

Windows Domänenkonzeptionierung

Projektdokumentation

Tim Meusel

Nikolai Luis

Marcel Reuter

21. April 2018



heinrich-hertz-europakolleg
der bundesstadt bonn
berufskolleg mit beruflichem gymnasium

Betreuer

Wolfgang Dreser

Danksagung

Ein besonderer Dank gebührt Ulli Kehrle. Ohne seine unermüdlichen Erklärungen zum Thema \LaTeX und seine Hilfestellungen, auch in den späten Abendstunden, würde diese Dokumentation nicht in dieser Form existieren.

Inhaltsverzeichnis

1	Vorwort	7
2	Vorbereitung	8
2.1	DHCP-Konzept	8
2.2	DNS-Namensraum	9
2.3	Windows Domänen Konzept	10
2.3.1	Namenskonzept User	10
2.3.2	Bezeichnung Hardwarekomponenten	10
2.3.3	EDV-Struktur Active Directory	11
3	Installation	12
3.1	Windows Server 2016	12
3.2	Active Directory	13
3.3	DNS-Dienst	14
3.4	DHCP-Dienst	14
3.5	Datei-Dienst	14
4	Umsetzen der Anforderungen	16
4.1	Einrichtung DHCP Dienst	16
4.1.1	Test des Failovers	19
4.2	Einrichtung DNS Dienst	21
4.3	Dateidienst/Freigaben einrichten	21
4.3.1	Ressourcen-Manager	25
4.4	Active Directory Domänendienst	26
4.4.1	EDV-Struktur im Active Directory	27
4.4.2	Replikation	29
4.4.3	Benutzerkonten erstellen	30
4.4.4	Gruppenkonten erstellen	31
4.4.5	Computerkonten erstellen	33
4.4.6	Skript zum Anlegen von Nutzern, Computern	33
4.4.7	Anmeldeskript	33

4.4.8	Servergespeicherte Benutzerprofile	34
4.4.9	Heimatverzeichnisse	35
4.4.10	Speichervolumen Begrenzung	39
4.5	Einrichten von Druckern	41
4.6	Gruppenrichtlinien	43
4.7	Kontorichtlinien	43
4.7.1	Kennwortrichtlinien	44
4.7.2	Anmelderichtlinien	44
4.7.3	Administrator Account umbenennen	45
4.8	Zugriffsrechte	46
4.8.1	Zugriff auf Lokale Laufwerke	46
4.8.2	Zugriff auf Eingabeaufforderung	47
4.8.3	Zugriff auf Systemadministration	47
4.9	Datenaustausch	48
5	Glossar	50
6	Literatur	51
7	Anhang	52
8	Erklärung	57

Abbildungsverzeichnis

2.1	Gliederung der OUs im Active Directory	11
3.1	Rollen- und Funktionsverwaltung	13
4.1	Gliederung der DNS Struktur für IPv4 Adressen	18
4.2	IP Konfiguration aller Interfaces	20
4.3	IP Konfiguration eines Interfaces	20
4.4	Erstellen von neuen Freigaben	22
4.5	Die einzelnen Aufgaben beim erstellen einer neuen Freigabe	24
4.6	Kontingentvorlagen im Ressourcen-Manager für Dateiserver	26
4.7	Struktur im Active Directory	28
4.8	Hinzufügen eines DCs zu einer vorhandenen Domäne	29
4.9	Auswahl der Replikationsquellen für einen neuen DC	30
4.10	Gruppenrichtlinienverwaltung innerhalb einer Domäne	36
4.11	Ansicht der vorhandenen Ordnerumleitungen	36
4.12	Eigenschaften der Ordnerumleitung für AppData 1	37
4.13	Eigenschaften der Ordnerumleitung für AppData 2	38
4.14	Erstellung eines neuen Kontingents	40
4.15	kontingenteinträge	41
4.16	Übersicht für neue Rollen	42
4.17	Ansicht der Druckverwaltung	42
4.18	Übesicht über alle Drucker	43
4.19	Realisierte Kennwortrichtlinie	44
4.20	Detailansicht der Anmeldezeiten	45
4.21	Gruppenrichtlinienverwaltungs-Editor	46
4.22	Konfiguration für Wechselmedienzugriff	47
4.23	GPO Editor für Zugriff auf die Systemsteuerung	48
4.24	GPO Editor für Laufwerkseigenschaften	49

Quelltextverzeichnis

4.1	Ausgabe der IP Konfiguration auf einem Windows 7	19
4.2	Lokaler Pfad zur Freigabe	23
4.3	Remote Pfad zur Freigabe	23
4.4	Powershell Script zum Anlegen von AD Nutzern	33
4.5	Benötigte Pfade zur Kontingentverwaltung	40

1 Vorwort

Als Vorbereitung für die Abschlussprüfungen im Juni 2018 haben die Schüler der Fachklassen des Heinrich-Hertz-Europakollegs Bonn ein Szenario in dem Bereich der Serveradministration gestellt bekommen. Dieses wurde innerhalb eines Teams von zwei bis zu drei Leuten eigenständig erarbeitet. Die Hardware, worauf das Test-szenario durchgeführt werden konnte, wurde von der Schule gestellt. Den Schülern wurde freigestellt, ob Sie diese verwenden oder eigene Mittel verwenden möchten.

Die Aufgabenstellung wurde über Moodle zur Verfügung gestellt und kann dem Anhang 7 entnommen werden. Die Arbeit und das Verfassen dieser Dokumentation wurde eigenständig durchgeführt.

2 Vorbereitung

Um eine vollständige und schnelle Umsetzung des Projektes zu gewährleisten wurde zunächst eine Testumgebung aufgebaut. Des Weiteren wurde zu Beginn ein Konzept erarbeitet, welches die DNS Namenkonvention und die DHCP Vorgaben beinhaltet. Dieses Konzept wurde abschließend dem zuständigen Lehrer, in diesem Projekt als Rolle des Auftraggebers, vorgelegt und abgenommen. Eine vorausschauende Planung und Konzeptionierung zusammen mit dem Auftraggeber bringt den Vorteil, dass Fehler frühzeitig identifiziert und verbessert werden können, sowie eine effiziente Hardware Planung.

2.1 DHCP-Konzept

Die Firma Mikado besitzt insgesamt acht Abteilungen. Pro Abteilung wird ein Netzwerkdrucker vorgesehen. Zum aktuellen Zeitpunkt verwendet die Firma ein Class C Ipv4 Netz, welches beibehalten werden soll. Die Aufteilung der IP Adressen für die Clients, sowie den Netzwerkdruckern, soll über einen DHCP Server vergeben werden. Dabei wird das folgende DHCP Konzept verwendet:

- Jede Abteilung erhält einen eignen Adressbereich, in dem maximal 251 Hosts verwendet werden können
- Netzwerkdrucker erhalten den Ende eines jeden Netzwerkbereichs

Der aktuelle Standard in der Wirtschaft ist aktuell, keine Subnetzmetze mit einer Subnetzmaske kleiner 24 zu nutzen (Ausnahme sind Transfernetze). Wird ein größeres Netz benötigt, so sollte es ein vielfaches eines Class C Netz sein. Von den 256 Adressen entfällt eine für die Broadcastadresse, eine für die Netzadresse, eine für das Gateway und zwei für die VRRP Adressen. Die Aufteilung sieht anschließend wie folgt aus:

Abteilung	Netzadresse	Broadcastadresse
Leitung	192.168.0.0	192.168.0.255
Entwicklung	192.168.1.0	192.158.1.255
Einkauf	192.168.2.0	192.168.2.255
Disposition	192.168.3.0	192.168.3.255
Produktion	192.168.4.0	192.168.4.255
Konstruktion	192.168.5.0	192.168.5.255
Buchhaltung / Rechnungswesen	192.168.6.0	192.168.6.255
Verkauf	192.168.7.0	192.168.7.255

Tabelle 2.1: IP-Adressen Setup

Die Rechner der Administratoren erhalten ein separates Netzwerk, in dem ebenfalls die entsprechenden Windows Server vorhanden sein werden.

2.2 DNS-Namensraum

Die Firma Mikado hat bereits den Domännennamen mikado.spiel erworben. Dieser kann für die Domänen Struktur verwendet werden. Mikado ist in diesem Fall die Second-Level-Domain der DNS Namensauflösung und spiel die First-Level-Domain. Es können weitere Subdomains (Third-Level-Domains) wie beispielsweise verkauf, konstruktion oder einkauf hinzugefügt werden. Die DNS Namensauflösung ist für die Auflösung von FQDNs in eine IP Adresse und umgekehrt. Jeder Rechnernamen in der internen Domäne ist ebenfalls im DNS eingetragen und kann von diesem aufgelöst werden. Der Windows Server 2016, welcher den Domain Controller besitzt, ist gleichzeitig auch ein DNS Server. Dadurch können die entsprechenden Einträge unmittelbar durch den Domain Controller an den DNS Server weitergeben werden.

2.3 Windows Domänen Konzept

2.3.1 Namenskonzept User

Um eine Eindeutigkeit der User herzustellen, empfiehlt es sich hier die Personalnummer des Anwenders zu verwenden. Innerhalb der AD Struktur darf es kein Benutzername doppelt vorhanden sein, da ansonsten die Anmeldung an der Domäne nicht funktioniert. Die Personalnummer wird in der Regel jedem Nutzer bei Beginn der Tätigkeit innerhalb der Firma vergeben, da diese ebenfalls für die Buchhaltung entsprechend verwendet werden kann.

Eine Kombination aus Nachname, Vorname oder Nachname_Vorname wird nicht verwendet, da es vorkommen kann, dass es Doppelnamen innerhalb der Firma gibt. Das gleiche gilt für die eMail-Adresse.

2.3.2 Bezeichnung Hardwarekomponenten

Neben den eindeutigen Benutzernamen müssen auch die verwendeten Hardwarekomponenten einen eindeutigen Bezeichner besitzen. Dabei wird folgendes Konzept zur Nutzung empfohlen:

- Rechner erhalten den Prefix PC gefolgt von einer fortlaufenden Nummer
- Drucker erhalten den Prefix DR gefolgt von einer fortlaufenden Nummer

Die Namensgebung der entsprechenden Rechner, Drucker oder Server ist in erster Linie wichtig für die Zuordnung der DNS Namen, damit hier die Namensauflösung zuverlässig klappt. Ebenfalls kann die Serverbezeichnung helfen, festzustellen welche Funktion ein Server hat. Für die Firma Mikado wird folgende Namensgebung bei den Servern verwendet:

- w16dc01
- w12r2dc02

Der erste Teil des Namens für den Server gibt an, um welches Betriebssystem es sich auf dieser Maschine handelt. So kann hier unmittelbar festgestellt werden, ob eine Version seit geraumer Zeit veraltet ist. Das hintere Segment gibt die Funktion des Servers wieder. So sind beide Server Domain Controller (DC) und nach der Reihenfolge nummeriert. Ein Linux Server wird mit li geprefixt. Danach folgt ebenfalls die Rolle (zum Beispiel dc oder fileserv), gefolgt von einer Numerierung.

2.3.3 EDV-Struktur Active Directory

Die EDV Struktur wird gegliedert wie die Aufteilung der einzelnen Abteilungen. So erhält jede Abteilung eine eigene Organisationseinheit. Dies macht es im späteren Verlauf einfacher dem Anwender bestimmte Rechte oder aber auch IP Adressen zuzuweisen, da diese auf die Organisationseinheiten fest zugewiesen werden können.

Im folgenden Abbild ist der Aufbau dargestellt:

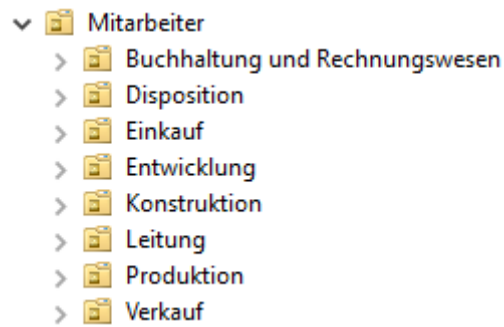


Abbildung 2.1: Gliederung der OUs im Active Directory

Die Aufteilung in Standorte ist nicht erforderlich, da die Firma Mikado nur den Hauptsitz in Köln besitzt.

3 Installation

Die Installation der Testumgebung wird in einem Hypervisor auf einer Physikalischen Maschine getestet, da diese Anwendungen im Testbetrieb keine großen Anforderungen haben. Das Basis Betriebssystem ist ein Hypervisor Server, welcher von Microsoft kostenlos zur Verfügung gestellt wird. Auf diesem können unterschiedliche virtuelle Maschinen angelegt werden, welche Ressourcen des Hostsystems verwenden werden.

3.1 Windows Server 2016

Für die Installation des Windows Server 2016 Datacenter wird in dem Hypervisor zunächst eine leere virtuelle Maschine angelegt. Diese kann anschließend mit dem Image für Windows Server 2016 installiert werden. Bei der Installation des Servers wird eine grafische Benutzeroberfläche verwendet, da auch unerfahrene Informationstechniker diese bedienen sollen. Innerhalb der Testumgebung sollen die virtuellen Maschinen eine Festplattengröße von 75GB und einer Arbeitsspeicher Größe von sechs GB nicht überschreiten. Die virtuellen Maschinen können im Falle eines Übergangs in den Produktivbetrieb mit weiteren Ressourcen ausgestattet werden. Nach der erfolgreichen Installation und Neustart des Servers, muss erstmalig ein Administrator Kennwort festgelegt werden. Dieses muss folgende Anforderungen besitzen:

- Sonderzeichen
- Großbuchstaben
- Zahlen
- Kleinbuchstaben

Nachdem die Basis Installation nun erfolgt ist, muss der Windows Server 2016 für die Rolle als Domain Controller vorbereitet werden. Hierzu wird zunächst eine statische IP Adresse vergeben, da innerhalb der Domäne ein separater DHCP Server auf einem Windows Server 2012R2 im späteren Verlauf installiert wird. Desweiteren

muss der Rechnername angepasst werden, da Windows während der Installationsroutine einen für den Server festgelegten Namen vordefiniert. Um im Nachhinein die Unterscheidung der Server zu verbessern, muss hier ein eindeutiger und aussagekräftiger Name verwendet werden. Der Server muss anschließend neugestartet werden.

3.2 Active Directory

Um eine Rolle auf einem Windows Server installieren zu können, muss diese über den Server-Manager hinzugefügt werden. Über den Punkt Verwalten -> Rollen und Funktionen hinzufügen, können dem Server neue Rollen zugewiesen werden. Rollen oder Funktionen können entweder auf einer virtuellen Festplatte oder aber innerhalb des Computers installiert werden. Der Server zeigt eine Auflistung aller Rollen und Funktionen an. Sobald eine Rolle ausgewählt wurde, weist der Server auf weitere Funktionen hin, die benötigt werden, damit diese ausgewählte Rolle verwendet werden kann.

Damit die Rolle „Active Directory-Domänendienste“ installiert werden kann, bedarf es folgende weitere Funktionen:

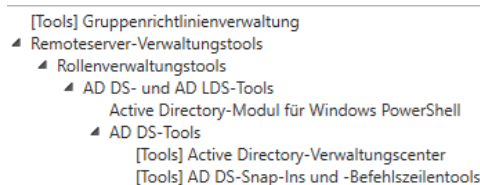


Abbildung 3.1: Rollen- und Funktionsverwaltung

Mit der Schaltfläche „Features hinzufügen“, werden anschließend Funktionen für die Installationsroutine zugefügt. Nach klicken auf „weiter“ wird die Meldung ausgegeben, dass der AD-Domänendienst einen DNS Server innerhalb des Netzwerks benötigt. Sofern dieser nicht vorhanden sein, wird er auf der gleichen Maschine zusätzlich installiert. Der DNS Server wird benötigt da dieser für die Auflösung der Rechnernamen und Druckernamen zuständig ist. Weitere Erläuterungen hierzu kann im DNS Kapitel entnommen werden. Abschließend wird eine Übersicht der Installationsroutine angezeigt, welche mit „Installieren“ bestätigt werden kann.

3.3 DNS-Dienst

Bereits während der Installation des Domain Controllers, stellt Windows sicher, ob ein DNS Server installiert werden soll. Jeder DC sollte in der Regel auch ein DNS Server sein, damit neue Einträge unmittelbar direkt übertragen werden können und der DNS Dienst immer den aktuellsten Stand der Umgebung kennt.

3.4 DHCP-Dienst

Die Installation des DHCP Dienstes kann über den Server-Manager unter dem Punkt Verwalten -> Rollen und Funktionen hinzufügen ausgewählt werden. Wie auch bei der Installation des Active Directorys, zeigt auch hier die Installationsroutine weitere Tools an, die für die Verwendung des DHCP Servers empfohlen werden. Diese können über den Punkt „Funktionen hinzufügen“ ausgewählt werden. Nach Bestätigung auf weiter, zeigt die Installationsroutine Informationen über das DHCP an. Zusätzlich erhält der Benutzer Hinweise das beispielsweise der aktuelle Server auf dem der DHCP Server installiert werden soll eine statische IP Adresse besitzen soll, sowie die Subnetze bereits vorher geplant werden sollen. Nach erneutem Bestätigen auf Weiter, zeigt die Installationsroutine die Übersicht der Installation an. Hierbei kann ebenfalls ausgewählt werden, ob der Server selbständig Neustarts durchführen soll. Da es sich hierbei aktuell um eine Testumgebung handelt, kann dieses Kontrollkästchen aktiviert werden. Zum Schluss muss die Installation mit „installieren“ bestätigt werden. Der Server beginnt nun mit der Installation des DHCP Servers.

Nachdem der Server neugestartet wurde, ist der DHCP Server aktiv und muss abschließend noch Konfiguriert werden.

3.5 Datei-Dienst

Der Dateidienst spielt gerade in größeren Unternehmen eine wichtige Rolle, da viele Benutzer Dateien mit anderen Benutzern teilen oder zur Verfügung stellen wollen. Hierzu kann der von Windows eigene Dateidienst verwendet werden, da dieser mit Hilfe des Distributed File Systems und deren Verwaltungsoberfläche eine einfache Administration ermöglicht.

Um den Windows Dateidienst verwenden zu können, muss dieser zunächst über den Server-Manager hinzugefügt werden. Die Firma Mikado braucht in erster Linie

die Rolle als DFS-Namespace. Damit die Verwaltung des Dateidienstes dem Administrator vereinfacht wird, sollte zusätzlich zu dem DFS-Namespace auch der Ressourcen-Manager installiert werden. Dies ist ein gesondertes Tool und wird nicht automatisch während der Installationsroutine mit installiert. Der Ressourcen Manager kann jedoch auch problemlos nachträglich installiert werden.

Die Installation ist nun abgeschlossen und der Dateidienst, sowie die Freigaben können konfiguriert werden.

4 Umsetzen der Anforderungen

4.1 Einrichtung DHCP Dienst

Bereits nach der Installation zeigt der Server Manager an, dass weitere Konfigurationsschritte für den DHCP Server notwendig sind. So muss beispielsweise der DHCP Server innerhalb der Domäne autorisiert werden, damit die Clients eine entsprechende IP Adresse abrufen können. Zusätzlich muss das DHCP verschiedene Sicherheitsgruppen anlegen, die der DHCP Server benötigt. Nach klicken auf „weiter“ werden Anmeldeinformationen für die Domäne abgefragt. Hier muss ein Domänen Administrator eingetragen sein, da nur dieser entsprechende Autorisierungen des DHCP Servers durchführen darf. Windows füllt diesen, da der DHCP Server auf der gleichen Virtuellen Maschine wie der Domaincontroller installiert ist, standardmäßig mit dem Administrator aus, da dieser bereits während der Installationsroutine als Domänen Administrator hinzugefügt wurde. Der Nutzer hat die Möglichkeit, alternative Anmeldeinformationen anzugeben. Die Autorisierung des DHCP Servers ist nötig, falls mehrere DHCP Server innerhalb einer Domäne arbeiten, da andernfalls es Konflikte zwischen diesen bei der Vergabe der IP Adressen geben könnte.

Mit klicken auf „Commit ausführen“ wird die Autorisierung, sowie das Anlegen der entsprechenden Sicherheitsgruppen im Active Directory durchgeführt.

Im Anschluss erhält der Administrator eine Zusammenfassung der Konfiguration, ob die Konfiguration durchgelaufen ist.

Die Grundkonfiguration des DHCP Server ist abgeschlossen. Als nächsten Schritten müssen nun innerhalb des DHCP Servers Bereiche definiert werden. Hierzu muss zunächst unter Tools -> DHCP die Verwaltungskonsole des DHCP aufgerufen werden, da nur in dieser Bereiche und Konfigurationen durchgeführt werden können.

Um einen Bereich zu konfigurieren, muss zunächst im DHCP Verwaltungstool der DHCP Server ausgewählt werden. Anschließend gibt es die Auswahl zwischen IPv4 oder IPv6. Die Firma Mikado verwendet IPv4, weshalb hier der Bereich auf IPv4

beschränkt werden kann. Mit Rechtsklick auf IPv4 öffnet sich ein Untermenü, wo „neuer Bereich“ ausgewählt wird. Es öffnet sich ein Bereitstellungs-assistent, welcher den Administrator durch die Konfiguration leitet. Mit klicken auf „weiter“, muss zunächst ein Name für den Bereich und eine Beschreibung festgelegt werden. Sobald diese definiert wurde, muss die Start und End IP Adresse definiert werden, sowie die Subnetzlänge.

Sollte ein IP Adressen Netzwerk viele IP Adressen beinhalten, so schlägt der Assistent vor, die IP Adressen in Bereichsgruppen aufzuteilen.

Nach bestätigen der IP Adressen wird abgefragt, ob IP Adressen ausgenommen werden sollen. Beispielsweise bei Servern oder Applikationen die immer die gleiche IP Adresse benötigen. Sollten hier keine Ausnahmen definiert werden müssen, wird anschließend die Lease Time abgefragt. Die Lease Time bestimmt, wie lange eine IP Adresse für einen Client gültig sein darf. Sobald die Lease Time abläuft, führt der Client erneut eine DHCP Anfrage durch, um erneut die IP Adresse für sich zu reservieren. Da es sich bei der Firma Mikado um fest definierte PCs handelt, empfiehlt es sich hier die Lease Time auf den Standardwert von 8 Tage belassen. Sollte beispielsweise die Firma Mikado eine WLAN Infrastruktur für Kunden anbieten, so sollte die Lease Time für diesen Bereich auf wenige Stunden herabgesetzt werden. Hinweis: Das WLAN sollte aus Sicherheitsgründen eine eigene Layer 2 Domäne bekommen.

Eine kurze Lease Time sollte ebenfalls verwendet werden, wenn der DHCP Server nur einen sehr beschränkten Raum für IP Adressen besitzt. Sollte der DHCP Server keine IP Adressen mehr vergeben können, weil beispielsweise alle vergeben sind, so können keine neuen Geräte mit der Infrastruktur kommunizieren.

Im nächsten Schritt wird abgefragt, ob die DHCP Optionen aktiviert werden sollen. Diese definieren das Standardgateway, den DNS Server, sowie den WINS Server für diesen Bereich, welche in der DHCP Abfrage dem Client zugeschickt wird.

Sobald das Standardgateway abgefragt wurde, werden nachträglich noch die Einstellungen für die Domäne sowie den DNS Server und den WINS Server abgefragt. Abschließend muss entschieden werden, ob dieser Bereich bereits aktiviert wird oder nachträglich aktiviert werden muss. Sobald dies bestätigt wurde, ist der Bereich fertig konfiguriert.

Diese Einstellung muss nun für jede Abteilung, sowie für die Server IP Range definiert werden.

Bei der Server IP Range ist besonders, dass hier entsprechend die Server eine Manuelle IP Adressen erhalten, beziehungsweise aus der Adressvergabe des DHCP

Server ausgenommen werden. Die Administrationsrechner erhalten ebenfalls eine fest zugewiesene IP Adresse und sind in dem gleichen IP Bereich wie die Server.

Der Aufbau des DHCP Bereiche sieht nun wie folgt aus:

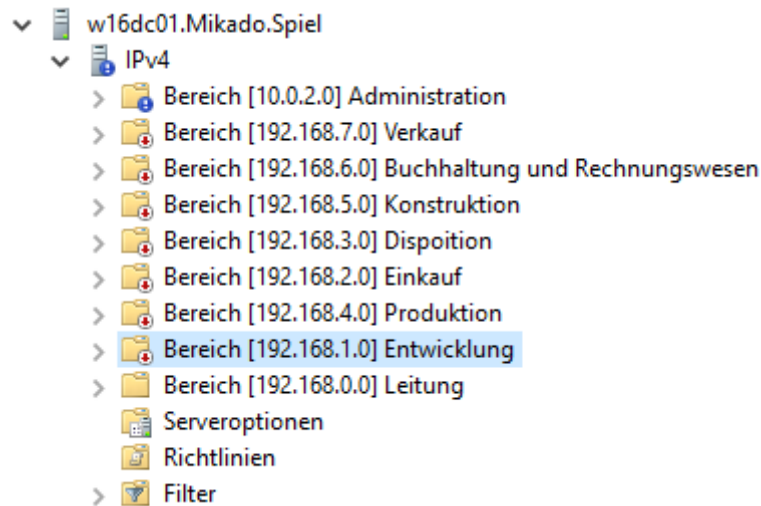


Abbildung 4.1: Gliederung der DNS Struktur für IPv4 Adressen

Bereiche, welche deaktiviert sind, erhalten an dem Ordnersymbol einen kleinen roten Pfeil nach unten. Besondere Bereiche oder Bereiche, welche eine Ausnahme oder eine Aktion erfordern, haben ein weißes Ausrufezeichen. Aktivierte Bereiche, wie zum Beispiel der Bereich „Leitung“ erhält keine besonderen Symbole.

Bei dem Anlegen der einzelnen Bereiche wird ebenfalls festgelegt, dass bei neuen Lease Abrufen der Clients, diese automatisch als DNS Einträge (A Records, optional PTR Records) festgelegt werden. Dies kann jedoch deaktiviert werden. Um einen Bereich zu verändern, kann mit einem Rechtsklick die Eigenschaften wie IP Adressbereich etc. abgeändert werden. Ebenfalls kann hier unter dem Reiter DNS auch ein DHCP Namensschutz eingerichtet werden. Dies sorgt dafür, das bereits vorhandene DNS Einträge überschrieben werden können.

Innerhalb eines Bereiches können Reservierungen für beispielsweise Drucker festgelegt werden. Hierzu muss ein entsprechender Bereich aufgeklappt und anschließend mit Rechtsklick auf Reservierungen die Reservierung hinzugefügt werden.

Da innerhalb einer Domäne immer ein DHCP Server erreichbar sein sollte, sollte unter den Eigenschaften des IPv4 ein sekundärer DHCP Server eingetragen werden. Dieser übernimmt die Aufgaben und Bereiche, falls der Primäre DHCP Server nicht mehr antwortet.

Der DHCP Server ist nun vollständig Konfiguriert und kann nun verwendet werden.

4.1.1 Test des Failovers

Um den Test des DHCP Failovers überprüfen zu können, wurde zunächst der Windows 7 Client, welcher innerhalb des Netzwerks ist, gestartet und anschließend die Eingabeaufforderung gestartet. Zudem wurden beide DC mit entsprechender DHCP Rolle gestartet.

Innerhalb der Eingabeaufforderung wird nun folgender Befehl eingegeben damit die aktuelle IP Konfiguration ausgegeben wird:

```
ipconfig /all
```

Quelltext 4.1: Ausgabe der IP Konfiguration auf einem Windows 7

Die Eingabeaufforderung, zeigt folgendes Ergebnis:

```

C:\Users\000001>ipconfig /all

Windows-IP-Konfiguration

    Hostname . . . . . : pc0001
    Primäres DNS-Suffix . . . . . : Mikado.Spiel
    Knotentyp . . . . . : Hybrid
    IP-Routing aktiviert . . . . . : Nein
    WINS-Proxy aktiviert . . . . . : Nein
    DNS-Suffixsuchliste . . . . . : Mikado.Spiel

Ethernet-Adapter LAN-Verbindung:

    Verbindungsspezifisches DNS-Suffix: Mikado.Spiel
    Beschreibung. . . . . : Intel(R) PRO/1000 MT-Desktopadapter
    Physikalische Adresse . . . . . : 08-00-27-F7-5A-41
    DHCP aktiviert. . . . . : Ja
    Autokonfiguration aktiviert . . . . . : Ja
    Verbindungslokale IPv6-Adresse . . . . . : fe80::4d63:fac7:6324:c17c%11(Bevorzugt)
    IPv4-Adresse . . . . . : 10.0.2.16(Bevorzugt)
    Subnetzmaske . . . . . : 255.255.255.0
    Lease erhalten. . . . . : Dienstag, 3. April 2018 20:25:58
    Lease läuft ab. . . . . : Mittwoch, 11. April 2018 20:25:58
    Standardgateway . . . . . : 10.0.2.2
    DHCP-Server . . . . . : 10.0.2.15
    DHCPv6-IAID . . . . . : 235405351
    DHCPv6-Client-DUID. . . . . : 00-01-00-01-22-51-98-60-08-00-27-F7-5A-41

    DNS-Server . . . . . : 10.0.2.15
    NetBIOS über TCP/IP . . . . . : Aktiviert

Tunneladapter isatap.Mikado.Spiel:

    Medienstatus. . . . . : Medium getrennt
    Verbindungsspezifisches DNS-Suffix: Mikado.Spiel
    Beschreibung. . . . . : Microsoft-ISATAP-Adapter
    Physikalische Adresse . . . . . : 00-00-00-00-00-00-00-E0
    DHCP aktiviert. . . . . : Nein
    Autokonfiguration aktiviert . . . . . : Ja
  
```

Abbildung 4.2: IP Konfiguration aller Interfaces

Der Primäre DHCP Server 10.0.2.15 hat dem Client die IP Adresse 10.0.2.16 zugewiesen. Eine IP aus einem nicht reservierten Bereich. Um den Gegentest durchführen zu können, wird nun der DHCP-Dienst auf dem Primären DHCP abgeschaltet und der Client neugestartet. Nach dem Neustart des Clients, wurde erneut der oben stehende Befehl abgesetzt. Das Ergebnis sieht danach wie folgt aus:

```

    DHCP aktiviert. . . . . : Ja
    Autokonfiguration aktiviert . . . . . : Ja
    Verbindungslokale IPv6-Adresse . . . . . : fe80::4d63:fac7:6324:c17c%11(Bevorzugt)
    IPv4-Adresse . . . . . : 10.0.2.16(Bevorzugt)
    Subnetzmaske . . . . . : 255.255.255.0
    Lease erhalten. . . . . : Dienstag, 3. April 2018 20:25:58
    Lease läuft ab. . . . . : Mittwoch, 11. April 2018 20:25:58
    Standardgateway . . . . . : 10.0.2.2
    DHCP-Server . . . . . : 10.0.2.14
    DHCPv6-IAID . . . . . : 235405351
    DHCPv6-Client-DUID. . . . . : 00-01-00-01-22-51-98-60-08-00-27-F7-5A-41
  
```

Abbildung 4.3: IP Konfiguration eines Interfaces

Der Client halt selbständig über den DHCPDISCOVER festgestellt, dass der primäre Server nicht erreichbar ist und vom sekundären Server die IP Adresse, sowie die Leasetime erhalten. Der Sekundäre Server hat somit die Aufgaben des Primären DHCP Servers übernommen.

4.2 Einrichtung DNS Dienst

Bereits während der Installation des Active Directory Domänendienst wird der DNS Dienst angelegt und bereits vorkonfiguriert. Er ist so eingestellt, dass dieser automatisch aktualisiert wird. Zusätzlich zu den automatischen Aktualisierungen, können manuelle Einträge als Host A Eintrag hinzugefügt werden. Diese Einträge können über den DNS-Manager verwaltet werden. Es gibt zwei Arten der Forward DNS Einträge:

- Host A
- Host AAAA

Host A definiert eine IPv4 Adresse und Host AAAA definiert eine IPv6 Adresse. Wenn ein DNS Eintrag manuell eingetragen wird, muss der FQDN des Servers/- Rechners und deren IP Adresse angegeben werden.

Jede Domäne sollte einen DNS Server haben. Gibt es innerhalb einer Domäne weitere Domänen, so muss dem DNS Server der übergeordneten Domäne dies mitteilen, damit dieser den DNS Server kennt. DNS Server arbeiten in der Regel nach dem Prinzip, wissen wo etwas zu finden ist. Sollte der DNS Server beispielsweise keinen Eintrag in der eigenen Datenbank finden, so prüft er hier die übergeordnete DNS Struktur, ob ihm dieser Name bekannt ist. DNS Server haben mehrere Zonen, eine Primäre und eine Sekundäre Zone. Eine Sekundäre Zone wird meist dann verwendet, wenn eine Domäne auf eine andere Domäne Zugreifen muss. Die Sekundäre Zone erstellt eine Kopie dieser und legt sie auf den Server ab.

4.3 Dateidienst/Freigaben einrichten

Das Anlegen von neuen Freigaben ist Assistentengesteuert, damit hier die Anpassungen alle auf einmal durchgeführt werden können. Um eine Freigabe hinzufügen zu können, muss zunächst im Server Manager -> Datei- und Speicherdienste -> Freigaben unter Aufgaben eine neue Freigabe ausgewählt werden:

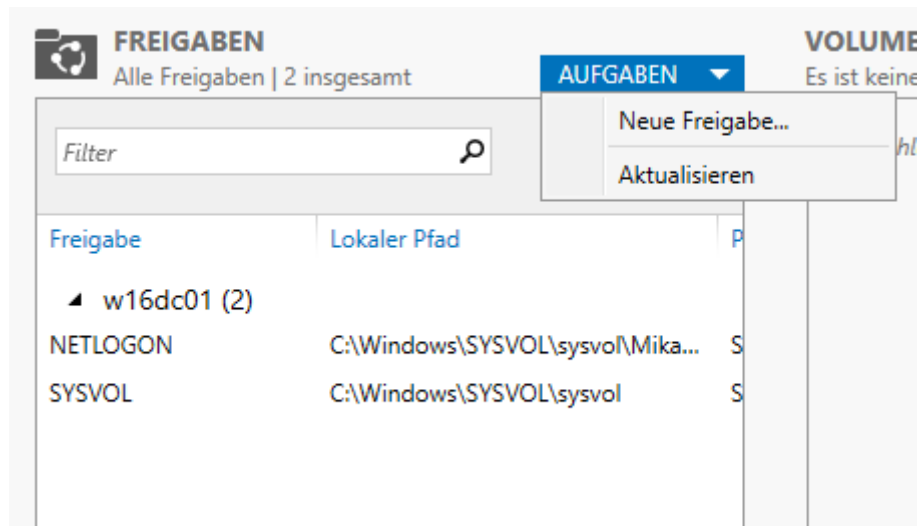


Abbildung 4.4: Erstellen von neuen Freigaben

Zum aktuellen Zeitpunkt besitzt der Server zwei Freigaben. Diese wurden während der Installation des ActiveDirectorys angelegt. NetLogon soll dabei für Anmeldeskripte zur Verfügung stehen.

Sobald auf neue Freigabe geklickt wurde, öffnet sich der Assistent für die Freigabe, in dem ein Profil aus folgenden ausgewählt werden muss:

- SMB-Freigabe - Schnell
- SMB-Freigabe - Erweitert
- SMB-Freigabe - Anwendungen
- NFS-Freigabe - Schnell
- NFS-Freigabe - Erweitert

Der Unterschied zwischen schnell und erweitert ist in diesem Fall nur wie viele Informationen während des Assistenten abgefragt werden sollen. Eine „SMB Freigabe für Anwendungen“ soll eine Freigabe für Hyper-V Manager oder Datenbanken darstellen.

Der Assistent gibt zu jedem Profil auf der rechten Seite eine kurze Beschreibung mit, um was es sich bei diesem Profil handelt. Für die Firma Mikado müssen mehrere SMB Freigaben angelegt werden, weshalb hier „SMB-Freigabe - Erweitert“ ausgewählt wird.

Im nächsten Schritt wird nun der Server ausgewählt, auf dem die Freigabe durchgeführt werden soll, sowie der Speicherort. Da innerhalb der Testumgebung zwei

DC Servers vorhanden sein werden, kann dies auf dem Master DC hinterlegt werden. Ein Praktischer Anwendungsfall wäre hier beispielsweise die Speicherung der Daten auf einem separaten Datei Server, da auf diesen entsprechende Sicherungen durchgeführt werden können.

Als nächstes wird der Freigabename abgefragt, welcher hier verwendet werden soll. Hier könnte man nun beispielsweise Abteilungsordner anlegen, welche den Nutzer bei jeder Anmeldung zugewiesen werden, damit jeder Mitarbeiter auch eine Ablage für die Abteilung besitzt.

Der Server zeigt nach der Eingabe des Namens unmittelbar den Lokalen, wie auch den Remotepfad zu dieser Freigabe an:

C:\Shares\Leitung

Quelltext 4.2: Lokaler Pfad zur Freigabe

\\w16dc01\Leitung

Quelltext 4.3: Remote Pfad zur Freigabe

Nachdem der Freigabename definiert wurde, werden weitere Einstellungen abgefragt. Diese können für die Abteilungsfreigabeordner auf dem Standard belassen werden. Im späteren Verlauf werden noch zwei Ordner „Profiles\$“ und „Home\$“ angelegt. Bei diesen beiden Freigaben handelt es sich um die servergespeicherten Profile. Dabei ist hier die Besonderheit, das bei dem Punkt „andere Einstellungen“ das Zwischenspeichern der Freigabe zulassen deaktiviert ist, sowie das \$ am Ende des Freigabennamens vorhanden ist. Nur mit diesem \$ Zeichen wird diese Freigabe nicht für die Benutzer sichtbar sein.

Damit nicht alle Nutzer Zugriff auf dieses Laufwerk erhalten können, werden entsprechende Berechtigungen definiert. Innerhalb des ActiveDirectory werden Sicherheitsgruppen für jede Abteilung erstellt, worin die Benutzer der Abteilung Mitglieder sind.

In diesem Beispiel wäre das die Sicherheitsgruppe: LGs-Leitung

Diese Gruppe soll Lese und Schreibberechtigung auf dieser Freigabe besitzen, dazu muss unter Berechtigungen anpassen -> hinzufügen die Sicherheitsgruppe ausgewählt werden. Innerhalb dieses Fensters, kann die Berechtigung festgelegt werden, die diese Gruppe erhält. Da in diesem Fall diese Gruppe Schreib und Leseberechtigung auf diese Freigabe erhalten sollen, wird folgende Berechtigung festgelegt:

- Lesen, ausführen
- Ordnerinhalt auflisten
- Lesen
- Schreiben

Ändern, sowie Vollzugriff erhalten die Benutzer in diesem Falle nicht. Nach bestätigen auf „weiter“, wird diese zuvor hinzugefügte Gruppe den Berechtigungen hinzugefügt. Im nächsten Schritt wird die Ordnerverwaltungseigenschaft für den Verwendungszweck des Freigegeben Ordners festgelegt. Dies wird wie eine Klassifizierungsregel innerhalb der Datenverwaltungsrichtlinie festgelegt.

Da es sich bei der Freigabe des Abteilungslaufwerks um eine Gruppenfreigabe (Benutzer sollen die Möglichkeit haben Daten untereinander austauschen zu können) handelt, muss dieses entsprechend ausgewählt werden. Auch hier gibt es wieder die Besonderheit, bei den Profiles und Home Freigaben. Da es sich bei diesen beiden um Ordner handeln, die in der Regel nur von einem einzelnen Benutzer verwendet werden, muss hier die Benutzerdateien ausgewählt werden.

Zum Schluss des Assistenten kann ein Speicherkontingent festgelegt werden. Hiermit wird der Speicherbereich limitiert, den der Benutzer zur Verfügung gestellt bekommt. Für die Abteilungslaufwerke ist dies nicht erforderlich. Wichtig ist dies in Bezug auf die Servergespeicherten Profile, sowie umgeleitete Ordner. Hierbei soll der Anwender nur eine maximale Menge von 200MB ablegen können, damit An- oder Abmeldungen nicht lange dauern. Benutzer sollen in der Regel Daten, die sie während der Arbeit brauchen auf dem Abteilungslaufwerk ablegen.

Abschließend erhält der Administrator eine Übersicht über die Freigabeeigenschaften. Sobald nun auf „erstellen“ geklickt wird, wird der Freigabe Ordner auf dem Server mit den entsprechenden Berechtigungen angelegt. Das Ergebnis sollte wie folgt aussehen:

Die Freigabe wurde erfolgreich erstellt.

Aufgabe	Fortschritt	Status
SMB-Freigabe erstellen	<div></div>	Abgeschlossen
SMB-Berechtigungen festlegen	<div></div>	Abgeschlossen
Ordnerverwendung festlegen	<div></div>	Abgeschlossen

Abbildung 4.5: Die einzelnen Aufgaben beim erstellen einer neuen Freigabe

Die Eigenschaften, welche zuvor festgelegt wurden, können nach abschließen des Assistenten weiterhin bearbeitet und angepasst werden.

Damit Servergespeicherte Profile innerhalb einer Freigabe abgelegt werden können, muss zunächst wie oben beschrieben jeweils eine Freigabe für „profiles\$“ und eines für „home\$“ angelegt werden.

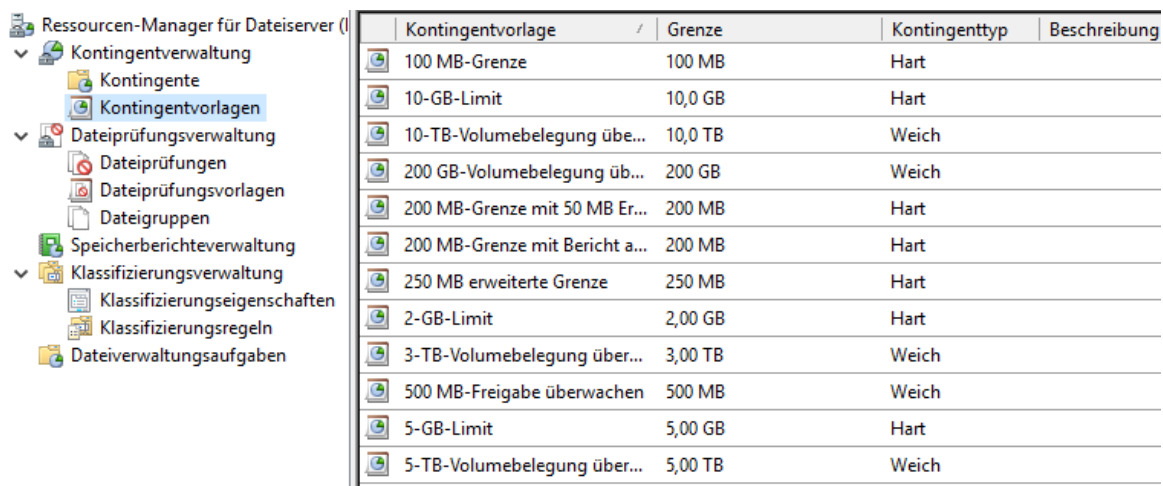
Hier sollte die Berechtigung auf eine bestimmte Benutzergruppe limitiert werden. Sinnvoll erscheint es hier eine Sicherheitsgruppe über das AD anzulegen und diese entsprechend Berechtigung darauf zu gewähren. Die Berechtigungen auf diese Ordner sollten wie folgt aussehen:

Ordner auflisten/Daten lesen, Attribute lesen, Ordner erstellen/Daten anhängen

Nur so kann ein Nutzer beim Anmelden ein Benutzerprofil innerhalb dieses Ordners anlegen und verwalten. Der Nutzer erhält auch nur auf diesen Ordner die Berechtigungen. Andere Ordner kann der Nutzer nicht sehen oder verändern.

4.3.1 Ressourcen-Manager

Über den Ressourcen Manager des Dateidienstes hat der Administrator die Möglichkeit, verschiedene Kontingente zuzuweisen oder angepasste Kontingente zu erstellen. Bei einer Überschreitung können verschiedene Aktionen durchgeführt werden. Beispielsweise kann dem Benutzer eine Systemerzeugte Meldung angezeigt oder eine Email an den Administrator oder dem Benutzer versendet werden. Voraussetzung hierfür ist ein SMTP Server. Zusätzlich kann der Administrator verschiedene Dateitypen für das Speichern auf gewissen Laufwerken verbieten. So kann hier festgelegt werden, das beispielsweise keine Excel Makros mit *.xslm Endung auf einem Laufwerk abgelegt werden kann. Der Ressourcen Manager kann zusätzlich zu diesen Funktionen auch Logs erzeugen, sowie Klassifizierungen der Inhalte durchführen. Hierzu kann entsprechend ein Zeitplan festgelegt werden, indem das System diese Ordner überprüft.



Kontingentvorlage	Grenze	Kontingenttyp	Beschreibung
100 MB-Grenze	100 MB	Hart	
10-GB-Limit	10,0 GB	Hart	
10-TB-Volumebelegung übe...	10,0 TB	Weich	
200 GB-Volumebelegung übe...	200 GB	Weich	
200 MB-Grenze mit 50 MB Er...	200 MB	Hart	
200 MB-Grenze mit Bericht a...	200 MB	Hart	
250 MB erweiterte Grenze	250 MB	Hart	
2-GB-Limit	2,00 GB	Hart	
3-TB-Volumebelegung über...	3,00 TB	Weich	
500 MB-Freigabe überwachen	500 MB	Weich	
5-GB-Limit	5,00 GB	Hart	
5-TB-Volumebelegung über...	5,00 TB	Weich	

Abbildung 4.6: Kontingentvorlagen im Ressourcen-Manager für Dateiserver

4.4 Active Directory Domänendienst

Nachdem die Grundinstallation abgeschlossen wurde, kann mit der eigentlichen Konfiguration begonnen werden. Bereits nach der Basis Installation, meldet der Windows Server „Konfiguration erforderlich“ an und zeigt einen Link um den Server zum DomainController (DC) hinaufzustufen. Anschließend muss die Art des Domänencontrollers festgelegt werden. Da es sich hierbei um eine neue Gesamtstruktur mit neuem DC handelt, muss hier „Neue Gesamtstruktur hinzufügen“ ausgewählt werden. Der DC benötigt nun die Stammdomäne, welche „Mikado.Spiel“ lautet. Dies kann der Fully Qualified Domain Name sein, muss mindestens jedoch eine Second-Level-Domain sein. Anschließend muss mit weiter bestätigt werden.

Im nachfolgenden Dialog können Domänencontrolleroptionen eingestellt werden. Dabei muss nun für die Gesamtstrukturfunktionsebene, sowie der Domänenfunktionsebene der älteste DC definiert werden. Da innerhalb der Testumgebung sowohl ein DC auf einem Windows Server 2012 R2 und einer auf Windows Server 2016 installiert werden muss, muss hier Windows Server 2012 R2 ausgewählt werden. Dies kann nachträglich nicht nach unten korrigiert werden.

Der Kontrollkästchen bei DNS Server sollte gesetzt werden, da jeder DC auch DNS Server sein kann. Da es sich hierbei um den ersten DC in der Gesamtstruktur handelt, muss dieser ebenfalls als Globaler Katalog definiert werden.

Der Globale Katalog dient für domänenübergreifende Suchfunktionen für AD Objekte. Er speichert ausgewählte Attribute aller Objekte aus allen Domänen.

Abschließend muss hier ein Wiederherstellungskennwort definiert werden, welches benötigt wird falls AD-Objekte gelöscht wurden um diese wiederherzustellen. Das Kennwort muss nach dem Booten in den Verzeichnisdienst Wiederherstellungsmodus eingegeben werden. Ohne dieses können gelöschte AD-Objekte nicht wiederhergestellt werden.

Windows schlägt anschließend einen NetBIOS Domänennamen vor, welcher sich aus dem ersten Bestandteil des FQDNs zusammensetzt. Dieser kann, muss jedoch nicht angepasst werden.

Nach erneutem bestätigen auf „weiter“, werden die Speicherorte für die AD DS Datenbanken, sowie Protokolldateien abgefragt. Diese können ebenfalls bei Bedarf angepasst werden. Die nächste Seite, zeigt nun eine Gesamtübersicht der Änderungen an, welche zuvor definiert worden sind. Ebenfalls kann hieraus ein PowerShell Skript erzeugt werden, welches gegebenenfalls angepasst werden kann.

Abschließend überprüft die Installationsroutine ein letztes Mal, ob alle Einstellungen und Anforderungen erfüllt sind. Dabei werden bereits einige Warnung angezeigt, welche ignoriert werden können. Sobald die Installationsroutine mit „installieren“ durchgelaufen ist, wird der Lokale Administrator des Windows Servers automatisch Mitglied der Gruppen Organisations-, Schema- und Domänen-Admins und hat somit die Berechtigung Änderungen und Anpassungen durchführen zu dürfen. Ebenso wird der DNS Server des Windows Servers innerhalb der IP Konfiguration hinterlegt. Der Windows Server 2016 wird dabei mehrmals neugestartet und in die Domäne eingebunden.

4.4.1 EDV-Struktur im Active Directory

Der Aufbau des Active Directory, sollte im Regelfall analog der Unternehmensstruktur aufgeteilt sein. Innerhalb des ADs werden diese in Organisationseinheiten aufgeteilt. Letztendlich können solche Organisationseinheiten auch Standorte widerspiegeln. Organisationseinheiten sollen bei den Verwaltungsaufgaben helfen. Jeder Angelegte Benutzer, welcher keiner Organisationseinheit hinterlegt wurde, wird in den Container „User“ abgelegt. Bei mehreren Hundert Nutzern wären diese alle in dem User Container enthalten. Dies könnte jedoch gerade in Bezug auf die Rechtevergabe Probleme verursachen, da unterschiedliche Nutzer auch unterschiedliche Berechtigungen erhalten. So könnte man je Organisationseinheit unterschiedliche Berechtigungen zuweisen ohne jeden Nutzer einzeln verändern zu müssen.

Um neue Organisationseinheiten hinzufügen zu können, muss auf die Domäne mit Rechtsklick -> Neu -> Organisationseinheit geklickt werden. Anschließend kann ein

Name für diese Organisationseinheit festgelegt werden. Außerdem wird festgelegt, ob die Gruppe gelöscht werden kann. Dies soll das versehentliche Löschen der Gruppe vorbeugen.

Nachdem alle Organisationseinheiten definiert wurden, sieht die Struktur nun wie folgt aus:

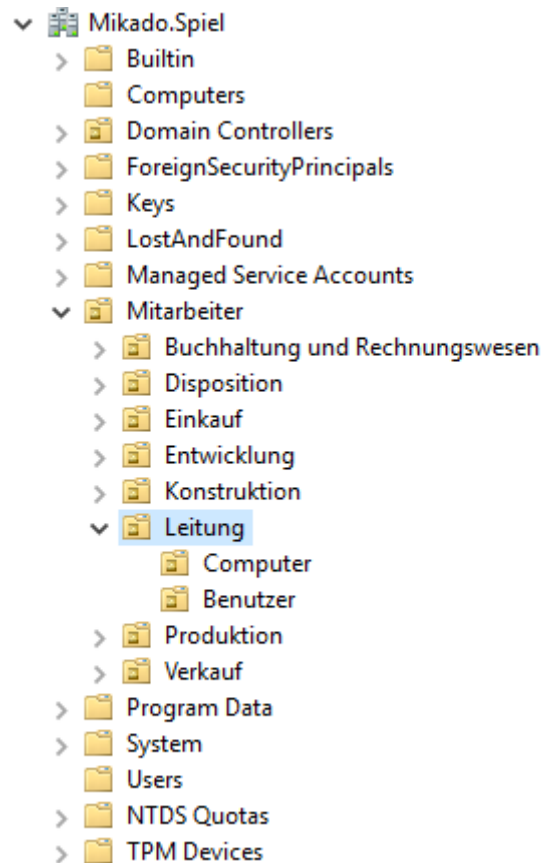


Abbildung 4.7: Struktur im Active Directory

Jede Abteilung hat eine einzelne Organisationseinheit zugewiesen bekommen. Unter dieser Abtrennung werden anschließend zwei zusätzliche Organisationseinheiten angelegt, welche nach Benutzer und Computer unterschieden wird. Dies hat den Vorteil, dass im Späteren Verlauf die Gruppenrichtlinien auf einzelne Abteilungen beschränkt werden können. Um erweiterbare Funktionen einblenden lassen zu können, empfiehlt es sich unter dem Punkt Ansicht die Erweiterten Features zu aktivieren.

4.4.2 Replikation

Innerhalb einer Domäne sollte es immer zwei DomainController, sowie zwei DHCP Server geben. Falls einer der beiden Server ausfällt, können sich die Nutzer weiterhin Anmelden und erhalten weiterhin eine IP Adresse.

Damit ein zusätzlicher Server in die Domäne integriert werden kann, muss zunächst eine zusätzliche Maschine aufgesetzt werden. Hier wurde sich für einen Windows Server 2012 R2 entschieden. Nachdem der Server installiert wurde, kann unter Server-Manager der Domain Controller, wie der erste DC installiert werden. Domain Controller sind innerhalb einer Domäne gleichberechtigt, so kann jeder Server die gleichen Aufgaben des anderen übernehmen.

Nachdem die Installation der ActiveDirectory Domänendienste abgeschlossen wurde, muss dieser zunächst zum Domain Controller heraufgestuft werden. Wichtig ist hierbei, dass die Option „Domänencontroller zu einer vorhandenen Domäne hinzufügen“ ausgewählt sein muss, damit der DC in die vorhandenen Mikado Domäne zugefügt wird.

Damit die Domäne ausgewählt werden kann, kann Rechts auf „auswählen“ geklickt werden. Es öffnet sich ein Windows Anmeldefenster, wo die Anmeldeinformationen von einem Domänen Administrator eingetragen werden müssen. Wichtig ist hier, dass ein Benutzer eingetragen wird, welcher die Berechtigung hat, Computer oder Server in die Domäne aufnehmen zu dürfen. Anschließend werden die Domänen Informationen abgefragt und angezeigt:

Wählen Sie den Bereitstellungsvorgang aus.

- ☒ Domänencontroller zu einer vorhandenen Domäne hinzufügen
- ☐ Neue Domäne zu einer vorhandenen Gesamtstruktur hinzufügen
- ☐ Neue Gesamtstruktur hinzufügen

Geben Sie die Domäneninformationen für diesen Vorgang an.

Domäne:

Geben Sie die Anmeldeinformationen für diesen Vorgang an.

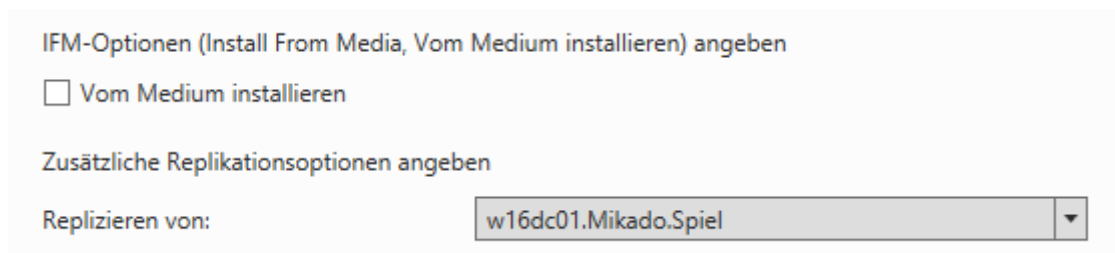
Benutzername:

Abbildung 4.8: Hinzufügen eines DCs zu einer vorhandenen Domäne

Nachdem die Domäne ausgewählt wurde, kann mit „weiter“ bestätigt werden.

Jeder Domain Controller, sollte gleichzeitig ein DNS Server beinhalten, sowie ein Globaler Katalog sein, damit hier abfragen schneller durchgeführt werden können. Der DNS Server auf dem zweiten DomainController, kann zudem innerhalb der DHCP Konfiguration als Sekundärer DNS Server eingetragen werden. Auch hier muss wieder ein Wiederherstellungskennwort eingetragen werden, welches im Falle vom versehentlichen Löschen von Ordnern oder AD Strukturen benötigt wird.

Als nächsten Schritt muss die DNS Delegierung, sowie ausgewählt werden, von welchem DC repliziert werden soll. Da es zum aktuellen Zeitpunkt, bereits einen DC (w16dc01) gibt, kann dieser nachfolgend ausgewählt und mit „weiter“ bestätigt werden:



IFM-Optionen (Install From Media, Vom Medium installieren) angeben

☐ Vom Medium installieren

Zusätzliche Replikationsoptionen angeben

Replizieren von: w16dc01.Mikado.Spiel ▼

Abbildung 4.9: Auswahl der Replikationsquellen für einen neuen DC

Wie auch bei dem ersten DC, werden auf dem zweiten DC Verzeichnisse für die Protokollierung, sowie die Datenbank angelegt. Abschließend gibt die Installationsroutine die Übersicht für die anstehenden Änderungen. Mit klicken auf „Installieren“, wird der DC Konfiguriert und der Windows Server einmal neugestartet.

Die Replikation ist nun abgeschlossen. Alle Änderungen, welche fortan auf dem DC01 durchgeführt werden, werden innerhalb weniger Sekunden auf den DC02 repliziert. Sollte eine Replizierung der Daten aussetzen, so ruft der DC02 automatisch nach einer Stunde die Informationen ab.

Nachdem der Server erneut gestartet wurde, kann die Anmeldung mit dem Administrator vom DC01 durchgeführt werden.

4.4.3 Benutzerkonten erstellen

Benutzer können über die „Active Directory Benutzer und Computerverwaltungsübersicht“ manuell hinzugefügt werden. Hierzu kann innerhalb einer OU mit Rechtsklick -> Neu -> Benutzer ein Benutzer hinzugefügt werden. Der Benutzer wird nun direkt in die richtige OU angelegt.

In dem dann neu eröffneten Fenster muss nun ein Vorname, Nachname und Benutzername festgelegt werden. Der Benutzername muss innerhalb einer Domäne eindeutig sein und besteht bei der Firma Mikado aus einer 5 stelligen Personalnummer. Eine Personalnummer darf nie doppelt vergeben werden, da diese zusätzlich in der Buchhaltung als Referenz für den Mitarbeiter verwendet wird. Nachdem diese Informationen eingetragen wurden, muss mit „weiter“ bestätigt werden. Es folgt die Abfrage nach dem Benutzerkennwort, womit sich dieser an einem Rechner oder Domäne anmelden kann. Das Kontrollkästchen bei „Benutzer muss Kennwort bei der nächsten Anmeldung ändern“ sollte angehakt sein, damit der Anwender ein eigenes von ihm definierte Kennwort erstellen kann. Hier kann man beispielsweise nun ein Kennwort verwenden, welches der Standardrichtlinien entspricht. Als Beispiel wäre hier „Mikado2018!“ möglich, da es sowohl klein-, Großbuchstaben, sowie Sonderzeichen und Zahlen enthält. Dieses Passwort ist allerdings unsicher und sollte nicht in realen Setups genutzt werden.

Nachdem der Anwender sich hiermit an einem Rechner innerhalb der Domäne anmeldet, wird automatisch die Änderung des Kennworts verlangt. Ohne dieses ist keine Anmeldung an der Domäne möglich.

Sollte es sich bei dem angelegten Nutzer um einen Service Account handeln, beispielsweise FTP Zugriff oder sonstiges, empfiehlt es sich hier, das Kennwort nicht ablaufen zu lassen, sowie das Kontrollkästchen bei „Benutzer muss Kennwort bei der nächsten Anmeldung ändern“ rauszunehmen, da andernfalls die Funktion dieses Service Accounts eingeschränkt sein könnte.

Zum Schluss wird eine Übersicht über den Nutzer angezeigt.

4.4.4 Gruppenkonten erstellen

Ein Gruppenkonto, kann entweder in einer Abteilungs OU oder in dem Container User erstellt werden. Hierzu muss man innerhalb des gewünschten Verzeichnis mit der rechten Maustaste > Neu > Gruppe die Gruppe hinzufügen. Es öffnet sich ein neues Fenster, wo weitere Einstellungen vorgenommen werden können. In der Regel muss hier zunächst ein Gruppen Namen definiert werden. Dabei sollte geachtet werden, dass der Gruppenname eindeutig zu der Funktion der Gruppe ist, da im späteren Verlauf nur der Gruppennamen angezeigt wird, jedoch nicht deren Funktion. Zusätzlich ist gegebenenfalls hilfreich anzugeben, für welche Abteilung dieses Gruppe ist.

Gruppen haben drei Gruppenbereiche und zwei Gruppentypen zur Auswahl. Die Gruppenbereiche geben an, welche Benutzerkonten und Computerkonten Mitglied

von dieser Gruppe sein dürfen und von welcher Domäne. Hierzu gibt es folgende Erläuterung:

Gruppenbereich	Mitgliedschaft	Verwendbarkeit
Lokal (in Domäne)	Benutzer- und Computerkonten beliebiger Domänen, globale und universelle Gruppen beliebiger Domänen, lokale Gruppen derselben Domäne	Nur in derselben Domäne
Global	Benutzer- und Computerkonten derselben Domäne, globale Gruppen derselben Domäne	In beliebigen Domänen
Universal	Benutzer- und Computerkonten beliebiger Domänen, globale und universelle Gruppen beliebiger Domänen	In beliebigen Domänen

Tabelle 4.1: Gruppenbereiche in Domänen

Die zwei Gruppentypen sind unterteilt in **Sicherheit** und **Verteilung**. **Sicherheitsgruppen** können Sicherheitsrichtlinien zugewiesen werden und können somit den Zugriff auf Ressourcen zulassen oder verweigern. Bei **Verteilungsgruppen** wird der Nutzer, welcher Mitglied dieser Gruppe ist, in einen Verteiler hinzugefügt. Verteilergruppen erhalten nach dem Erstellen ebenfalls eine Email Adresse, an denen Benutzer beispielsweise eine Email schreiben könnten.

Nachdem eine Sicherheitsgruppe erstellt wurde, kann sie nachträglich mit einem doppelklick auf dieser bearbeitet werden. Unter den Reitern Mitglieder, können Benutzer hinzugefügt werden. Dieser Änderungen werden bei Sicherheitsgruppen erst nach erneuter Anmeldung mit dem Benutzerkonto sichtbar.

Bereits beim Anlegen der einzelnen Organisationseinheiten, hat das Active Directory automatisch Sicherheitsgruppen mit dem selbigen Namen angelegt. Alle Benutzer, die in den einzelnen Organisationseinheiten sind, sind automatisch Mitglied dieser Sicherheitsgruppe.

4.4.5 Computerkonten erstellen

Computerkonten können analog zu den Benutzerkonten erstellt werden. Die Computerkonten sollten auch hier unmittelbar direkt in der richtigen OU hinterlegt werden, damit Computerrichtlinien exakt angewandt werden können. Der Computername sollte ebenfalls wie auch der Benutzername eindeutig sein, damit hier innerhalb der Domäne keine Konflikte auftreten können. Zusätzlich zu dem Benutzernamen muss definiert werden, welcher Nutzergruppe den Computer in die Domäne integrieren kann. Dies ist in der Regel nicht für alle Nutzer gestattet. Wichtig bei der Namensgebung ist auch die Konvention für den DNS Server, da unmittelbar nach Anlegen des Computers, dieser ebenfalls dem DNS bekannt wird. Sobald dieser sich im Netzwerk meldet, wird er über den DHCP Server in die Zone aufgenommen und hinterlegt.

4.4.6 Skript zum Anlegen von Nutzern, Computern

Anlegen von Nutzern oder Computern und Zuweisung für deren Richtlinie, kann entweder manuell durchgeführt werden oder aber mittels Script ausgeführt werden [Gmb16]. Zusätzlich zu diesem Skript, gibt es ebenfalls noch das Anmeldeskript, worauf nachträglich im nächsten Kapitel eingegangen wird.

```
$password = "XTi114!" | ConvertTo-SecureString -AsPlainText -Force
New-ADUser -Name 'Nikolai Luis' -SamAccountName 00003 -UserPrincipalName 00003 \
-DisplayName 'Nikolai Luis' -GivenName Nikolai -Surname Louis -Path \
"OU=Benutzer,OU=Leitung,OU=Mitarbeiter,DC=Mikado,DC=Spiel" -AccountPassword \
$password -ChangePasswordAtLogon $True -Enabled $True -ProfilePath \
\\w16dc01\profiles$\00003 -hmdir \\w16dc01\home$\00003
```

Quelltext 4.4: Powershell Script zum Anlegen von AD Nutzern

Das oben stehende PowerShell Skript, fügt einen vordefinierten Benutzer an die angegebene OU und DC ein. Er erhält ein Passwort „XTi114!“, welches nach der Anmeldung direkt geändert werden muss. Bedingt dadurch das die PS Eingabe keine Klartext Passwörter verwenden kann, muss dieses zuvor in einen Sicheren String umgewandelt werden.

4.4.7 Anmeldeskript

Ein Anmeldeskript wird während der Anmeldung eines Nutzers geladen und angewendet. Im Script können Netzlaufwerke, Drucker oder Freigaben eingefügt sein.

Es gibt verschiedene Möglichkeiten, Benutzern ein Anmeldeskript zur Verfügung zu stellen. Der einfachste Weg wäre über eine Gruppenrichtlinie das Anmeldeskript zur Verfügung zu stellen. Es kann jedoch auch unmittelbar direkt an das Benutzerprofil beigefügt oder an einen Computer zugewiesen werden.

Das Anmeldeskript ist immer in einem freigegeben Ordner „Netlogon“ auf einem DC gespeichert, wo der Nutzer hinterlegt ist. Innerhalb des Benutzerprofil oder Gruppenrichtlinie, wird anschließend nur der Name des Skripts hinterlegt. Das ActiveDirectory ergänzt eigenständig den Pfad zu diesem Skript.

Zusätzlich zum Anmelden eines Benutzers, kann ein Skript auch beim Abmelden, starten oder Herunterfahren des Computers. Es spielt keine Rolle, wie viele Anmeldeskripte einem Benutzer zugewiesen wurden. Windows arbeitet alle Skripte nacheinander ab.

Die Anmeldeskripte werden nach dem Hinterlegen im Netlogon Verzeichnis auf die anderen DCs repliziert, sodass alle DCs die gleichen Skripte besitzen.

4.4.8 Servergespeicherte Benutzerprofile

Servergespeicherte Benutzerprofile werden immer dann wichtig sein, wenn sich ein Benutzer an mehreren unterschiedlichen Rechnern anmeldet. Die erzeugten und bearbeiteten Daten oder Dokumente werden beim Abmelden auf den Server zurückgesichert. Meldet sich ein Benutzer an einem anderen Rechner wieder an, werden die Daten und das Profil vom Server heruntergeladen. Es gibt insgesamt zwei Arten von Servergespeicherten Profilen. Einmal die veränderbaren Benutzerprofile, dabei werden alle Änderungen innerhalb der Sitzung zum Server zurückgesichert. Die andere Art sind verbindliche Profile. Diese aktualisieren ein bereits vorhandenes Profil mit den Neuerungen, welche auf dem Server vorhanden sind.

Im Fall der Firma Mikado, werden Veränderbare Benutzerprofile verwendet, da im späteren Verlauf zusätzlich die Richtlinie angewandt wird, dass Benutzerprofile nach Abmelden vom Rechner entfernt werden.

Um die Servergespeicherten Profile konfigurieren zu können, muss unter der Verwaltungskonsole des Active Directorys die Benutzereigenschaften aufgerufen werden. Diese Einstellungen können bereits während des Anlegens oder mittels Anlegeskript erzeugt werden.

Unter dem Reiter „Profil“ kann unter Profilpfad der Pfad zu der Freigabe eingetragen werden. Wichtig ist hierbei die Variable „%username%“. Damit weiß das Active Directory, dass diese Stelle durch den Benutzernamen, in unserem Fall die Personalnummer ersetzt werden soll. Sobald ein Benutzer sich nun mit seinem Be-

nutzernamen an einem Domänenrechner anmeldet, wird für ihn ein entsprechendes Profil innerhalb des Profiles Ordner angelegt.

Benutzerprofile sind immer von der Windows Version abhängig. Ein Nutzer, welcher mit seiner Benutzerkennung an einem Windows XP Client angemeldet war, kann sich mit diesem Profil nicht an einem Windows 7 Rechner anmelden. Die Struktur der Verzeichnisse ist unterschiedlich.

4.4.9 Heimatverzeichnisse

Zusätzlich zu servergespeicherten Profilen, wird in der Regel auch eine Umleitung der persönlichen Verzeichnisse (Eigene Dokumente, Desktop) durchgeführt. Dies hat den Vorteil, dass eine An- und Abmeldung schneller durchgeführt werden kann, als wenn diese Ordner innerhalb des Profils gespeichert werden. Die entsprechenden Dokumente sind für einen Benutzer anschließend über ein Netzlaufwerk zu erreichen, wo unter anderem auch das Benutzerprofil abgelegt ist. Wichtig ist dabei, dass diese Ablage von dem Profilserver separiert ist, da andernfalls ein Benutzer an diese Daten nicht drankommen könnte, falls der Profilserver nicht erreicht wäre. Heimatverzeichnisse und Ordnerumleitungen werden nicht in dem Pprofil des Benutzers hinterlegt, sondern innerhalb einer Gruppenrichtlinie festgelegt. Diese kann anschließend entweder an einen Nutzer oder aber Computer zugewiesen sein.

Um die Umleitung der Ordner zu aktivieren, muss zunächst die Default Domain Policy angepasst werden. Hierzu wird unter Tools die Gruppenrichtlinienverwaltung geöffnet.

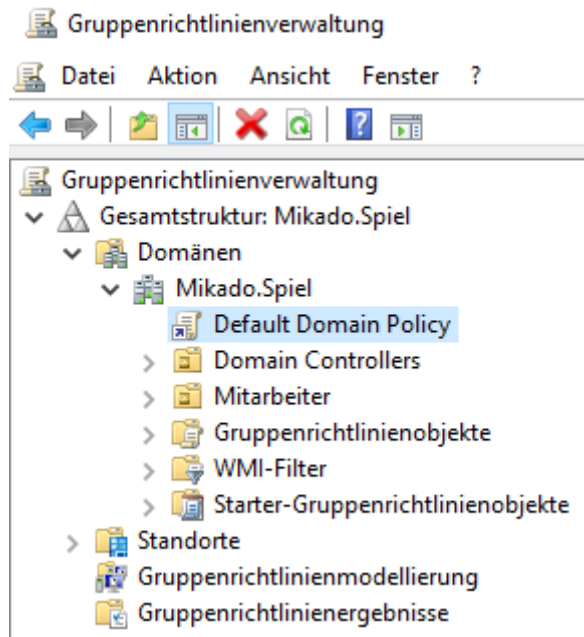


Abbildung 4.10: Gruppenrichtlinienverwaltung innerhalb einer Domäne

Mit Rechtsklick auf Default Domain Policy kann diese bearbeitet und angepasst werden. Es empfiehlt sich hier gegebenenfalls ein zusätzliches Gruppenrichtlinienobjekt anzulegen. Innerhalb diesem muss um die Ordnerumleitung verwalten zu können unter Benutzerkonfiguration -> Windows-Einstellungen navigiert werden. Unter dem Punkt Ordnerumleitung, werden alle Benutzerordner angezeigt:

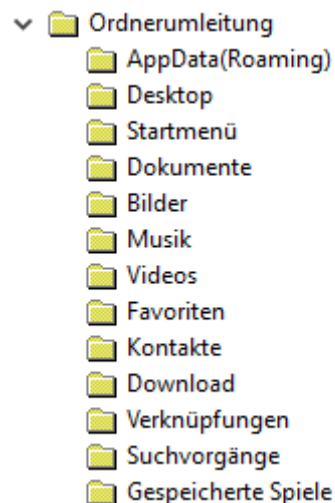


Abbildung 4.11: Ansicht der vorhandenen Ordnerumleitungen

Wichtig hierbei ist, dass die größten Ordner umgeleitet werden. Dazu gehören AppData, Desktop, Dokumente, Bilder, Musik. Um die Umleitung zu aktivieren, muss ein Ordner ausgewählt werden und anschließend über Rechtsklick Eigenschaften bearbeitet werden.

Unter den Eigenschaften kann nun das Ziel sowie Einstellungen vorgenommen werden. Unter dem Punkt Ziel muss zunächst als Zielordner „Einen Ordner für jeden Benutzer im Stammpfad erstellen“ ausgewählt sein. Anschließend wird das Stammverzeichnis unter Angabe des UNC-Pfades festgelegt. Unmittelbar nach Eingabe des UNC-Pfades, zeigt das Fenster bereits eine Vorschau des Pfades zu diesem Nutzer an:

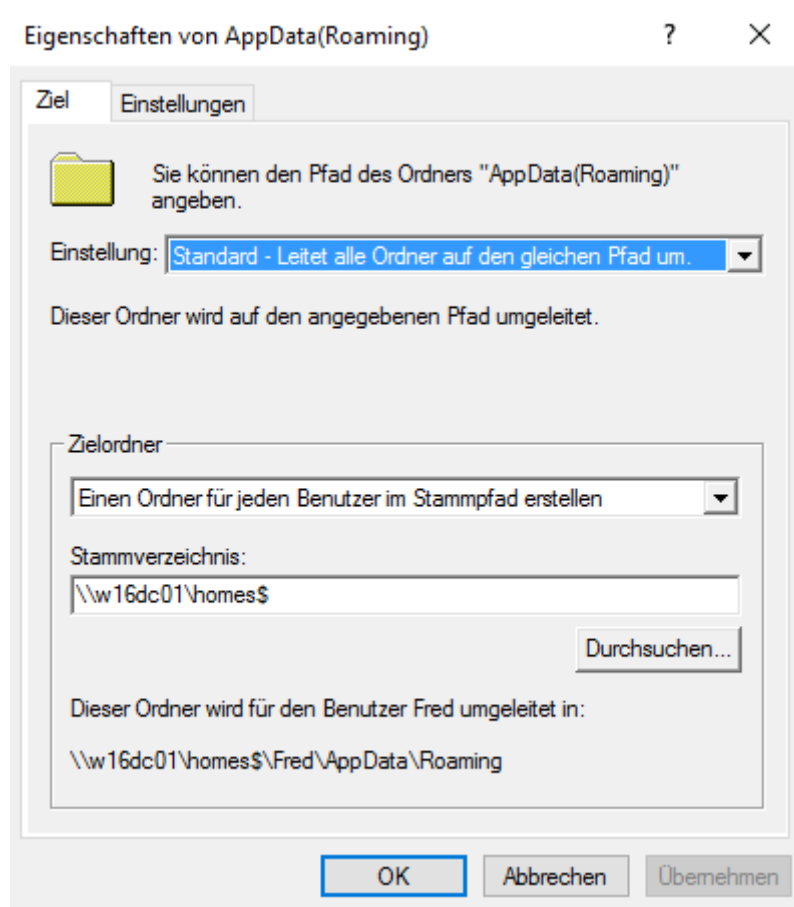


Abbildung 4.12: Eigenschaften der Ordnerumleitung für AppData 1

Exemplarisch wurde dies für die AppDaten des Anwenders durchgeführt. Zusätzlich zu diesen Einstellungen kann festgelegt werden, ob dem Nutzer exklusive Zugriffsrechte für Dokumente erteilt werden. Dies kann ein Nachteil für den Administrator sein, da dieser im Falle einer Problemlösung innerhalb des Profils den

Besitz übernehmen muss und anschließend wieder zurückschreiben muss. Sollten dabei Fehler unterlaufen, so könnte der Benutzer nicht mehr auf diese Daten zugreifen. Die Einstellung „Den Inhalt von <Ordnername> an den neuen Speicherort verschieben“ sollte aktiviert werden, da durch diesen der Ordner auf dem Rechner gelöscht und an den zuvor definierten Speicherort verschoben wird. Sollte diese Option nicht aktiviert sein, so verbleibt eine Kopie des Ordners auf dem Rechner. Im letzten Abschnitt kann festgelegt werden, was passieren sollen, falls die Richtlinie entfernt wird.

Zum Abschluss sollten die Einstellungen wie folgt aussehen:

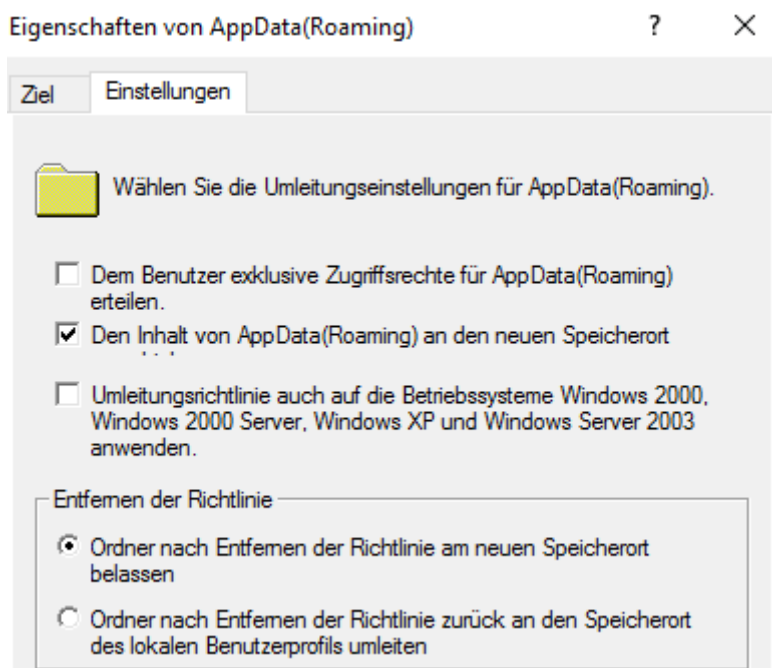


Abbildung 4.13: Eigenschaften der Ordnerumleitung für AppData 2

Nach Klicken auf „ok“ wird eine Fehlermeldung ausgegeben, die für ältere Betriebssysteme gedacht ist. Diese kann jedoch bei Verwendung von Windows 7 oder neuer ignoriert und mit „Ja“ bestätigt werden. Die zuvor eingestellten Anpassungen, müssen nun für die restlichen Ordner ebenfalls durchgeführt werden, damit die Ordnerumleitung auch auf die restlichen Aktiviert wird.

Die Ordner Bilder, Musik und Videos, können dem Ordner Dokumente folgen, so muss für diese nicht zusätzlich ein Pfad mit angegeben werden.

Die Benutzerkonfiguration für die Ordnerumleitung ist nun abgeschlossen. Nachträglich müssen noch weitere Computerkonfigurationen vorgenommen werden,

damit auch der Computer für Servergespeicherte Profile konfiguriert ist. So müssen beispielsweise Einstellungen vorgenommen werden, das der Computer auf das Netzwerk wartet, oder aber das die Sicherheitsgruppe „Administrator“ dem Servergespeicherten Profil hinzugefügt wird, damit hier bei einer Problemlösung am Benutzerprofil der Profilbesitzer nicht gewechselt werden muss.

Diese Einstellungen, müssen ebenfalls in der Default Domain Policy, oder aber in der zuvor erstellten Policy unter dem Punkt Computerkonfiguration > Richtlinien > Administrative Vorlagen angepasst werden.

Folgende Punkte müssen hier für eine erfolgreiche Umleitung der Ordner eingerichtet werden:

- System -> Benutzerprofile -> Sicherheitsgruppe „Administrator“ zu servergespeicherten Profilen hinzufügen
- System -> Benutzerprofile -> Zeitlimit für langsame Netzwerkverbindung für Benutzerprofile steuern
- System -> Anmelden -> Beim Neustart des Computers und bei der Anmeldung immer auf das Netzwerk warten
- Netzwerk -> Offlinedateien -> Alle Offlinedateien vor der Abmeldung synchronisieren
- Netzwerk -> Offlinedateien -> Untergeordnete Ordner immer offline verfügbar machen

Nachdem diese Einstellungen innerhalb der Computerkonfiguration aktiviert wurden, ist die Ordnerumleitung aktiviert und kann verwendet werden. Sollte hierbei eine Benutzerdefinierte Domain Policy verwendet worden sein, so muss diese zusätzlich noch für die einzelne Domäne hinterlegt werden.

Ein Heimatverzeichnis muss nicht mittels Anmeldeskript angebunden werden. Dieses kann ebenfalls über eine Gruppenrichtlinie oder innerhalb des Nutzerprofiles unter Eigenschaften -> Profil -> Basisordner verlinkt werden.

4.4.10 Speichervolumen Begrenzung

Wie bereits in Kapitel 4.3 erläutert, gibt es verschiedene Möglichkeiten, das Dateilimit innerhalb eines Verzeichnisses zu limitieren. Die Anforderung der Firma Mikado besteht darin, dass ein Angestellter ein maximales Speichervolumen von 200MB besitzt. Um diese Kontingentgrenze definieren zu können, muss zunächst innerhalb des Ressourcen Managers für Dateiserver, ein neues Kontingent angelegt werden.

Hierzu kann eine bestehende Kontingentgrenze als Vorlage verwendet werden. Anschließend muss der Kontingentpfad angegeben werden. In diesem Fall:

C:\Shares\profiles

C:\Shares\home

Quelltext 4.5: Benötigte Pfade zur Kontingentverwaltung

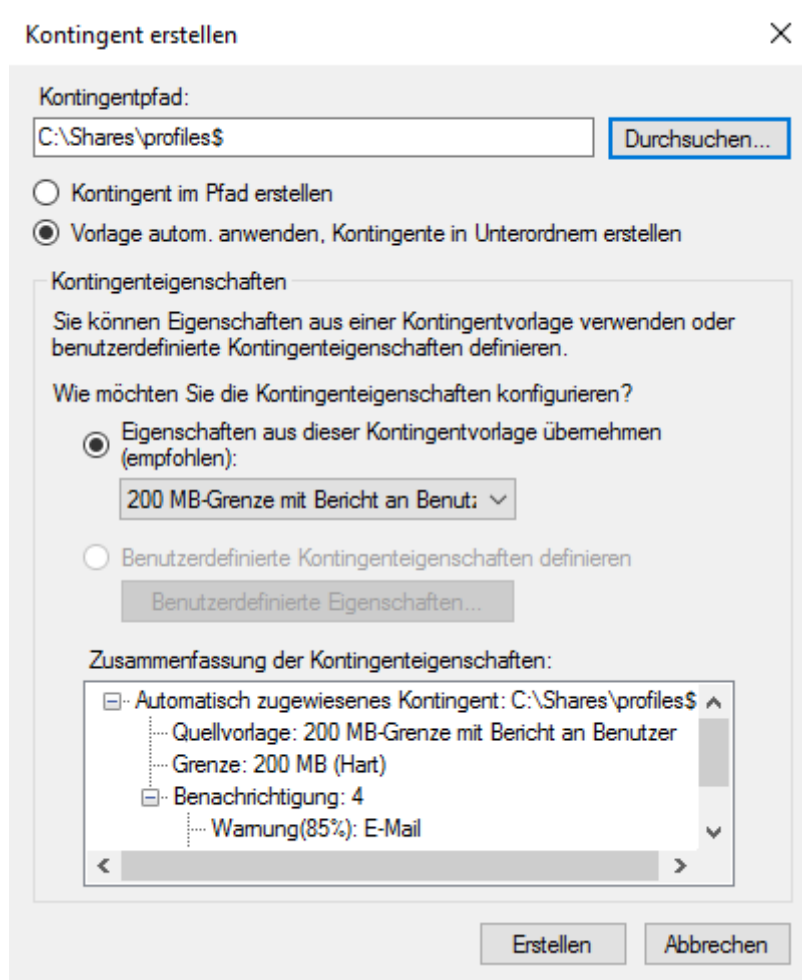


Abbildung 4.14: Erstellung eines neuen Kontingents

Nachdem der Pfad zu dem Kontingent angelegt wurde, muss „Vorlage automatisch Anwenden. Kontingente in Unterordnern erstellen“ ausgewählt werden. Dies bedeutet, dass das Kontingentlimit nur auf die Unterordner bezogen wird, welche innerhalb dieses Ordners angelegt werden, jedoch nicht auf das gesamte Verzeichnis. Dies hat den Vorteil, dass jeder Benutzer ein eigenes Kontingent von 200MB besitzt.

Als Kontingenttyp wird hier hart ausgewählt. Der Unterschied zwischen harter Kontingent und weicher Kontingent ist der folgende:

Weiche Kontingentgrenze:

- Die Speichergrenze kann überschritten werden, eine Aktion, wie beispielsweise Email Versand, Fehler oder Befehl wird ausgeführt. Speichererweiterung um 50MB möglich.
- Dient nur der Überwachung

Harte Kontingentgrenze:

- Die Speichergrenze kann nicht überschritten werden
- Limitierung des Speicherplatzes

Abschließend sehen die Kontingenteinträge wie folgt aus:



	C:\Shares\home\$*	---	2...	Hart (...)	200 MB-Grenz...	Ja
	C:\Shares\profiles\$*	---	2...	Hart (...)	200 MB-Grenz...	Ja

Abbildung 4.15: kontingenteinträge

Um eine Weiche Kontingentgrenze zu definieren, muss die Eigenschaft „Benutzerdefinierte Kontingentgrenze definieren“ ausgewählt sein. Sobald auf Benutzerdefinierte Eigenschaft geklickt wird, öffnet sich ein neues Fenster, wo die Grenzen, wie weiche- oder harte Kontingentgrenze, sowie deren Aktion ausgewählt und definiert werden kann.

4.5 Einrichten von Druckern

Innerhalb einer Domäne kann es einen Druck- und Dokumentenserver geben. Dieser stellt den Clients Drucker oder Dokumente zur Verfügung. Hierbei handelt es sich um eine Rolle, welche innerhalb des Server-Managers hinzugefügt werden muss.

Sollte es innerhalb der Domäne Unix Systeme, wie Ubuntu oder Archlinux geben, so sollte hier der Punkt LPD-Dienst aktiviert werden.

Nachdem die Rolle hinzugefügt wurde, kann diese über die Druckverwaltung administriert werden.

Ein Druckerserver bietet die Möglichkeit, Netzwerkdrucker und deren Treiber zur Verfügung zu stellen, so muss ein Client, welcher den Drucker über ein Anmeldeskript zugewiesen bekommt die Installation nicht manuell anstoßen und Windows

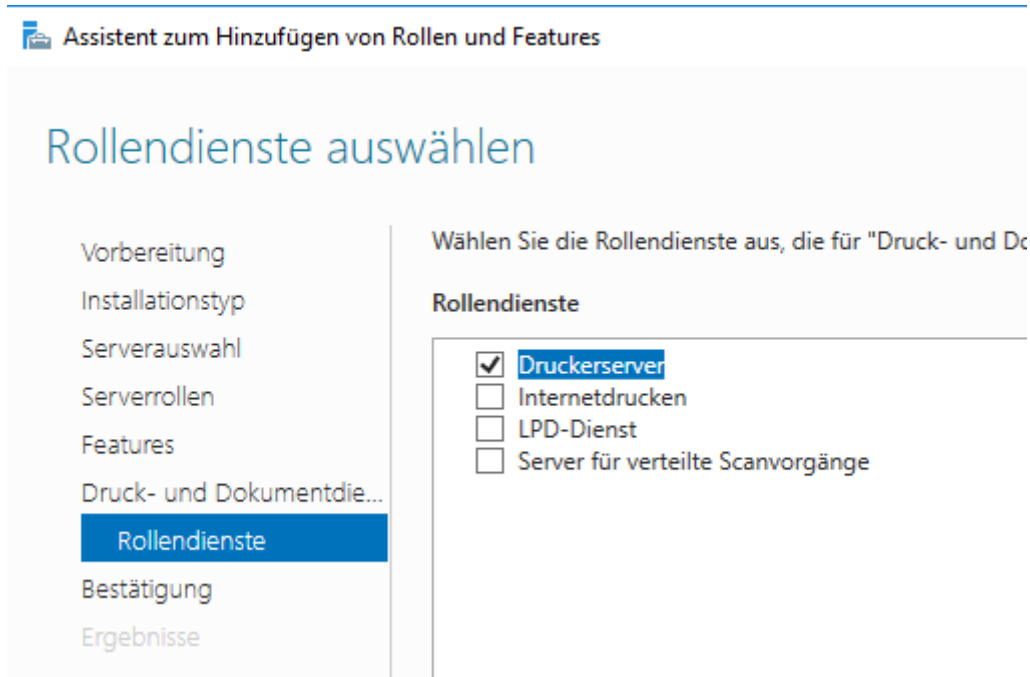


Abbildung 4.16: Übersicht für neue Rollen

muss nicht die Windows Updates für die Druckertreiber durchsuchen. Druckertreiberaktualisierungen können so zentral gesteuert werden.

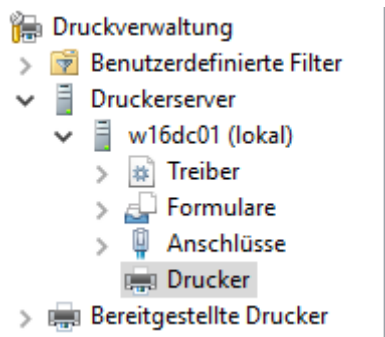


Abbildung 4.17: Ansicht der Druckverwaltung

Über Rechtsklick, können unter „Drucker hinzufügen“ weitere Drucker hinzugefügt werden. Diese können anschließend über die GPO dem Benutzer zur Verfügung gestellt werden. Der Netzwerkdruckerassistent durchsucht eigenständig das Netzwerk, nach dem angegebenen Druckern.




 DR1000	Bereit	0	w16dc01 (lokal)
 Microsoft Print to PDF	Bereit	0	w16dc01 (lokal)
 Microsoft XPS Document Writer	Bereit	0	w16dc01 (lokal)

Abbildung 4.18: Übersicht über alle Drucker

4.6 Gruppenrichtlinien

Gruppenrichtlinien bestehen aus zwei Teilen und sind ein mächtiges Verwaltungstool. Der erste Teil besteht aus der Computerkonfiguration. Diese bezieht immer auf einem Computer, egal welcher Nutzer angemeldet ist. Der zweite Teil besteht aus der Benutzerkonfiguration, welche spezifisch für die Nutzer definiert werden können. Ein kleines Beispiel soll dies verdeutlichen:

Die Kennwortrichtlinie ist innerhalb der BenutzerKonfiguration so eingestellt, dass eine Komplexität von 8 Zeichen benötigt wird. Sobald ein Nutzer versucht das Kennwort auf dem Rechner anzupassen, kann dieser jedoch ein Kennwort mit nur einer Länge vergeben, da die Computerkonfiguration keine Richtlinie für das Kennwort vorgibt.

Gruppenrichtlinien werden immer an eine Sicherheitsgruppe gebunden, welche anschließend einem Benutzer zugewiesen werden kann. Standardmäßig sind keine Richtlinien oder Einschränkungen festgelegt. Innerhalb einer Sicherheitsgruppe, können mehrere Gruppenrichtlinien zugewiesen sein. Wichtig ist hierbei die Verknüpfungsreihenfolge der einzelnen GPOs. Sollte in der ersten Gruppenrichtlinie etwas deaktiviert sein, jedoch in der zweiten aktiviert, so greift hier die Gruppenrichtlinie, welche an erster Stelle steht.

Unterschieden wird auch ob eine GPO erzwungen ist. Sollte eine GPO erzwungen werden, so greift stets die GPO wo diese Einstellung festgelegt wurde.

4.7 Kontorichtlinien

Kontorichtlinien, sind Vorgaben die ein Benutzer erfüllen muss. Sie können beispielsweise die Länge eines Kennworts sein oder andere ähnliche Einstellungen.

4.7.1 Kennwortrichtlinien

Für die Mikado.Spiel Domäne als Testumgebung sind folgende Kennwortrichtlinien definiert worden:

Eigenschaft	Vorgabe
Kennwort erforderlich	Ja
Länge	8 Zeichen
Alter	50 Tage
Wiederbenutzbar	Nach 12 Kennwörtern

Tabelle 4.2: Kennwortrichtlinien

Um diese Kennwortrichtlinie festlegen zu können, muss entweder innerhalb der Standard Gruppenrichtlinie (Default Global Policy) oder in einer neuen zuvor definierten Gruppenrichtlinie folgende Werte unter Computerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen -> Kontorichtlinien geändert werden:







Richtlinie	Richtlinieneinstellung
 Kennwort muss Komplexitätsvoraussetzungen entsprechen	Aktiviert
 Kennwortchronik erzwingen	12 gespeicherte Kennwörter
 Kennwörter mit umkehrbarer Verschlüsselung speichern	Nicht definiert
 Maximales Kennwortalter	50 Tage
 Minimale Kennwortlänge	8 Zeichen
 Minimales Kennwortalter	30 Tage

Abbildung 4.19: Realisierte Kennwortrichtlinie

Nun ist die Kontorichtlinie für die Sicherheitsgruppe aktiv, für die diese Richtlinie zugewiesen ist.

4.7.2 Anmelderichtlinien

Zusätzlich zu Kennwortrichtlinien, hat die Firma Mikado die Richtlinie, das sich die Mitarbeiter nur während der Arbeitszeit von Montag bis Freitag zwischen 08:00Uhr bis 18:00 Uhr im Netzwerk anmelden dürfen. Hierzu ist seitens des Domaincontroller

zu limitieren, das eine Anmeldung auch außerhalb dieser Zeiten durchgeführt werden kann. Diese Einstellung wird nicht in einer Gruppenrichtlinie definiert, sondern für jeden Benutzer innerhalb der Active Directory-Benutzer und Computer verwaltungsoberfläche festgelegt.

Unter dem Reiter Konto > Anmeldezeiten, können die Anmeldezeiten durch auswählen festgelegt werden.

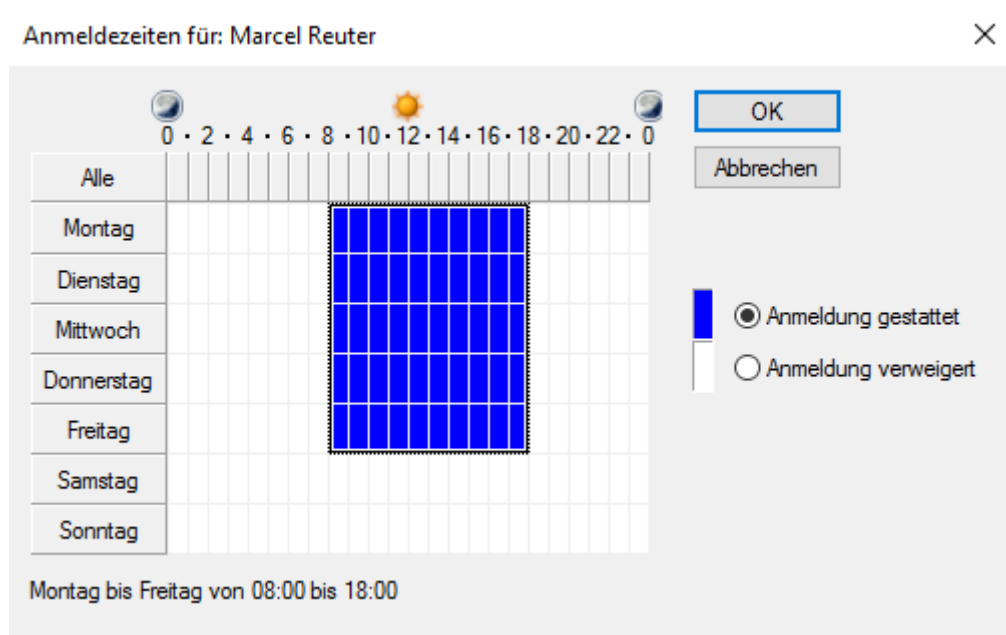


Abbildung 4.20: Detailansicht der Anmeldezeiten

Sollte ein Benutzer versuchen außerhalb dieser Zeiten eine Anmeldung durchzuführen, so erhält er folgende Meldung:

„Das Konto sieht es nicht vor, dass Sie sich zu dieser Zeit anmelden. Wiederholen Sie diesen Vorgang später.“

4.7.3 Administrator Account umbenennen

Die Anpassung des Lokalen Administrator eines Clients kann ebenfalls über eine Gruppenrichtlinie festgehalten und verändert werden. Hierzu muss unter Benutzerkonfiguration -> Einstellungen -> Systemsteuerungseinstellungen -> Lokale Benutzer und Gruppen zunächst mit Rechtsklick Neu -> Lokaler Benutzer hinzugefügt werden. Unter dem Drop Down Menü „Benutzername“ kann „Administrator (integriert)“ ausgewählt werden und wie unten stehend umbenannt werden.

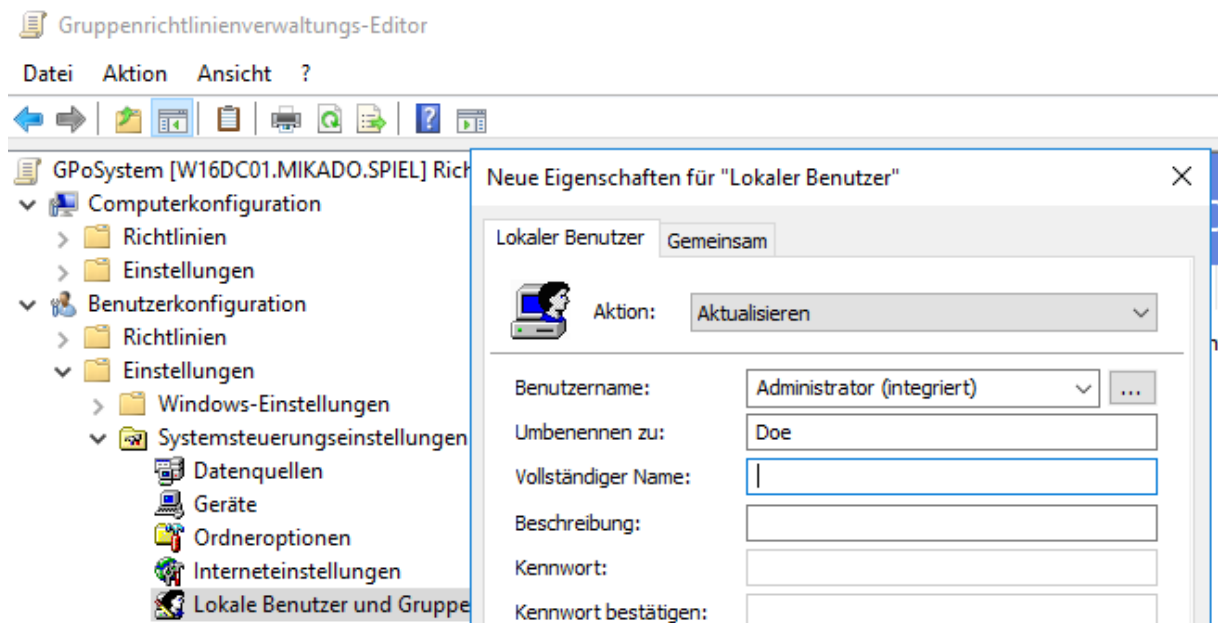


Abbildung 4.21: Gruppenrichtlinienverwaltungs-Editor

Die Umbenennung soll helfen, damit Nutzer oder Schadsoftware das Administrator Konto schlechter finden können.

4.8 Zugriffsrechte

Zugriffsrechte dienen in erster Linie dazu das System vor ungewollten Zugriff zu schützen. Sie schützen jedoch nicht nur den Computer, sondern auch das Netzwerk vor Schadsoftware, welche unter anderem durch USB Massenspeicher auf den Rechner übertragen werden können.

4.8.1 Zugriff auf Lokale Laufwerke

Damit Benutzer am Rechner keine Viren in das Netzwerk einschleusen können, sollen Laufwerke, wie auch USB Massenspeicher am Rechner deaktiviert werden. Diese Einstellung wird innerhalb der Gruppenrichtlinie festgelegt. Damit nicht alle Nutzer von diesen Anpassungen betroffen sind, kann eine neue Gruppenrichtlinie hierfür definiert werden, welche nur an bestimmte Sicherheitsgruppen zugewiesen werden. Ausgenommen werden hier beispielsweise Administratoren oder die Führungsebene.

Um diese Einschränkung festlegen zu können, muss unter Benutzerkonfiguration -> Richtlinie -> Administrative Vorlage -> System -> Wechselmedienzugriff folgende Richtlinie aktiviert werden:

Wechselmedienzugriff		
Markieren Sie ein Element, um dessen Beschreibung anzuzeigen.	Einstellung	Status
	Zeit (in Sekunden) bis zur Erzwungung des Neustarts festlegen	Nicht konfigur...
	CD und DVD: Lesezugriff verweigern	Nicht konfigur...
	CD und DVD: Schreibzugriff verweigern	Nicht konfigur...
	Benutzerdefinierte Klassen: Lesezugriff verweigern	Nicht konfigur...
	Benutzerdefinierte Klassen: Schreibzugriff verweigern	Nicht konfigur...
	Diskettenlaufwerke: Lesezugriff verweigern	Nicht konfigur...
	Diskettenlaufwerke: Schreibzugriff verweigern	Nicht konfigur...
	Wechseldatenträger: Lesezugriff verweigern	Nicht konfigur...
	Wechseldatenträger: Schreibzugriff verweigern	Nicht konfigur...
	Alle Wechselmedienklassen: Jeglichen Zugriff verweigern	Aktiviert

Abbildung 4.22: Konfiguration für Wechselmedienzugriff

Sollte diese Regel aktiviert werden, sind alle Wechseldatenträger an diesem Rechner, wo der Benutzer angemeldet ist, deaktiviert. Diese Regel greift, bevor andere Regeln für spezifische Wechseldatenträger definiert wurden.

4.8.2 Zugriff auf Eingabeaufforderung

Der Zugriff auf die Eingabeaufforderung sollte im Regelfall nur deaktiviert werden, falls kein Anmeldeskript oder Skript beim An- oder Abmelden hinterlegt ist, da dieses andernfalls nicht ausgeführt werden kann. Sollte kein Anmeldeskript oder sonstige Skripte vorhanden sein, die eine Eingabeaufforderung bedürfen, kann diese Richtlinie unter Benutzerkonfiguration -> Administrative Vorlage -> System -> Zugriff auf Eingabeaufforderung verhindern aktiviert werden.

Zuweisen von Laufwerken und Druckern, kann ebenfalls über eine Gruppenrichtlinie festgelegt werden.

4.8.3 Zugriff auf Systemadministration

Um den Zugriff auf Systemeinstellungen zu verbieten, damit hier keine Änderungen an dem Computersystem vorgenommen werden kann, wird diese Konfigurationsmöglichkeit für jeden Benutzer deaktiviert. Damit kann ein Benutzer die Systemsteuerung, sowie Informationen zu Konfiguration des Computers nicht mehr abrufen.

fen oder verändern. Diese Richtlinie kann innerhalb der Gruppenrichtlinie unter Benutzerkonfiguration -> Administrative Vorlagen -> Systemsteuerung aktiviert werden.

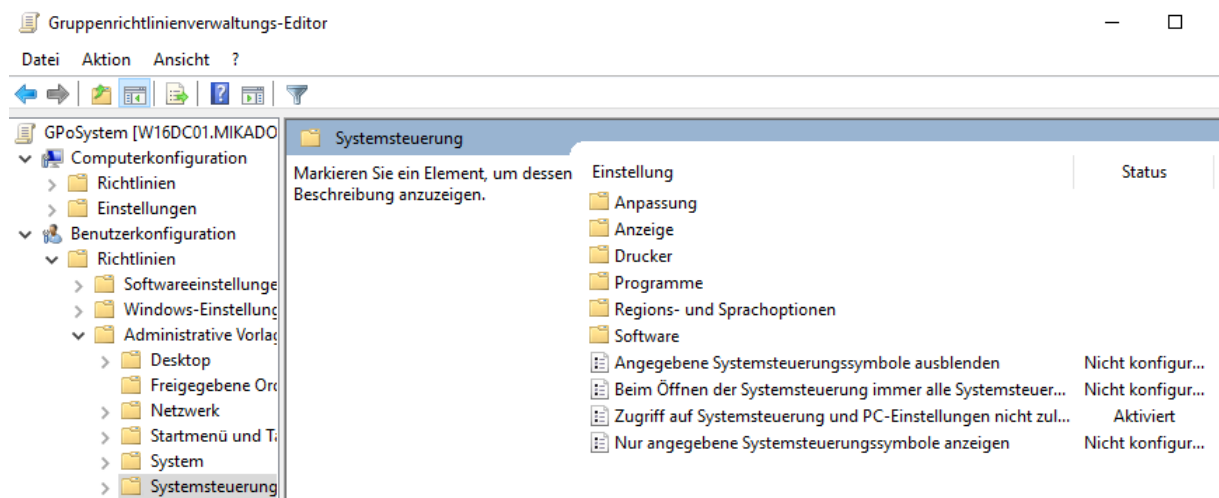


Abbildung 4.23: GPO Editor für Zugriff auf die Systemsteuerung

4.9 Datenaustausch

Für den Datenaustausch der Mitarbeitern, sowie Abteilungsleitern, sind folgende Anforderungen definiert worden:

Die Abteilungsleiter untereinander uneingeschränkt Daten austauschen können.

Hierzu muss zunächst eine Sicherheitsgruppe „LGsAbteilungsleiter“ erstellt werden, damit nicht jeder Mitarbeiter einzeln in die Freigabe ausgewählt werden muss. Anschließend muss eine Freigabe erstellt werden „ExchangeAbt“ auf die die Sicherheitsgruppe Lese, sowie Schreibberechtigung besitzt. Dieses Laufwerk kann nun über eine zusätzliche Gruppenrichtlinie an die Abteilungsleitern über die Sicherheitsgruppe zugewiesen werden.

Die nächste Anforderung ist, dass Abteilungsleitern, Aufträge für Mitarbeiter einstellen können, diese die Daten jedoch nur abrufen können.

Hierzu muss zunächst eine Sicherheitsgruppe für die Mitarbeiter „LGsMitarbeiter“ erstellt werden und zusätzlich eine Freigabe, welche „Auftraege“ lautet. Auf diese Freigabe muss nun die Sicherheitsgruppe „LGsAbteilungsleiter“ lese, sowie schreibberechtigung besitzen. Mitarbeiter erhalten hier mit der Sicherheitsgruppe „LGsMitarbeiter“ nur Leseberechtigung.

Dies kann ebenfalls in umgekehrter Reihenfolge für Aufträge gemacht werden, welche Mitarbeiter den Abteilungsleitern lesend zur Verfügung stellen. Eine zusätzliche Freigabe „beaAuftraege“ wird benötigt.

Die Zuweisung der Laufwerksbuchstaben für die Clients, kann über eine separate oder zuvor erstellte Gruppenrichtlinie zugewiesen werden. Die Richtlinie/Konfiguration ist hierzu unter Benutzerkonfiguration -> Einstellungen -> Windows-Einstellungen -> Laufwerkszuordnung -> neu hinzugefügt werden.

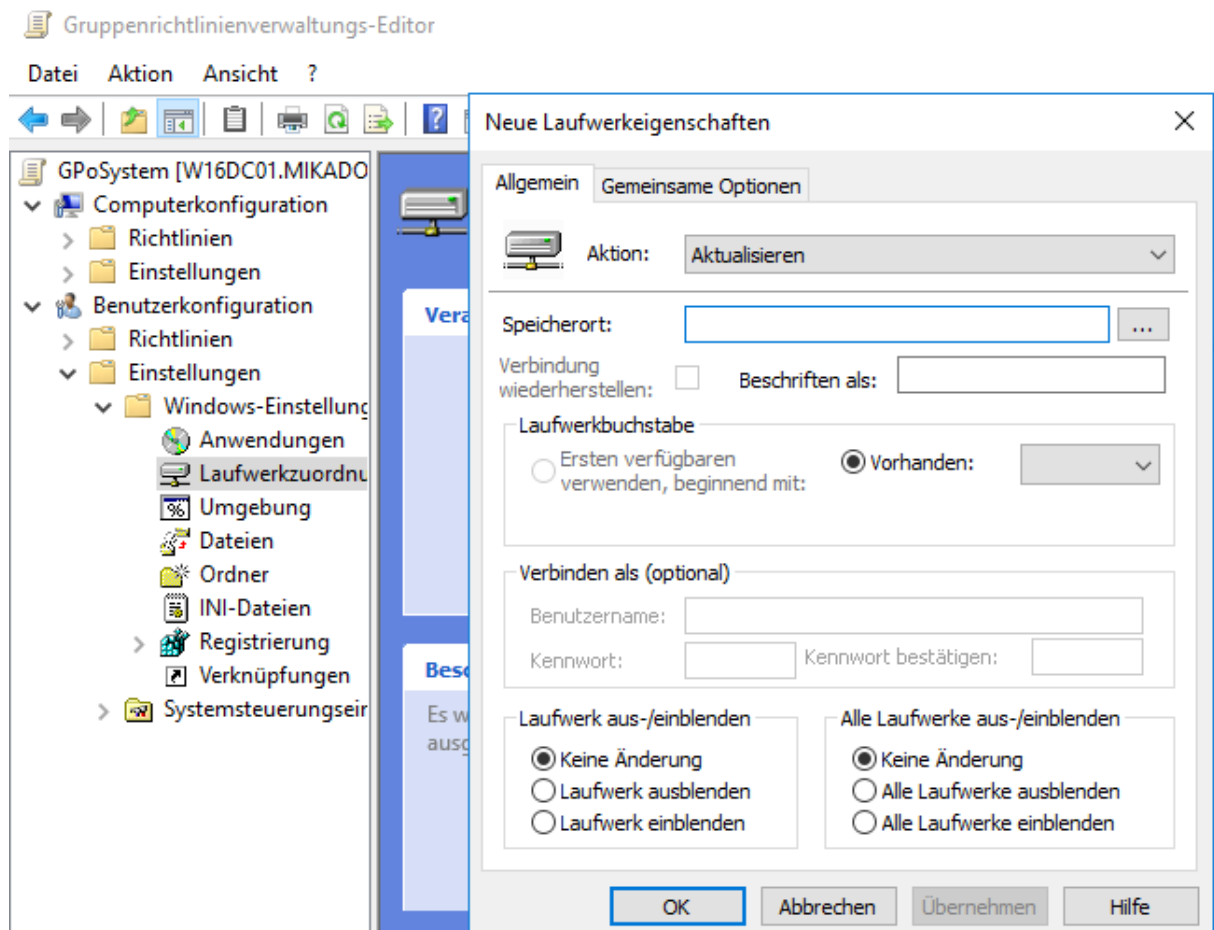


Abbildung 4.24: GPO Editor für Laufwerkseigenschaften

Hier hat der Administrator nun die Möglichkeit, den Speicherort für diese Freigabe festzulegen. Die Zuweisung der GPO als solches, wird über die Sicherheitsrichtlinie „LGsMitarbeiter“ und „LGsAbteilungsleiter“ durchgeführt.

5 Glossar

DC Domain Controller, ein Server, welcher einen Verzeichnisdienst zur Verfügung stellt. 10

VRRP Virtual Router Redundancy Protocol, Zwei Router in Einer Layer 2 Domäne haben jeweils eine IP-Adresse konfiguriert und machen darüber Healthchecks. Sie agieren im Active/Passive Modus, eine Service IP-Adresse (auch VIP - Virtual IP) ist auf dem aktiven Router konfiguriert. Sie dient als Gateway innerhalb des Layer 2. 8

6 Literatur

- [Gmb16] Microsoft Deutschland GmbH. *Bulk Active Directory User creation to specific OU*. März 2016. URL: <https://gallery.technet.microsoft.com/scriptcenter/Bulk-Active-Directory-User-b53bb1f6>.

7 Anhang

Szenario zur Vorbereitung RNA-Abschlussprüfung 2018

Zeitraum:	November 2017 bis April 2018
für die Klasse:	TI114
Fachlehrer:	W. Dreser
Hilfsmittel, Hard- und Software:	Server, HyperV2012R2, OS W7, VMs 2 x W2k12R2 Basisinstallation, VMs 2 x W7Prof Basisinstallation,

Szenario

Die Firma <<Mikado>>, ein Unternehmen der Spielzeugmanufaktur in Köln beschließt eine Umorganisation der EDV-Infrastruktur. Zum kommenden Geschäftsjahr - Juli 2018 - soll die neue Infrastruktur implementiert sein.

Im Oktober 2017 wurde bereits die Hardwarestruktur auf den technologisch neuesten Stand gebracht. Damit die Neustrukturierung der inneren Abläufe und deren Darstellung in der EDV-Welt reibungslos von statten geht, wird ihre Firma <TI114-Consult> damit beauftragt, ein entsprechendes Konzept zu entwickeln und dem zukünftigen Gesamtvorstand vorzustellen.

Aktuell werden für die Betriebssystemstruktur drei Linux-Server mit Windows XP Clienten eingesetzt. Diese Konstellation ist, als Ergebnis einer Mitarbeiterbefragung nicht performant genug.

Zu diesem Zweck bietet die Firma <TI114-Consult> an, eine Testumgebung aufzubauen, damit während der Präsentation die komplexen Zusammenhänge deutlich werden.

Aufgabenstellung

Sie als Mitarbeiter der Firma <TI114-Consult> erhalten nun von ihrem Projektleiter die Aufgabe diese Testumgebung zu entwickeln. Dabei sind folgende Randbedingungen sind zur Konzeption zu beachten:

- Insgesamt beschäftigt die Firma zukünftig nur noch max. 100 Mitarbeiter in den verschiedenen Abteilungen. Die Leitung der Firma besteht insgesamt aus 3 Personen. Die Abteilungen im Einzelnen werden sein:

Entwicklung, Einkauf, Disposition, Produktion, Konstruktion,
Buchhaltung und Rechnungswesen, Verkauf

- Insgesamt sollen ca. 50 Client-PCs zur Verfügung stehen.
- Zwei Domänencontroller werden zukünftig in einer Domäne eingesetzt.
- Je Abteilung ist ein Netzwerkdrucker vorgesehen.
- Die Firma möchte Ihren Internetauftritt demnächst intern auf einem eigenen Server gestalten. Dazu hat sie den Domänennamen <<Mikado.Spiel>> erworben.

Die PCs verteilen sich wie folgt auf die einzelnen Abteilungen:

Entwicklung	10 PCs
Einkauf	5 PCs
Disposition	5 PCs
Produktion	5 PCs
Konstruktion	10 PCs
Buchhaltung und Rechnungswesen	5
Verkauf	5
Chef-PCs	3
PCs zur Administration	2

Alle Schritte gemäß Rahmenbedingungen sind zu planen und in Form einer Schulungsunterlage zu dokumentieren.

Sie können die Arbeit in Partnerarbeit durchführen.

Gutes Gelingen!

Rahmenbedingungen der Fa. Mikado.

Teil A: Konfiguration und Austesten des W2K12-Servernetzes.

Für die Umsetzung der EDV-Kommunikationsstruktur der Firma sind folgende Aspekte umzusetzen:

Planen Sie ein neues DHCP-, DNS- und Windowsdomänenkonzept mit

- einem geeignetem DHCP – Konzept so, dass die IP- Adressen möglichst effizient genutzt werden,
- einem geeigneten DNS-Namensraum für den neuen Firmenbereich,
- einer beispielhaften Bezeichnung aller Hardwarekomponenten,
- einer geeigneten Dokumentation (Skizze) der DNS – Struktur sowie
- der Darstellung des Windowsdomänenkonzeptes.

Zur Darstellung ist es sinnvoll Skizzen anzufertigen. Die ergänzende Beschreibung muss unter Verwendung der Fachterminologie erfolgen.

Als zentrale Verwaltungseinheiten werden zwei Domänencontroller eingesetzt. Folgende Optionen müssen geplant werden:

- Darstellung der EDV-Struktur der Firma im Active Directory.
- Ein Namenskonzept für User, das auch das Einsetzen von Scripten unterstützt. Erstellen Sie zur Verwaltung der Mitarbeiter ein geeignetes Script. Die Namen sind frei wählbar. Es reicht aus beispielhaft ca. 5 User anzulegen.
- Serverbasierte Benutzerprofile für alle Mitarbeiter werden auf einem Server gespeichert. Auf den Client-PCs ist eine Speicherung von Benutzerprofilen zu unterbinden.
- Für alle Mitarbeiter sind serverseitig Heimatverzeichnisse auf einem Server zu planen. Es können zwei Konzepte gegenübergestellt werden.
- Für die Angestellten wird das maximale Speichervolumen auf 200 MB eingestellt.

Hinweis: Es ist hilfreich, auch hier entsprechende Planungsskizzen anzufertigen!

Zur Erhöhung der Netzwerksicherheit sollen mindestens folgende Bedingungen umgesetzt werden:

- Alle Mitarbeiter werden verpflichtet, ein Kennwort festzulegen, das den Kennwortkomplexitätsvorgaben Rechnung trägt und mindestens 8 Zeichen lang sein soll.

Das Kennwort soll immer nach 50 Tagen neu gesetzt werden, wobei alte Kennwörter erst wieder nach zwölf neuen benutzt werden können.

- Die Angestellten dürfen sich von montags bis freitags nur in der Zeit von 8.00 bis 18.00 Uhr in das Netzwerk einloggen. Für die Abteilungsleiter und die Chefs gilt diese Einschränkung nicht.
- Der Zugriff auf alle lokalen Laufwerke der Arbeitsstationen ist für die Mitarbeiter zu unterbinden. Ebenso der Zugriff auf USB- Speichermedien.
- Der Zugriff auf die Konsoleneingabe soll für alle Mitarbeiter unterbunden werden.
- Treffen Sie für die Domänencontroller und alle Client-PCs Maßnahmen, dass das Konto des Administrators nicht als solches erkennbar ist.
- Der Zugriff auf Programme zur Systemadministration wie Systemsteuerung, Datenbankrepository für Informationen zur Konfiguration der Computer, etc. sind für alle Mitarbeiter zu unterbinden.

Zum Datenaustausch zwischen den Mitarbeitern und den Abteilungsleitern ist eine geeignete Ordnerstruktur zu planen (Skizze mit allen entscheidenden Zugriffsbedingungen ist sinnvoll). Dort wo es notwendig erscheint, können Skripte Anwendung finden.

Dabei sollen

- die Abteilungsleiter untereinander uneingeschränkt Daten austauschen können,
- die Abteilungsleiter Aufträge an ihre Mitarbeiter einstellen können, die Mitarbeiter diese Daten lediglich abrufen können,
- die Mitarbeiter ihre bearbeiteten Aufträge ablegen können und die Abteilungsleiter nur abrufen können,
- die Kommunikationsordner für alle Mitarbeiter nach dem Login im Objekt Arbeitsplatz der jeweiligen Clients über Laufwerksbuchstaben ansprechbar sein.

Teil B: Erweiterung des W2K12-Servernetzes. Optional.
--

In Erweiterung der Testumgebung sollen auch zwei Linuxserver in die Windowsdomäne integriert werden. Diese sollten als Web- und Dateiserver zum Einsatz kommen.

8 Erklärung

Hiermit erklären wir, dass wir die Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt haben. Diese Arbeit wurde keinem anderen Prüfungsausschuss in gleicher oder vergleichbarer Form vorgelegt.

.....
Tim Meusel

.....
Marcel Reuter

.....
Nikolai Luis