


Übungsprotokoll

SYTS – Server

	Übungsdatum: KW 18/2022 – KW /2022	Klasse: 4AHIT	Name: Felix Schneider
	Abgabedatum: 11.10.2022	Gruppe: SYTS_2	Note:
Leitung: DI (FH) Alexander MESTL	Mitübende: -		
Übungsbezeichnung: Debian DC mit Samba			

Inhaltsverzeichnis:

1	Aufgabenstellung.....	3
2	Abstract (English).....	3
3	Theoretische Grundlagen	4
4	Übungsdurchführung	5
4.1	Setup Debian	5
4.2	Downgrade Win Server	6
4.3	Install necessary packages.....	7
4.4	Config Interfaces and DNS.....	7
4.5	Config KRB5	8
4.6	Connect to DC with Kerberos Ticket.....	9
4.7	Win Client: Install RSAT	10
5	Ergebnisse.....	13
6	Code.....	13
7	Kommentar.....	13

1 Aufgabenstellung

Unser bestehendes Unternehmensnetzwerk soll um einen zweiten DC erweitert werden.

Dazu setzen wir eine Debian-Maschine auf, installieren und konfigurieren Samba im AD-Modus und werden den Server über RSAT administrieren.

Es gibt dazu einige sehr gute Anleitungen (ein Beispiel ist hier als Ressource angeführt), der Teufel liegt aber wie so oft im Detail!

2 Abstract (English)

Our existing company network is to be extended by a second DC.

To do this, we will set up a Debian machine, install and configure Samba in AD mode and administer the server via RSAT.

There are some very good instructions on how to do this (one example is listed here as a resource), but as so often, the devil is in the detail!

3 Theoretische Grundlagen

Um eine Debian-Maschine als Domain Controller in einem Active Directory zu konfigurieren, benötigen Sie grundlegendes Wissen über die folgenden theoretischen Grundlagen:

- **Active Directory:** Active Directory (AD) ist ein Verzeichnisdienst von Microsoft, der Benutzerkonten, Computer und andere Netzwerkressourcen zentral verwaltet. Es ist wichtig, die grundlegenden Konzepte, Funktionen und Komponenten des Active Directory zu verstehen, um einen Domain Controller zu konfigurieren.
- **Domain:** Eine Domain ist eine logische Organisationseinheit in einem Active Directory. Sie enthält eine Gruppe von Computern, Benutzern, Gruppenrichtlinien und anderen Ressourcen, die in einer hierarchischen Struktur organisiert sind. Verstehen Sie die Struktur und Hierarchie einer Domain und wie sie sich auf die Konfiguration des Domain Controllers auswirken kann.
- **DNS:** Das Domain Name System (DNS) ist ein Netzwerkprotokoll, das den Namen einer Netzwerkressource in deren IP-Adresse auflöst. In einem Active Directory fungiert DNS als wichtiger Bestandteil für die Namensauflösung und die Standortbestimmung von Active Directory-Domänencontrollern. Kenntnisse über DNS-Konzepte, -Zonen, -Einträge und -Auflösung sind entscheidend, um einen Debian-Domain-Controller richtig zu konfigurieren.
- **LDAP:** Das Lightweight Directory Access Protocol (LDAP) ist ein Protokoll, das für den Zugriff auf und die Verwaltung von Verzeichnisdiensten verwendet wird. LDAP wird häufig in Active Directory-Umgebungen eingesetzt, um Benutzer, Gruppen und andere Objekte im Verzeichnis zu suchen und zu verwalten. Verstehen Sie die grundlegenden LDAP-Konzepte und -Funktionen, um eine Debian-Maschine als Domain Controller zu konfigurieren.
- **Samba:** Samba ist eine Open-Source-Software, die die Kommunikation zwischen Linux/Unix-basierten Systemen und Windows-basierten Systemen ermöglicht. Samba kann verwendet werden, um eine Debian-Maschine als Domain Controller in einem Active Directory zu konfigurieren. Erfahren Sie mehr über Samba und die Konfigurationsoptionen, um eine reibungslose Integration in das Active Directory zu gewährleisten.
- **RSAT:** Die Remote Server Administration Tools ermöglichen das Administrieren jedes Servers in einer Domain von einem anderen Computer aus. Dabei muss man nur die zusätzlichen Features installieren.

Es ist wichtig zu beachten, dass die Konfiguration eines Debian-Domain-Controllers in einem Active Directory komplex sein kann und tiefergehendes technisches Wissen erfordert. Es wird empfohlen, sich mit den offiziellen Dokumentationen von Debian, Samba und dem Active Directory vertraut zu machen, um detaillierte Anleitungen und Anweisungen zur Konfiguration zu erhalten.

4 Übungsdurchführung

4.1 Setup Debian

64-Bit-PC Netinst-ISO, 32

New

Create Virtual Machine

Name and operating system

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: 23DebDC

Machine Folder: C:\Users\trueberryless\VirtualBox VMs

Type: Linux

Version: Debian (64-bit)

2048 MB

Create a virtual hard disk now

can leave this setting unchanged.

VDI (VirtualBox Disk Image)

Dynamically allocated

16.00 GB

Expert Mode Next Cancel



Controller: IDE

IDE Secondary Device 0: [Optical Drive] debian-11.7.0-amd64-netinst.iso (389.00 MB)

Graphical install

Install

Hostname: debian

Domain name: htl.com

Username	Password
root	toor
felix	xilef

Package Manager Server: Austria

GNOME (GUI)

4.2 Downgrade Win Server

Um den Windows Server herunter zu stufen, muss man zuerst den Forest auf die alte Version – in unserem Fall 2008R2 setzen – und anschließend die Domain runter setzen. Mehr Informationen zu diesen Befehlen finden Sie [hier](#).

```
PS C:\Users\Administrator> Set-ADForestMode -Identity htl.com -ForestMode Windows2008Forest

Bestätigung
Möchten Sie diese Aktion wirklich ausführen?
Ausführen des Vorgangs "Set" für das Ziel "CN=Partitions,CN=Configuration,DC=htl,DC=com".
[Y] Ja [A] Ja, alle [N] Nein [K] Nein, keine [H] Anhalten [?] Hilfe (Standard ist "J"): a
PS C:\Users\Administrator> Get-ADForest | select Name,ForestMode

Name          ForestMode
----          -
htl.com Windows2008Forest

PS C:\Users\Administrator> Get-ADDomain | select DNSRoot,DomainMode

DNSRoot          DomainMode
-----          -
htl.com Windows2012R2Domain

PS C:\Users\Administrator> Set-ADForestMode -Identity htl.com -ForestMode Windows2008R2Forest

Bestätigung
Möchten Sie diese Aktion wirklich ausführen?
Ausführen des Vorgangs "Set" für das Ziel "CN=Partitions,CN=Configuration,DC=htl,DC=com".
[Y] Ja [A] Ja, alle [N] Nein [K] Nein, keine [H] Anhalten [?] Hilfe (Standard ist "J"): a
PS C:\Users\Administrator> Get-ADForest | select Name,ForestMode

Name          ForestMode
----          -
htl.com Windows2008R2Forest

PS C:\Users\Administrator> Set-ADDomainMode -Identity htl.com -DomainMode Windows2008R2Domain

Bestätigung
Möchten Sie diese Aktion wirklich ausführen?
Ausführen des Vorgangs "Set" für das Ziel "DC=htl,DC=com".
[Y] Ja [A] Ja, alle [N] Nein [K] Nein, keine [H] Anhalten [?] Hilfe (Standard ist "J"): a
PS C:\Users\Administrator> Get-ADDomain | select DNSRoot,DomainMode

DNSRoot          DomainMode
-----          -
htl.com Windows2008R2Domain
```

4.3 Install necessary packages

In diesem Code Beispiel sehen Sie alle notwendigen Pakete:

```
apt-get install acl attr samba winbind libpam-winbind libnss-winbind  
krb5-config krb5-user dnsutils python3-setproctitle
```

Des Weiteren benötigen Sie ein Time Protokoll, damit die Domain Controller eine auf 5min genaue gleiche Uhrzeit haben:

```
apt-get install ntp
```

4.4 Config Interfaces and DNS

Stellen Sie sicher, dass ein Netzwerkinterface mit dem Server verbunden ist, sodass Sie diesen DNS-Server nutzen können.

```
auto enp0s3  
iface enp0s3 inet dhcp  
  
auto enp0s8  
iface enp0s8 inet static  
    address 192.168.23.4  
    netmask 255.255.255.0  
~
```

Damit sollten Sie htl.com auflösen können:

```
root@debian:~# ip -c a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP  
    group default qlen 1000  
    link/ether 08:00:27:67:9d:f2 brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3  
        valid_lft 86223sec preferred_lft 86223sec  
    inet6 fe80::a00:27ff:fe67:9df2/64 scope link  
        valid_lft forever preferred_lft forever  
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP  
    group default qlen 1000  
    link/ether 08:00:27:51:53:9c brd ff:ff:ff:ff:ff:ff  
    inet 192.168.23.4/24 brd 192.168.23.255 scope global enp0s8  
        valid_lft forever preferred_lft forever  
    inet6 fe80::a00:27ff:fe51:539c/64 scope link  
        valid_lft forever preferred_lft forever
```

```
root@debian:~# nslookup htl.com  
Server:          192.168.23.1  
Address:         192.168.23.1#53  
  
Name:   htl.com  
Address: 192.168.23.1  
Name:   htl.com  
Address: 10.0.3.15
```

4.5 Config KRB5

In der Datei `/etc/krb5.conf` müssen Sie einerseits diese Konfiguration in den ersten paar Zeilen setzen:

```
[libdefaults]
    dns_lookup_realm = false
    dns_lookup_kdc = true
    default_realm = HTL.COM
```

Andererseits müssen Sie noch die Server für die Domain konfigurieren:

```
[realms]
    HTL.COM = {
        kdc = dc-master.htl.com
        admin_server = dc-master.htl.com
    }
```

Löschen Sie die Samba Konfiguration (`/etc/samba/smb.conf`), da diese beim Verbinden mit dem Windows Domain Controller automatisch generiert wird.

Anschließend konfigurieren Sie `/etc/resolv.conf` folgendermaßen und deaktivieren Sie den NetworkManager oder verändern Sie die Schreibberechtigungen für diese Datei, damit sie nicht mehr vom System verändert wird.

```
domain htl.com
search htl.com
nameserver 192.168.23.1
```

```
# Deactivate NetworkManager
Systemctl disable --now NetworkManager

# Or change permissions
Chattr +i /etc/resolv.conf
```


4.6 Connect to DC with Kerberos Ticket

Fordern Sie nun ein Kerberos Ticket an, mit welchem Sie sich anschließend zum DC verbinden können:

```
kinit Administrator
```

Geben Sie anschließend das Passwort des Administratorkontos des DCs ein (Admin123).

```
root@debian:~# kinit Administrator
Password for Administrator@HTL.COM:
root@debian:~# klist

Ticket cache: FILE:/tmp/krb5cc_0
Default principal: Administrator@HTL.COM

Valid starting     Expires            Service principal
06/02/2023 01:32:07 06/02/2023 11:32:07  krbtgt/HTL.COM@HTL.COM
    renew until 06/03/2023 01:32:03
```

```
samba-tool domain join htl.com DC -U"HTL\Administrator"
```

Nun sollte am Windows Server der Debian Computer auftauchen:









Active Directory-Benutzer und -gruppen	Name	Typ	Domänencont...	Standort	Beschreibung
> Gespeicherte Abfragen	DC-MASTER	Computer	GC	Default-First-Si...	
v htl.com	DEBIAN	Computer	GC	Default-First-Si...	
> Built-in					
> Computers					
> Domain Controllers					
> ForeignSecurityPrincipal:					
> Managed Service Account					
> Users					

4.7 Win Client: Install RSAT

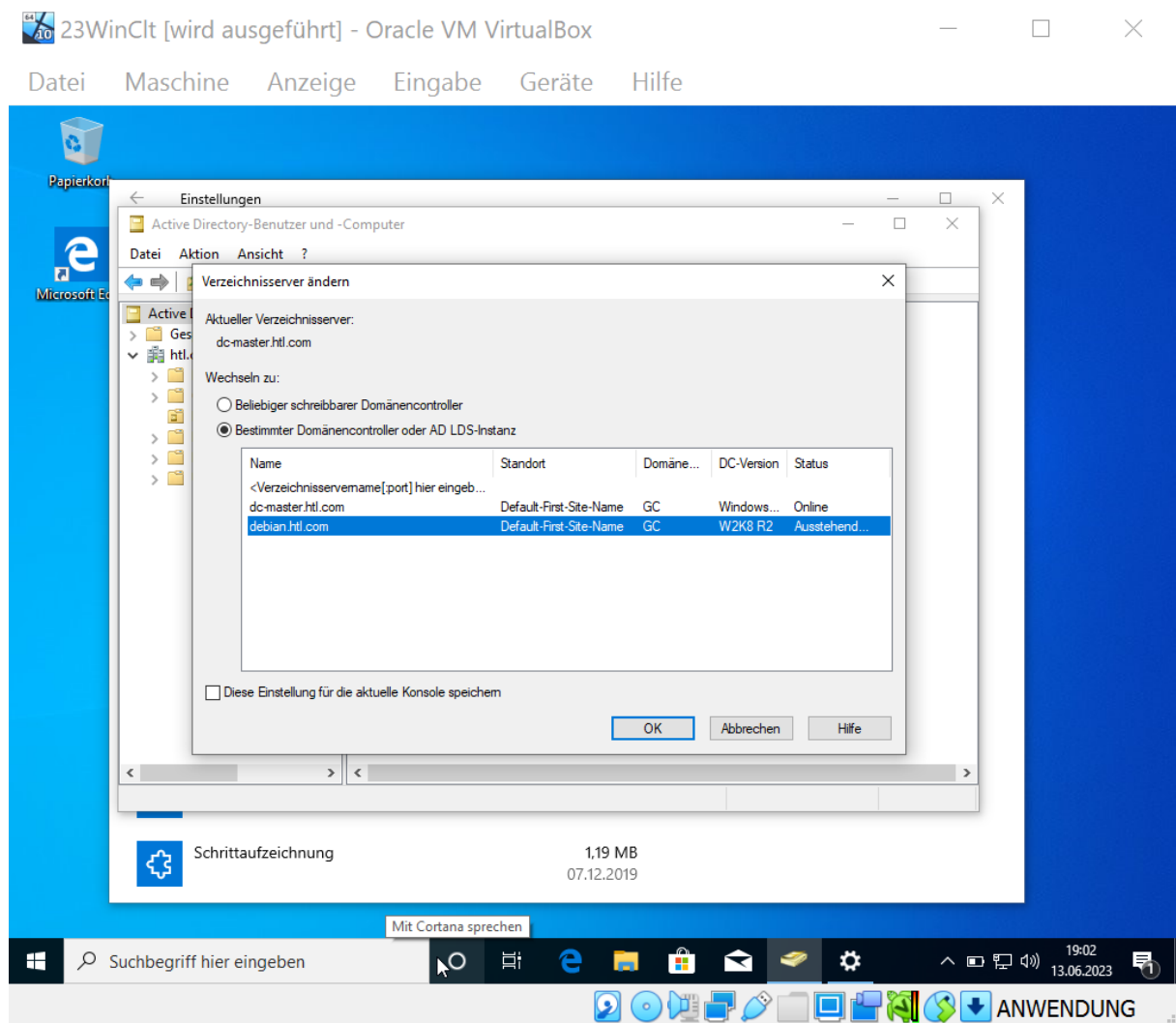
Die **Remote Server Administration Tools** ermöglichen – wie der Name schon sagt – das remote verwalten der Server. Deswegen installieren wir diese auf einem Client in der Domain und verwalten dann den Debian Samba Domain Controller Server.

Gehen Sie dafür in die „Apps & Features“ → „optionale Features“ → „Features hinzufügen“ und fügen Sie folgende Features hinzu:

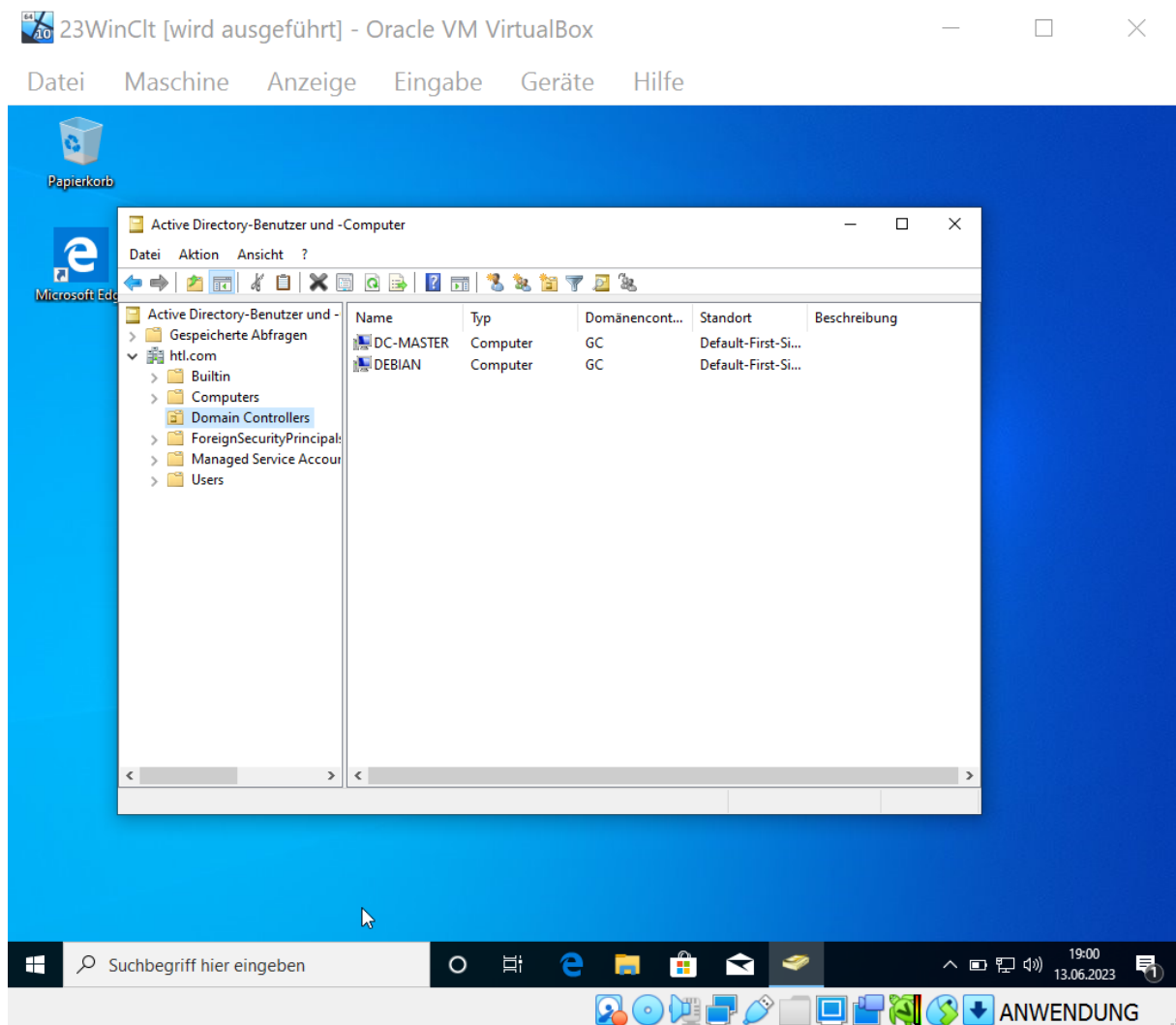
- RSAT Server Manager
- RSAT DHCP
- RSAT DNS
- RSAT Active Directory
- RSAT Gruppenrichtlinien

Optionale Features		
		07.12.2019
	Microsoft-Remotehilfe	2,89 MB 07.12.2019
	OpenSSH-Client	10,1 MB
	RSAT: DHCP-Servertools	13,7 MB 13.06.2023
	RSAT: DNS-Servertools	11,8 MB 13.06.2023
	RSAT: Server-Manager	59,3 MB 13.06.2023
	RSAT: Tools für Active Directory Domain Services und Lightweight Directory Services	33,0 MB 13.06.2023
	RSAT: Tools zur Gruppenrichtlinienverwaltung	36,0 MB 12.06.2023

Nachdem man diese Windows Features installiert hat, kann man über das Startmenu ganz normal – wie beim Server – auf die Features zugreifen (unter der Voraussetzung, dass man mit einem **Administratorkonto** angemeldet ist – sonst könnte ja jeder Benutzer irgendetwas einstellen). Beispielsweise kann man „Active Directory Domain Services“ aufrufen und anschließend die Domain und den Server, welchen man konfigurieren will, auswählen.



Anschließend kann man alle Aktionen wie auf einem Windows Server managen.



5 Ergebnisse

Die Virtuelle Maschine mit Debian als Betriebssystem ist erfolgreich der Domain als Domain Controller beigetreten und hilft dieser als redundanter Server gegen einen Ausfall. Somit wissen wir nun, dass auch UNIX Server einem Active Directory nicht nur beitreten, sondern auch administrieren können.

6 Code

- Forest / Domain Mode ändern bzw. Hinauf- / Hinunterstufen:
<https://azurecloudai.blog/2019/10/30/downgrading-active-directory-domain-and-forest-functional-levels-part-2/>
- Samba und andere notwendige Pakete installieren (Debian / Ubuntu):
https://wiki.samba.org/index.php/Distribution-specific_Package_Installation#Debian/Ubuntu
- Berechtigungen ändern:

```
Chattr +i /etc/resolv.conf
```

- AD joinen (Kerberos Ticket):

```
kinit Administrator
```

```
samba-tool domain join htl.com DC -U"HTL\Administrator"
```

7 Kommentar

Dies war eine der einfacheren Übungen. Nichtsdestotrotz hat mir eine grundlegende Erklärung / Auffrischung von RSAT bei dieser Übung gefehlt. Aber vielleicht war ich ja einmal abwesend...