Debian 7 an das Active Directory anbinden

Debian 7 an das Active Directory anbinden

Inhalt

Windows Server Vorbereitung

Um dieses HowTo schreiben zu können, wurde das Ganze in einer Virtuellen Umgebung mit Oracle VM VirtualBox nachgestellt.

- ✓ Microsoft Windows Server 2008 R2 SP1
- ✓ Windows Security Updates
- ✓ Active Directory Domaindienste
- ✓ Debian 7.2 Wheezy Standard Installation
- ✓ Putty 0.63
- ✓ WinSCP 5.1.7

Debian 7.1 Wheezy Client downloaden und Installieren

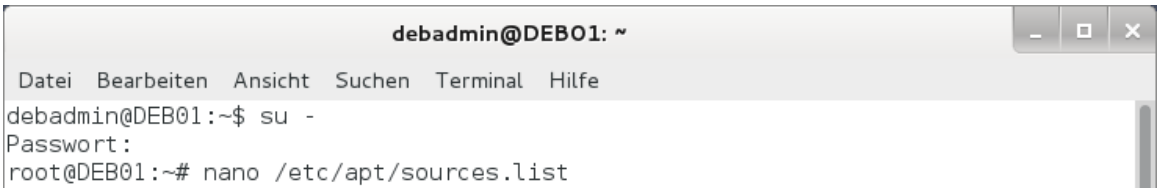
Hier findet ihr das ISO Image von → Debian 7.1 Wheezy

In diesen Howto werde ich euch nicht erklären wie ihr Debian 7 installieren könnt, denke das bekommt ihr auch alleine hin. Anbei ein YouTube Video bzw. die Debian Installationsanleitung

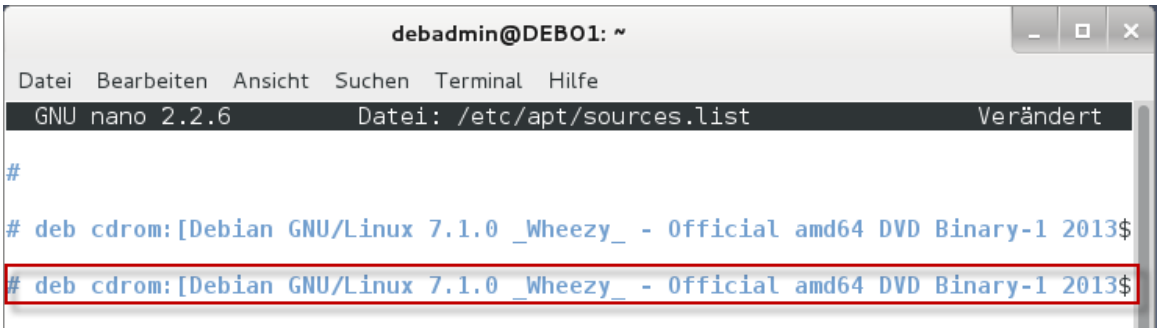
Debian 7.1 Wheezy Client für den Domain Join vorbereiten

/etc/apt/sources.list anpassen

Nach der Installation und dem ersten Login, mache ich mich zum root mit dem Befehl
su – (Passwort)



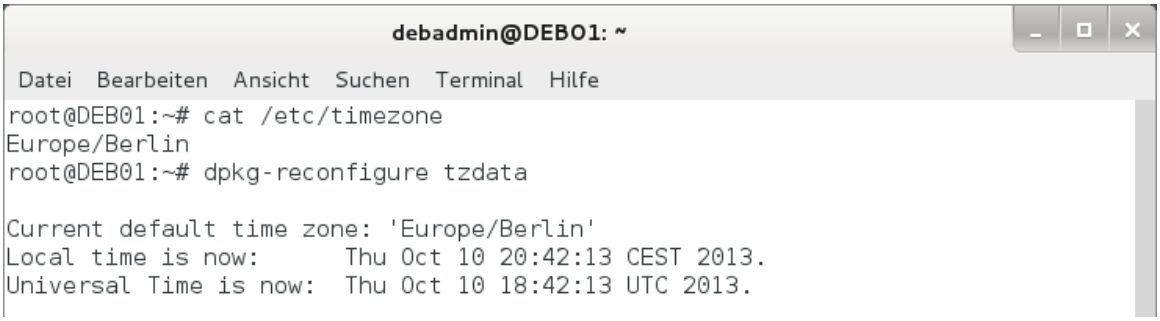
Danach kommentiere ich in der ***/etc/apt/sources.list*** den CD-Rom Eintrag aus, denn wenn man Dateien mit ***apt-get install*** installieren möchte, greift Debian immer als erstes auf das CD-Rom Laufwerk zu, das möchte ich vermeiden, ich beziehe die Software aus dem Internet.



nano /etc/apt/sources.list
 # deb cdrom (Auskommentieren)

Timezone anpassen wenn nötig

Mit ***cat /etc/timezone*** kontrolliere ich nochmals die Zeitzone.
Sollte diese versehentlich bei der Installation nicht gesetzt worden sein kann ich mit folgendem Befehl → ***dpkg-reconfigure tzdata***



NTP/SSH/VIM Installieren

apt-get install ssh auto-apt vim vim-gnome ntp ntpdate
auto-apt update-local

apt-get update && apt-get upgrade

catman (erzeugt oder aktualisiert die formatierten Manual Seiten)
updatedb

Ab hier setze ich die Software Putty ein um eine SSH Verbindung vom meinen Windows 7 Client zum Linux Client aufzubauen --> http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Netzwerkkarte konfigurieren

nano /etc/network/interfaces

auto eth0
iface eth0 inet static
  address 192.168.178.158
  netmask 255.255.255.0
  network 192.168.178.0
  broadcast 192.168.178.255
  gateway 192.168.178.1

/etc/init.d/networking restart

resolv.conf Datei anpassen

nano /etc/resolv.conf

domain htdom.local
search htdom.local
nameserver 192.168.178.100
nameserver 192.168.178.1

[Optional gibt man noch folgende Parameter an, um eine Art Round Robin zwischen zwei DNS Servern zu erreichen, siehe ***man resolv.conf***]
options rotate
options timeout:1

Host Datei anpassen

nano /etc/hosts

127.0.0.1 localhost.localdomain localhost
192.168.178.158 deb01.htdom.local deb01
192.168.178.100 ads01.htdom.local ads01 htdom.local

Admingruppe der sudoers hinzufügen

/usr/sbin/groupadd admin
/usr/sbin/usermod -a -G admin <benutzername>

cp /etc/sudoers /etc/sudoers.old
rm /etc/sudoers && nano /etc/sudoers

/etc/sudoers

Defaults env_reset
Defaults mail_badpass
Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

Host alias specification
User alias specification

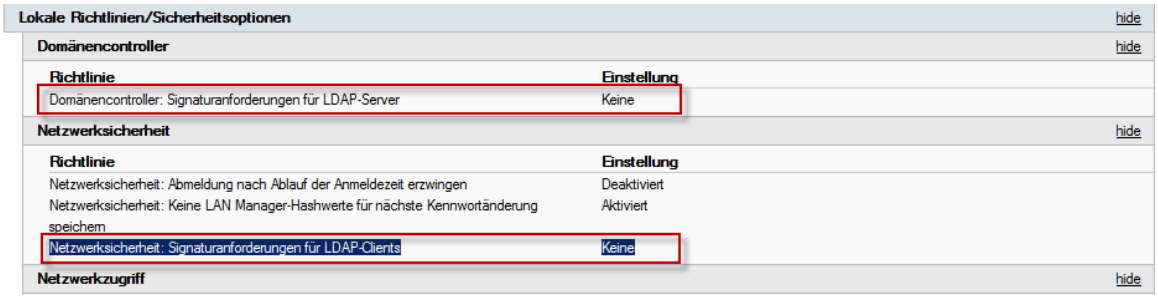
User_Alias MYADMINS = debadmin

Cmnd alias specification
Cmnd_Alias UPDATE = /usr/bin/apt-get update, /usr/bin/apt-get upgrade
Cmnd_Alias MOUNT = /sbin/mount*
Cmnd_Alias UMOUNT = /sbin/umount*

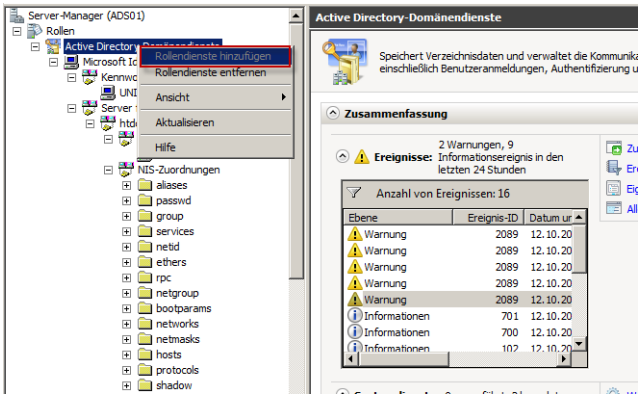
```
Cmnd_Alias     NET     = /sbin/ifconfig, /sbin/ifdown, /sbin/ifup, /sbin/ifquery, /sbin/route
Cmnd_Alias     REBOOT  = /sbin/shutdown, /sbin/reboot, /sbin/halt
Cmnd_Alias     MYAPPS  = UPDATE, MOUNT, UMOUNT, NET, REBOOT

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Users listed above (MYADMINS) can run updates and upgrades, mount and umount netshares,
show net configuration, and reboot the system
MYADMINS ALL = MYAPPS

# Allow members of group sudo and admin to execute any command
%sudo   ALL=(ALL:ALL) NOPASSWD:ALL
%admin  ALL=(ALL:ALL) NOPASSWD:MYAPPS

### /etc/sudoers ##########################################################

chmod 440 /etc/sudoers
shutdown -r now
```

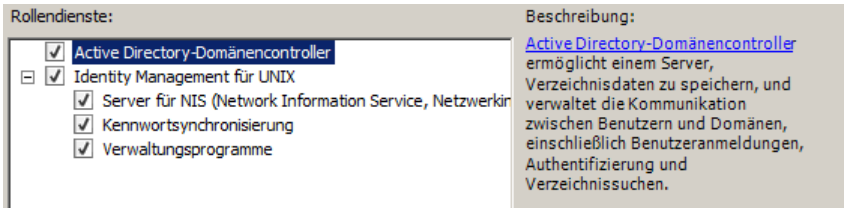
Active Directory Server für die Authentifizierung der Unix/Linux Clients vorbereiten.

Zum einen muss die Gruppenrichtlinie der "***Default Domain Policy***" angepasst werden.



Und zum zweiten müssen die "***Identity Management für UNIX***" nachinstalliert werden, diese findet man erst, wenn ein Server zum Domänencontroller hochgestuft wurde und die Rolle Active Directory Domänendienste vorhanden sind.





NTP Client installieren & konfigurieren

cp /etc/ntp.conf /etc/ntp.old
rm /etc/ntp.conf
nano /etc/ntp.conf

Client:/etc/ntp.conf

Abweichungen
driftfile /var/lib/ntp/ntp.drift

NTP-Server im LAN (siehe oben)
server 192.168.178.100

Zugriff durch NTP-Server gestatten
restrict 192.168.178.100

Zugriff vom localhost gestatten (ntpq -p)
restrict 127.0.0.1

allen anderen Rechnern Zugriff verwehren
restrict default notrust nomodify nopeer

###

ntpdate 192.168.178.100
12 Oct 19:50:48 ntpdate[4738]: the NTP socket is in use, exiting

Sollte das ntpdate IP-Adresse nicht funktionieren muss mit ***ps aux | grep ntpd*** der NTP Dienst gesucht und beendet werden

ps aux | grep ntpd

root 3087 0.0 0.1 20172 3084 pts/0 Ss 13:06 0:00 -bash
ntp 11658 0.0 0.1 34780 2232 ? Ss 13:40 0:00 /usr/sbin/ntpd -p /var/run/ntpd.pid -g -u
root 11689 0.0 0.0 16832 1272 pts/0 R+ 13:48 0:00 ps aux

kill 11658

ntpdate 192.168.178.100
/etc/init.d/ntp start

hwclock –systohc
ntpq -p
ntpdc -p

```
root@DEB01:~# cp /etc/ntp.conf /etc/ntp.old
root@DEB01:~# rm /etc/ntp.conf
root@DEB01:~# nano /etc/ntp.conf
root@DEB01:~# ntpdate 192.168.178.100
12 Oct 19:50:48 ntpdate[4738]: the NTP socket is in use, exiting
root@DEB01:~# ps aux | grep ntpd
ntp       2773  0.0  0.1  41044  2372 ?        Ss   18:31   0:00 /usr/sbin/ntpd -p /var/run/ntpd.pid -g -u 114:123
root      4740  0.0  0.0   9896   928 pts/0    S+   19:51   0:00 grep ntpd
root@DEB01:~# kill 2773
root@DEB01:~# ntpdate 192.168.178.100
12 Oct 19:51:42 ntpdate[4741]: step time server 192.168.178.100 offset 1.254793 sec
root@DEB01:~# /etc/init.d/ntp start
[ ok ] Starting NTP server: ntpd.
root@DEB01:~# hwclock --systohc
root@DEB01:~# ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 ads01.htdom.loc 65.55.56.206     3 u   20   64    1    0.306  -35.086   0.000
root@DEB01:~# ntpdc -p
     remote           local      st poll reach  delay   offset    disp
=============================================================================
=ads01.htdom.loc 192.168.178.158  3   64    1 0.00031 -0.035086 2.81874
root@DEB01:~#
```

Samba und Kerberos Installieren

apt-get install krb5-user libpam-krb5 winbind samba ldap-utils cifs-utils

/etc/init.d/samba stop
/etc/init.d/winbind stop
/etc/init.d/ntp stop

cp /etc/samba/smb.conf /etc/samba/smb.old
cp /etc/nsswitch.conf /etc/nsswitch.old
cp /etc/krb5.conf /etc/krb5.old
cp –r /etc/pam.d /etc/pam.d.old
cp –r /var/lib/samba /var/lib/samba.old

Kerberos 5 konfigurieren

rm /etc/krb5.conf && nano /etc/krb5.conf

```
### /etc/krb5.conf ######################################################

[logging]
    default = FILE:/var/log/krb5/krb5.log
    kdc = FILE:/var/log/krb5/krb5kdc.log
    admin_server = FILE:/var/log/krb5/kadmind.log

[libdefaults]
    default_realm = HTDOM.LOCAL
    clockskew = 300

#The following krb5.conf variables are only for MIT Kerberos.
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true

[realms]
    HTDOM.LOCAL = {
        kdc = ads01.htdom.local
        default_domain = htdom.local
        admin_server = ads01.htdom.local
    }

[domain_realm]
    .htdom.local = HTDOM.LOCAL
    htdom.local = HTDOM.LOCAL

### /etc/krb5.conf ######################################################
```

Samba konfigurieren

rm /etc/samba/smb.conf && nano /etc/samba/smb.conf

testparm
testparm-v
testparm -v | grep idmap
Error - rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)

ulimit -n 16384
nano /etc/security/limits.conf
        *   -   nofile   16384

```
#@faculty        soft    nproc           20
#@faculty        hard    nproc           50
#ftp             hard    nproc           0
#ftp             -       chroot          /ftp
#@student        -       maxlogins       4
*                -       nofile          16384
# End of file
```

/etc/samba/smb.conf

[global]
    workgroup = HTDOM
    realm = HTDOM.LOCAL
    netbios name = DEB01
    security = ads
    server string = %h server
    load printers = no
    local master = no
    domain master = no
    preferred master = no
    dns proxy = no
    winbind uid = 10000-20000
    winbind gid = 10000-20000
    winbind use default domain = yes
    interfaces = eth0 lo
    syslog = 0
    log file = /var/log/samba/log.%m
    max log size = 1000
    panic action = /usr/share/samba/panic-action %d
    invalid users = root
    template homedir = /home/%D/%U
    template shell = /bin/bash
    winbind offline logon = yes
    winbind refresh tickets = yes

/etc/samba/smb.conf

/etc/init.d/samba restart

kinit <benutzername>@HTDOM.LOCAL (Passwort)
klist

```
root@DEB01:/etc# cd
root@DEB01:~# rm /etc/krb5.conf
root@DEB01:~# nano /etc/krb5.conf
root@DEB01:~# rm /etc/samba/smb.conf
root@DEB01:~# nano /etc/samba/smb.conf
root@DEB01:~# /etc/init.d/samba restart
[ ok ] Stopping Samba daemons: nmbd smbd.
[ ok ] Starting Samba daemons: nmbd smbd.
root@DEB01:~# kinit ldapusr@HTDOM.LOCAL
Password for ldapusr@HTDOM.LOCAL:
root@DEB01:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: ldapusr@HTDOM.LOCAL

Valid starting       Expires              Service principal
12.10.2013 20:31:44  13.10.2013 06:31:48  krbtgt/HTDOM.LOCAL@HTDOM.LOCAL
        renew until 13.10.2013 20:31:44
```

ldapsearch -h 192.168.178.100 -b DC=htdom,DC=local -D <benutzername>@htdom.local -W -x (Passwort)

/etc/nsswitch.conf konfiguriern

rm /etc/nsswitch.conf
nano /etc/nsswitch.conf

/etc/nsswitch.conf
Example configuration of GNU Name Service Switch functionality.
If you have the `glibc-doc' and `info' packages installed, try:
`info libc "Name Service Switch"' for information about this file.

passwd: compat winbind
group: compat winbind
shadow: compat

hosts: files dns wins
networks: files

protocols: db files
services: db files
ethers: db files
rpc: db files

netgroup: nis

###

/etc/init.d/winbind restart

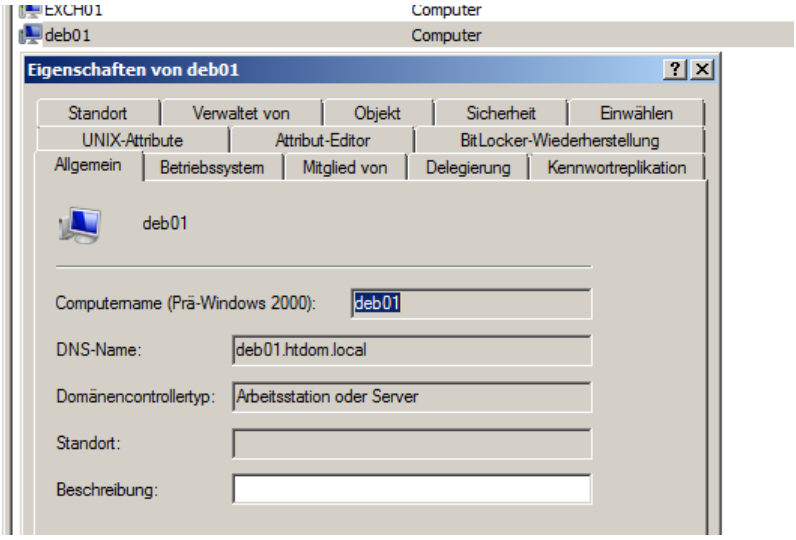
Debian 7.1 Wheezy Client in das Active Director aufnehmen

Ab hier sind wir soweit das wir den Debian 7 Client an das Active Directory anbinden können. Das funktioniert mit folgendem Befehl:

net ads join -U Administrator (Passwort)

```
root@DEB01:~# net ads join -U Administrator
Enter Administrator's password:
Using short domain name -- HTDOM
Joined 'DEB01' to realm 'htdom.local'
```

Nach erfolgreichen Domain Join findet man den Debian Client in der Computer OU im Active Directory



/etc/pam.d/common-session konfigurieren für die Home Laufwerke

cp /etc/pam.d/common-session /etc/pam.d/common-session.old
nano /etc/pam.d/common-session

session required pam_mkhomedir.so umask=0022 skel=/etc/skel

net ads dns register -P -d 10

Verbindung zu Active Directory testen

Hier ein paar Befehle wie man die Verbindung zu Active Directory testen kann.

/etc/init.d/winbind restart

wbinfo –t (zeigt an ob der RPC trust secret passt)
wbinfo -a Administrator (Passwort) (zeigt mir an ob sich AD-User Administrator über winbind Authentifizieren kann)
wbinfo –u (zeigt mir alle Active Directory Benutzer an)
wbinfo –g (zeigt mir alle Active Directory Gruppen an)

getent passwd
getent group

Hier überprüfen wir noch die Services Samba und winbind ob sie sauber laufen

ps -ef | grep samba
ps -ef | grep winbind

http://www.debuntu.org/how-to-managing-services-with-update-rc-d/

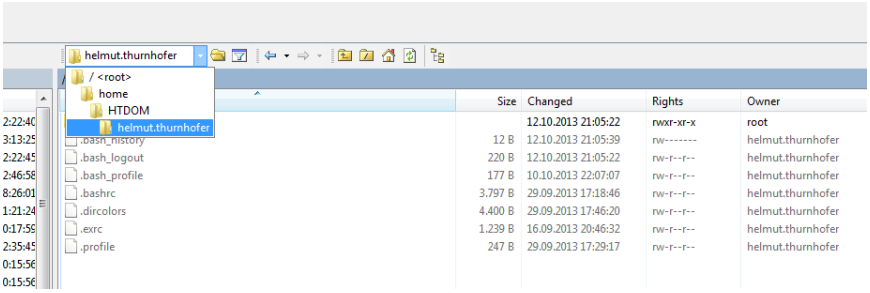
http://wiki.ubuntuusers.de/Dienste

update-rc.d samba defaults
update-rc.d winbind defaults

ls -l /etc/rc?.d/*winbind
ls -l /etc/rc?.d/*samba

Als Active Directory Benutzer am Linux Client anmelden

Hier sieht man dass ich mich als Active Directory Benutzer über WinSCP am Linux Client angemeldet habe.



Und hier die Verbindung mit Putty

```
login as: helmut.thurnhofer
helmut.thurnhofer@192.168.178.158's password:
Linux DEB01 3.2.0-4-amd64 #1 SMP Debian 3.2.51-1 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Oct 12 21:10:39 2013 from 192.168.178.30
helmut.thurnhofer@DEB01:~$ ls -la
insgesamt 40
drwxr-xr-x 2 helmut.thurnhofer domänen-benutzer 4096 Okt 12 21:13 .
drwxr-xr-x 3 root              root             4096 Okt 12 21:05 ..
-rw------- 1 helmut.thurnhofer domänen-benutzer   80 Okt 12 21:13 .bash_history
-rw-r--r-- 1 helmut.thurnhofer domänen-benutzer  220 Okt 12 21:05 .bash_logout
-rw-r--r-- 1 helmut.thurnhofer domänen-benutzer 3797 Sep 29 17:18 .bashrc
-rw-r--r-- 1 helmut.thurnhofer domänen-benutzer 4400 Sep 29 17:46 .dircolors
-rw-r--r-- 1 helmut.thurnhofer domänen-benutzer 1239 Sep 16 20:46 .exrc
-rw-r--r-- 1 helmut.thurnhofer domänen-benutzer  247 Sep 29 17:29 .profile
-rw------- 1 helmut.thurnhofer domänen-benutzer  882 Okt 12 21:13 .viminfo
helmut.thurnhofer@DEB01:~$
```

Viel Spaß beim Nachmachen.

Gruß Helmut