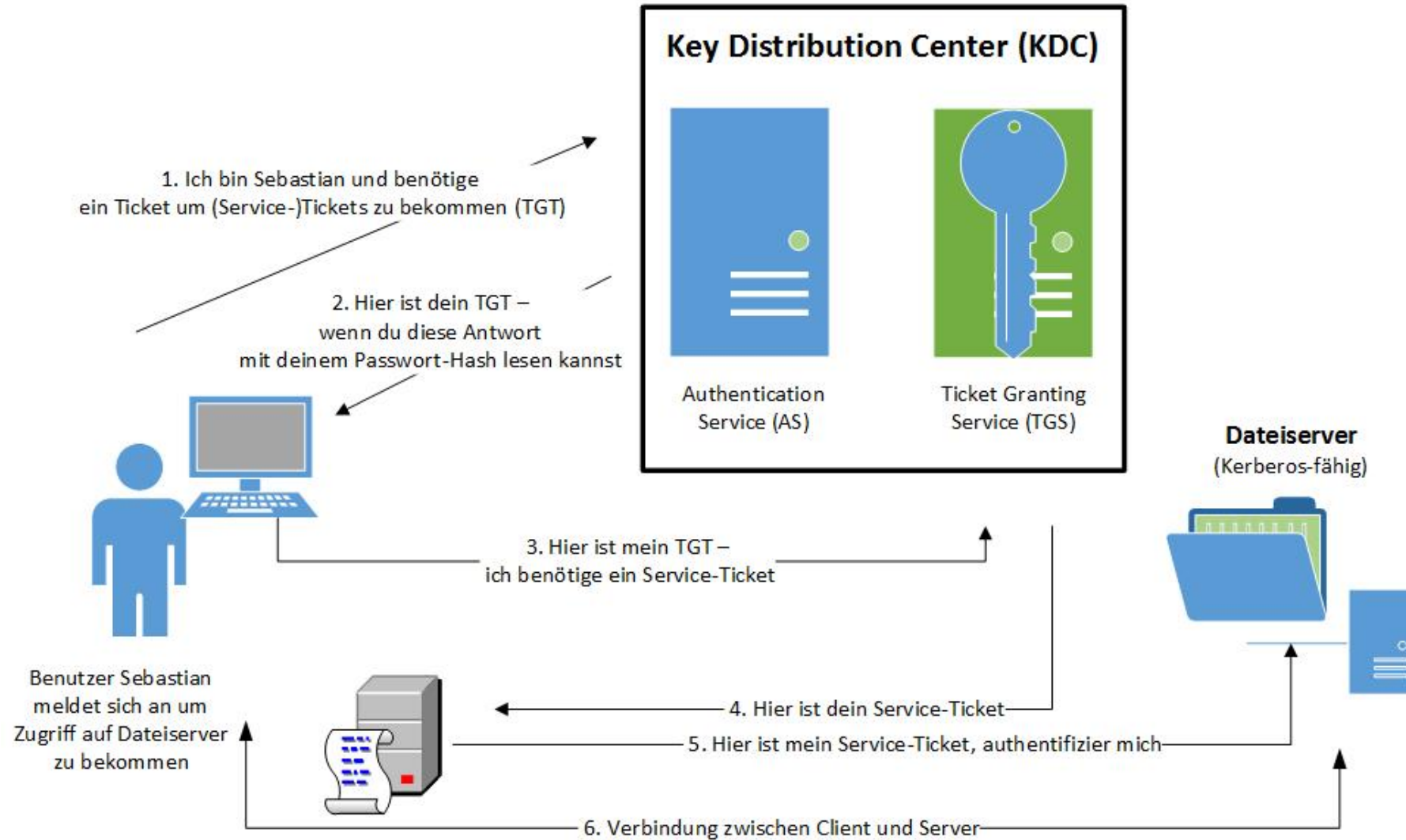
Quelle: Benutzerverwaltung – LDAP, Andrei Galea 20.5.2015

# Kerberos

- Protokoll zur Authentifizierung von Benutzern (RFC 4120)
- Benutzer erhält nach Authentifizierung ein sog. Ticket Granting Ticket (TGT) = „Digitale Eintrittskarte“
- Mit gültigem TGT kann er Diensttickets = „Eintrittskarten für bestimmte Dienste“ erhalten

→ Nur einmal Passwort eingeben (TGT erhalten) um dann Zugriff auf verschiedene Dienste (Diensttickets) zu erhalten

# Kerberos Ticket-Austausch



# Kerberos - Funktionsweise

- 3 Parteien
  - Client
  - Dienst-Server
  - Kerberos-Server, **KeyDistributionCenter**  
(Authentication Service und Ticket Granting-Service)
- Authentifizierung Client ↔ Server
- Session Key  
Client ↔ Kerberos-Server ↔ Server (Dienst)

# CIFS

- **Common Internet File System-Protokoll**
- erweiterte Version von Server Message Block (SMB)
- Dateizugriff über Netzwerkverbindungen/-freigaben
- Replikation über DFS-R zwischen Domain Controllern
- Nutzt DNS (SRV-Records) zum Auffinden von Dateifreigaben

... 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
- SRV-Records werden auf DCs unter `C:\Windows\system32\config\netlogon.dns` protokolliert
- Muss kein 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.



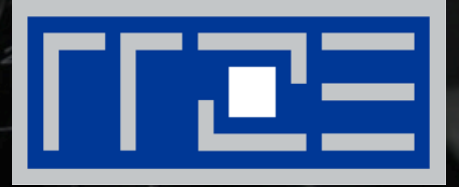
# DNS-Einträge

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“ (Forest) und seine „Bäume“ (Tree)
- Domain
  - Informationen, die sie selbst und die in ihr erstellten Objekte beschreiben

# Aufbau – Datenbank

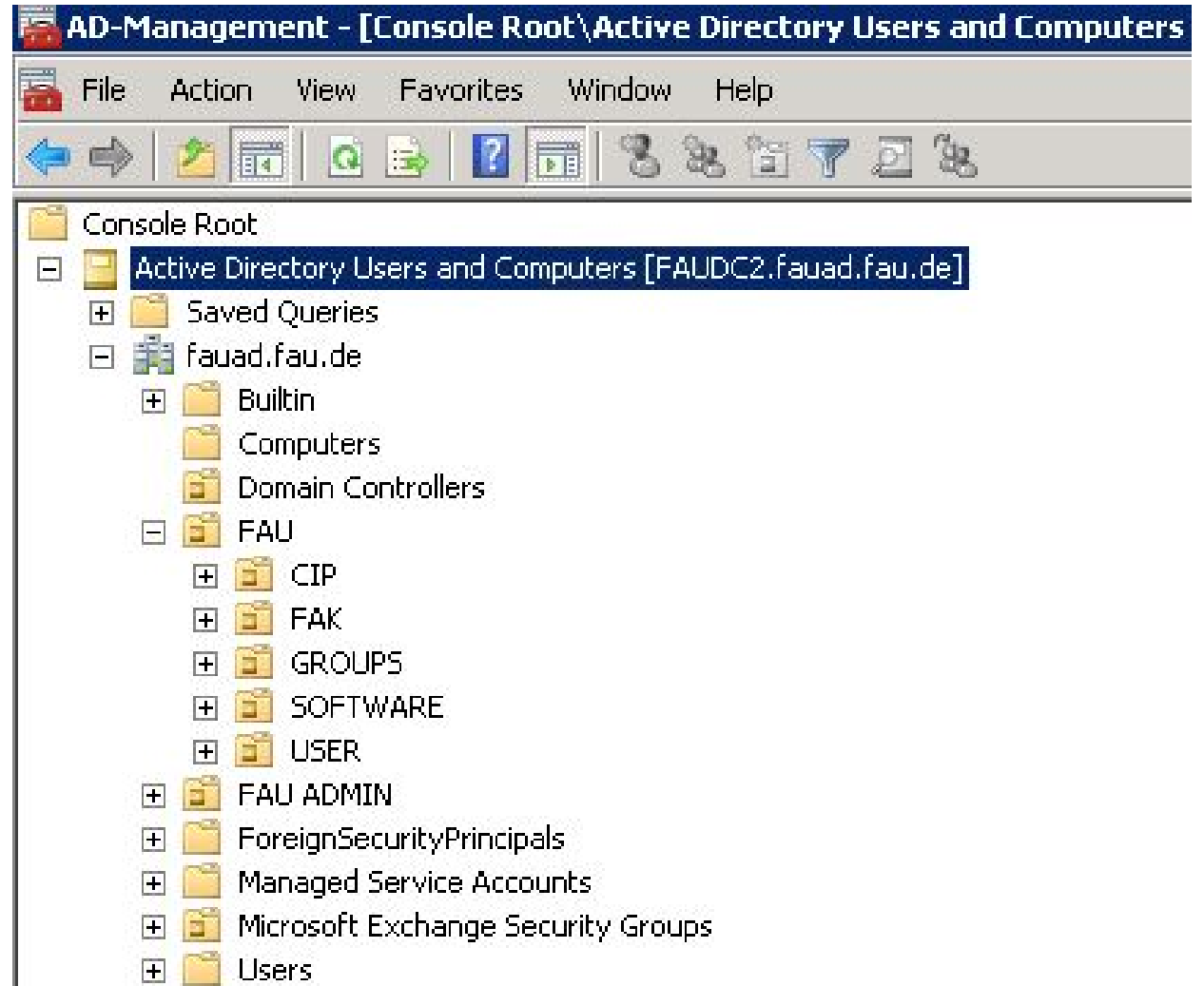
- Jet-DB
  - hierarchisch, relational, verteilt, skalierbar
  - Begrenzt auf 16 TB (2 Milliarden Objekte pro DC)
- 3 Haupttabellen
  - schema table (Schema)
  - link table (Objekt-Struktur)
  - data table (Daten)

# 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



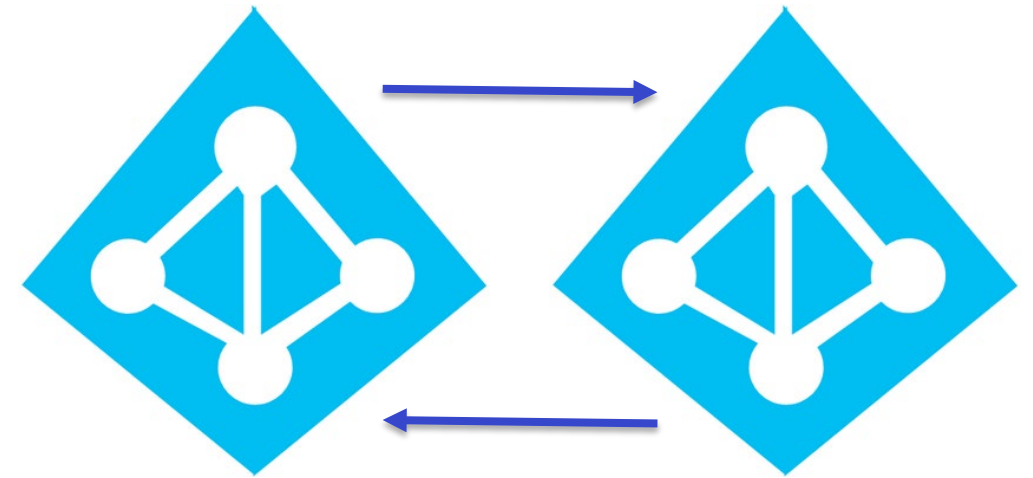
# Forest Strukturen – Single Forest

- 1 Forest (Gesamtstruktur)  
für alle Domains
  - wenig administrativer Overhead  
(„keep it simple and stupid“)
  - gemeinsamer Global Catalog
  - gleiches Schema für alle Domains



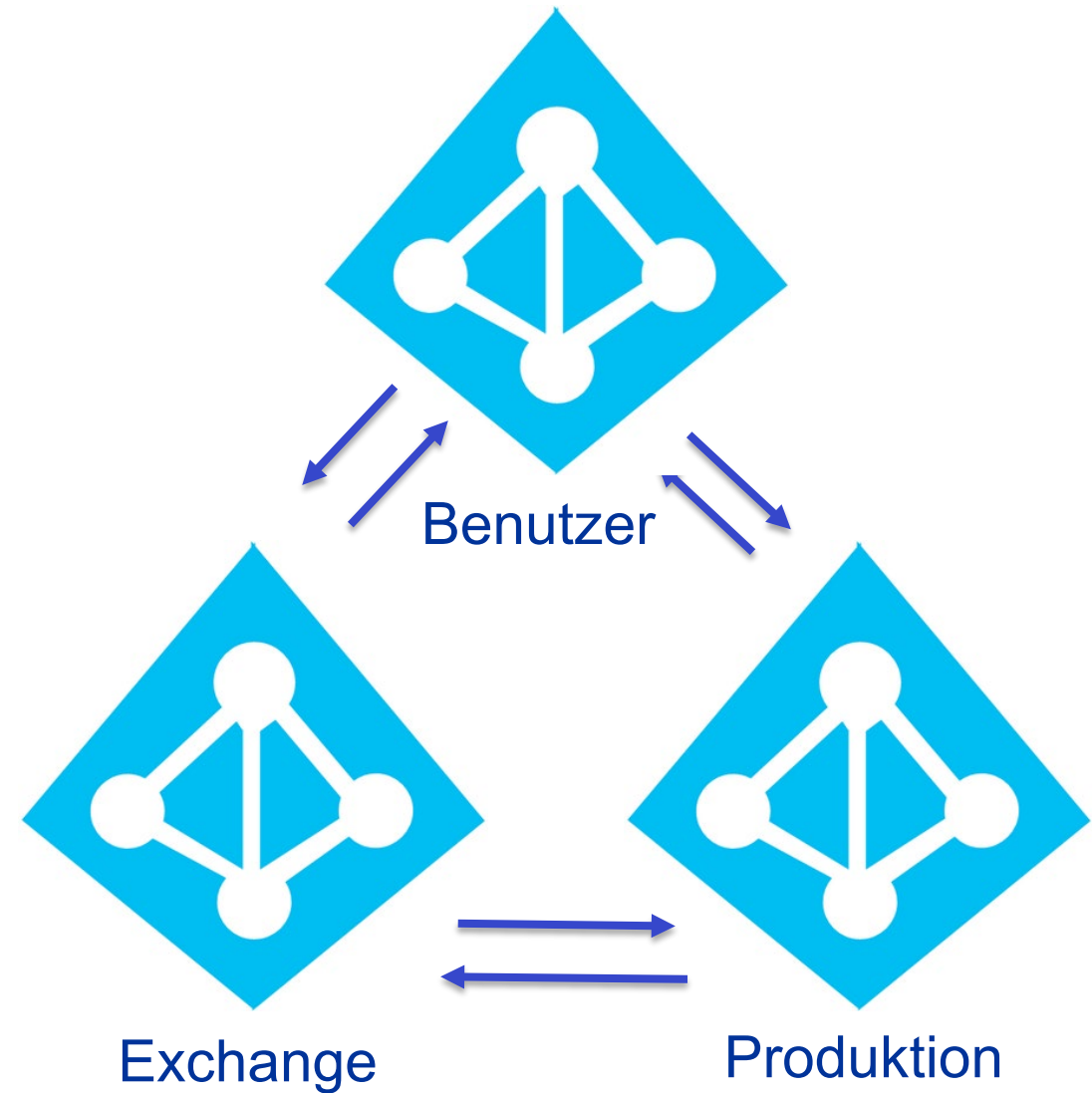
# Multi Forest Modell – Trusted Forest

- (mind.) 2 Forests
  - Teile der Organisation
    - › Autonom
    - › Isoliert
    - › Eigenständig
  - Zugriff auf Ressourcen über Trust möglich



# Multi Forest Modell – Resource Forest

- Ressourcen in eigenem Forest
- Modell für Service-Provider
- Administrative Trennung
- Abschirmung



# Multi Forest Modell – Secured Forest

- 2 getrennte Forests
- Keine Vertrauensstellung
- Absicherung von Anwendungen und Daten
  - Netzsegment
  - Firewall
- Getrennte Benutzerkonten notwendig



Organisation



High Security

# Aufbau – Hierarchie

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

→ Planung sehr wichtig !



# REPLIKATION ACTIVE DIRECTORY



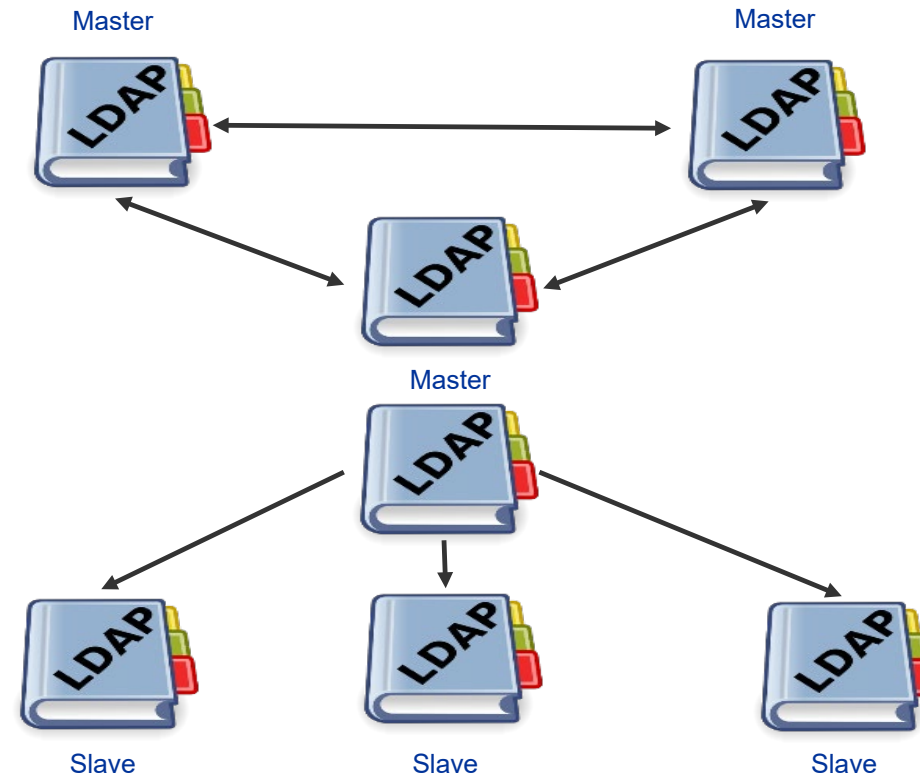
- Multi-Master-Replikation
- FSMO-Rollen

# 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 (Forest)
- 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 (Forest)
- 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):  
 $SID = \text{Domain SID} + \text{relative Objekt ID (RID)}$
- Zuständig wenn Objekte über Domaingrenzen hinweg verschoben werden

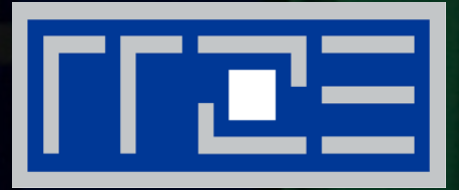
# FSMO – PDC Emulator

- 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

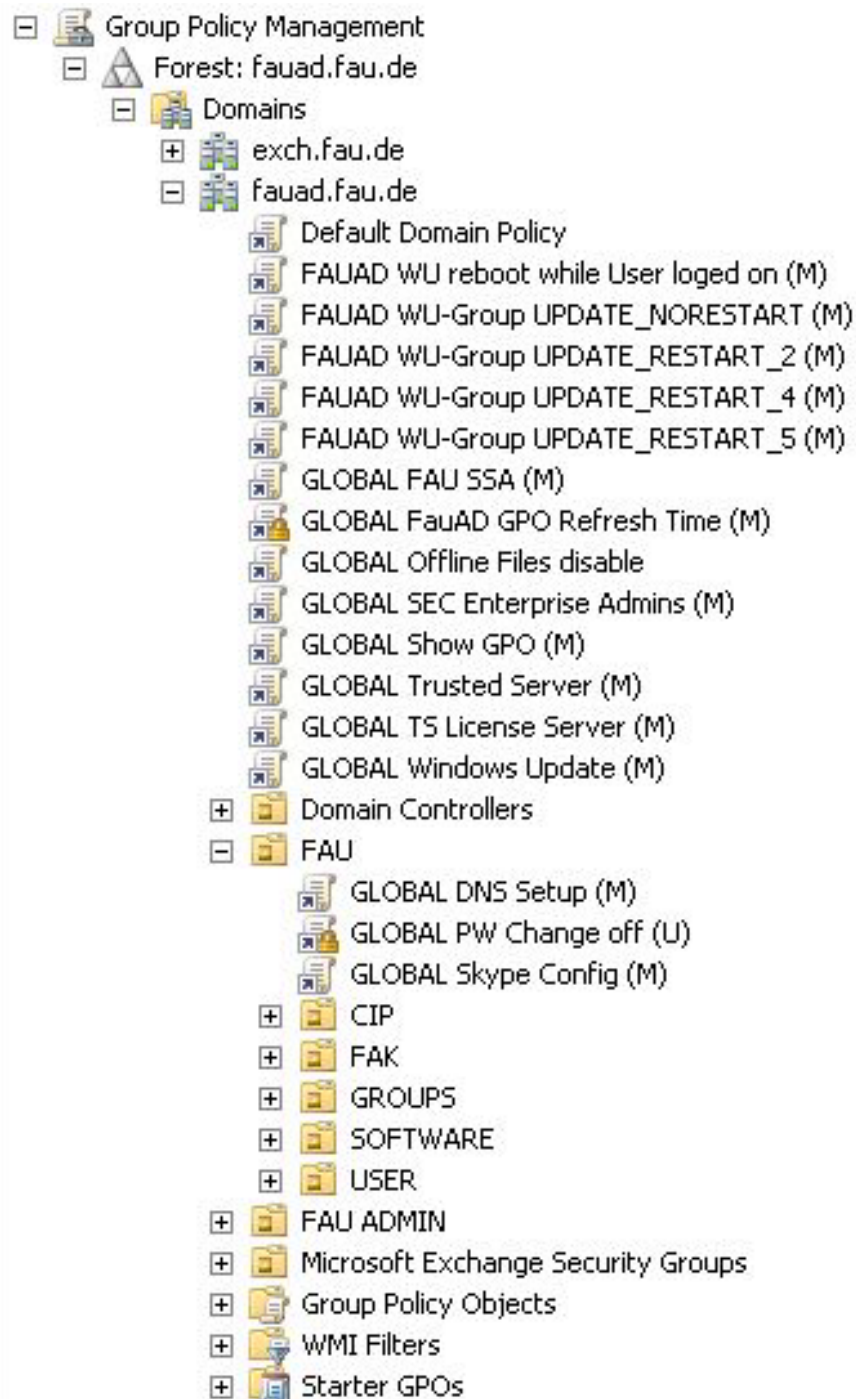
- 1x pro Domain
- Zuständig für Inter-Domain-Kommunikation
- **Global Catalog**
  - Such-Cache zum Auffinden aller Objekte in einer Domain oder eines Forrests
  - Wird durch Multi-Master-Replikation aktualisiert

# GRUPPENRICHTLINIEN ACTIVE DIRECTORY



- Benutzer
- Maschine



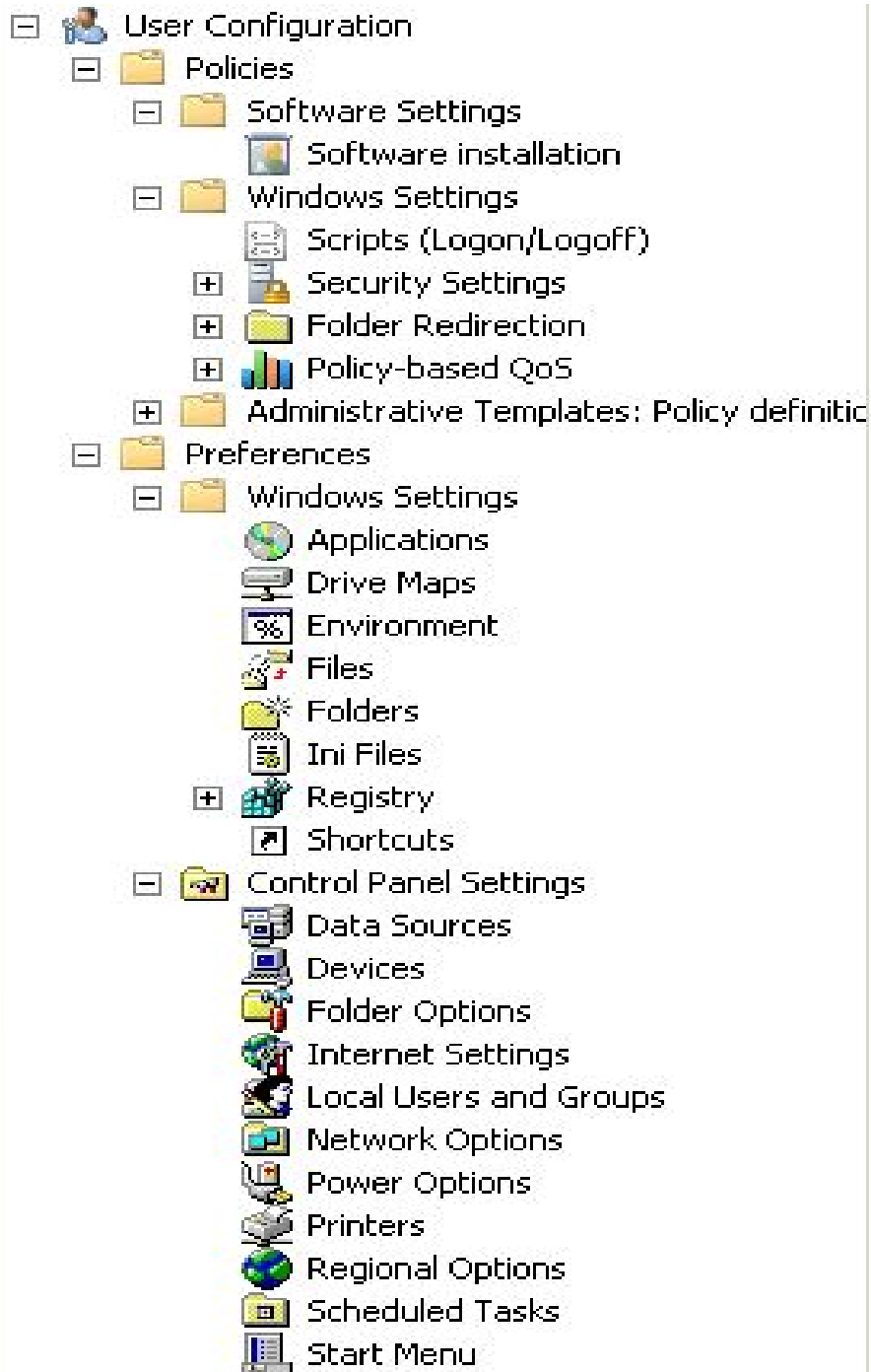


# Gruppenrichtlinien

## Group Policy Object (GPO)

---

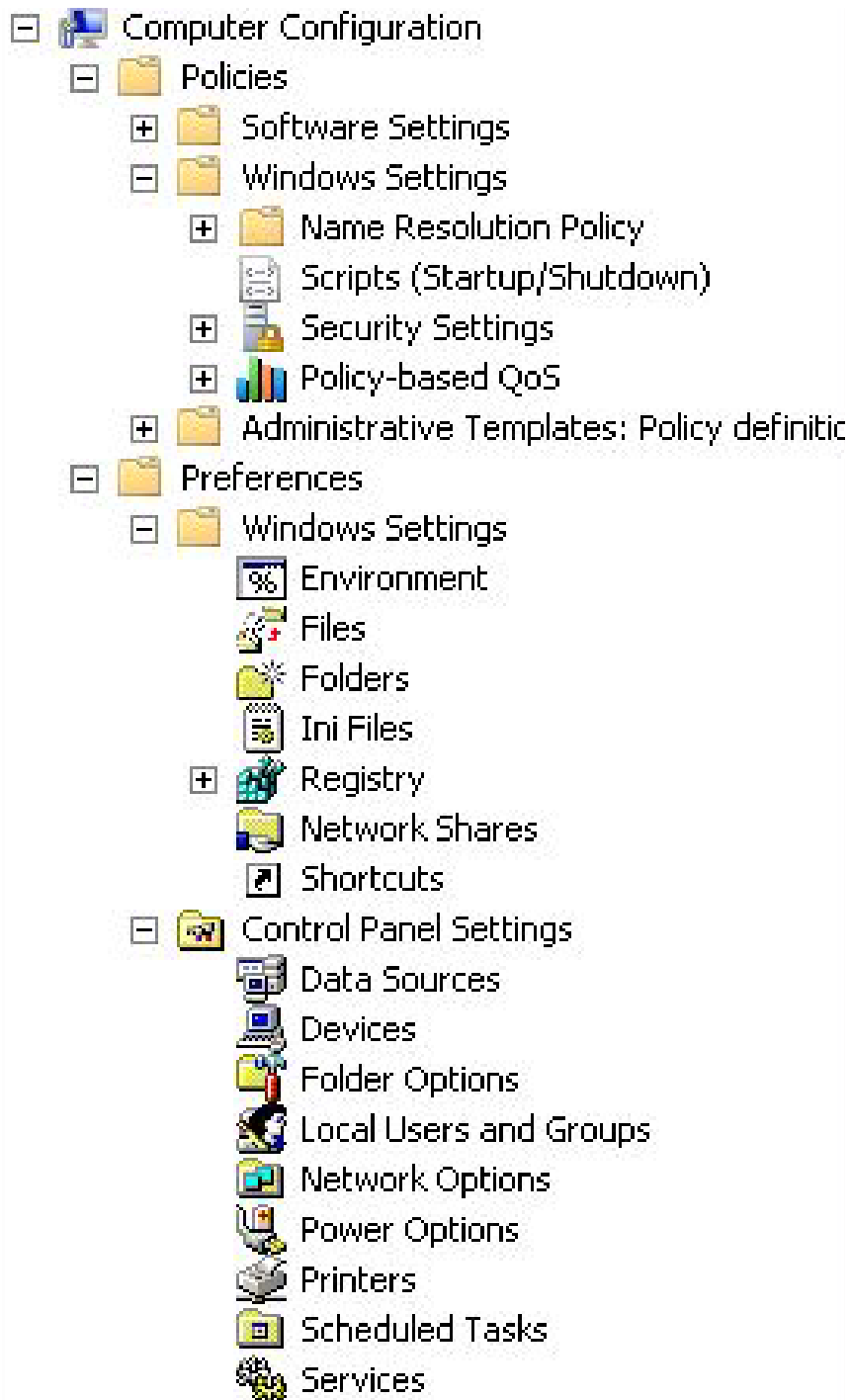
- Zentrale Verteilung von Konfigurationen für
  - Benutzer
  - Computer
- Wirken hierarchisch  
„Je näher am Objekt, desto wirksamer“
- Erweiterbar durch ADM / ADMX-Vorlagen



# Gruppenrichtlinie Benutzer

---

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

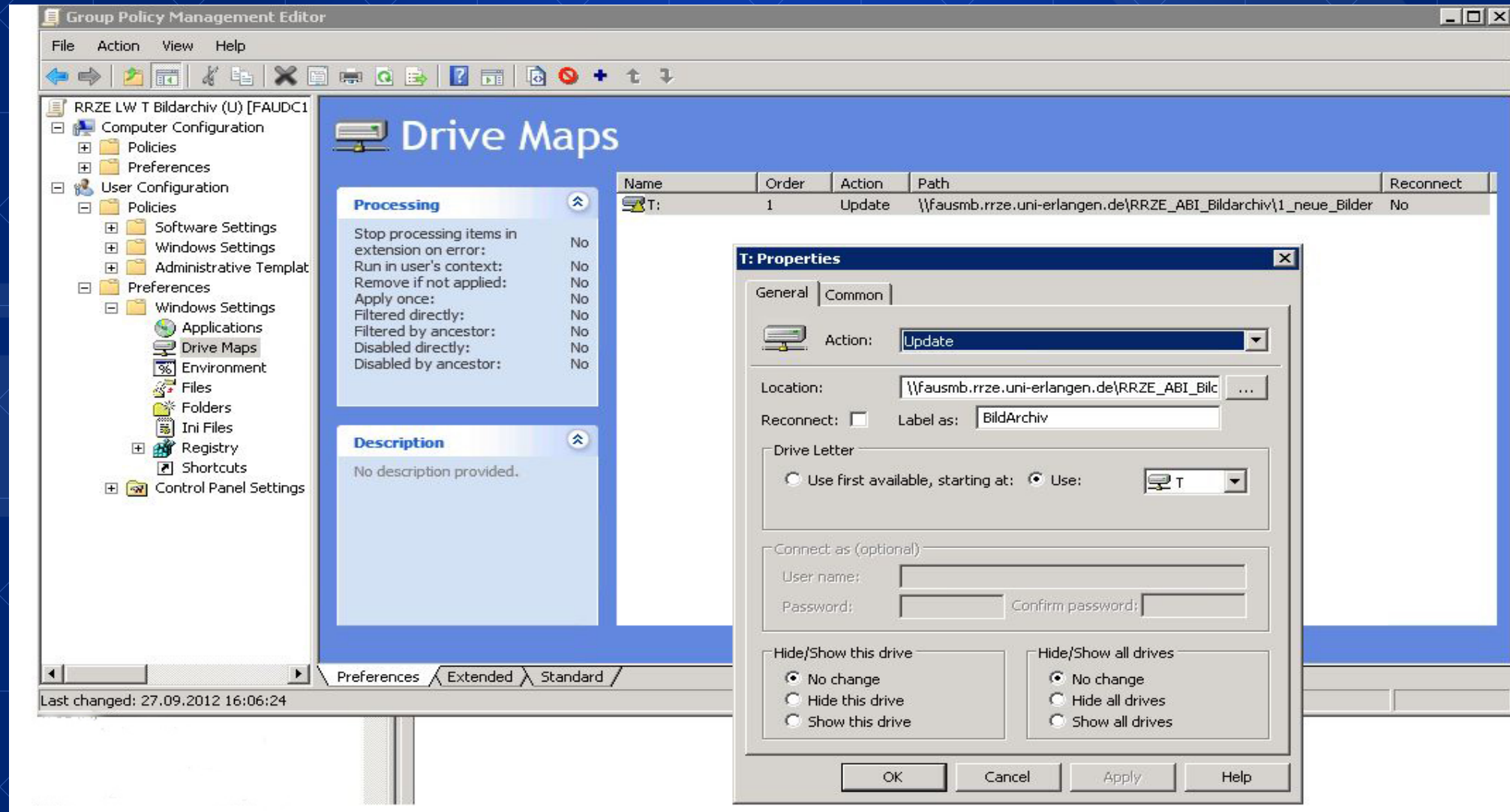


# Gruppenrichtlinie Computer

---

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

# Gruppenrichtlinien – ein Beispiel





# Gruppenrichtlinien – hinter den Kulissen

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    </Drive>
11  </Drives>
12
```



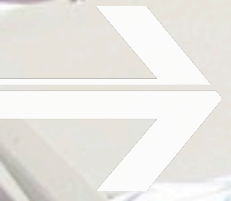
# ACTIVE DIRECTORY SICHERHEIT / SECURITY



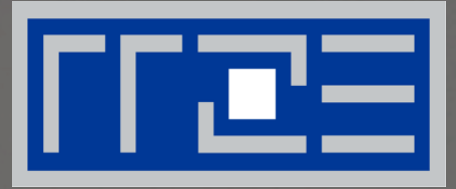
- Sicherheit – schnell umsetzbar

# Active Directory – Sicherheitsempfehlungen

- Identische Installation (Baseline) aller Domain Controller (DC)
- Wenig zusätzliche Software auf DCs installieren
- Lokale Firewall aktivieren
- „Plug and Play“-Service deaktivieren
- Druckspooler-Service deaktivieren
- RDP-Zugriff auf DCs auf (wenige) Admin-Rechner beschränken
- Separate Admin-Accounts verwenden
- Sinnvolle Password Policies setzen
- Sind alle notwendigen Sicherheitsupdates installiert?



# BLICK IN DIE FAUAD



Live-Demo



# Fehlersuche – Hilfe zur Selbsthilfe (1)

- 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 ?

# Fehlersuche – Hilfe zur Selbsthilfe (2)

- Werden Gruppenrichtlinien/Policies „gezogen“?
  - gpresult /r
  - rsop
  - gpupdate [/force]
- RRZE-Clientanalyse-Tool
  - <https://www.downloads.rrze.fau.de/windows/Install-RRZE-ClientAnalyse.exe>
- Windows-Webseite – <https://windows.rrze.fau.de>

# Fehlersuche – RRZE-Clientanalyse

RRZE Client-Analyse

Folgende Information wurden gesammelt :

Protokoll des Client-Rechners am 07.07.2021

-----

Allgemeine Informationen:

-----

Computername: [REDACTED]  
Benutzername: [REDACTED]  
Logon-Domäne: FAUAD  
Logon-Server: \\FAUDC1  
Site: ERL  
SCCM-Client: 5.00.9049.1035

IP-Adresse: 10.11.47.152  
Subnetzmaske: 255.0.0.0  
Default Gateway: 10.0.0.1  
IPv6-Adresse: fd00:638:a000:f100:10:11:47:152  
Default Gateway: ::  
DHCPv6 DUID: 00-01-00-01-20-B0-AC-AA-C8-5B-76-FE-EB-30

Betriebssystem: Windows\_NT  
Version: Microsoft Windows 10 Enterprise  
Release ID: 2004  
Fullversion: 10.0.19041.1052  
Letzter Start: 7. Juli 2021 08:27

Homedrive: C:  
Homepath: \\Users\\[REDACTED]  
Homeshare:

Freier Speicher auf Laufwerk C: 27,6 GB

SW HW

Protokoll auf Desktop speichern Protokoll per E-Mail senden Protokoll ausdrucken Protokoll schließen

LOG

# Weitere Vorträge zur „Systemausbildung“

05.05.2021 – Systemüberwachung / Monitoring

12.05.2021 – Backup / Archiv

19.05.2021 – Einblicke in das Management von Apple-Geräten

09.06.2021 – Storage & Filesysteme

16.06.2021 – IT-Sicherheit

23.06.2021 – Windows-Dienste

30.06.2021 – Virtualisierung

07.07.2021 – **Benutzerverwaltung: MS Active Directory**

14.07.2021 – Kerberos

Immer mittwochs  
(ab 14:15 Uhr)  
- online -

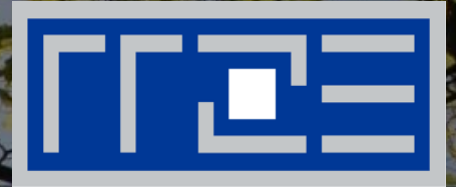
**Details:** [www.rrze.fau.de/veranstaltungen/veranstaltungskalender/](http://www.rrze.fau.de/veranstaltungen/veranstaltungskalender/)

# RRZE-Veranstaltungskalender und Mailinglisten

- Anleitung Kalender abonnieren oder bookmarken
  - [www.rrze.fau.de/veranstaltungen/veranstaltungskalender/](http://www.rrze.fau.de/veranstaltungen/veranstaltungskalender/)
- 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>



# REGIONALES RECHENZENTRUM ERLANGEN [RRZE]



**Vielen Dank für Ihre Aufmerksamkeit!**

Regionales RechenZentrum Erlangen [RRZE]  
Martensstraße 1, 91058 Erlangen  
[www.rrze.fau.de](http://www.rrze.fau.de)