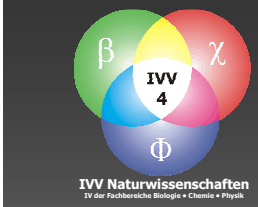


Westfälische
Wilhelms-Universität
Münster

AD als Benutzerdatenbank für heterogene DV-Systeme

Am Beispiel der Einbindung von Linux-Rechnern in die Benutzer- und Ressourcenverwaltung eines Active Directory

Herbsttreffen 2004
Böblingen

15-NOV-2004

Heinz-Hermann Adam
(adamh@nwz.uni-muenster.de)

1

Agenda

- Einführung
- Linux-Authentifizierung
  - Pluggable Authentication Modules
  - Name Service Switch
- Active Directory
  - Schemaerweiterung
- Installation und Konfiguration
  - NSS- und PAM-Module
  - SaMBa-Client-Tools
- Zusammenfassung

2

Was ist die IVV Naturwissenschaften?

- Teil des dezentralen IV-Systems der Universität Münster
- Zusammenschluß der naturwissenschaftlichen Fachbereiche
- Ziel: Gemeinsame Befriedigung des Bedarfs an fachspezifischen IV-Mitteln (Hardware, Software, Dienste)
  - Selbsthilfeorganisation
  - Nutzung von Synergieeffekten
- Kein "Rechenzentrum"
- Active Directory Domäne & OpenVMS-Cluster
  - ca. 20 Server
  - über 1.100 Arbeitsplätze
  - über 5.000 Benutzer
- Betriebssysteme
  - Linux
  - Mac OS
  - OpenVMS
  - Tru64 UNIX, u.a.
  - Windows
- Anwendungssoftware
  - Windows > 150 Produkte
  - Mac > 30 Produkte

3

Integration weiterer Betriebssysteme

- Einheitlicher Zugang (Single sign-on) auf:
  - Windows
  - OpenVMS (Pathworks + EXTAUTH)
  - Tru64 UNIX (SSO, LDAP, Kerberos)
  - Linux (PAM, NSS, LDAP, Kerberos)
  - Mac OS X (Netinfo, LDAP, SSL, Kerberos)
  - Who's next?
- Nutzung zentraler Ressourcen auch durch diese Systeme

4

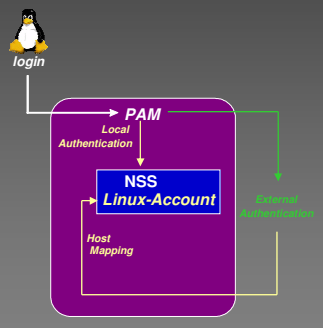
Ressourcen für Nicht-Windows-Clients

- Server Message Block/Common Internet File System-Shares werden von Windows und Pathworks bereitgestellt
- Clients hierfür sind auf den anderen Plattformen vorhanden
  - Tru64 Unix: Samba, Sharity
  - Linux: Samba, Sharity
  - Mac OS: Samba, Dave
- Zusätzlich sind auf Windows Server die Services for Macintosh (SFM) verfügbar

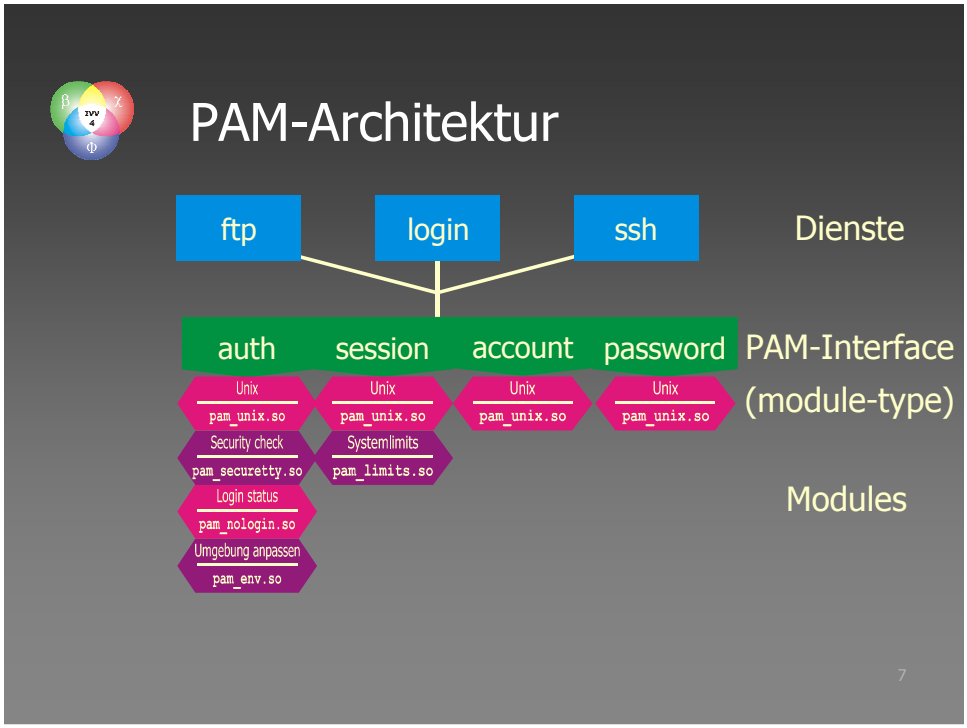
5

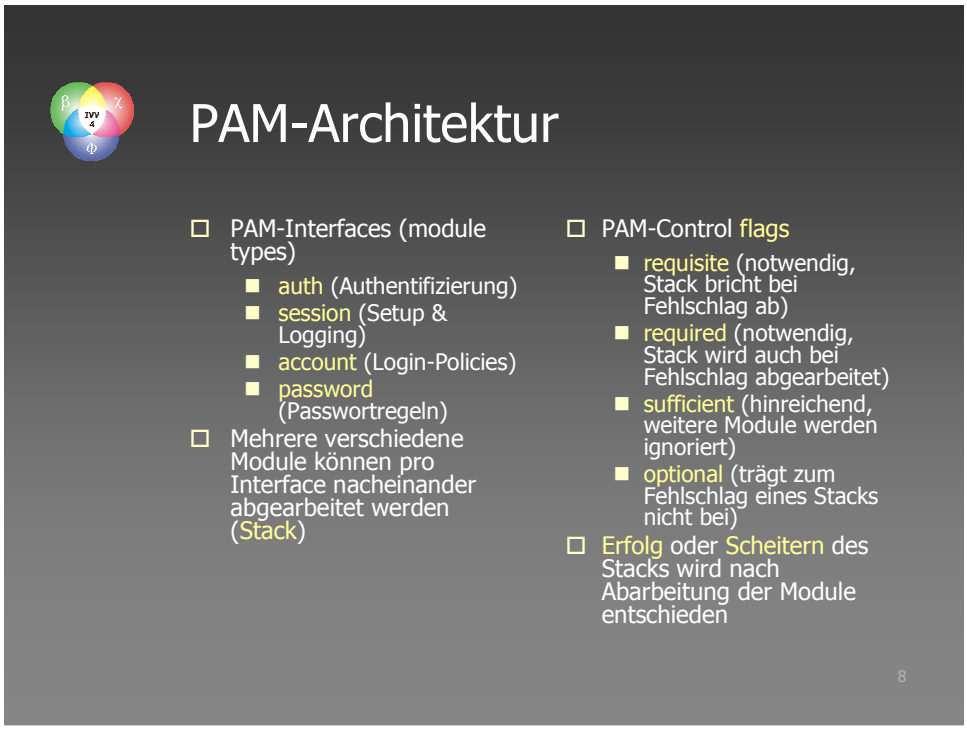
Linux-Authentifizierung

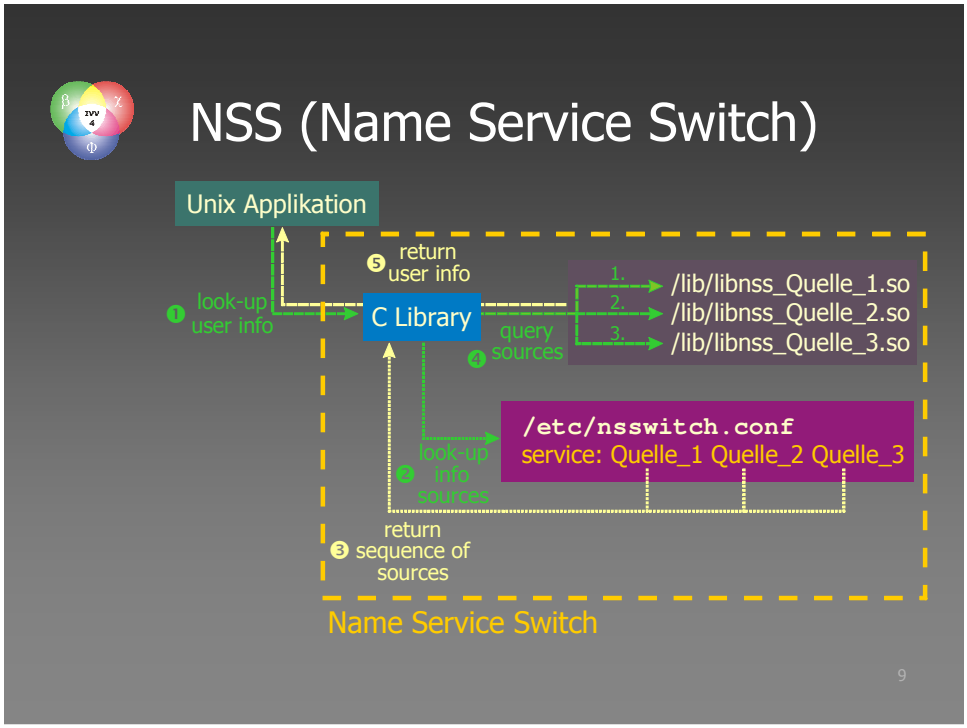
- Verwendet Pluggable Authentication Modules
  - Gegen interne und externe Quellen (flat files, NIS, Kerberos …)
- Benutzer-Informationen per Name Service Switch
  - ebenfalls aus internen wie externen Quellen
- Unix spezifische Informationen

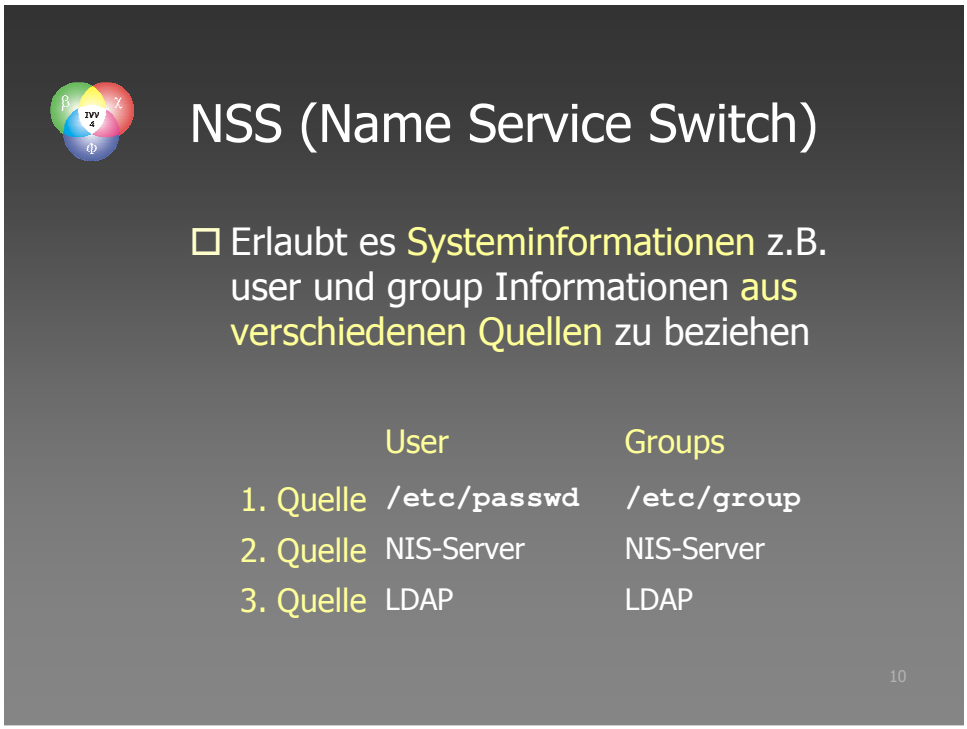


6


PAM-Architektur
ftp
login
ssh
Dienste
auth
session
account
password
PAM-Interface
(module-type)
Unix
pam_unix.so
Unix
pam_unix.so
Unix
pam_unix.so
Unix
pam_unix.so
Security check
pam_securetty.so
Systemlimits
pam_limits.so
Login status
pam_nologin.so
Umgebung anpassen
pam_env.so
Modules
7


PAM-Architektur
PAM-Interfaces (module types)
auth (Authentifizierung)
session (Setup & Logging)
account (Login-Policies)
password (Passwortregeln)
Mehrere verschiedene Module können pro Interface nacheinander abgearbeitet werden (Stack)
PAM-Control flags
requisite (notwendig, Stack bricht bei Fehlschlag ab)
required (notwendig, Stack wird auch bei Fehlschlag abgearbeitet)
sufficient (hinreichend, weitere Module werden ignoriert)
optional (trägt zum Fehlschlag eines Stacks nicht bei)
Erfolg oder Scheitern des Stacks wird nach Abarbeitung der Module entschieden
8


NSS (Name Service Switch)
Unix Applikation
return
user info
look-up
user info
C Library
query
sources
1.
2.
3.
/lib/libnss_Quelle_1.so
/lib/libnss_Quelle_2.so
/lib/libnss_Quelle_3.so
/etc/nsswitch.conf
service: Quelle_1 Quelle_2 Quelle_3
look-up
info
sources
return
sequence of
sources
Name Service Switch
9


NSS (Name Service Switch)
Erlaubt es Systeminformationen z.B. user und group Informationen aus verschiedenen Quellen zu beziehen
User
Groups
1. Quelle
/etc/passwd
/etc/group
2. Quelle
NIS-Server
NIS-Server
3. Quelle
LDAP
LDAP
10

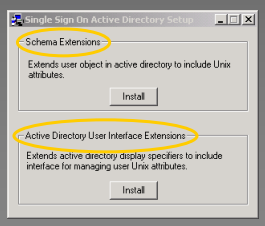
Active Directory

- X.500-basierter Verzeichnisdienst
  - Erweiterbares Schema, d.h. Objekt kann um beliebige Attribute erweitert werden oder neue Objekte können kreiert werden
  - Zugriff über Light-weight Directory Access Protocol (plattformunabhängig)
  - Authentifizierung über Kerberos (plattformunabhängig)

11

Schemaerweiterung - Unix

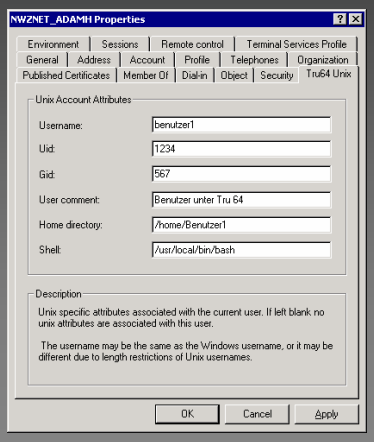
- Tru64 UNIX V5 Associated Products Volume 2 Windows2000_SSO\windows_kit\setup.exe
  - Erweitert das Schema basierend auf Microsoft Services for Unix (msSFU)
  - Erweitert das Active Directory Users and Computer Interface (nur SSO 2.0, ab T64 V5.1A)



12

Schemaerweiterung – Unix user

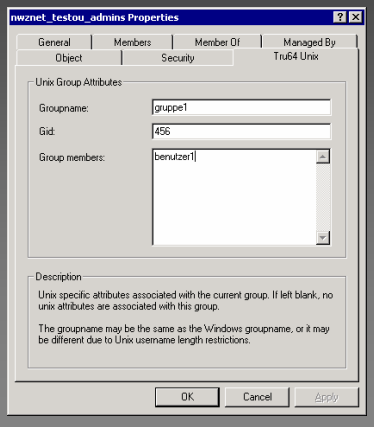
- Benutzeraccount
  - gecos : User comment
  - gidNumber : Gid
  - loginShell : Shell
  - msSFUHomeDirectory : Home directory
  - uid : Username
  - uidNumber : Uid



14

Schemaerweiterung – Unix groups

- Benutzergruppe
  - gidNumber : Gid
  - memberUID : Group members
    - nur für ältere nss_ldap-Versionen
  - msSFUName : Groupname



16

Implementation

- Name Service (passwd, group)
  - LDAP V3 mit SSL-Verschlüsselung
- Authentifizierung
  - Kerberos V5
- Homedirectories
  - SaMBa-Client Tools

17

Installation zusätzlicher Pakete

- Authentifizierung
  - pam_krb5 (SuSE 9.1 included)
- Name Service
  - nss_ldap (SuSE 9.1 included)
- Einbindung von Ressourcen
  - pam_mount (SuSE 9.1 included)
- Korn Shell
  - pdksh (SuSE 9.1 included)

18

NSS Konfiguration

- In **`/etc/nsswitch.conf`** wird die Liste der Name Service Quellen definiert
  - LDAP
    - SuSE
      - `passwd: compat ldap`
      - `groups: compat ldap`

19

LDAP Konfiguration

- In **`/etc/ldap.conf`** wird die LDAP Anbindung konfiguriert

```
host DC1 DC2 DC3
ssl on
base dc=child,dc=root,dc=tld
binddn cn=ldap,cn=users,
  dc=child,dc=root,dc=tld
bindpw
[...]
scope sub
pam_filter objectclass=user
pam_login_attribute sAMAccountName
pam_password ad
```

20

LDAP Konfiguration

- Konfiguration (fortgesetzt)

```
nss_base_passwd dc=child,dc=root,dc=tld?sub
nss_base_shadow dc=child,dc=root,dc=tld?sub
nss_map_objectclass posixAccount User
nss_map_objectclass shadowAccount User
nss_map_attribute uid sAMAccountName
nss_map_attribute uniqueMember member
nss_map_attribute homeDirectory
  msSFUHomeDirectory
nss_map_objectclass posixGroup Group
nss_map_attribute cn sAMAccountName
```

21

LDAP Proxy-Benutzer im Windows

- Benötigt Rechte im Active Directory
  - Alle Attribute lesen
    - Benutzer
    - Gruppen
- Kann durch entsprechende Beschränkungen abgesichert werden
  - Smart Card erforderlich für Anmeldung
- Pro Linux-Rechner ein Account zweckmäßig
  - Denial-of-Service attacken
  - Verwendung von sicheren Passworten

22

LDAP Anbindung überprüfen

- `# getent passwd` muss zusätzlich zu den lokalen auch Benutzer aus dem Active Directory liefern:

```
root:x:0:0:root:/root:/bin/bash
[...]
ntp:x:74:65534:NTP
  daemon:/var/lib/ntp:/bin/false
[...]
user1:x:123456:123:Benutzer Nummer Eins
  :/home/user1:/bin/bash
user2:x:123457:456:Benutzer Nummer Zwei
  :/home/user2:/bin/ksh
user3:x:1234:890:Benutzer Nummer Drei
  :/home/user3:/bin/bash
[...]
```

23

PAM Konfiguration

- Standard-Linux
  - Für jeden Dienst befindet sich in `/etc/pam.d` eine Konfigurationsdatei mit dessen Namen, deren Inhalt bestimmt wie eine Authentifizierung durchgeführt wird.
  - `# ls /etc/pam.d`
    `su rlogin other xdm ssh login...`

24

PAM Konfiguration

- SuSE
  - Alle Dienste können an einer Stelle konfiguriert werden.
  - Generisches PAM **pam_unix2.so** in jedem Stack, das verschiedene Authentifizierungsdienste benutzen kann (**/etc/passwd**, NIS, LDAP, Kerberos)
  - Wird über **/etc/security/pam_unix2.conf** konfiguriert
    - Kerberos V5:
      - `auth:  use_krb5 nullok`
      - `account:  use_krb5`
      - `password:  use_krb5 nullok`
      - `session:  none`

25

Kerberos Konfiguration

- In **/etc/krb5.conf** wird die Kerberos-Anbindung konfiguriert

```
[libdefaults]
  default_realm = CHILD.ROOT.TLD
  default_tgs_enctypes = des3-hmac-sha1 des-cbc-crc
  default_tkt_enctypes = des3-hmac-sha1 des-cbc-crc
  dns_lookup_kdc = true
  clockskew = 300
[realms]
  CHILD1.ROOT.TLD = {
   kdc = DC1.child.root.tld
   default_domain = child.root.tld
   kpasswd_server = DC1.child.root.tld
  }
[domain_realm]
  .child.root.tld = CHILD.ROOT.TLD
```

- Zeitsynchronisation per NTP aktivieren

26

Homedirectories via SaMBa

- Müssen beim Login verfügbar sein
  - pam_mount Modul
- Für jeden Benutzer ein eigener Mount
  - Session-Security im SMB/CIFS

27

SMB Client-Konfiguration

- In **`/etc/samba/smb.conf`** wird SaMBa konfiguriert
  - Konfiguration

```
[global]
   workgroup = CHILD
   os level = 0
   time server = No
   unix extensions = Yes
   encrypt passwords = yes
   map to guest = Bad User
   […]
   wins support = No
   […]
   security = DOMAIN
```

28

Pam_mount Konfiguration

- In **/etc/security/pam_mount.conf** wird das automatische Mounten beim Login konfiguriert
  - Konfiguration

```
debug 0
mkmountpoint 1
[…]
volume * smb fileserver & ~
 uid=&,gid=&,dmask=0700,fmask=0700
 ,workgroup=CHILD - -
```

29

Pam_mount Konfiguration

- Einbauen des pam_mount.so in den PAM-Stack, z.B. **/etc/pam.d/sshd**

```
#%PAM-1.0
auth     required   pam_unix2.so # set_secrpc
auth     required   pam_nologin.so
auth     required   pam_env.so
auth     optional   pam_mount.so   use_first_pass
[…]
session required    pam_unix2.so   none # trace
  or debug
session required    pam_limits.so
session optional    pam_mount.so
[…]
```

30

Homedirectories via SaMBa

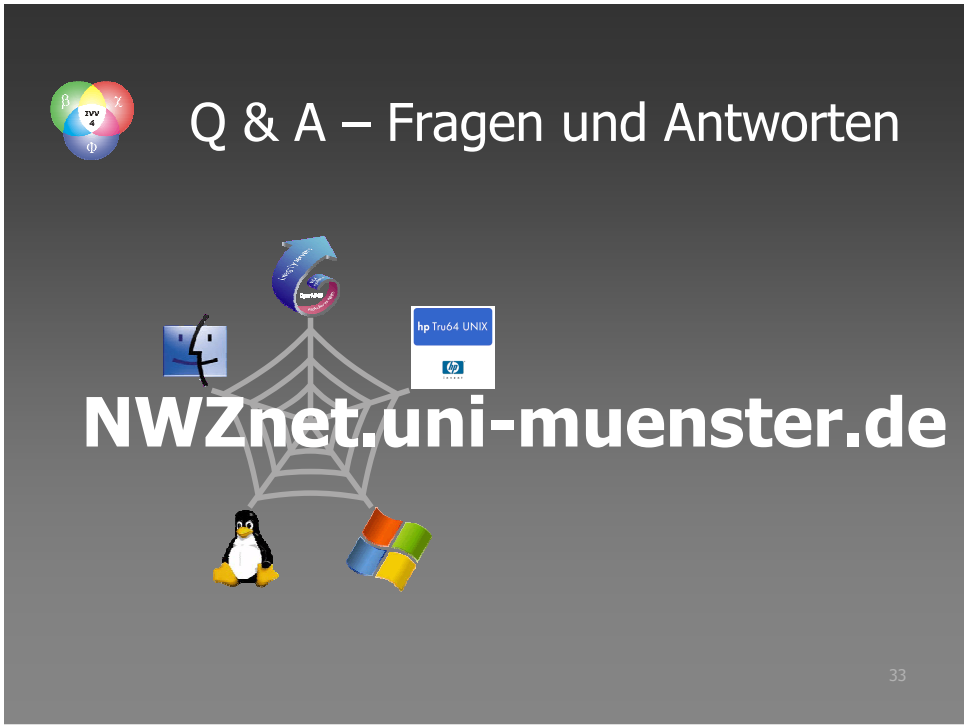
- Beschränkungen
  - Unterstützt keine „hohen UIDs“
    - gepatchter Kernel nötig
  - Unterstützt kein Windows Dfs
    - neue Shares, 1 für jeden Benutzer
  - Unterstützt keine Special Files, z.B. Sockets
    - für KDE-Sessions unbrauchbar
    - KDE-Special Files nach /tmp umbiegen

31

Zusammenfassung

- Integration von Nicht-Windows Betriebssystemen in Active Directory, am Beispiel von Linux
  - Statusbericht, noch nicht alle Fragen sind gelöst
- Einführung in die verwendeten Konzepte
  - Linux
  - Windows 2000 Active Directory
- Einbindung einer SuSE Linux 9.1 Workstation in AD
  - Name Service
    - LDAP
  - Authentifizierung
    - Kerberos
  - Homedirectories
    - SMB/CIFS + pam_mount
- Offene Fragen und Probleme

32


Q & A – Fragen und Antworten
hp Tru64 UNIX
NWZnet.uni-muenster.de
33