|  |  |  |  |
| --- | --- | --- | --- |
| **Übungsprotokoll**  **SYTS – Server** | | | |
|  | **Übungsdatum:**  KW 45/2022 –  KW 49/2022 | **Klasse:**  4AHIT | **Name:**  Felix Schneider |
| **Abgabedatum:**  6. Dezember 2022  (Nikolaus) | **Gruppe:**  SYTS\_2 | **Note:** |
| **Leitung:**  DI (FH) Alexander MESTL | **Mitübende:**  - | | |
| **Übungsbezeichnung**:  Ubuntu Client der Windows Domain hinzufügen | | | |

**Inhaltsverzeichnis:**

[1 Aufgabenstellung 3](#_Toc121250066)

[2 Abstract (English) 4](#_Toc121250067)

[3 Theoretische Grundlagen 5](#_Toc121250068)

[3.1 SSSD 5](#_Toc121250069)

[3.2 Samba / Winbind 6](#_Toc121250070)

[4 Übungsdurchführung 7](#_Toc121250071)

[4.1 Ubuntu Client aufsetzen 7](#_Toc121250072)

[4.2 (Windows Server aufsetzen) 7](#_Toc121250073)

[4.3 SSSD Variante 7](#_Toc121250074)

[4.3.1 Hostname bearbeiten 7](#_Toc121250075)

[4.3.2 Pakete installieren 8](#_Toc121250076)

[4.3.3 Active Directory-Domäne entdecken 8](#_Toc121250077)

[4.3.4 Server joinen 9](#_Toc121250078)

[4.3.5 SSSD Configuration 10](#_Toc121250079)

[4.3.6 User Directory automatisch hinzufügen 10](#_Toc121250080)

[4.3.7 Kerberos installieren 11](#_Toc121250081)

[4.3.8 Tests 11](#_Toc121250082)

[4.4 Samba / Winbind Variante 12](#_Toc121250083)

[4.4.1 Pakete installieren 12](#_Toc121250084)

[4.4.2 Kerberos konfigurieren 12](#_Toc121250085)

[4.4.3 Samba konfigurieren 13](#_Toc121250086)

[4.4.4 Winbind als Namesquelle 13](#_Toc121250087)

[4.4.5 Home Ordner für User hinzufügen 14](#_Toc121250088)

[5 Kommentar 15](#_Toc121250089)

[5.1 Beichte 15](#_Toc121250090)

[5.2 Hypothetische Fragen 16](#_Toc121250091)

[5.3 SS 17](#_Toc121250092)

# Aufgabenstellung

Um zu testen, wie weit Domänen auch betriebssystemübergreifend betrieben werden können, werden wir nun einen Ubuntu-Client in die Domäne aufnehmen. Das Ziel ist, dass der Client unter den Computer-Konten des AD auftaucht und man sich an ihm statt mit lokalen Unix-Benutzern mit AD-Benutzern anmelden kann.

​Hinweis: die Screenshots im Anhang wurden mit einer 20.04 LTS-Maschine gemacht!

Als ersten Schritt setzt bitte eine VM mit Ubuntu auf (z. B. aktuelles 22.04 LTS) und recherchiert die Pakete die man braucht, um einer Domäne beizutreten.

*(Ihr solltet in der Liste der Pakete, die ihr installieren wollt, auf jeden Fall auch krb5 drin haben - das ist für die Kerberos-Tickets zur Authentifizierung in der Domäne erforderlich. Beim Installieren werden gleich ein paar Basis-Parameter abgefragt, deswegen: Achtung! Es geht um die Domäne, die hier Realm heisst und um die DCs - siehe Screenshot 1! Wer sich vertippt, muss später die /etc/krb5.conf anpassen. Danach muss die Maschine in das "interne Netz" der Domäne. Dann kann man sich bereits ein Kerberos-Ticket ausstellen lassen - siehe Screenshot 2!*

*Dann braucht man "nur mehr" eine passende /etc/samba/smb.conf und schon kann man mit dem Computer-Konto der Domäne beitreten - siehe Screenshot 3!*

*Das klingt sehr einfach - in Wirklichkeit ist es schon einiges an Konfiguration! Das alles findet man aber tiptop beschrieben bei den Ubuntu-, Samba- und Winbind-Dokus.*

*Nach dem Domänenbeitritt sollten die Befehle wbinfo -u und wbinfo -g bereits AD-Benutzer bzw. AD-Gruppen anzeigen. Als nächsten Schritt muss man in der /etc/nsswitch.conf einstellen, dass winbind als "Namensquelle" verwendet wird, dann liefert z. B. auch getent passwd zusätzlich zu den lokalen Benutzern auch die Domänenbenutzer - siehe Screenshot 4.)*

PAM, die Pluggable Authentication Modules, konfigurieren sich in Ubuntu mittlerweile fast von selber, lediglich das Erstellen der User-Home-Laufwerke muss man noch manuell erlauben. In /etc/security/group.conf kann man außerdem einstellen, dass pam\_group die AD-Benutzer in die Unix-Gruppen zur Verwendung von USB-Devices usw. aufnimmt (da sind sie standardmäßig nicht drinnen).

Danach kann man sich mit einem Domänenbenutzer anmelden - siehe Screenshot 5 und 6.

# Abstract (English)

To test the extent to which domains can be operated across operating systems, we will now add an Ubuntu client to the domain. The goal is to have the client show up under the AD computer accounts and to be able to log in to it with AD users instead of local Unix users.

Note: the screenshots in the attachment were made with a 20.04 LTS machine!

As a first step, please set up a VM with Ubuntu (e.g. current 22.04 LTS) and research the packages you need to join a domain.

(You should definitely have krb5 in the list of packages you want to install - this is required for the Kerberos tickets to authenticate in the domain. During installation you will be asked for some basic parameters, therefore: Attention! It's about the domain, which is called realm here, and about the DCs - see screenshot 1! If you make a mistake, you have to change /etc/krb5.conf later. After that the machine has to be in the "internal network" of the domain. Then you can already get a Kerberos ticket - see screenshot 2!

Then you "only" need a matching /etc/samba/smb.conf and you can join the domain with your computer account - see screenshot 3!

This sounds very simple - in reality it is quite some configuration! All this is described in the Ubuntu, Samba and Winbind docs.

After joining the domain, the commands wbinfo -u and wbinfo -g should already show AD users or AD groups. The next step is to set /etc/nsswitch.conf to use winbind as "name source", then e.g. getent passwd will also return domain users in addition to local users - see screenshot 4).

PAM, the Pluggable Authentication Modules, configure themselves in Ubuntu, only the creation of user home drives must be allowed manually. In /etc/security/group.conf you can also configure pam\_group to include AD users in the Unix groups for using USB devices etc. (they are not in there by default).

After that you can log in with a domain user - see screenshot 5 and 6.

# Theoretische Grundlagen

Wir wollen einen Ubuntu Client, zum Beispiel Ubuntu 20.04 LTS, einer Windows Domain hinzufügen, sodass wir uns auf dem Ubuntu Client mit AD-Benutzern einloggen können.

Hierfür können mehrere verschiedene Lösungswege versucht werden:

* Samba / Winbind
* SSSD
* Automatischer Beitritt beim Aufsetzen

Der automatische Beitritt wäre zu einfach, weil man einfach eine Checkbox anhaken muss:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Damit die Ubuntu Maschine dem Windows Server beitreten kann, müssen natürlich ein paar logische Voraussetzungen eingestellt werden:

* Beide Maschinen benötigen eine Netzwerkkarte, welche ins gleiche **interne Netzwerk** führt, eine zweite Netzwerkkarte, die geNATet ist, ist nicht zwingend, aber empfehlenswert, weil man dadurch die notwendige Internetverbindung hat, um die notwendigen Pakete zu installieren.
* Der Windows Server muss **DNS** richtig konfiguriert haben, um den Domainennamen auch auflösen zu können.

Damit man sich schlussendlich anmelden kann, muss man **Kerberos** konfigurieren, um ein gültigest Ticket zu erhalten, mit welchem man sich im der Domain anmelden kann.

## SSSD

Hierfür benötigt man einige Softwarepackete, wie zum Beispiel sssd-ad, sssd-tools und **realm**, sowie adcli. Und anschließend kann man schon der Domain joinen. Das REALM Service übernimmt sehr viele Konfigurationen, wie zum Beispiel, die pam und nss Module und die **SSSD** Konfiguration.

## Samba / Winbind

Wenn man mithilfe von Winbind der Windows Domaine beitreten will, muss man einige Konfigurationen in diesen Dateien tätigen:

* /etc/krb5.conf – Kerberus ist für die Authentifizierung an der Windows Domain zuständig. Ohne Kerberus könnte man sich nicht am Ubuntu Client mit Domainenbenutzern anmelden. Beim Installieren des Packets werden alle Konfigurationen automatisch abgefragt.
* **/etc/samba/smb.conf** – Hier wird winbind konfiguriert. Unter anderem muss man den Domainenname, NetBIOS-Namen, Realm und Hostnamen angeben und zusätzliche Felder konfigurieren
* /etc/nsswitch.conf – Hier muss man von sssd alles auf winbind umstellen
* /etc/pam.d/common-session (optional) – Hier kann man das Automatische Hinzufügen des „Homedirectories“ einstellen, damit der User z.B. auf /home/%U sein Verzeichnis findet.
* /etc/netplan/01-netcfg.yaml – Hier muss man DNS Einstellungen treffen, damit diese auf das Active Directory verweisen.

# Übungsdurchführung

## Ubuntu Client aufsetzen

Während bei anderen Protokollen normalerweise bei diesem Schritt ein Verweis auf ein anderes Protokoll vorliegt, kommt hier ein Wissensfakt:

VMBOX 7.0.0 bietet die neue Möglichkeit, dass Virtuelle Maschinen automatisch aufgesetzt werden. Dafür muss man nur die ISO, den RAM, den dynamischen Festplattenspeicher, einen Benutzer und paar weitere Einstellungen auswählen bzw. eingeben. Bis dahin alles ganz fein…

ALLERDINGS! Es ist nach dieser automatischen Installation nicht einmal möglich, das Terminal zu starten, weil es angeblich Probleme mit den Gast-Editions gibt.

Aus diesem Grund kommt hier nun ein Verweis auf ein Protokoll mit einer manuellen Installation eines Ubuntu Clients: [..\SYTB\2. Klasse\SYTB\_Protokoll\_2Ubuntu\_FelixSchneider.docx](../SYTB/2.%20Klasse/SYTB_Protokoll_2Ubuntu_FelixSchneider.docx).

## (Windows Server aufsetzen)

Anleitung: <https://htlkrems3500-my.sharepoint.com/personal/f_schneider_htlkrems_at/Documents/Schule/SYTB/3.%20Klasse/SYTB_Protokoll_8_WindowsServer.pdf>

## SSSD Variante

<https://ubuntu.com/server/docs/service-sssd-ad>

### Hostname bearbeiten

<NameUbunut>.<DomainName>

Wie Sie sehen können, bekommt der Ubuntu Client als Hostnamen bereits den Domainnamen angehängt, damit er später der Domaine auch joinen kann.

sudo hostnamectl set-hostname 23ubuclt.htl.com

Mit dem Befehl „hostnamectl“ sehen Sie nochmals wichtige Informationen bzgl. der VM:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

DNS haben wir bei Ubuntu nicht speziell konfiguriert, das ist auch nicht notwendig, da ja der Windows Server unser Domain Name Service - Server ist.

Um zu überprüfen, ob der Domain Name Service – Server auch richtig gefunden wurde, können wir diesen Befehl verwenden („| grep Current“ ist optional, es beschränkt nur die Suche):

systemd-resolve --status | grep Current

Hier sehen Sie den DNS Server 192.168.23.1 (der andere kommt von der NAT Netzwerkkarte):

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

### Pakete installieren

Damit diese betriebssystem-unterschiedlichen Maschinen auch in einer Domain sein können, gibt es mehrere Möglichkeiten (sssd, winbind, …), die als Pakete bei Ubuntu einfach zu installieren sind.

sudo apt update

sudo apt -y install realmd libnss-sss libpam-sss sssd sssd-tools adcli samba-common-bin oddjob oddjob-mkhomedir packagekit

### Active Directory-Domäne entdecken

Wie Sie sehen entdeckt der Ubuntu Client die Domain des Server, außerdem können Sie hier nochmals die notwendigen (required-package) Pakete sehen:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

### Server joinen

Joinen Sie dem Server und melden Sie sich mit dem Administrator Account an:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Wie Sie sehen sind Sie dem Server gejoined:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

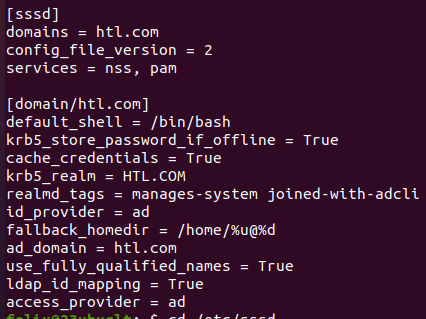
Auch im AD sieht man, dass der Ubuntu Client gejoined ist:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

### SSSD Configuration

In der Datei /etc/sssd/sssd.conf sieht man die Konfiguration des Services sssd. Darunter findet man zum Beispiel die Domain und Einstellungen bzgl. Cache (damit man sich auch anmelden kann, wenn Server offline), Qulifikationsname, Access Provider und mehr…



Die Permissions dieser Datei müssen 0600 sein und der Owner ist root:root.



### User Directory automatisch hinzufügen

Dieser Befehl fügt beim Anmelden eines Benutzers am Ubuntu Client automatisch seinen zugeordneten /home Folder hinzu, damit der User auch auf seine Daten zugreifen kann.



### Kerberos installieren

Damit Sie ein gültiges Kerberos Ticket erhalten müssen Sie das Packet krb5-user installieren. Dieses benötigen Sie zur Authentifizierung in der Domaine.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

### Tests

Nachdem Sie diese Schritte vollendet haben, sollte nun alles funktioniert:

1. Sie können Benutzerinformationen über den Ubuntu Client herausfinden
2. Sie können sich am Ubuntu Client mit einem AD Benutzer anmelden
3. Sie haben Zugriff auf das /home Verzeichnis des angemeldeten Benutzers

Also ist alles so, als wären Sie auf einem Windows Client angemeldet, nur besser, weil das Betriebssystem Ubuntu heißt…

Bei mir hat leider nach dem Beitritt zur Domain das Informationsabfragen und das Anmelden nicht funktioniert, deswegen hier ein Beispielscreenshot, wie es aussehen sollte (DANKE Vocki!):

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

## Samba / Winbind Variante

<https://www.server-world.info/en/note?os=Ubuntu_20.04&p=samba&f=4>

Da die SSSD Variante nicht viel Erfolg zeigt, habe ich zusätzlich auch noch die Samba-Variante ausprobiert, wie es ursprünglich in der Angabe als *kursiver Auftrag* angewiesen war… [auch diese Variante hat bei mir nicht funktioniert, weil schlussendlich der Ubuntu Client keine IP-Adresse mehr bekommen hat (siehe SS ganz zum Schluss)].

### Pakete installieren

Hierfür muss man wieder eine Reihe an Paketen installieren:

sudo apt -y install winbind libpam-winbind libnss-winbind krb5-config samba-dsdb-modules samba-vfs-modules

### Kerberos konfigurieren

Anschließend kommen bei der Installation des krb5-config Pakets einige Fragen bzgl. der Kerberos Konfiguration. Da ich diese nicht als Screenshot habe, sehen Sie hier die /etc/krb5.conf-Datei, welche die gleichen Informationen enthält, die Sie angeben sollten:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Hierbei sehen Sie, dass Sie als Kerberos Realm HTL.COM einstellen müssen. Außerdem müssen Sie beim Kerberos Server für Ihr Realm den dc-master eintragen und da dieser in unserem Fall auch der administrative Server ist, müssen Sie auch dort „dc-master“ eingeben.

### Samba konfigurieren

Die wichtigste Konfiguration findet dann in der Datei /etc/samba/smb.conf statt:

*Ein Bild, das Text enthält.

Automatisch generierte Beschreibung*

Auch hier müssen Sie wiederholt Domainname, Realmname und NetBIOS Name eintragen.

### Winbind als Namesquelle

In der Datei /etc/nsswitch.conf müssen Sie konfigurieren, dass winbind die Namensquelle ist. Anschließend sollte man mittel Befehlen, wie zum Beispiel „getent passwd [clemens@htl.com](mailto:clemens@htl.com)“ oder „groups [clemens@htl.com](mailto:clemens@htl.com)“, Informationen bzgl. Benutzer und Gruppen herausfinden können.

*Ein Bild, das Text enthält.

Automatisch generierte Beschreibung*

### Home Ordner für User hinzufügen

PAM, die Pluggable Authentication Modules, bieten die Möglichkeit, das /home/%U Verzeichnis komplett automatisch nach dem erfolgreichen Anmelden zu erstellen, sodass der Nutzer Zugriff auf seine Daten hat. Heutzutage muss man hierfür nicht mehr viel konfigurieren, ausschließlich der /etc/pam.d/common-session-Datei:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Die Zeile „session optional pam\_mkhomedir.so“ sorgt dafür, dass das Verzeichnis automatisch eingebunden wird.

# Kommentar

## Beichte

Bei mir hat diesmal alles funktioniert, bis auf die entscheidenden letzten Schritte: Das Anmelden selbst. Das ist halt dadurch noch trauriger als es ohnehin schon ist, weil das eigentlich der entscheidende Punkt der Übung gewesen wäre. Weshalb das nicht funktioniert, kann ich beim besten Willen nicht erklären, ich kann nur folgende Daten liefern:

* Ich habe insgesamt für diese Übung drei Windows Server und vier Ubuntu Clients neu aufgesetzt und eingerichtet. Teilweise hat mich das sogar einen Schritt weitergebracht, doch für den letzten Schritt fehlt mir die Zeit und Hoffnung…
* Ubuntu Client ist 100%ig der Domaine beigetreten (SSSD Variante)

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

* Nichtsdestotrotz bekomme ich keine Benutzerinformationen und (wie Sie in der Angabe beschrieben habe) keine Auflistung der Benutzer oder Gruppen



Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Damit ich mich trotz der Unfunktionalitäten meiner Konfigurationen etwas beruhigter fühle, hat mir Alex einen Screenshot geschickt, weil bei ihm die Übung doppelt (also zwei Mal) funktioniert hat:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

## Hypothetische Fragen

Zwei hypothetische Fragen: Wenn jetzt bei jeder Übung in diesem Schuljahr bei mir etwas nicht funktioniert, obwohl ich alles drei Mal geprüft und versucht habe, bekomme ich dann auf jedes Protokoll bestenfalls eine 2? Würde ich dann wirklich wegen unbekannter Fehler eine 2 ins Zeugnis bekommen?

Andere Frage: Wie kann man den Titel des Protokolls anpassen, weil da immer noch „SYTx\_Protokoll\_Vorlage“ steht… 😊

## SS

Ich habe noch nie einen Screenshot gemacht, der so viele Fehler aufweist wie dieser 😊:Ein Bild, das Text enthält.

Automatisch generierte Beschreibung