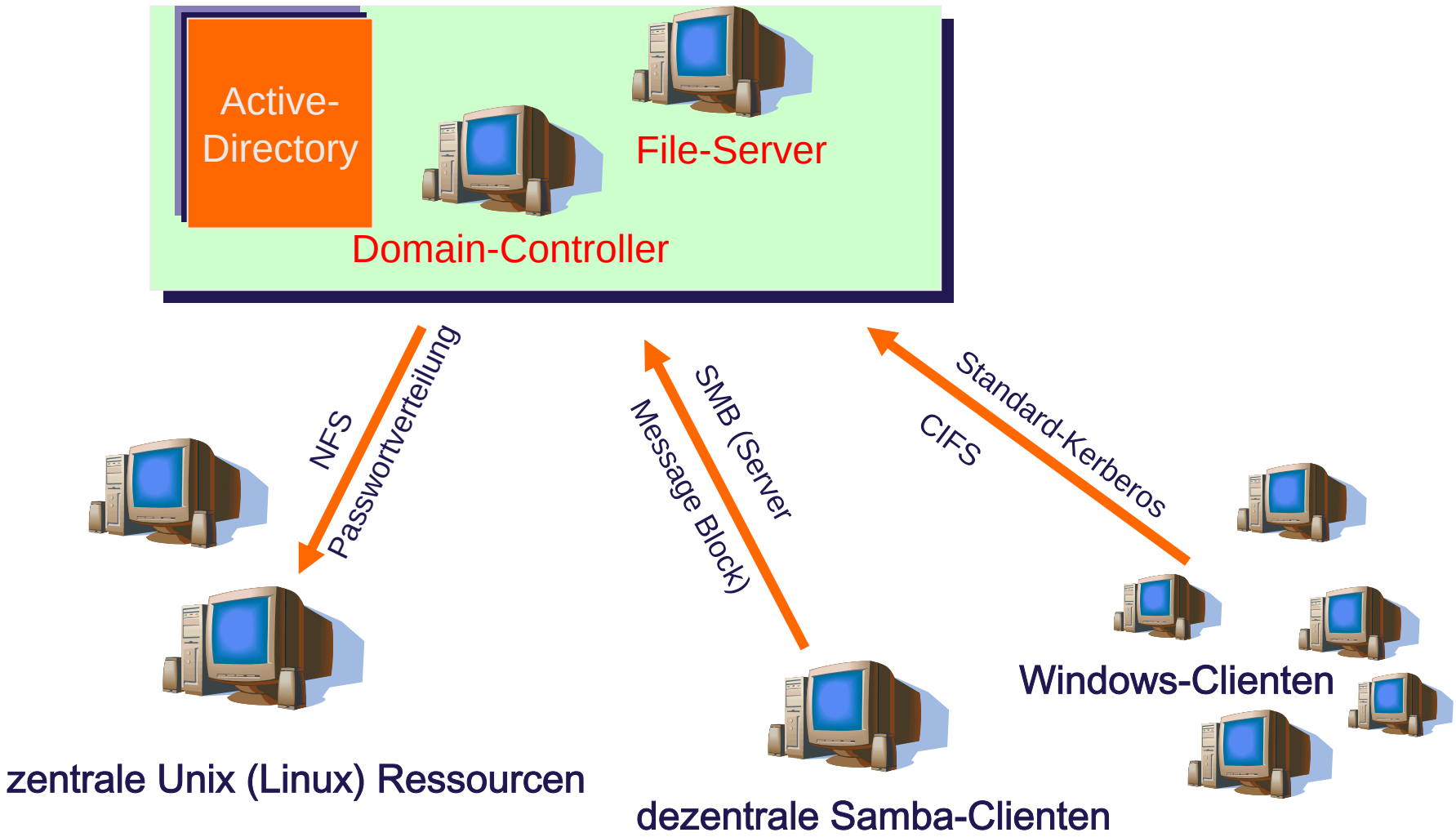
Benutzerverwaltung und Datenhaltung einmal anders: LDAP, Windows, VPP5000, Linux-Cluster, Power3+4

Forschungszentrum Karlsruhe
Frank Schmitz, Abteilung IWR
frank.schmitz@iwr.fzk.de

Globale Datenhaltung und Benutzerverwaltung



Motivation:

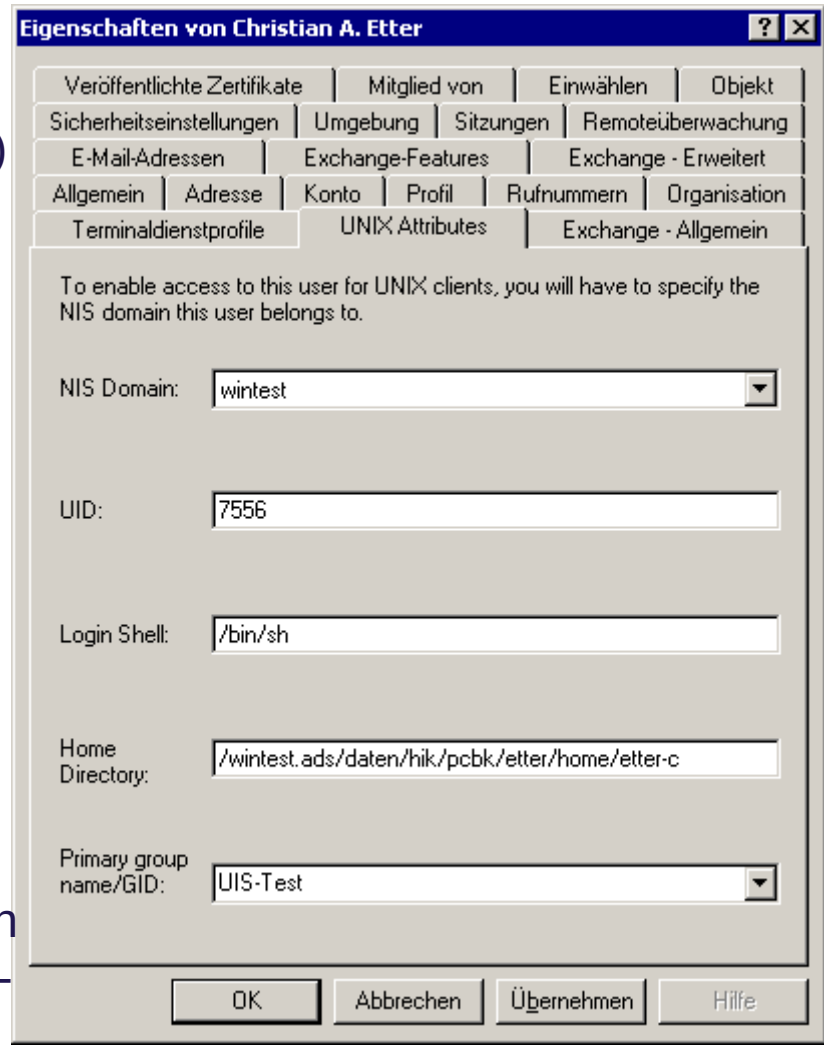
- Ablösung einer komplexen DCE/DFS Umgebung (diese war nur im AIX-Umfeld im Forschungszentrum/Universität Karlsruhe verfügbar)
- Integration aller zentralen Unix-Server (Power3/4, VPP5000, Linux-Cluster) in eine gemeinsame administrative Umgebung
- dezentralen Systeme (FZKA-Domäne, Samba-Clienten) können auf gemeinsame Daten zugreifen
- Nutzung des zentralen SAN-Umfeldes für die Datenhaltung
- zentraler Einsatz von TSM, Archivierung auch für Windows Nutzer

Randbedingungen:

- keine hohe I/O-Leistung für die zentrale Nutzung gefordert
- jedoch sollen die Daten „sicher“ sein
- Benutzerverwaltung ist zentral für die Unix und Windows Systeme zu erschlagen
- WORK-Bereiche bleiben weiterhin mit hoher I/O-Leistung verfügbar (→ GPFS und lokale Lösungen)
- kein Backup außerhalb der globalen Datenhaltung (GPFS!)
- Namensraum auf allen Rechnern gleich
- Archivierung (TSM) der globalen Daten von Unix aus

Teil 1: Benutzerverwaltung und Synchronisierung

- Optionen:
  - NIS (SFU, Gruppenzugehörigkeit)
  - ssl/ldap
  - passwd
- Basis: Services for Unix 3.0
- Erweiterung des ADS Schema
- Sicherheitserwägungen
  - keine NIS-Clients
  - Granularität (Hostsliste für NFS)
- Einschränkungen
  - Sicherheit
  - HOME auf verschiedenen Servern
  - abweichende Unix- und Windows-Namen



Komponenten:

-Active Directory:

- -Hierarchisch aufgebauter Verzeichnisdienst
- -Verwaltung von: Benutzer, Gruppen, Computer, Drucker
  Anwendungen, Netzwerkfreigaben, ...
- -Zentrale Definition von Zuständigkeitsbereichen
- -Reduktion der campusweiten Administration
- -Unterstützung des standardisierten Protokolls LDAP
- -Einbindung verschiedener Funktionalität/Komponenten
  (CMS-Benutzerverwaltung, Accounting, SFU (Services for Unix))

-Active Directory – SFU (Services for Unix):

- Speicherung von Unix-Attributen
- Abfangen von Passwort-Änderungen und Übersetzungen in crypt-hash
- Benutzerverwaltung: password-reset, UID, GID, home
- Autorisierung: restriktiv, auf Host-Ebene

Komponenten:

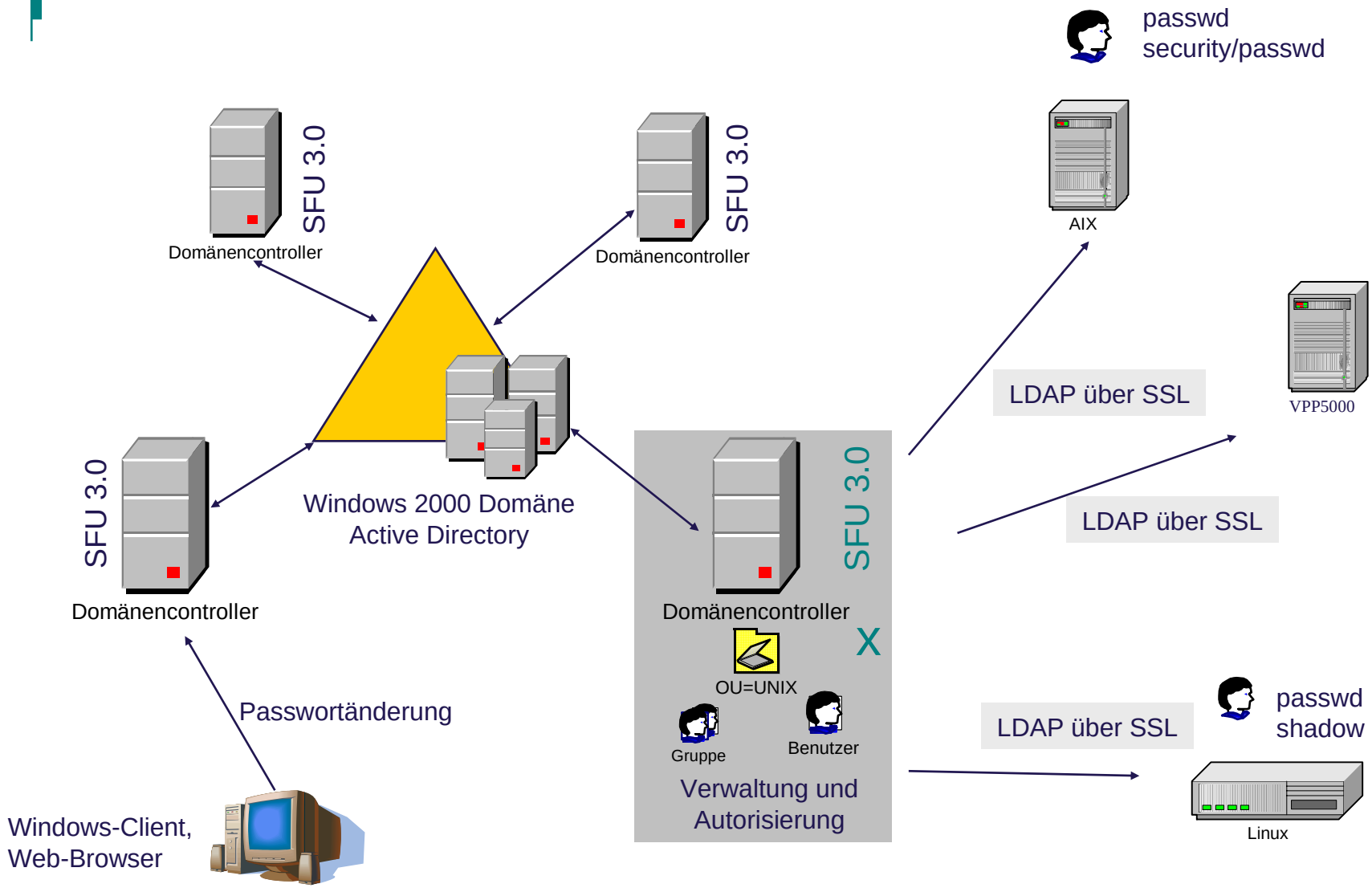
-Eigenentwicklung Windows

- Ersatz für NIS
- Bereitstellung von DLL (Anzeige Unix-Attribute, Primary Group ...)
- Aufbereiten der Daten und Bereitstellung für (scp und) ldap

-Eigenentwicklung Unix

- cron job / perlscript / shellscript
- Übertragung der Daten von ADS-DC (SSL)
- Aktualisierungen in passwd und shadow
- Vorteile: dezentral, transparent für Unix-Administrator, selektive Synchronisierung von Benutzerkonten, Verschlüsselung keine root-Previlegien an zentraler Stelle notwendig

Übersicht Benutzerverwaltung:

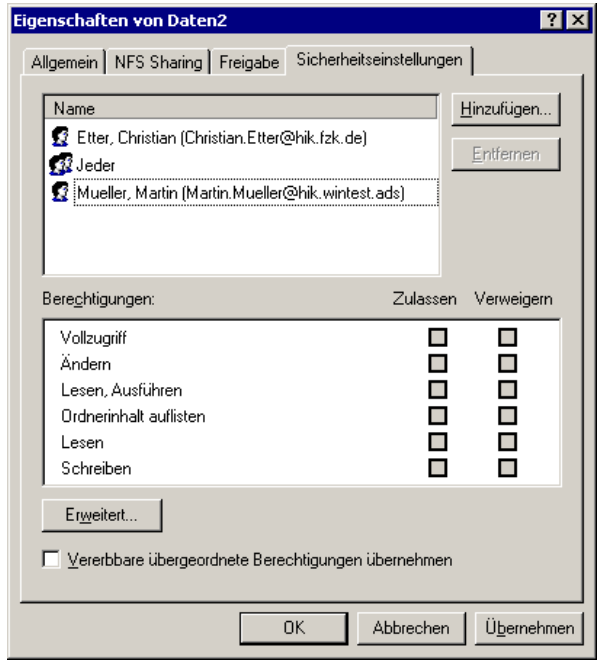


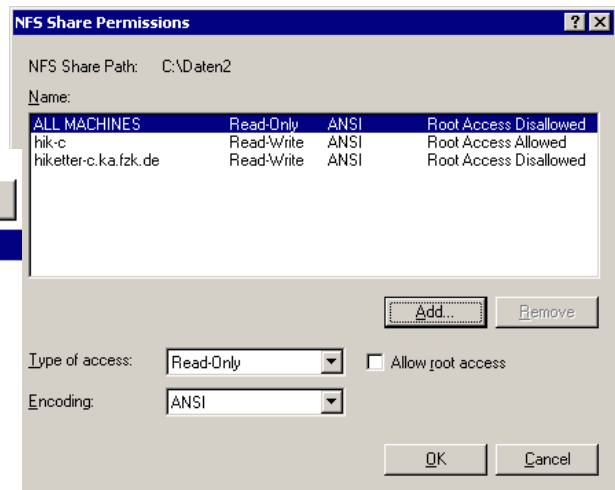
Teil 2: Globale Datenhaltung

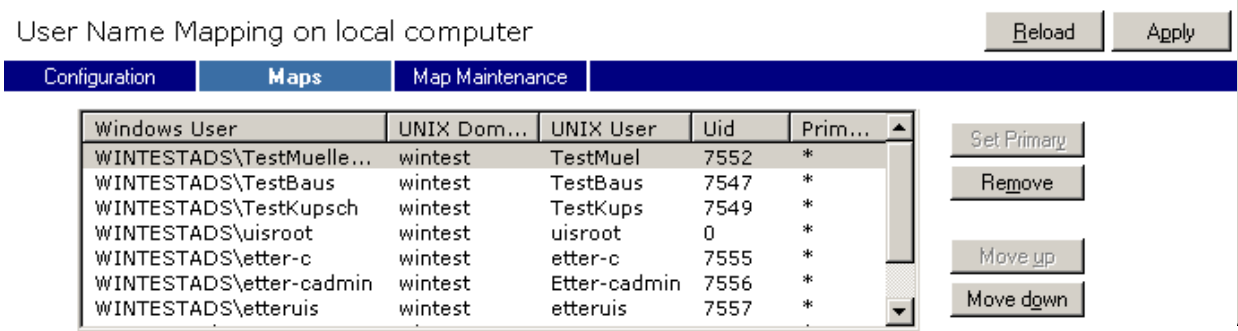
- Basis: MS Services for Unix 3 NFS
  - Verfügbar seit 05/2002
  - Migration nach SFU 3.5
- Genutzte Funktionalität: NFS-Server
  - Gute Performance (http://www.etestinglabs.com/main/reports/microsoft.asp) !
- Einsatz: Installation auf Fileserver
  - Nachteil: Keine Unterstützung von MS-DFS, d.h. Verzeichnis-baum muss Unix-seitig auf anderem Weg sichergestellt werden (Automounter)
- Voraussetzungen: Integrierte Benutzerverwaltung
  - Autorisierung von NFS-Exports mittels UID-Host-Kombination
  - Automatisches oder manuelles Mapping

Verfahren:

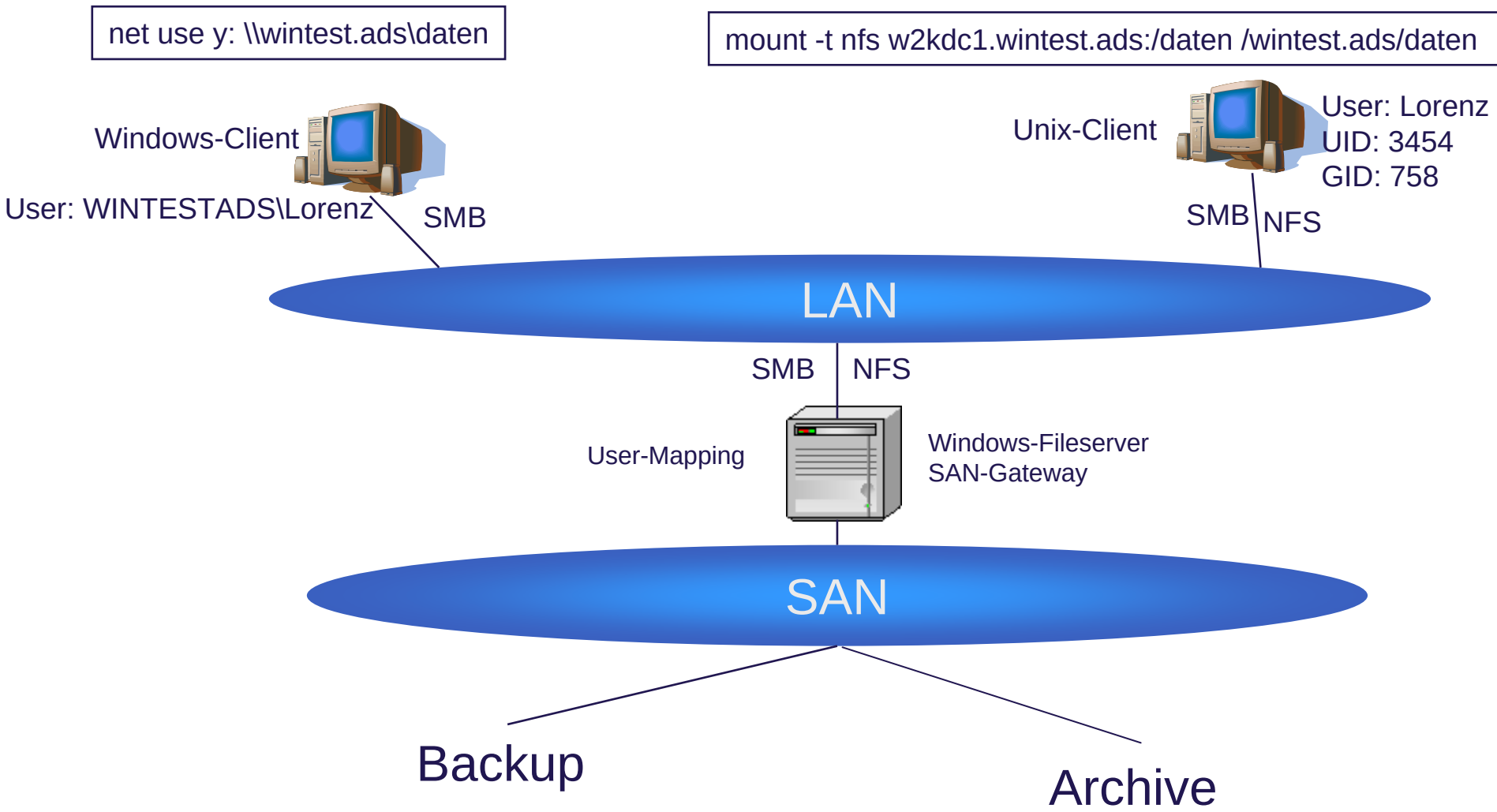
- Export analog zu Windows Freigaben
- Setzen von Berechtigungen auf NTFS-Ebene
- Explizites Mapping von Windows Benutzern oder Gruppen zu Unix-counterpart
- Impliziertes Mapping durch Zuordnung AD-Domain zu NIS-Domain







Übersicht Datenhaltung:



Was ändert sich für den Benutzer?

- Passwortänderung durch den Benutzer in Windows oder über owa2000
- Nach max. 30 Minuten ist der Zugang auf die Unix-Systeme aktiviert oder eine Passwort-änderung auf allen Systemen vollzogen
- Der Benutzer verfügt über ein lokales HOME-Vezeichnis (nur für '.'-Dateien, Quota), das globale HOME-Verzeichnis im Windows (NTFS) und einen GLOBALWORK-Bereich (GLOBALHOME, HOME=LOCALHOME, WORK, GLOBALWORK)

Performance

WRITE-Performance nach $WORK (sync)

iwraixb7 → 295 MByte/s (GFPS)

VPP5000 → 120 MByte/s (striping)

WRITE-Performance im $GLOBALHOME

15-20 MByte/s

READ-Performance im $GLOBALHOME liegt bei

20-30 MByte/s
(nur Cache-Effekt am Fileserver)

VORSICHT → Einschränkungen für Windows-Clienten

Bei Arbeiten auf einem Windows-Clienten sollten folgende Aktionen unterbleiben:

- Löschen/Kopieren von Dateien/ Verzeichnissen die nur anhand von Groß/Kleinschreibung unterschieden werden können.
- für WINDOWS (NTFS) gibt es keine Unterscheidung bei der Klein/ Großschreibung

VORSICHT

Dateinamen sollten folgende Sonderzeichen nicht enthalten:

? „ / \ < > * | :

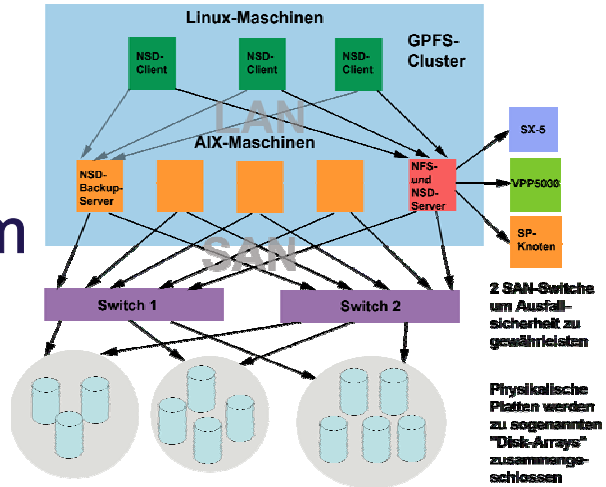
Es sollte jedoch auch darauf geachtet werden, Leerzeichen und überlange Dateinamen zu verwenden. Auch sollte man bei dem absoluten Dateibaum bei etwa 200 Zeichen aufhören. Windows kann Dateinamen mit mehr als 255 Zeichen nicht mehr anzeigen.
Weiterhin gibt es Einschränkungen bei DOS-typischen Dateiendungen (con, aux, com1, lpt1, prn)

Beispiel:

..../a/Test und ..../A/tEST sind vom Unix her angelegt. Für Windows existieren nur ....\a\tEST und ....\A\tEST mit einem Inhalt!
Jedoch führt das Löschen einer Datei nur auf der Windows-Explorer Ebene zum ‚Löschen' beider Dateien! Unix-seitig bleibt eine Datei erhalten!

AIX 2004/2005

GPFS-Filesystem im SAN für AIX, Linux (NFS), UXP/V (NFS) bestehend aus einem über 700 m gespiegelten Filesystem auf zwei FastT500, zwei FastT700 für WORK



drei Power4-Systeme mit 4 Prozessoren (p630) und vier 8-Prozessor Power4-Rechner (p655) mit jeweils 64 GByte Hauptspeicher

64 Prozessoren Power3 werden im Sommer 2005 stillgelegt,
256 Prozessoren Power3 im Virtuellen Rechenzentrum stehen noch zur Verfügung (nicht GBV und GBH)

Vektorrechner 2004/2005

VPP5000 mit 8 Prozessoren,
80 GByte Hauptspeicher,
764 GByte RAID
WORK-Bereich
VPP5000 mit 4 Prozessoren,
30 GByte Hauptspeicher,
517 GByte RAID
WORK-Bereich

NEC SX-5 mit 8 Prozessoren und SX-6i im Projekt CampusGrid (www.CampusGrid.de) ließen sich auch integrieren

Linux-Cluster 2004/2005

32 Prozessoren Intel PIII 700 Mhz
auf 16 Doppelprozessorboards (hpc*L*ine),
16 GByte Hauptspeicher, 2 x Fast-Ethernet,
für Ausbildungszwecke

32 Prozessoren Athlon 1800+ und besser mit 1533-1991 Mhz auf 16 Doppelprozessor-boards, 38 GByte Hauptspeicher, Gbit-Ethernet für die interne Kommunikation

Opteron InfiniBand-Cluster V20z ließe sich auch integrieren ➔ CampusGrid