

Autor	Luis Lüscher
Datum	18. Oktober 2020
Version	2.0
Klassifikation	Öffentlich
Seiten	54, inkl. Deckblatt

Portfolio

M159

Directory Services konfigurieren und in Betrieb nehmen



Änderungsverzeichnis

Version	Status	Name	Datum	Beschreibung
0.1	Erledigt	Lüscher, Luis	23.08.2020	Dokument wurde erstellt
0.2	Erledigt	Lüscher, Luis	29.08.2020	Punkt 1 wurde vollständig beschrieben.
0.3	Erledigt	Lüscher, Luis	29.08.2020	Punkt 2 wurde vollständig beschrieben.
0.4	Erledigt	Lüscher, Luis	30.08.2020	Punkt 3 wurde vollständig beschrieben.
0.5	Erledigt	Lüscher, Luis	02.09.2020	Punkt 4 wurde vollständig beschrieben.
0.6	Erledigt	Lüscher, Luis	05.09.2020	Punkt 5 wurde vollständig beschrieben.
0.7	Erledigt	Lüscher, Luis	06.09.2020	Punkt 6 wurde vollständig beschrieben.
0.8	Erledigt	Lüscher, Luis	06.09.2020	Punkt 7 wurde vollständig beschrieben.
0.9	Erledigt	Lüscher, Luis	06.09.2020	Punkt 8 wurde vollständig beschrieben.
1.0	Erledigt	Lüscher, Luis	06.09.2020	Punkt 9 wurde vollständig beschrieben.
1.1	Erledigt	Lüscher, Luis	06.10.2020	Punkt 10 wurde vollständig beschrieben.
1.2	Erledigt	Lüscher, Luis	08.10.2020	Punkt 11 wurde vollständig beschrieben.
1.3	Erledigt	Lüscher, Luis	12.10.2020	Punkt 12 wurde vollständig beschrieben.
1.4	Erledigt	Lüscher, Luis	13.10.2020	Punkt 13 wurde vollständig beschrieben.
1.5	Erledigt	Lüscher, Luis	14.10.2020	Punkt 14 wurde vollständig beschrieben.
1.6	Erledigt	Lüscher, Luis	15.10.2020	Punkt 15 wurde vollständig beschrieben.
1.7	Erledigt	Lüscher, Luis	16.10.2020	Punkt 16 wurde vollständig beschrieben.
1.8	Erledigt	Lüscher, Luis	16.10.2020	Überarbeitung gesamter Dokumentation (Orthografie, Syntax, Escheinungsbild).
1.9	Erledigt	Lüscher, Luis	16.10.2020	Final Check 1 von 2
2.0	Erledigt	Lüscher, Luis	1^8.10.2020	Final Check 2 von 2

Lizenz

Creative Commons License



Dieses Werk ist unter einer Creative Commons Lizenz vom Typ Namensnennung – Nicht kommerziell – Weitergabe unter gleichen Bedingungen 3.0 Schweiz (CC BY-NC-SA 3.0 CH) zugänglich. Um eine Kopie dieser Lizenz einzusehen, konsultieren Sie <https://creativecommons.org/licenses/by-nc-sa/3.0/ch/> oder wenden Sie sich brieflich an Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

Sie dürfen:

Teilen - das Material in jedwedem Format oder Medium vervielfältigen und weiterverbreiten

Bearbeiten – das Material remixen, verändern und darauf aufbauen

Unter folgenden Bedingungen:

Namensnennung – Sie müssen angemessene Urheber- und Rechteangaben machen, einen Link zur Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden. Diese Angaben dürfen in jeder angemessenen Art und Weise gemacht werden, allerdings nicht so, dass der Eindruck entsteht, der Lizenzgeber unterstützt gerade Sie oder Ihre Nutzung besonders.

Nicht kommerziell – Sie dürfen das Material nicht für kommerzielle Zwecke nutzen.

Weitergabe unter gleichen Bedingungen – Wenn Sie das Material remixen, verändern oder anderweitig direkt darauf aufbauen, dürfen Sie Ihre Beiträge nur unter derselben Lizenz wie das Original verbreiten.

Keine weiteren Einschränkungen – Sie dürfen keine zusätzliche Klauseln oder technische Verfahren einsetzen, die anderen rechtlich untersagen, was die Lizenz erlaubt.

Inhaltsverzeichnis

1. Planen und VMs vorbereiten.....	6
1.1. Spezifikation.....	6
1.2. Logische Netzwerklayout.....	9
1.3. Standardeinstellung.....	10
1.3.1. Firewall	10
1.3.2. Tastaturlayout	12
1.3.3. Lokale PW-Richtlinien	12
1.3.4. Verstärkte Sicherheitskonfiguration für IE	13
1.3.5. Netzwerkadapter	14
1.3.6. Ordneroptionen	15
2. RouterOS und VMnet konfigurieren	16
3. Neue Gesamtstruktur aufsetzen	19
4. Client in Domäne einbinden	23
5. Active Directory erste Schritte	26
5.1. User und Gruppen.....	26
5.2. UNC.....	27
5.2.1. UNC unter WIN	27
5.2.2. UNC unter Unix	27
5.3. Freigabe erstellen.....	27
5.4. AD – Papierkorb.....	29
5.4.1. Was ist das?.....	29
5.4.2. Vor- und Nachteile.....	29
5.4.3. Aktivieren des AD - Papierkorb.....	29
5.5. ABE	31
5.5.1. Was ist das?.....	31
5.5.2. Aktivierung von ABE.....	31
6. Directory Information Tree.....	34
6.1. DIT erstellen.....	34
6.1.1. Struktur – Allgemein	35
6.1.2. Struktur – Detailliert.....	35
6.2. Struktur im AD anlegen	36
7. DC2 zur Gesamtstruktur hinzufügen.....	37
7.1. Domain Controller hinzufügen	37
8. DNS in Active Directory	38
8.1. Fragen über DNS in Active Directory	38
8.2. Neue Forward-Zone übertragen	39
9. Mit GPOs arbeiten	40
9.1. Netzlaufwerk mit GPO erzeugen.....	40
9.2. Verknüpfung auf dem Desktop anlegen	41
9.3. Verändern der Passworrichtlinien	42
9.4. GPResult	42
10. Konfigurieren von Standorten und Subnetzen	43

11. GPO mit Standort verknüpfen	44
12. Roaming Profiles und Folder Redirection.....	46
13. Deploy MSI mit GPO.....	47
14. ADDS - DNS und Replikation Fehleranalyse	48
14.1. Replmon	48
14.2. RepAdmin	48
14.3. DCDiag	48
14.3.1. Bestandene Tests	48
14.4. Gruppenrichtlinien-Eventlog.....	49
14.5. Active Directory Log Level	52
15. LDAP – PowerShell Tool.....	52
15.1. LDAP Abfragen und LDAP Queries (CMD Prompt)	52
15.2. LDAP Abfragen und LDAP Queries (PowerShell).....	52
15.2.1. Benutzeranleitung	52
16. DFS einrichten und Namespace anlegen	53

1. Planen und VMs vorbereiten

Hinweise

Verwenden Sie als VM-Netz immer «Host-only», sofern Sie allein arbeiten. Ansonsten können Sie Probleme mit Ihren Klassenkameraden im selben physischen Netzwerk bekommen. Alle die zu zweit über zwei Notebook hinweg arbeiten, müssen Ihre Subnetze mit der Lehrperson absprechen, damit es keine doppelten Subnetze gibt. Dazu wird auf dem BSCW eine Liste geführt «Subnetze.xlsx»

Auf dem Server 1 und dem Server 2 werden jeweils ein DNS-Serverdienst installiert. Server 1 soll den DNS-Server von Server 2 als primären DNS-Server verwenden und umgekehrt. Natürlich kann diese Konfiguration produktiv erst vorgenommen werden, wenn Server 2 über den installierten DNS-Dienst verfügt.

Demote = Herabstufen eines Domänencontrollers (Wenn dieser aus der AD-Umgebung entfernt wird)

Verwenden Sie als Domänenname einen einfachen Namen bestehend aus a-z & 0-9

1.1. Spezifikation

Domäne

Domänenname	Base.dom
Domänenadministrator	a_tk3ll
Kennwort Domänenadministrator	Admin1234!

Standort 1

Name	Zürich
Subnetz	10.11.1.0/24
DC-Name	mtzhwdc01
DC-IP-Adresse (CIDR)	10.11.1.10/24

Standort 2

Name	Oberengstringen
Subnetz	10.11.2.0/24
DC-Name	mtzowdc02
DC-IP-Adresse (CIDR)	10.11.2.10/24

Router

IP-Adresse Interface 1 (CIDR)	10.11.1.1
VM-Netz Interface 1	eth1
IP-Adresse Interface 2 (CIDR)	10.11.2.1
VM-Netz Interface 2	eth2

DC1 (Windows Server Desktop)

Name	mtzhwdc01
IP-Adresse (CIDR)	10.11.1.10/24
VM-Netz Netzwerk-Interface	eth0
Gateway	10.11.1.1
DNS-Server1	10.11.2.10
DNS-Server2	10.11.1.10
Lokaler Administrator	Administrator
Kennwort lokaler Administrator	Admin1234!
Kennwort-Demote	Admin1234!

DC2 (Windows Server Desktop)

Name	mtzowdc02
IP-Adresse (CIDR)	10.11.2.10/24
VM-Netz Netzwerk-Interface	eth0
Gateway	10.11.2.1
DNS-Server1	10.11.1.10
DNS-Server2	10.11.2.10
Lokaler Administrator	Administrator
Kennwort lokaler Administrator	Admin1234!
Kennwort-Demote	Admin1234!

DC3 (Windows Server Core)

Name	mtzhwdc03
IP-Adresse (CIDR)	10.11.1.12/24
VM-Netz Netzwerk-Interface	eth0
Gateway	10.11.1.1
DNS-Server1	10.11.2.10
DNS-Server2	10.11.1.10
Lokaler Administrator	Administrator
Kennwort lokaler Administrator	Admin1234!
Kennwort-Demote	Admin1234!

Client1

Name	c00001
IP-Adresse (CIDR)	10.11.1.11/24
VM-Netz Netzwerk-Interface	eth0
Gateway	10.11.1.1
DNS-Server1	10.11.1.10
DNS-Server2	10.11.2.10
Lokaler Administrator	Administrator
Kennwort Lokaler Administrator	Admin1234!

Client2

Name	c00002
IP-Adresse (CIDR)	10.11.1.11/24
VM-Netz Netzwerk-Interface	eth0
Gateway	10.11.1.1
DNS-Server1	10.11.1.10
DNS-Server2	10.11.2.10
Lokaler Administrator	Administrator
Kennwort Lokaler Administrator	Admin1234!

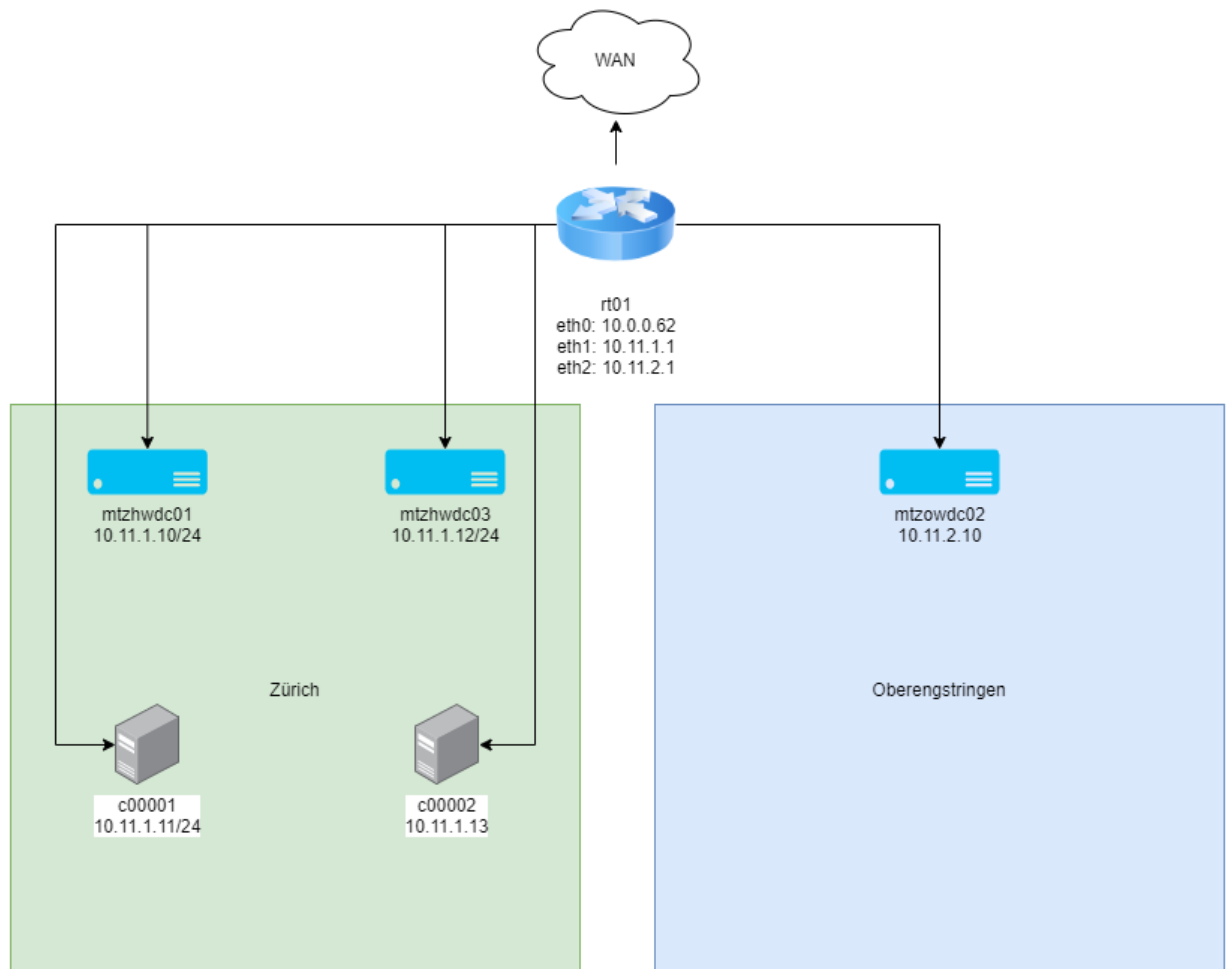
AD Testbenutzer ohne Domänenadministrationsrechten

Login	tk3ll
Passwort	Admin1234!

AD Testbenutzer mit Domänenadministrationsrechten

Login	a_tk3ll
Passwort	Admin1234!

1.2. Logische Netzwerklayout

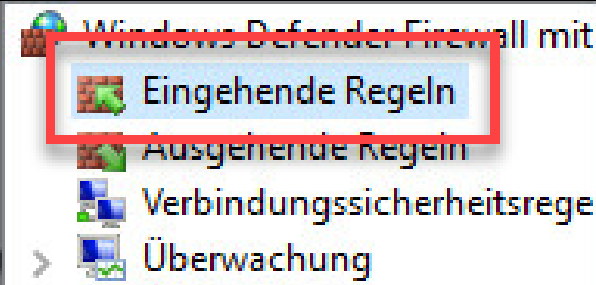
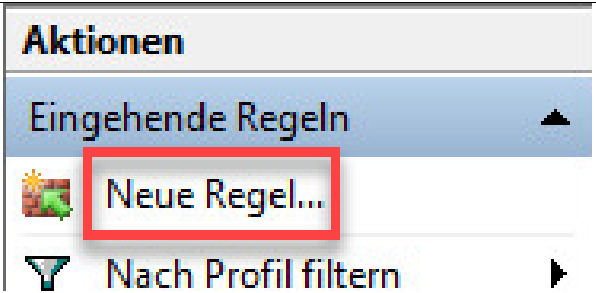
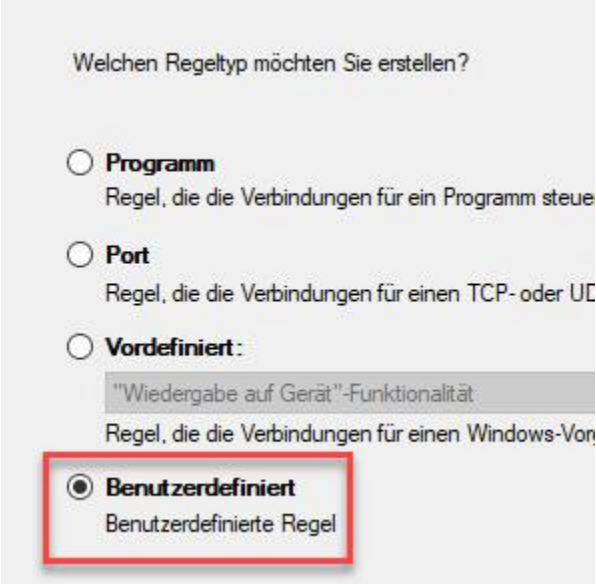
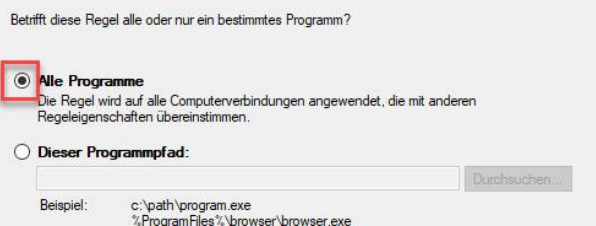


Der Standort des C00002 kann innerhalb der LB2 verändert werden, da einige Aufgaben einen Client im Subnetz Oberengstringen benötigen. In diesem Fall wird die letzte Oktette der IP-Adresse übernommen. Der Netzanteil wird entsprechend verändert sowie die DNS-Server (gemäss Vorgaben, jeweilig anderen DNS-Server).

1.3. Standardeinstellung

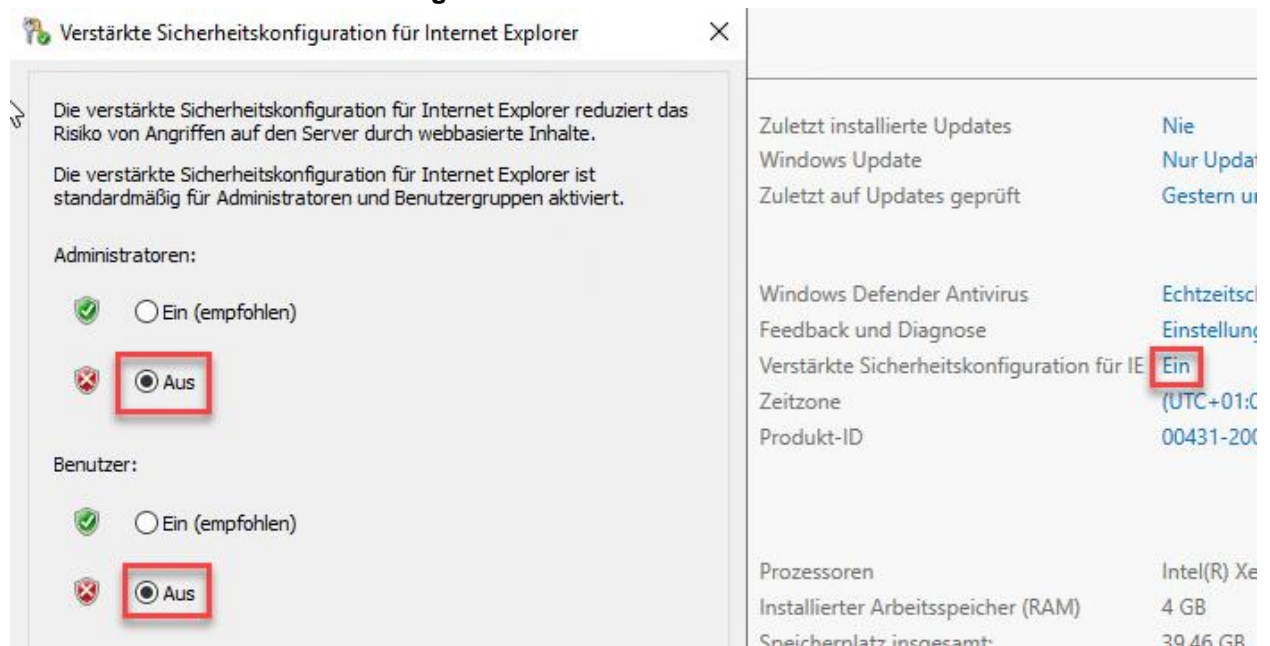
Folgende Einstellungen müssen Sie auf sämtliches System vornehmen. Auf dem «Windows Core Server» müssen Sie lediglich 1.3.1 und 1.3.2 einstellen.

1.3.1. Firewall

Ping erlauben	
Bild	Text
	<p>Zu Beginn öffnen wir die Windows Firewall und wählen den Punkt «Eingehende Regeln» aus.</p>
	<p>Danach kann man oben rechts auf «neue Regel...» klicken.</p>
	<p>Nun wählt man im öffnenden Fenster den Punkt «Benutzerdefiniert» aus.</p>
	<p>Dann muss man auswählen, für welche Programme die Regel gelten sollte. Hier wählt man «Alle Programme»</p>

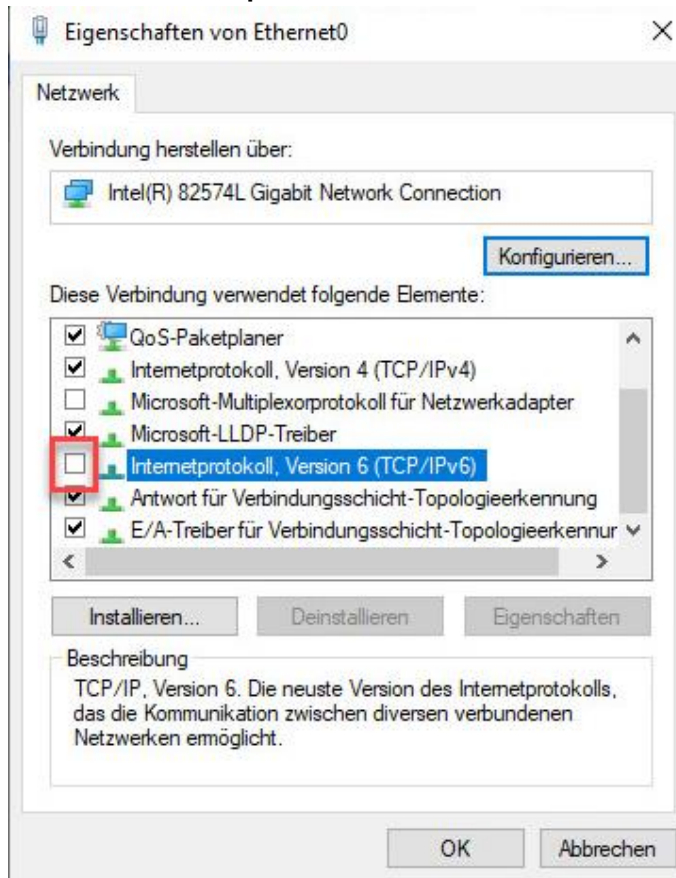
<p>Für welche Ports und Protokolle gilt diese Regel?</p> <p>Protokolltyp: ICMPv4</p> <p>Protokollnummer: 1</p> <p>Lokaler Port: Alle Ports</p> <p>Beispiel: 80, 443, 5000-5010</p> <p>Remoteport: Alle Ports</p> <p>Beispiel: 80, 443, 5000-5010</p> <p>ICMP-Einstellungen: Anpassen...</p>	<p>Nun muss man den entsprechenden Protokoll Typ auswählen => ICMPv4. Danach klickt man auf «Anpassen...»</p>
<p>Diese Regel auf die folgenden ICMP-Verbindungen (Internet Control Message-Protokoll) anwenden:</p> <p><input type="radio"/> Alle ICMP-Typen</p> <p><input checked="" type="radio"/> Bestimmte ICMP-Typen</p> <ul style="list-style-type: none"><input type="checkbox"/> Zu großes Paket<input type="checkbox"/> Ziel nicht erreichbar<input type="checkbox"/> Quelldrosselung<input type="checkbox"/> Umleiten<input checked="" type="checkbox"/> Echoanforderung<input type="checkbox"/> Routerankündigung<input type="checkbox"/> Routeranfrage<input type="checkbox"/> Zeit überschritten<input type="checkbox"/> Parameterproblem<input type="checkbox"/> Zeitstempelanforderung<input type="checkbox"/> Adressmaskenanforderung	<p>Nun wählt man «Bestimmten ICMP-Typen» aus. Zudem setzt man ein Haken bei «Echoanforderung».</p>
<p>Für welche lokalen IP-Adressen gilt diese Regel?</p> <p><input checked="" type="radio"/> Beliebige IP-Adresse</p> <p><input type="radio"/> Diese IP-Adressen:</p> <p>Hinzufügen... Bearbeiten... Entfernen</p> <p>Passen Sie Schnittstellentypen an, für die die Regel angewendet wird: Anpassen...</p> <p>Für welche Remote-IP-Adressen gilt diese Regel?</p> <p><input checked="" type="radio"/> Beliebige IP-Adresse</p> <p><input type="radio"/> Diese IP-Adressen:</p> <p>Hinzufügen... Bearbeiten... Entfernen</p> <p>< Zurück Weiter > Abbrechen</p>	<p>In diesem Schritt kann man alles bei den bereits gesetzten Werten belassen.</p>

1.3.4. Verstärkte Sicherheitskonfiguration für IE



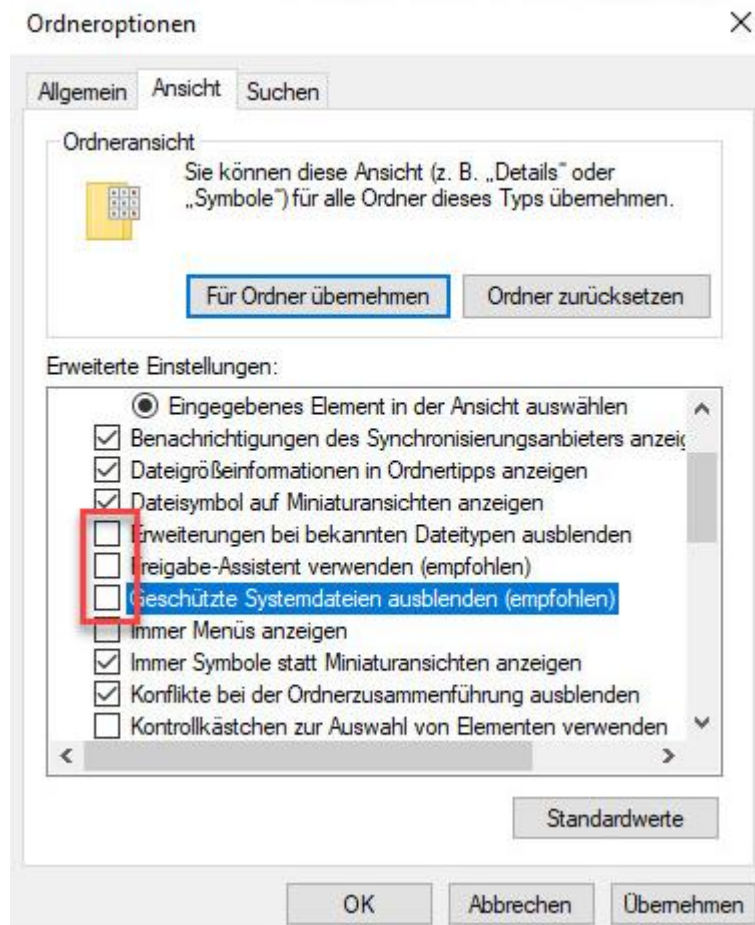
Um die verstärkten Sicherheitskonfigurationen für den IE auszuschalten, öffnet man den Server-Manager und dann links auf den Reiter «Lokaler Server». Hier muss man dann auf den Punkt «Verstärkte Sicherheitskonfiguration für IE» gehen. Danach öffnet sich ein Fenster in welchem man beide Werte auf «Aus» setzen.

1.3.5. Netzwerkadapter



Auf dem Netzwerkadapter muss man nur den Haken bei «Internetprotokoll, Version 6 (TCP/IPv6)» entfernen.

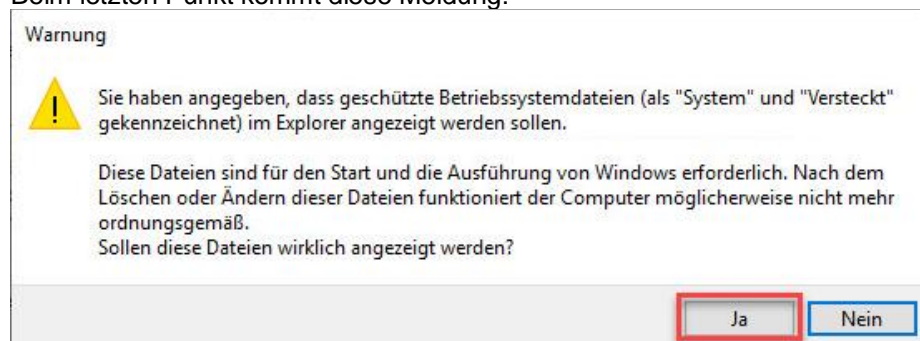
1.3.6. Ordneroptionen



Bei folgenden Punkten muss man den Haken entfernen:

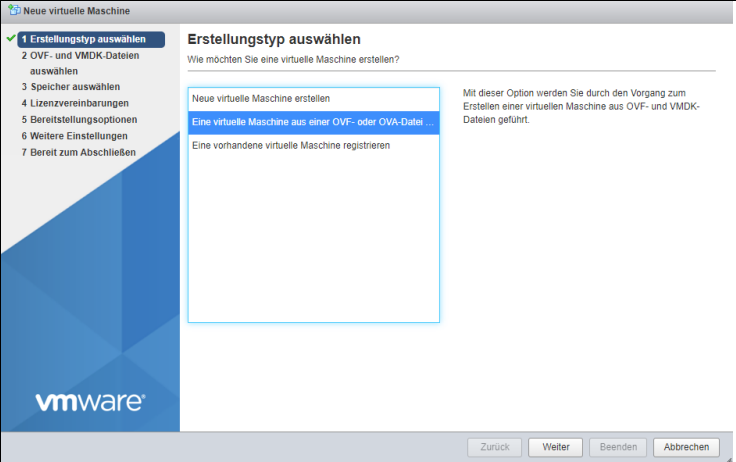
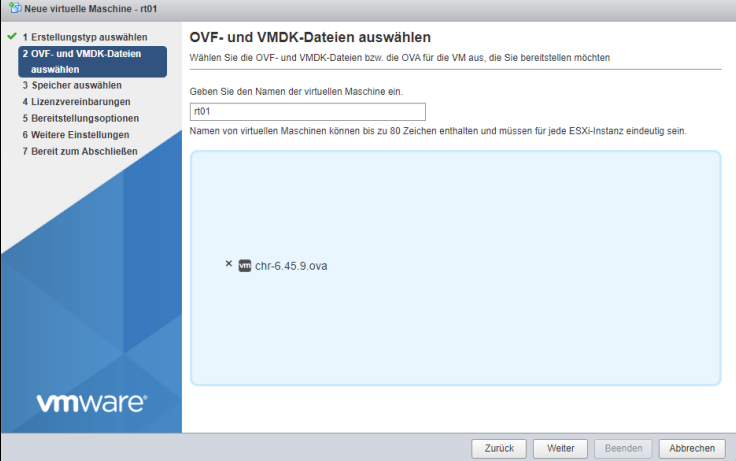
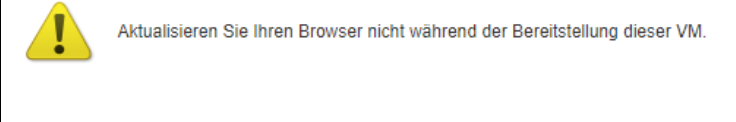
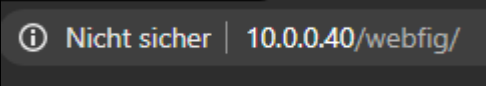
- Erweiterung bei bekannten Dateitypen ausblenden
- Freigabe-Assistent verwenden (empfohlen)
- Geschützte Systemdatei ausblenden (empfohlen)

Beim letzten Punkt kommt diese Meldung:



Wenn diese Meldung auftaucht, einfach mit «Ja» bestätigen.

2. RouterOS und VMnet konfigurieren

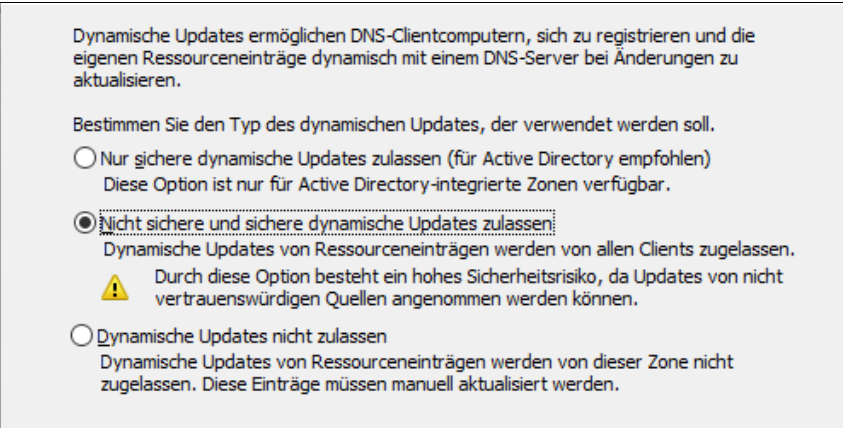

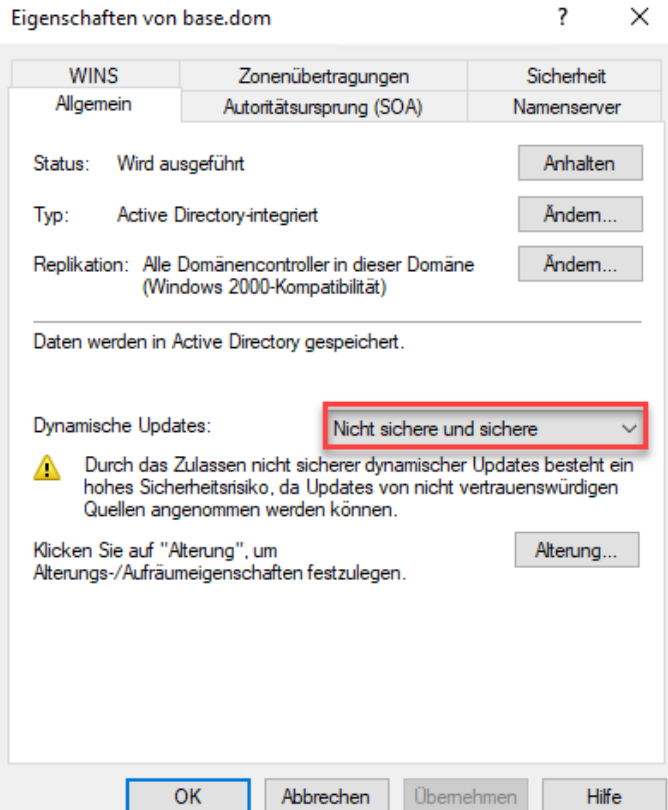

Router OS ESX und erste Konfiguration		
Bild		Text
		Im ESX muss man nun als Erstellungstyp eine OVA Datei auswählen.
		Sobald diese von ESx richtig erkannt wird, wird die VM aufbereitet.
		Während dem Aufbereitungsprozess, sollte der Browser nicht neu gestartet werden.
		Nun kann man im Browser, die entsprechende IP-Adresse eingeben.

Mode	<input checked="" type="radio"/> Router <input type="radio"/> Bridge
Address Acquisition	<input checked="" type="radio"/> Static <input type="radio"/> Automatic <input type="radio"/> PPPoE
IP Address	<input type="text" value="10.0.0.66"/>
Netmask	<input type="text" value="255.255.255.0 (/24)"/> ▼
Gateway	<input type="text" value="10.0.0.1"/>
DNS Servers	▼
MAC Address	<input type="text" value="00:0C:29:25:70:14"/>
IP Address	<input type="text" value="10.11.1.1"/>
Netmask	<input type="text" value="255.255.255.0 (/24)"/> ▼
DHCP Server	<input checked="" type="checkbox"/>
DHCP Server Range	▲ <input type="text" value="10.11.1.240"/>
NAT	<input checked="" type="checkbox"/>
VPN Access	<input type="checkbox"/>
VPN Address	10.0.0.40
Router Identity	<input type="text" value="MikroTik"/>
Password	<input type="password" value="....."/>
Confirm Password	<input type="password" value="....."/>

Und danach beginnt im Browser, der Einrichtungsprozess. Nun kann man die gewünschten Parameter eingeben.

<pre>Ethernet-Adapter Ethernet0: Verbindungsspezifisches DNS-Suffix: IPv4-Adresse : 10.11.1.10 Subnetzmaske : 255.255.255.0 Standardgateway : 10.11.1.1 C:\Users\Administrator>ping 10.11.2.10 Ping wird ausgeführt für 10.11.2.10 mit 32 Bytes Daten: Antwort von 10.11.2.10: Bytes=32 Zeit<1ms TTL=127 Antwort von 10.11.2.10: Bytes=32 Zeit<1ms TTL=127 Antwort von 10.11.2.10: Bytes=32 Zeit<1ms TTL=127 Antwort von 10.11.2.10: Bytes=32 Zeit<1ms TTL=127 Ping-Statistik für 10.11.2.10: Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust), Ca. Zeitangaben in Millisek.: Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms</pre>	<p>Folgendes Ergebnis erhalte ich, wenn ich versuche den anderen DC zu erreichen. Der Ping ist erfolgreich, das Routing funktioniert.</p>
<pre>Ethernet-Adapter Ethernet0: Verbindungsspezifisches DNS-Suffix: IPv4-Adresse : 10.11.2.10 Subnetzmaske : 255.255.255.0 Standardgateway : 10.11.2.1 C:\Users\Administrator>ping 10.11.1.10 Ping wird ausgeführt für 10.11.1.10 mit 32 Bytes Daten: Antwort von 10.11.1.10: Bytes=32 Zeit<1ms TTL=127 Antwort von 10.11.1.10: Bytes=32 Zeit<1ms TTL=127 Antwort von 10.11.1.10: Bytes=32 Zeit<1ms TTL=127 Antwort von 10.11.1.10: Bytes=32 Zeit<1ms TTL=127 Ping-Statistik für 10.11.1.10: Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust), Ca. Zeitangaben in Millisek.: Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms</pre>	<p>Folgendes Ergebnis erhalte ich, wenn ich versuche den anderen DC zu erreichen. Der Ping ist erfolgreich, das Routing funktioniert.</p>

3. Neue Gesamtstruktur aufsetzen

Active Directory & DNS	
Bild	Text
 <p>Dynamische Updates ermöglichen DNS-Clientcomputern, sich zu registrieren und die eigenen Ressourceneinträge dynamisch mit einem DNS-Server bei Änderungen zu aktualisieren.</p> <p>Bestimmen Sie den Typ des dynamischen Updates, der verwendet werden soll.</p> <p><input type="radio"/> Nur sichere dynamische Updates zulassen (für Active Directory empfohlen) Diese Option ist nur für Active Directory-integrierte Zonen verfügbar.</p> <p><input checked="" type="radio"/> <u>Nicht sichere und sichere dynamische Updates zulassen</u> Dynamische Updates von Ressourceneinträgen werden von allen Clients zugelassen.</p> <p> Durch diese Option besteht ein hohes Sicherheitsrisiko, da Updates von nicht vertrauenswürdigen Quellen angenommen werden können.</p> <p><input type="radio"/> Dynamische Updates nicht zulassen Dynamische Updates von Ressourceneinträgen werden von dieser Zone nicht zugelassen. Diese Einträge müssen manuell aktualisiert werden.</p>	<p>Bei der Einrichtung der einzelnen Zonen ist wichtig, dass man «Nicht sichere und sichere dynamische Updates» zulässt.</p>
 <p>Eigenschaften von base.dom</p> <p>WINS Zonenübertragungen Sicherheit Allgemein Autoritätsursprung (SOA) Namensserver</p> <p>Status: Wird ausgeführt <input type="button" value="Anhalten"/></p> <p>Typ: Active Directory-integriert <input type="button" value="Ändern..."/></p> <p>Replikation: Alle Domänencontroller in dieser Domäne (Windows 2000-Kompatibilität) <input type="button" value="Ändern..."/></p> <p>Daten werden in Active Directory gespeichert.</p> <p>Dynamische Updates: Nicht sichere und sichere <input type="button" value="v"/></p> <p> Durch das Zulassen nicht sicherer dynamischer Updates besteht ein hohes Sicherheitsrisiko, da Updates von nicht vertrauenswürdigen Quellen angenommen werden können.</p> <p>Klicken Sie auf "Alterung", um Alterungs-/Aufräumeigenschaften festzulegen. <input type="button" value="Alterung..."/></p> <p><input type="button" value="OK"/> <input type="button" value="Abbrechen"/> <input type="button" value="Übernehmen"/> <input type="button" value="Hilfe"/></p>	<p>So sieht dann dies auf der AD-Zone aus.</p>

<p>Eigenschaften von MTZHWDC01</p> <table border="1"> <tr> <td>Allgemein</td> <td>Betriebssystem</td> <td>Mitglied von</td> <td>Delegierung</td> <td>Standort</td> </tr> <tr> <td>Verwaltet von</td> <td>Objekt</td> <td>Sicherheit</td> <td>Einwählen</td> <td>Attribut-Editor</td> </tr> </table> <p>Kanonischer Name des Objekts: base.dom/Domain Controllers/MTZHWDC01</p> <p>Objektklasse: Computer</p> <p>Erstellt am: 29.08.2020 14:49:14</p> <p>Geändert am: 29.08.2020 14:59:49</p> <p>Aktualisierungssequenznummer:</p> <p>Aktuelle: 12635</p> <p>Ursprüngliche: 12293</p> <p><input checked="" type="checkbox"/> Objekt vor zufälligem Löschen schützen</p>	Allgemein	Betriebssystem	Mitglied von	Delegierung	Standort	Verwaltet von	Objekt	Sicherheit	Einwählen	Attribut-Editor	<p>Nun fügen wir noch eine Sicherheitseinstellung hinzu. Sodass unser DC nicht aus Versehen gelöscht werden kann. Dafür den DC in der AD öffnen und danach unter dem Reiter «Objekt» den Haken bei «Objekt vor zufälligen Löschen schützen» setzen.</p>
Allgemein	Betriebssystem	Mitglied von	Delegierung	Standort							
Verwaltet von	Objekt	Sicherheit	Einwählen	Attribut-Editor							
<p>Windows-IP-Konfiguration</p> <p>Ethernet-Adapter Ethernet0:</p> <p>Verbindungsspezifisches DNS-Suffix:</p> <p>IPv4-Adresse : 10.11.1.10</p> <p>Subnetzmaske : 255.255.255.0</p> <p>Standardgateway : 10.11.1.1</p> <p>C:\Users\Administrator>nslookup</p> <p>Standardserver: mtzowdc02.base.dom</p> <p>Address: 10.11.2.10</p> <p>> 10.11.2.10</p> <p>Server: mtzowdc02.base.dom</p> <p>Address: 10.11.2.10</p> <p>Name: mtzowdc02.base.dom</p> <p>Address: 10.11.2.10</p> <p>> mtzowdc02</p> <p>Server: mtzowdc02.base.dom</p> <p>Address: 10.11.2.10</p> <p>Name: mtzowdc02.base.dom</p> <p>Address: 10.11.2.10</p>	<p>Der nslookup vom DC01 ist erfolgreich.</p>										

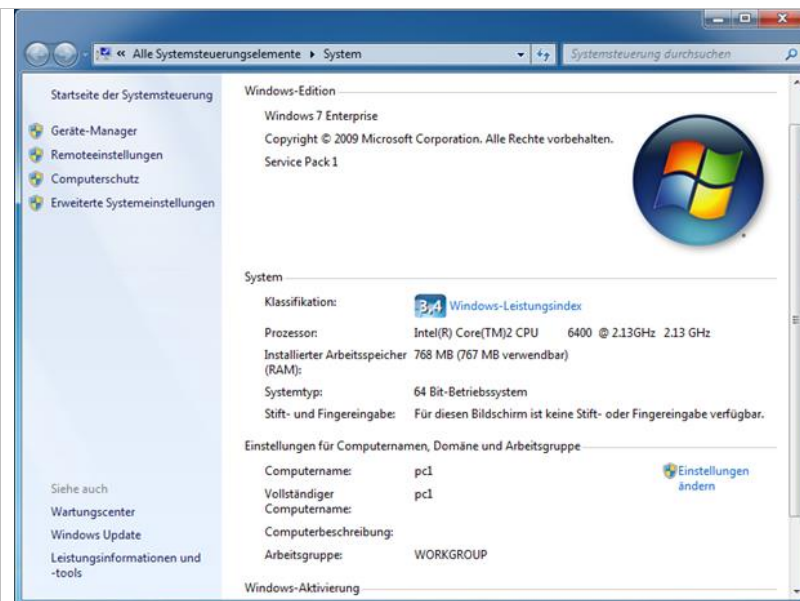
<pre>Ethernet-Adapter Ethernet0: Verbindungsspezifisches DNS-Suffix: IPv4-Adresse : 10.11.1.11 Subnetzmaske : 255.255.255.0 Standardgateway : 10.11.1.1 C:\Windows\system32>nslookup Standardserver: mtzowdc02.base.dom Address: 10.11.2.10 > 10.11.1.13 Server: mtzowdc02.base.dom Address: 10.11.2.10 Name: c00002.base.dom Address: 10.11.1.13 > c00002 Server: mtzowdc02.base.dom Address: 10.11.2.10 Name: c00002.base.dom Address: 10.11.1.13</pre>	<p>Der nslookup vom c00001 ist erfolgreich.</p>
<pre>Ethernet-Adapter Ethernet0: Verbindungsspezifisches DNS-Suffix: IPv4-Adresse : 10.11.1.13 Subnetzmaske : 255.255.255.0 Standardgateway : 10.11.1.1 C:\Windows\system32>nslookup Standardserver: mtzowdc02.base.dom Address: 10.11.2.10 > 10.11.1.11 Server: mtzowdc02.base.dom Address: 10.11.2.10 Name: c00001.base.dom Address: 10.11.1.11 > c00001 Server: mtzowdc02.base.dom Address: 10.11.2.10 Name: c00001.base.dom Address: 10.11.1.11</pre>	<p>Der nslookup vom c00002 ist erfolgreich.</p>

<pre>Windows-IP-Konfiguration Ethernet-Adapter Ethernet0: Verbindungsspezifisches DNS-Suffix: IPv4-Adresse : 10.11.2.10 Subnetzmaske : 255.255.255.0 Standardgateway : 10.11.2.1 C:\Users\Administrator>nslookup Standardserver: mtzhwdc01.base.dom Address: 10.11.1.10 > 10.11.1.10 Server: mtzhwdc01.base.dom Address: 10.11.1.10 Name: mtzhwdc01.base.dom Address: 10.11.1.10 > mtzhwdc01 Server: mtzhwdc01.base.dom Address: 10.11.1.10 Name: mtzhwdc01.base.dom Address: 10.11.1.10</pre>	<p>Der nslookup vom DC02 ist erfolgreich.</p>
--	---

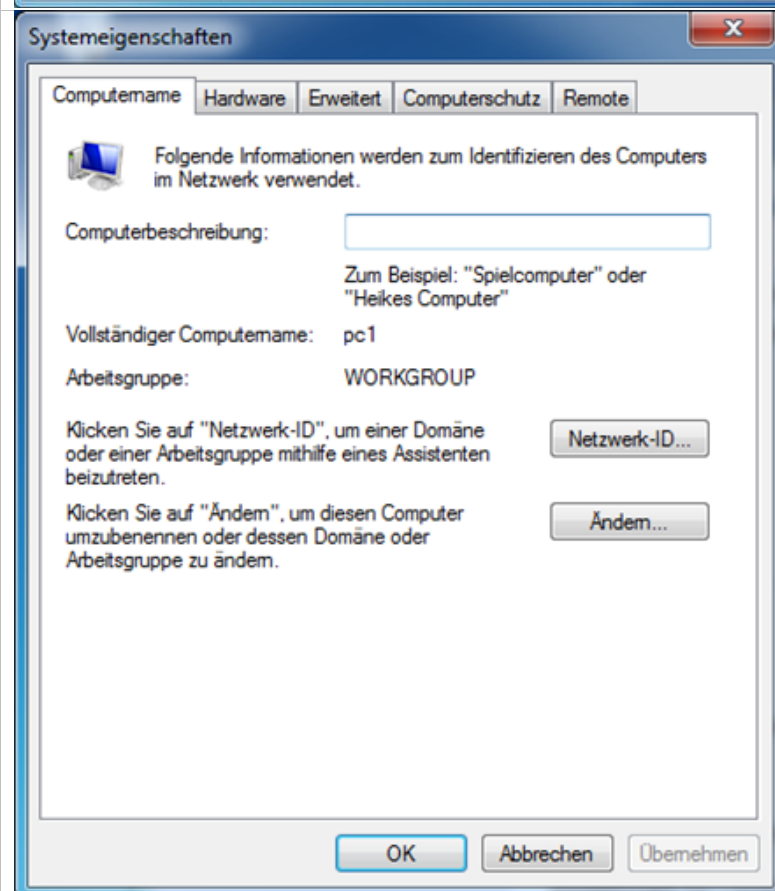
4. Client in Domäne einbinden

Damit der Computer im Active Directory verfügbar ist und Active Directory Benutzer sich anmelden können, muss der Client der Domäne hinzugefügt werden. Im Klartext: Der Computer muss ein Objekt im Active Directory werden.

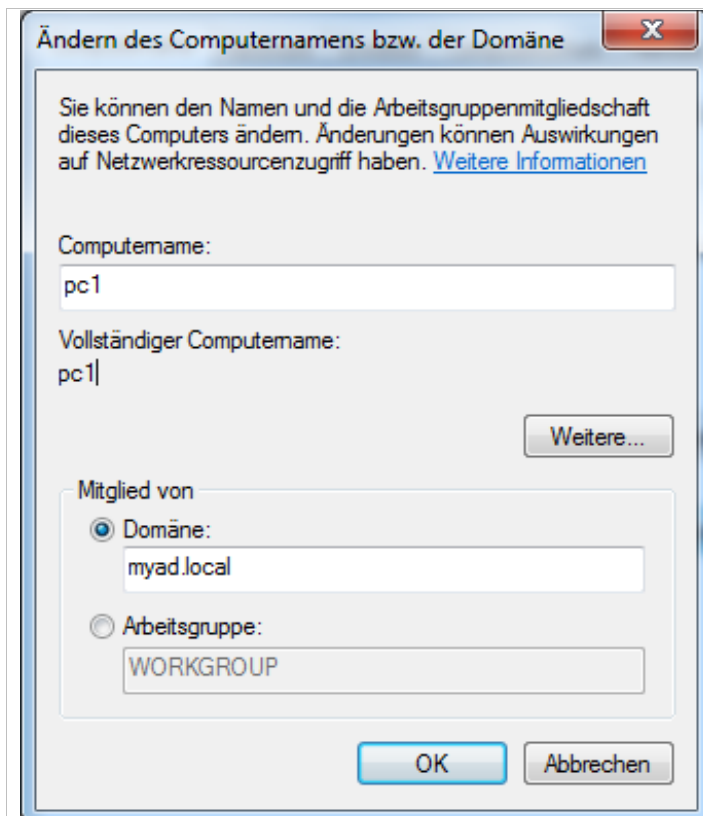
Voraussetzung ist, dass der Domänencontroller und das DNS korrekt installiert sind. Windows 7/10 Home Premium und Basic können keiner Domäne hinzugefügt werden. Hierzu ist Professional, Enterprise, Ultimate oder Education notwendig.



Um den Client in die Domäne aufzunehmen unter **Systemsteuerung\Alle Systemsteuerungselemente\System** im Bereich **Einstellungen für Computernamen, Domäne und Arbeitsgruppe** den Punkt **Einstellungen ändern** aufrufen.

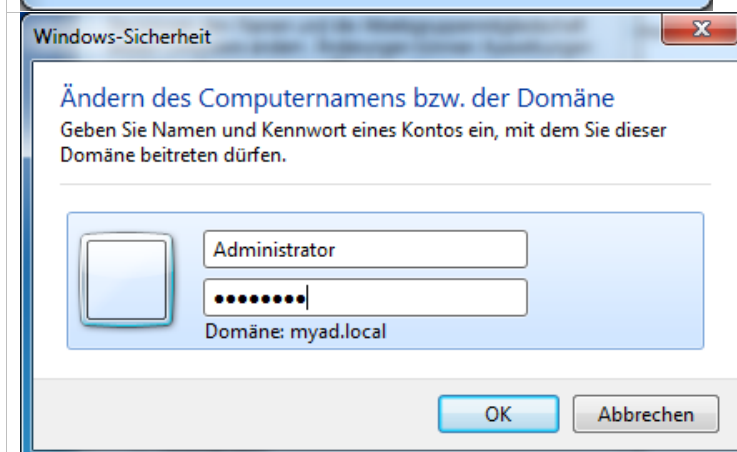


Im Reiter Computername auf **Ändern** klicken.

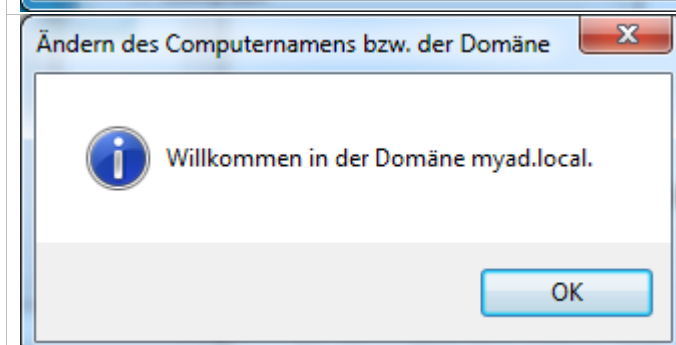


Den Name des Computers angeben. Dieser muss eindeutig sein und darf im Active Directory noch nicht vorhanden sein. Unter Domäne die URL der Domäne eintragen.

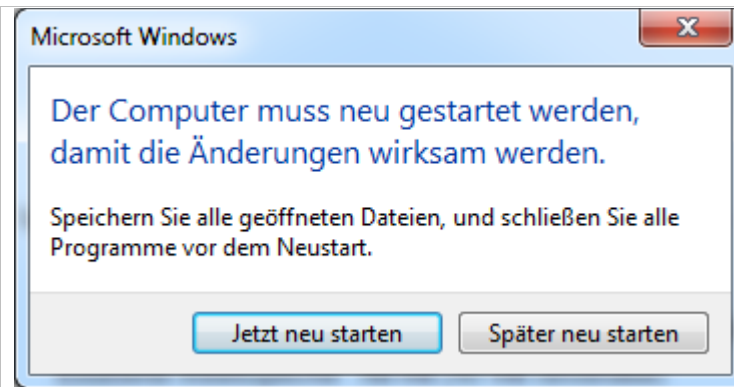
Mit einem Klick auf **OK**, wird nach dem Domänencontroller gesucht. Wurde der Domänencontroller gefunden, erscheint ein Anmeldefenster.



Einen Domänenbenutzer angeben, der über die Rechte verfügt einen Computer der Domäne hinzuzufügen. Standardmäßig haben dieses Recht Domänen-Administratoren.



Nun erhält man folgendes Fenster.

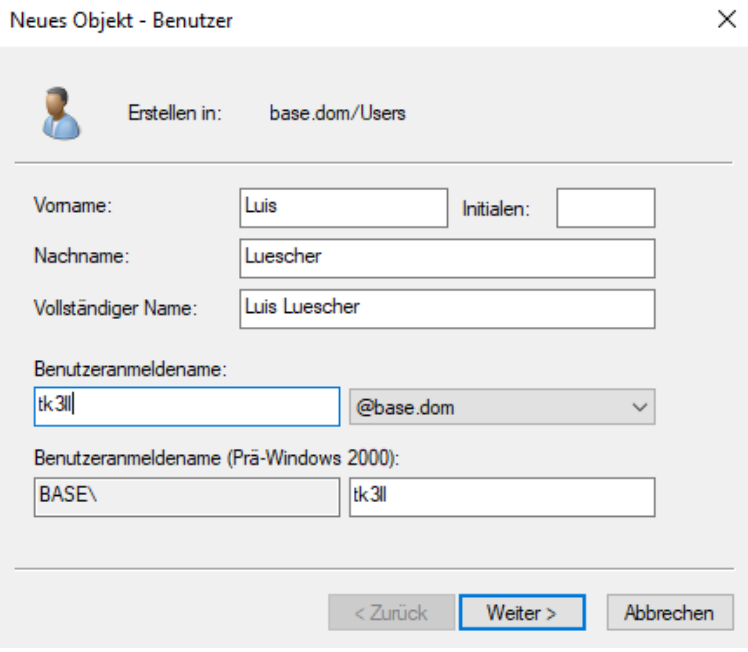
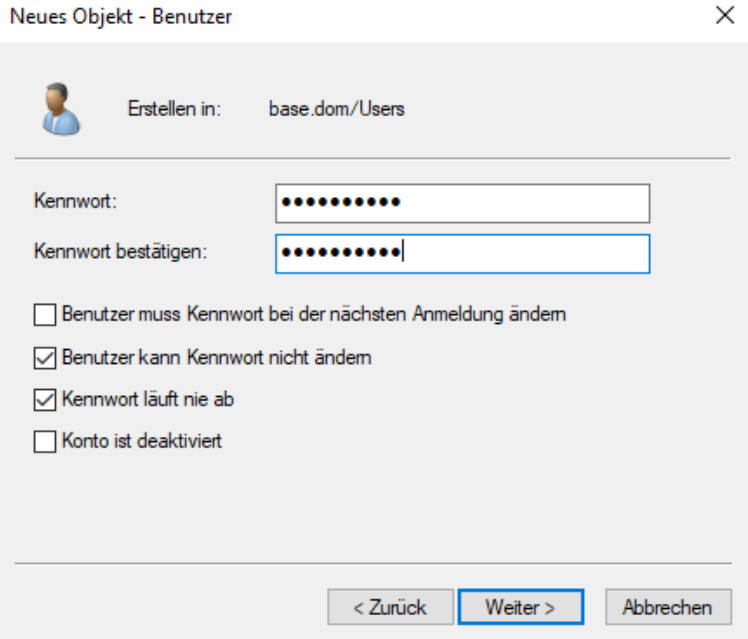


Nach einem Neustart ist der Computer der Domäne hinzugefügt.

Domänenbenutzer können sich jetzt am Computer anmelden. Der neu hinzugefügte Domänencomputer befindet sich standardmäßig in der Organisationseinheit Computer.

5. Active Directory erste Schritte

5.1. User und Gruppen

User erstellen in Active Directory	
Bild	Text
	<p>Im AD muss man unter der OU «Users» mittels rechtsklick auf «Neu» und dann auf «Benutzer». Danach öffnet sich dieses Fenster. Hier kann man verschiedene Werte für den User angeben. Wie den Namen und den entsprechenden Benutzernamen. Die Werte kann man mit «Weiter» bestätigen.</p>
	<p>Nun muss man noch das Benutzerkennwort angeben. Ich habe zudem noch eingestellt, dass der User das Passwort nicht zurücksetzen kann und das Passwort nie abläuft. Der User wird dann mittels «Weiter» erstellt.</p>

5.2. UNC

Uniform Naming Convention kurz UNC wird zur Bezeichnung von Adressen freigegebener Betriebsmittel in einem Rechnernetz genutzt. Die UNC-Adresse stellt einen Netzwerkpfad dar, über den man Ressourcen anderer Rechner in dem Netzwerk ansprechen und nutzen kann.

5.2.1. UNC unter WIN

Das Format eines solchen Netzwerkpfades unter Windows ist:

\\Servername\Freigabe\Pfad bzw. \\IP-Adresse\Freigabe\Pfad

5.2.2. UNC unter Unix

Das Eingabeformat unter Unix ist:

//Servername/Freigabe/Pfad bzw. //IP-Adresse/Freigabe/Pfad

5.3. Freigabe erstellen

Version 10.0.17763.2701

Freigabename	Ordnerpfad	Typ	Anzahl der Clientverbindungen	Beschreibung	Aktionen
ADMIN\$	C:\Windows	Windows	0	Remoteverwaltung	Freigeben
C\$	C:\	Windows	0	Standardfreigabe	Weitere Aktion
Daten	C:\Daten	Windows	0	Alle Daten der Freigabe	
IPC\$		Windows	0	Remote-IPC	
NETLOGON	C:\Windows\SYSVOL	Windows	0	Ressource für Authentifizierung	
SYSVOL	C:\Windows\SYSVOL	Windows	1	Ressource für Authentifizierung	

So sieht die entsprechende Freigabe in der Computerverwaltung aus.

Netzwerkfehler

Auf \\MTZHWDC01\Daten konnte nicht zugegriffen werden.

Sie haben keine Berechtigung für den Zugriff auf \\MTZHWDC01\Daten. Wenden Sie sich an den Netzwerkadministrator, um den Zugriff anzufordern.

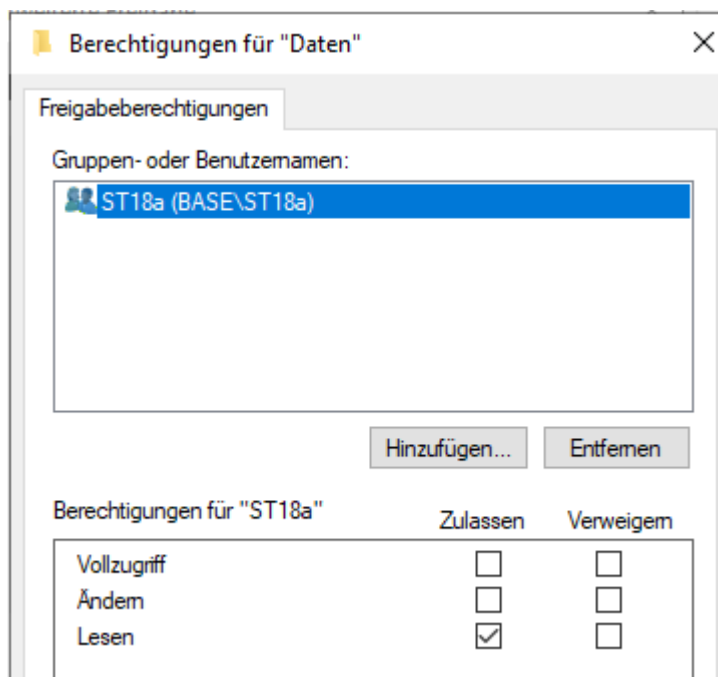
[Weitere Informationen zu Berechtigungen finden Sie unter "Windows-Hilfe und Support".](#)

Schließen

Als ich versuche mit dem Admin auf den freigegebenen Ordner zuzugreifen, erhalte ich folgende Meldung. Der Zugriff ist für diesen User nicht gewährleistet.



Für den User «tk3ll» in der Gruppe ST18a ist der Zugriff möglich. Da die Gruppe ST18a berechtigt ist.



Die Gruppe «ST18a» ist berechtigt auf dem freigegebenen Ordner zu Lesen.

5.4. AD – Papierkorb

5.4.1. Was ist das?

Der AD-Papierkorb gibt es seit Windows Server 2008 R2. Er erlaubt es, versehentlich gelöschte Objekte im laufenden Betrieb wiederherzustellen, das heisst ohne einen DC für eine autorisierte Wiederherstellung von AD-Objekten aus dem AD-backup offline nehmen. Der AD-Papierkorb ist in der Voreinstellung nicht eingeschaltet.

5.4.2. Vor- und Nachteile

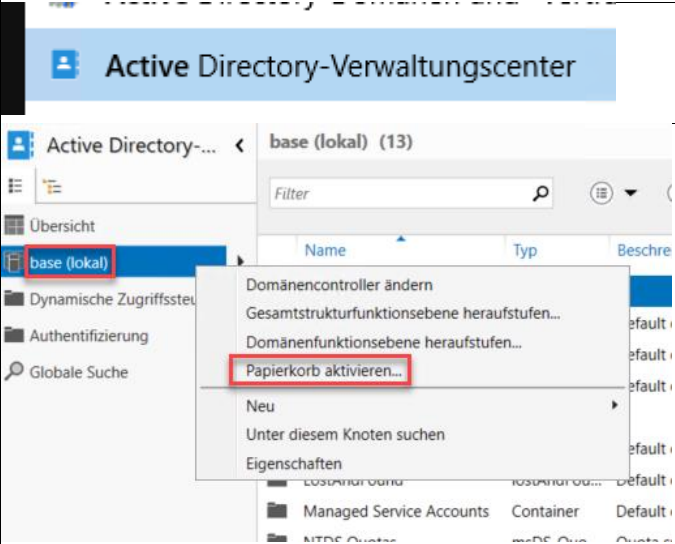
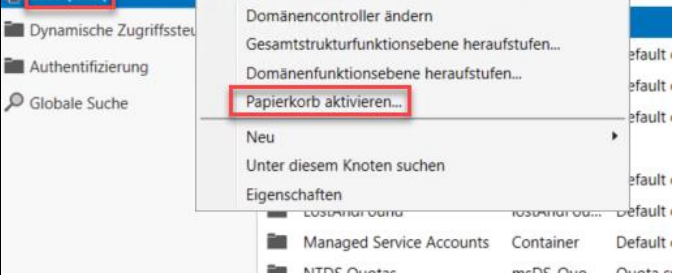
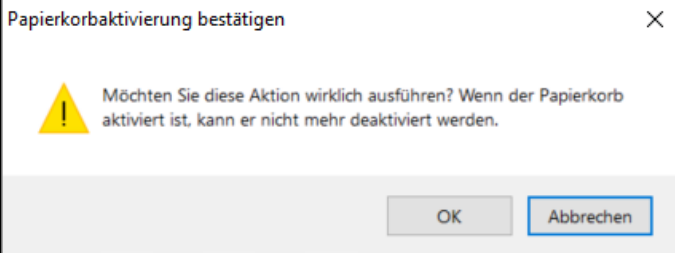
Vorteile:

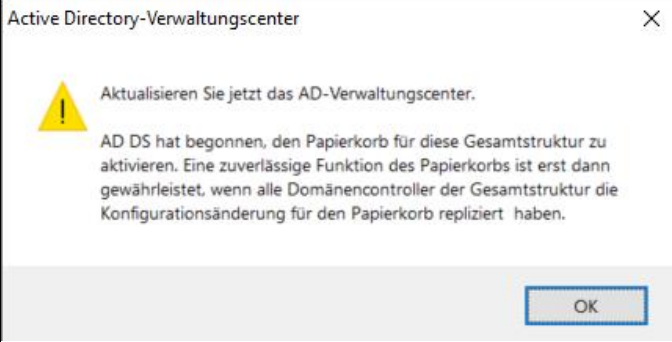
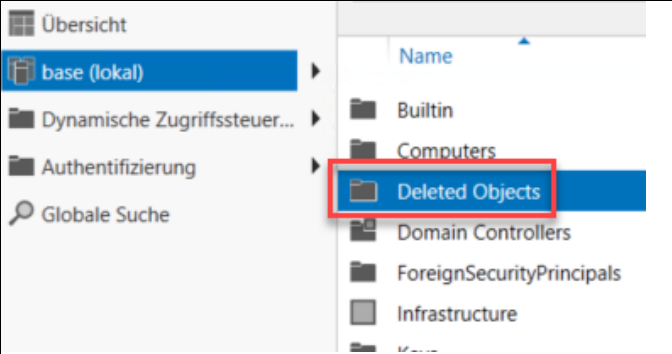
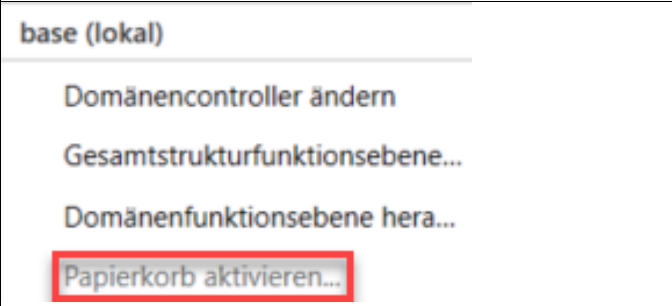
- Kein aufwändiges Backup der Verzeichnisdatenbank mehr notwendig.
- Wenn man aus Versehen etwas löscht, kann dies rückgängig gemacht werden.
- Die Attribute der einzelnen Objekte werden gespeichert (Im Gegensatz zu der «Reanimierung» der Tombstone)
- Objekte werden nur entfernt und nicht als gelöscht angezeigt (Vor- und Nachteil)

Nachteil:

- Die Aktivierung kann nicht rückgängig gemacht werden.
- Kann zu Performance Problemen führen, wenn zu voll.
- Objekte werden nur entfernt und nicht als gelöscht angezeigt (Vor- und Nachteil)

5.4.3. Aktivieren des AD - Papierkorb

Wie aktiviert man den AD – Papierkorb	
Bild	Text
	Zu Beginn öffnet man das AD-Verwaltungscenter
	Danach wählt man die entsprechende Domäne aus und öffnet mittels rechtsklick dieses Menü. Hier kann man dann auf «Papierkorb aktivieren» klicken.
	Nun kann man die Papierkorbaktivierung bestätigen, indem man auf «OK» klickt.

	<p>Diese Warnmeldung kann man einfach mittels «OK» bestätigen. Man muss nur noch das Verwaltungszentrum kurz aktivieren.</p>
	<p>Nun sieht man einen Ordner «Deleted Objects» dies ist der Papierkorb.</p>
	<p>Um zu überprüfen, ob die Installation erfolgreich war, kann man einfach schauen, ob es möglich ist den Papierkorb zu aktivieren. Ist dies ausgegraut, dann ist der Papierkorb aktiviert.</p>

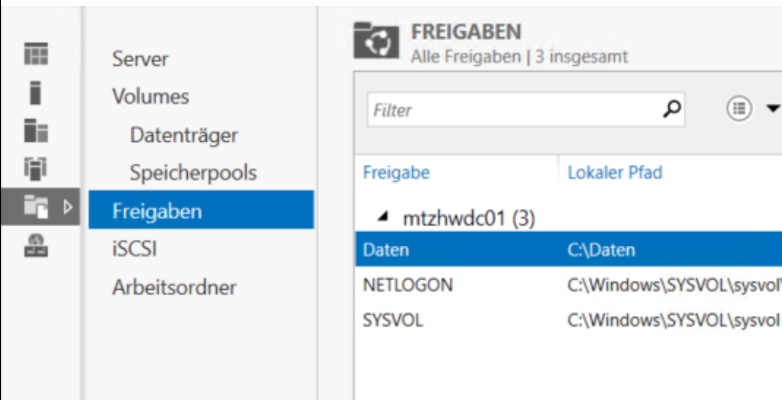
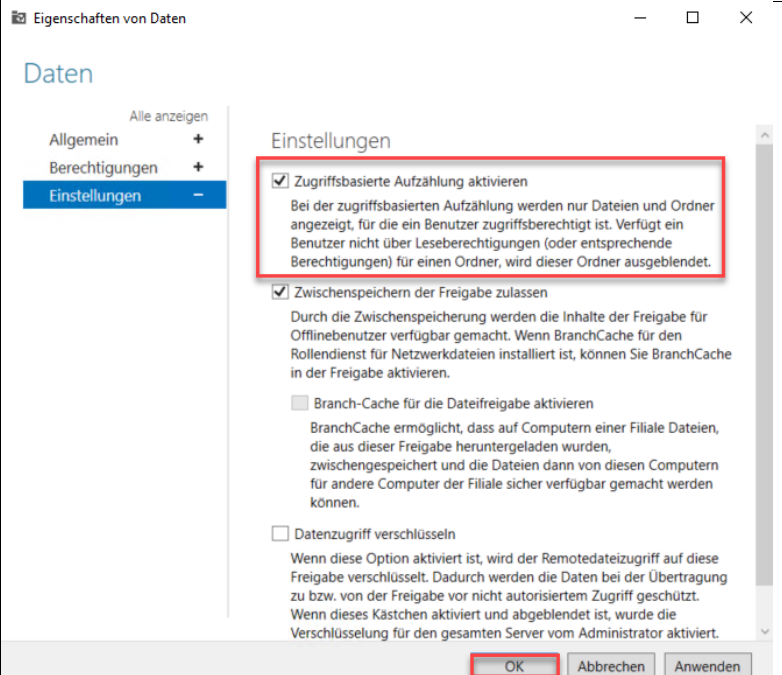
5.5. ABE

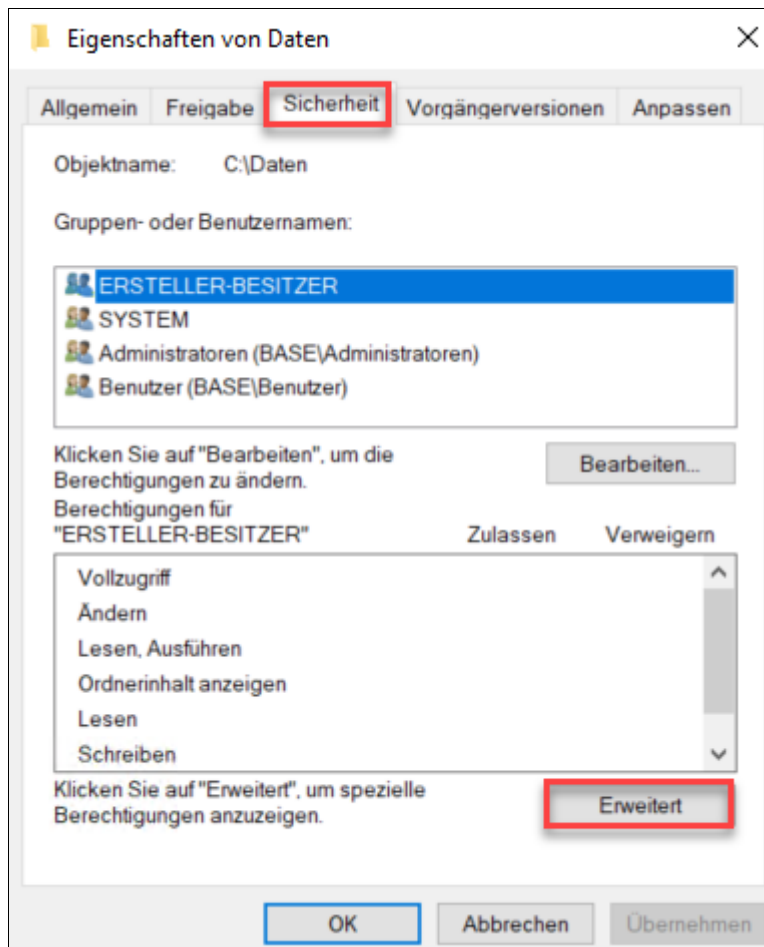
5.5.1. Was ist das?

Unter Windows Server 2003 R2 führte Microsoft die Access Based Enumeration kurz ABE oder zu Deutsch Zugriffsbasierte Aufzählung als separat zu installierendes Add-on ein. Seine Aufgabe besteht darin, Ordner und Dateien für Benutzer auszublenden, wenn sie dafür nicht die erforderlichen Zugriffsrechte besitzen.

Das wesentliche Anliegen hinter den ABE besteht darin, Benutzern von File-Servern einen höheren Komfort zu bieten und gleichzeitig mehr Sicherheit zu erreichen. Sie verhindern, dass Anwender durch Verzeichnisbäume navigieren können, in denen sie ohnehin keine Befugnisse haben. Dies erhöht vor allem für weniger geübte User die Übersichtlichkeit und schützt davor, dass Neugierige aufgrund der Ordnerstrukturen Rückschlüsse auf deren Inhalte ziehen.

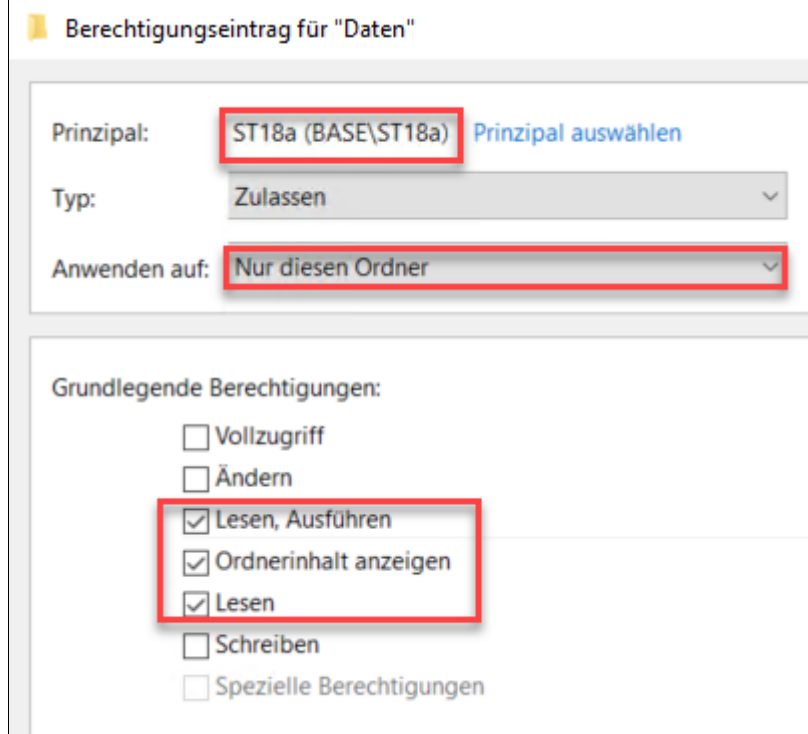
5.5.2. Aktivierung von ABE

Wie aktiviert man ABE?	
Bild	Text
	<p>Zum Beginn öffnet man im Servermanager die Datei-/Speicherdienste => Freigabeneinstellungen. Nun wählt man den entsprechenden Ordner aus. Und öffnet dessen Eigenschaften.</p>
	<p>Nun setzt man unter dem Punkt «Einstellungen» den Haken bei «Zugriffsbasierte Aufzählung aktivieren».</p>

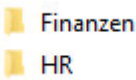
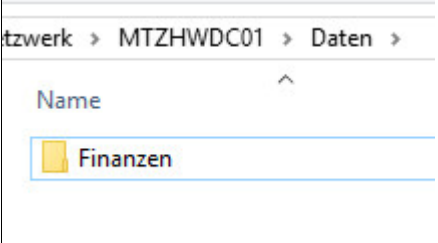
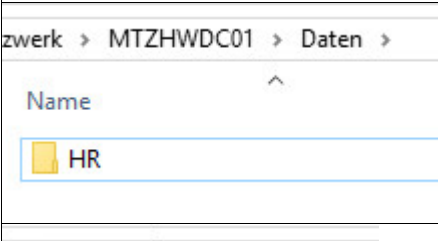
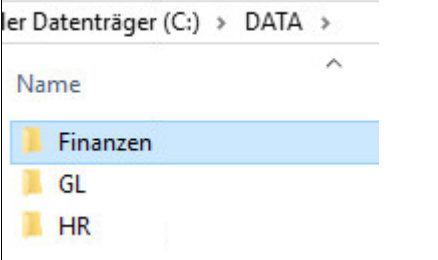
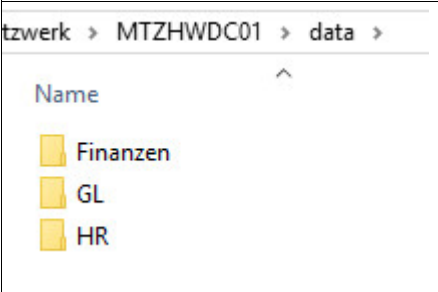
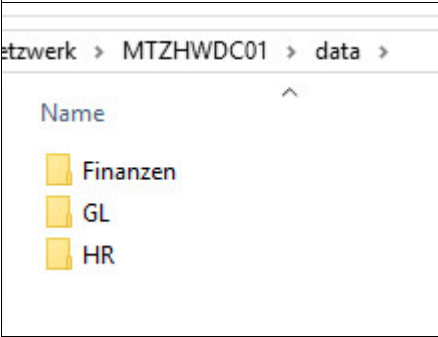


Damit die zugriffsbasierte Aufzählung funktioniert, müssen natürlich die NTFS-Rechte entsprechend gesetzt werden:

1. Eigenschaften des freigegebenen Ordners im Explorer öffnen
2. Sicherheit
3. Erweitert



Nun muss man die entsprechenden Gruppen angeben beim Prinzipal, sowie unter dem Punkt «Anwenden auf:» auf «Nur diesen Ordner» setzen. Die grundlegenden Berechtigung können bei den Standard Werten belassen werden.

	<p>Die entsprechenden Einträge unter dem Punkt Sicherheit sollten auch in den Unterordner erstellt werden. So sieht die Ordnerstruktur auf dem MTZHWDC01 aus. (Sicht des Administrator)</p>
	<p>Der User tk3ll der Gruppe St18a sieht nur den Ordner «Finanzen».</p>
	<p>Der User tk3ir der Gruppe St18b sieht nur den Ordner «HR».</p>
	<p>Auf dem MTZHWDC01 habe ich einen weiteren shared Folder erstellt, welcher <u>kein</u> ABE aktiviert hat.</p>
	<p>Der User tk3ll der Gruppe St18a sieht nur alle Ordner, obwohl die Berechtigungen gesetzt sind.</p>
	<p>Der User tk3ir der Gruppe St18b sieht nur alle Ordner, obwohl die Berechtigungen gesetzt sind.</p>

6. Directory Information Tree

Erstellen Sie aus den nachfolgenden Daten einen passenden DIT und legen sie die entsprechende Struktur in der AD an.

6.1. DIT erstellen

Richtlinien für den DIT:

- ✓ Jede Abteilung kommt im DIT nur einmal vor
- ✓ Standorte sind im DIT abgebildet
- ✓ Alle Abteilungen, welche an beiden Standorten vorkommen, sollen über einen fiktiven Standort mit einem sinnvollen Namen abgedeckt sein
- ✓ Pro Standort gibt es einmal intern und extern

Rot: An beiden Standorten vorhanden.

Blau: Nur an Standort 1 vorhanden.

Grün: Nur an Standort 2 vorhanden.

Standort 1

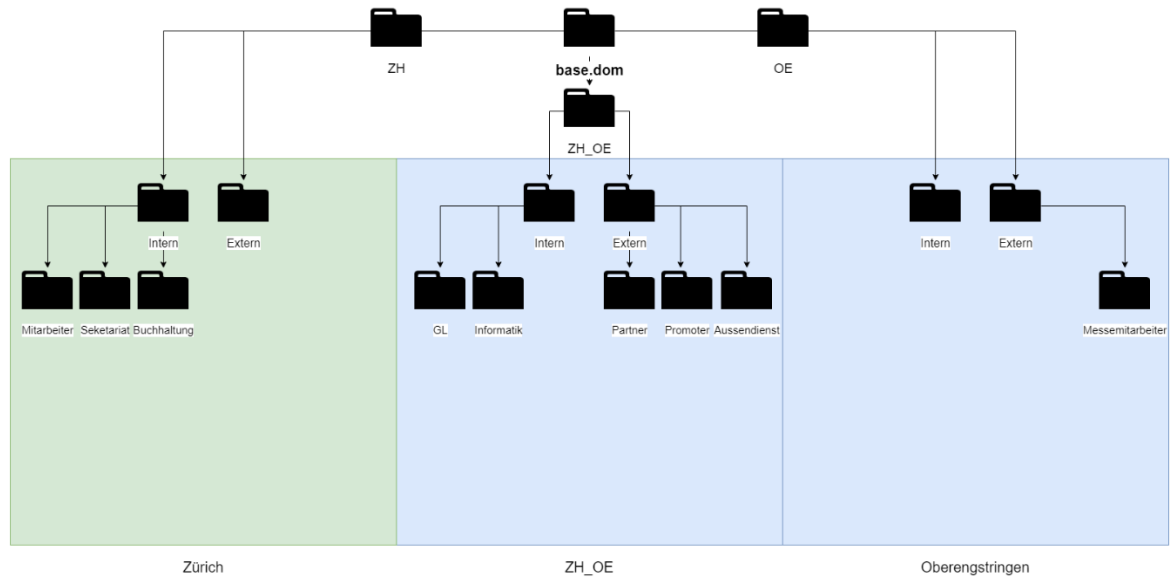
- GL (intern)
- Mitarbeiter (intern)
- Sekretariat (intern)
- Aussendienst (extern)
- Buchhaltung (intern)
- Promoter (extern)
- Partner (extern)
- Informatik (intern)

Standort 2

- GL (intern)
- Aussendienst (extern)
- Promoter (extern)
- Messemitarbeiter (extern)
- Partner (extern)
- Informatik (intern)

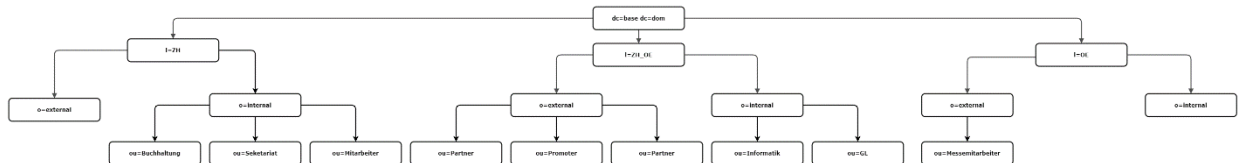
6.1.1. Struktur – Allgemein

Dies ist die Struktur in einer einfacheren Variante.

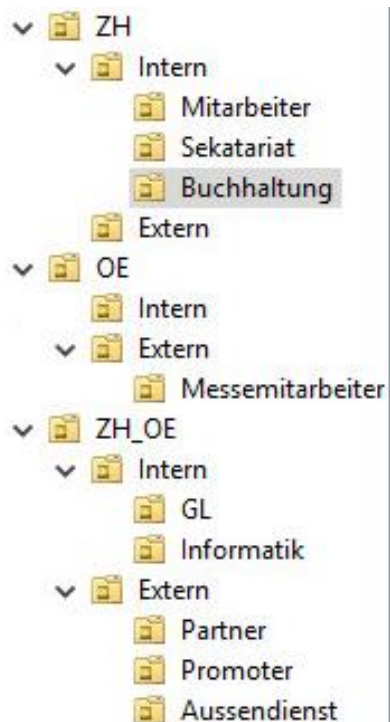


6.1.2. Struktur – Detailliert

Dies ist die Struktur der AD in einer detaillierten Version.



6.2. Struktur im AD anlegen



Folgende Struktur wurde in der AD angelegt.

7. DC2 zur Gesamtstruktur hinzufügen

7.1. Domain Controller hinzufügen

Der Domain Controller wurde zur base.dom Domäne hinzugefügt.

Active Directory-Benutzer und -Gruppen				
Gespeicherte Abfragen				
base.dom				
Builtin				
Computers				
Domain Controllers				
ForeignSecurityPrincipals				
Name	Typ	Domänencont...	Standort	
MTZHWDC01	Computer	GC	Default-First-Si...	
MTZOWDC02	Computer	GC	Default-First-Si...	

8. DNS in Active Directory

8.1. Fragen über DNS in Active Directory

1. Was macht der CMD-Befehl «ipconfig /flushdns»
 - a. Der Client / Server löscht den Namenscache für IP-Einträge und aktualisiert sie vom angeschlossenen DNS-Server neu.
2. Was macht der CMD-Befehl «ipconfig /displaydns»
 - a. Die Option Ipconfig/displaydns gibt den Inhalt des DNS Caches aus.
3. Was macht der PS-Befehl «Show-DnsServerCache -ComputerName "DNS-Servername"»
 - a. Es zeigt den Cache vom DNS Server an
4. Unter welchem Pfad sind die Zonenfiles abgespeichert, welche vom Windows DNS Server verwaltet werden (Keine Active Directory integrierte Zonen)
 - a. C:\Windows\System32\dns
5. Wo werden Active Directory integrierte Zonen abgespeichert?
 - a. Active Directory integriertes DNS speichert Zonendaten in Anwendungsverzeichnis der Partitionen.
6. Was ist der Unterschied zwischen einer in Active Directory integrierten Zone und einer Standard Windows DNS Server Zone?
 - a. Eine Active Directory integrierte Zone wird im Active Directory hinterlegt und sind daher auf allen Domänen Controllern hinterlegt. Die Active Directory Zonen-Synchronisation ist schneller und sicherer als die Synchronisation über eine normale DNS-Zone.
7. Was macht der CMD-Befehl «ipconfig /registerdns»
 - a. Es erstellt oder aktualisiert entweder einen Host-A/AAAA-Eintrag innerhalb des in Active Directory integrierten DNS.
8. Warum ist es nicht notwendig, dass mein DNS Server eine Weiterleitung eingerichtet hat?
 - a. Wenn der DNS-Server eine Anfrage eingerichtet hat, die er nicht beantworten kann (externe Domain), dann gibt er sie an den Server weiter, auf den die Weiterleitung konfiguriert ist. (beispielsweise, wenn ich eine Abfrage für google.com eingebe).
9. Was ist eine rekursive Namensauflösung?
 - a. Bei einer rekursiven Namensauflösung, wird immer der nächste Server angefragt. Als beispiel, wenn ich nach Google.com suche, dann sucht mein Client in seinem Cache, gibt die Anfrage an den Konfigurierten DNS-Server weiter, dieser gibt es an den Provider weiter usw. bis die ersten Server eine Antwort hat und diese dann nach und nach zurückgibt.
10. Was ist eine iterative Namensauflösung?
 - a. Bei der iterativen Namensauflösung ist der DNS-Client/Server direkt so konfiguriert, dass er bei den Root-Servern anfragt und nicht zuerst beim Provider etc.
11. Wie erfährt eine sekundäre Zone über Änderungen, wenn keine Benachrichtigungen aktiviert sind?
 - a. Sie erfährt die Änderungen, wenn die Primäre Zone geändert wird. An der Sekundären Zone können nicht direkt Änderungen vorgenommen werden.
12. Was ist eine bedingte Weiterleitung?
 - a. Eine bedingte Weiterleitung ist eine Weiterleitung unter Bedingungen. Beispielsweise, wenn eine Anfrage für eine gewisse Domain kommt, dann leite sie dorthin etc.
13. Wie wird eine bedingte Weiterleitung im englischen genannt?
 - a. Im Englischen wird die bedingte Weiterleitung «Conditional Forwarders» genannt. Dazu existiert auch ein Ordner auf dem DNS Server.

8.2. Neue Forward-Zone übertragen

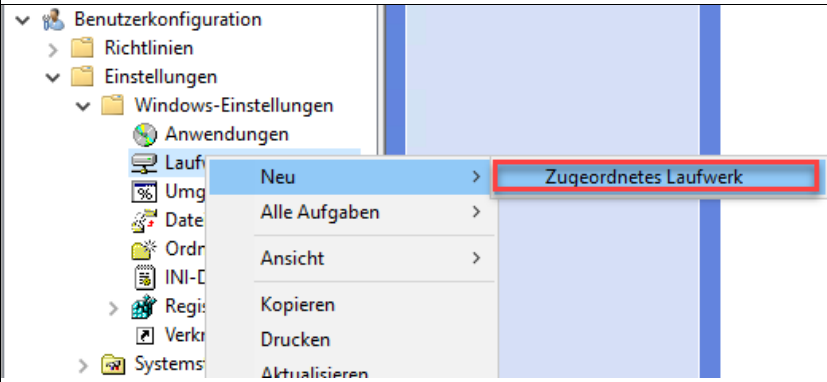
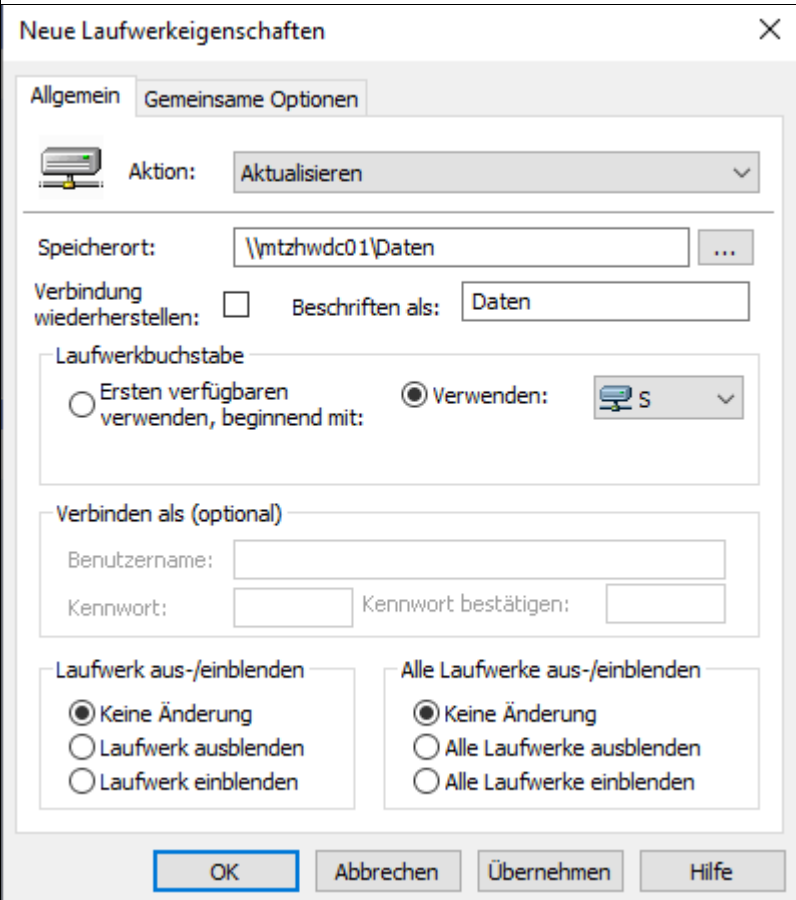

Eigenschaften von lab.base ? X

Namensserver	WINS	Zonenübertragungen
Allgemein	Autoritätsursprung (SOA)	
Status:	Wird ausgeführt	Anhalten
Typ:	Sekundär	Ändern...
Replikation:	Keine Active Directory-integrierte Zone	Ändern...
Zonendateiname:		
lab.base.dns		
Masterserver:		
IP-Adresse	Vollqualifizierter Domänenname ...	
10.11.1.10	mtzhwdc01.base.dom	

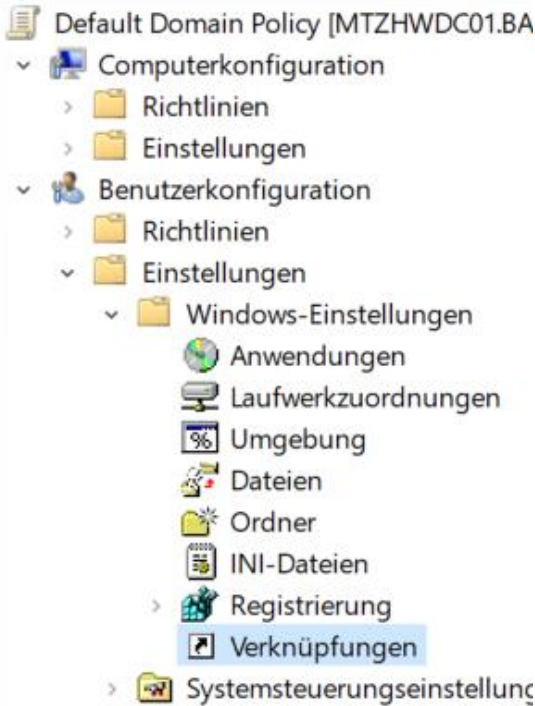
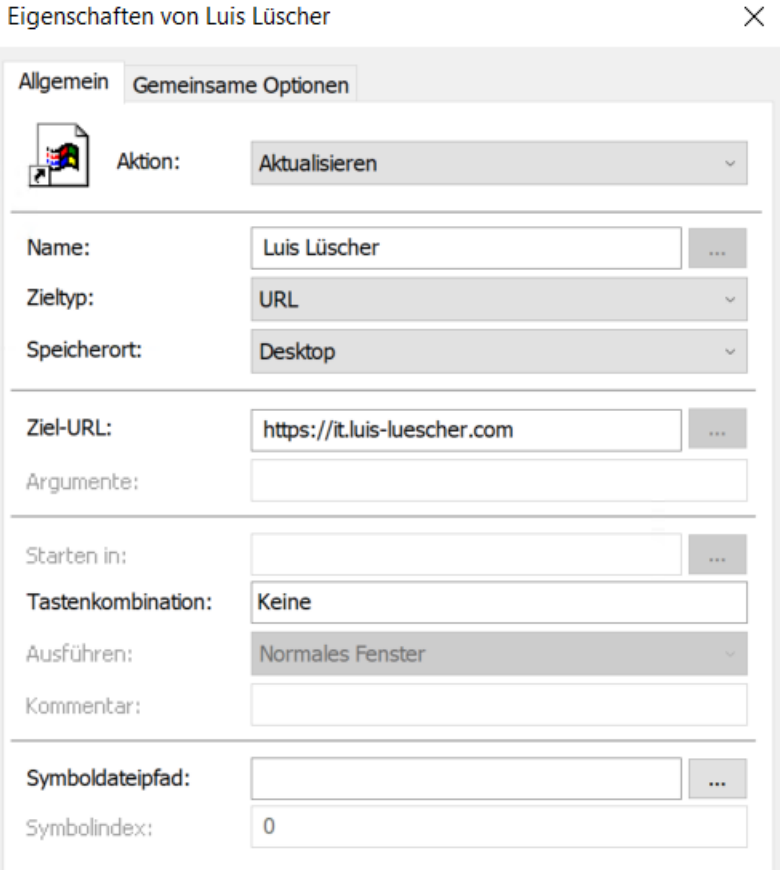
Folgender Screenshot vom DC02.

9. Mit GPOs arbeiten

9.1. Netzlaufwerk mit GPO erzeugen

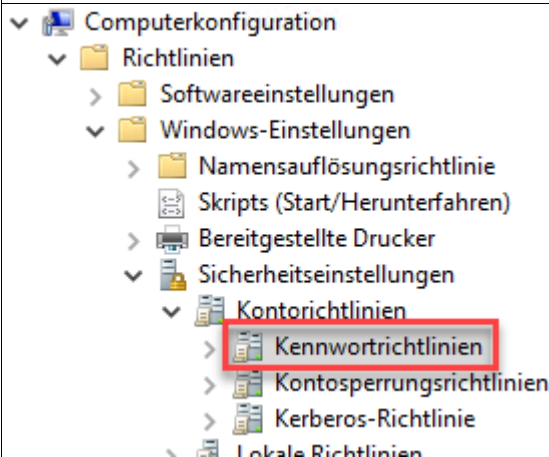


















Netzlaufwerk mit GPO erzeugen	
Bild	Text
	<p>Im Gruppenrichtlinien-Editor kann man auf die Laufwerkzuordnung klicken und dann ein neues Laufwerk erstellen.</p>
	<p>Hier dann die folgende Werte setzen:</p> <ul style="list-style-type: none"> - Aktion: Aktualisieren - Speicherort: Pfad zum Ordner. - Beschriften als: Entsprechender Laufwerkbuchstabe auswählen. <p>Danach auf «Übernehmen» klicken und mit «OK» bestätigen.</p>
	<p>Nun sieht man die Netzwerkadresse Daten (S:).</p>

9.2. Verknüpfung auf dem Desktop anlegen

Verknüpfung auf Website erstellen	
Bild	Text
 <p>Default Domain Policy [MTZHWDC01.BA]</p> <ul style="list-style-type: none"> Computerkonfiguration <ul style="list-style-type: none"> Richtlinien Einstellungen Benutzerkonfiguration <ul style="list-style-type: none"> Richtlinien Einstellungen <ul style="list-style-type: none"> Windows-Einstellungen <ul style="list-style-type: none"> Anwendungen Laufwerkzuordnungen Umgebung Dateien Ordner INI-Dateien Registrierung Verknüpfungen Systemsteuerungseinstellung 	<p>Zu Beginn muss man den Gruppenrichtlinienverwaltungs – Editor öffnen. Danach öffnet man den Punkt «Verknüpfungen» unter der Benutzerkonfiguration. Hier dann mittels Rechtsklick auf «Neu» klicken.</p>
 <p>Eigenschaften von Luis Lüscher</p> <p>Allgemein Gemeinsame Optionen</p> <p>Aktion: Aktualisieren</p> <p>Name: Luis Lüscher</p> <p>Zieltyp: URL</p> <p>Speicherort: Desktop</p> <p>Ziel-URL: https://it.luis-luescher.com</p> <p>Argumente:</p> <p>Starten in:</p> <p>Tastenkombination: Keine</p> <p>Ausführen: Normales Fenster</p> <p>Kommentar:</p> <p>Symboldateipfad:</p> <p>Symbolindex: 0</p>	<p>Hier dann die folgende Werte setzen:</p> <ul style="list-style-type: none"> - Aktion: Aktualisieren - Name: Gewünschten Name - Zieltyp: URL - Speicherort: Desktop - Ziel URL: Gewünschte URL

				<p>Danach sollte man, wenn man sich mit einem AD-User anmeldet, die entsprechende Verknüpfung sehen. Ansonsten einfach die Group Policy updaten.</p>
Name	Reihenfolge	Aktion	Verknüpfung	<p>So sieht der Eintrag im Editor aus.</p>
 Luis Lüscher	1	Aktuali...	%DesktopDir%\Luis Lüscher	

9.3. Verändern der Passwortrichtlinien

Veränderung der Passwortrichtlinien																
Bild		Text														
		Im Gruppenrichtlinien-Editor kann man auf die Kennwortrichtlinien gehen.														
<table><thead><tr><th>Richtlinie</th><th>Richtlinieneinstellung</th></tr></thead><tbody><tr><td> Kennwort muss Komplexitätsvoraussetzungen entsprechen</td><td>Deaktiviert</td></tr><tr><td> Kennwortchronik erzwingen</td><td>24 gespeicherte Kennwörter</td></tr><tr><td> Kennwörter mit umkehrbarer Verschlüsselung speichern</td><td>Deaktiviert</td></tr><tr><td> Maximales Kennwortalter</td><td>Nicht definiert</td></tr><tr><td> Minimale Kennwortlänge</td><td>Nicht definiert</td></tr><tr><td> Minimales Kennwortalter</td><td>Nicht definiert</td></tr></tbody></table>	Richtlinie	Richtlinieneinstellung	 Kennwort muss Komplexitätsvoraussetzungen entsprechen	Deaktiviert	 Kennwortchronik erzwingen	24 gespeicherte Kennwörter	 Kennwörter mit umkehrbarer Verschlüsselung speichern	Deaktiviert	 Maximales Kennwortalter	Nicht definiert	 Minimale Kennwortlänge	Nicht definiert	 Minimales Kennwortalter	Nicht definiert	Nun kann man die entsprechenden Richtlinieneinstellungen tätigen. Bei einigen muss man die Definierung ausschalten, damit sie nicht mehr berücksichtigt werden. Zudem muss man die Komplexitätsvoraussetzung deaktivieren.	
Richtlinie	Richtlinieneinstellung															
 Kennwort muss Komplexitätsvoraussetzungen entsprechen	Deaktiviert															
 Kennwortchronik erzwingen	24 gespeicherte Kennwörter															
 Kennwörter mit umkehrbarer Verschlüsselung speichern	Deaktiviert															
 Maximales Kennwortalter	Nicht definiert															
 Minimale Kennwortlänge	Nicht definiert															
 Minimales Kennwortalter	Nicht definiert															

9.4. GPResult

<https://school.luis-luescher.com/ad/file.html>

<https://school.luis-luescher.com/ad/file2.html>

10. Konfigurieren von Standorten und Subnetzen

```
Ethernet-Adapter Ethernet0:

    Verbindungsspezifisches DNS-Suffix:
    IPv4-Adresse . . . . . : 10.11.1.11
    Subnetzmaske . . . . . : 255.255.255.0
    Standardgateway . . . . . : 10.11.1.1

C:\Users\tk3ll>set logonserver
LOGONSERVER=\\MTZHWDC01
```

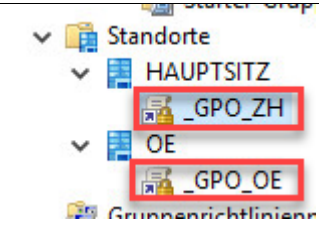
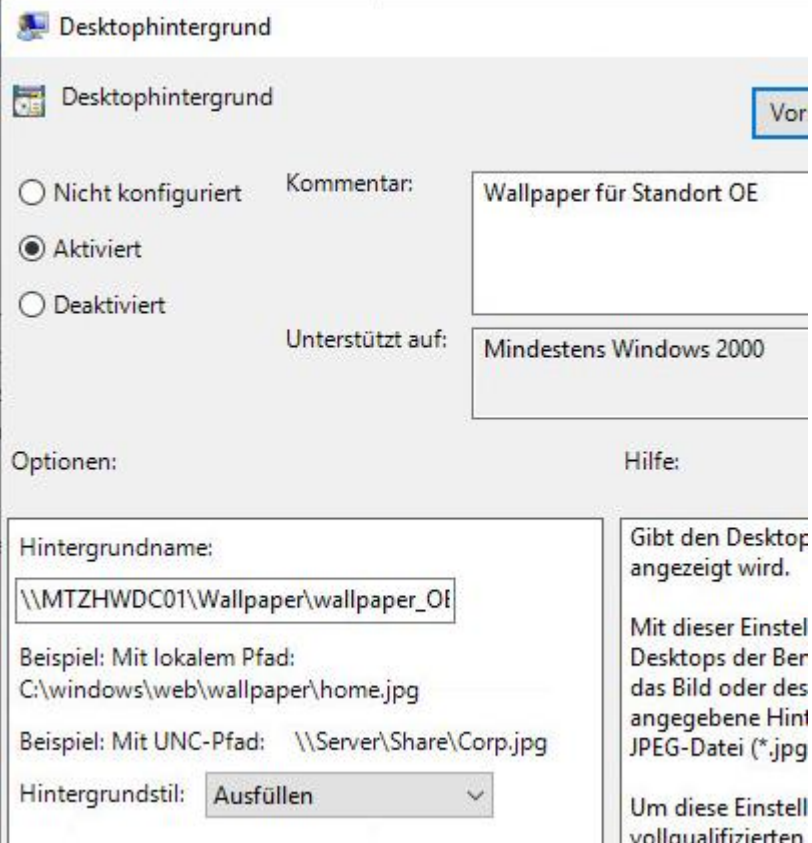
Nun habe ich auf einem Client im Subnetz 1 (10.11.1.0/24) den Logonserver MTZHWDC01 (entsprechender Server am Standort)

```
Verbindungsspezifisches DNS-Suffix:
IPv4-Adresse . . . . . : 10.11.2.13
Subnetzmaske . . . . . : 255.255.255.0
Standardgateway . . . . . : 10.11.2.1

C:\Users\tk3lr>set logonserver
LOGONSERVER=\\MTZOWDC02
```

Nun habe ich auf einem Client im Subnetz 2 (10.11.2.0/24) den Logonserver MTZOWDC02 (entsprechender Server am Standort)

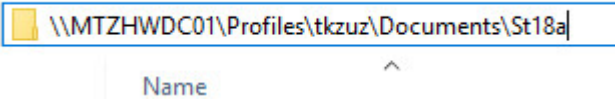
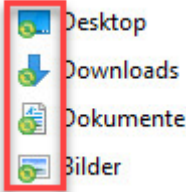
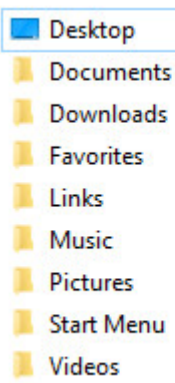
11. GPO mit Standort verknüpfen

GPO mit Standort verknüpfen	
Bild	Text
	<p>Unter den einzelnen Standorten ist die Verknüpfung zu den GPOs einsehbar. Man erkennt es an dem kleinen Verknüpfungslogo unten links.</p>
	<p>Die entsprechende Regel für den Standort OE sieht folgendermassen aus. Ich habe das Hintergrundbild mittels UNC-Pfad angegeben.</p> <p>Gibt den Desktop angezeigt wird.</p> <p>Mit dieser Einstell Desktops der Ber das Bild oder des angegebene Hint JPEG-Datei (*.jpg)</p> <p>Um diese Einstell vollqualifizierten</p>

Desktophintergrund	
<input type="radio"/> Nicht konfiguriert	Kommentar: Wallpaper für Standort ZH
<input checked="" type="radio"/> Aktiviert	
<input type="radio"/> Deaktiviert	
Unterstützt auf:	Mindestens Windows 2000
Optionen:	Hilfe:
<p>Hintergrundname:</p> <p><input type="text" value="\\MTZHWDC01\Wallpaper\wallpaper_ZH"/></p> <p>Beispiel: Mit lokalem Pfad: C:\windows\web\wallpaper\home.jpg</p> <p>Beispiel: Mit UNC-Pfad: \\Server\Share\Corp.jpg</p> <p>Hintergrundstil: <input type="text" value="Ausfüllen"/></p>	<p>Gibt den Desktop angezeigt wird.</p> <p>Mit dieser Einstellung Desktops der Benutzer das Bild oder das angegebene Hintergrundbild als JPEG-Datei (*.jpg)</p> <p>Um diese Einstellung vollqualifizierte</p>





Die entsprechende Regel für den Standort ZH sieht folgendermassen aus. Ich habe das Hintergrundbild mittels UNC-Pfad angegeben.

12. Roaming Profiles und Folder Redirection

Roaming Profiles und Folder Redirection	
Bild	Text
	Sobald die Folder Redirection funktioniert sollte man den UNC-Pfad des entsprechenden Ordner sehen.
	Man erkennt ebenfalls das die Folder Redirection sowie die Roaming Profiles funktionieren an dem kleinen grünen Synchronisation-Kreis unten links.
	So sieht der entsprechende User Ordner aus auf dem Server mtzhwdc01.

13. Deploy MSI mit GPO

Organisieren ▾

Name	Herausgeber	Installiert am	Größe	Version
 7-Zip 18.06 (x64 edition)	Igor Pavlov	20.09.2020	5.10 MB	18.06.00.0
 Microsoft Visual C++ 2008 Redistributable - x64 9.0.3...	Microsoft Corporation	30.08.2020	13.2 MB	9.0.30729.6161
 Microsoft Visual C++ 2008 Redistributable - x86 9.0.3...	Microsoft Corporation	30.08.2020	10.1 MB	9.0.30729.6161
 VMware Tools	VMware, Inc.	30.08.2020	84.7 MB	10.2.5.8068406

Ereignis 302, Application Management Group Policy

Allgemein

Details

Die Installation der Anwendung 7-Zip 18.06 (x64 edition) von der Richtlinie Default Domain Policy wurde durchgeführt.

Protokollname:

System

Quelle:

Application Management Gr

Protokolliert:

20.09.2020 14:39:22

Ereignis-ID:

302

Aufgabenkategorie:

Keine

Ebene:

Informationen

Schlüsselwörter:

Klassisch

Benutzer:

SYSTEM

Computer:

mtzhwdc01.base.dom

Vorgangscode:

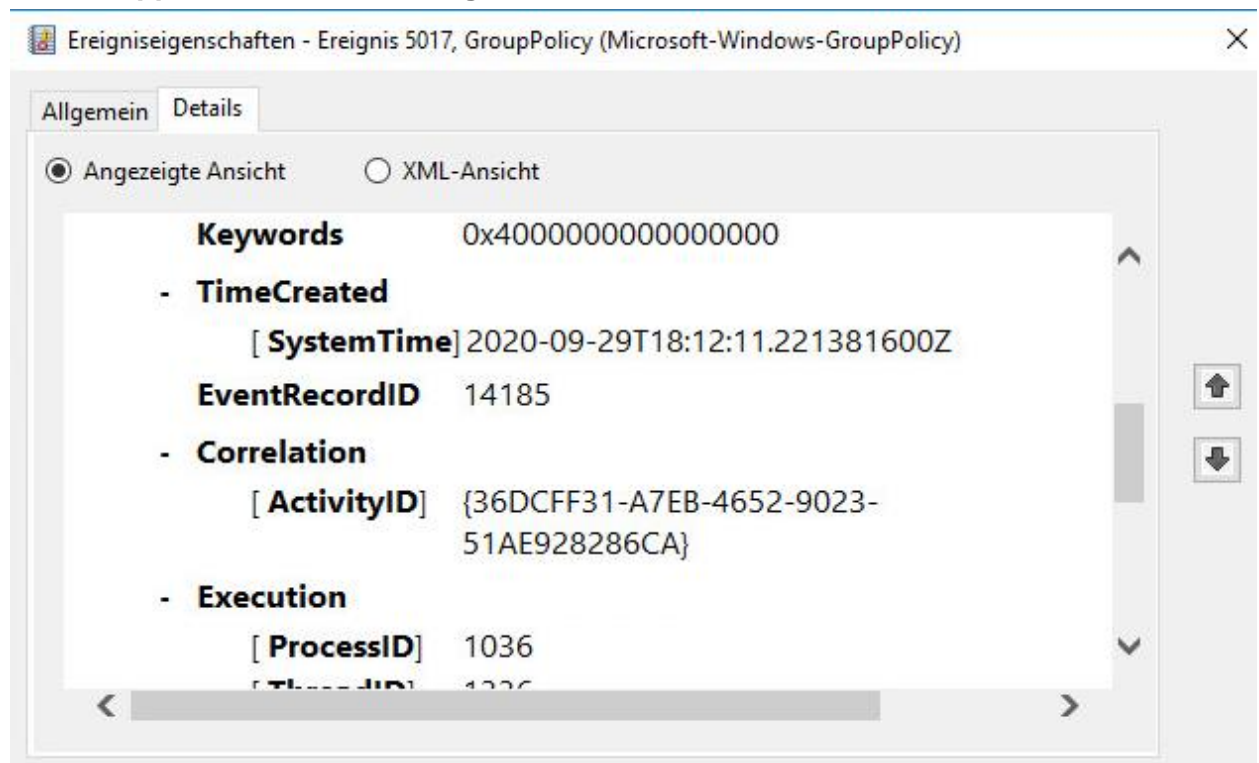
Weitere Informationen:

[Onlinehilfe](#)

9. MTZHWDC01 hat den Test NCSecDesc bestanden.
10. MTZHWDC01 hat den Test NetLogons bestanden.
11. MTZHWDC01 hat den Test ObjectsReplicated bestanden.
12. MTZHWDC01 hat den Test Replications bestanden.
13. MTZHWDC01 hat den Test RidManager bestanden.
14. MTZHWDC01 hat den Test Services bestanden.
15. MTZHWDC01 hat den Test SystemLog bestanden.
16. MTZHWDC01 hat den Test VerifyReferences bestanden.
17. ForestDnsZones hat den Test CheckSDRefDom bestanden.
18. ForestDnsZones hat den Test CrossRefValidation bestanden.
19. DomainDnsZones hat den Test CheckSDRefDom bestanden.
20. DomainDnsZones hat den Test CrossRefValidation bestanden.
21. Schema hat den Test CheckSDRefDom bestanden.
22. Schema hat den Test CrossRefValidation bestanden.
23. Configuration hat den Test CheckSDRefDom bestanden.
24. Configuration hat den Test CrossRefValidation bestanden.
25. base hat den Test CheckSDRefDom bestanden.
26. base hat den Test CrossRefValidation bestanden.
27. base.dom hat den Test LocatorCheck bestanden.
28. base.dom hat den Test Intersite bestanden.

Von insgesamt 28 Tests wurden 28 Tests bestanden.

14.4. Gruppenrichtlinien-Eventlog



Ereigniseigenschaften - Ereignis 5017, GroupPolicy (Microsoft-Windows-GroupPolicy) X

Allgemein Details

Der Systemaufruf zum Abrufen von Kontoinformationen wurde abgeschlossen.
CN=C00001,OU=Sekretariat,OU=Intern,OU=ZH,DC=base,DC=dom
Der Aufruf wurde in 922 Millisekunden abgeschlossen.

Protokollname: Microsoft-Windows-GroupPolicy/Betriebsbereit
Quelle: GroupPolicy (Microsoft-Win Protokolliert: 29.09.2020 20:12:11
Ereignis-ID: 5017 Aufgabenkategorie: Keine
Ebene: Informationen Schlüsselwörter:
Benutzer: SYSTEM Computer: c00001.base.dom
Vorgangscod: Info
Weitere Informationen: [Onlinehilfe](#)

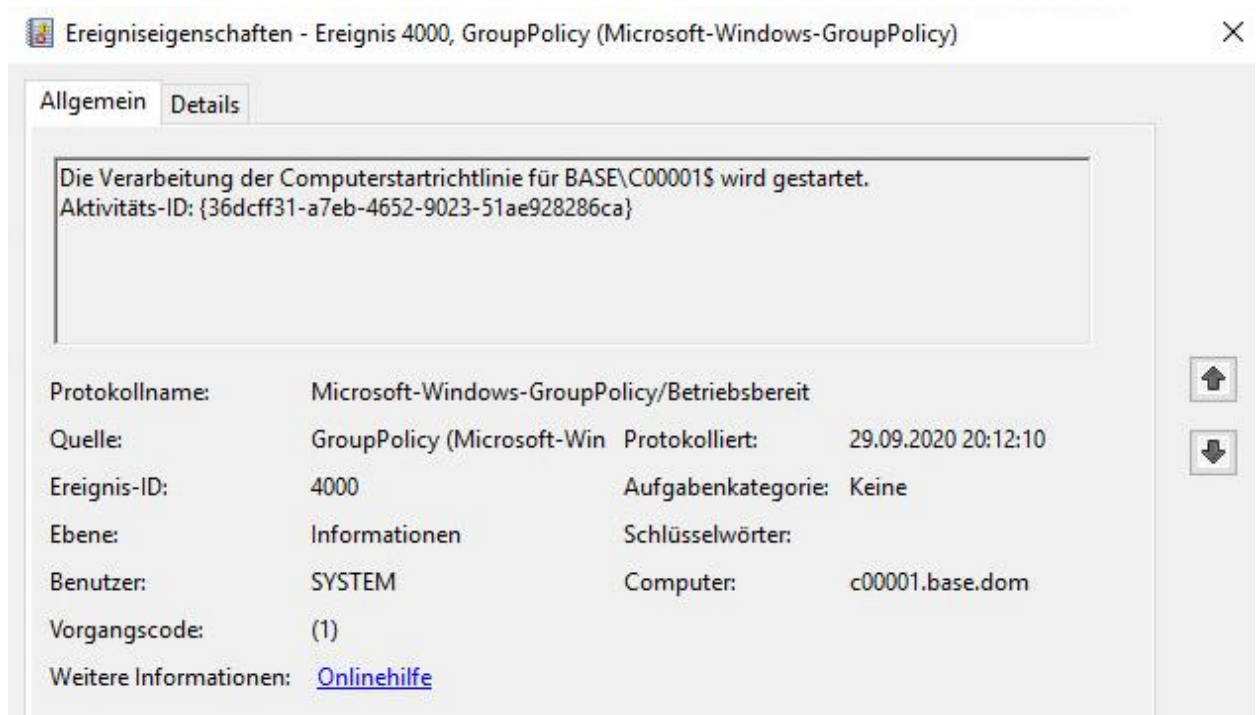
Ereigniseigenschaften - Ereignis 4000, GroupPolicy (Microsoft-Windows-GroupPolicy) X

Allgemein Details

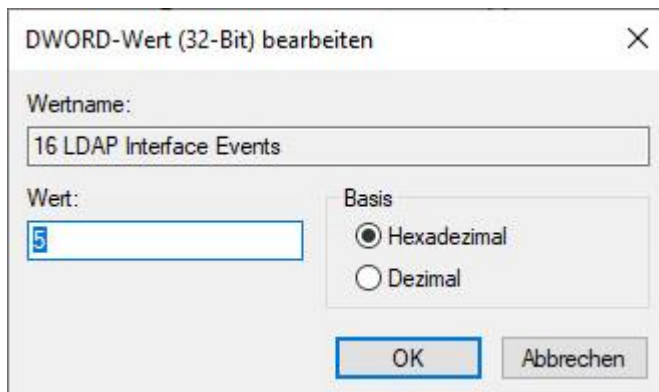
☒ Angezeigte Ansicht ☐ XML-Ansicht

Opcode 1
Keywords 0x4000000000000000
- TimeCreated
[**SystemTime**] 2020-09-29T18:12:10.121711700Z
EventRecordID 14181
- Correlation
[**ActivityID**] {36DCFF31-A7EB-4652-9023-51AE928286CA}
- Execution
[**ProcessID**] 1036

Kopieren Schließen



14.5. Active Directory Log Level



In der Registry alle Einträge unter diesem Verzeichnis «HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/NTDS/Diagnostic» auf 5 stellen. So werden alle Logs auf dem höchsten Level ausgeführt.

Nun kann man die entsprechenden Logs in der Ereignisanzeige anzuzeigen. Bei mir sind zu Beginn auf Level 0 **9 Einträge** getätigt worden, auf Level 5 waren es dann ca. **273 Einträge**. Die Einträge kommen so zu Stande das nun jede Kleinigkeit geloggt wird. Zum Beispiel wenn ein Client die Verbindung zum DC verliert oder ähnliches.

15. LDAP – PowerShell Tool

15.1. LDAP Abfragen und LDAP Queries (CMD Prompt)

Damit Sie diese LDAP-Befehle in der CMD ausführen können, müssen Sie die RSAT Tools für Ihren Server installieren. Sie finden eine Anleitung dazu im Ordner Tools.

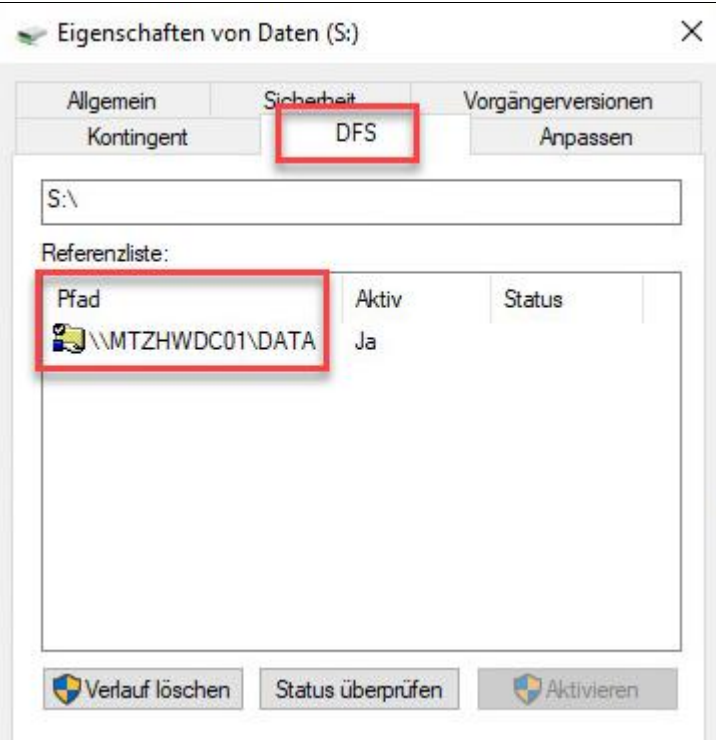
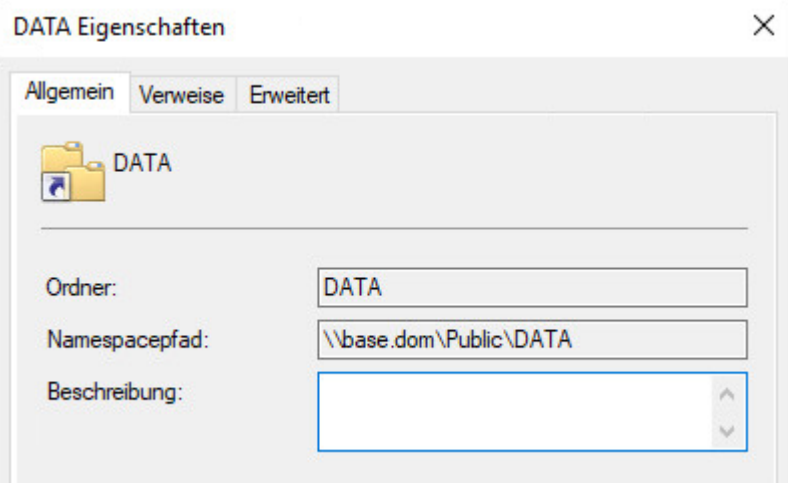
Die einzelnen Schritte wurden auf dem [BSCW](#) und auf meiner [Website](#) hochgeladen.

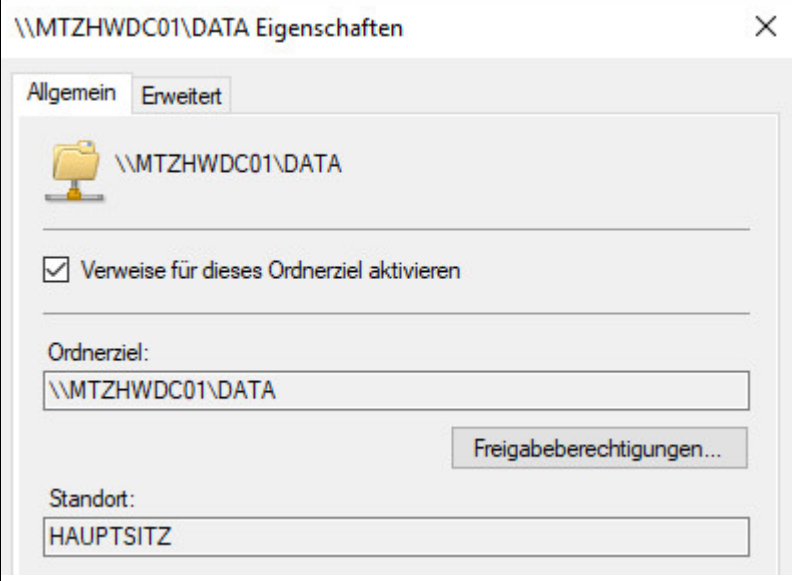
15.2. LDAP Abfragen und LDAP Queries (PowerShell)

15.2.1. Benutzeranleitung

Die Benutzeranleitung wird aus ästhetischen Gründen separat geführt. Die Anleitung ist auf meiner [Website](#) als PDF verfügbar.

16. DFS einrichten und Namespace anlegen

DFS einrichten und Namespace anlegen	
Bild	Text
 <p>The screenshot shows the 'Eigenschaften von Daten (S:)' dialog box. The 'DFS' tab is selected and highlighted with a red box. Below it, the 'Referenzliste' table shows a path '\\MTZHWDC01\DATA' highlighted with a red box. The table has columns 'Pfad', 'Aktiv', and 'Status'.</p>	<p>Sobald DFS richtig konfiguriert wurde und ein Namespace angelegt wurde. Kann man in den Eigenschaften des Netzlaufwerk den Reiter «DFS» sehen. Hier sieht man ebenfalls auch den Pfad für das Netzlaufwerk.</p>
 <p>The screenshot shows the 'DATA Eigenschaften' dialog box. The 'Allgemein' tab is selected. The 'Namespacepfad' field is filled with '\\base.dom\Public\DATA'.</p>	<p>Unter den Namespaces kann man die Eigenschaften des Namespace einsehen, so zum Beispiel den Namespacepfad in diesem Fall «\\base.dom\Public\DATA».</p>

	<p>Unter den Ordnerzielen kann man nun die Eigenschaften einsehen, also wohin der entsprechende Namespace hinzeigt. In diesem Fall auf den UNC-Pfad «\\MTZHWDC01\\DATA».</p>
--	--