Windows-Linux
Kooperation

Thorsten Butz

www.thorsten-butz.de

Kontakt:

post@thorsten-butz.de

http://www.thorsten-butz.de/public/thorstenbutz.vcf

Agenda

Teil 1: Linux@Hyper-V

Teil 2: Subsystem for UNIX-based Applications (SUA), NFS-Server/Client

Teil 3: Windows/Linux SSO: Active Directory-Authentifizierung für Linux-Clients

Die Laborumgebung

Alle Beispiele in dieser Präsentation beziehen sich auf das folgende Setup:

sea-srv-01 (WS 2008, EN, x86-32)
DC für "contoso.com", DNS, IPv4: 10.0.0.150

nue-srv-01 (SLES 10, SP2, EN, x86-64)
Memberserver, IPv4: 10.0.0.151

rdu-srv-01 (CentOS 5.3)
Memberserver, IPv4: 10.0.0.152

Die Memberserver beziehen die Systemzeit mittels NTP von "sea-srv-01".

Teil 1: Linux@Hyper-V

- Unterstützte Linuxdistribution(en):
  - SUSE Linux Enterprise Server 10
    mit Service Pack 1 oder 2
    x86-32 oder x86-x64 Edition
- Voraussetzungen
  - XEN-Kernel
  - GCC plus "kernel-source"
  - Microsofts "Linux Integration Components" (LIC), Version 1

LIC Version 1 und 2 (Beta) sind verfügbar über

https://connect.microsoft.com

(Anmeldung erforderlich) oder über das MS Download Center (nur LIC Version 1): Linux Integration Components for Windows Server 2008 Hyper-V

http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=ab7f4983-93c5-4a70-8c79-0642f0d59ec2

Das LICv1-Paket enthält eine detaillierte Anleitung:

Linux ICs for Hyper-V.rtf

Einschränkungen

- 1 virtuelle CPU
- Kein Heartbeat
- Keine Zeitsynchronisation durch Hyper-V
- Herunterfahren "von außen" nicht möglich
- Mausintegration nur durch Citrix Satori-Projekt
- ALT-GR-Taste bei deutscher Tastaturbelegung u. U. funktionslos: KB 963709

Offizielle Liste zu den unterstützten OS:

http://www.microsoft.com/windowsserver2008/en/us/hyperv-supported-guest-os.aspx

Citrix Satori:

http://www.xen.org/download/satori.html

Citrix Blogeintrag zur Satori-Maus:

http://community.citrix.com/blogs/citrite/simoncr/2009/03/24/The+Tale+of+an+Enlightened+Mouse%3bjsessionid=F21824A5555A48ACC453F8D2FF226D46

KB 963709

"The AltGr key does not work on a Linux virtual machine on a Windows Server 2008-based server that has the Hyper-V role enabled"

http://support.microsoft.com/kb/963709/

Es reicht u. U. bereits diesen Registry-Schlüssel zu setzen:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Virtualization\Worker

"KeyboardWorkaroundEnabled" = 1

LIC und der Problemfall XEN

- LIC v2 BETA für Hyper-V R2 seit März 2009 verfügbar
- LIC v1 und v2 unterstützen keinen Kernel jenseits Version 2.6.18
- Linuxdistributionen und ihre Kernel
  - Ubuntu 8.04-2 LTS: KRNL 2.6.24
  - CentOS 5.3: KRNL 2.6.18
  - SLES 10, SP2: KRNL 2.6.16
  - SLES 11: KRNL 2.6.27

Neu in den LICv2:

Wegfall des "x2v-Shim", kein sogenannter "Hypercall-Adapter" mehr. Es ist nicht mehr notwendig, mittels eines speziellen Eintrags im Bootloadermenu (/boot/grub/menu.lst) einen XEN-Kernel zu starten.

Problemfall XEN:

Seit Anfang 2005 wird die Aufnahme von XEN in den offiziellen Linuxkernel in Aussicht gestellt, jedoch immer wieder kontrovers diskutiert. Die Linux-Entwickler bemängel(te)n die "Qualität des Quellcodes" von XEN.

In der Zwischenzeit etablierte sich eine "**paravirt_ops**" genannte Abstrak-tionsschicht, die seit Version 2.6.20 in den Hauptentwicklungszweig des Linuxkernels integriert ist.

Die XEN-Entwickler arbeite(te)n an Xen-Patches mit "sauberem Code", die diese neue Schnittstelle verstärkt nutzen. Seit Version 2.6.23 lassen sich Gastsysteme auf Basis dieser neueren Patches auf modernen XEN-Versionen virtualisieren.

Parallel zu dieser Entwicklung erfreut sich in der Linuxgemeinde **KVM** ständig wachsender Beliebtheit, eine alternative Virtualisierungslösung, die den Linuxkernel selbst zum Hypervisor macht, jedoch auf Intel-VT/AMD-V-CPUs angewiesen ist (im Gegensatz zu XEN).

Zum Weiterlesen:

Kernel-Log: Morton stellt Aufnahme des Xen-Dom0-Codes in Frage; Dateisysteme für SSDs (Thorsten Leemhuis)

http://www.heise.de/open/Kernel-Log-Morton-stellt-Aufnahme-des-Xen-Dom0-Codes-in-Frage-Dateisysteme-fuer-SSDs--/artikel/134016

"Enlightening" CentOS

- Benötigte Pakete:
  gcc, kernel-devel, make, gnupg;
  für Satori: xorg-x11-server-sdk

  Beispiel:

```
yum --disablerepo=\* --enablerepo=c5-media  Ã
install gcc kernel-devel
```

- LIC installieren:

```
<lic-v2>/setup.pl drivers
```

21.06.2009 www.thorsten-butz.de 6

Das Vorgehen im Detail:

`mkdir /media/CentOS`

`mount /dev/hdc /media/CentOS`

`..` montiert das IDE-DVDRom "hdc" nach /media /CentOS
("mount" zeigt die aktuell eingebunden Laufwerke)

`yum --disablerepo=\* --enablerepo=c5-media install gcc kernel-devel`
(Falls nötig make, gnupg etc. in gleicher Weise installieren)

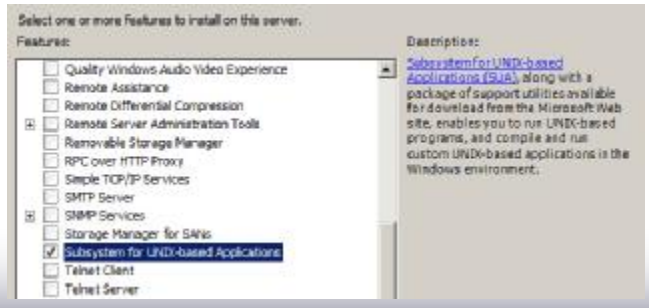
Vorausgesetzt die LICv2-CD ist als "media/CDROM" eingebunden:
`mkdir /root/lic-v2`
`cp /media/CDROM /root/lic-v2`
`/root/lic-v2/setup.pl drivers`

Es entstehen unmittelbar neue Geräte, zum Beispiel
`/dev/seth` oder `/dev/sda`

Siehe auch:
Linux ICs v2 Beta for Hyper-V - Read Me.pdf
(Bestandteil des LICv2-Pakets)

Teil 2: Subsystem for UNIX-based Applications (SUA)

- Interix Subsystem
- Nachfolger der SFU 3.5
- Native UNIX/POSIX-Funktionalität, Keine Emulation
- Kein X-Server enthalten



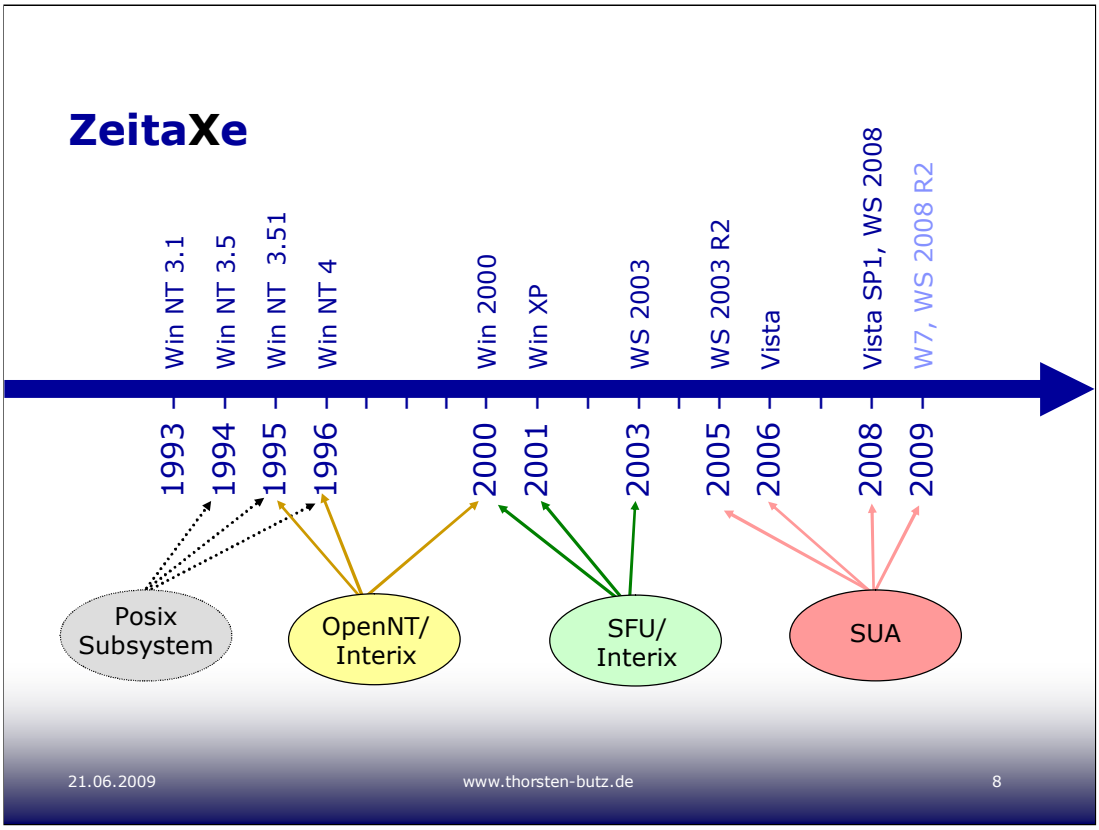
Zum Weiterlesen:

"Subsystem for UNIX-based Applications and POSIX Compliance" (MS Technet)

http://technet.microsoft.com/en-us/library/cc754351.aspx

InterOp: Windows Services For UNIX (Charlie Russel), TechnetMag US, Spring 2005

http://technet.microsoft.com/en-us/magazine/2005.05.interop.aspx



Vorgeschichte

1994 führt Microsoft in Windows NT 3.5 das erste Posix-Subsystem ein (erste Ansätze von Posix-Konformität waren gemäß Wikipedia auch schon in der vorherigen Veröffentlichung von Windows NT vorhanden). Vorangig diente dies wohl dazu, dass Aufträge der US-Regierung und des US-Militärs einfacher oder überhaupt nur zu erhalten waren, wenn das Betriebssystem "posix compliant" war.

OpenNT, später Interix: Versionen 1.0 – 2.2

Ursprünglich entwickelt von "Softway Systems" für Windows NT 3.51,

1999 übernahm MS die Firma

Services for Unix (SFU): Interix 3.0 to 3.5

Eigenständiges Softwarepaket für Win2000, WinXP und WS 2003

SUA in WS 2003 R2: Interix 5.2

SUA in WS 2008/Vista: Interix 6.0

SUA in WS 2008R2/W7: Interix 6.1

Zum Weiterlesen/Weiterschauen:

http://www.computerwoche.de/heftarchiv/1999/38/1088842/

http://www.interopsystems.com/SUAfamiliarization-02.wmv

http://en.wikipedia.org/wiki/Windows_nt

Verzeichnisse

- %SUA_ROOT_WIN%
  c:\Windows\SUA = /
- %SystemDrive%
  c:\ = **/dev/fs/C**
- \\sea-srv-01\sales =
  /net/sea-srv-01/sales

Das **Win32-** und das **Posix-Subsystem** unterscheiden auf sehr unterschiedliche Weise die Groß-/Kleinschreibung, was leider in folgendem Fall zu schweren Inkompatibiläten führt.

Das Win32-Subsystem arbeitet "case-preserving", speichert die gewählte Schreibweise zwar, unterscheidet dann aber nicht mehr. So ist es zum Bsp. mit "notepad.exe" nicht möglich zwei Dateien "Brief.txt" und "brief.txt" im selben Verzeichnis zu erzeugen.

Das Posix-Subsystem arbeitet dagegen streng "case-sensitive".

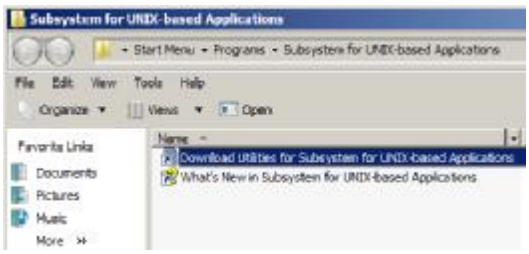
Zur Demonstration:

Erstellen Sie ein Verzeichnis (**mkdir c:\sales**), erstellen Sie dort mit "notepad.exe" eine Datei "**Brief.txt**" (großer Anfangsbuchstabe) und eine Datei "**brief.txt**" (kleine Buchstaben) mit "vi" (vi ist ein Texteditor, den Sie über eine SUA-Shell wie die CShell starten müssen). Füllen sie die Dateien mit Text, so dass die Inhalte zu unterscheiden sind.

```
cd /dev/fs/C/sales/
ln Brief.txt gross.txt          [erstellt einen Hardlink]
ln brief.txt klein.txt          [SYNTAX: ln <BestehendeDatei> <NeuerLink>]
                                [Win32 und Interix eindeutig unterscheiden]

ln -s Brief.txt Gross_sym.txt   [erstellt einen Symlink]
ln -s brief.txt klein_sym.txt   [Dateien können von Win32 nicht verarbeitet
                                 werden.]

Alternative "mklink", SYNTAX:
mklink /H <NeuerLink> <BestehendeDatei>     [erstellt einen Hardlink]
mklink <NeuerLink> <BestehendeDatei>        [erstellt einen Symlink]
```

Installation in 3 Schritten

1. `servermanagercmd –i Subsystem-UNIX-Apps`
2. Download/Installation "Utilities and SDK" (Microsoft)
3. Download/Installation "SUA Community Toolkit" (Interop Systems)



Zu 2.

Utilities and SDK for Subsystem for UNIX-based Applications in Microsoft Windows Vista RTM/Windows Vista SP1 and Windows Server 2008 RTM

http://go.microsoft.com/fwlink/?LinkId=59121

~ 480 MB

Zu 3.

Verschiedene Toolkits stehen zur Auswahl unter

http://www.suacommunity.com/

U. a. das "Complete Toolset" (~ 190 MB):

ftp://warehousepage:XcR2kioV@ftp.interopsystems.com/pkgs/bundles/pkg-current-bundlecomplete60.exe

Populäre Anwendungen: SSH

- Installation: `pkg_update -L openssh`
  Start/Stop: `/etc/init.d/sshd start|stop`
  (SSHD startet nach der Installation automatisch)
- Benutzer anlegen, Heimverzeichnis festlegen:
  `net user thorsten /HOMEDIR:c:\users\thorsten /DOMAIN`
- Shell definieren:
  `chsh -u thorsten /usr/local/bin/bash`

Das SSH-Howto im Detail

Die nachfolgenden Beispiele erzeugen einen Beispiel-Benutzer, legen das Heimverzeichnis und die Standardshell fest. "**net**" ist eine Windows-Anwendung, "**chsh**" und "**finger**" müssen aus einer Unix-Shell heraus ausgeführt werden.

Lokalen Benutzer erzeugen (Beispiel):

```
net user /add anton
net user thorsten /HOMEDIR:c:\users\thorsten
```

Domänen-Benutzer erzeugen:

```
net user /add anton /domain
net user thorsten /HOMEDIR:c:\users\thorsten /DOMAIN
```

oder

```
net user thorsten /HOMEDIR:\\sea-srv-01\users$\thorsten /DOMAIN
```

In der Unix-Shell:

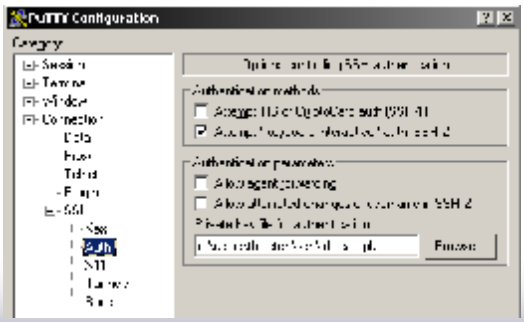
```
chsh -u thorsten /usr/local/bin/bash
finger -l thorsten
```

Zertifikatsbasiertes Login

- `ssh-keygen -t rsa`
- `mv id_rsa.pub ~/.ssh/authorized_keys`
- id_rsa auf den SSH-Client kopieren
- Ggf. "id_rsa" mit PuTTYGen konvertieren in "id_rsa.ppk"
- Zugriffsrechte beachten!

id_rsa = Private Key

id_rsa.pub = Public Key



21.06.2009 www.thorsten-butz.de 12

Die Zugriffsrechte des Benutzerprofils anpassen:

Der **SSHD** erwartet eine sichere Konfiguration der Zugriffsrechte im Heimverzeichnis der Benutzer. Leider decken sich die "Vorstellungen" des SSHD so gar nicht, mit den Standardberechtigungen eines Windowsprofils.

Windows erzeugt Benutzerprofile, deren Besitzer nicht das entsprechende Benutzerkonto ist (siehe **Abbildung rechts**).

Der SSHD erwartet jedoch, dass genau dies der Fall ist: der Benutzer muss Besitzer seines Heimverzeichnis sowie des Verzeichnis ".ssh" und der Datei "authorized_keys" sein.

Soll ein Benutzer sich mittels Zertifikat anmelden können, so sind folgende Anpassungen durchzuführen. Es empfiehlt sich, diese Änderungen mittels Unix-Shell vorzunehmen.

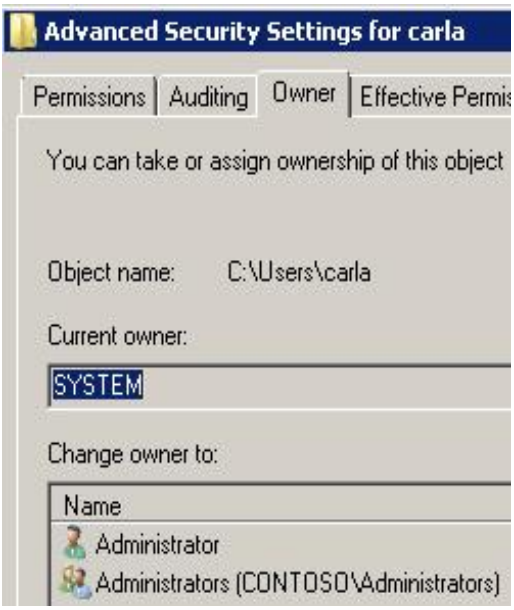
Zugriffsrechte setzen:

a) als Administrator

```
chown <benutzername> /dev/fs/C/Users/<benutzername>
```

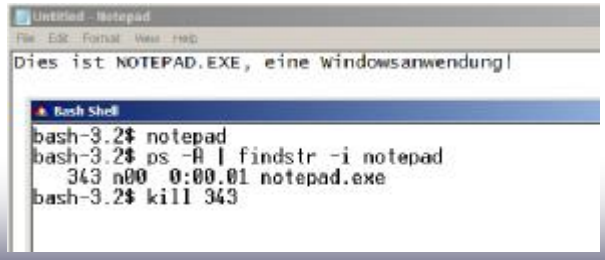
b) als Benutzer

```
chmod 700 ~/.ssh
chmod 700 ~/.ssh/authorized_keys
chmod 700 ~
```



Win32 und Interix Hand in Hand

- Der Windows-Kernel stellt beide Subsysteme gleichrangig zur Verfügung
- Win32 unterstützt nicht alle Unix-spezifischen Eigenschaften:
  - Groß-/Kleinschreibung im Dateisystem
  - Symlinks
  - SetUID, ROOT



"findstr"

Der o.g. Befehl "findstr" entspricht dem Unix-Befehl "grep". Der Parameter "-i" erlaubt das Suchen unter Missachtung der Groß-/Kleinschreibung.

Die Abbildung oben zeigt, dass das "pipen" zwischen Win32- und Posix-Applikationen möglich ist.

SetUID:

"Setuid (Set User ID, manchmal auch suid) ist ein erweitertes Unix-Dateirecht für Dateien oder Verzeichnisse des Unix-Betriebssystems. Ausführbare Programme, bei denen dieses Bit gesetzt ist, werden mit den Rechten des Benutzers ausgeführt dem die Datei gehört, anstatt mit den Rechten desjenigen Benutzers, der die Datei ausführt. Auf den meisten Systemen funktioniert dies nur für ausführbare Binärdateien, nicht jedoch für interpretierte Scripts."

Quelle: http://de.wikipedia.org/wiki/Setuid

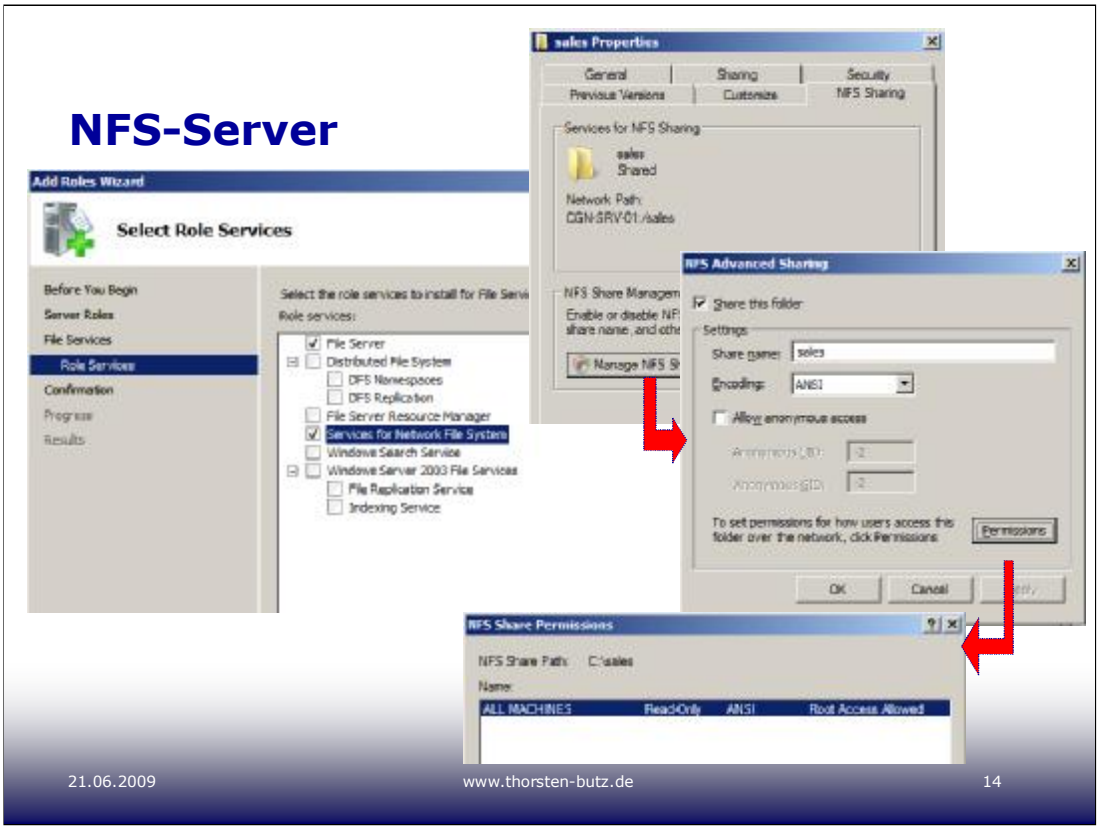
Symlinks:

Windows erlaubt zwei Arten von "symbolischen Links":

a) Win32: **mklink**

b) Posix: **ln –s**

(Für ein Beispiel siehe auch Folie 9!)



WS 2008 (R2) unterstützt NFS 2 (RFC 1094) und NFS 3 (RFC 1813):

http://go.microsoft.com/fwlink/?LinkId=44502

Die Neuerungen zu NFS in WS 2008:

- keine Unterstützung mehr für PCNFS
- "Gateway for NFS" wurde entfernt
- 64-bit-Support
- Unterstützung für "Special Devices" (mknod)
- Active Directory Lookup
- "User name mapping" wird nur noch client-seitig unterstützt, der Dienst ist (letztmalig) in WS 2003 R2 verfügbar.

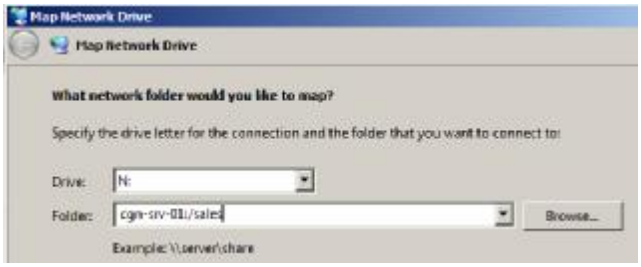
Die Neuerungen zu NFS in WS 2008 R2:

- Netgroup support
- RPCSEC_GSS support
- WMI-Unterstützung für NFS
- Unmapped UNIX User

Services for NFS Step-by-Step Guide for Windows Server 2008 R2

http://go.microsoft.com/fwlink/?LinkId=151755

NFS-Client



- UNIX/Linux, Windows:
  `showmount –e <nfs-server>`
- UNIX/Linux-CLient:
  `mount –t nfs <nfs-server>:/<share> /mnt/<localname>`
- Windows-Client:
  `net use * \\<nfs-server>\<share>`

Zur Demonstration:

Öffnen Sie auf einem Linuxhost (hier: CentOS) die Datei "/etc/exports":

```
vi /etc/exports
```

Ergänzen Sie die Datei mit nachfolgender Zeile

```
/pub 10.0.0.0/24(rw,root_squash,async)
```

Stellen Sie sicher, dass "/pub" existiert:

```
mkdir /pub
```

Starten Sie den NFS-Dienst:

```
/etc/init.d/nfs start
```

bzw. `/etc/init.d/nfs restart`

In anderen Distributionen heißt das Startscript u. U. anders, zum Bsp.

```
/etc/init.d/nfs-kernel-server start
```

Nun können Sie von ihrem Windowsclient die Freigabe "mappen":

```
net use p: \\rdu-srv-01\pub
```

wobei "rdu-srv-01" der Hostname des Linuxservers ist, oder:

```
mount \\rdu-srv-01\pub p:
```

Teil 3: Windows/Linux SSO

- Microsofts "Server for NIS"
- SaMBa (mit Kerberos und LDAP Support)
- **Native Anbindung mit Kerberos und LDAP**

NIS ("Network Information System"), ursprünglich auch YP ("Yellow pages") genannt, entstand bei SUN Microsystems als eine vergleichsweise schlichte Technologie zur zentralen Benutzeranmeldung in UNIX-Netzwerken. NIS gilt als nicht mehr zeitgemäß, da das Verfahren vergleichsweise leicht zu komprimittieren ist.

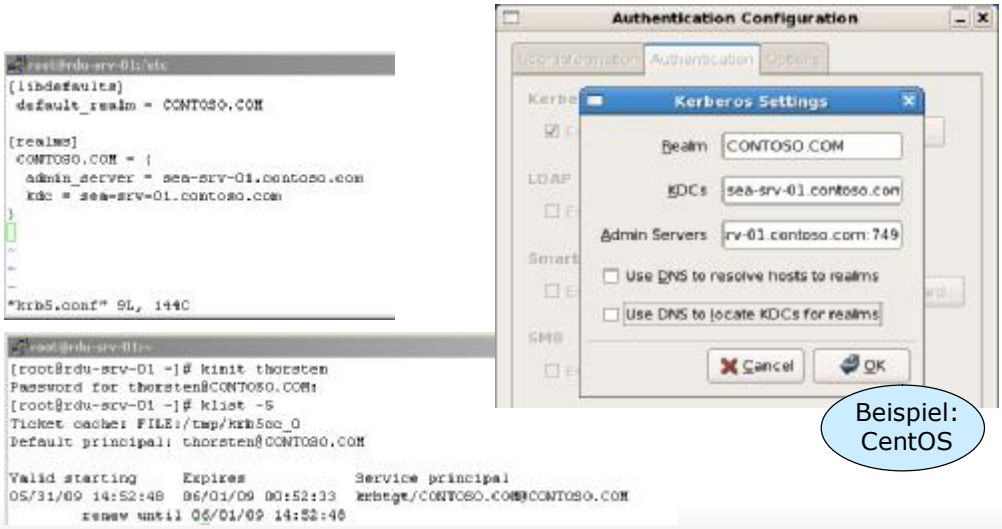
SaMBa wird seit der ersten Hälfte der 1990er Jahre lebhaft von der OpenSource-Community entwickelt und gehört zu den populärsten OpenSource-Lösungen. Andrew Tridgell begann mit der Analyse des proprietären SMB/CIFS-Protokolls, bis heute ist das Protokoll nicht vollständig standardisiert und offengelegt.

Kerberos (RFC 4120) und **LDAP** (RFC 4511) sind standardisierte Protokolle. Einen guten Überblick über die verschiedenen Ansätze zum "Single Sign On" (SSO) in Windows/Linux-Netzwerken gibt der nachfolgend Artikel.

Zum Weiterlesen:

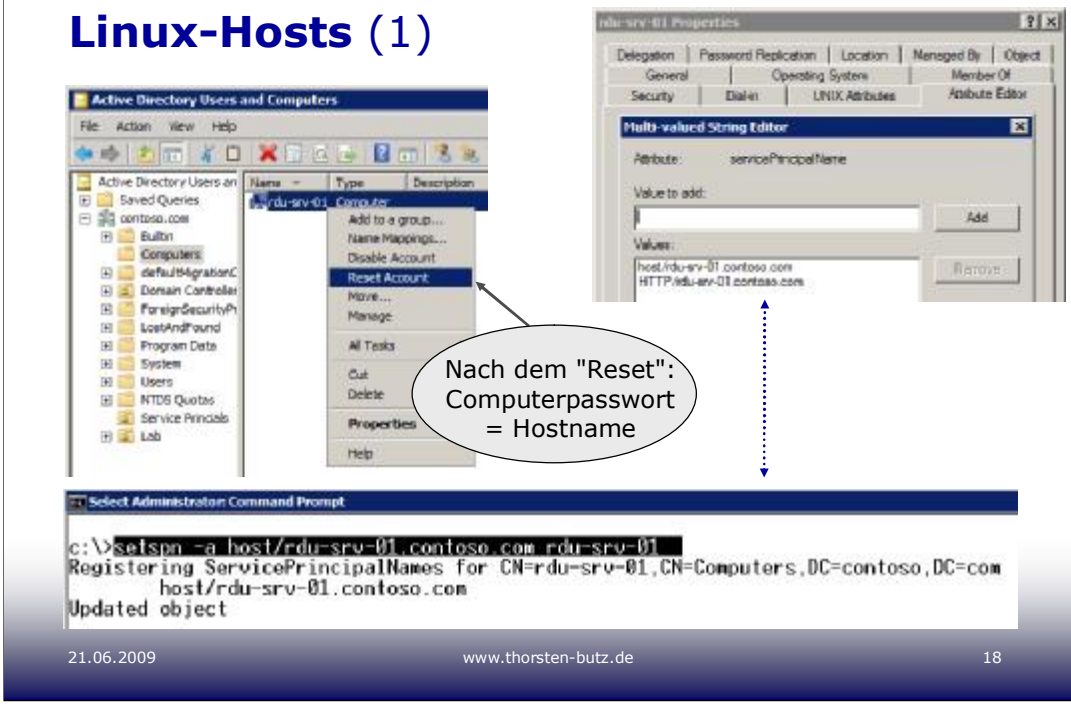
"**Authenticate Linux Clients with Active Directory**"
von Gil Kirkpatrick im "Technet Magazine", December 2008
(technet.microsoft.com/en-us/magazine/dd228986.aspx)

Kerberos Auth. gegen AD




```
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = CONTOSO.COM
 dns_lookup_realm = true
 dns_lookup_kdc = true
 ticket_lifetime = 24h
 forwardable = yes

[realms]
 CONTOSO.COM = {
  kdc = sea-srv-01.contoso.com:88
  admin_server = sea-srv-01.contoso.com:749
 }

[domain_realm]
 contoso.com = CONTOSO.COM
 .contoso.com = CONTOSO.COM

[appdefaults]
 pam = {
   debug = false
   ticket_lifetime = 36000
   renew_lifetime = 36000
   forwardable = true
   krb4_convert = false
 }
```

Beispiel-Listing /etc/krb5.conf für CentOS 5.3:



Domänenbeitritt auf Windows-Seite (Teil 1/2)

Das Active Directory verlangt von Windows-Clients den Beitritt in die Domäne, damit DC und Client wechselseitig sicher stellen können, dass der "Gesprächspartner" authentisch ist. Dies schützt vor "Man-in-the-Middle-Attacken."

Beim Domäneneintritt wird ein Maschinenkonto generiert, ein Vorgang, den der Linuxclient in dieser Form nicht kennt (zumindest nicht in Abwesenheit von SaMBa).

Aus diesem Grund muss der Austausch eines initialen Passworts zwischen Kerberos-Server und Kerberos-Client manuell initiiert werden (siehe Abbildungen oben):

a) **Neues Computerkonto erstellen**
(Das Passwort des neuen Computerkontos ist unbekannt.)

b) **Computerkonto zurücksetzen ("Reset Account")**
(Nun lautet das Passwort gleich dem Hostnamen, hier also "rdu-srv-01".)

c) `setspn -a host/rdu-srv-01.contoso.com rdu-srv-01`

(Ein Host-Principal für das neue Computerkonto wird erstellt.)

Domänenbeitritt eines Linux-Hosts (2)

- Keytab manuell erzeugen:
  - kpasswd, kvno, ktutil ... (auf dem Linux-Host)
  - ktpass (auf dem DC, anschließend Keytab nach Linux kopieren)
- Beitritt mit Hilfe von SaMBa:
  `net ads join –U <domain-admin>`

Domänenbeitritt auf Linux-Seite (Teil 2/2)

Variante a)

```
kpasswd rdu-srv-01
> rdu-srv-01                [Dies ist das aktuelle PW des Computerkontos im AD!]

ktutil:
> addent -password -p rdu-srv-01.contoso.com -k 5 -e rc4-hmac
> wkt /etc/krb5.keytab [wkt = write keytab]
> quit
```

Um Herauszufinden, welche "Key version number" der Kerberosdienst verwendet, kann man den nachfolgenden Befehl verwenden:

```
"kvno rdu-srv-01"
(kvno = "print key version numbers of Kerberos principals")
```

Variante b)

"ktpass" ist ein Windowswerkzeug, das Keytabs erzeugen kann, die man anschließend auf den Linuxhost übertragen kann.

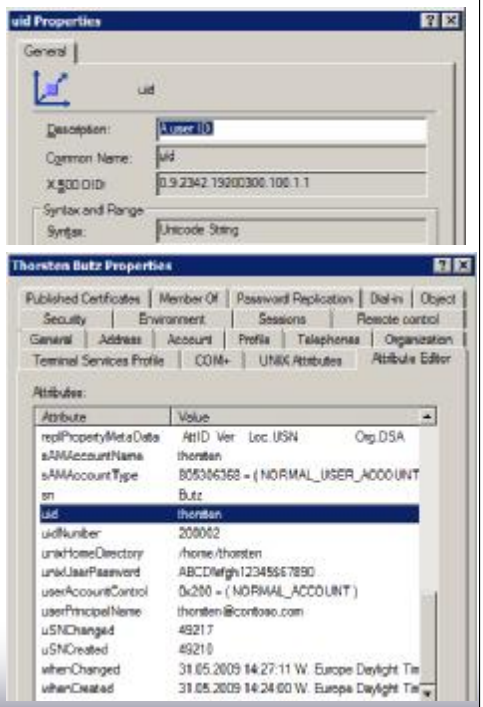
Variante c)

Wenn geplant ist, ohnehin SaMBa einzusetzen, ist sicherlich dies die beste aller genannten Varianten:

```
net ads join join –U administrator
```

RFC 2307

RFC2307-Attribut	WS 2008 AD-Schema-Attribut
uid	uid samAccountName
uidNumber	uidNumber
gidNumber	gidNumber
gecos	gecos description displayName name
homeDirectory	unixHomeDirectory
loginShell	loginShell



RFC 2397 (http://www.ietf.org/rfc/rfc2307.txt):

"An Approach for Using LDAP as a Network Information Service"

UNIX/Linux erwartet beim Login eines Anwenders Auskunft über einige Attribute des Benutzerkontos, um beispielsweise das Heimverzeichnis ansprechen zu können.

Gemäß RFC 2307 sucht Linux das Attribut "**homeDirectory**", das es im Active Directory-Schema durchaus gibt. Jedoch entspricht "homeDirectory" dem Feld "**Local Path**" im Profil des Benutzers, was in in aller Regel zur Anpassung der Anmeldung an Windowsclients verwendet wird.

Aus diesem Grund wird üblicherweise das AD-Schema-Attribut "**unixHomeDirectory**" verwendet, so dass sich Windows- und UNIX-Pfade unterscheiden lassen. "unixHomeDirectory" ist auf dem Karteireiter "**UNIX-Attributes**" sichtbar.

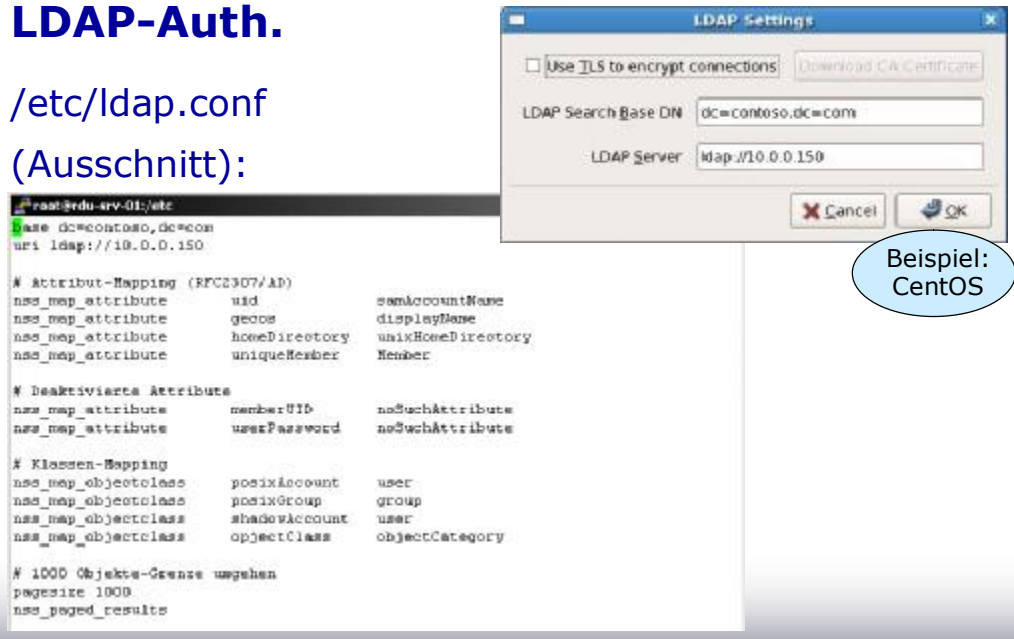
Dieses "Umbiegen"/Zuordnen der Attribute ermöglicht die "**/etc/ldap.conf**" auf dem Client, die auf der nachfolgenden Seite beschrieben wird. Das oben genannte Beispiel findet sich in der nachfolgend fett gedruckten Direktive:

```
# Attribut-Mapping (RFC2307/AD)
nss_map_attribute       uid             samAccountName
nss_map_attribute       gecos           displayName
nss_map_attribute       homeDirectory   unixHomeDirectory
nss_map_attribute       uniqueMember    Member
```

LDAP-Auth.

/etc/ldap.conf

(Ausschnitt):



Beispiel: CentOS


```
uri ldap://10.0.0.150
# Attribut-Mapping (RFC2307/AD)
nss_map_attribute       uid             samAccountName
nss_map_attribute       gecos           displayName
nss_map_attribute       homeDirectory   unixHomeDirectory
nss_map_attribute       uniqueMember    Member
# Deaktivierte Attribute
nss_map_attribute       memberUID       noSuchAttribute
nss_map_attribute       userPassword    noSuchAttribute
# Klassen-Mapping
nss_map_objectclass     posixAccount    user
nss_map_objectclass     posixGroup      group
nss_map_objectclass     shadowAccount   user
nss_map_objectclass     opjectClass     objectCategory
# 1000 Objekte-Grenze umgehen
pagesize 1000
nss_paged_results
# Binding
binddn ldapsearch@contoso.com
bindpw password
timelimit 120
bind_timelimit 120
idle_timelimit 3600
nss_initgroups_ignoreusers
root,ldap,named,avahi,haldaemon,dbus,radvd,tomcat,radiusd,news,mailman,nscd,gdm
ssl no
tls_cacertdir /etc/openldap/cacerts
pam_password md5
```

Beispiel-Listing /etc/ldap.conf

Abschlussarbeiten

- PAM-Konfiguration (/etc/pam.d/<configfile>):

```
auth     sufficient pam_krb5.so  minimum_uid 1000
account  sufficient pam_krb5.so  minimum_uid 1000
password sufficient pam_krb5.so  use_authtok
session  optional   pam_krb5.so  minimum_uid 1000
```

- Namensauflösung (/etc/nsswitch.conf):

```
passwd: files ldap
group:  files ldap
shadow: files ldap
```


Die "**/etc/nsswitch.conf**" wird lediglich um die oben gezeigten "ldap"-Einträge ergänzt, mehr ist dort nicht zu tun.
Die "**/etc/pam.d/system-auth-ac**" (CentOS-spezifisch) ist nachfolgend vollständig gelistet.

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        sufficient    pam_krb5.so use_first_pass
auth        required      pam_env.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        required      pam_deny.so

account     required      pam_access.so
account     required      pam_unix.so broken_shadow
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     [default=bad success=ok user_unknown=ignore] pam_krb5.so
account     required      pam_permit.so

password    requisite     pam_cracklib.so try_first_pass retry=3
password    sufficient    pam_unix.so md5 shadow nullok try_first_pass use_authtok
password    sufficient    pam_krb5.so use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     optional      pam_mkhomedir.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
session     optional      pam_krb5.so
```

(Kommerzielle) Alternativen

- Likewise (vormals Centeris),
  Open Source-Edition verfügbar
- Quest Authentication Services
- Centrify Suite 2008/Direct Control
- Symark PowerADVantage

"**Likewise**" ist in der freien Variante Bestandteil der (zum Zeitpunkt des Verfassens) aktuellen Ubuntu-Distribution (9.04).

Die "**Quest Authentication Services**" hießen vormals "Vintela Authentication Services".

Zum Weiterlesen:

ix Heft 5/2009, Seite 66:

Massenware, Unix-AD-Integration mit 3rd-Party-Produkten

(Mark Pröhl)

Zum Weiterlesen

- Connect-Newsgroup Hyper-V.Linux
  nntp://connectnews.microsoft.com/microsoft.beta.windowsserver.hyper-v.linux
  (Anmeldung via "connect.microsoft.com" erforderlich)
- SUA-Community/InterOp-Systems Learning Center
  www.interopsystems.com/learning.htm
- Dreiteiliges AD/Unix-Tutorial
  von Mark Pröhl und Michael Weiser in "iX", Heft 10/11/12 2008
  (www.heise.de/kiosk, kostenpflichtig)
- "Authenticate Linux Clients with Active Directory"
  von Gil Kirkpatrick im "Technet Magazine", December 2008
  (technet.microsoft.com/en-us/magazine/dd228986.aspx)
- Weitere Informationen und Howtos zum Vortrag:
  www.thorsten-butz.de

21.06.2009 www.thorsten-butz.de 24

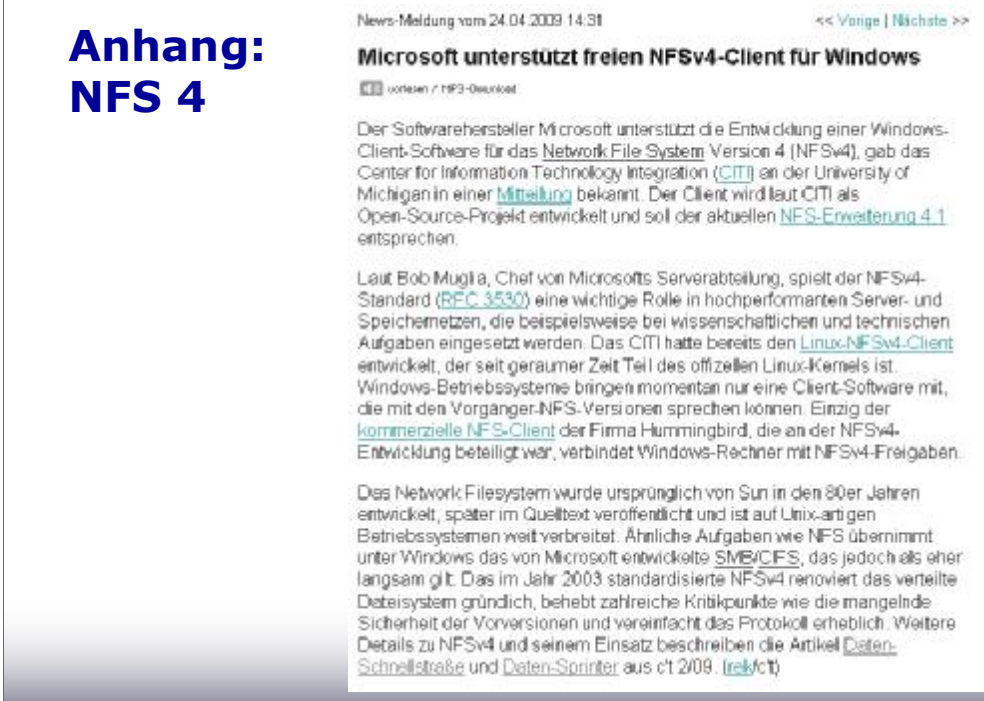
Im Juni 2009 erscheint auf der Connect-Seite zu den "Linux Integration Components" der **RC der LIC für Hyper-V Version 2**. Mit dem Erscheinen des Windows Server 2008 R2 wird aller Voraussicht nach die finale Version bereit stehen.

Auf meiner Webseite "**www.thorsten-butz.de**" finden sich in loser Folge Beiträge zu technischen Themen. Als ein Beispiel sei das Erleuchten des CentOS genannt, den ausführlichen Blogeinstrag findet man hier:

http://www.thorsten-butz.de/index.php/enlightening-centos/

Verfasst von Thorsten Butz im Juni 2009.

Anhang: NFS 4



News-Meldung vom 24.04.2009 14:31 << Vorige | Nächste >>

Microsoft unterstützt freien NFSv4-Client für Windows

vorlesen / MP3-Download

Der Softwarehersteller Microsoft unterstützt die Entwicklung einer Windows-Client-Software für das Network File System Version 4 (NFSv4), gab das Center for Information Technology Integration (CITI) an der University of Michigan in einer Mitteilung bekannt. Der Client wird laut CITI als Open-Source-Projekt entwickelt und soll der aktuellen NFS-Erweiterung 4.1 entsprechen.

Laut Bob Muglia, Chef von Microsofts Serverabteilung, spielt der NFSv4-Standard (RFC 3530) eine wichtige Rolle in hochperformanten Server- und Speichernetzen, die beispielsweise bei wissenschaftlichen und technischen Aufgaben eingesetzt werden. Das CITI hatte bereits den Linux-NFSv4-Client entwickelt, der seit geraumer Zeit Teil des offiziellen Linux-Kernels ist. Windows-Betriebssysteme bringen momentan nur eine Client-Software mit, die mit den Vorgänger-NFS-Versionen sprechen können. Einzig der kommerzielle NFS-Client der Firma Hummingbird, die an der NFSv4-Entwicklung beteiligt war, verbindet Windows-Rechner mit NFSv4-Freigaben.

Das Network Filesystem wurde ursprünglich von Sun in den 80er Jahren entwickelt, später im Quelltext veröffentlicht und ist auf Unix-artigen Betriebssystemen weit verbreitet. Ähnliche Aufgaben wie NFS übernimmt unter Windows das von Microsoft entwickelte SMB/CIFS, das jedoch als eher langsam gilt. Das im Jahr 2003 standardisierte NFSv4 renoviert das verteilte Dateisystem gründlich, behebt zahlreiche Kritikpunkte wie die mangelnde Sicherheit der Vorversionen und vereinfacht das Protokoll erheblich. Weitere Details zu NFSv4 und seinem Einsatz beschreiben die Artikel Daten-Schnellstraße und Daten-Sprinter aus c't 2/09. (rek/c't)

Zum Weiterlesen:

http://www.heise.de/netze/Microsoft-unterstuetzt-freien-NFSv4-Client-fuer-Windows--/news/meldung/136743

http://connectivity.hummingbird.com/products/nc/nfs/index.html

Kostenpflichtig:

http://www.heise.de/kiosk/archiv/ct/09/02/180_Daten-Schnellstrasse

http://www.heise.de/kiosk/archiv/ct/09/02/183_Daten-Sprinter