Studienprogramm Sachbearbeiter:in Digitale Forensik
Praktikum Betriebssysteme
Dozent: Leander Hossfeld
hossfeld@hs-mittweida.de
Stand: 20.04.2023

HOCHSCHULE MITTWEIDA
University of Applied Sciences

Betriebssysteme

Praktikum 5 (Teil 2)

In diesem Praktikum lernen Sie die Nutzung der LDAP Lightweight Services zum Einlesen einer AD Datenbank eines DC auf einem Client PC, kennen.

Vorbereitung

Nutzen Sie bitte für die Bearbeitung die bereitgestellte Windows VM:

https://download.hs-mittweida.de/intranet/lehre/CB/Bodach/BKA%20Studiengang/Betriebssysteme/Praktikum%20Blockwochen/Windows/Windows10-Pwnd.ova

Zusätzlich finden Sie hier die für das Praktikum zu nutzende ISO-Datei **PRBlock2.iso**:

https://download.hs-mittweida.de/intranet/lehre/CB/Bodach/BKA%20Studiengang/Betriebssysteme/Praktikum%20Blockwochen/Windows/PRBlock2.iso

Allgemeine Hinweise

Kopieren Sie bitte die **Windows10-BS-Pwnd.ova** Datei und die ISO Datei **PRBlock2.iso** auf ihre lokale Festplatte in ein separates Verzeichnis, auf das Sie Zugriff haben, bestenfalls Laufwerk D:.

Sachverhalt

Von einem Actice Directory Domain Controller Server sollen die Datenbank Eintragungen überprüft und der Nutzer mit der SID -1771 ermittelt werden.

Um was für einen Windows Server handelt es sich, von dem die lokalen Kopien der NTDS.dit Datenbank stammen?

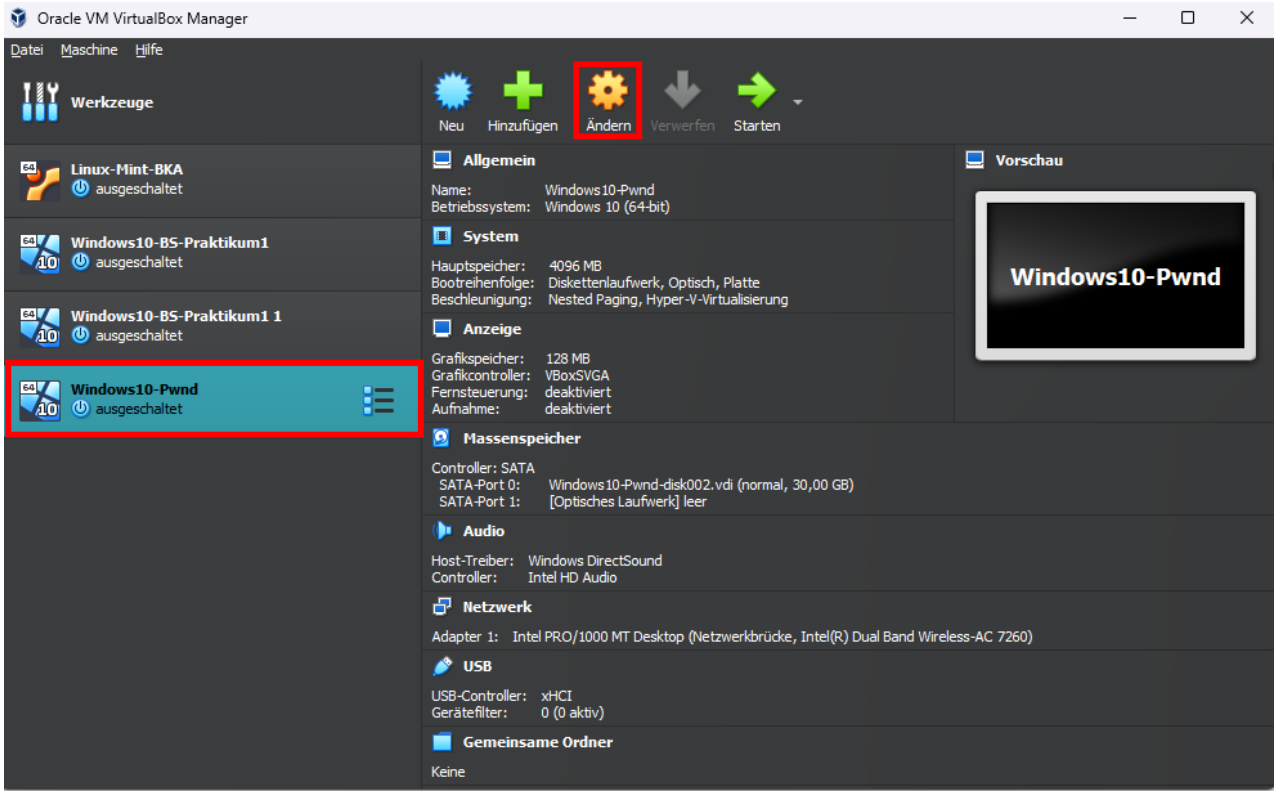
Inhaltsverzeichnis

1. Aufgabenstellung vorbereiten

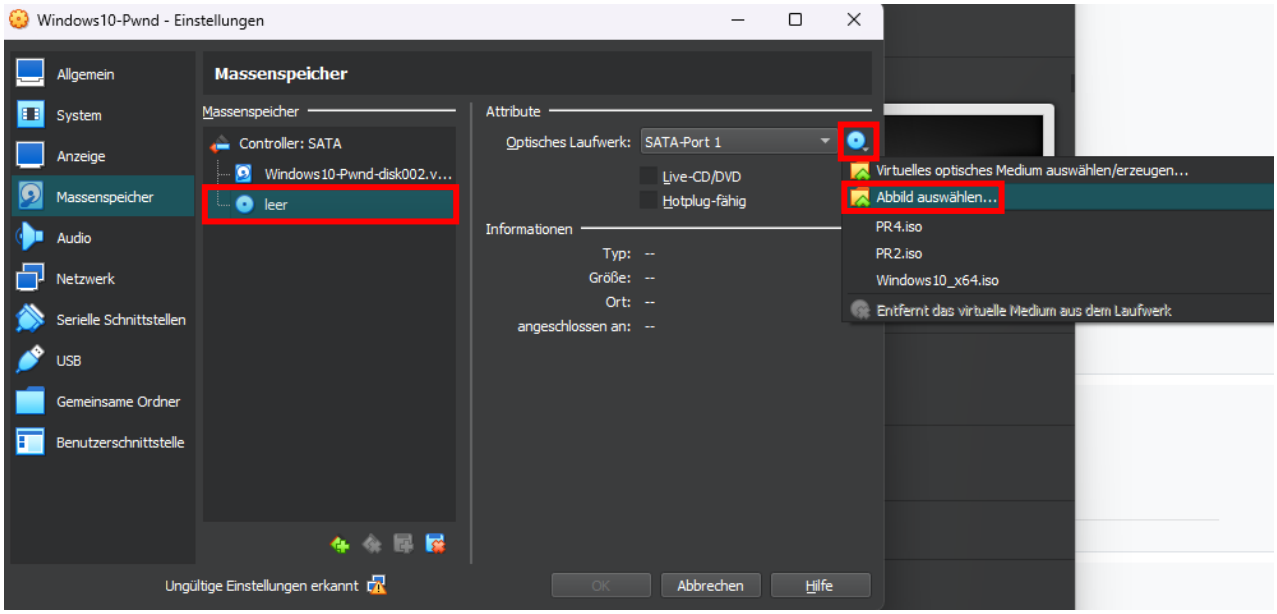
Öffnen Sie Virtualbox.

Importieren Sie zuerst die OVA-Datei.

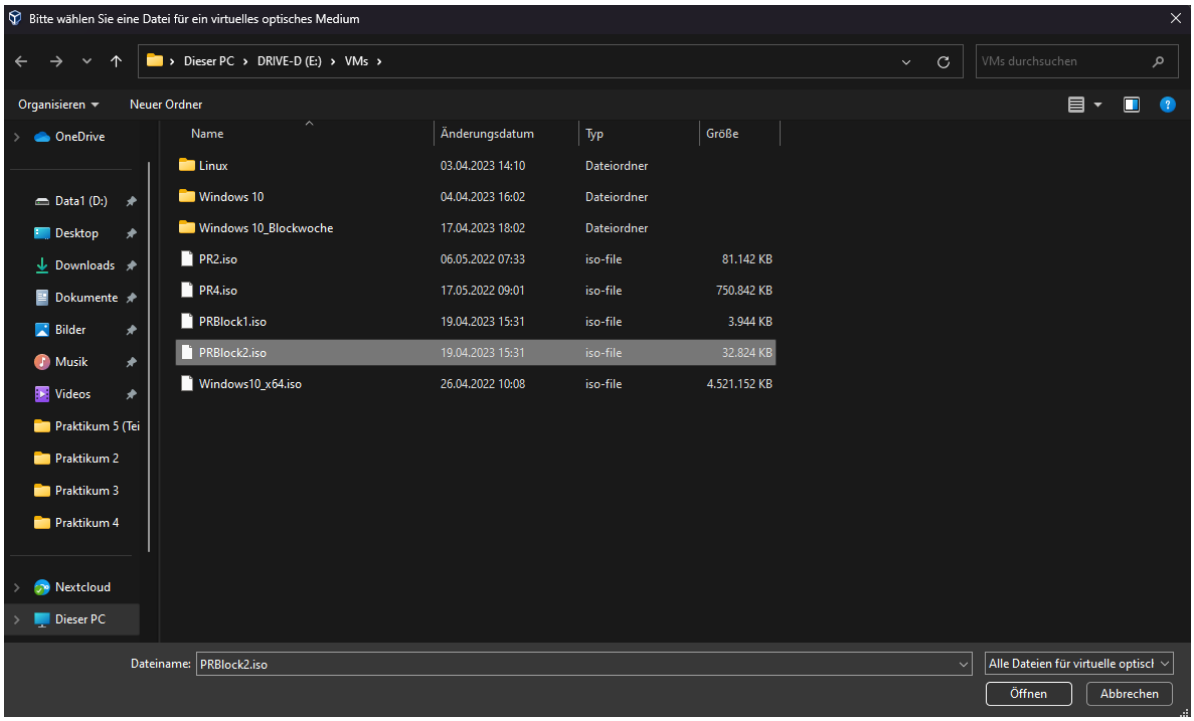
Wählen dann die VM Windows-10-BS-Pwnd aus. Gehen Sie auf **Ändern** (nicht Doppelklicken auf die VM, das würde diese Starten).

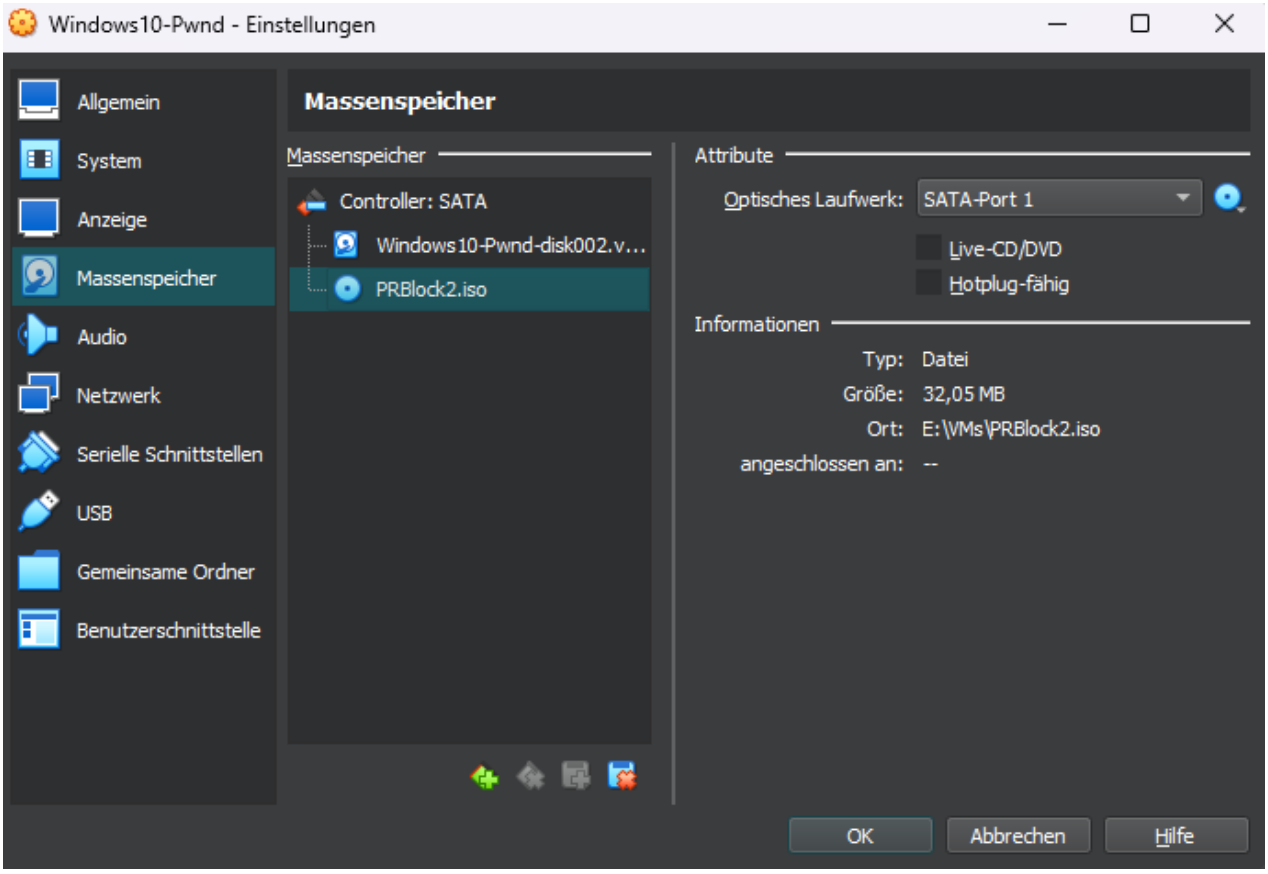


- Wählen Sie den Massenspeicher aus



- Binden Sie bei der CD die heruntergeladene Abbilddatei **PRBlock2.iso** ein





2. Aufgabenstellung Durchführung

2.1 Datenbank Datei vorbereiten

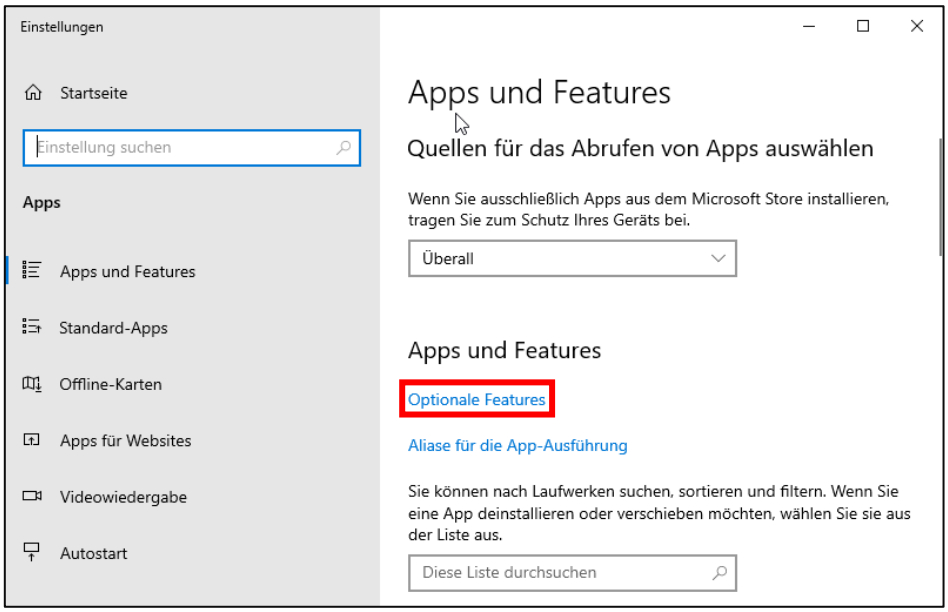
Aufgabe soll es sein eine gesicherte Active Directory Datenbank von einem Domänen Controller auf einem Client PC einzulesen und Zugriff auf die Datenbank zu erhalten.

Die zu nutzende Datenbank ntds.dit befindet sich auf der CD im Verzeichnis ntds.

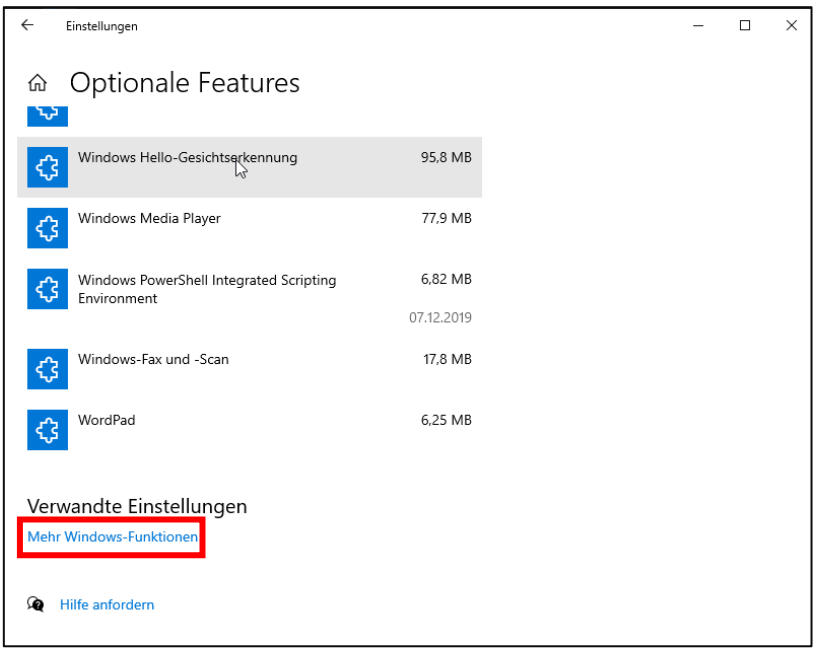
Bitte kopieren Sie diese Datenbank auf den Desktop von Nutzer 1.

2.2 Installation der LDAP-Tools von den Windows Features

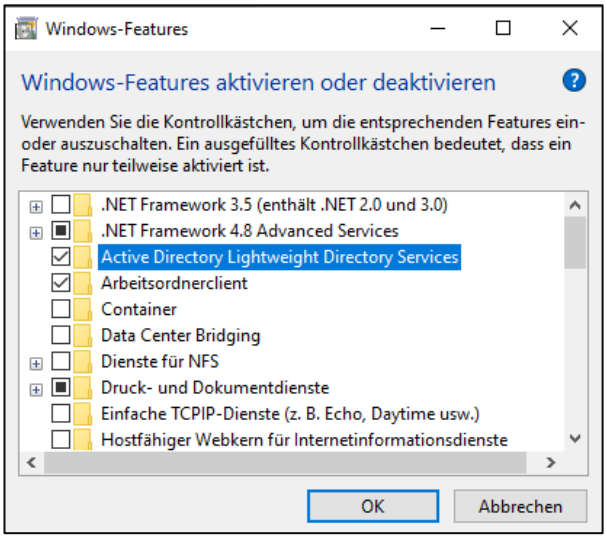
Rufen Sie über Rechtsklick auf den Start Button Apps & Features auf.



Wählen Sie Optionale Features aus.

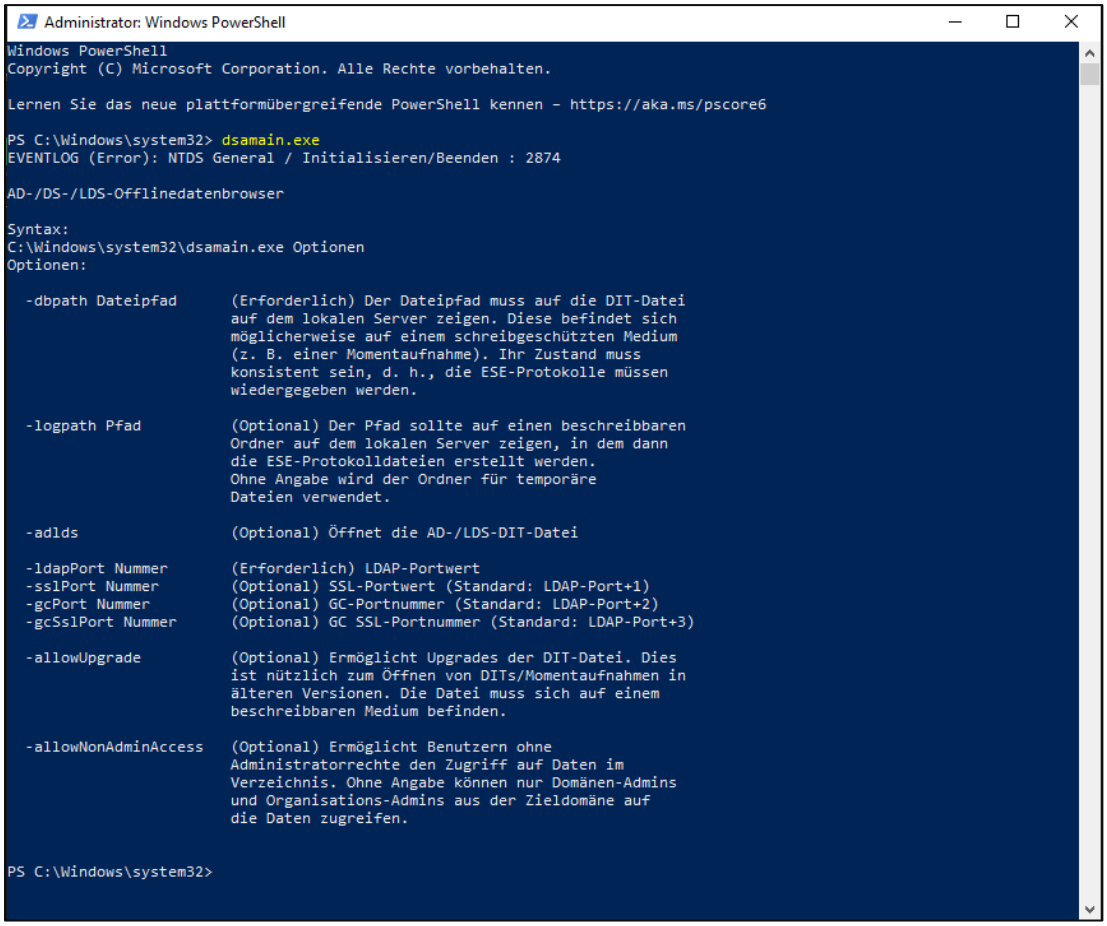


Scrollen Sie nach unten, dort befindet sich der Punkt Mehr Windows-Funktionen.



Aktivieren Sie Active Directory Lightweight Directory Services.

Überprüfen Sie, ob die Anwendung dsamain.exe verfügbar ist. Öffnen Sie dazu mit Rechtsklick auf Start eine Windows PowerShell Admin Konsole und starten Sie dsamain.exe.

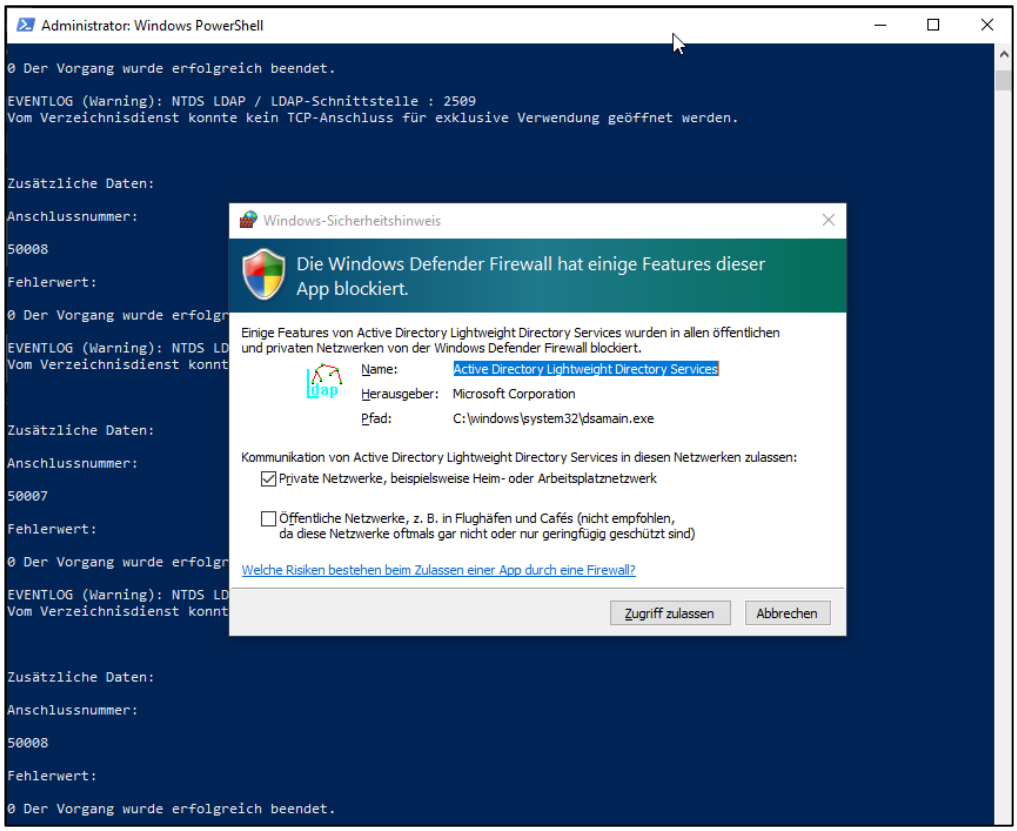


2.3 Datenbank mit DSAMAIN als LDAP-Server verfügbar machen

Nutzen Sie das PowerShell Administrator Fenster um die Datenbank als LDAP-Server zu starten:

```
dsamain.exe -dbpath C:\Users\Nutzer1\Desktop\ntds.dit -ldapport 50005 -allowNonAdminAccess
```

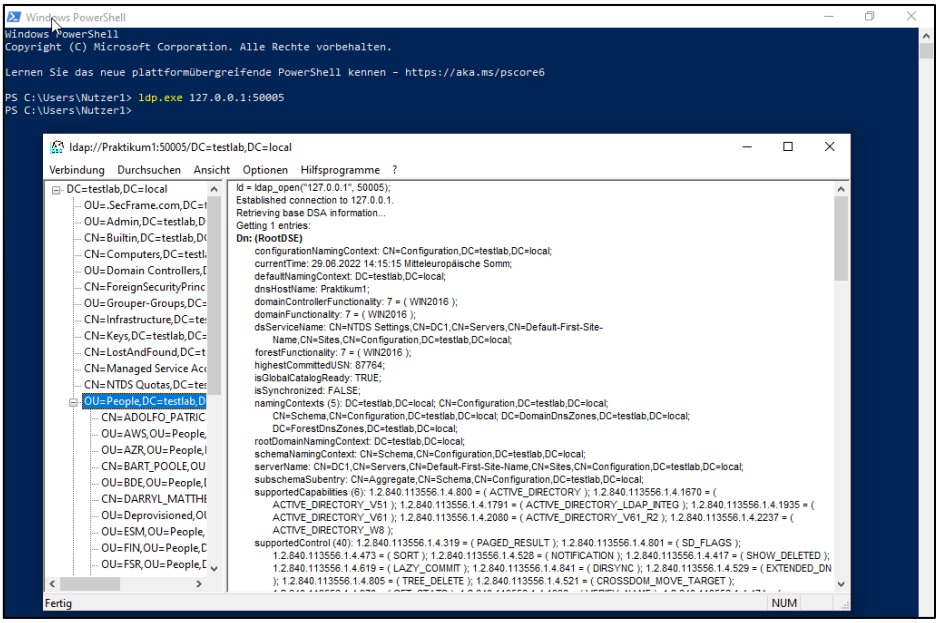
Achten Sie darauf, dass die VM-Netzwerkzugriff aktiviert hat.



Bestätigen Sie die Firewall Ausnahme!

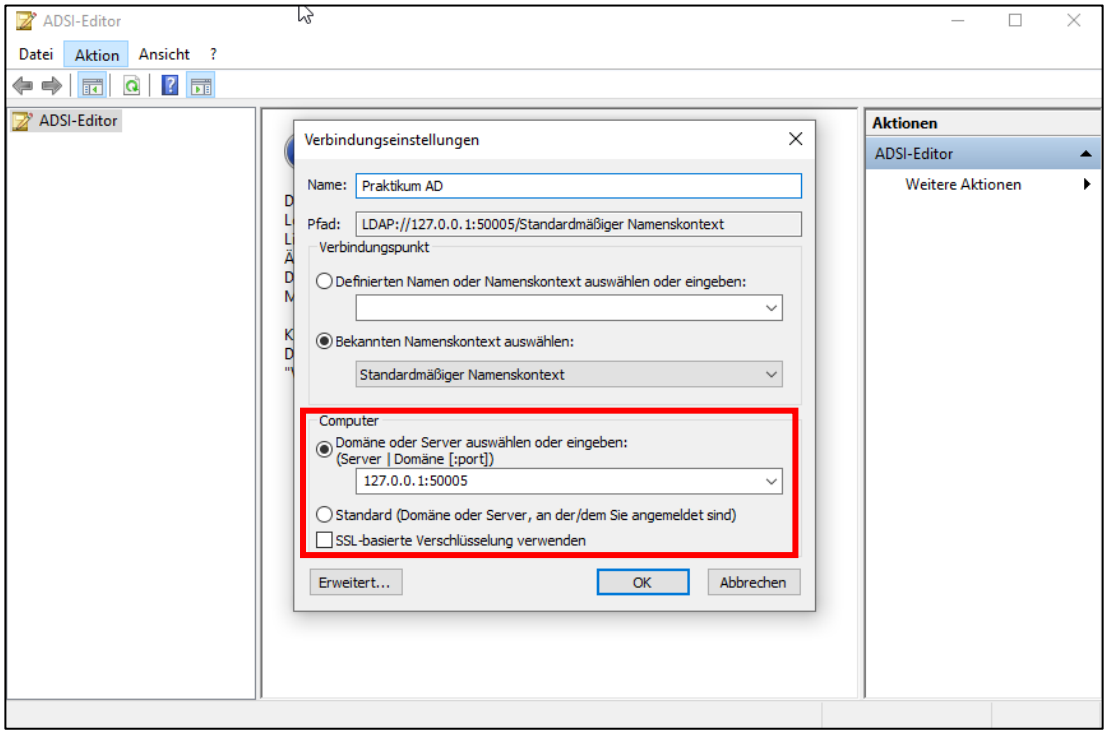
Der LDAP-Server ist jetzt unter 127.0.0.1:50005 erreichbar. Überprüfen Sie die Zugriffsmöglichkeit in einem zweiten PowerShell Fenster, **ohne das vorherige zu schließen**!

```
ldp.exe 127.0.0.1:50005
```

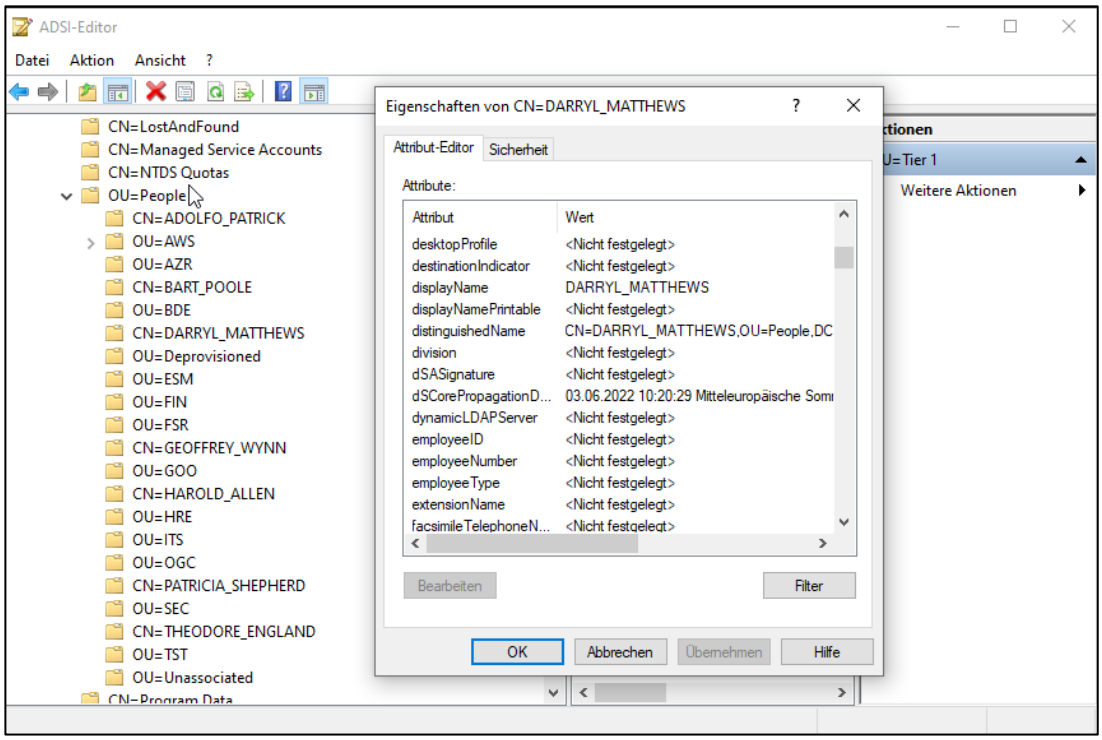


2.4 Abruf via ADSI-Editor

Über Start > Windows Verwaltungsprogramme hat man die Möglichkeit den ADSI-Editor zu öffnen.



Wenn man sich hier mit dem Server über 127.0.0.1:50005 unter Computer verbindet kann man ebenfalls auf die Einstellungen zugreifen.



2.5 Abruf via PowerShell Kommandos

Führen Sie jetzt den ersten Teil des PowerShell Skriptes für den Abruf der Domänen-Informationen aus

```
PS C:\Users\Nutzer1> ldp.exe 127.0.0.1:50005
PS C:\Users\Nutzer1> $DN = ([adsi]"LDAP://localhost:50005").distinguishedName;
PS C:\Users\Nutzer1> $DomainObj = New-Object System.DirectoryServices.DirectoryEntry("LDAP://localhost:50005/$DN");
PS C:\Users\Nutzer1> $objSearcher = New-Object System.DirectoryServices.DirectorySearcher -ArgumentList $DomainObj;
PS C:\Users\Nutzer1> $ObjSearcher.PageSize = $PageSize; $objSearcher.SizeLimit = 100000;
PS C:\Users\Nutzer1> $ObjSearcher.Filter = '(objectCategory=user)'
PS C:\Users\Nutzer1> $Users = $ObjSearcher.FindAll();
PS C:\Users\Nutzer1> $ObjSearcher.Filter = '(objectCategory=group)'
PS C:\Users\Nutzer1> $Groups = $ObjSearcher.FindAll();
PS C:\Users\Nutzer1> $ObjSearcher.Filter = '(objectCategory=computers)'
PS C:\Users\Nutzer1> $Computers = $ObjSearcher.FindAll();
PS C:\Users\Nutzer1> $ObjSearcher.dispose();
PS C:\Users\Nutzer1>
```

Jetzt kann man Skript basiert oder manuell darauf zugreifen:

```
PS C:\Users\Nutzer1> $Users.properties[1]

Name                           Value
----                           -----
distinguishedname              {CN=Gast,CN=Users,DC=testlab,DC=local}
countrycode                    {0}
samaccountname                 {Gast}
objectsid                      {1 5 0 0 0 0 0 5 21 0 0 0 207 193 126 18 129 212 50 55 186 108 112 232 245 1 0 0}
adspath                        {LDAP://localhost:50005/CN=Gast,CN=Users,DC=testlab,DC=local}
samaccounttype                 {805306368}
primarygroupid                 {514}
cn                             {Gast}
objectguid                     {184 248 23 136 211 203 176 65 154 211 134 205 224 179 49 60}
objectcategory                 {CN=Person,CN=Schema,CN=Configuration,DC=testlab,DC=local}
description                    {Vordefiniertes Konto für Gastzugriff auf den Computer bzw. die Domäne}
objectclass                    {top, person, organizationalPerson, user}
codepage                       {0}
name                           {Gast}


PS C:\Users\Nutzer1> $Groups.properties[0]

Name                           Value
----                           -----
objectcategory                 {CN=Group,CN=Schema,CN=Configuration,DC=testlab,DC=local}
usnchanged                     {40416}
distinguishedname              {CN=Administratoren,CN=Builtin,DC=testlab,DC=local}
grouptype                      {-2147483643}
whencreated                    {02.06.2022 11:46:00}
samaccountname                 {Administratoren}
description                    {Administratoren haben uneingeschränkten Vollzugriff auf den Computer bzw. die Domäne.}
instancetype                   {4}
adspath                        {LDAP://localhost:50005/CN=Administratoren,CN=Builtin,DC=testlab,DC=local}
samaccounttype                 {536870912}
objectsid                      {1 2 0 0 0 0 0 5 32 0 0 0 32 2 0 0}
whenchanged                    {03.06.2022 08:21:41}
objectguid                     {3 126 19 90 93 227 85 78 153 216 25 23 174 138 60 218}
member                         {CN=LEILA_GREENE,OU=AWS,OU=Tier 2,DC=testlab,DC=local, CN=ETHAN_SIMS,OU=AWS,OU=People,DC=testlab,DC=local, C...
cn                             {Administratoren}
usncreated                     {8199}
admincount                     {1}
iscriticalsystemobject         {True}
objectclass                    {top, group}
systemflags                    {-1946157056}
dscorepropagationdata          {03.06.2022 08:20:29, 03.06.2022 08:20:27, 03.06.2022 08:20:27, 03.06.2022 08:20:26...}
name                           {Administratoren}


PS C:\Users\Nutzer1>
```

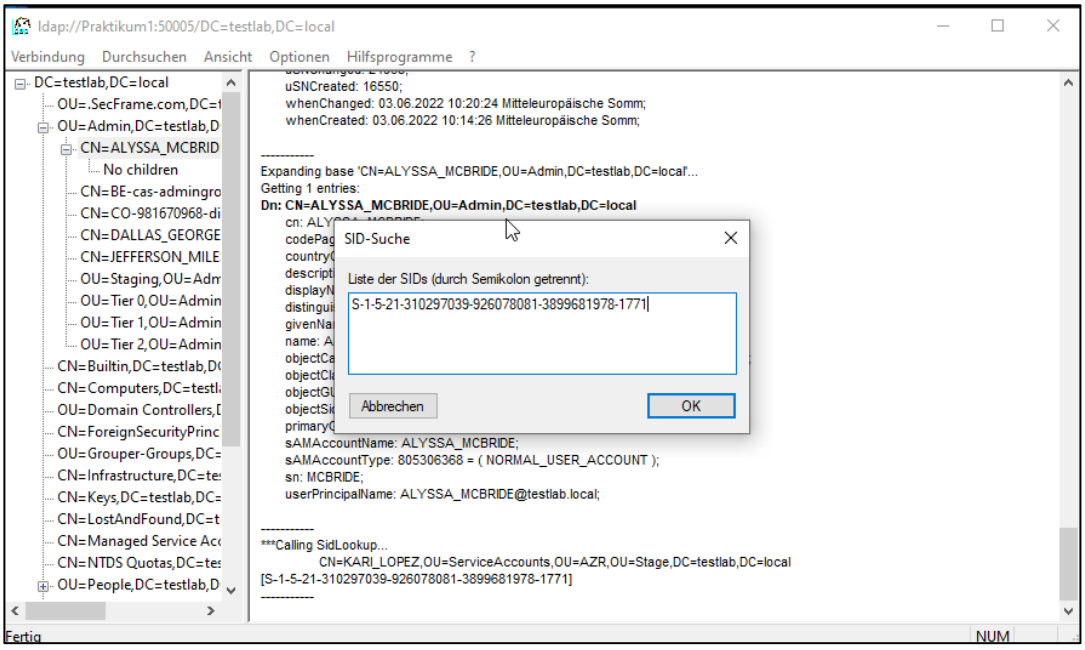
```
PS C:\Users\Nutzer1> $Computers.properties[1]

Name                           Value
----                           -----
logoncount                     {58}
codepage                       {0}
objectcategory                 {CN=Computer,CN=Schema,CN=Configuration,DC=testlab,DC=local}
description                    {Created with secframe.com/badblood.}
operatingsystem                {Windows 11 Pro}
usnchanged                     {87400}
instancetype                   {4}
name                           {OGCWAPPS1000000}
badpasswordtime                {0}
pwdlastset                     {132996721544131943}
serviceprincipalname           {WSMAN/OGCWAPPS1000000, WSMAN/OGCWAPPS1000000.testlab.local, TERMSRV/OGCWAPPS1000000, TERMSRV/OGCWAPPS100000...
objectclass                    {top, person, organizationalPerson, user...}
badpwdcount                    {0}
samaccounttype                 {805306369}
managedby                      {CN=SANDY_MORIN,OU=Test,OU=HRE,OU=Tier 2,DC=testlab,DC=local}
lastlogontimestamp             {133006026206370156}
usncreated                     {24731}
objectguid                     {133 240 132 93 64 22 177 66 164 47 61 127 254 143 157 152}
localpolicyflags               {0}
whencreated                    {03.06.2022 08:20:00}
adspath                        {LDAP://localhost:50005/CN=OGCWAPPS1000000,OU=Devices,OU=ITS,OU=Stage,DC=testlab,DC=local}
useraccountcontrol             {4096}
cn                             {OGCWAPPS1000000}
countrycode                    {0}
primarygroupid                 {515}
whenchanged                    {25.06.2022 03:50:20}
operatingsystemversion         {10.0 (22000)}
dnshostname                    {OGCWAPPS1000000.testlab.local}
dscorepropagationdata          {03.06.2022 08:20:29, 03.06.2022 08:20:27, 03.06.2022 08:20:27, 03.06.2022 08:20:27...}
lastlogon                      {133008042203882150}
distinguishedname              {CN=OGCWAPPS1000000,OU=Devices,OU=ITS,OU=Stage,DC=testlab,DC=local}
msds-supportedencryptiontypes  {28}
iscriticalsystemobject         {False}
samaccountname                 {OGCWAPPS1000000$}
objectsid                      {1 5 0 0 0 0 0 5 21 0 0 0 207 193 126 18 129 212 50 55 186 108 112 232 193 8 0 0}
lastlogoff                     {0}
displayname                    {OGCWAPPS1000000}
accountexpires                 {9223372036854775807}


PS C:\Users\Nutzer1>
```

2.6 Suchen Sie den Mitarbeiter mit der SID -1771 am Ende

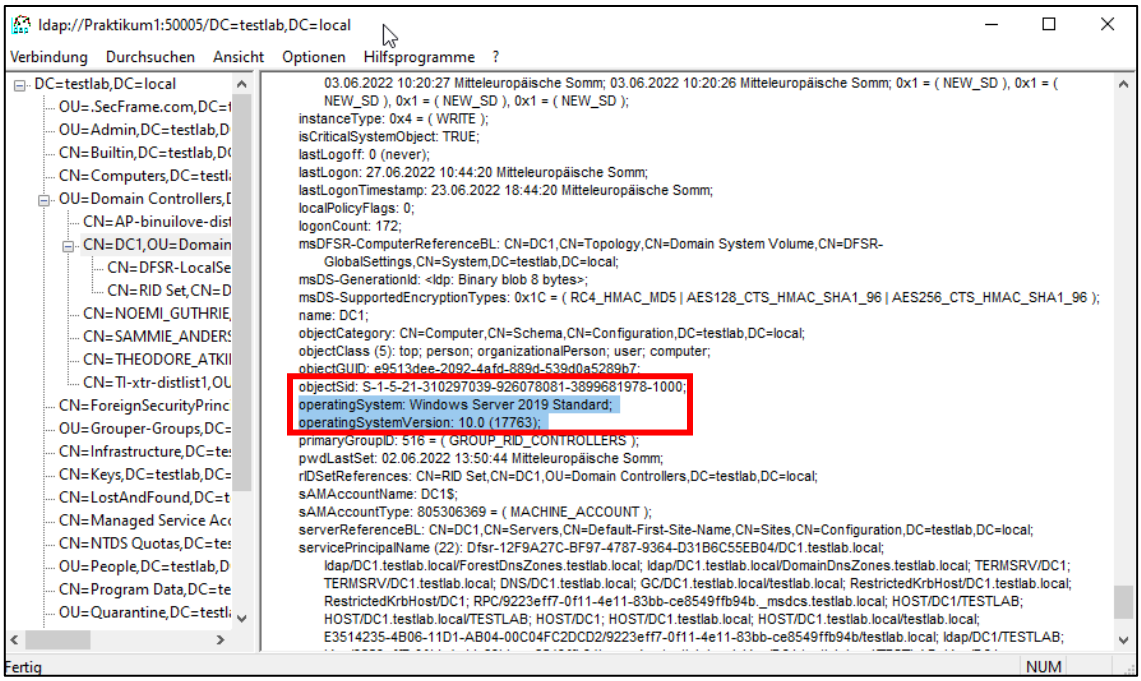
Der einfachste Weg ist die Anwendung ldp.exe. Diese verfügt über eine SID-Suchfunktion unter Hilfsprogramme. Was man dafür allerdings benötigt, ist die komplette SID. Hier bietet es sich an diese von einem der Accounts zu nehmen und die letzte SID-Kennung auszutauschen.




```
***Calling SidLookup...
        CN=KARI_LOPEZ,OU=ServiceAccounts,OU=AZR,OU=Stage,DC=testlab,DC=local
[S-1-5-21-310297039-926078081-3899681978-1771]
```

2.7 Windows Server feststellen

Für die Feststellung des Servers hilft uns auch die Anwendung ldp.exe weiter. Nach dem Verbinden werden diese Daten angezeigt.



Auch PowerShell kann uns diese Informationen liefern.

```
PS C:\Users\Nutzer1> $Computers.properties[0]

Name                           Value
----                           -----
ridsetreferences               {CN=RID Set,CN=DC1,OU=Domain Controllers,DC=testlab,DC=local}
logoncount                     {172}
codepage                       {0}
objectcategory                 {CN=Computer,CN=Schema,CN=Configuration,DC=testlab,DC=local}
msdfsr-computerreferencebl     {CN=DC1,CN=Topology,CN=Domain System Volume,CN=DFSR-GlobalSettings,CN=System,DC=testlab,DC=local}
iscriticalsystemobject         {True}
operatingsystem                {Windows Server 2019 Standard}
usnchanged                     {87190}
instancetype                   {4}
name                           {DC1}
badpasswordtime                {0}
pwdlastset                     {132986442446587104}
serviceprincipalname           {Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/DC1.testlab.local, ldap/DC1.testlab.local/ForestDnsZones.testlab....
objectclass                    {top, person, organizationalPerson, user...}
badpwdcount                    {0}
samaccounttype                 {805306369}
lastlogontimestamp             {133004762601526128}
usncreated                     {12293}
msds-generationid              {54 145 198 1 83 51 22 94}
objectguid                     {238 61 81 233 146 32 253 74 136 157 83 157 10 82 137 183}
localpolicyflags               {0}
whencreated                    {02.06.2022 11:50:18}
adspath                        {LDAP://localhost:50005/CN=DC1,OU=Domain Controllers,DC=testlab,DC=local}
useraccountcontrol             {532480}
cn                             {DC1}
countrycode                    {0}
primarygroupid                 {516}
whenchanged                    {23.06.2022 16:44:20}
operatingsystemversion         {10.0 (17763)}
dnshostname                    {DC1.testlab.local}
dscorepropagationdata          {03.06.2022 08:20:29, 03.06.2022 08:20:27, 03.06.2022 08:20:27, 03.06.2022 08:20:26...}
lastlogon                      {133007930601526406}
distinguishedname              {CN=DC1,OU=Domain Controllers,DC=testlab,DC=local}
msds-supportedencryptiontypes  {28}
samaccountname                 {DC1$}
objectsid                      {1 5 0 0 0 0 0 5 21 0 0 0 207 193 126 18 129 212 50 55 186 108 112 232 232 3 0 0}
lastlogoff                     {0}
serverreferencebl              {CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=testlab,DC=local}
accountexpires                 {9223372036854775807}


PS C:\Users\Nutzer1>
```