

Block 4

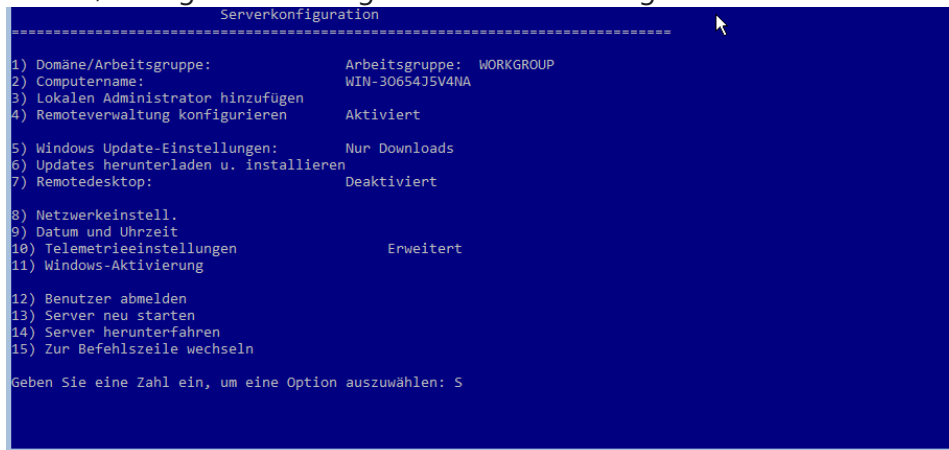
Mailserver mithilfe Windows Exchange erstellen

Windows Exchange ist von Microsoft proprietäre Betriebssystem fürs Konfigurieren von Mailservern. Ich dokumentiere den Installationsvorgang und stelle eine virtuelle Umgebung auf, um die Features von Exchange zu zeigen.

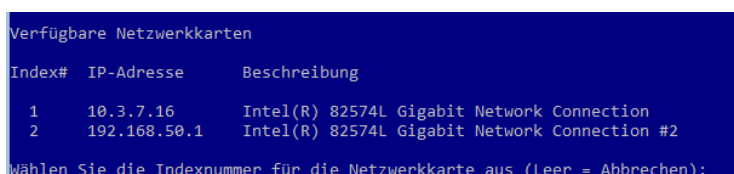
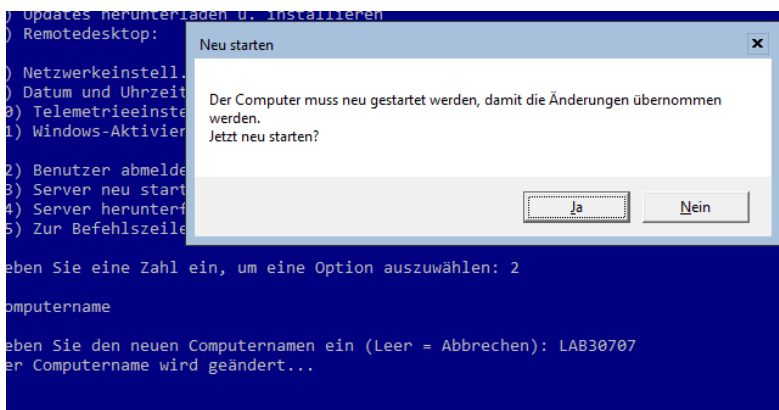
1. Windows Core

Ein Mailserver wird nur zusätzlich mit einem Hauptserver (Domänencontroller) aufgesetzt. Deswegen möchte ich als erstens ein Windows 2016 Core Domänencontroller/Router installieren.

Nach der Installation von Windows Core muss man die Einstellungen konfigurieren. Mit dem Befehl ‚sconfig‘ hat man Zugriff auf die Einstellungen von Windows Server.



Mit 2) ändert man den Servernamen und mit 8) konfiguriert man die Netzwerkkarten.



Die Serverrollen und Features kann man nur mit Befehlen installieren und konfigurieren.

Um die Domänenfeatures zu installieren, muss man in den Powershell-Shell starten (powershell) und dann den folgenden Powershell-Befehl eingeben:

,Install-WindowsFeature –Name AD-Domain-Services –IncludeManagementTools‘

Nach der Installation kann man die einzelnen Befehle, die bezüglich Domänen sind mit den Befehl:

,Get-Command –Module ADDSDeployment‘ anschauen.

```
PS C:\Users\Administrator> Get-Command -Module ADDSDeployment

CommandType      Name                                           Version      Source
-----
Cmdlet            Add-ADDSReadonlyDomainControllerAccount      1.0.0.0      ADDSDeployment
Cmdlet            Install-ADSDomain                             1.0.0.0      ADDSDeployment
Cmdlet            Install-ADSDomainController                  1.0.0.0      ADDSDeployment
Cmdlet            Install-ADDSForest                           1.0.0.0      ADDSDeployment
Cmdlet            Test-ADSDomainControllerInstallation          1.0.0.0      ADDSDeployment
Cmdlet            Test-ADSDomainControllerUninstallation        1.0.0.0      ADDSDeployment
Cmdlet            Test-ADSDomainInstallation                   1.0.0.0      ADDSDeployment
Cmdlet            Test-ADDSForestInstallation                  1.0.0.0      ADDSDeployment
Cmdlet            Test-ADDSReadonlyDomainControllerAccountCreation 1.0.0.0      ADDSDeployment
Cmdlet            Uninstall-ADSDomainController                1.0.0.0      ADDSDeployment
```

Man kann entweder die Installation mit Schritten starten oder die Installation mit nur ein Befehl starten.

Ich starte die Installation mit nur ein Befehl und gleichzeitig füge ich die Parameter in den Befehl:

,Install-ADDSForest –DomainName lab30707.local –DomainNetbiosName LAB307SEVEN – SafeModeAdministratorPassword (Convertto-SecureString –AsPlainText „Passwordxyz“ –Force)‘

```
PS C:\Users\Administrator> Install-ADDSForest -DomainName lab30707.local -DomainNetbiosName LAB307SEVEN -SafeModeAdministratorPassword (Convertto-SecureString -AsPlainText "Admin1" -Force)

Der Zielservers wird als Domänencontroller konfiguriert und neu gestartet, wenn dieser Vorgang abgeschlossen ist.
Möchten Sie diesen Vorgang fortsetzen?
[J] Ja [A] Ja, alle [N] Nein [K] Nein, keine [H] Anhalten [?] Hilfe (Standard ist "J"):
```

Nach dem Neustarten die Remotezugriff Rolle installieren:

,Install-WindowsFeature –Name RemoteAccess –IncludeManagementTools‘

,Install-WindowsFeature –Name Routing –IncludeManagementTools‘

Zone erstellen: **Add-DnsServerPrimaryZone -Name lab30707.local -ReplicationScope "Forest" – PassThru**

Die Reverselookup-Zone kann man mit den folgenden Befehl erstellen:

,Add-DnsServerPrimaryZone -NetworkId "192.168.07.0/24" -ReplicationScope Domain‘

Danach kann man eine neue A-Eintrag machen:

,Add-DnsServerResourceRecordA -Name server -IPv4Address 192.168.07.1 -ZoneName lab30707.local‘

```
PS C:\Users\Administrator> Add-DnsServerPrimaryZone -NetworkId "192.168.50.0/24" -ReplicationScope Domain
PS C:\Users\Administrator> Sync-DnsServerZone -passthru

ZoneName              ZoneType      IsAutoCreated  IsDsIntegrated  IsReverseLookupZone  IsSigned
-----
_msdcs.lab30707.local Primary       False          True             False                 False
0.in-addr.arpa        Primary       True           False            True                  False
127.in-addr.arpa      Primary       True           False            True                  False
255.in-addr.arpa      Primary       True           False            True                  False
50.168.192.in-addr.arpa Primary       False          True             True                  False
lab30707.local         Primary       False          True             False                 False

PS C:\Users\Administrator>
```

Die DNS-Einträge kann man mit **,Get-DnsServerResourceRecord -ZoneName lab30707.local‘** nachschauen.

```

HostName      RecordType Type      Timestamp      TimeToLive      RecordData
-----
@              A          1          22.11.2022 08:00:00 00:10:00      10.3.7.16
@              A          1          22.11.2022 08:00:00 00:10:00      192.168.50.1
@              NS         2          0               01:00:00      lab30707.lab30707.local.
@              SOA        6          0               01:00:00      [22][lab30707.lab30707.local.][...
msdcs          NS         2          0               01:00:00      lab30707.lab30707.local.
_gc._tcp.Default-First... SRV        33        22.11.2022 08:00:00 00:10:00      [0][100][3268][LAB30707.lab3070...
_kerberos._tcp.Default... SRV        33        22.11.2022 08:00:00 00:10:00      [0][100][88][LAB30707.lab30707...
_ldap._tcp.Default-Fir... SRV        33        22.11.2022 08:00:00 00:10:00      [0][100][389][LAB30707.lab30707...
_gc._tcp       SRV        33        22.11.2022 08:00:00 00:10:00      [0][100][3268][LAB30707.lab3070...
_kerberos._tcp SRV        33        22.11.2022 08:00:00 00:10:00      [0][100][88][LAB30707.lab30707...
_kpasswd._tcp  SRV        33        22.11.2022 08:00:00 00:10:00      [0][100][464][LAB30707.lab30707...
_ldap._tcp     SRV        33        22.11.2022 08:00:00 00:10:00      [0][100][389][LAB30707.lab30707...
_kerberos._udp SRV        33        22.11.2022 08:00:00 00:10:00      [0][100][88][LAB30707.lab30707...
_kpasswd._udp  SRV        33        22.11.2022 08:00:00 00:10:00      [0][100][464][LAB30707.lab30707...
DomainDnsZones A          1          22.11.2022 09:00:00 00:10:00      10.3.7.16
DomainDnsZones A          1          22.11.2022 09:00:00 00:10:00      192.168.50.1
_ldap._tcp.Default-Fir... SRV        33        22.11.2022 09:00:00 00:10:00      [0][100][389][LAB30707.lab30707...
_ldap._tcp.DomainDnsZones SRV        33        22.11.2022 09:00:00 00:10:00      [0][100][389][LAB30707.lab30707...
ForestDnsZones A          1          22.11.2022 09:00:00 00:10:00      192.168.50.1
ForestDnsZones A          1          22.11.2022 09:00:00 00:10:00      10.3.7.16
_ldap._tcp.Default-Fir... SRV        33        22.11.2022 09:00:00 00:10:00      [0][100][389][LAB30707.lab30707...
_ldap._tcp.ForestDnsZones SRV        33        22.11.2022 09:00:00 00:10:00      [0][100][389][LAB30707.lab30707...
lab30707       A          1          0               01:00:00      10.3.7.16
lab30707       A          1          0               01:00:00      192.168.50.1

```

PS C:\Users\Administrator>

Reverselookup-Einträge fügt man mit

,Add-DNSServerResourceRecordPTR -ZoneName 07.168.192.in-addr.arpa -Name 01 -PTRDomainName lab30707.lab30707.local' hinzu.

Um den Clients Internetzugang zu geben, muss man noch ein Forwarder hinzufügen:

Add-DnsServerForwarder -IPAddress 8.8.8.8 -PassThru

Die DHCP-Rolle installiert man mit **,Install-WindowsFeature DHCP -IncludeManagementTools'**

Ein DHCP-Server kann man mit **,Add-DhcpServerInDC -DNSName lab30707.lab30707.local -IPAddress 192.168.07.1'**

Ob der DHCP-Server erstellt wurde, kann man mit **,Get-DhcpServerInDC'** kontrollieren.

```

PS C:\Users\Administrator> Get-DhcpServerInDC

IPAddress      DnsName
-----
192.168.50.1   lab30707.lab30707.local

PS C:\Users\Administrator>

```

Ein DHCP-Scope erstellt man mit **,Add-DhcpServerV4Scope -name "LAB30707-DHCP" -StartRange 192.168.07.2 -Endrange 192.168.07.9 -SubnetMask 255.255.255.0'**

Die Einstellungen für den DHCP-Server konfiguriert man mit **,Set-DhcpServerV4OptionValue -ComputerName lab30707.lab30707.local -ScopeID 192.168.7.2 -DNSServer 192.168.7.1 -Router 192.168.07.1 –DnsDomain lab30707.local'**

```
PS C:\Users\Administrator> Get-DhcpServerV4OptionValue -ScopeID 192.168.50.2
```

OptionId	Name	Type	Value	VendorClass	UserClass	PolicyName
3	Router	IPv4Add...	{192.168.50.1}			
6	DNS-Server	IPv4Add...	{192.168.50.1}			
51	Lease	DWord	{691200}			

```
PS C:\Users\Administrator> get-dhcpserverv4lease -scopeid 192.168.50.0
```

IPAddress	ScopeId	ClientId	HostName	AddressState	LeaseExpiryTime
192.168.50.253	192.168.50.0	00-50-56-35-3b-40		InactiveReservation	

```
PS C:\Users\Administrator>
```

Die ScopeID ist die erste IP-Adresse, dass vom DHCP-Server verteilt wird.

Ich möchte für den Ubuntu Client eine Reservierung erstellen. Mit **,Add-DhcpServerV4Reservation -ScopeID 192.168.07.2 -IPAddress 192.168.07.253 -ClientID "00-50-56-35-3B-40"** erstellt man eine DHCP-Reservierung. Die Client ID ist die MAC-Adresse des Clients.

Mit **,Get-DhcpServerV4OptionValue –ScopeID 192.168.07.2'** und **,Get-DhcpServerV4Lease –ScopeID 192.168.07.0'** kann man die DHCP-Leases und die DHCP-Einstellungen nachschauen.

Set-DhcpServerV4DnsSetting -ComputerName "lab30707.lab30707.local" -DynamicUpdates "Always" -DeleteDnsRRonLeaseExpiry \$True

```
PS C:\Users\Administrator> Install-WindowsFeature DHCP -IncludeManagementTools
```

Success	Restart	Needed	Exit Code	Feature	Result
True	No		Success	{DHCP-Server}	

```
PS C:\Users\Administrator> Add-DhcpServerInDC -DNSName lab30707.lab30707.local -IPAddress 192.168.50.1
PS C:\Users\Administrator>
```

Mit **,Install-RemoteAccess -VpnType Vpn'** und **,netsh routing ip nat install'** installiert man die Routing Rollen für VPNs/NAT und LAN Routing.

Die Schnittstellen fügt man mit den folgenden Befehlen hinzu:

```
netsh routing ip nat add interface Ethernet0
netsh routing ip nat set interface Ethernet0 mode=full
netsh routing ip nat add interface Ethernet1
```

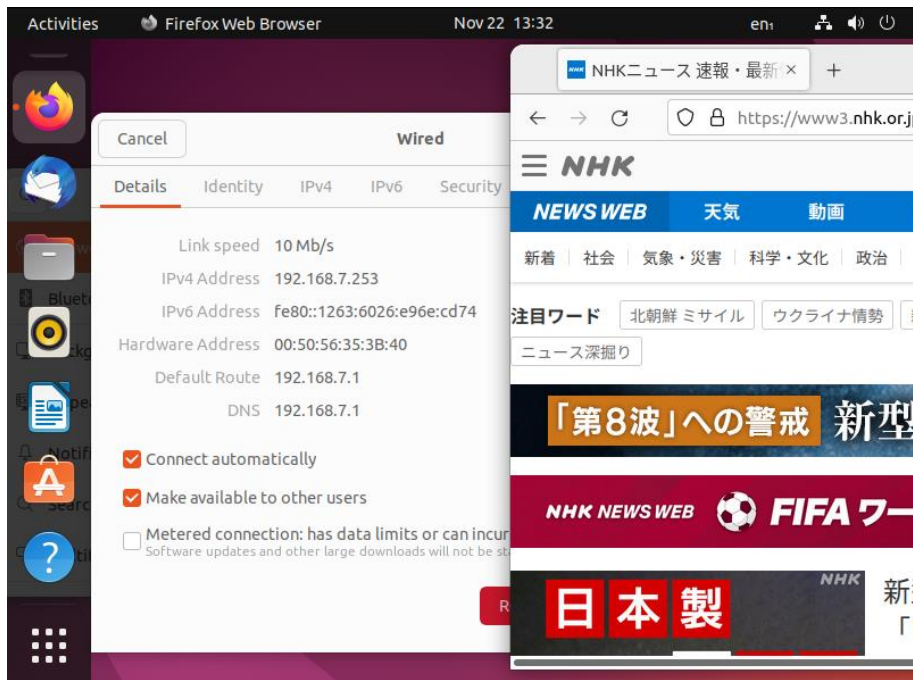
```
PS C:\Windows\System32> cmd.exe /c "netsh routing ip nat add interface Ethernet0"
Die Ethernet0-Schnittstelle gehört bereits zu diesem Protokoll.
Falscher Parameter.

Falscher Parameter.

PS C:\Windows\System32> cmd.exe /c "netsh routing ip nat set interface Ethernet0 mode=full"
PS C:\Windows\System32> cmd.exe /c "netsh routing ip nat add interface Ethernet1"
```

2. Clients

Nach dem man den Core Server erfolgreich konfiguriert hat, sollte der Client Zugang zum Internet haben ohne direkter Verbindungen mit den Bridge/NAT Adapter.
Hier hat z.B. der Ubuntu Client (Live-Umgebung) seine eigene reservierte IP-Adresse und kann Webseiten auf den Firefox-Browser zugreifen.



Bei ein Windows Client ist es möglich, in die Domäne eines Servers hinzugefügt werden.
Im Vergleich zu neueren Version von Windows ist die Einstellung, mit dem man den Client in die Domäne hinzufügen kann, in ein anderen Menü verschoben.
Die Einstellung befindet sich in die Kontoeinstellungen.

Geschäfts-, Schul- oder Unikonto einrichten

Sie erhalten Zugriff auf Ressourcen wie E-Mail, Apps und das Netzwerk. Durch das Herstellen einer Verbindung kann Ihr Unternehmen bzw. Ihre Schule/Uni einige Elemente auf diesem Gerät steuern, beispielsweise, welche Einstellungen Sie ändern können. Genauere Informationen hierzu erhalten Sie von den zuständigen Mitarbeitern.

E-Mail-Adresse

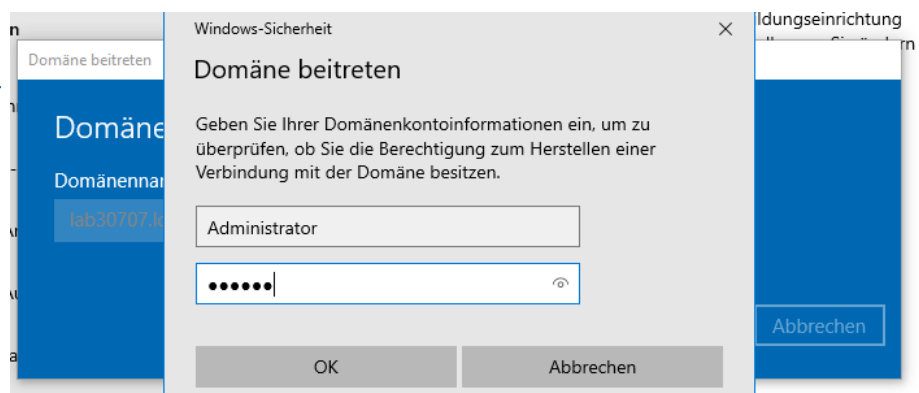
Alternative Aktionen:

Über diese Aktionen wird das Gerät als unternehmenseigenes Gerät eingerichtet, und Ihre Organisation erhält vollständige Kontrolle über das Gerät.

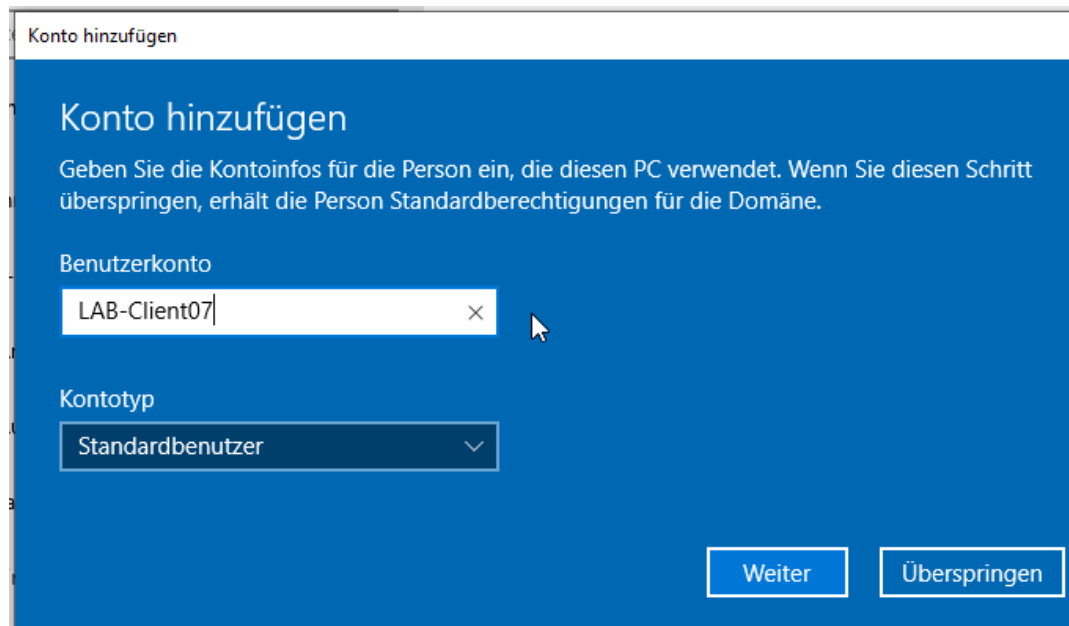
[Dieses Gerät in Azure Active Directory einbinden](#)

[Dieses Gerät in eine lokale Active Directory-Domäne einbinden](#)

Weiter



Nach dem man den Administrator-Passwort eingegeben hat, kann man entscheiden, ob man ein Domänenkonto erstellen oder einfach den PC in die Domäne hinzufügen will.



Nach dem man den Ubuntu Client installiert, muss man realmd mit apt installieren.

sudo apt install sssd-ad sssd-tools realmd adcli

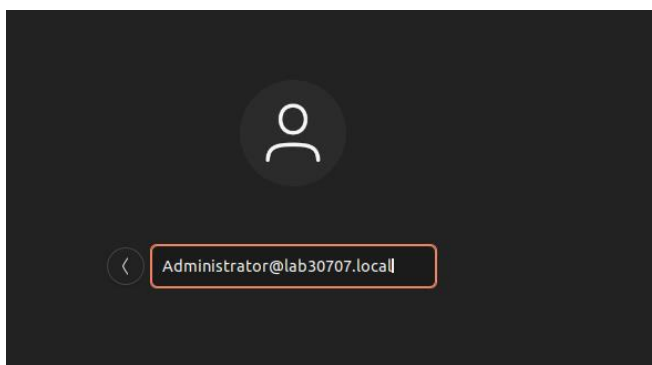
```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

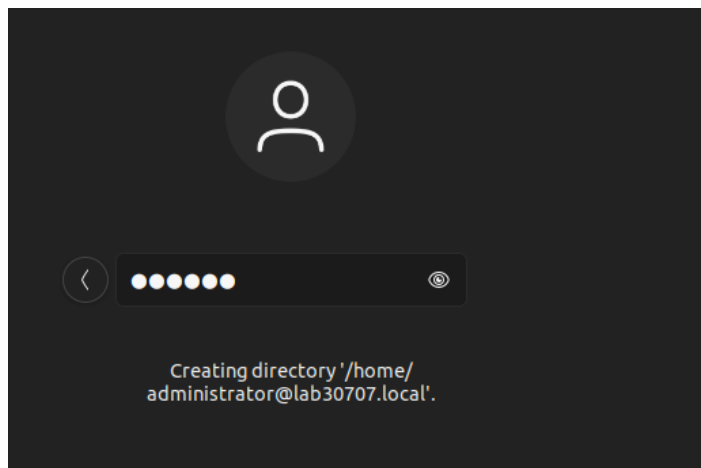
lab-client107@labclient107-virtual-machine:~$ sudo apt update
[sudo] password for lab-client107:
Hit:1 http://at.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://at.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://at.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu jammy-security InRelease

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
336 packages can be upgraded. Run 'apt list --upgradable' to see them.
lab-client107@labclient107-virtual-machine:~$ sudo apt install sssd-ad sssd-tools realmd adcli
```

Mit **'sudo realm join lab30707.local'** die Domäne joinen.

```
lab-client107@labclient107-virtual-machine:~$ sudo realm join lab30707.local
Password for Administrator:
lab-client107@labclient107-virtual-machine:~$
```





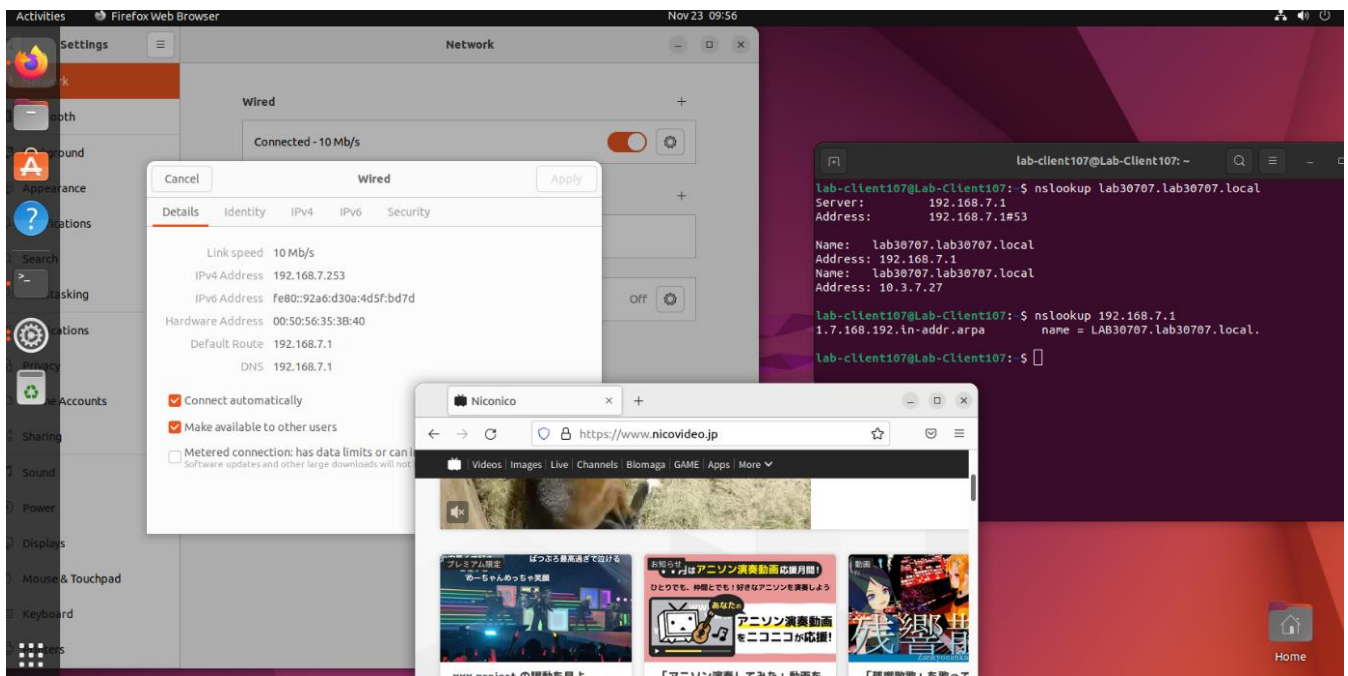
(Ubuntu unterstützt aus irgendein Grund manchmal die .local Domänenadressen nicht. Deswegen muss man die folgenden Befehle nach der Reihe nach eintippen und die Verbindungen aus- und einschalten.)

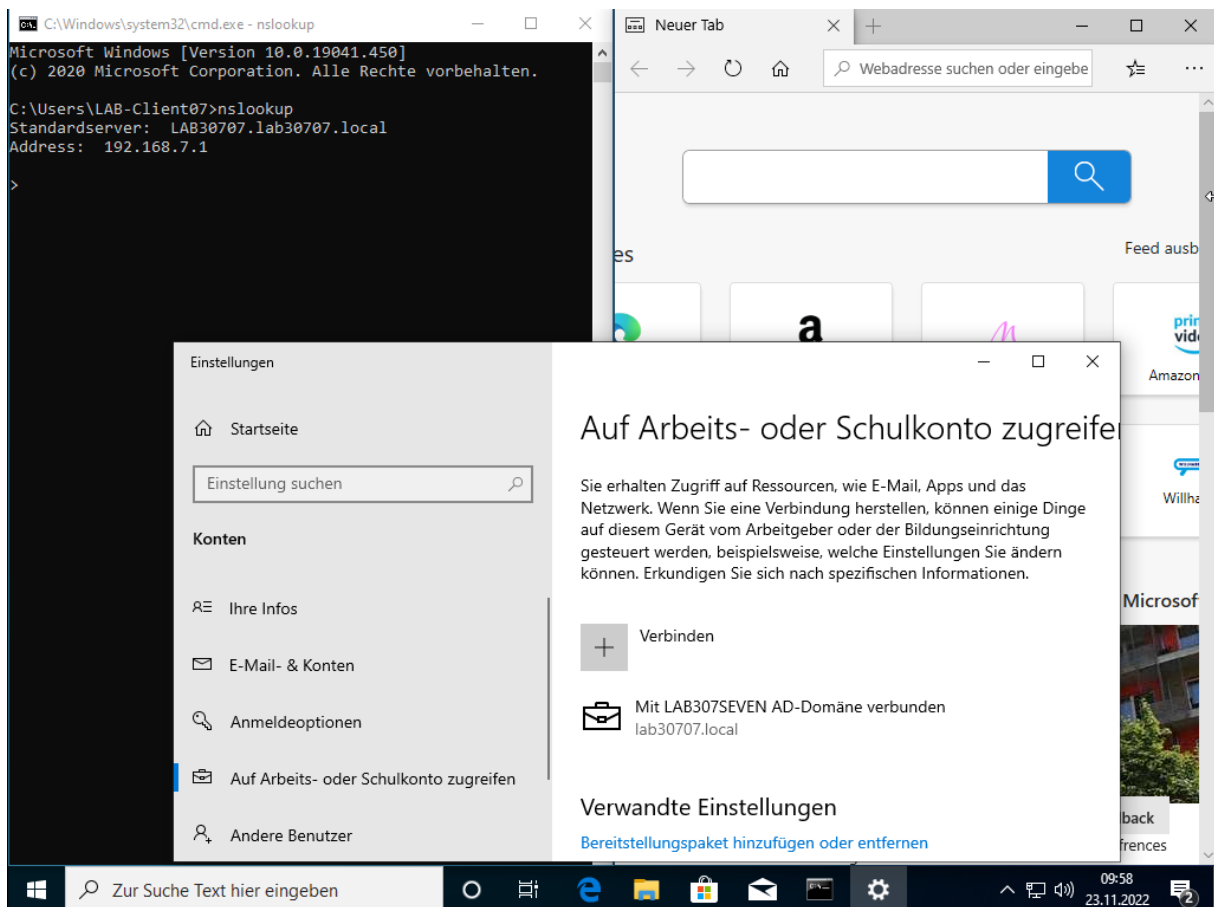
```

sudo rm -f /etc/resolv.conf
sudo ln -s /run/systemd/resolve/resolv.conf /etc/resolv.conf
sudo service systemd-resolved restart
  
```

Nach der Installation muss man die gleiche Befehle später eintippen.)

DNS-Auflösung funktioniert einwandfrei und Internetzugang ist für den Ubuntu und Windows 10 Client verfügbar.





3. Exchange Mail Server

Nach dem man den Domänencontroller und die Clients aufgesetzt hat, kann man auch ein Mailserver für das Netzwerk einsetzen.

Für die Installation von Exchange braucht man ein Windows Server 2016 mit einer grafischen Oberfläche, das in ein Active Directory ist. Um Exchange zu installieren, muss man den Exchange Setup ISO auf den virtuellen CD-Laufwerk des Server2016 GUI mounten. (Als Administrator der Domäne anmelden.)

MICROSOFT EXCHANGE SERVER 2016, KUMULATIVES UPDATE 13

? ✕

Einführung

Willkommen bei Microsoft Exchange Server!

Exchange Server unterstützt Sie dabei, die Benutzerproduktivität zu steigern und Ihre Daten zu schützen, und bietet genau die Kontrolle, die Sie benötigen. Dank flexibler Bereitstellungsoptionen können Sie die Lösung auf Ihre speziellen Anforderungen abstimmen, beispielsweise können Sie mit einer Hybridbereitstellung sowohl von den Vorteilen einer lokalen Lösung als auch von denen einer Online-Lösung profitieren. Mithilfe der Funktionen zur Verwaltung der Compliance können Sie sich vor einem Verlust vertraulicher Daten schützen und dafür sorgen, dass interne Richtlinien und behördliche Auflagen erfüllt werden. Und natürlich können Ihre Benutzer von jedem beliebigen Standort aus und über praktisch jedes Gerät auf ihre E-Mails, Kalender und Voicemails zugreifen. Dieser Assistent leitet Sie durch die Installation von Exchange Server.

Planen Ihrer Exchange Server-Bereitstellung:

[Informationen zu Exchange Server](#)

[Informationen zu unterstützten Sprachen](#)

[Den Bereitstellungs-Assistenten für Exchange Server verwenden](#)

 Exchange

weiter

MICROSOFT EXCHANGE SERVER 2016, KUMULATIVES UPDATE 13

? ✕

Serverrollenauswahl

Wählen Sie die Exchange-Serverrollen aus, die Sie auf diesem Computer installieren möchten:

☒ Postfachrolle

☒ Verwaltungstools

☐ Edge-Transport-Rolle

☒ Für die Installation von Exchange Server erforderliche Windows Server-Rollen und -Funktionen automatisch installieren

 Exchange

zurück

weiter

Alle Rollen auswählen und Exchange Organisationname schreiben.

Exchange-Organisation

Geben Sie den Namen für diese Exchange-Organisation an:

LAB30707

☒ Active Directory-Sicherheitsmodell für geteilte Berechtigungen auf die Exchange-Organisation anwenden

Das Sicherheitsmodell von Active Directory mit strikt geteilten Berechtigungen wird normalerweise von großen Organisationen verwendet, die die Zuständigkeit für die Verwaltung von Exchange und Active Directory auf verschiedene Personengruppen aufteilen. Die Anwendung dieses Sicherheitsmodells beseitigt die Möglichkeit für Exchange-Server und Administratoren, Active Directory-Objekte wie Benutzer, Gruppen und Kontakte zu erstellen. Die Möglichkeit zum Verwalten von Nicht-Exchange-Attributen für diese Objekte wird ebenfalls beseitigt.

Sie sollten dieses Sicherheitsmodell nicht anwenden, wenn dieselbe Person oder Gruppe sowohl Exchange als auch Active Directory verwaltet. Klicken Sie auf '7', um weitere Informationen zu erhalten.



zurück

weiter

Bereitschaftsüberprüfung

Der Computer wird überprüft, um festzustellen, ob das Setup fortgesetzt werden kann.

Analyse der Voraussetzungen

100%

Fehler:

This computer requires .NET Framework 4.7.2 (<https://support.microsoft.com/kb/4054530>). Weitere Informationen finden Sie unter: <https://docs.microsoft.com/Exchange/plan-and-deploy/system-requirements?view=exchserver-2016>

Fehler:
Dieser Computer erfordert das im Microsoft Knowledge Base-Artikel KB3206632 beschriebene Update (<http://support.microsoft.com/kb/3206632>). Ohne dieses Update funktioniert Exchange Server 2016 nicht zuverlässig unter Windows Server 2016. Weitere Informationen finden Sie unter: <http://technet.microsoft.com/library/EXCHG.150/ms.exch.setupreadiness.Windows16SARollupUpdateNotInstalled.aspx>

Fehler:
Es steht ein Neustart aufgrund einer vorherigen Installation einer Windows Server-Rolle oder -Funktion aus. Starten Sie den Computer neu, und führen Sie Setup erneut aus. Weitere Informationen finden Sie unter: <http://technet.microsoft.com/library/EXCHG.150/ms.exch.setupreadiness.PendingRebootWindowsComponents.aspx>

Fehler:



wiedeholen

Es fehlen viele Programme und Libraries, um Exchange zu installieren. Diese Programme soll man im Internet suchen und installieren.

Nach dem man alle Libraries und Programme installiert, kann man mit der Installation weiter fortfahren.

Wenn gefragt, alle Rollen auswählen und die Installation beginnen.

Setup abgeschlossen

Setup wurde erfolgreich abgeschlossen. Starten Sie den Computer neu, um die Installation von Microsoft Exchange Server abzuschließen.

Weitere Aufgaben nach der Installation finden Sie online unter "<https://docs.microsoft.com/Exchange/plan-and-deploy/post-installation-tasks/post-installation-tasks?view=exchserver-2016>". Sie können nach dem Fertigstellen von Setup auch das Exchange Admin Center starten.

☒ Exchange Admin_Center starten, nachdem Exchange-Setup fertig gestellt wurde.



fertig stellen

Nach der Installation den Server neustarten.

Exchange kann man mit den Browser oder mit der Shell bearbeiten.

Es wird empfohlen, den Web Admin Center mit einen modernen Browser zuzugreifen.

The screenshot shows two overlapping windows. The top window is a PowerShell console titled 'Computer: mail.lab30707.local'. It displays the 'Exchange-Verwaltungsshell' (Exchange Management Shell) welcome message and a list of commands. The bottom window is the 'Exchange Admin Center' login page in a browser. The browser's address bar shows 'https://localhost/owa/auth/login.aspx?replaceCurrent...'. The login page has a blue header with the Exchange logo and a white login form. The form includes fields for 'Domäne\Benutzername:' (containing 'Administrator@lab30707.local') and 'Kennwort:' (password). Below the fields is a blue 'Anmelden' (Sign in) button. The browser's status bar at the bottom indicates a 'Zertifikatsfehler' (Certificate error).

```
Willkommen bei der Exchange-Verwaltungsshell.

Vollständige Liste der Cmdlets: Get-Command
Nur Exchange-Cmdlets: Get-ExCommand
Cmdlets, die einer bestimmten Zeichenfolge entsprechen: Hilfe *<string>*
Allgemeine Hilfe abrufen: Hilfe
Hilfe für ein Cmdlet abrufen: Help <cmdlet name> oder <cmdlet name> -?
Exchange-Teamblog: Get-ExBlog
Vollständige Ausgabe für einen Befehl anzeigen: <command> | Format-List

Kurzübersichtsleitfaden anzeigen: QuickRef
Tipp des Tages Nr. 42:

Möchten Sie aufzeichnen, was genau geschieht, wenn Sie die Exchange-Verwaltungsshell verwenden? Verwenden Sie das Cmdlet
Start-Transcript. Alle Aktionen, die Sie durchführen, nachdem Sie dieses Cmdlet ausgeführt haben, werden in einer von I
hnen angegebenen Textdatei aufgezeichnet. Wenn Sie die Aufzeichnung der Sitzung beenden möchten, verwenden Sie das Cmdle
t Stop-Transcript.

Beachten Sie, dass das Cmdlet Start-Transcript die Zieltextdatei standardmäßig überschreibt. Wenn Sie Ihre Sitzung an ei
ne vorhandene Datei anfügen möchten, verwenden Sie den Parameter Append:

Start-Transcript c:\MySession.txt -Append

AUSFÜHRlich: Verbindung mit mail.lab30707.local wird hergestellt.
AUSFÜHRlich: Verbunden mit mail.lab30707.local.
```

Exchange Admin Center

Domäne\Benutzername:
Administrator@lab30707.local

Kennwort:
[password field]

[Anmelden](#)