Administration von PCs im Active Directory der GWDG

Christina Buck

Der rote Faden

09.00 – 12.30 Uhr

- Active Directory (AD)
- Administration im AD
- Computer-Migration
- Benutzer-Migration
- Speicherplatz
- Mailen
- Drucken

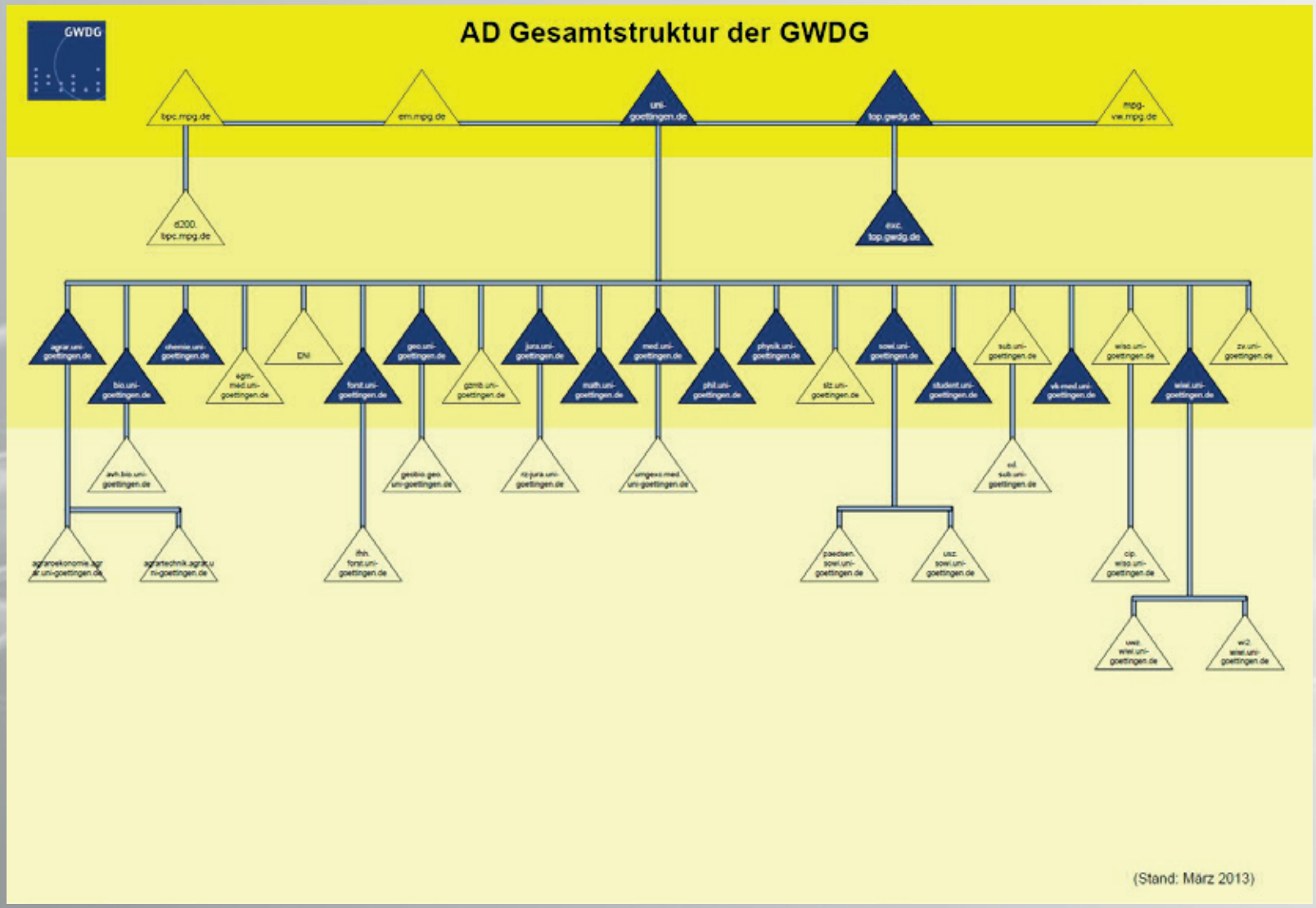
13.30 – 15.30 Uhr

- Sophos Anti-Virus
- Fragerunde

Das

ACTIVE DIRECTORY

Die Active-Directory-Gesamtstruktur der GWDG



Das Active Directory der GWDG

- ca. 15 000 GWDG-Benutzerkonten
- ca. 15 900 aktive studentische Benutzerkonten
- Über 10000 Systeme in 40 Domänen

Arbeiten im Active Directory - „Single Sign-On“

- Nur ein Benutzerkonto für alle Systeme und zentralen Dienste innerhalb des Active Directory.
- Einmalige Authentifizierung für alle im Active Directory vorhandenen Ressourcen.
- Benutzerkonto aus Vor- + Nachname:
  Max Mustermann wird zu mmuster
- Servergespeicherte Profile ermöglichen eine persönliche Umgebung an allen AD-PCs.

Aufbau des GWDG-AD-Forrest

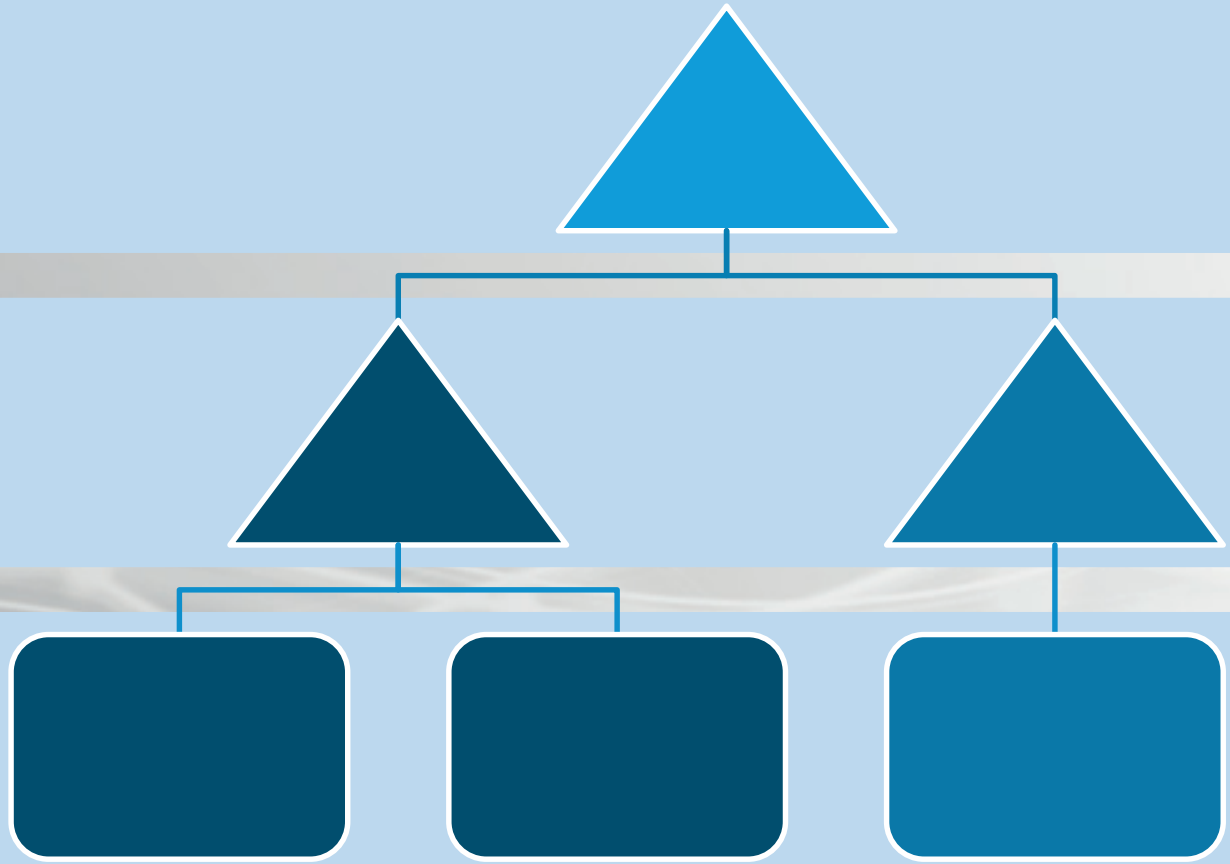
Benutzerdomäne

- Benutzerkonten
- Zentrale Server/Dienste

Ressourcendomäne

- Universelle Gruppen
- Computerkonten

Organisationseinheiten (OUs)



Die Benutzerdomäne

Default Domain Policy

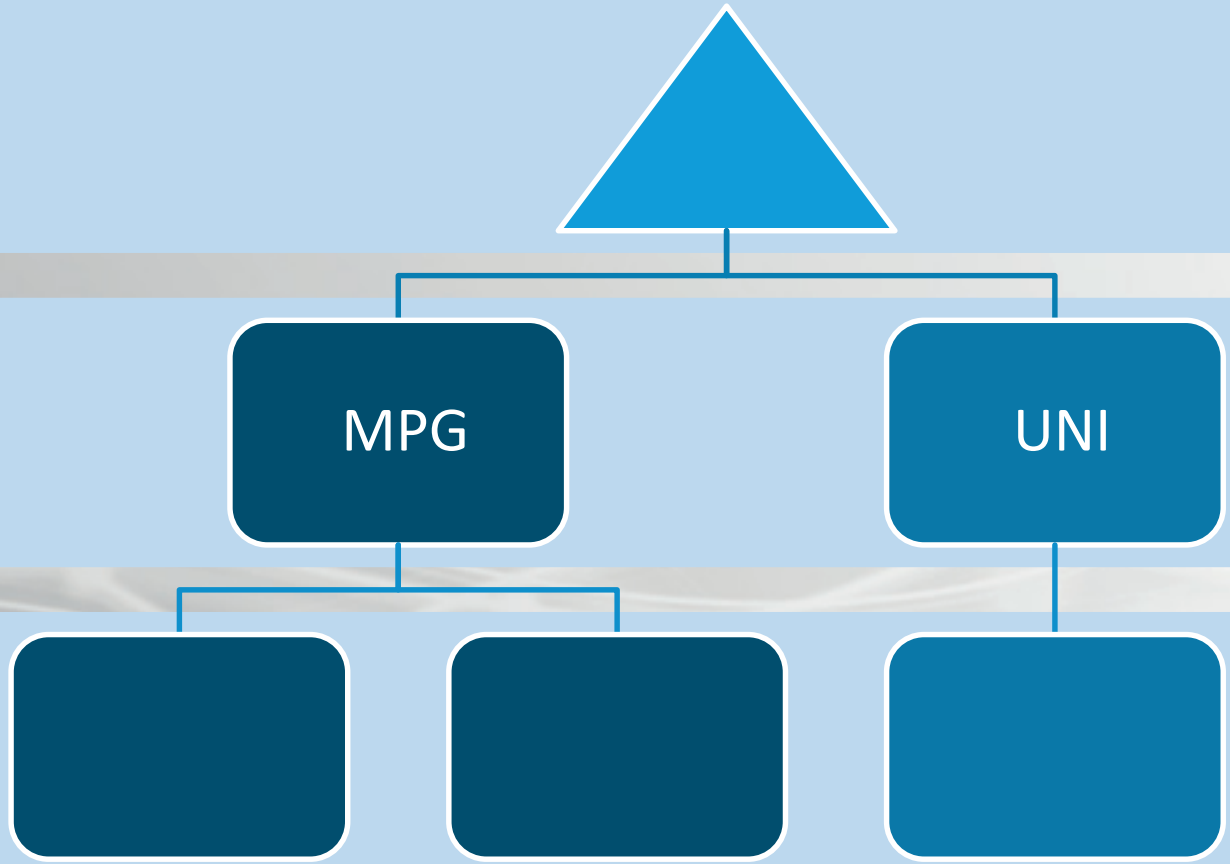
- Kennwortrichtlinien
- Log-on News

GPOs auf Mandantenebene

- Ordnerumleitungen

GPOs auf Institutsebene

- Log-on-Skripte

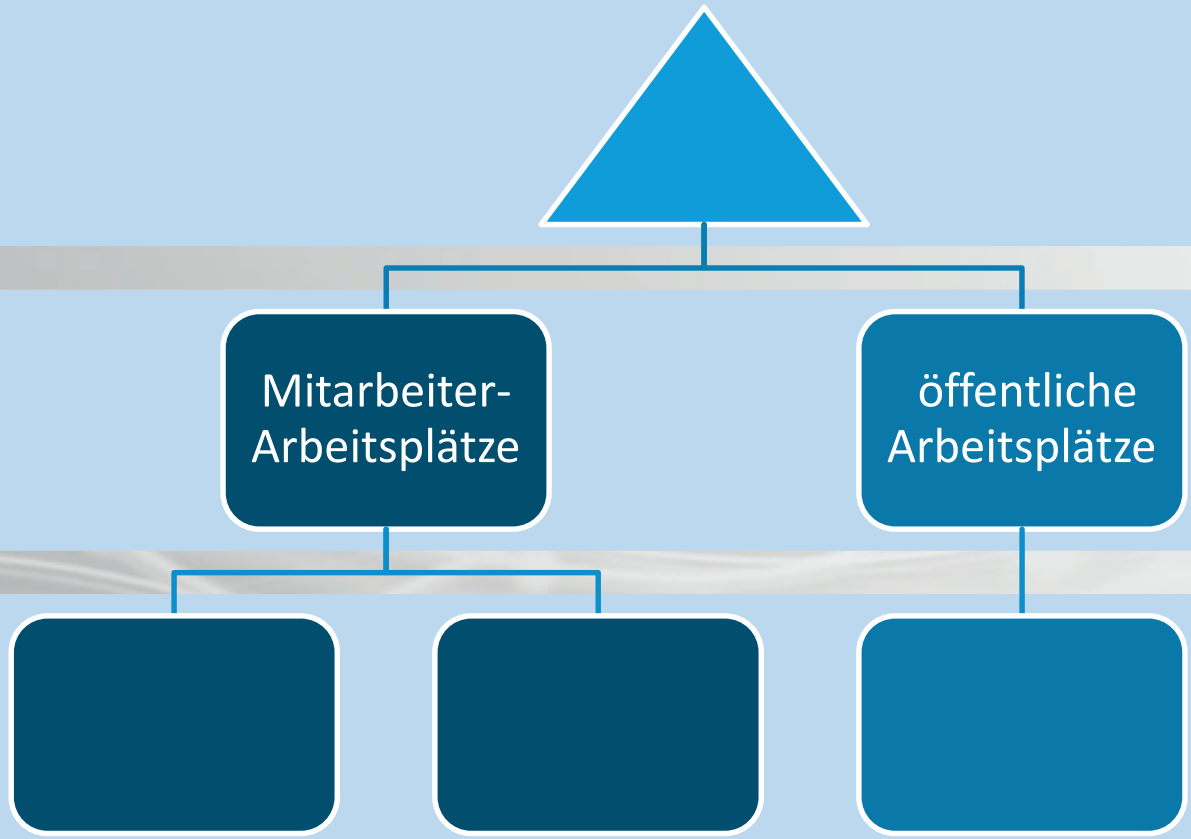


Die Ressourcendomäne

Default Domain Policy
- Kennwortrichtlinien
- IPv6 deaktivieren
- Zertifikatseinstellungen

Sicherheitsrelevante Einstellungen
- Firewall
- Dienste starten
- WSUS

GPOs auf Abteilungsebene
- Softwareverteilung
- Weitere Portausnahmen
- Ortsabhängige Log-on-Skripte



Domänen und Organisationseinheiten (OU)

- Zuordnung der OUs in eine Fachdomäne
- Namensschema für die OU:
  Institutskürzel + Abteilungsnummer (Bsp.: UHDP100)
- 1. Ebene Institut (UHDP)
  2. Ebene Abteilung (UHDP100)
  3. Ebene Unterteilung nach Benutzern und Computern, darunter Gruppen

Das Namensschema

- Name: Institutskürzel + Abteilungsnummer, z.B. Uxyz100
- Benutzergruppen:
  - Uxyz100-admins (Administratorgruppe)
  - Uxyz100 (Mitarbeiter + Studenten)
- Benutzerkonto: „eindeutig zuzuordnen“
  - 0Benutzername (Administratorkonto) 0mmuster
  - Uxyz100-Gast1 (Gäste, falls gewünscht)
- Computer: UG-Uxyz100-C001
- Drucker: Uxyz100-P01
- Server: UG-Uxyz100-VS1 / S1

Funktionen von Gruppenrichtlinien

- **Benutzerkonfiguration in der GWDG-Domäne**
  - Domänen-Richtlinien
    - Ordner umleiten (z.B. „Eigene Dateien“)
    - Sicherheitseinstellungen (z.B. Kennwortrichtlinien)
  - OU-Richtlinien
    - Logon-Skripte (Drucker- und Laufwerksverbindungen)

- **Computerkonfiguration in der Institutsdomäne**
  - Zentrale Softwareverteilung
  - Konfiguration der Firewall (z.B. für Sophos)
  - Windows-Update-Einstellungen

Logon-Skripte

Einzufügende Skriptzeilen:

```
rem löschen der alten Druckerverbindungen
rem con2prt /f
rem Anlegen der Drucker
con2prt /c \\gwd-winprint.top.gwdg.de\kmlp4s

rem festlegen des STANDARD-Druckers
rem con2prt /cd \\gwd-
winprint.top.gwdg.de\kmlp4s
net use w: /delete
net use /PERSISTENT:NO
net use W: \\wfs-zentral\UMYZ_all$
```

- Sicherheitsrelevante Konfigurationen durch zentrale Gruppenrichtlinien (NT4: 386, 2008 R2: 11.346)

- WSUS (Windows Server Update Services)
- Zentrale Softwareverteilung (per Gruppenrichtlinie oder Baramundi)
- Zentraler Fileservice
- Zentrales Druckmanagement
- Zentrale Antivirenlösung (Sophos Enterprise Console)

ADMINISTRATION IM AD

Informationspolitik

- Alle wichtigen Informationen unsererseits erfolgen über die Mailingliste gwdg-ad.
  - Melden Sie sich daher unbedingt an!
  - Anmeldung über: https://listserv.gwdg.de/mailman/listinfo/gwdg-ad
- Geben Sie uns Bescheid, wenn es einen Personalwechsel gibt und informieren Sie uns bei Änderungen der Kontaktdaten, am besten über support@gwdg.de.

Administration im Active Directory

- Zentrale Verwaltung der Arbeitsstationen über den Terminalserver „GWD-WinTS3“
  - „Active Directory Benutzer und –Computer“
    - Verwalten von Gruppenmitgliedschaften
    - Erstellen und Zuordnen von Computerkonten
    - Aufruf der „Computerverwaltung“ der Arbeitsstationen
  - „Sophos Enterprise Console“
    - Zentrale Verwaltung der Anti-Viren-Software

Die Administratorengruppe Uxyz100-Admins

- Universelle Gruppen ermöglichen das Hinzufügen von Konten aus anderen Domänen.
- Die Gruppe wird nach der Migration des Rechners in die Gruppe der lokalen Administratoren eingefügt.
- **Vorteil:** Vereinfacht die Zuordnung von Administratoren
  - Das Hinzufügen und Entfernen von Benutzerkonten ist mit wenigen Mausklicks durchgeführt, z.B. bei Urlaubsvertretung oder Personalwechsel.
  - Ermöglicht zentralen Zugriff (z.B. Sophos).

Rechtevergabe in den gemeinsamen Freigaben

- Administratives Konto zur Verwaltung (0mmuster)
- Freigaberechte (durch GWDG-Mitarbeiter konfiguriert)
- NTFS-Rechte:
  1. Ordnerstruktur erstellen (Verwaltung, Technik,..)
  2. Gruppenstruktur erstellen (Verwaltung, Technik,..)
  3. Vererbung aufheben
  4. individuelle Einstellungen
- Freigabe- und NTFS-Rechte müssen für einen erfolgreichen Zugriff konfiguriert sein

Die wichtigsten NTFS-Rechte

- **Lesen** (Ordner auflisten, Dateien lesen, Attribute lesen)
- **Lesen, Ausführen** (Lesen und Ordner durchsuchen, Dateien Ausführen)
- **Schreiben** (Dateien u. Ordner erstellen, Attribute schreiben)
- **Ändern** (Lesen, Ausführen, Schreiben und löschen)
- **Vollzugriff** (alles, auch Rechteveränderung ist möglich)

Windows Server Update Service (WSUS)

- monatliche E-Mail-Benachrichtigung bei Updatefehlern

- Unterstützung:
  - FAQ für WSUS auf den Webseiten der GWDG oder support@gwdg.de

- Notwendig:
  - Namensschema muss eingehalten werden!
  - Nicht mehr vorhandene Computer aus dem Active Directory austragen (rechte Maustaste > löschen)!

Zentrale Softwareverteilung per GPO

- Microsoft Office 2003 Professional (nur mit Lizenznachweis)
- MS Office 2010 (nur mit Lizenznachweis)
- Open Office
- Firefox
- Foxit Reader
- Flash Player
- Java Runtime

Zentrale Verteilung per baramundi

- Windows 7, Windows 8
- MS Office 2010, MS Office 2013
- LibreOffice
- Firefox, Thunderbird, Chrome
- QuickTime
- TeamViewer 8
- Skype
- VLC Player
- PDF Creator
- Flash Player
- Java
- KeyPath
- Image Burn
- Sophos (selbst gepackt)
- Uvm. – alles weitere kann evtl. gepackt werden

MIGRATION VON COMPUTERN INS AD

Migration eines Windows-Rechners in das Active Directory

- Computername an das Namensschema anpassen
- IP-Adresse über das IPAM einrichten (lassen)
- Computerkonto im AD erstellen
- Notwendige Einstellungen vornehmen
- Computer in die Domäne heben

Computername anpassen + IPAM

- Computername anpassen:
  - Strukturierte Namensvergabe bei den Rechnern
    nach Standort, Abteilung, IP-Adresse
- IP-Adresse über das IPAM einrichten (lassen):
  - Netzwerkbeauftragter des Instituts
  - https://ipam.gwdg.de/

Computerkonto im AD anlegen

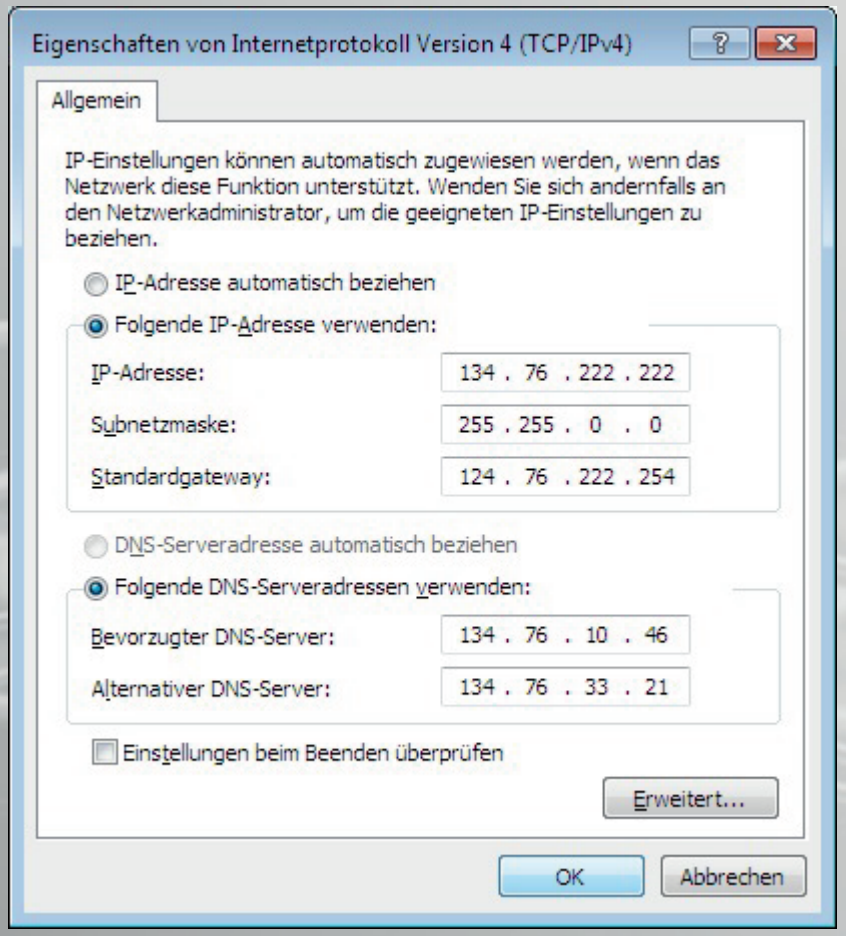
- Computerkonto im AD anlegen, erst danach in die Domäne heben.

- Falls umgekehrt, wird ein Computerkonto unter „Computers“ erzeugt.
  - Dieses Konto kann von einem Institutsadmin nicht in die eigene OU verschoben werden!

Wichtige Einstellungen

- DNS hat sich geändert
  - DDNS Server der GWDG für AD: 134.76.26.21, 134.76.26.26 gilt nicht mehr
  - DNS-Server der GWDG: 134.76.10.46, 134.76.33.21
- WINS Server der GWDG: 134.76.26.21, 134.76.26.26,
  - 134.76.11.71 wird langfristig entfallen
- Weitere Einstellungen

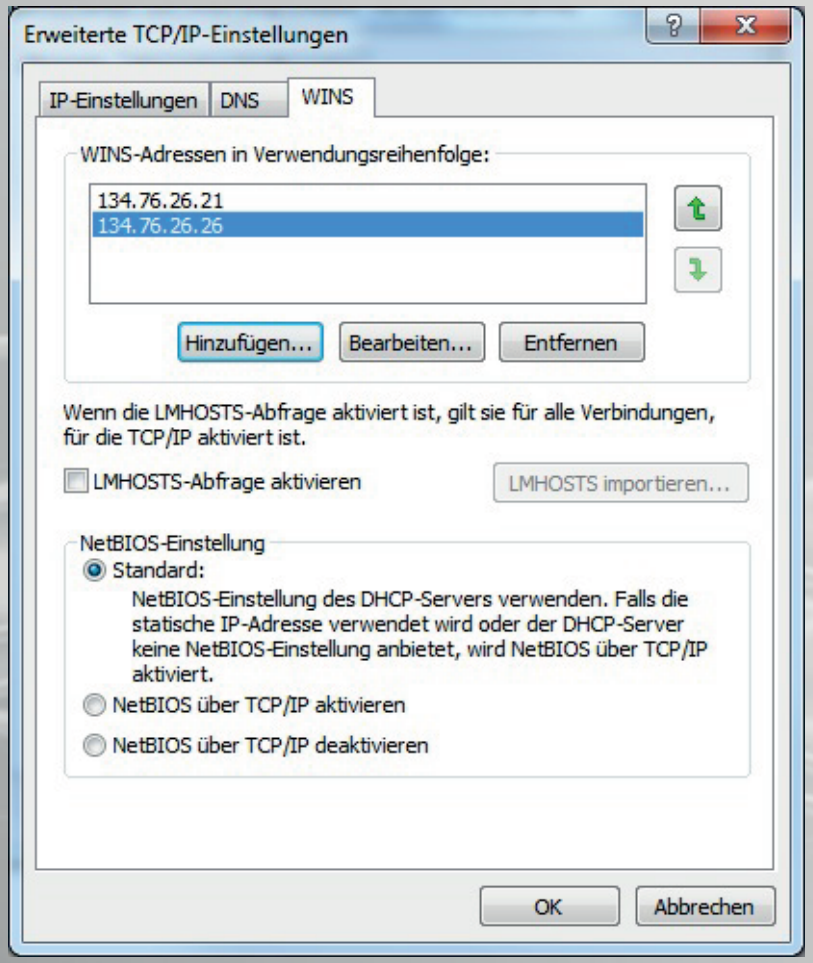
Konfiguration der DNS-Netzwerkeinstellungen



DDNS: dynamischer Domain-Name-Server-Eintrag

DNS: Domain-Name-Server
Ermöglicht die Umsetzung von Internet-Name in Internet-Adresse.

Konfiguration des WINS-Netzwerkeinstellungen



WINS: Windows-Name- Service-Eintrag
Ermöglicht die Umsetzung von NetBIOS-Computernamen in IP-Adressen

LMHOSTS:
Lokale Umsetzungstabelle

134.76.11.71 nicht verwenden!

Weitere Einstellungen

- **Dateirechte**
  - NTFS ggf. einschränken
  - keine Freigaben aus Sicherheitsgründen!

Computer in die Domäne heben

- **Computer in die Domäne heben**
  XP: Arbeitsplatz-Eigenschaften > Computername > Ändern... > von „Arbeitsgruppe“ zu „Domäne“ z. B. „Top.GWDG.de“> Neustart
- Vista/W7: Start > Computer > Eigenschaften > Einstellungen ändern
- **Ordneroptionen**
  - Offlinedateien nicht synchronisieren
  - keine einfache Dateifreigabe / Freigabe-Assistent!
- **Benutzerverwaltung**
  „Administrator“ umbenennen, Admin-Gruppe „Uxyz100-admins“ eintragen

Besondere Merkmale für öffentliche Rechner

- Erweiterte Sicherheitseinstellungen im Betriebssystem per Richtlinie:
  z. B. Schreibrechte auf der Systempartition entfernen
- Besondere Einstellungen in den GPOs (Konfigurationen für „aktive Desktop“, Einschränkungen beim Ausführen von Software, eingeschränkte Benutzeranmeldung, etc.)
- Installation des BS: WDS (Windows Deployment Services)
- Bereitstellung von Software:
  - zentrale Verteilung durch Gruppenrichtlinien
  - Terminalserver
- Besondere Richtlinieneinstellungen in der Sophos Enterprise Konsole

MIGRATION DER BENUTZERUMGEBUNG INS AD

Vorbereitung einer Migration
Daten und Einstellungen sichern

- **Daten sichern**
  Kopieren der Daten auf das persönliche Laufwerk P: (\\Winfs-Uni\Benutzername$)
  Standard: min. 20 GB Speicherplatz

- **Programme und Dateien vom Desktop entfernen**
  (diese vergrößern das servergespeicherte Profil!)

Vorbereitung einer Migration
Daten und Einstellungen sichern

- **persönliche Einstellungen sichern mit**
  - **XP -> XP**
    „Übertragen von Dateien und Einstellungen“
  - **Vista/Windows 7 -> XP/Vista/Windows 7**
    “Windows- Easy Transfer“
- **Lohnt sich nur bei vielen Einstellungen**

SPEICHERPLATZ

Zentrale Speicherplätze

- Die zentralen Speicherplätze:

  Persönlicher Speicherbereich (Windows Failover Cluster 2008 R2)

  \\WinFS-UNI.top.gwdg.de\mmuster$

  Gemeinsamer Speicherbereich

  \\wfs-fakultaet\INST-all$

  Bsp. \\wfs-agrar.top.gwdg.de\uaao-all$

Der persönliche Speicherbereich

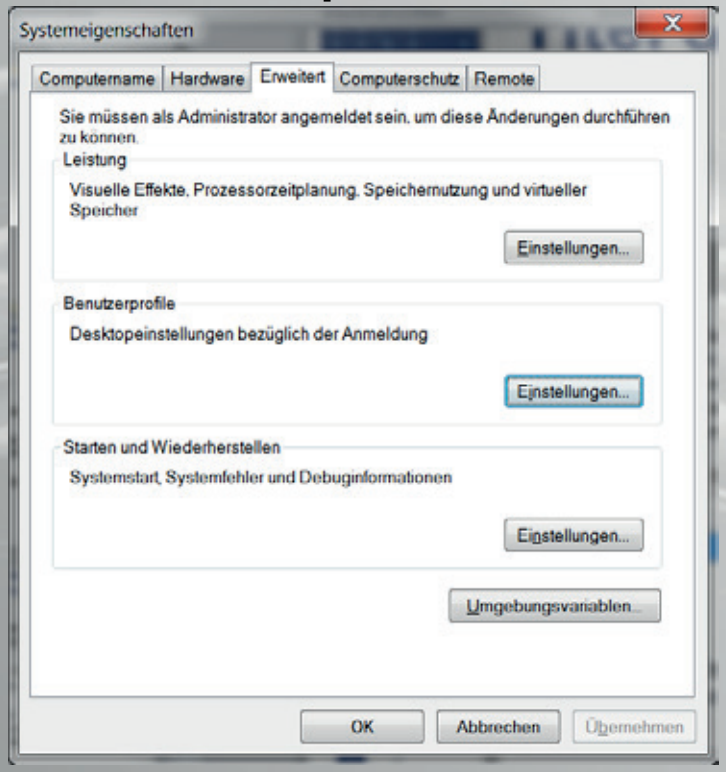
- Das „P:“-Laufwerk wird automatisch bei der Anmeldung im Active Directory verbunden.
- Der Ordner „Eigene Dateien“ auf der Arbeitsstation wird in den persönlichem Speicherbereich („P:“-Laufwerk) umgeleitet.
- Das „P:“-Laufwerk ist auf 25 GB quotiert und kann auf Anfrage erweitert werden. (support@gwdg.de)
- Der Profilpfad liegt innerhalb des persönlichen Speicherbereiches
  P:_GWDGsys\Profile2 - bei XP Professional
  P:_GWDGsys\Profile2.V2 - bei Vista und Windows7

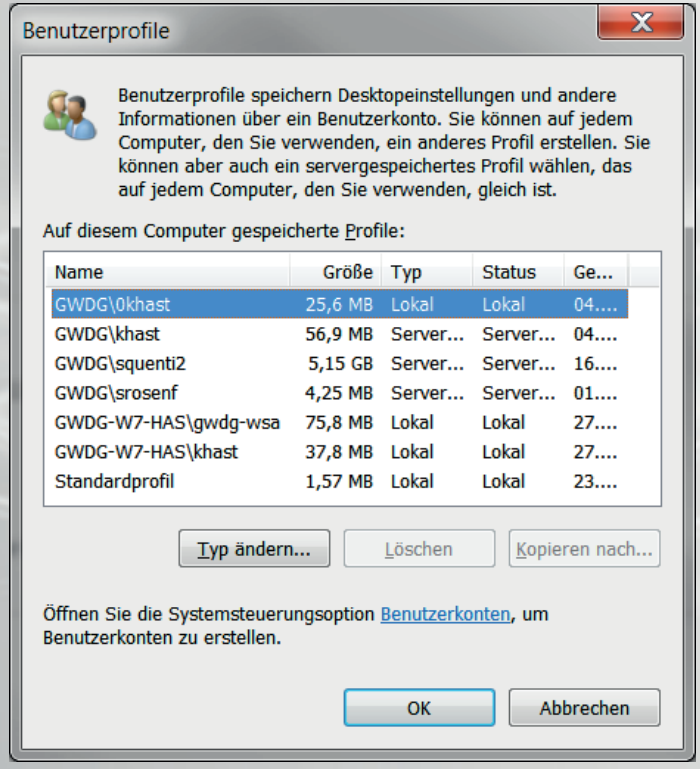
Servergespeicherte Profile

- Profilgröße max. ca. 200 MB
- Löschen von servergespeicherten Profilen
  - Auf der Arbeitsstation
    - XP: unproblematisch, direkt löschen
    - Vista / Win7 / Win 8: über Systemsteuerung löschen!
  - Im P: LW – Homeverzeichnis
- Häufige Fehler:
  - Speicherbereich im Profil
    - Mozilla Firefox, Thunderbird und Outlook
    - Desktop
  - Tiefe Ordnerstukturen, lange Dateinamen (macht auch beim Backup Probleme)

Vista und Windows 7/8: Profile löschen

- Start > Systemsteuerung > System > Erweiterte Systemeinstellungen > Benutzerprofile > Einstellungen



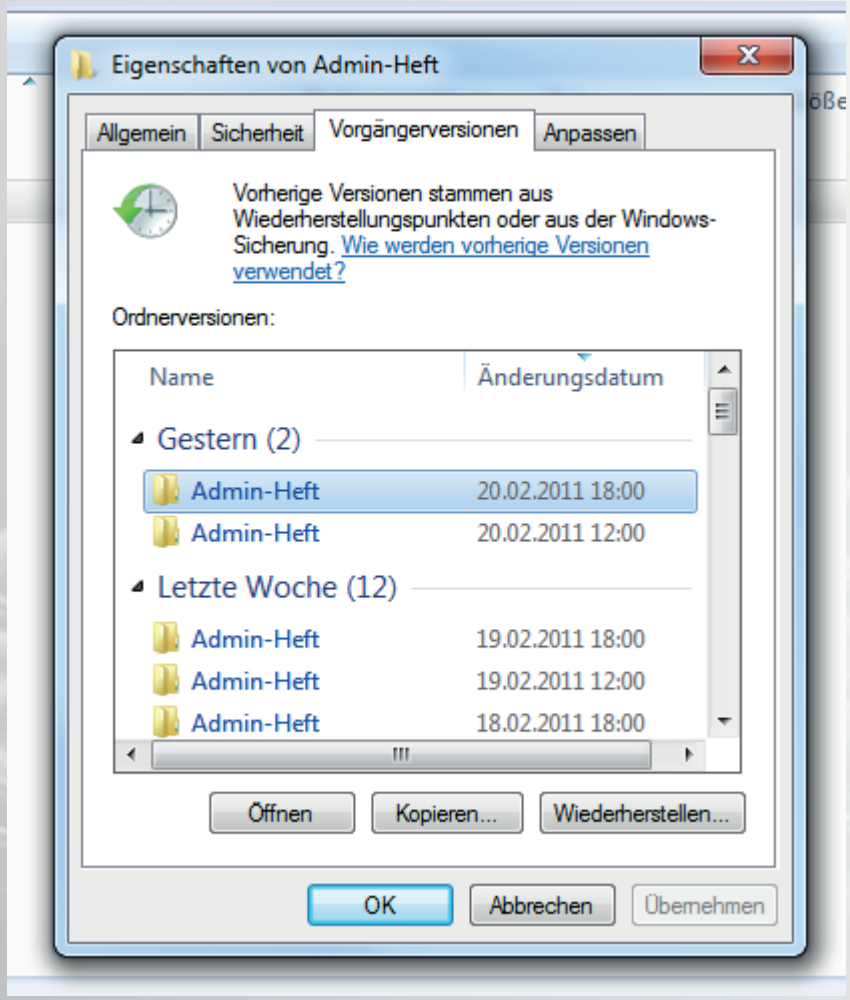


Der gemeinsame Speicherbereich

- Gemeinsam genutzte Daten
- Geeignet für Institute oder Abteilungen
- Auch als institutsübergreifender Speicherbereich nutzbar z. B. Arbeits- und Projektgruppen
- Kann mit Hilfe eines Logon-Skriptes verbunden werden:
  („W:“-Laufwerk)

Schattenkopien - Restore

- Wiederherstellung älterer Versionen
- twcli32.msi ab Betriebssystem Windows XP Pro SP3 standardmäßig vorhanden
- Funktioniert nicht offline bei Verwendung von Offlinesynchronisation
- Funktion fällt mittelfristig weg



MAILEN

Mailen

- **Exchange-2010-Server**
  - http://www.gwdg.de/index.php?id=2549
- **Outlook**
  - Ab Version 2010 mit Exchange nutzen
  - Webzugriff: OWA
- **Alternativen**
  - Thunderbird 7 (Achtung Profilpfad!)
  - Webzugriff: Squirrel Webmail

- **Kursangebot**
  - Ganztägiger Kurs am 29.09.2014, es sind noch Plätze frei!

DRUCKEN

Zentral verwaltete Institutsdrucker

- Installation auf Windows-Clustershare „GWD-Winprint“
  - Ausfallsicherheit
  - Zugriffsberechtigungen
  - Vorkonfigurierte Druckereinstellungen
  - Hohe Verfügbarkeit
  - Weniger Sicherheitslücken
  - Druckertreiber werden automatisch installiert
  - Logon-Skripte
  - Statistik auf Wunsch

Drucker verbinden

- **Logon-Skripte**
  - Automatische Verbindung der Drucker im Active Directory
- **Manuelle Verbindung**
  - \\GWD-Winprint.top.gwdg.de\[Drucker]
    - (Start > Ausführen > „\\GWD-Winprint“ > Doppelklick auf die gewünschte Warteschlange)

PAUSE!

GWDG

SOPHOS

Sophos-Installation in 2 Varianten: Manuelle Installation

- Installation vom Web-Server „Antivir.GWDG.de“
  - Benutzername „Sophos“
    Passwort „********“
- Konfiguration nach der Installation notwendig
- Sophos Enterprise Console Version 5.2
  - Für Systeme innerhalb des Active Directory der GWDG

Die Sophos Enterprise Console auf dem Terminalserver „GWD-WinTS3“

- Rechteverwaltung in der Sophos Enterprise Console
- „Synchronisation“: Einrichtung der Strukturen in Anlehnung an die Strukturen des ADs
- Konfiguration der Sophos-Software auf den Rechnern durch Zuweisen von Richtlinien
- Installation und Überwachung des Anti-Viren-Programms „Sophos Anti-Virus“

Voraussetzungen für die zentrale Administration

- An den Arbeitsplatzrechnern:
  - Ordneroptionen: keine „einfache Dateifreigabe“
- Einstellungen per Richtlinie im AD
  - **Firewall**:
    - Datei- und Druckerfreigabe
    - Ports 8192, 8193 und 8194 frei
  - **Aktivierte Dienste**:
    - Computer-Browser
    - Task-Planer
    - Server
    - Remote-Registrierung

Voraussetzungen bei den Rechnern für die zentrale Administration (Win 7 + 8)

- Aktivierte Dienste:
  - Aufgabenplanung
  - Computerbrowser
  - Remote-Registrierung
  - Server
- Eingeschaltet:
  - Netzwerkerkennung
  - Freigabe von Dateien

Sophos-Richtlinien

- **Update-Richtlinie**: aus welchem CID erfolgt die Aktualisierung und in welchem Benutzerkontext?
- **Antivirus- und HIPS- Richtlinie**: Konfiguration des Sophos-Klienten, Festlegung einer Benachrichtigung (z. B. per E-Mail) und Einrichtung einer zeitgesteuerten automatischen Überprüfung, Maßnahmen bei Virenfund
- **Firewall und NAC:** werden nicht verwendet
- **Application Control**: Blockieren von unerwünschten Anwendungen

Sophos-Richtlinien II

- **Data Control:** Kontrolle ungewollter Datenübertragung
- **Device Control:** Zugriffssteuerung für Computerhardware
- **Manipulationsschutz:** Wer darf die Sophos-Software auf dem Rechner konfigurieren?
- **Patch**: Sind die aktuellen Sicherheits-Patches installiert?
- **Web Control**: Welche Webseiten dürfen Benutzer im Browser öffnen?

Rechner hinzufügen und schützen

- Synchronisation mit dem Active Directory
- automatische Installation von Sophos ist möglich

- Manuelles Hinzufügen von Computern zu den Sophos-Gruppen

- Schützen der Klienten durch Installation von Sophos (Account mit Admin-Rechten auf den Klienten erforderlich: Admin-Gruppe)

Häufige Fehler in der Enterprise Console

- Software kann nicht installiert werden
- Gruppenrichtlinien werden nicht übernommen
- Fehlen von administrativen Rechten
- Fehlen der Wins-Server-Einträge
- Fehler durch Software von Drittanbietern: z.B. „Intel Management & Security Status".

WEITERE ANGEBOTE

RRZN-Handbücher

- Viele gute Titel zu Office, Mailen, Bildbearbeitung, Programmieren
- Anfänger-Bücher, aber auch Spezialisten-Bücher
- Beim Operating der GWDG zum Selbstkostenpreis (~4-8 Euro) kaufen

- Verfügbare Titel unter: http://www.gwdg.de/index.php?id=619

Kurse – Termine

- 08.05.2014 - Die SharePoint-Umgebung der GWDG (Buck)
- 22.05.2014 - Einführung in das IP-Adressmanagement-System der GWDG für Netzwerkbeauftragte (Beck)
- 02.07.2014 – Einführung in Windows 8 (Buck)
- 30.07.2014 – Installation und Administration von Windows 8 (Buck)
- 09.10.2014 - Die SharePoint-Umgebung der GWDG (Buck)
- 29.09.2014 - Outlook – E-Mail und Groupware (Helmvoigt)
- 16.10.2014 - Windows-Client-Management mit Baramundi (Becker, Körmer, Quentin, Rosenfeld)
- 04.12.2014 - Die SharePoint-Umgebung der GWDG (Buck)