Installation Ubuntu Server 24.04 LTS

Die Installation des Ubuntu Servers Erfolgt in Virtualbox. Achten Sie bei der Einrichtung der VM darauf, dass die unbeaufsichtigte Installation nicht durchgeführt wird, da einzelne Schritte relevant sind.

Beim Bootvorgang wählen Sie „Try or Install" um das Setup zu starten. Wählen Sie im nächsten Schritt Deutsch als Installations- und Systemsprache. Bei Der Wahl der Tastatur setzen Sie ebenfalls auf German und German.

Die Installationsart sollte Standard sein. Minimal führt dazu, dass viele „übliche" Programme wie `PING` nicht installiert werden. Üblicherweise benötigen Sie den unteren teil der Third-Party-Driver nicht, wenn Sie nicht auf echter Hardware arbeiten. Hier werden dann RAID-Controller oder WLAN-Karten ergänzt.

Die Netzwerkkonfiguration belassen wir auf DHCP, da später die Konfigurationsdatei manuell angepasst werden soll. Üblicherweise würde aber hier eine feste IP für einen Server vergeben werden, wobei darauf zu achten ist, die Subnetzmaske als CIDR anzuhängen. Proxy bleibt leer.

Nach der Bestätigung der Netzwerkkonfiguration testet der Server automatisch den schnellsten/nächsten Updateserver.

Die Festplattenpartitionierung kann auf Default belassen werden. Die Verwendung von LVM ist mittlerweile Standard. LVM steht für Logical Volume Manager und ist eine Variante Software-RAID um auch nachträglich Erweiterungen oder Redundanzen hinzuzufügen. Bestätigen Sie ihre Wahl.

Setzen Sie Ihren user-account und ihren Hostname dc1.

Im nächsten Schritt können Sie sich für Ubuntu Pro anmelden, einen Dienst, welcher ihnen erweiterten Support und Features wie Kernel-Live-Patches und längeren Support.

Aktivieren Sie auf jeden Fall die Installation des openSSH-Servers. Unten könnten Sie SSH-Keys aus z.B. github importieren, um sie später ohne Passwort per SSH auf den Server zu verbinden.

Die nachfolgenden Features sind „snaps" von Ubuntu und sollen im Rahmen der Meisterausbildung nicht genutzt werden, da diese nicht auf „Nicht-Ubuntu" Systemen funktionieren. Hierbei handelt es sich um vorkonfektionierte Programmpakete.

Nun läuft die Installation durch. Am Ende steht nichts im Log, sondern darunter entsteht ein Button zum Neustarten des Systems.

Denken Sie nach dem Neustart daran, dass Sie innerhalb des etz wieder den Cache-Server verwenden:

```
1 echo 'Acquire::http::Proxy "http://10.10.224.119:3142";' | sudo tee /
    etc/apt/apt.conf.d/02proxy
```

Ein Linux-Server als Active Directory Domain Controller

Ein Linux-Server der Active Directory beherrscht, ist eine Möglichkeit, um auf den Einsatz eines MS-Servers zu verzichten. Es existieren ein paar Einschränkungen aber das Projekt Samba ist im stetigen Wachstum und entwickelt immer neue Funktionen hinzu. In dieser Arbeitsanweisung werden Sie einen Samba4 Active Directory Server installieren und im Anschluss Diesen mit den MS-Remote Server Administration Tools verwalten. Die Funktionalität dieses Servers enthält: DNS, Kerberos, Benutzer und Gruppen, Netzlaufwerke und Gruppenrichtlinien.

Vorgaben die in dieser Anleitung genutzt werden.

```
DNS-Server:
Name: dc1.tnXX.ito
Server Type: Authoritative.
Forward Lookup Zone: tnXX.ito
Reverse Lookup Zone: 2XX.168.192.in-addr.arpa.

DC-Server
AD DC Hostname: DC1
AD DNS Domain Name: tnXX.ito
Kerberos Realm: tnXX.ito
NT4 Domain Name: tnXX
IP Adresse 192.168.2XX.250
Server Role: Domain Controller
DNS Forwarder: 192.168.2XX.1

DHCP Server
Subnet: 192.168.2XX.0 255.255.255.0
Range: 192.168.2XX.100 192.168.2XX.200
```

Einrichtung der festen IP inklusive DNS-Anpassung

In der aktuellen Version von Ubuntu Server wird bei der Netzwerkkonfiguration auf netplan gesetzt. Hierbei wird eine .yaml Datei angelegt, welche in der MAAS-Installation (Cloud-Config) automatisch dem Rechner zugewiesen würde.

Als erstes legen wir eine neue Datei an:

```
sudo nano /etc/netplan/01-tnXX-netz.yaml
```

```
# This file describes the network interfaces available on your system
# For more information, see netplan(5).
network:
  ethernets:
    enp0s3:
      addresses: [192.168.2XX.250/24]
        routes:
          - to: 0.0.0.0/0
            via: 192.168.2XX.1
        dhcp4: no
        nameservers:
          addresses: \[192.168.2.XX.250,1.1.1.1\]
          search: \[tnXX.ito\]
        optional: true
  version: 2
```

Die Anpassung des Hostnamen wurde auch kompatibel mit der Cloud-Config gemacht daher neuer Vorgehensweise:

```
sudo hostnamectl set-hostname dc1
sudo nano /etc/cloud/cloud.cfg
```

```
preserve_hostname: true # Erhält den Hostnamen nach dem Neustart
```

Erweitern der Hosts-Datei:

```
sudo nano /etc/hosts
```

```
127.0.0.1 localhost
127.0.1.1 dc1.tnXX.ito dc1
```

Einagben Überprüfen:

```
sudo hostname
sudo nslookup dc1
```

Beides sollte den oberen Eingaben entsprechen.

Installation der benötigten Komponenten

```
sudo apt update
sudo apt install samba samba-dsdb-modules samba-vfs-modules krb5-config
     winbind libpam-winbind libnss-winbind acl dnsutils chrony isc-dhcp-
    server krb5-user smbclient
```

Während der Installation werden Sie nach dem Realm für Kerberos gefragt:

```
Realm = MKXX.ITO (Alles groß schreiben)
Server = DC1.MKXX.ITO
Administrator Server = DC1.MKXX.ITO
```

Linux fit für ACL

Um mit Samba auch die vollen Windows ACL und Benutzer-Attribute zu unterstützen müssen diese ebenfalls im ext4 Dateisystem ihres Servers aktiviert werden. > Bevor Sie das tun wäre jetzt der Punkt einen Sicherungspunkt der VM zu machen Bei Tippfehlern werfen Sie sich selbst aus dem System.

```
sudo nano /etc/fstab
```

```
UUID=xxx / ext4 defaults 0 0
```

Wird zu:

```
UUID=xxx / ext4 user_xattr,acl,barrier=1,errors=remount-ro,defaults 0 0
```

Speichern und Neustart

Zeitserver Einrichten

Als Zeitserver verwenden wir den Dienst chrony.

```
sudo nano /etc/chrony/chrony.conf
```

Am Ende Anhängen:

```
allow 0.0.0.0/24
```

Dienst neu starten:

```
sudo systemctl restart chrony
```

Testen ob der Dienst aktiv ist:

```
ss -tulpen:
```

```
udp 0 0 0.0.0.0:123 0.0.0.0:* 0 22432 1180/chronyd
```

Samba Installation und Provisionierung

Samba Installieren

Sichern der Orginalkonfiguration

```
sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.bak
```

Provisionierung des Samba4 zu einem Active Directory Domain-Controller mit UNIX-Erweiterung:

```
sudo samba-tool domain provision --use-rfc2307 --interactive --dns-
    backend=SAMBA_INTERNAL
```

Fragen beantworten: * Realm: TNXX.ITO * Domain: TNXX * Server Role: dc * DNS backend: SAMBA_INTERNAL * DNS forwarder: 1.1.1.1 * Administrator password: 3 von 4: klein, groß, Zahl Zeichen und mindestens 7 Zeichen lang!!!!!!!!!!!!! zB. passw0rd#

Fertig.

Startverhalten von Samba an AD-DC anpassen

```
sudo systemctl enable --now samba-ad-dc
```

Samba nur auf den angegeben Netzwerkkarten starten, auf diese Weise gibt es keine Konflikte mit dem internen Nameserver edit in /etc/samba/smb.conf unter global

```
bind interfaces only = yes
interfaces = lo enp0s3
```

Kerberos-Konfiguration von Samba übernehmen

Samba legt bei der Provisionierung eine vorgefertigte Konfigurationsdatei für Kerberos also dem Authentifizierungsdienst, welcher auch eine Synchrone Uhr braucht.

Original sichern:

```
sudo mv /etc/krb5.conf /etc/krb5.conf.bak
```

Link erstellen:

```
sudo cp -al /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

Anpassung der Netzwerkverbindung um DNS-Anfragen durch den Internen-DNS zu beantworten

```
sudo nano /etc/netplan/01-tnXX-netz.yaml
```

```
...
nameservers:
  addresses: [192.168.2XX.250]
  search: [tnXX.ito]
...
```

```
sudo rm /etc/netplan/50-cloud-init.yaml
sudo netplan apply
```

Internen Resolver übernehmen

```
sudo rm /etc/resolv.conf
echo -e \"nameserver 127.0.0.1\\nsearch TNXX.ITO\" \| sudo tee
/etc/resolv.conf
```

Überprüfen der DNS-Konfiguration

Testen des SRV record für ldap über TCP

```
host -t SRV \_ldap.\_tcp.tnXX.ito
```

> _ldap._tcp.tnXX.ito has SRV record 0 100 389 dc1.tnXX.ito.

Testen des SRV record für kerberos über UDP

```
host -t SRV \_kerberos.\_udp.tnXX.ito
```

> _kerberos._udp.mkXX.ito has SRV record 0 100 88 dc1.tnXX.ito.

Und die Namensauflösung des Servers

```
host -t A dc1.tnXX.ito
```

> dc1.tnXX.ito has address 127.0.0.1

Wenn hier Alles antwortet funktioniert der DNS

Kerberos

Samba erzeugt eine passende Konfigurationsdatei für den Kerberos-Dienst diese verlinken wir anstelle der Original-Datei die uns mitinstalliert wurde.

```
sudo mv /etc/krb5.conf /etc/krb5.conf.orig
sudo cp -al /var/lib/samba/private/krb5.conf /etc/krb5.conf
sudo reboot
```

Login-Versuch mit Anlegung des Maschinenaccounts

```
kinit administrator@TNXX.ITO
```

> Es erfolgt eine Ausgabe ihres Passwort-Ablaufdatums

```
klist
```

> Das komplette Kerberos Ticket wird angezeigt

```
sudo smbclient -L localhost -U 'administrator'
```

> Sie sehen eine auflistung der Servereigenschaften, der Freigaben und der Serverrolle

```
sudo smbclient //localhost/netlogon -U 'administrator'
```

Sie sehen das leere netlogon Verzeichnis des Servers und raus geht es mit „exit”

DHCP-Server einrichten

```
sudo nano /etc/dhcp/dhcpd.conf
```

suchen sie den auskommentierten Eintrag „authoritative;” und kommentieren Sie ihn ein. Weiter unten finden Sie ein Beispiel:

```
# A slightly different configuration for an internal subnet.
#subnet 10.5.5.0 netmask 255.255.255.224 {
#  range 10.5.5.26 10.5.5.30;
#  option domain-name-servers ns1.internal.example.org;
```

```
#  option domain-name "internal.example.org";
#  option subnet-mask 255.255.255.224;
#  option routers 10.5.5.1;
#  option broadcast-address 10.5.5.31;
#  default-lease-time 600;
#  max-lease-time 7200;
#}
```

welches wir anpassen:

```
# A slightly different configuration for an internal subnet.
Subnet 192.168.2XX.0 netmask 255.255.255.0 {
  range 192.168.2XX.100 192.168.2XX.200;
  option domain-name-servers 192.168.2XX.250;
  option domain-name "tnXX.ito";
  option subnet-mask 255.255.255.0;
  option routers 192.168.2XX.1;
  option broadcast-address 192.168.2XX.255;
  default-lease-time 600;
  max-lease-time 7200;
}
```

speichern und den dienst neu starten mit:

```
sudo systemctl restart isc-dhcp-server
```

Benutzer anlegen und Verwalten

Zur Verwaltung der Nutzer der Domäne haben sie (mindestens) 2 Möglichkeiten:

RSAT

Nutzen Sie einen Windows PC, nehmen diesen in die Domäne auf, und nutzen die Remote Server Administration Tools von Microsoft. https://learn.microsoft.com/de-de/troubleshoot/windows-server/system-management-components/remote-server-administration-tools

Diese werden über Features hinzugefügt. Prüfen Sie welcher Installationsweg bei ihrer Windows Version passt. (winver ausführen)

Hiermit können Sie Benutzer, Gruppen und auch Gruppenrichtlinien setzen.

CLI

Über das samba-tool kann mit sudo-rechten ebenfalls das Management erfolgen, allerdings Textbasiert:

Nutzer mit Vor und Nachnamen erstellen und ein Passwort vergeben:

```
sudo samba-tool user add dieterbecker 'passw0rd#' --given-name=Dieter
    --surname=Becker
```

Wenn auf das Passwort und die Genauen Namen verzichtet wird, erfolgt trotzdem ein Passwort Abfrage Dialog.

Das Ganze erweitert um den Profilpfad:

```
sudo samba-tool user add dieterbecker 'passw0rd#' --given-name=Dieter
    --surname=Becker --profile-path='\\tnXX\profiles\dieterbecker'
```

und/oder mit Home-Verzeichnis

```
sudo samba-tool user add dieterbecker 'passw0rd#' --given-name=Dieter
    --surname=Becker --home-drive=U --home-directory='\\tnXX\
    dieterbecker'
```

Nutzer anzeigen:

```
sudo samba-tool user list
```

Nutzer Löschen:

```
sudo samba-tool user delete dieterbecker
```

Passwort ändern:

```
sudo samba-tool user setpassword dieterbecker
```

Gruppe anlegen:

```
sudo samba-tool group add Geschaeftsleitung
```

Gruppe löschen:

```
sudo samba-tool group delete Geschaeftsleitung
```

Nutzer oder Gruppe zu Gruppe hinzufügen:

```
sudo samba-tool group addmembers \"Geschaeftsleitung\" dieterbecker
```

Nutzer aus Gruppe entfernen:

```
sudo samba-tool group removemembers \"Geschaeftsleitung\" dieterbecker
```

Gruppenmitglieder Anzeigen:

```
sudo samba-tool group listmembers \"Geschaeftsleitung\"
```

User auf Ubuntu umsetzen

Damit die Nutzer auch unter Linux verfügbar werden, muss der winbind Dienst wissen, wie die AD-User mit ihren IDs am Server gemappt werden sollen. Daher anpassen der smb.conf:

Unter `[Global]` unter den vorhandenen Einträgen ergänzen:

```
password server = DC1.TNXX.ITO
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
winbind enum groups = yes
winbind cache time = 10
winbind use default domain = yes
winbind nss info = rfc2307
```

Zum übernehmen den Dienst neu starten:

```
sudo systemctl restart samba-ad-dc
```

User testen:

```
getend passwd
```

Gruppen testen:

```
getend group
```

> Es sollten Nutzer und Gruppen mit TNXX auftauchen. Sollte dem nicht der fall sein, bitte in der Datei `/etc/nsswitch.conf` alle Einträge mit `sss` durch `winbind` ersrtzen und dann nochmals versuchen.

Freigaben für die Gruppen erstellen

Damit die Nutzer und Gruppen nun auch Laufwerke bekommen müssen die Verzeichnisse erstellt und Freigegeben werden:

```
sudo mkdir -p /srv/samba/projekte
```

Admins zugang geben:

```
sudo chown root:"TNXX\Domain Admins" /srv/samba/projekte
sudo chmod 0770 /srv/samba/projekte
```

ACL auf Domänenadmins erweitern:

```
sudo setfacl -m g:"TNXX\Domain Admins":rwx /srv/samba/projekte
```

```
2 sudo setfacl -d -m g:"TNXX\Domain Admins":rwx /srv/samba/projekte
```

Und damit die Rechte auch setzbar werden:

```
1 sudo samba-tool privilege grant "TNXX\Domain Admins"
     SeDiskOperatorPrivilege
```

Eintrag in der smb.conf dafür:

```
1 [Projekte]
2 path = /srv/samba/projekte
3 read only = no
4 vfs objects = acl_xattr
5 map acl inherit = yes
6 inherit acls = yes
7 inherit permissions = yes
8 nt acl support = yes
```

Jetzt kann die Freigabe vom Admin mit den Jeweiligen User-Gruppenrechten gesetzt werden. Hierfür in einer Windows-Umgebung die Eigenschaften des Netzlaufwerkes anpassen.

PDF herunterladen