

--- LogoDIDACT 2.0 --- Die Schulserverlösung

Dokumentation

Version 21.12.28.0



--- LogoDIDACT 2.0 --- Die Schulserverlösung: Dokumentation

Copyright ©

Inhaltsverzeichnis

I. LogoDIDACT 2.0 Überblick	I – 1
I.1. LogoDIDACT 2.0	I – 3
I.1.1. Überblick	I – 3
I.1.1.1. Module und Bausteine	I – 3
I.1.1.2. Die Architektur der Version 2.0	I – 4
I.1.1.3. Software und Lizenzierung	I – 6
I.1.1.4. Empfohlene Peripherie	I – 7
II. Installation des Servers	II – 1
II.1. LogoDIDACT-Server-Installation	II – 5
II.1.1. Vor der Installation	II – 5
II.1.2. Upgrade auf LogoDIDACT 2.0	II – 5
II.1.2.1. Upgrade auf Ubuntu 16.04	II – 6
II.1.2.2. Umstellung der Netzwerkkonfiguration auf systemd	II – 8
II.1.3. Neuinstallation	II – 9
II.1.3.1. Voraussetzungen	II – 10
II.1.3.2. Basisinstallation	II – 10
II.1.3.3. Systemaufbau durch Puppet	II – 22
II.1.3.4. LogoDIDACT Update	II – 24
II.1.3.5. Aktualisierung des Open vSwitch	II – 25
II.1.3.6. Änderung des root-Kennwortes	II – 26
III. Konfiguration des Servers und seiner Dienste	III – 1
III.1. USV	III – 9
III.1.1. Sinn und Zweck der USV	III – 9
III.1.2. Geeignete Modelle	III – 9
III.1.2.1. APC Smart-UPS SMX750i oder SMX1000i	III – 9
III.2. Backup	III – 13
III.2.1. Backup Konzept in LogoDIDACT	III – 13
III.2.1.1. Art und Ablauf der Sicherung	III – 14
III.2.1.2. Zeitplan für Sicherungen in LogoDIDACT	III – 14
III.2.1.3. Benachrichtigung über durchgeführte Sicherungen	III – 14
III.2.1.4. Dateien, die nicht gesichert werden	III – 15
III.2.1.5. Internet-Surfdaten aus dem Backup ausschließen	III – 16
III.2.1.6. Art und Anzahl der Sicherungen festlegen (Backup-Rotation)	III – 16
III.2.2. Backupfestplatte neu initialisieren	III – 16
III.2.3. "Hot-Plug" Sicherung über LD-USB-BAK	III – 18
III.2.3.1. USB-Platte für Hot-Plug neu einrichten	III – 18
III.2.3.2. Sicherung mit USB Hot-Plug durchführen	III – 18
III.2.3.3. USB Hot-Plug im Monitoring überwachen	III – 20
III.2.4. Sicherung des Auslieferungszustandes	III – 20
III.2.5. Technischer Ablauf des Backups und mögliche Probleme	III – 22
III.2.6. Backup auf NAS per iSCSI	III – 22
III.2.6.1. Separates Netzwerkinterface für NAS einrichten	III – 23
III.2.6.2. Das NAS-Gerät konfigurieren	III – 24
III.2.6.3. Sicherung auf NAS am Server einrichten	III – 40
III.2.7. Restauration im Fehlerfall	III – 43
III.2.7.1. Restauration im lauffähigen System	III – 43
III.2.7.2. Disaster Recovery - Notfallwiederherstellung	III – 43
III.3. Server und Systemdienste	III – 47
III.3.1. Netzwerk-Konfiguration am Server	III – 47
III.3.1.1. Physische Netzwerkzuordnung	III – 48
III.3.1.2. Externe IP-Adresse des Servers anpassen	III – 49
III.3.1.3. Interface extern auf DHCP stellen	III – 50

III.3.1.4. Interne IP-Adresse des ldhost anpassen	III – 50
III.3.1.5. Netzwerkbereich anpassen	III – 51
III.3.1.6. IP-Adresse des logosrv anpassen	III – 53
III.3.1.7. Trunks, Bonding und LACP	III – 54
III.3.1.8. Netzwerke und VLANs in LogoDIDACT 2.0	III – 56
III.3.2. Der Host und seine Container	III – 58
III.3.2.1. Befehle zum Verwalten der Container (LXC's)	III – 58
III.3.3. Konfigurations-Management mit Puppet	III – 60
III.3.3.1. Grundlagen zu Puppet	III – 61
III.3.3.2. Puppet Tools und Befehle	III – 62
III.3.3.3. logoDIACT 2.0 mit Puppet managen	III – 63
III.3.3.4. Container aufbauen	III – 68
III.3.3.5. Container löschen	III – 70
III.3.4. Aktivierung samba4-ad	III – 70
III.3.4.1. Samba 4 Domänennamen festlegen	III – 71
III.3.4.2. Samba 4 Domäne aufbauen (lassen)	III – 72
III.3.4.3. Samba 4 Administration und Tools	III – 73
III.3.5. Reverse-Proxy	III – 74
III.3.5.1. Vorbereitungen und Voraussetzungen	III – 75
III.3.5.2. Container rev-proxy aufbauen	III – 75
III.3.5.3. Den Reverse Proxy für Webdienste aktivieren	III – 76
III.3.5.4. Ports an den Reverse Proxy weiterleiten	III – 77
III.3.6. Zertifikate mit Let's Encrypt	III – 77
III.3.6.1. Digitale Zertifikate	III – 78
III.3.6.2. Let's encrypt aktivieren	III – 78
III.3.6.3. Zertifikat erstellen	III – 79
III.3.6.4. Zertifikat prüfen	III – 83
III.3.6.5. Zertifikate aktualisieren	III – 83
III.3.7. Verwendung eigener Zertifikate	III – 83
III.3.8. Interne Certification Authority (CA)	III – 84
III.3.9. Zugriff auf LDAP per SSL/TLS	III – 84
III.3.9.1. Port über Firewall an Rev-Proxy leiten	III – 85
III.3.9.2. Zertifikat für Rev-Proxy erstellen und prüfen	III – 85
III.3.9.3. Konfiguration für LDAP im Rev-Proxy	III – 86
III.3.9.4. LDAP von außen testen	III – 86
III.3.9.5. Den Zugriff auf LDAP in der Firewall absichern	III – 89
III.3.9.6. Konfiguration für Samba4-AD	III – 90
III.3.9.7. Spezielle LDAP-Benutzer und Attribute	III – 91
III.3.10. Virtuelle Maschinen mit KVM	III – 93
III.3.10.1. KVM am Server aktivieren	III – 94
III.3.10.2. Virtio Treiber installieren	III – 94
III.4. Konfiguration des logosrv	III – 95
III.4.1. Firewall	III – 95
III.4.1.1. Fernzugriff auf den Server	III – 95
III.4.1.2. Ports und Protokolle	III – 100
III.4.1.3. Sperren von Tor-Verbindungen	III – 102
III.4.2. Proxy-Server	III – 102
III.4.3. Webfilter	III – 103
III.4.3.1. Schlagwortfilter Schwellwert ändern	III – 103
III.4.3.2. Vorratsdatenspeicherung für Internetauswertung anpassen	III – 103
III.4.4. Drucker Einstellungen cups/pykota	III – 103
III.4.4.1. Bestätigung des Druckauftrags am Client deaktivieren	III – 103
III.4.4.2. Druckeragent bzw. Printagent Symbol am Client ausschalten	III – 104
III.4.5. DHCP-Optionen	III – 104

III.4.5.1. IP-Adress-Vergabe für fremde Rechner sperren	III – 104
III.4.5.2. Adressbereich für dynamische IPs anpassen	III – 104
III.4.6. DNS-Server	III – 105
III.4.6.1. Verbotene Namen	III – 105
III.4.6.2. DNS Rechnereintrag per wimport_data	III – 105
III.4.6.3. Dynamisches DNS	III – 106
III.4.7. Laufwerke und Zugriffsberechtigungen	III – 106
III.4.7.1. Zusätzliche Freigabe und Laufwerk einrichten	III – 106
III.4.7.2. Zugriffsberechtigung ACLs in LogoDIDACT	III – 107
III.4.7.3. Zugriff für Lehrer auf Schüler Homelaufwerke	III – 109
III.4.7.4. Lesender Zugriff der Lehrer auf Schüler-Homes	III – 109
III.4.7.5. Vollzugriff der Lehrer auf Schüler-Homes	III – 109
III.4.7.6. Vollzugriff der Lehrer auf Lehrer-Tausch	III – 110
III.4.7.7. Vollzugriff aller Benutzer auf Schulweiter Tausch	III – 110
III.4.7.8. Vollzugriff auf Klassen-Tauschlaufwerke	III – 111
III.4.7.9. Klassentauschlaufwerke deaktivieren	III – 112
III.4.7.10. Tauschlaufwerke zyklisch löschen	III – 112
III.4.7.11. Anpassung der Dateigröße beim Austeilen	III – 113
III.4.8. Cron-Jobs	III – 113
III.4.9. Befehle und Skripte am logosrv	III – 114
III.4.10. Apache Webserver	III – 115
III.4.10.1. Aktivierung interner Webseiten über public_html	III – 115
III.4.10.2. Schulinterne Homepage im Intranet aktivieren	III – 116
III.4.11. Rechte und Berechtigungen	III – 118
III.4.11.1. Zugriff auf Funktionen in der LogoDIDACT-Console ändern	III – 118
III.4.11.2. Gruppe Datenschutz und Verwaltung	III – 120
III.4.12. Benutzer und Kennwörter	III – 121
III.4.12.1. Benutzer	III – 121
III.4.12.2. Kennwörter	III – 124
III.4.13. Log-Dateien	III – 126
III.4.13.1. Rotieren und Komprimieren von Log-Dateien	III – 126
III.4.14. Radius-Server	III – 127
III.5. Softwareverteilung mit LD Deploy	III – 129
III.5.1. Vorteile von LD Deploy	III – 129
III.5.2. Voraussetzungen und Einschränkungen	III – 129
III.5.2.1. Voraussetzungen	III – 129
III.5.2.2. Einschränkungen	III – 130
III.5.2.3. Dringende Empfehlungen	III – 130
III.5.3. Parallelbetrieb von LD Deploy und Rembo/mySHN®	III – 130
III.5.3.1. Neuinstallationen nur mit LD Deploy	III – 130
III.5.3.2. Ergänzung bestehender Rembo-Installationen mit LD Deploy	III – 131
III.5.4. Installation von LD Deploy	III – 133
III.5.5. Freigegebene und Entwickler-Pakete	III – 134
III.5.5.1. Offizielle Pakete	III – 134
III.5.5.2. Entwickler-Pakete für Testzwecke	III – 135
III.5.6. Aktualisierung von LD Deploy Paketen	III – 136
III.5.7. Windows 10 bereitstellen	III – 137
III.5.7.1. Die richtige Windows 10 Variante bereitstellen	III – 138
III.5.7.2. Image importieren	III – 140
III.5.7.3. Import eines Images prüfen	III – 140
III.5.7.4. Torrent Infos	III – 142
III.5.8. Das Control Center starten	III – 143
III.5.9. Eine Windows 10 Umgebung erstellen	III – 144
III.5.9.1. Ein Betriebssystem erstellen	III – 145

III.5.9.2. Dem Betriebssystem ein Image zuordnen	III – 145
III.5.9.3. Konfiguration erstellen und Betriebssystem verknüpfen	III – 147
III.5.9.4. Den Domänenbeitritt konfigurieren	III – 149
III.5.9.5. Das Betriebssystem mit der Domäne verknüpfen	III – 150
III.5.9.6. Die Konfiguration mit der OU Computers verknüpfen	III – 152
III.5.10. Background Deployment	III – 153
III.5.10.1. Hintergrund-Verteilung in Windows 10	III – 153
III.5.10.2. Background Deployment aktivieren	III – 154
III.5.10.3. Verhalten an den Windows 10 Clients	III – 155
III.5.11. Synchronisation der Geräteliste wimport_data	III – 156
III.5.11.1. Automatischer Abgleich beim Anlegen oder Löschen	III – 156
III.5.11.2. Fehler in der Synchronisation zwischen Control Center und Geräteliste	III – 157
III.5.11.3. Fehler durch doppelten dhcpd Prozess im logosrv	III – 158
III.5.11.4. Manueller Abgleich der Geräteliste bei Namensänderung	III – 158
III.5.12. Client-Konfiguration mit AutoConf	III – 158
III.5.12.1. Vordefinierte Rollen für AutoConf	III – 158
III.5.12.2. Aktualisieren eines Playbooks	III – 159
III.5.13. Protokollierung mit graylog	III – 161
III.5.13.1. Installation Container graylog	III – 161
III.5.13.2. Webinterface von graylog	III – 162
III.6. Microsoft Produktaktivierung mit LD Deploy	III – 163
III.6.1. Neue Produktaktivierung in LogoDIDACT 2.0	III – 163
III.6.2. Grundlagen der Lizenzierung und Aktivierung	III – 164
III.6.2.1. Der Microsoft KMS (Key Management Service)	III – 164
III.6.2.2. Lizenzrecht und Lizenztechnik	III – 164
III.6.2.3. Der richtige Volumenlizenzvertrag für KMS	III – 165
III.6.3. Windows 10 KMS-Host mit LD Deploy aufsetzen	III – 167
III.6.3.1. Voraussetzungen	III – 167
III.6.3.2. Windows 10 Professional 1903 für KMS bereitstellen	III – 168
III.6.3.3. Eine win10kms Umgebung im Control-Center erstellen	III – 168
III.6.3.4. Die Datenträgerverwaltung starten	III – 170
III.6.3.5. Virtuelle Maschine win10kms im Control Center eintragen	III – 172
III.6.3.6. Virtuelle Maschine win10kms mit Konfiguration verknüpfen	III – 174
III.6.3.7. Virtuelle Maschine aktivieren	III – 175
III.6.3.8. Virtuelle Maschine starten	III – 176
III.6.3.9. Die wichtigsten virsh Befehle	III – 176
III.6.3.10. Aufbau der virtuellen Maschine per Virt-Viewer beobachten	III – 176
III.6.3.11. Tools installieren	III – 178
III.6.3.12. Windows 10 Key am KMS-Host eingeben und aktivieren	III – 180
III.6.3.13. Probleme mit KMS-Keys und mögliche Ursachen	III – 180
III.6.3.14. Office Volume License Pack installieren	III – 181
III.6.3.15. Office Key über Volumenaktivierungstool eingeben und aktivieren	III – 183
III.6.3.16. Office KMS-Key per Kommandozeile einspielen und aktivieren....	III – 186
III.6.3.17. KMS-Client-Emulator starten und Aktivierung prüfen	III – 187
III.6.3.18. Emulator wiederkehrend als Aufgabe ausführen	III – 189
III.6.4. Umgebung für Microsoft KMS konfigurieren	III – 192
III.6.4.1. DNS-Eintrag im logosrv erstellen	III – 192
III.6.4.2. Ports am KMS-Host öffnen	III – 192
III.6.4.3. GVLK am Windows Client eintragen	III – 193
III.6.4.4. Aktivierungsskript für Clients	III – 193
III.7. Unifi WLAN-Lösung	III – 195
III.7.1. Installation Container Unifi	III – 195

III.7.2. Unifi im Rev-Proxy freischalten	III – 196
III.7.3. Zertifikat für Unifi aktivieren	III – 197
III.7.4. Unifi Erstanmeldung	III – 197
III.7.5. Admin-Anmeldung und Spracheinstellung	III – 200
III.7.6. Unifi Konfiguration von Hostname und Mail	III – 201
III.7.7. SSH-Zugang für Unifi Access Points	III – 202
III.7.8. WLAN Konfiguration	III – 203
III.7.8.1. WLAN mit WPA2-Verschlüsselung	III – 203
III.7.8.2. WLAN für die Aufnahme von Tablets	III – 205
III.7.8.3. AccessPoints einbinden	III – 205
III.8. Tablet-Management mit LD Mobile	III – 207
III.8.1. Vorteile von LD Mobile	III – 207
III.8.2. Voraussetzungen für LD Mobile	III – 207
III.8.3. Installation der MariaDB-Datenbank	III – 208
III.8.4. Prüfung der Verzeichnisstruktur	III – 209
III.8.5. Festlegung von MariaDB als Datenbank	III – 210
III.8.6. Datenbank-Migration auf MariaDB 10.5	III – 210
III.8.7. Installation Container LD Mobile	III – 211
III.8.8. Router für Zugriff von außen konfigurieren	III – 212
III.8.9. LD Mobile im Rev-Proxy freischalten	III – 212
III.8.10. Zertifikat für LD Mobile aktivieren	III – 213
III.8.10.1. Zertifikat mit acme.sh beantragen	III – 213
III.8.10.2. Zertifikat mit acmetool beantragen	III – 214
III.8.11. Ports für Apple- und Google-Server freischalten	III – 214
III.8.12. Admin-Anmeldung in LD Mobile	III – 215
III.8.13. Lizenzen prüfen und anfordern	III – 216
III.8.14. Die LD Mobile APPs zuweisen	III – 217
III.8.15. Device Enrollment Program - DEP	III – 221
III.8.16. Anbindung an Apple DEP	III – 221
III.8.16.1. Serverzertifikat speichern	III – 222
III.8.16.2. Im Apple School Manager Portal anmelden	III – 223
III.8.16.3. MDM-Server hinzufügen und Zertifikat laden	III – 223
III.8.16.4. Server Token erzeugen	III – 225
III.8.16.5. Server-Token in LD Mobile laden	III – 226
III.8.17. Anbindung an Apple VPP	III – 228
III.8.18. Geräte im ASM zuweisen	III – 228
III.8.19. DEP-Geräte in LD Mobile synchronisieren	III – 229
III.8.20. DEP-Profil erstellen	III – 230
III.8.20.1. DEP-Profil für gemeinsam genutzte iPads	III – 230
III.8.21. Regelwerk anlegen	III – 231
III.8.22. Richtlinien anlegen	III – 232
III.8.22.1. WLAN-Richtlinie	III – 233
III.9. LogoDIDACT an Office 365 anknüpfen	III – 237
III.9.1. Office 365 Konfiguration	III – 237
III.9.1.1. Tenant und Domainname	III – 237
III.9.1.2. Eine neue Domäne anlegen	III – 239
III.9.1.3. Tenant und Domäne für Schulträger	III – 239
III.9.1.4. Das kostenfreie Office 365 A1 beantragen	III – 240
III.9.1.5. Ein administratives Konto anlegen	III – 244
III.9.1.6. Den Tenant mit der Domäne verbinden	III – 247
III.9.1.7. DNS-Konfiguration für weitere Dienste	III – 251
III.9.1.8. DNS-Server von Microsoft beim Provider eintragen	III – 254
III.9.1.9. Domäne als Standard festlegen	III – 259
III.9.2. Der LogoDIDACT Connector für Azure-AD	III – 260

III.9.2.1. Entwicklerpakete für Azure-AD einspielen	III – 260
III.9.2.2. Den Connector für Azure-AD installieren	III – 260
III.9.2.3. Den Connector für Azure-AD konfigurieren	III – 262
III.9.2.4. Eine APP in Azure-AD registrieren	III – 265
III.9.2.5. Einen geheimen Clientschlüssel in Azure-AD anlegen	III – 267
III.9.2.6. Der APP administrative Rechte zuweisen	III – 269
III.9.2.7. Connector an ID koppeln	III – 271
III.9.2.8. Benutzern im Control Center Office 365 Lizenzen zuweisen	III – 272
III.9.2.9. Benutzer zu Azure AD synchronisieren	III – 275
III.9.3. Das Kennwortportal SSP konfigurieren	III – 277
III.9.4. Die Zwei-Faktor-Sicherheit in Azure-AD deaktivieren	III – 279
III.9.5. Besprechungs-Richtlinien in Teams anpassen	III – 280
III.9.6. Richtlinien in Teams unberührt lassen	III – 283
III.9.7. Benutzer und Rechte anpassen	III – 283
III.9.7.1. Umgang mit bestehenden Benutzern in Azure	III – 283
III.9.7.2. Benutzern Admin-Rollen zuweisen	III – 284
III.9.7.3. Erstellen manueller Teams verbieten	III – 285
III.10. Nextcloud	III – 287
III.10.1. Voraussetzungen	III – 287
III.10.2. Die Container für Nextcloud und Collabora aktivieren	III – 288
III.10.3. Templates kopieren und anpassen	III – 289
III.10.4. Nextcloud im Rev-Proxy eintragen	III – 289
III.10.5. Zertifikate für Nextcloud und Collabora beantragen	III – 290
III.10.6. Zugriff auf Nextcloud erlauben	III – 291
III.10.7. Änderung des Objektspeichers	III – 292
III.10.7.1. Ankopplung an Samba4	III – 293
III.10.7.2. Umstellung auf Nextcloud files	III – 293
III.10.8. Deaktivierung von Plugins	III – 296
III.10.9. Update von Nextcloud über mehrere Versionen	III – 297
III.10.10. Konfiguration der Nextcloud für OnlyOffice anstelle Collabora	III – 298
III.11. Kopano	III – 303
III.11.1. Voraussetzungen	III – 303
III.11.2. Installation der Datenbank MariaDB 10.3	III – 303
III.11.3. Prüfung der Verzeichnisstruktur	III – 304
III.11.4. Festlegung von MariaDB 10.3 als Datenbank	III – 305
III.11.5. Datenbank-Migration auf MariaDB 10.3	III – 305
III.11.5.1. Voraussetzungen	III – 305
III.11.5.2. Größe der Kopano-Datenbank und freien Speicherplatz prüfen	III – 305
III.11.5.3. Kopano-Dienste anhalten	III – 306
III.11.5.4. Datenbank erstellen lassen	III – 306
III.11.5.5. Datenbank-Migration starten	III – 306
III.11.5.6. Kopano-Dienste wieder starten	III – 307
III.11.5.7. Alte Datenbanken im Container mysql56 löschen	III – 307
III.11.6. Installation Container Kopano	III – 307
III.11.7. Kopano im Rev-Proxy freischalten	III – 308
III.11.8. Zertifikat für Kopano aktivieren	III – 309
III.11.8.1. Zertifikat mit acme.sh beantragen	III – 309
IV. Installation der Arbeitsstationen	IV – 1
IV.1. Arbeitsstationen	IV – 5
IV.1.1. Vorbereiten und Testen der Arbeitsstationen	IV – 5
IV.1.1.1. Ändern der Bootreihenfolge auf Netzwerkbetrieb	IV – 5
IV.1.1.2. Umstellen der Netzwerkkarte auf Netzwerkbetrieb	IV – 6
IV.1.2. Die Rechneraufnahme mit LD Deploy	IV – 7
IV.1.3. Die Phasen in LD Deploy	IV – 7

IV.1.4. Musterarbeitsstation mit Windows 10	IV – 8
IV.1.4.1. Windows 10 Image Download	IV – 8
IV.1.4.2. Windows 10 Image Synchronisation	IV – 10
IV.1.4.3. Hardwareerkennung und Systemanpassungen	IV – 11
IV.1.4.4. Fehlersuche und Behebung	IV – 16
IV.1.4.5. Windows 10 Installation anpassen	IV – 17
IV.1.4.6. Windows 10 Updates installieren	IV – 20
IV.1.4.7. Windows 10 Image erstellen	IV – 20
IV.1.5. Treiber-Aktualisierung ohne Imageerstellung	IV – 24
IV.1.5.1. Treiber aktualisieren	IV – 25
IV.1.5.2. Treiber hochladen	IV – 25
IV.1.5.3. Treiber verteilen	IV – 27
IV.1.6. Tools für die Systemanpassung von Windows 10	IV – 27
IV.1.7. Systemanpassung in LD Deploy mit AutoConf	IV – 28
IV.1.7.1. Rollen, Playbooks und Phasen	IV – 28
IV.1.7.2. Installation von Tools zur Automatisierung per AutoConf	IV – 29
IV.1.7.3. Anpassung von Windows 10 mit LD Deploy	IV – 29
IV.1.7.4. Systemanpassungen für Windows 10	IV – 32
IV.1.7.5. Anpassungen mit AutoConf anwenden und testen	IV – 33
IV.1.7.6. Drucker	IV – 35
IV.1.7.7. SMART-Board Kalibrierung und Lizenzierung	IV – 46
IV.1.7.8. Promethean Board Konfiguration und Kalibrierung	IV – 53
IV.1.8. Funktionsupgrade von Windows 10	IV – 57
IV.1.8.1. Image-Konfiguration und Partition für das Funktionsupgrade	IV – 58
IV.1.8.2. Ansible-Konfiguration für das Funktionsupgrade	IV – 61
IV.1.8.3. Konfigurationen einem Rechner zuweisen	IV – 63
IV.1.8.4. Image neu einspielen und Anpassungen vornehmen	IV – 64
IV.1.8.5. Funktionsupgrade durchführen	IV – 64
IV.1.8.6. In Audit-Mode wechseln und Image erstellen	IV – 65
IV.1.9. Installation Office 2019	IV – 67
IV.1.9.1. XML-Datei erstellen	IV – 67
IV.1.9.2. Setup mit Optionen ausführen	IV – 68
IV.1.10. Linux am Client	IV – 68
IV.1.10.1. Konfiguration um Linux erweitern	IV – 69
IV.1.10.2. Linux Master-Installation durchführen	IV – 73
IV.1.10.3. Linux Image importieren und zuweisen	IV – 77
IV.1.10.4. Linux-Image am Client aufspielen	IV – 78
IV.2. LogoDIDACT-Agent und Console	IV – 79
IV.2.1. Installation unter Windows	IV – 80
V. Administration und Betrieb	V – 1
V.1. Anleitung LogoDIDACT-Console	V – 3
V.1.1. Benutzerverwaltung	V – 3
V.1.1.1. Anlegen neuer Benutzer über Listen	V – 3
V.1.1.2. Versetzen, Löschen und Anlegen beim Schuljahreswechsel	V – 8
V.1.1.3. Anlegen einzelner Benutzer	V – 12
V.1.1.4. Verwalten mehrerer Schularten	V – 17
V.1.1.5. VPN-Keys erzeugen und VPN-Zugang freischalten	V – 18
V.1.2. Raumsteuerung	V – 20
V.1.2.1. Rembo/mySHN® Funktionen	V – 20
V.1.3. Surfverhalten	V – 21
V.1.3.1. Auswertung der Internetzugriffe	V – 21
V.1.3.2. Statistische Auswertungen	V – 24
V.1.4. Service- und Support Modul	V – 25
V.1.4.1. Lehrer der Gruppe Support zuordnen	V – 25

V.1.4.2. Kontakte für externen Support anlegen	V – 26
V.1.4.3. Das Hauptfenster im Modul Service und Support	V – 27
V.1.4.4. Störungen bearbeiten, weiterleiten und abschließen	V – 28
V.2. Anleitung ITB Funktionen	V – 31
V.2.1. Server	V – 32
V.2.1.1. Dienste	V – 32
V.2.1.2. Geräteaufnahme	V – 32
V.2.1.3. Geräteliste	V – 34
V.2.1.4. Raumeinstellungen	V – 37
V.2.1.5. Rechneinstellungen	V – 38
V.2.1.6. Rechner zeitgesteuert herunterfahren	V – 39
V.2.1.7. Rechner zeitgesteuert aufwecken (Wake-On-LAN)	V – 41
V.2.2. Drucker	V – 42
V.2.2.1. Druckerzuordnungsliste	V – 42
V.2.2.2. Druckquota	V – 43
V.2.2.3. Druckkosten	V – 45
V.2.2.4. Druckauswertung	V – 46
V.2.3. Webfilter	V – 48
V.2.3.1. Kategorien	V – 48
V.2.3.2. Filterlisten	V – 49
V.2.4. Rembo/mySHN® Statistik und Images	V – 50
VI. Anwender	VI – 1
VI.1. Übersicht	VI – 5
VI.1.1. Selbstheilende Arbeitsstationen	VI – 5
VI.1.2. Benutzer, Rechte und Rollen	VI – 5
VI.1.3. Verzeichnisstruktur in LogoDIDACT	VI – 5
VI.1.3.1. Netzlaufwerke H:, T: und P:	VI – 5
VI.1.3.2. Verzeichnisstruktur und Ordneransicht der Schüler	VI – 6
VI.1.3.3. Verzeichnisstruktur und Ordneransicht der Lehrer	VI – 7
VI.1.3.4. Reduzierte Ansicht für Lehrer durch Eintrag in Klassen	VI – 7
VI.2. Anleitung LogoDIDACT-Console	VI – 11
VI.2.1. Schnelleinstieg	VI – 11
VI.2.1.1. Internet an/aus	VI – 11
VI.2.1.2. Bildschirme sperren	VI – 14
VI.2.2. Benutzeroberfläche	VI – 16
VI.2.3. Raumsteuerung	VI – 18
VI.2.3.1. Austeilen und Einsammeln von Dateien	VI – 20
VI.2.3.2. Bildschirmübertragung	VI – 23
VI.2.3.3. Klassenarbeitsmodus	VI – 25
VI.2.3.4. Didaktische Funktionen	VI – 33
VI.2.4. Benutzerverwaltung	VI – 34
VI.2.4.1. Die Möglichkeiten als Lehrer	VI – 35
VI.2.4.2. Erstellen der Benutzerkärtchen	VI – 35
VI.2.4.3. Bearbeiten der Kennwörter	VI – 38
VI.2.4.4. Kennwortrichtlinien in der LogoDIDACT-Console ändern	VI – 39
VI.2.4.5. Eigenes Kennwort ändern	VI – 39
VI.2.5. Service- und Support für Lehrer	VI – 40
VI.2.5.1. Problemstellung	VI – 40
VI.2.5.2. Die Lösung in der Übersicht	VI – 41
VI.2.5.3. Vorteile	VI – 41
VI.2.5.4. Anzeige von Störungen	VI – 41
VI.2.5.5. Das Hauptfenster im Ticketsystem	VI – 42
VI.2.5.6. Neue Störung per Assistent erfassen	VI – 43
VI.2.5.7. Störungen bearbeiten	VI – 47

VI.2.5.8. Störungen weiterleiten	VI – 47
VI.2.5.9. Störungen abschliessen	VI – 49
VI.3. Arbeiten von Zuhause aus	VI – 51
VI.3.1. Remote-Einwahl Vorbereitungen	VI – 51
VI.3.2. Installation auf Windows-Clients	VI – 51
VI.3.3. VPN-Einwahl	VI – 52
VI.3.3.1. VPN-Einwahl per graphischer Oberfläche mit OpenVPN GUI	VI – 52
VI.3.4. Die LogoDIDACT-Console über OpenVPN	VI – 54
VI.3.4.1. Start der LogoDIDACT-Console per VPN	VI – 54
VI.3.5. Zugriff auf Web-Dienste per OpenVPN	VI – 56
VI.3.6. Zugriff auf Dateien per VPN	VI – 56
VI.3.6.1. Verbindung von Netzlaufwerken mit GUILogon	VI – 56
VI.4. Microsoft 365	VI – 59
VI.4.1. LogoDIDACT-Ankopplung an Office 365	VI – 59
VI.4.1.1. Automatisierung mit LD Azure Connect	VI – 59
VI.4.1.2. Vorteile	VI – 59
VI.4.1.3. Was macht der Connector LD Azure Connect	VI – 60
VI.4.2. Anmelden an Office 365	VI – 60
VI.4.2.1. Keine Anmeldung bei zu einfachem und kurzem Kennwort	VI – 62
VI.4.2.2. Kennwort- Sicherheit und Komplexität	VI – 63
VI.4.2.3. Der LogoDIDACT-Server ist die Zentrale für Benutzer-Identitäten	VI – 64
VI.4.2.4. Empfohlene Kennwort-Komplexität	VI – 65
VI.4.2.5. Das SSP Portal zum Ändern des Kennwortes	VI – 66
VI.4.3. Der richtige Umgang mit Teams	VI – 68
VI.4.3.1. Besprechungs-Richtlinien	VI – 68
VI.5. Nextcloud	VI – 71
VI.5.1. Nextcloud in LogoDIDACT	VI – 71
VI.5.1.1. Zugriff auf Nextcloud	VI – 71
VI.5.1.2. Anmeldung und Voraussetzung	VI – 72
VI.5.1.3. Teilen von Dokumenten	VI – 72
VI.5.1.4. Arbeiten mit Nextcloud und Collabora	VI – 76
VI.6. Webdienste	VI – 77
VI.6.1. Content Management System	VI – 77
VI.6.1.1. Erste Schritte	VI – 77
VI.6.1.2. Ihre Vorteile	VI – 83
VI.6.2. Raumbuchungssystem	VI – 83
VI.6.2.1. Räume anlegen	VI – 84
VI.6.2.2. Zeitreservierungen erstellen	VI – 86
VI.6.3. Webmailer	VI – 89
VI.6.3.1. Die Roundcube Oberfläche	VI – 90
VI.6.3.2. E-Mail Nachricht verfassen	VI – 91
VI.6.4. Interne Webseiten	VI – 92
VI.6.4.1. Zugriff auf Webseiten über private_html und public_html	VI – 92
VI.6.5. Zugriff per Browser auf Dateien	VI – 92
Stichwortverzeichnis	S – 1
A. Kennworterfassungsbogen	A – 1
B. Schulverwaltungsprogramme	A – 1
B.1. SchILD-NRW für Nordrhein-Westfalen	A – 1
B.1.1. Anlegen eines Export-Filters	A – 1
B.1.2. Durchführen des Daten-Exports	A – 4
B.2. SCHULKARTEI für Baden-Württemberg	A – 8
B.2.1. Anlegen eines Export-Filters	A – 8
B.2.2. Durchführen des Daten-Exports	A – 8

Teil I. LogoDIDACT 2.0 Überblick

Kapitel I.1. LogoDIDACT 2.0

I.1.1. Überblick

Herzlichen Glückwunsch, dass Sie sich für LogoDIDACT 2.0 entschieden haben!

Mit LogoDIDACT 2.0 haben Sie die mit Abstand beste, umfangreichste und kostengünstigste Schulserverlösung zur Verfügung, die es am Markt gibt. Sie können damit sämtliche Aufgaben und Anforderungen sowohl im pädagogischen Bereich als auch in der Schulverwaltung abdecken.

Eine Schulserverlösung muss vielen Anforderungen genügen, die teilweise weit über das hinaus gehen, was man sich zunächst unter dem Begriff Schulserver vorstellt. LogoDIDACT ist in diesem Sinne auch nicht nur eine Serversoftware, sondern ein Gesamtkonzept, das sowohl die technischen als auch pädagogischen Anforderungen der Schulen erfüllen und darüber hinaus sämtliche Themen wie Service & Support, Softwarepflege und Weiterentwicklung umfasst.

Nicht nur die Schulen sondern auch Schulträger und Systemhäuser brauchen heute – mehr denn je – eine Komplettlösung aus einem Guß mit optimal aufeinander abgestimmten Modulen und einer kontinuierlichen Update-Technik, Support für das Gesamtpaket und einem Automatisierungsgrad der extrem viel Zeit und Kosten einspart.

Gleichzeitig muss die Schulserverlösung auch alle pädagogischen Anforderungen der Schulen erfüllt und auch ohne umfangreiche PC-Kenntnisse einfach bedienbar sein. Darüber hinaus muss die Schulserverlösung offen und ausbaufähig, sicher und in der Praxis bewährt sein. Nicht zuletzt muss die Lösung in der Anschaffung, Implementierung und Wartung kostengünstig sein. Alle diese Anforderungen und noch viele mehr erfüllt die LogoDIDACT Schulserverlösung.

I.1.1.1. Module und Bausteine

Wenn in LogoDIDACT von Modulen die Rede ist, dann nur, um einen Überblick zu haben über die vielen Bausteine der Lösung.

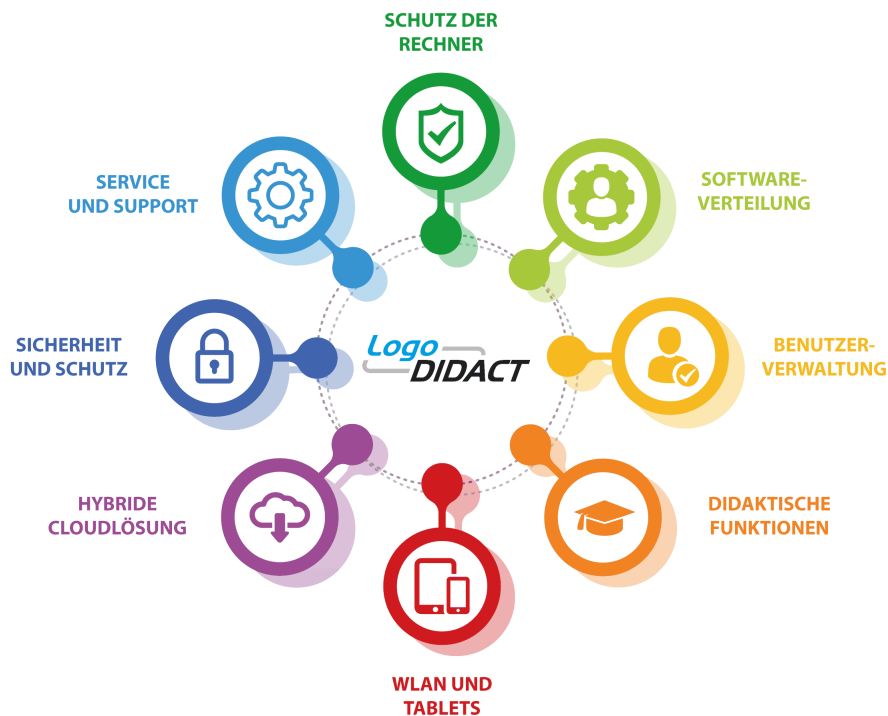


Abbildung I.1.1. Bausteine und Module des LogoDIDACT-Server

Die 8 Module des Schulservers lassen sich in drei Bereiche gliedern:

1. Systemmanagement

Hier geht es darum, dass die Computersysteme vor jeglicher Manipulation geschützt werden und bei jedem Neustart innerhalb von Sekunden wieder auf einem definierten und funktionsfähigen Zustand sind (= selbst heilende Arbeitsstationen). Ein noch viel wichtigeres Modul dieses Bereichs ist das Modul Softwareverteilung. Hier können Sie als Laie Software an nur einer Arbeitsstation installieren und dann einfach und kinderleicht auf alle ihre Computer verteilen. Ein weiteres Modul (Boot- und Partitionsmanagement) aus diesem Bereich ermöglicht es, dass mehrere Systeme auf den Arbeitsstationen nebeneinander betrieben werden können (z.B. Linux in Ergänzung zu Windows).

2. Benutzermanagement & Didaktische Funktionen

Die Funktionen und Module in diesem Bereich sollen ein komfortables und sicheres Unterrichten mittels der EDV ermöglichen und zwar derart, dass damit auch Lehrer ohne spezielles EDV-Fachwissen zu Recht kommen. Die zur Verfügung stehenden Funktionen reichen von einfachen Dingen, wie Internet ein- und ausschalten, über Drucker sperren bis hin zu Dateien austeilen und einsammeln. Jeder Benutzer hat auf dem Schulserver ein eigenes Verzeichnis (so genanntes Home-Verzeichnis) und einen eigenen Anmeldenamen. Es gibt Tauschverzeichnisse für Klassen oder Projektgruppen. Lehrer können selbstverständlich in die Tauschverzeichnisse und auch Homeverzeichnisse jedes Schülers schauen, während das umgekehrt natürlich nicht möglich ist.

Auch Themen wie das Arbeiten von zu Hause aus oder mit Notebooks und Tablets fallen in diesen Bereich, ebenso die künftige IdCloud-Lösung.

3. Sicherheit, Service & Support

Ein weiterer gewichtiger Bereich des Schulservers widmet sich dem Thema Serversicherheit, Service & Support. Auf dem Server wird täglich eine Datensicherung durchgeführt, ebenso gibt es verschiedene Virenscanner für Dateien und Mails, deren Signaturen teilweise stündlich aktualisiert werden. Wesentlich ist jedoch, dass diese Aufgaben und Dienste nicht nur automatisiert ablaufen, sondern die ITBs auch davon entlastet werden, sich um die Prüfung dieser Funktionen zu kümmern. Dies wird durch SBE oder LogoDIDACT Partner über die zusätzlichen Monitoringverträge sichergestellt.

I.1.1.2. Die Architektur der Version 2.0

Obwohl die Version 2.0 einen harten Wechsel vermuten lässt, soll sich dieser aus Endkundensicht als ebenso sanft und reibungsfrei darstellen, wie die Aktualisierungen der vergangenen Jahre seit Einführung von LogoDIDACT im März 2009. Rein technisch gesehen, unterscheidet sich die neue Version aber extrem von der bisherigen, weshalb auch die Version 2.0 gewählt wurde, um dies zu verdeutlichen. Zu einem großen Teil betrifft die Umstellung auf LogoDIDACT 2.0 den inneren Kern des Systems. Mit der Einführung der Virtualisierung wurde ein Modul geschaffen, das Weiterentwicklungen erheblich einfacher macht und die Flexibilität nochmals steigert.

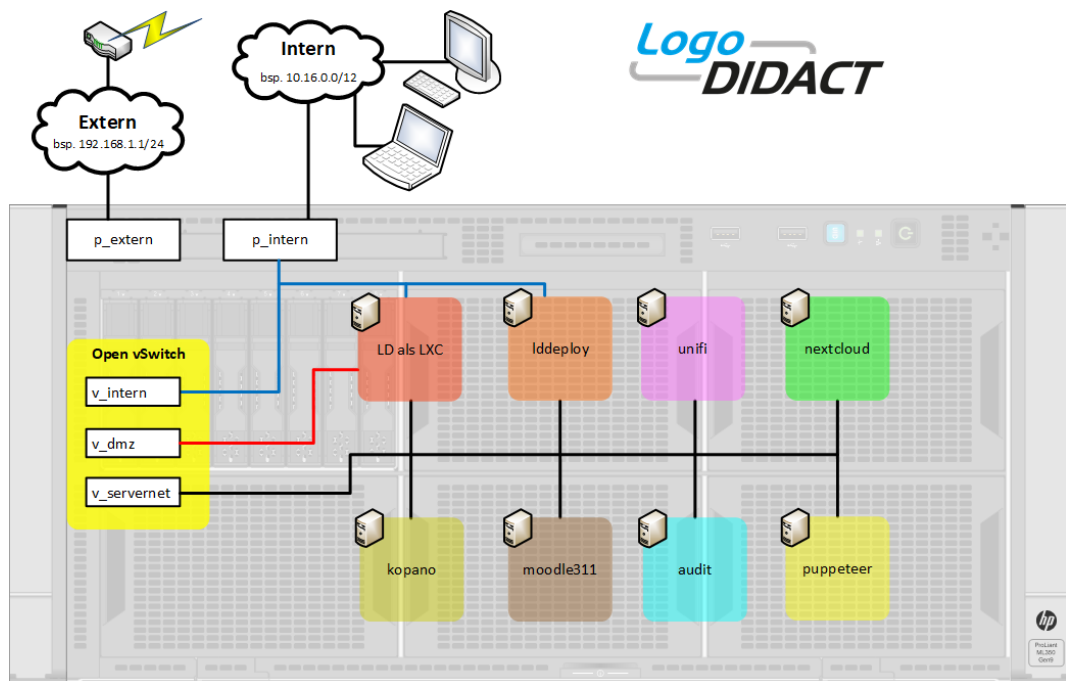


Abbildung I.1.2. Der Aufbau von LogoDIDACT 2.0 mit "schlankem" Host und Container-Virtualisierung

Das zentrale Basissystem bildet ein Ubuntu LTS (Long Term Support), für das Aktualisierungen und Support jeweils für 5 Jahre ab Versionsdatum gewährleistet sind. Wie anhand der Grafik Abbildung I.1.2, „Der Aufbau von LogoDIDACT 2.0 mit "schlankem" Host und Container-Virtualisierung“ erkennbar, wurde der gesamte bisherige LogoDIDACT-Server ebenfalls in einen Container ausgelagert ("LD als LXC").

Neben den verschiedenen Containern bietet ein virtueller Switch (Open vSwitch) zusätzliche Flexibilität und Möglichkeiten bei der Verteilung über mehrere physikalische Server. Zu den vielen Neuerungen gehört auch ein komplett überarbeitetes System- und Konfigurationsmanagement auf Basis von Puppet. Damit lassen sich die verschiedenen Container von zentraler Stelle aus (Container puppeteer) verwalten und Parameter verteilen und anpassen.

Mit der Umstellung auf LogoDIDACT 2.0 blieb es aber nicht bei der inneren Erneuerung des Servers. Die Aufteilung in Container ermöglicht auch praktische Neuerungen, die für Schulen sofort erkennbar und nutzbar sind. Dank dieser Aufteilung gibt es inzwischen auf die neue Version 3.11 der beliebten Lernplattform Moodle (Container moodle311) und auch ein aktuelles Modul für den webbasierten Zugriff auf Daten für Tablets und andere mobile Geräte (Container nextcloud).

Bereits Anfang 2016 eingeführt wurde ein so genannter WLAN-Controller (Container unifi), mit dem eine Lösung für das Management mobiler Geräte bereitsteht. Mit dem Softwarecontroller und speziellen Access Points bietet LogoDIDACT auch in diesem Bereich eine kostengünstige Lösung, die eine automatische Lastverteilung leistet. Entscheidend dabei ist, dass es sich um eine lokale Lösung handelt und nicht um eine Cloud-Lösung oder einen Hardwarecontroller.

Das neue Modul audit im gleichnamigen Container, bietet eine ähnliche Auswertung, wie beim Surfverhalten, nur eben für Geräte, d.h. darüber lässt sich feststellen wer sich zu welcher Zeit an welchem System an- oder abgemeldet hat.

I.1.1.2.1. Vorteile der Virtualisierung auf Basis von LXC

Mit der Einführung der Virtualisierung des LogoDIDACT Servers wurde bereits im Jahr 2013 begonnen und es ging dabei zunächst ganz konkret um die Beseitigung von Problemen beim Update ver-

schiedener Bausteine. So lässt sich beispielsweise die Lernplattform Moodle und die Groupware Zarafa in LogoDIDACT 1.0 nicht unabhängig voneinander auf den aktuellsten Stand updaten, weil beide Systeme jeweils zwingend eine bestimmte PHP-Version benötigen, auf die sie bisher gleichzeitig zugreifen. Um derlei Probleme zu lösen, wurden verschieden Virtualisierungstechnologien geprüft. Die Entscheidung fiel dabei auf LXC (LinuX Containers), wobei es sich dabei weniger um richtige virtuelle Maschinen als vielmehr um virtuelle Umgebungen handelt. Im Gegensatz zu richtigen virtuellen Maschinen, bietet der Ansatz über LXC jedoch sehr viele Vorteile:

1. Isolierung von Anwendungen, Prozessen und Ressourcen
2. Nutzung gleicher Ressourcen (Kernel, Bibliotheken..) trotz Isolierung
3. Deutlich weniger Overhead als bei echten virtuellen Maschinen
4. LogoDIDACT mit LXC bleibt lauffähig auf „richtiger“ VM
5. Lastverteilung (Trennung über LXC ermöglicht physikalische Trennung)

Aus diesem Ansatz der Applikationsvirtualisierung heraus entstand im Laufe der letzten zwei Jahre eine tiefgreifende Änderung in der Architektur des gesamten Systems und daraus die Version LogoDIDACT 2.0.

I.1.1.3. Software und Lizenzierung

In diesem Kapitel finden Sie einen groben Überblick über die wichtigsten Softwarekomponenten, die mit dem Server ausgeliefert werden und Angaben zur Lizenzierung von optionalen Komponenten.

I.1.1.3.1. Die LogoDIDACT Distribution

Der LogoDIDACT-Server ist keine Software, die auf einem bestehenden Betriebssystem installiert wird, sondern bildet eine eigene, unabhängige und in sich geschlossene Distribution mit Paketserver und verschiedenen Repositories.

I.1.1.3.2. Softwarepakete

Die einzelnen Softwarepakete hier alle mit Namen, Beschreibung und Versionsangaben aufzuführen, macht bei einer auf Linux basierenden Distribution wie sie LogoDIDACT darstellt wenig Sinn. Zum Einen würde eine solche Liste den Rahmen der Dokumentation sprengen und zum Zweiten sind die Versionen einzelner Softwarekomponenten aufgrund der Weiterentwicklung und Softwarepflege ständigen Änderungen unterworfen.

Die durchgängige Weiterentwicklung des gesamten Servers und damit der nahezu 700 Softwarepakete ist auch Sinn und Zweck des Gesamtkonzeptes mit LogoDIDACT

Bis auf die Lizenzierung der LogoDIDACT Server- und Clientlizenzen sind alle weiteren Bausteine und Softwarekomponenten kostenfrei.



Anmerkung

Eine Liste der am Server aktuell installierten Dienste mit Versionsangabe und Kurzbeschreibung erhält man durch folgenden Befehl am Server:

```
dpkg -l
```

Nach einer Standardinstallation sind dies im LogoDIDACT-Server derzeit nahezu 700 Pakete (Stand 10/2017).

In der nachfolgenden Tabelle erfolgt eine unvollständige Auflistung einiger wichtiger Softwareprodukte mit Versionsangabe (Stand 4/2019):

Tabelle I.1.1. Unvollständige Auflistung einiger Softwarekomponenten in LogoDIDACT

Komponenten	Version	Beschreibung
Hostsystem	Ubuntu 16.04 LTS	Das Basissystem innerhalb dessen die virtuellen Maschinen in LXC's (Linux Container) laufen.
Linux-Kernel	v4.15 (vom 28. Jan. 2018)	Die aktuelle Kernelversion lässt sich am Server mit <code>uname -a</code> ermitteln.
Iddeploy	Iddeploy-agent 44, control-center 24, control-service 28 (April 2019)	Software zum Verteilen von Images und neuen Softwarepaketen.
Puppet	1.1.40	System-Management zur Automatisierung der Verwaltung des Hosts und aller Container
postgresql	10.7	Datenbankserver
samba	4.3.11	SMB Datei/Druck/Anmelde-Server (emuliert Windows-Server)
nginx	1.10.3	Reverse-Proxy
ldap	2.4.9	Open LDAP-Server (Lightweight Directory Access Protocol)

I.1.1.4. Empfohlene Peripherie

In den folgenden Abschnitten wird aufgeführt, welche Rolle der LogoDIDACT-Server im Netzwerk einnimmt und welche Empfehlungen es hinsichtlich des Einsatzes zusätzlicher Geräte gibt.

Dabei hat sich die Konstellation mit Server, Router, USV und weiteren Bestandteilen wie Backupsystemen und einem Kabelkonzept in der Praxis an mehr als 1000 LogoDIDACT Schulen über viele Jahre hin bewährt.

I.1.1.4.1. Mindestanforderungen an die Server-Hardware

Die Dimensionierung der Serverhardware für den LogoDIDACT-Server 2.0 hängt entscheidend von der Größe des Netzwerkes bzw. der Anzahl angeschlossener Arbeitsstationen ab.

Bei der Dimensionierung der Hardware sollte man auch unbedingt berücksichtigen, dass der Server die zentrale Komponente im System darstellt und in der Regel für fünf Jahre rund um die Uhr zuverlässig und ohne Unterbrechung sämtliche Dienste im Netzwerk bereitstellen muss, damit die "digitale Bildung" an der Schule überhaupt gelingen kann. Die meisten Systemhäuser und Behörden haben inzwischen verstanden, dass "die Cloud" den Großteil der Anforderungen vor Ort nicht löst und auch keine Lösungen für den reibungslosen IT-Betrieb der dezentralen Strukturen bietet.

Unabhängig davon, ob die Serverleistung im Rechenzentrum oder durch einen dezentralen Server vor Ort erbracht wird, hat die Bedeutung des Servers und damit auch seiner Dimensionierung deutlich zugenommen. Die Anforderungen an die Sicherheit und Verfügbarkeit sind ebenso gestiegen, wie an die Funktionalität.

In dieser Hinsicht gibt es auch in LogoDIDACT-Server 2.0 viele neue Module und Bausteine, welche die Schulen gerne einsetzen wollen, so dass auch die Mindestanforderungen stetig steigen.

Mindestanforderungen:

- Prozessor mit 8 echten Kernen
- 32 GB Arbeitsspeicher
- 1.2 TB Festplattenkapazität (SAS-Platten min. 10k)
- RAID-Controller mit 2 GB WriteCache
- 2 Netzwerkschnittstellen (min. Gigabit)

Komponente:	Art:	Plattenplatz:	RAM-Bedarf:	CPU:
ldhost	verbindlich			2
logosrv	verbindlich			1
puppet	verbindlich			1
samba4-ad	verbindlich			1
ca-g1	verbindlich			1
rev-proxy	verbindlich (Webdienste)			1
deploy-g1 (lddeploy)	verbindlich			1
ctrl-g1 (lddeploy)	verbindlich			1
postgresql10 (lddeploy)	verbindlich			1
graylog-g1 (lddeploy)	verbindlich			1
nexus-g1 (lddeploy)	verbindlich			1
win10kms (KVM)	empfohlen			2
unifi	optional			1
nextcloud	optional			1
collabora	optional			1
mysql56 (ldmobile)	optional / veraltet			1
ldmobile	optional			1
mariadb105 (ldmobile)	optional (ersetzt mysql56)			1
kopano-g1	optional			2
pydio	abgekündigt / veraltet			1
xibo	abgekündigt / veraltet			1
rembo5	abgekündigt / veraltet			1
moodle 3.0	veraltet			1
moodle 3.11	optional			1

Grundsätzlich sollte der Server ein Gerät sein, das auch tatsächlich für den Serverbetrieb geeignet ist, d.h. bei dem Mainboard, Festplatten, Netzteil und andere Komponenten (wie ECC-RAM) speziell für Server und den Dauerbetrieb ausgelegt sind. Empfohlen ist ebenfalls der Einsatz eines richtigen RAID-Controllers (kein Fake-RAID) und damit einhergehend ein redundantes System aus mindestens zwei Festplatten (RAID-1).

Weitere Informationen zu empfohlener Serverhardware finden Sie in den FAQs zu LogoDIDACT.

I.1.1.4.2. Kabelkonzept

Auch wenn einem auf den ersten Blick so etwas wie ein Kabelkonzept mit einer Farbgestaltung seltsam erscheinen mag, hat dies in der Praxis viele Vorteile. Für die Bearbeitung von Störungen per telefonischer Hotline hat sich diese klare Festlegung von farbigen Kabeln zwischen Server, Switch, Router, DSL-Modem oder Splitter bei Schulen bestens bewährt.

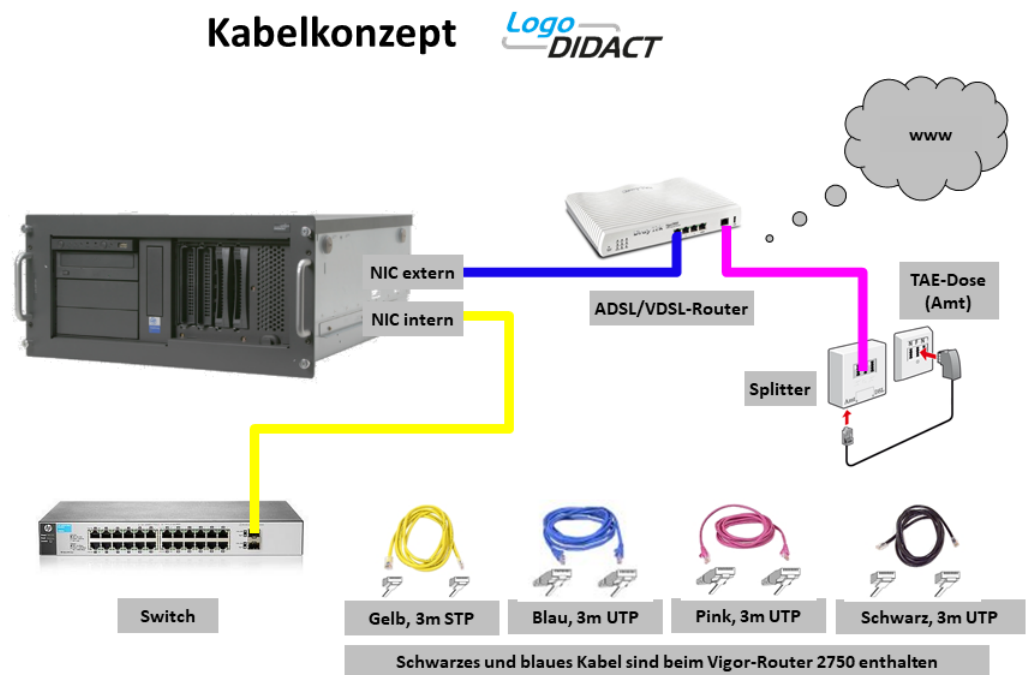


Abbildung I.1.3. Der LogoDIDACT-Server und die empfohlene Peripherie

I.1.1.4.3. Unterbrechungsfreie Stromversorgung USV

Selbstverständlich gehört zu jedem vernünftigen Serversystem eine unterbrechungsfreie Stromversorgung (kurz USV bzw. im englischen UPS = uninterruptable power supply). Dieses Gerät hat im wesentlichen zwei Aufgaben. Zum Einen schützt es den Server vor kurzfristigen Überspannungen und Stromschwankungen und zum Zweiten lässt sich der Server bei längerem Stromausfall geregelt herunterfahren.

Teil II. Installation des Servers

Inhaltsverzeichnis

II.1. LogoDIDACT-Server-Installation	II – 5
II.1.1. Vor der Installation	II – 5
II.1.2. Upgrade auf LogoDIDACT 2.0	II – 5
II.1.2.1. Upgrade auf Ubuntu 16.04	II – 6
II.1.2.2. Umstellung der Netzwerkkonfiguration auf systemd	II – 8
II.1.3. Neuinstallation	II – 9
II.1.3.1. Voraussetzungen	II – 10
II.1.3.2. Basisinstallation	II – 10
II.1.3.3. Systemaufbau durch Puppet	II – 22
II.1.3.4. LogoDIDACT Update	II – 24
II.1.3.5. Aktualisierung des Open vSwitch	II – 25
II.1.3.6. Änderung des root-Kennwortes	II – 26

Kapitel II.1. LogoDIDACT-Server-Installation

II.1.1. Vor der Installation

II.1.1.1. Aufbau des Netzwerks

Bitte überlegen Sie sich im Vorfeld schon den grundsätzlichen Aufbau Ihres Netzwerks.

Um die Migration von einem bereits bestehenden System hin zu LogoDIDACT möglichst einfach zu gestalten, wäre es am einfachsten, dieselben Netzwerkeinstellungen weiterzuverwenden, damit Geräte wie Printserver oder Router nicht neu konfiguriert werden müssen.

Nicht selten zeigt sich jedoch auch, dass bestehende Netzwerkstrukturen ihrem Namen nicht gerecht werden und eher strukturlos wirken oder, wie oft bei 192.168er Netzwerken der Fall, schnell an ihre Grenzen stoßen. Hier sollte dann ein Schlußstrich gezogen und eine neue Struktur gebildet werden, die übersichtlich aufgebaut und flexibel ist und zudem ausreichend Platz für zukünftiges Wachstum bietet. Bewährt hat sich hier ein Netz im privaten 10er Bereich, z.B. 10.16.0.0 mit Netzmaske 255.240.0.0

Das dritte Oktett bietet dann beispielsweise die Möglichkeit, eine Raumnummer unterzubringen und das vierte Oktett eine Rechnernummer. Bei größeren Netzen lassen sich durch Öffnung der Netzmaske auch weitere Informationen, wie z.B. eine Gebäudenummer, mit einbeziehen. Beispiele:

```
1. Schüler PC in Raum 215: 10.16.215.1
16. Schüler PC in Raum 215: 10.16.215.16
    Lehrer PC in Raum 215: 10.16.215.101
    Drucker 1 in Raum 215: 10.16.215.201
    Drucker 2 in Raum 215: 10.16.215.202
```

Die Voreinstellung bei der Installation ist das Netz 10.16.0.0/255.240.0.0. Sofern machbar, sollte man diese Vorgaben verwenden, weil sich diese in der Praxis bei Tausenden Installationen bewährt haben und es viele Vorteile gibt. Eine Ausnahme ist der Betrieb des LogoDIDACT Servers in einer Umgebung, bei der das externe Netzwerk selbst den 10erIP-Bereich belegt. Das ist z.B. konkret der Fall, wenn der LogoDIDACT Server an einer Baden-Württemberger Schule im Verwaltungsnetzwerk an das so genannte KISS-Netz (**K**ommunikations-**I**nfrastruktur zwischen **S**chulen und **S**chulverwaltung) angeschlossen wird. Dieses öffentliche Netz der Schulbehörde in Baden-Württemberg ist selbst ein 10er Netz, weshalb in diesem Fall der LogoDIDACT Server dann in das private 172er Netz gelegt wird (IP des logosrv 172.16.1.1 mit Subnetzmaske 255.240.0.0).

II.1.2. Upgrade auf LogoDIDACT 2.0

Seit Januar 2016 ist das Upgrade der Version LogoDIDACT auf LogoDIDACT-Server 2.0 verfügbar. Ausführliche Informationen und Unterlagen wie eine Liste der häufig gestellten Fragen und Antworten (FAQ) sowie Videos und PDFs zur Umstellung finden sich auf der Homepage (Anmeldung/Login erforderlich) unter:

<https://portal.sbe.de/support/logodidact-2-0/>.

Das Upgrade auf 2.0 mündet in einem entsprechend alten Stand, der noch auf Ubuntu 14.04 basiert. Ebenfalls auf einem alten Versionsstand befindet sich Puppet zum Systemmanagement. Deshalb ist es wichtig, diese Komponenten zunächst auf einen aktuellen Stand zu bringen.

Möglicherweise ist es einfacher bei einem so veralteten System nur die Nutzerdaten zu sichern und das System über eine Neuinstallation gegebenenfalls auf neue Hardware aufzusetzen und dann die Daten der Benutzer wieder zurückzuspielen.

Falls man doch den Weg des Upgrades gehen will oder muss, sind hier stichpunktartig die durchzuführenden Arbeiten aufgeführt:

- Puppet Update auf Version 0.79 (durch `ldupdate` im `puppeteer`)
- Puppet Update auf Version 0.9.79 (durch `ldupdate` im `puppeteer`)
- Puppet Upgrade auf Version 1.0.x (durch `puppet-10-upgrade` im `puppeteer`)
- Installation systemkritischer Aktualisierungen (durch `upgrade-retained-packages` im `ldhost`)
- Upgrade auf Ubuntu 16.04 (durch `ld-do-release-upgrade-from-1404-to-1604` im `ldhost`)
- Umstellung der Netzwerkkonfiguration auf `systemd`



Anmerkung

Wenden Sie sich bei Fragen zur Umstellung an Ihren zertifizierten LogoDIDACT-Partner

II.1.2.1. Upgrade auf Ubuntu 16.04

Um das Upgrade auf Ubuntu 16.04 durchzuführen ist mindestens ein auf Puppet 1.0.70 aktualisierter LogoDIDACT 2.0 Server Voraussetzung. Mit dem Rezeptstand Puppet 1.0.75 wird auf die Verfügbarkeit des Upgrades hingewiesen und ebenso, wie Sie dieses durchführen.

```

Welcome to...

LogoDIDACT 2.0
ldhost.schule.local physical

Server : musterstadt-gym / Musterschule Musterstadt
Load   : 0.97 / 0.30 / 0.10
Puppet : 2017-10-08/11:21 R:727 C:191
LXC    : logosrv/puppeteer/rembo5

1. You can update 23 package(s) by running "ldupdate" in puppeteer
2. Upgrade to Ubuntu 16.04 LTS (xenial) can be started by running ld-do-release-upgrade-from-1404-to-1604.
    
```

Geben Sie im `ldhost` dazu den folgenden Befehl ein:

`ld-do-release-upgrade-from-1404-to-1604`

```

musterstadt-gym / physical / 14:49 / 1.0.74 / ssh@10.31.255.254
root@ldhost:~# ld-do-release-upgrade-from-1404-to-1604
#####
#                               #
#                               #
#####
Sie haben die Aktualisierung Ihres logoDIDACT 2.0 Servers auf die Ubuntu 16.04
LTS Basis gestartet.

Im Rahmen der Aktualisierung muss der Server neu gestartet werden. Auch werden
zuvor alle Dienste gestoppt.
Die Aktualisierung wird längere Zeit (meist mehr als eine Stunde) dauern.

Beachten Sie die etwaige Hinweise in der Knowledge Base für logoDIDACT 2.0
(https://sbe.de/knowledge-base/)

Soll dieser Vorgang fortgesetzt werden? (Ja/Nein) [Nein]
    
```

Bitte beachten Sie die Hinweise zur Dauer der Umstellung (ca. 1 Stunde) und bestätigen Sie durch Eingabe von **Ja**. Sofern Sie kein aktuelles Backup haben, das nicht älter als 5 Stunden alt ist, erhalten Sie eine Fehlermeldung und das Upgrade auf 16.04 wird nicht durchgeführt.

```
I: 14:51:20 => `gem install inifile --no-rdoc --no-user-install`
I: 14:51:21 => |- Successfully installed inifile-3.0.0
I: 14:51:21 => |- 1 gem installed
I: 14:51:21 => |- Installing ri documentation for inifile-3.0.0...
I: 14:51:21 => `gem install versionomy --no-rdoc --no-user-install`
I: 14:51:26 => |- Successfully installed blockenspiel-0.5.0
I: 14:51:26 => |- Successfully installed versionomy-0.5.0
I: 14:51:26 => |- 2 gems installed
I: 14:51:26 => |- Installing ri documentation for blockenspiel-0.5.0...
I: 14:51:26 => |- Installing ri documentation for versionomy-0.5.0...
E: 14:51:26 => Da das letzte gefundene Backup nicht den Umstellungsanforderungen
entspricht (entweder fehlerhaft oder bereits älter als 5 Stunden), wird die Ums
tellung abgebrochen. Erstellen Sie ein Backup Ihres Systems und führen Sie danac
h den Vorgang erneut aus.

musterstadt-gym / physical / 14:51 / 1.0.74 / ssh@10.31.255.254
root@ldhost:~#
```

Falls Sie das Upgrade auf Ubuntu 16.04 in einer bereits laufenden produktiven Umgebung durchfüh- ren, sollten Sie nun unbedingt eine aktuelles Backup erstellen, um im Falle eines Fehlers wieder auf den alten Stand zurückkommen zu können.

Bei einer Neuinstallation hingegen, können Sie die Abfrage nach dem Backup als Voraussetzung deaktivieren. Im Falle eines Fehlers müssen Sie dann allerdings die gesamte Installation inkl. Upda- tes von Neuem beginnen. Öffnen Sie zur Deaktivierung der Backupprüfung mit einem Editor Ihrer Wahl (z.B. nano) die Datei `/etc/ld-upgrade/settings.yaml`. Ändern Sie dort im Abschnitt `backup` den Wert von `true` auf `false`.

```
---
check:
  backup:
    ensure: true
    age_in_h: 5
  dpkg_lock:
    ensure: true
  hostname:
    ensure: true
    value: ldhost
  ld_puppet:
    ensure: true
    version: 1.0.70
```

Starten Sie das Upgrade erneut durch Eingabe von

`ld-do-release-upgrade-from-1404-to-1604`

Im Laufe des Upgrades werden alle Dienste gestoppt und am Ende erfolgt ein automatischer Reboot des Servers.



Achtung

Nach dem Neustart erfolgt der eigentliche Umbau bzw. das Upgrade auf Ubuntu 16.04 LTS. Dieser Vorgang wird von Puppet **vollkommen automatisch** durchgeführt und darf nicht unterbrochen werden.

Melden Sie sich nach etwa 45-60 Minuten wieder am Server an. An der Begrüßung unmittelbar nach dem Login ist an oberster Stelle dann erkennbar, ob bzw. dass der Server auf Ubuntu 16.04 umgestellt wurde.


```
[Match]
MACAddress=98:f2:b3:e6:25:db
[Link]
Name=p_intern
```

Sofern weitere physische Schnittstellen vorhanden sind, können Sie diese nach dem gleichen Schema definieren, auch wenn Sie diese noch nicht verwenden.

Damit Änderungen am Namen übernommen werden, ist es wichtig, den folgenden Befehl auszuführen, damit das initramfs-Image neu aufgebaut wird, in welchem die Schnittstellen in Ubuntu 16.04 oder höher festgelegt sind.

update-initramfs -u



Achtung

Wenn Sie Änderungen an der Zuordnung von Netzwerkschnittstellen vornehmen, müssen Sie danach den Server **ldhost** neu starten.

II.1.3. Neuinstallation

Die Neuinstallation des LogoDIDACT-Servers ist über die SBE-Toolbox DVD möglich. Die DVD liegt als ISO-Datei im Downloadbereich der SBE-Homepage:

<https://portal.sbe.de/support/downloads/>

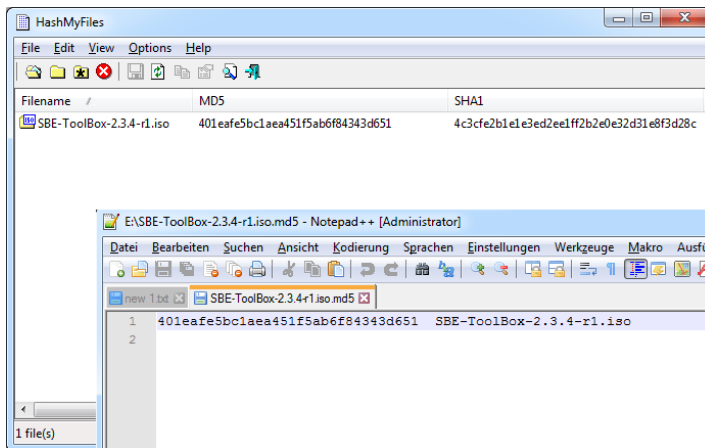
Bitte verwenden Sie immer die aktuellste Version. Die ToolBox-DVD beinhaltet zahlreiche SBE-Tools sowohl für Support und Diagnosezwecke als auch zum Management von virtuellen Maschinen und nicht zuletzt zur Installation von LogoDIDACT 2.0.



Achtung

Verwenden Sie bitte ausschließlich die DVD zur Installation und keine Variante für USB-Stick, da nur der auf der DVD enthaltene Installer den UEFI-Modus am Server unterstützt.

Prüfen Sie die heruntergeladene ISO-Datei in jedem Fall über die ebenfalls im Download bereitgestellte MD5-Prüfsummendatei. Verwenden Sie dazu ein Tool, wie z.B. HashMyFiles (https://www.nirsoft.net/utils/hash_my_files.html), um die Prüfsumme über die ISO-Datei zu bilden und einen Text-Editor (z.B. Notepad++) um die Prüfsumme zu vergleichen.



II.1.3.1. Voraussetzungen

Für LogoDIDACT benötigen Sie zwei Key-Dateien `logodidact.key` und `myshn.key`, die das Produkt für Testzwecke oder dauerhaft freischalten.

Kopieren Sie die Dateien direkt auf einen USB-Stick (ohne Unterordner), den Sie für die Installation bereithalten. Ohne einen gültigen LogoDIDACT-Key kann die Installation nicht durchgeführt werden.

Grundlegend notwendig ist auch ein barrierefreier Zugang zum Internet. Wir empfehlen dringend die Konstellation zu verwenden, wie sie in LogoDIDACT als grundlegende Konzept vorgesehen. Dabei hängt am externen Netzwerk-Interface des Servers ein entsprechender Router zumeist mit integriertem Modem für den jeweiligen physikalischen Zugang des Providers (DSL, VDSL, UMTS, LTE, Kabel). Diese Konstellation ist im Abschnitt I.1.1.4, „Empfohlene Peripherie“ näher beschrieben und hat sich bei tausenden LogoDIDACT Installationen bewährt.

II.1.3.2. Basisinstallation

II.1.3.2.1. Schritt 1: Ändern der Bootreihenfolge am Server

Abhängig vom BIOS Ihres Servers müssen Sie dort eventuell die Startreihenfolge so abändern, dass das DVD-ROM Laufwerk als erstes sogenanntes Boot Device aufgeführt wird. Sofern der Server den UEFI-Modus unterstützt, sollten Sie diesen aktivieren bzw. verwenden. Der UEFI-Mode ist z.B. zwingend erforderlich, wenn am Server mehr als 2 TB Plattenplatz vorhanden sind.



Tipp

In das BIOS-Setup gelangt man häufig über die Taste **Entf**, **F2**, **F8** oder **F10** während des Bootvorgangs.



Achtung

Falls der Server über kein integriertes DVD-Laufwerk verfügt und Sie ein externes DVD-Laufwerk verwenden müssen, schließen Sie dieses unbedingt nur an einem USB 2.0 Port an. Falls der Server nur über USB 3 Ports verfügt, stellen Sie im BIOS den Port auf USB 2-Kompatibilität um.

Installieren Sie auf **keinen Fall** über einen USB 3 Port ohne Anpassung, da die Installation in 90% der Fälle an irgendeiner Stelle abbricht.

II.1.3.2.2. Schritt 2: Start von DVD

Abhängig davon, ob der Server UEFI unterstützt oder nicht, ergibt sich beim Boot von DVD ein etwas anderes Bild. Im normalen Legacy-Boot ist der Hintergrund blau und die Texteinträge grau.

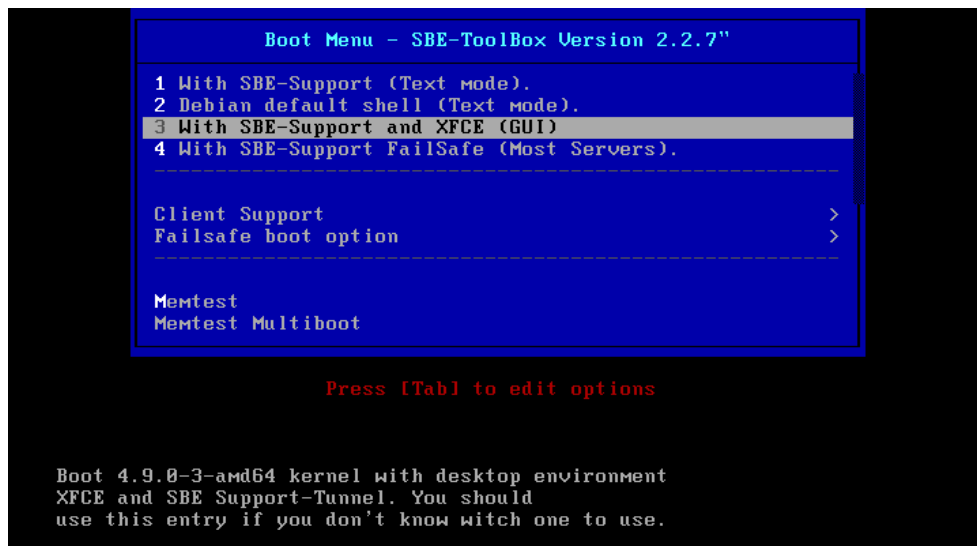


Abbildung II.1.1. LogoDIDACT Auswahlmenü bei Legacy-Boot

Im UEFI-Mode hingegen ist die Hintergrundfarbe schwarz und die Textfarbe weiß. Die Menüeinträge sind in beiden Fällen jedoch gleich.

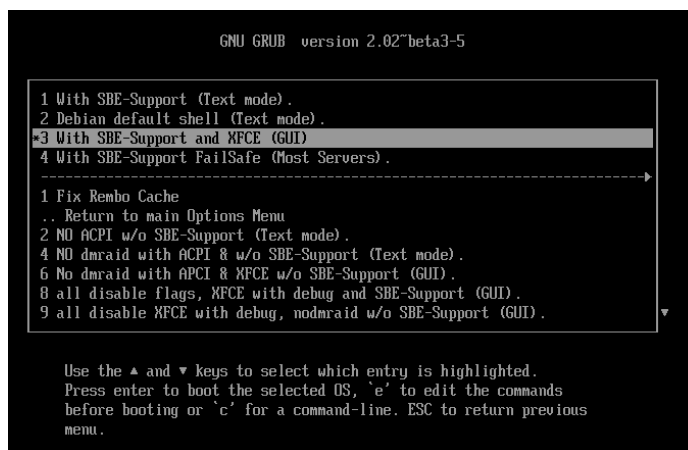


Abbildung II.1.2. LogoDIDACT Auswahlmenü bei UEFI-Boot

Wählen Sie innerhalb von 30 Sekunden bitte den dritten Eintrag **With SBE-Support and XFCE (GUI)** über die **Auf- und Ab-Pfeiltasten** und bestätigen Sie die Auswahl mit der **Eingabetaste**.

Bei XFCE handelt es sich um eine graphische Oberfläche (GUI) über welche die Installation des Servers im weiteren Verlauf einfach und komfortabel durchgeführt werden kann.

II.1.3.2.3. Schritt 3: Hardwareerkennung und Start mit graphischer Oberfläche

Im Normalfall werden alle notwendigen Hardwarekomponenten erkannt und initialisiert, so dass nach wenigen Sekunden die graphische Oberfläche startet. Gleichzeitig wird das ToolBox-Menü gestartet und der ToolBox-Monitor, der Statusinformationen zur Installation ausgibt.

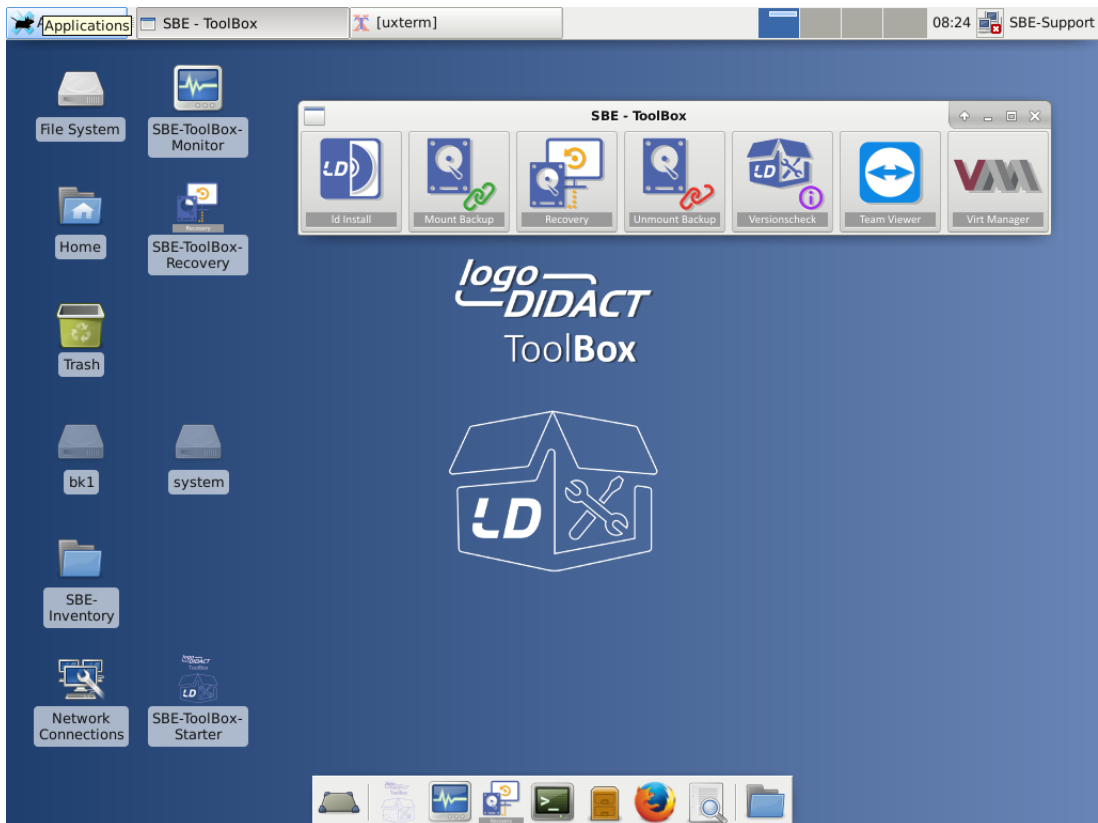


Abbildung II.1.3. Graphische Oberfläche XFCE mit ToolBox-Menü und ToolBox-Monitor

Im Normalfall wird die Hardware des Servers problemlos erkannt und damit auch die Netzwerkkarten für das interne und externe Interface. Die ToolBox-Software versucht dabei alles technisch machbare, um über eine der erkannten Netzwerkkarten einen Zugang zum Internet herzustellen. In aller Regel gelingt dies und vor allem in Standardumgebungen mit direkt angeschlossenem Router wird das keine Probleme bereiten.

Sobald der Internetzugang hergestellt werden konnte, zeigt der ToolBox-Monitor dies mit dem Eintrag **VERBUNDEN** in der ersten Zeile an. Weitere Prüfungen erfolgen erst beim Start der Installation über den Installer.

II.1.3.2.4. Schritt 4: Version des Installers prüfen

Für die Installation von LogoDIDACT 2.0 prüfen Sie zunächst über die Schaltfläche **Versionscheck**, ob Sie tatsächlich die neueste DVD-Version verwenden. Sofern eine Internetverbindung hergestellt werden kann, erhalten Sie die Anzeige der gerade eingesetzten DVD-Version sowie der neuesten Version online.



Abbildung II.1.4. Prüfung der Version der Toolbox-DVD

Sofern Sie die neueste Version einsetzen, fahren Sie mit dem nächsten Punkt fort, falls nicht, laden Sie sich diese herunter. Bitte verwenden Sie ausschließlich immer die neueste Toolbox-Version.

II.1.3.2.5. Schritt 5: Den LogoDIDACT Installer starten

Starten Sie die Installation über das erste Symbol in der Toolbox-Menüleiste.



Abbildung II.1.5. Der Installer befindet sich als erstes Symbol auf der ToolBar

II.1.3.2.6. Schritt 6: LogoDIDACT Lizenzvereinbarung

Akzeptieren Sie die LogoDIDACT Lizenzvereinbarung um mit der Installation fortzufahren. Klicken Sie dazu in den Text und lesen Sie sich die Vereinbarung durch. Sofern Sie mit den Lizenzbestimmungen einverstanden sind, wählen Sie **Akzeptieren**.

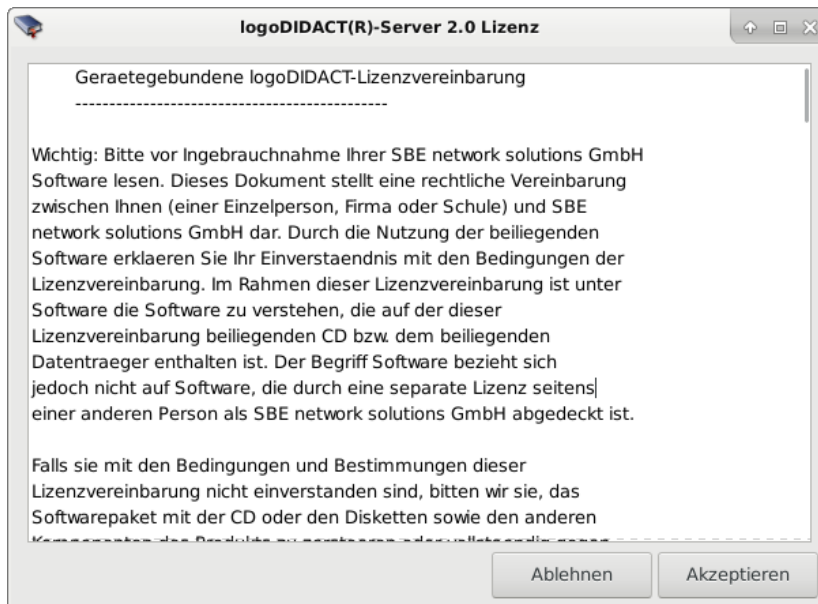
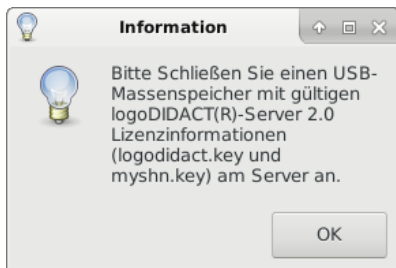


Abbildung II.1.6. Lizenzvereinbarung bestätigen

II.1.3.2.7. Schritt 7: USB-Stick mit Lizenzkeys anschließen

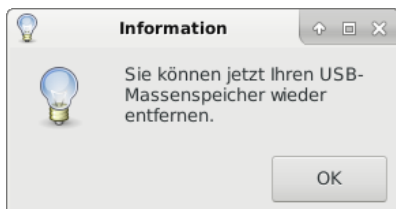
Sofern Sie den USB-Stick noch nicht eingesteckt haben, werden Sie dazu aufgefordert.



Sobald der Stick eingesteckt wurde, wird er eingebunden (gemountet). Ungeachtet dessen müssen Sie ihn explizit über das Drop-Down-Menü anwählen und diese mit **OK** bestätigen.



Die Lizenzinformationen werden übertragen und danach kann der USB-Stick wieder entfernt werden.



Es erfolgt eine Übersicht mit Informationen zum Lizenzkey.



II.1.3.2.8. Schritt 8: Uhrzeit und Zeitzone

Die Uhrzeit am Server muss stimmen, da ansonsten SSL Verbindungen nicht funktionieren. Deswegen wird anhand der Zeitzone die Uhrzeit am Server durch das Network Time Protocol (NTP) gesetzt. Wenn Sie keine Zeitzone angeben, wird automatisch Europe/Berlin verwendet.

Geben Sie deshalb an dieser Stelle nichts ein, sondern übernehmen Sie die Zeitzone mit **OK**.



II.1.3.2.9. Schritt 9: Schulnamen eingeben

Geben Sie als LongName den vollen Namen Ihrer Schule ein, wie er für die Einrichtung verwendet wird. In der Regel handelt es sich dabei um die Kombination aus einem Personennamen (z.B. Albert-Dürer-Schule) oder der Schulart (z.B. Gymnasium) und dem zugehörigen Ort.

II.1.3.2.10. Schritt 10: Namen der Domäne bzw. Kürzel festlegen

Während der LongName keine weitere technische Bedeutung hat, spielt der Kurzname (ShortName) eine wichtige Rolle und wird an verschiedenen Stellen verwendet. Primär wird damit der Domänenname festgelegt und das Kürzel sollte möglichst eindeutig sein.



Anmerkung

Der Eintrag ShortName bestimmt den Domänennamen!

Nicht erlaubt sind Leerzeichen, Sonderzeichen, Umlaute und auch kein Unterstrich! Wir empfehlen die Verwendung von Kurzbezeichnungen, die auch gegenüber anderen Schulen in Ihrer Umgebung eindeutig sind. Der Domänenname muss dabei nicht "schön" sein und kurze Namen haben durchaus Vorteile.

Problemlos und für alle leicht verständlich sind z.B. Kombinationen des kfz-Kennzeichens mit einer Kurzbezeichnung des Schulnamens, also z.B. hn-hfs als Abkürzung für „Hans-Fallada-Schule Heilbronn“ (LongName).

Wenn Sie sich an dieser Stelle der Installation noch nicht 100% mit dem Domänennamen sicher sind, können Sie diesen auch später noch ändern, bevor der Domänencontroller aufgebaut wird.

Im Folgenden verwenden wir für die beispielhafte Installation den Kurznamen **musterstadt-gym**.

II.1.3.2.11. Schritt 11: Kennwort für Benutzer root

Geben Sie im folgenden Dialog das Kennwort für den Benutzer `root` ein. Achten Sie hierbei bitte darauf, vor allem nach Abschluss der Installation ein sehr sicheres Kennwort zu wählen.

Der `root` Benutzer hat uneingeschränkten Zugang zu Server, Konfigurationseinstellungen und Dateien. Nach der Eingabe des Kennworts werden Sie aufgefordert, das Kennwort zur Sicherheit noch einmal zu bestätigen.

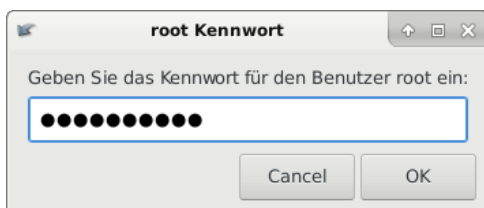


Achtung

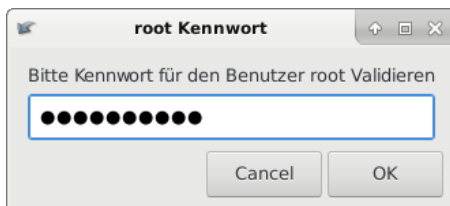
Während der Installation und der Einrichtung des Systems sollten Sie ein Kennwort verwenden, das nicht zu komplex ist, da Sie dieses mehrfach eingeben müssen und man Fehlautorisierungen vermeiden will.

Auf keinen Fall sollten sie aber ein zu einfaches Kennwort wie z.B. **muster** verwenden.

Sobald der Server online ist, laufen Sie sonst Gefahr, dass er sofort gehackt wird, da sich das Kennwort **muster** inzwischen auf zahlreichen Hackerlisten im Internet wiederfindet.



Bestätigen Sie die Eingabe des Kennwortes nochmals.



II.1.3.2.12. Schritt 12: Kennwort für administrative Benutzer

Das Kennwort für administrative Benutzer setzt das Kennwort für die Benutzer **admin**, **itb** und **pgmadmin**, die für die Verwaltung und Konfiguration der entsprechenden Systemdienste benötigt werden. Nach Eingabe des Kennworts müssen Sie dieses wiederum ein zweites Mal zur Bestätigung eingeben.



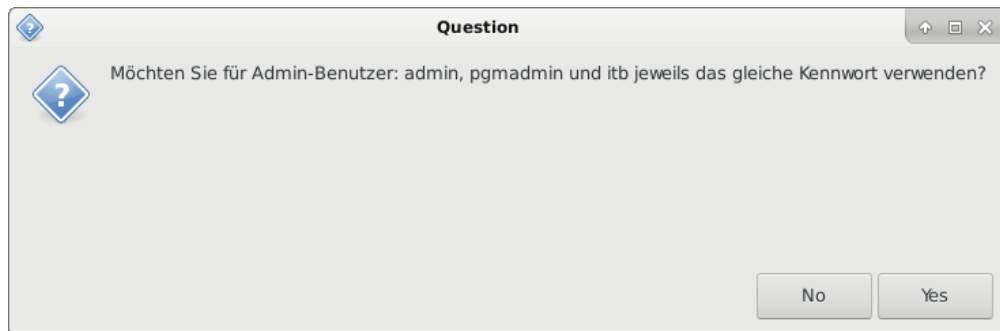
Anmerkung

Im Gegensatz zum Kennwort für den Benutzer **root** ist ein einfaches Kennwort für die administrativen Benutzer während der Installation kein Sicherheitsproblem.

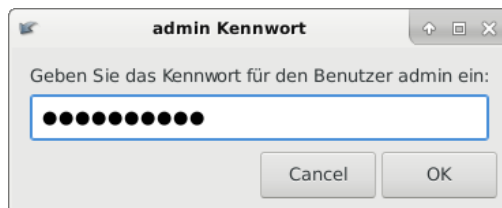
Um eventuelle Authentifizierungsprobleme während der Installation und der Einrichtung des Systems zu vermeiden, können Sie also ein einfaches Kennwort, wie z.B. **muster** verwenden.

Nach der Installation und der Einrichtung müssen jedoch auch diese Kennwörter auf sichere Werte umgestellt werden.

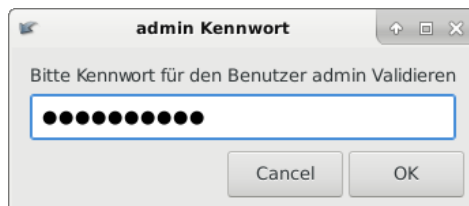
Sie sollten zunächst für alle drei administrativen Benutzer ein einheitliches Kennwort definieren und den Dialog mit YES bestätigen.



Geben Sie das einheitliche Kennwort ein



und bestätigen Sie es durch erneute Eingabe



II.1.3.2.13. Schritt 13: Externe Netzwerkkarte zuweisen

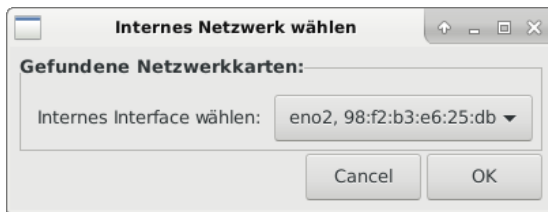
Wählen Sie im ersten Schritt die Netzwerkkarte für das sogenannte externe Interface aus, an dem im Normalfall der Router hängt. Die Zuordnung dieses Interfaces wird dadurch erleichtert, dass nicht nur der Interfacename und die MAC-Adresse angezeigt werden, sondern auch eine gegebenenfalls dynamisch vom Router zugewiesene IP-Adresse.

Es ist empfehlenswert immer die erste physikalische Netzwerkschnittstelle (eth0) als das Interface **extern** festzulegen.



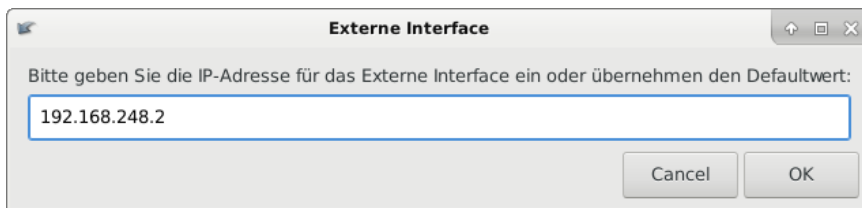
II.1.3.2.14. Schritt 14: Interne Netzwerkkarte zuweisen

Wählen Sie anschließend die Netzwerkkarte für **intern** und damit den Anschluss des Servers, der in aller Regel zum zentralen Switch führt.



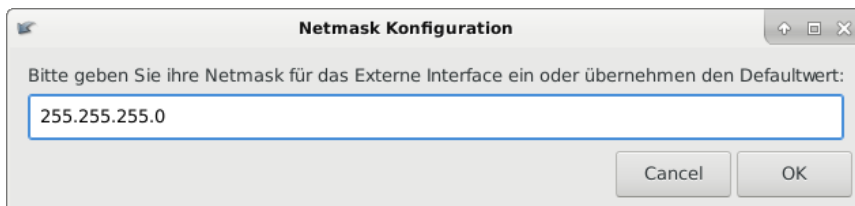
II.1.3.2.15. Schritt 15: Externe IP-Adresse

Legen Sie die IP-Adresse für die externe Netzwerkschnittstelle fest. Die externe Netzwerkschnittstelle stellt die Verbindung zum Internet her (meist über einen Router). Die IP-Adresse muss dabei in demselben Netz liegen wie der daran angeschlossene Router.



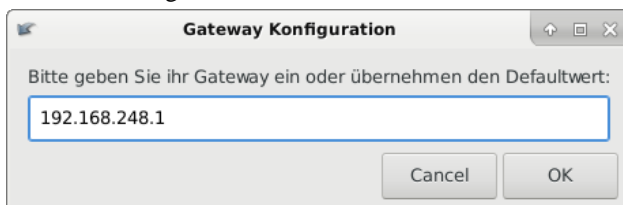
II.1.3.2.16. Schritt 16: Externe Subnetzmaske

Netzmaske für den gewählten externen IP-Bereich. Die Netzmaske sollte mit der Netzmaske des Routers übereinstimmen.



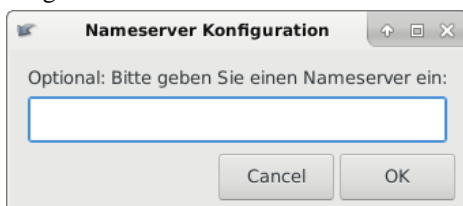
II.1.3.2.17. Schritt 17: IP des Routers / Gateways

Bitte geben Sie hier die IP-Adresse des Routers oder Gateways an, das an der externen Netzwerkschnittstelle angeschlossen ist.



II.1.3.2.18. Schritt 18: Festlegen des Nameservers

Bitte tragen Sie im folgenden Dialog nur dann einen Nameserver ein, wenn Sie sich absolut sicher sind, dass dies notwendig ist. Normalerweise ist hier keine Änderung notwendig, weshalb Sie keine Eingabe machen sollten. Klicken Sie einfach auf **OK**.



II.1.3.2.19. Schritt 19: Übersicht zur Netzwerkkonfiguration

Im folgenden Dialog erhalten Sie nochmals eine Übersicht der gemachten Netzwerkkonfiguration.



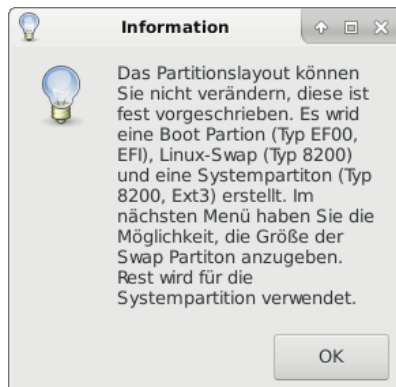
II.1.3.2.20. Schritt 20: Auswahl der Festplatte

Im nächsten Schritt wählen Sie die Festplatte im Server aus, auf welche installiert wird. Sie können in der Regel anhand der Größe zwischen der Systemplatte bzw. einem RAID-Verbund unterscheiden und z.B. einer Festplatte für die Datensicherung.

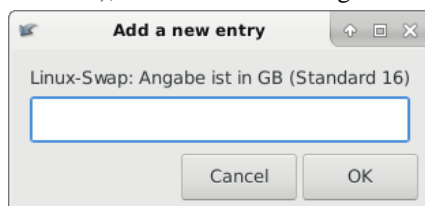


II.1.3.2.21. Schritt 21: Partitionieren und Formatieren der Festplatte

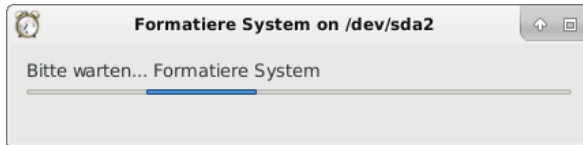
Die Partitionierung der Platte geschieht automatisch und Sie haben darauf keinen Einfluss. Das System nimmt sich den gesamten zur Verfügung stehenden Plattenplatz und teilt ihn entsprechend den Anforderungen sinnvoll auf. Bestätigen Sie den Dialog deshalb mit **OK**.



Übernehmen Sie den vorgeschlagenen Standardwert von 16 GB für die Auslagerungsdatei (Swap-Partition), indem Sie keine Eingabe vornehmen, sondern auf **OK** klicken.

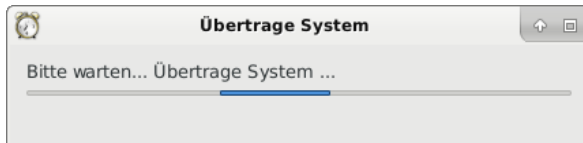


Die Platte wird nun formatiert, was je nach Größe und Geschwindigkeit der Platte ein klein wenig dauern kann.

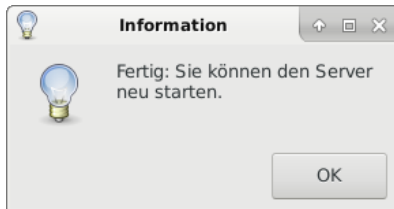


II.1.3.2.22. Schritt 22: Das System übertragen

Im letzten Schritt der Grundinstallation wird das System von der DVD auf die Festplatte des Servers übertragen. Dieser Vorgang dauert selbst bei einem sehr schnellen Server mindestens 15-20 Minuten, da die Geschwindigkeit maßgeblich vom DVD-Laufwerk bestimmt bzw. beschränkt wird.



Wenn alle Daten kopiert sind, kann der Server neu gestartet werden.



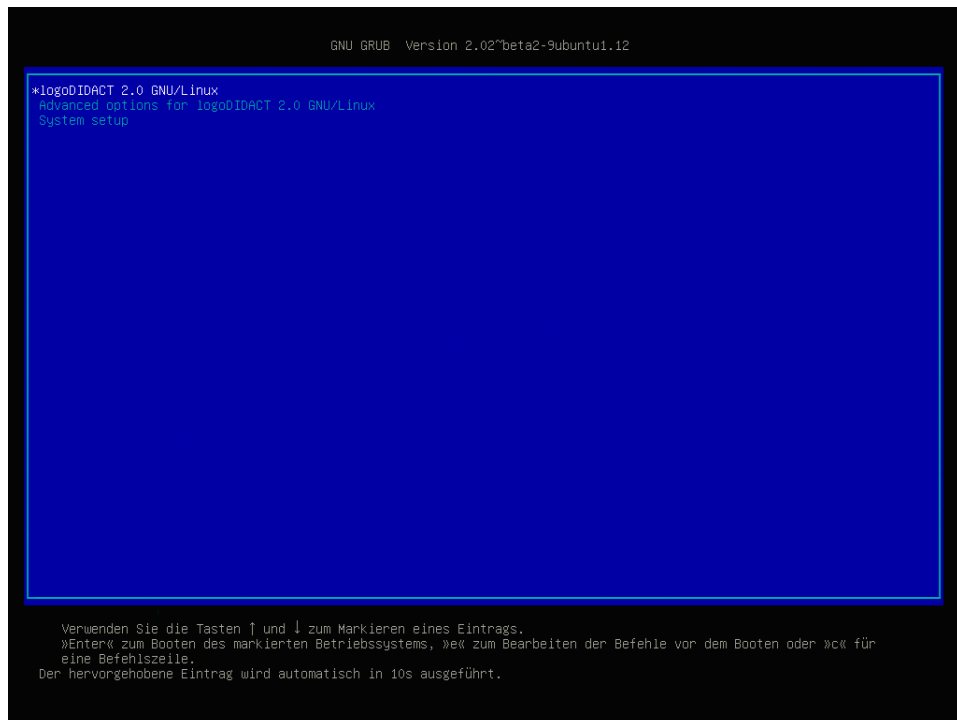
II.1.3.2.23. Schritt 23: Neustarten des Servers

Der Neustart des Servers erfolgt über das Menü rechts oben und den Eintrag **Log Out**.

Entfernen Sie die DVD aus dem Laufwerk und auch ggf. alle USB-Massenspeichergeräte. Wählen Sie anschließend **Restart**, um den LogoDIDACT-Server das erste Mal neu zu starten.

II.1.3.2.24. Schritt 24: Der erste Neustart des Servers

Sofern das System richtig übertragen wurde, startet zunächst der Bootloader **Grub** und wenige Augenblicke danach der LogoDIDACT-Server.



II.1.3.2.25. Schritt 25: Login Shell

Nach dem Starten des Servers werden Sie aufgefordert, Benutzernamen und Kennwort einzugeben. Geben Sie als Benutzername `root` ein und bestätigen Sie die Eingabe mit der **Eingabetaste**. Anschließend geben Sie das während der Installation gesetzte Kennwort ein. Beachten Sie, dass bei der Eingabe des Kennwortes aus Sicherheitsgründen nichts angezeigt wird, also auch keine "*" Zeichen, wie das in manchen Systemen der Fall ist.

```

ubuntu 14.04.4 LTS ldhost tty1
ldhost login: root
Password:
Last login: Fri Jul 21 09:30:09 CEST 2017 on tty1
Welcome to Ubuntu 14.04.4 LTS (GNU/Linux 3.13.0-88-generic x86_64)

* Documentation:  https://help.ubuntu.com/
root@ldhost:~#

```

II.1.3.2.26. Schritt 26: Laden des deutschen Tastaturlayouts

Während des ersten Deployments bzw. Aufbaus des Servers, ist es möglich, dass das System zeitweise das falsche Tastaturlayout verwendet. Bitte geben Sie zunächst das Minuszeichen "-" ein, um zu prüfen, ob der deutsche Zeichensatz geladen ist. Falls ein anderes Symbol erscheint, laden Sie nochmals den deutschen Tastaturzeichensatz:

```
loadkeys de
```

II.1.3.2.27. Schritt 27: Testen der Netzwerkumgebung

Prüfen Sie zunächst, ob Ihr Netzwerk richtig funktioniert. Pingen Sie deshalb zunächst den Router an. Dieser hat in der Regel eine IP-Adresse aus dem so genannten Class-C-Netzwerk `192.x.x.x`. Viele Hersteller verwenden per Standard die IP `192.168.1.1`. Die so genannte Default-IP finden Sie im Handbuch des Routers.

- **ping [Router IP-Adresse]**

Brechen Sie den Befehl ab mit der Tastenkombination **Strg+c**. Danach führen Sie einen ping auf eine externe IP-Adresse durch (z.B. 8.8.8.8):

- **ping [Externe IP-Adresse]**

Falls die Pings ankommen, sind Ihre Netzwerkinterfaces richtig konfiguriert.

Ebenfalls testen können Sie an dieser Stelle die Namensauflösung. Mit `ping -c3 google.de` werden drei Anfragen zum Server google.de gesendet. Kann der Name nicht aufgelöst werden, haben Sie vermutlich ein Problem mit Ihrer Internetverbindung bzw. Namensauflösung. Prüfen Sie in diesem Fall nochmals die Konfiguration von Modem bzw. Router.

Passen Sie die Netzwerkkonfiguration gegebenenfalls in `/etc/network/interfaces` an.



Anmerkung

Der erste Teil der Installation ist damit abgeschlossen und das Hostsystem auf Basis von Ubuntu 14.04 auf dem Server aufgespielt und grundlegend konfiguriert.

Mit dem zweiten Teil der Installation beginnt nun der automatisierte Aufbau und die Aktualisierung von Bausteinen, wie er für LogoDIDACT 2.0 typisch ist.

II.1.3.3. Systemaufbau durch Puppet

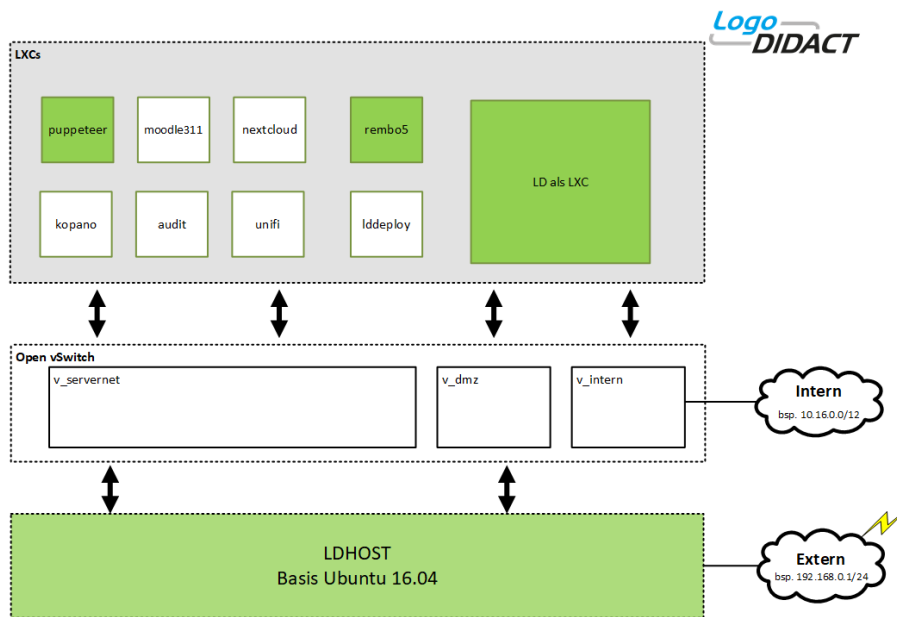
Bei der Grundinstallation wurde das Hostsystem Ubuntu 16.04 installiert und konfiguriert, ebenso der Container für das Konfigurations-Management-System puppet. Die Grundlagen zu puppet werden im Kapitel "Konfiguration des Servers und seiner Dienste" erläutert.



Achtung

Der zweite Teil der Installation von LogoDIDACT 2.0 läuft vollkommen automatisiert im Hintergrund ab. Sie dürfen den Server in dieser Phase des Deployments **auf keinen Fall ausschalten oder neu starten**.

In diesem zweiten Teil wird sowohl das Hostsystem als auch die drei Container puppeteer, logosrv und rembo5 aufgebaut und aktualisiert. Die folgende Abbildung veranschaulicht die Zusammenhänge.



II.1.3.3.1. Schritt 1: Das Deployment beobachten

Nach dem Start des Servers startet dieser seinen bis zu diesem Zeitpunkt einzigen Container puppeteer und es beginnt das so genannte Selbst-Deployment des puppeteer. Diesen automatischen Prozess kann man verfolgen, in dem man den folgenden Befehl gefolgt von der Eingabe-Taste eintippt:

```
watch -n1 "ps aux | grep -v grep | grep deploy"
```

Solange hierbei 2 Zeilen angezeigt werden, läuft das Deployment-Script noch!

```
Every 1,0s: ps aux | grep -v grep | grep deploy                               Fri Oct  6 16:22:19 2017
root      31558  0.0  0.0  22384  1600 ?        S    16:20   0:00 /bin/bash /var/lib/ld-puppet/1.deploy.d/onboot
```

Wie lange das Deployment dauert, hängt maßgeblich von der Geschwindigkeit des Servers ab. Auf einer schnellen Maschine mit performantem RAID-Controller, schnellen SAS-Festplatten und 8-Kern-Prozessor, sollte der Prozess nach etwa 20 Minuten erledigt sein.

```
Every 1,0s: ps aux | grep -v grep | grep deploy                               Fri Oct  6 16:34:41 2017
```

Den Schritt 2 können Sie überspringen, wenn Sie keine detaillierten Infos benötigen und es keine Probleme im Ablauf gibt.

II.1.3.3.2. Schritt 2: Ausführliche Infos zum Deployment

Wenn man mehr Infos und Details sehen möchte, kann man sich die Aktivitäten auch auf Basis der Protokolldateien anschauen. Dazu könnte man in den Container des puppeteer wechseln und sich die Log-Datei dort anschauen. Da der Container selbst aber nicht im Aufbau ist und während diese Phase auch automatisiert gestartet werden kann, schaut man sich die Vorgänge besser vom Hostsystem aus an, denn dieser hat auf Dateisystemebene Zugriff auf seine Container.

```
tail -f var/lib/lxc/puppeteer/rootfs/var/log/ld-puppet.deploy
```

Mittels des Befehls **tail** werden die letzten 10 Zeilen der Logdatei angezeigt, in die das Deployment-Script die Ausführung seiner Befehle protokolliert. Sie beenden die Anzeige durch Eingabe der Tastenkombination **strg+c**. Die Protokoll-Datei dient gleichzeitig als Quelle für die Analyse eventuell

auftretender Fehler. Der Server darf auf keinen Fall neu gestartet werden, bevor das Deployment-Script ein Mal komplett durchgelaufen ist.



Achtung

Nicht jeder Eintrag in der Logdatei, der "warning" oder "error" enthält oder in Rot auf einen vermeintlichen Fehler hindeutet, ist in Wirklichkeit ein Fehler. Die Protokolldatei ist primär für die Experten gedacht und generell hilfreich bei der Suche nach wirklichen Fehlern.

```
root@puppeteer:~ # tail -f /var/log/ld-puppet.deploy
Notice: /Stage[main]/Ld_puppet::Master/Ini_setting[ld_puppet::puppetdb::db::slow_queries]/value: value changed '10' to '0'
Notice: /Stage[main]/Ld_puppet::Master/Ini_setting[ld_puppet::puppetdb::db::passwd]/ensure: created
Notice: /Stage[main]/Ld_puppet::Master/Ini_setting[ld_puppet::puppetdb::db::username]/ensure: created
Notice: /Stage[main]/Ld_puppet::Master/Ini_setting[ld_puppet::puppetdb::db::protocol]/value: value changed 'hsqldb' to 'postgresql'
Notice: /Stage[main]/Ld_puppet::Master/Ini_setting[ld_puppet::jetty::host]/ensure: created
Notice: /Stage[main]/Ld_puppet::Master/Service[apache2]: Triggered 'refresh' from 21 events
Notice: /Stage[main]/Ld_puppet::Master/Service[puppetdb]: Triggered 'refresh' from 14 events
Notice: Finished catalog run in 59.54 seconds
Warning: Unable to fetch my node definition, but the agent run will continue:
Warning: undefined method 'include?' for nil:NilClass
Error: Could not update: Execution of '/usr/bin/gem install --no-rdoc --no-ri redis ' returned 3: ERROR: Error install
```

Sie können sich deshalb auf den oben aufgeführten ersten Befehl beschränken, der einfach anzeigt, ob der Prozess für das Deployment noch aktiv ist oder nicht.

II.1.3.3.3. Schritt 3: Neustart des Servers

Sobald das Deployment-Script das erste Mal durchgelaufen ist, können Sie den Server (Host) neu starten. Dies wird im Hostsystem auch angezeigt, wenn Sie dort den folgenden Befehl eingeben:

```
ldinfo
root@ldhost:~# ldinfo
Welcome to...
LogoDIDACT 2.0
ldhost.schule.local / physical

Server : Musterschule Musterstadt / musterstadt-gym
Load   : 0.14 / 0.39 / 0.46
Puppet : 2017-10-06 16:34 T:442/S:441/F:1 R:611
LXC    : logosrv/puppeteer/rembo5

Hints
1. A reboot of this machine is required.

root@ldhost:~#
```

Über den Befehl **ldinfo** bekommen Sie sowohl in jedem Container als auch im Hostsystem wertvolle Informationen. Im Hostsystem sehen Sie beispielsweise, welche Container (LXCs) aktiv sind.

Starten Sie den Server durch Eingabe von **reboot** neu. Achten Sie darauf, dass Sie sich auch wirklich im Hostsystem befinden und nicht innerhalb eines Containers. Wenn Sie den Befehl in einem Container absetzen, startet nur die virtuelle Maschine bzw. dieser Container neu.

II.1.3.4. LogoDIDACT Update

Nachdem der Server neu gestartet ist, melden Sie sich wieder als Benutzer **root** an. Wechseln Sie in den Container **LOGOSRV** durch Eingabe des Befehls:

```
lxc-attach -n logosrv
```

Starten Sie danach die Aktualisierung dieses Containers durch Eingabe von:

ldupdate

Der Update-prozess prüft, ob es aktuellere Pakete für LogoDIDACT gibt.

```

root@logosrv: ~
Server : Musterschule Musterstadt / musterstadt-gym
Load   : 0.12 / 0.13 / 0.14

musterstadt-gym / physical / 17:21 / 0.9.77 / attach
root@logosrv:~ # ldupdate
Loading newest logoDIDACT update component...
- http://packages.logodidact.com/update/ldupdate.gpg... OK

Updater: /var/spool/logodidact/update/ldrealupdate (Log: ldrealupdate.log)
-----
Checking logoDIDACT license... Software assurance till: 2018-10-04 00:00:00
Please wait, updating list of available packages...
Information about the upgrade:
- The following 26 packages will be updated:

  ld-acmetool, ld-base, ld-baselibs, ld-dhcp-server, ld-dns-server,
  ld-firewall, ld-hotspot, ld-ldap-server, ld-libhttpclient-ruby1.8,
  ld-mail-retriever, ld-netlogon, ld-netlogon-gui, ld-progs-agent,
  ld-progs-client, ld-proxy-reverse, ld-samba, ld-server, ld-site-icb,
  ld-vpn-server, ldc-lin, ldc-win, libsmbclient0, libwbclient0, samba,
  samba-common, smbclient

Proceed with the upgrade? [y/N] █

```

Bestätigen Sie das Einspielen durch Eingabe von **y**.

Der Container logosrv ist gewissermaßen der alte LogoDIDACT 1.0 Server, aus dem inzwischen etwa zwei Dutzend Bausteine und Module herausgenommen und in eigene Container verlagert wurden. Dieser Container (LXC) wird nicht von puppet verwaltet und muss deshalb (wie in der Vergangenheit) noch separat aktualisiert werden.

```

root@logosrv: ~
- Writing /etc/dhcp3/dhcpd.conf.logodidact
- Restarting DHCP server

Processing triggers for ld-base ...
* Stopping logoDIDACT update server daemon: ldupdateserver [ OK ]
* Starting logoDIDACT update server daemon: ldupdateserver
[2017-10-06 17:25:11] <INF> Starting server on 0.0.0.0:4283 [ OK ]

Erzeuge Paket: /usr/lib/mysn7/logoDIDACT/windows32.pak
Erzeuge Paket: /usr/lib/mysn7/logoDIDACT/windows64.pak
Erzeuge Paket: /usr/lib/mysn7/logoDIDACT/linux32.pak
Erzeuge Paket: /usr/lib/mysn7/logoDIDACT/linux64.pak
Reading package lists... Done
Building dependency tree
Reading state information... Done
Reading extended state information
Initializing package states... Done
Writing extended state information... Done

Current status: 0 updates [-26].
-----
musterstadt-gym / physical / 17:26 / 0.9.77 / attach
root@logosrv:~ # █

```

Wenn das Update durchgelaufen ist, starten Sie den Container neu:

reboot

Dabei wird lediglich der Container logosrv neu gestartet, nicht der gesamte Server.

II.1.3.5. Aktualisierung des Open vSwitch

Zwischen Host und virtuellen Maschinen fungiert in LogoDIDACT 2.0 ein virtueller Switch auf Basis von Open vSwitch, kurz OvS. Dass die Aktualisierung dieser Komponente systemkritisch ist, leuchtet sicherlich ein, wenn man an die Aktualisierung der Firmware eines physischen Switches denkt. Deshalb werden die Aktualisierungen bewusst zurückgehalten (retained), weil Sie zwingend mit einem Neustart des gesamten physischen Serversystems verbunden sind und bewusst und zeitlich eingeplant durchgeführt werden sollten.

Die Aktualisierung dieser systemkritischen Komponenten erfolgt über den Befehl:

upgrade-retained-packages



Achtung

Starten Sie den Server danach unbedingt neu, auch wenn das nirgends angezeigt wird! Der Befehl **upgrade-retained-package** kann ohne spezielle Kenntnisse nur direkt am Server ausgeführt werden und sorgt dafür, dass bewusst zurückgehaltene Pakete des OvS aktualisiert werden.

Damit der Open vSwitch diese übernimmt, sind unter Ubuntu 16.04 nacheinander die folgenden Befehle einzugeben, um die Datenbank des OvS neu aufzubauen:

```
systemctl stop openvswitch-switch.service
```

Bevor Sie die Datenbankdatei löschen, prüfen Sie, ob diese nur ein Symlink auf `/etc/openvswitch/conf.db` ist und löschen Sie gegebenenfalls die Originaldatei.

```
rm /var/lib/openvswitch/conf.db
```

Zum Abschluss muss der Server (ldhost) neu gestartet werden:

```
reboot
```

II.1.3.6. Änderung des root-Kennwortes

Nachdem der Server und seine Komponenten auf einem aktuellen Stand sind, können Sie das Kennwort des Benutzers root an zentraler Stelle für alle physischen und virtuellen Maschinen ändern. Wechseln Sie dazu in den Container des Puppeteer und geben Sie den folgenden Befehl ein:

```
puppet -passwd
```

Damit wird das root-Kennwort im Host und allen Containern aktualisiert, auch im logosrv.

Teil III. Konfiguration des Servers und seiner Dienste

Inhaltsverzeichnis

III.1. USV	III – 9
III.1.1. Sinn und Zweck der USV	III – 9
III.1.2. Geeignete Modelle	III – 9
III.1.2.1. APC Smart-UPS SMX750i oder SMX1000i	III – 9
III.2. Backup	III – 13
III.2.1. Backup Konzept in LogoDIDACT	III – 13
III.2.1.1. Art und Ablauf der Sicherung	III – 14
III.2.1.2. Zeitplan für Sicherungen in LogoDIDACT	III – 14
III.2.1.3. Benachrichtigung über durchgeführte Sicherungen	III – 14
III.2.1.4. Dateien, die nicht gesichert werden	III – 15
III.2.1.5. Internet-Surfdaten aus dem Backup ausschließen	III – 16
III.2.1.6. Art und Anzahl der Sicherungen festlegen (Backup-Rotation)	III – 16
III.2.2. Backupfestplatte neu initialisieren	III – 16
III.2.3. "Hot-Plug" Sicherung über LD-USB-BAK	III – 18
III.2.3.1. USB-Platte für Hot-Plug neu einrichten	III – 18
III.2.3.2. Sicherung mit USB Hot-Plug durchführen	III – 18
III.2.3.3. USB Hot-Plug im Monitoring überwachen	III – 20
III.2.4. Sicherung des Auslieferungszustandes	III – 20
III.2.5. Technischer Ablauf des Backups und mögliche Probleme	III – 22
III.2.6. Backup auf NAS per iSCSI	III – 22
III.2.6.1. Separates Netzwerkinterface für NAS einrichten	III – 23
III.2.6.2. Das NAS-Gerät konfigurieren	III – 24
III.2.6.3. Sicherung auf NAS am Server einrichten	III – 40
III.2.7. Restauration im Fehlerfall	III – 43
III.2.7.1. Restauration im lauffähigen System	III – 43
III.2.7.2. Disaster Recovery - Notfallwiederherstellung	III – 43
III.3. Server und Systemdienste	III – 47
III.3.1. Netzwerk-Konfiguration am Server	III – 47
III.3.1.1. Physische Netzwerkzuordnung	III – 48
III.3.1.2. Externe IP-Adresse des Servers anpassen	III – 49
III.3.1.3. Interface extern auf DHCP stellen	III – 50
III.3.1.4. Interne IP-Adresse des ldhost anpassen	III – 50
III.3.1.5. Netzwerkbereich anpassen	III – 51
III.3.1.6. IP-Adresse des logosrv anpassen	III – 53
III.3.1.7. Trunks, Bonding und LACP	III – 54
III.3.1.8. Netzwerke und VLANs in LogoDIDACT 2.0	III – 56
III.3.2. Der Host und seine Container	III – 58
III.3.2.1. Befehle zum Verwalten der Container (LXC's)	III – 58
III.3.3. Konfigurations-Management mit Puppet	III – 60
III.3.3.1. Grundlagen zu Puppet	III – 61
III.3.3.2. Puppet Tools und Befehle	III – 62
III.3.3.3. logoDIDACT 2.0 mit Puppet managen	III – 63
III.3.3.4. Container aufbauen	III – 68
III.3.3.5. Container löschen	III – 70
III.3.4. Aktivierung samba4-ad	III – 70
III.3.4.1. Samba 4 Domänennamen festlegen	III – 71
III.3.4.2. Samba 4 Domäne aufbauen (lassen)	III – 72
III.3.4.3. Samba 4 Administration und Tools	III – 73
III.3.5. Reverse-Proxy	III – 74
III.3.5.1. Vorbereitungen und Voraussetzungen	III – 75
III.3.5.2. Container rev-proxy aufbauen	III – 75
III.3.5.3. Den Reverse Proxy für Webdienste aktivieren	III – 76

III.3.5.4. Ports an den Reverse Proxy weiterleiten	III – 77
III.3.6. Zertifikate mit Let's Encrypt	III – 77
III.3.6.1. Digitale Zertifikate	III – 78
III.3.6.2. Let's encrypt aktivieren	III – 78
III.3.6.3. Zertifikat erstellen	III – 79
III.3.6.4. Zertifikat prüfen	III – 83
III.3.6.5. Zertifikate aktualisieren	III – 83
III.3.7. Verwendung eigener Zertifikate	III – 83
III.3.8. Interne Certification Authority (CA)	III – 84
III.3.9. Zugriff auf LDAP per SSL/TLS	III – 84
III.3.9.1. Port über Firewall an Rev-Proxy leiten	III – 85
III.3.9.2. Zertifikat für Rev-Proxy erstellen und prüfen	III – 85
III.3.9.3. Konfiguration für LDAP im Rev-Proxy	III – 86
III.3.9.4. LDAP von außen testen	III – 86
III.3.9.5. Den Zugriff auf LDAP in der Firewall absichern	III – 89
III.3.9.6. Konfiguration für Samba4-AD	III – 90
III.3.9.7. Spezielle LDAP-Benutzer und Attribute	III – 91
III.3.10. Virtuelle Maschinen mit KVM	III – 93
III.3.10.1. KVM am Server aktivieren	III – 94
III.3.10.2. Virtio Treiber installieren	III – 94
III.4. Konfiguration des logosrv	III – 95
III.4.1. Firewall	III – 95
III.4.1.1. Fernzugriff auf den Server	III – 95
III.4.1.2. Ports und Protokolle	III – 100
III.4.1.3. Sperren von Tor-Verbindungen	III – 102
III.4.2. Proxy-Server	III – 102
III.4.3. Webfilter	III – 103
III.4.3.1. Schlagwortfilter Schwellwert ändern	III – 103
III.4.3.2. Vorratsdatenspeicherung für Internetauswertung anpassen	III – 103
III.4.4. Drucker Einstellungen cups/pykota	III – 103
III.4.4.1. Bestätigung des Druckauftrags am Client deaktivieren	III – 103
III.4.4.2. Druckeragent bzw. Printagent Symbol am Client ausschalten	III – 104
III.4.5. DHCP-Optionen	III – 104
III.4.5.1. IP-Adress-Vergabe für fremde Rechner sperren	III – 104
III.4.5.2. Adressbereich für dynamische IPs anpassen	III – 104
III.4.6. DNS-Server	III – 105
III.4.6.1. Verbotene Namen	III – 105
III.4.6.2. DNS Rechnereintrag per wimport_data	III – 105
III.4.6.3. Dynamisches DNS	III – 106
III.4.7. Laufwerke und Zugriffsberechtigungen	III – 106
III.4.7.1. Zusätzliche Freigabe und Laufwerk einrichten	III – 106
III.4.7.2. Zugriffsberechtigung ACLs in LogoDIDACT	III – 107
III.4.7.3. Zugriff für Lehrer auf Schüler Homelaufwerke	III – 109
III.4.7.4. Lesender Zugriff der Lehrer auf Schüler-Homes	III – 109
III.4.7.5. Vollzugriff der Lehrer auf Schüler-Homes	III – 109
III.4.7.6. Vollzugriff der Lehrer auf Lehrer-Tausch	III – 110
III.4.7.7. Vollzugriff aller Benutzer auf Schulweiter Tausch	III – 110
III.4.7.8. Vollzugriff auf Klassen-Tauschlaufwerke	III – 111
III.4.7.9. Klassentauschlaufwerke deaktivieren	III – 112
III.4.7.10. Tauschlaufwerke zyklisch löschen	III – 112
III.4.7.11. Anpassung der Dateigröße beim Austeilen	III – 113
III.4.8. Cron-Jobs	III – 113
III.4.9. Befehle und Skripte am logosrv	III – 114
III.4.10. Apache Webserver	III – 115

III.4.10.1. Aktivierung interner Webseiten über public_html	III – 115
III.4.10.2. Schulinterne Homepage im Intranet aktivieren	III – 116
III.4.11. Rechte und Berechtigungen	III – 118
III.4.11.1. Zugriff auf Funktionen in der LogoDIDACT-Console ändern	III – 118
III.4.11.2. Gruppe Datenschutz und Verwaltung	III – 120
III.4.12. Benutzer und Kennwörter	III – 121
III.4.12.1. Benutzer	III – 121
III.4.12.2. Kennwörter	III – 124
III.4.13. Log-Dateien	III – 126
III.4.13.1. Rotieren und Komprimieren von Log-Dateien	III – 126
III.4.14. Radius-Server	III – 127
III.5. Softwareverteilung mit LD Deploy	III – 129
III.5.1. Vorteile von LD Deploy	III – 129
III.5.2. Voraussetzungen und Einschränkungen	III – 129
III.5.2.1. Voraussetzungen	III – 129
III.5.2.2. Einschränkungen	III – 130
III.5.2.3. Dringende Empfehlungen	III – 130
III.5.3. Parallelbetrieb von LD Deploy und Rembo/mySHN®	III – 130
III.5.3.1. Neuinstallationen nur mit LD Deploy	III – 130
III.5.3.2. Ergänzung bestehender Rembo-Installationen mit LD Deploy	III – 131
III.5.4. Installation von LD Deploy	III – 133
III.5.5. Freigegebene und Entwickler-Pakete	III – 134
III.5.5.1. Offizielle Pakete	III – 134
III.5.5.2. Entwickler-Pakete für Testzwecke	III – 135
III.5.6. Aktualisierung von LD Deploy Paketen	III – 136
III.5.7. Windows 10 bereitstellen	III – 137
III.5.7.1. Die richtige Windows 10 Variante bereitstellen	III – 138
III.5.7.2. Image importieren	III – 140
III.5.7.3. Import eines Images prüfen	III – 140
III.5.7.4. Torrent Infos	III – 142
III.5.8. Das Control Center starten	III – 143
III.5.9. Eine Windows 10 Umgebung erstellen	III – 144
III.5.9.1. Ein Betriebssystem erstellen	III – 145
III.5.9.2. Dem Betriebssystem ein Image zuordnen	III – 145
III.5.9.3. Konfiguration erstellen und Betriebssystem verknüpfen	III – 147
III.5.9.4. Den Domänenbeitritt konfigurieren	III – 149
III.5.9.5. Das Betriebssystem mit der Domäne verknüpfen	III – 150
III.5.9.6. Die Konfiguration mit der OU Computers verknüpfen	III – 152
III.5.10. Background Deployment	III – 153
III.5.10.1. Hintergrund-Verteilung in Windows 10	III – 153
III.5.10.2. Background Deployment aktivieren	III – 154
III.5.10.3. Verhalten an den Windows 10 Clients	III – 155
III.5.11. Synchronisation der Geräteliste wimport_data	III – 156
III.5.11.1. Automatischer Abgleich beim Anlegen oder Löschen	III – 156
III.5.11.2. Fehler in der Synchronisation zwischen Control Center und Geräteliste	III – 157
III.5.11.3. Fehler durch doppelten dhcpd Prozess im logosrv	III – 158
III.5.11.4. Manueller Abgleich der Geräteliste bei Namensänderung	III – 158
III.5.12. Client-Konfiguration mit AutoConf	III – 158
III.5.12.1. Vordefinierte Rollen für AutoConf	III – 158
III.5.12.2. Aktualisieren eines Playbooks	III – 159
III.5.13. Protokollierung mit graylog	III – 161
III.5.13.1. Installation Container graylog	III – 161
III.5.13.2. Webinterface von graylog	III – 162

III.6. Microsoft Produktaktivierung mit LD Deploy	III – 163
III.6.1. Neue Produktaktivierung in LogoDIDACT 2.0	III – 163
III.6.2. Grundlagen der Lizenzierung und Aktivierung	III – 164
III.6.2.1. Der Microsoft KMS (Key Management Service)	III – 164
III.6.2.2. Lizenzrecht und Lizenztechnik	III – 164
III.6.2.3. Der richtige Volumenlizenzvertrag für KMS	III – 165
III.6.3. Windows 10 KMS-Host mit LD Deploy aufsetzen	III – 167
III.6.3.1. Voraussetzungen	III – 167
III.6.3.2. Windows 10 Professional 1903 für KMS bereitstellen	III – 168
III.6.3.3. Eine win10kms Umgebung im Control-Center erstellen	III – 168
III.6.3.4. Die Datenträgerverwaltung starten	III – 170
III.6.3.5. Virtuelle Maschine win10kms im Control Center eintragen	III – 172
III.6.3.6. Virtuelle Maschine win10kms mit Konfiguration verknüpfen	III – 174
III.6.3.7. Virtuelle Maschine aktivieren	III – 175
III.6.3.8. Virtuelle Maschine starten	III – 176
III.6.3.9. Die wichtigsten virsh Befehle	III – 176
III.6.3.10. Aufbau der virtuellen Maschine per Virt-Viewer beobachten	III – 176
III.6.3.11. Tools installieren	III – 178
III.6.3.12. Windows 10 Key am KMS-Host eingeben und aktivieren	III – 180
III.6.3.13. Probleme mit KMS-Keys und mögliche Ursachen	III – 180
III.6.3.14. Office Volume License Pack installieren	III – 181
III.6.3.15. Office Key über Volumenaktivierungstool eingeben und aktivieren.....	III – 183
III.6.3.16. Office KMS-Key per Kommandozeile einspielen und aktivieren	III – 186
III.6.3.17. KMS-Client-Emulator starten und Aktivierung prüfen	III – 187
III.6.3.18. Emulator wiederkehrend als Aufgabe ausführen	III – 189
III.6.4. Umgebung für Microsoft KMS konfigurieren	III – 192
III.6.4.1. DNS-Eintrag im logosrv erstellen	III – 192
III.6.4.2. Ports am KMS-Host öffnen	III – 192
III.6.4.3. GVLK am Windows Client eintragen	III – 193
III.6.4.4. Aktivierungsskript für Clients	III – 193
III.7. Unifi WLAN-Lösung	III – 195
III.7.1. Installation Container Unifi	III – 195
III.7.2. Unifi im Rev-Proxy freischalten	III – 196
III.7.3. Zertifikat für Unifi aktivieren	III – 197
III.7.4. Unifi Erstanmeldung	III – 197
III.7.5. Admin-Anmeldung und Spracheinstellung	III – 200
III.7.6. Unifi Konfiguration von Hostname und Mail	III – 201
III.7.7. SSH-Zugang für Unifi Access Points	III – 202
III.7.8. WLAN Konfiguration	III – 203
III.7.8.1. WLAN mit WPA2-Verschlüsselung	III – 203
III.7.8.2. WLAN für die Aufnahme von Tablets	III – 205
III.7.8.3. AccessPoints einbinden	III – 205
III.8. Tablet-Management mit LD Mobile	III – 207
III.8.1. Vorteile von LD Mobile	III – 207
III.8.2. Voraussetzungen für LD Mobile	III – 207
III.8.3. Installation der MariaDB-Datenbank	III – 208
III.8.4. Prüfung der Verzeichnisstruktur	III – 209
III.8.5. Festlegung von MariaDB als Datenbank	III – 210
III.8.6. Datenbank-Migration auf MariaDB 10.5	III – 210
III.8.7. Installation Container LD Mobile	III – 211
III.8.8. Router für Zugriff von außen konfigurieren	III – 212
III.8.9. LD Mobile im Rev-Proxy freischalten	III – 212
III.8.10. Zertifikat für LD Mobile aktivieren	III – 213
III.8.10.1. Zertifikat mit acme.sh beantragen	III – 213

III.8.10.2. Zertifikat mit acmetool beantragen	III – 214
III.8.11. Ports für Apple- und Google-Server freischalten	III – 214
III.8.12. Admin-Anmeldung in LD Mobile	III – 215
III.8.13. Lizenzen prüfen und anfordern	III – 216
III.8.14. Die LD Mobile APPs zuweisen	III – 217
III.8.15. Device Enrollment Program - DEP	III – 221
III.8.16. Anbindung an Apple DEP	III – 221
III.8.16.1. Serverzertifikat speichern	III – 222
III.8.16.2. Im Apple School Manager Portal anmelden	III – 223
III.8.16.3. MDM-Server hinzufügen und Zertifikat laden	III – 223
III.8.16.4. Server Token erzeugen	III – 225
III.8.16.5. Server-Token in LD Mobile laden	III – 226
III.8.17. Anbindung an Apple VPP	III – 228
III.8.18. Geräte im ASM zuweisen	III – 228
III.8.19. DEP-Geräte in LD Mobile synchronisieren	III – 229
III.8.20. DEP-Profil erstellen	III – 230
III.8.20.1. DEP-Profil für gemeinsam genutzte iPads	III – 230
III.8.21. Regelwerk anlegen	III – 231
III.8.22. Richtlinien anlegen	III – 232
III.8.22.1. WLAN-Richtlinie	III – 233
III.9. LogoDIDACT an Office 365 ankoppeln	III – 237
III.9.1. Office 365 Konfiguration	III – 237
III.9.1.1. Tenant und Domainname	III – 237
III.9.1.2. Eine neue Domäne anlegen	III – 239
III.9.1.3. Tenant und Domäne für Schulträger	III – 239
III.9.1.4. Das kostenfreie Office 365 A1 beantragen	III – 240
III.9.1.5. Ein administratives Konto anlegen	III – 244
III.9.1.6. Den Tenant mit der Domäne verbinden	III – 247
III.9.1.7. DNS-Konfiguration für weitere Dienste	III – 251
III.9.1.8. DNS-Server von Microsoft beim Provider eintragen	III – 254
III.9.1.9. Domäne als Standard festlegen	III – 259
III.9.2. Der LogoDIDACT Connector für Azure-AD	III – 260
III.9.2.1. Entwicklerpakete für Azure-AD einspielen	III – 260
III.9.2.2. Den Connector für Azure-AD installieren	III – 260
III.9.2.3. Den Connector für Azure-AD konfigurieren	III – 262
III.9.2.4. Eine APP in Azure-AD registrieren	III – 265
III.9.2.5. Einen geheimen Clientschlüssel in Azure-AD anlegen	III – 267
III.9.2.6. Der APP administrative Rechte zuweisen	III – 269
III.9.2.7. Connector an ID koppeln	III – 271
III.9.2.8. Benutzern im Control Center Office 365 Lizenzen zuweisen	III – 272
III.9.2.9. Benutzer zu Azure AD synchronisieren	III – 275
III.9.3. Das Kennwortportal SSP konfigurieren	III – 277
III.9.4. Die Zwei-Faktor-Sicherheit in Azure-AD deaktivieren	III – 279
III.9.5. Besprechungs-Richtlinien in Teams anpassen	III – 280
III.9.6. Richtlinien in Teams unberührt lassen	III – 283
III.9.7. Benutzer und Rechte anpassen	III – 283
III.9.7.1. Umgang mit bestehenden Benutzern in Azure	III – 283
III.9.7.2. Benutzern Admin-Rollen zuweisen	III – 284
III.9.7.3. Erstellen manueller Teams verbieten	III – 285
III.10. Nextcloud	III – 287
III.10.1. Voraussetzungen	III – 287
III.10.2. Die Container für Nextcloud und Collabora aktivieren	III – 288
III.10.3. Templates kopieren und anpassen	III – 289
III.10.4. Nextcloud im Rev-Proxy eintragen	III – 289

III.10.5. Zertifikate für Nextcloud und Collabora beantragen	III – 290
III.10.6. Zugriff auf Nextcloud erlauben	III – 291
III.10.7. Änderung des Objektspeichers	III – 292
III.10.7.1. Ankopplung an Samba4	III – 293
III.10.7.2. Umstellung auf Nextcloud files	III – 293
III.10.8. Deaktivierung von Plugins	III – 296
III.10.9. Update von Nextcloud über mehrere Versionen	III – 297
III.10.10. Konfiguration der Nextcloud für OnlyOffice anstelle Collabora	III – 298
III.11. Kopano	III – 303
III.11.1. Voraussetzungen	III – 303
III.11.2. Installation der Datenbank MariaDB 10.3	III – 303
III.11.3. Prüfung der Verzeichnisstruktur	III – 304
III.11.4. Festlegung von MariaDB 10.3 als Datenbank	III – 305
III.11.5. Datenbank-Migration auf MariaDB 10.3	III – 305
III.11.5.1. Voraussetzungen	III – 305
III.11.5.2. Größe der Kopano-Datenbank und freien Speicherplatz prüfen	III – 305
III.11.5.3. Kopano-Dienste anhalten	III – 306
III.11.5.4. Datenbank erstellen lassen	III – 306
III.11.5.5. Datenbank-Migration starten	III – 306
III.11.5.6. Kopano-Dienste wieder starten	III – 307
III.11.5.7. Alte Datenbanken im Container mysql56 löschen	III – 307
III.11.6. Installation Container Kopano	III – 307
III.11.7. Kopano im Rev-Proxy freischalten	III – 308
III.11.8. Zertifikat für Kopano aktivieren	III – 309
III.11.8.1. Zertifikat mit acme.sh beantragen	III – 309

Kapitel III.1. USV

III.1.1. Sinn und Zweck der USV

Selbstverständlich gehört zu jedem vernünftigen Serversystem eine unterbrechungsfreie Stromversorgung (kurz USV bzw. im englischen UPS = uninterruptable power supply).

Die USV schützt den Server vor Überspannungen und Schwankungen im Stromnetz und versorgt den Server auch bei kurzzeitigem Stromausfall mit Energie. Eine USV ist dabei zunächst nicht viel mehr als eine Batterie mit etwas zusätzlicher Elektronik. Über ein Kabel zwischen USV und Server (seriell oder usb) teilt die USV dem Server bestimmte Ereignisse mit. Auf dem Server ist eine Softwarekomponente dafür verantwortlich, dass die Informationen und Ereignisse (z.B. Stromausfall) der USV entgegengenommen und entsprechende Maßnahmen (z.B. Server wird heruntergefahren) eingeleitet werden.

III.1.2. Geeignete Modelle

Grundsätzlich geeignet und vielfach im Einsatz sind verschiedene Modelle des Herstellers APC. Durch die sehr große Verbreitung der Modelle dieses Herstellers ist auch ein OpenSource-Projekt (<http://www.apcupsd.org>) entstanden, das die entsprechende Software auf Serverseite entwickelt und bereitstellt. Mit apcupsd steht eine entsprechend gut funktionierende Komponente zur Verfügung, die auch Bestandteil des LogoDIDACT-Server ist. Im Folgenden wird anhand eines Beispiels beschrieben, wie die Konfiguration auf Serverseite erfolgen muss, um ein USV-Modell per USB-Kabel anzusprechen.

III.1.2.1. APC Smart-UPS SMX750i oder SMX1000i

Das Modell SMX750i ist als Basismodell für die meisten Server geeignet und passt auch für Server mit redundantem Netzteil. Wer aufgrund seiner Serverdimensionierung mehr Leistung oder Reserven benötigt, sollte eine größere Variante verwenden, wie z.B. das Modell SMX1000i. Die Modellserie kann sowohl als Standgerät als auch für den Rackeinbau verwendet werden. Der Anschluss zwischen USV und Server erfolgt in der Regel über das beiliegende USB-Kabel.

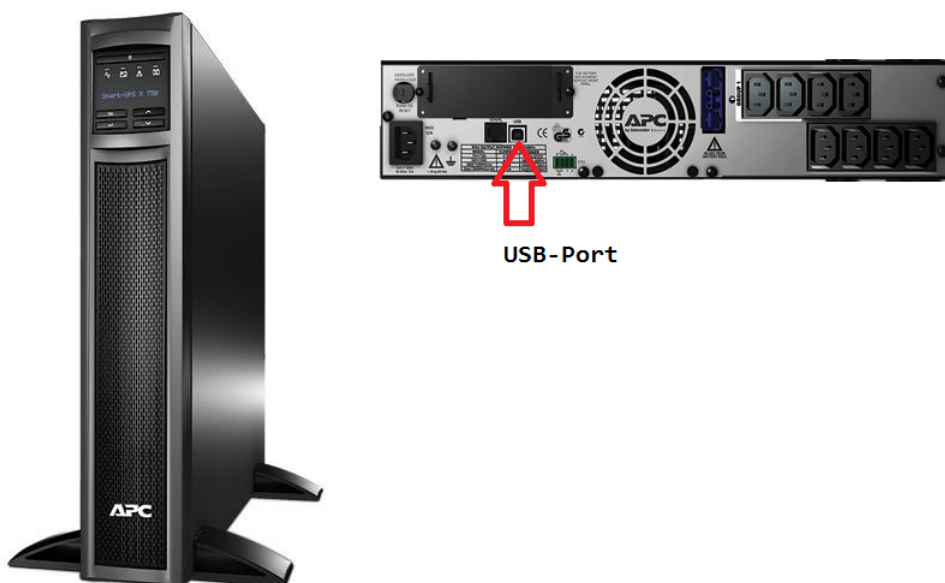


Abbildung III.1.1. Vorder- und Rückseite der Smart-UPS SMX750i

III.1.2.1.1. Installation des Serverdienstes apcupsd am Idhost

Zunächst wird der Serverdienst apcupsd auf Serverseite installiert über den folgenden Befehl: **apt-get install apcupsd** Der Dienst bzw. Daemon wird dadurch noch nicht gestartet. Dies erfolgt erst, nachdem man die Verbindung zwischen USV und Server konfiguriert hat.

III.1.2.1.2. Konfiguration für Betrieb über USB oder serielles Kabel

Wenn man direkt am Server steht, sieht man natürlich, ob und wie die USV am Server angeschlossen ist. Die einfachste und am häufigsten verwendete Variante ist über USB aber auch seriell ist möglich, sofern der Server über eine serielle Schnittstelle verfügt.

Die Konfiguration der Verbindung erfolgt über die Datei `/etc/apcupsd/apcupsd.conf`.

III.1.2.1.2.1. Konfiguration für USB-Verbindung

Wenn man per Fernwartung auf dem Server eingewählt ist und prüfen möchte, ob die USV per USB-Kabel am Server hängt, kann man dazu den Befehl **lsusb** verwenden. Anhand der Ausgabe und Herstellerbezeichnung kann man erkennen, ob eine USV per USB-Kabel angeschlossen ist:

```
Bus 002 Device 002: ID 8087:8002 Intel Corp.
Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 003 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
Bus 001 Device 002: ID 8087:800a Intel Corp.
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 005 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 004 Device 004: ID 051d:0003 American Power Conversion UPS
Bus 004 Device 003: ID 0461:4e29 Primax Electronics, Ltd
Bus 004 Device 002: ID 0424:2660 Standard Microsystems Corp. Hub
Bus 004 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
```

1. Öffnen Sie die Datei `/etc/apcupsd/apcupsd.conf` und passen Sie die folgenden Wert entsprechend auf die Kommunikation über USB an:

```
...
UPSCABLE usb
```

```
...
UPSTYPE usb
```

```
DEVICE
...
NISIP 0.0.0.0
```

2. In `/etc/default/apcupsd` den Wert `ISCONFIGURED` von `no` auf `yes` stellen

```
ISCONFIGURED=yes
```

3. Den Dämon apcupsd starten `/etc/init.d/apcupsd start`

4. Testen, ob Kommunikation funktioniert

```
apcaccess
```

Falls alles ok ist mit der Verbindung, dann sieht die Ausgabe in etwa wie folgt aus:

```
APC      : 001,027,0663
DATE     : 2019-02-11 17:31:15 +0100
HOSTNAME : ldhost
VERSION  : 3.14.12 (29 March 2014) debian
UPSNAME  : ldhost
CABLE    : USB Cable
MODEL    : Smart-UPS X 750
...
END APC  : 2019-02-11 17:31:30 +010
```

III.1.2.1.3. Installation und Konfiguration auf dem logosrv

Damit im so genannten ITB-Interface die Logs der USV per Browser angezeigt werden, ist es unter LogoDIDACT 2.0 erforderlich, dass der Deamon apcupsd auch im logosrv installiert und konfiguriert wird.

Wechseln Sie in den Container logosrv und installieren Sie dort das Paket für den Serverdienst apcupsd:

```
lxc-ssh -n logosrv
```

```
apt-get install apcupsd
```

Öffnen Sie die Datei `/etc/apcupsd/apcupsd.conf` und prüfen bzw. ändern Sie die folgenden Werte auf die Kommunikation über Netzwerk:

```
...
```

```
UPSTYPE net
```

```
DEVICE ldhost:3551
```

```
...
```

```
NETSERVER on
```

```
NISIP 127.0.0.1
```

```
NISPORT 3551
```

Öffnen Sie die Datei `/etc/default/apcupsd` und setzen Sie den Wert `ISCONFIGURED` von `no` auf `yes`, wie bereits auf dem ldhost durchgeführt. Starten Sie danach den Daemon apcupsd:

```
/etc/init.d/apcupsd start.
```

Sobald die Dienste im ldhost und logosrv installiert und richtig konfiguriert sind, funktioniert die Log-Ausgabe im ITB-Interface.

The screenshot shows a web browser window with the address bar displaying `https://itb/?view_ups_log`. The page header includes the logoDIDACT logo and the text "ITB Administrationsoberfläche". A navigation menu contains the following items: Benutzer, Server, Drucker, Webfilter, Virens Scanner, Diagnose, and Logs. The main content area is titled "USV Log" and displays the following text:

```
-- Aktueller Status --
APC      : 001,019,0490
DATE    : Tue Feb 12 11:56:01 CET 2019
        : HOSTNAME : logosrv
        : RELEASE  : 3.14.2
VERSION : 3.14.2 (15 September 2007) debian
        : UPSNAME  : logosrv
        : CABLE    : Custom Cable Smart
        : MODEL    : NETWORK UPS Driver
        : UPSMODE  : Net Slave
STARTIME: Tue Feb 12 11:55:56 CET 2019
STATUS  : COMMLOST
MBATTCHG : 5 Percent
MINTIMEL : 3 Minutes
MAXTIME  : 0 Seconds
        : NUMXFERS : 0
TONBATT  : 0 seconds
CUMONBATT: 0 seconds
        : XOFFBATT : N/A
STATFLAG : 0x07000100 Status Flag
END APC  : Tue Feb 12 12:00:05 CET 2019
```

At the bottom of the page, there is a copyright notice: © 2008 SBE network solutions GmbH.

Kapitel III.2. Backup

Selbstverständlich gehört zu jedem Serversystem auch die regelmäßige und vollautomatisierte Sicherung der Benutzer- und Systemdaten. In LogoDIDACT gibt es auch dafür vordefinierte und praxistaugliche Lösungen, die sich zudem an das jeweilige Sicherungsbedürfnis anpassen lassen.

III.2.1. Backup Konzept in LogoDIDACT

Das Backup-Konzept in LogoDIDACT sieht insgesamt drei verschiedene Sicherungsmöglichkeiten vor, die je nach Sicherheitsanforderung der Schule ausgewählt und kombiniert werden können:

- Sicherung auf interne zusätzliche Festplatte
- Sicherung auf externe USB-Platte
- Sicherung über Netzwerk auf externes Speichergerät (NAS = network attached storage)

Die Sicherung der Daten auf eine oder mehrere interne Festplatten oder/und eine oder mehrere externe USB-Platten ist die einfachste und kostengünstigste Variante und im Gegensatz zur "klassischen" Sicherung auf einem Bandlaufwerk auch deutlich schneller.

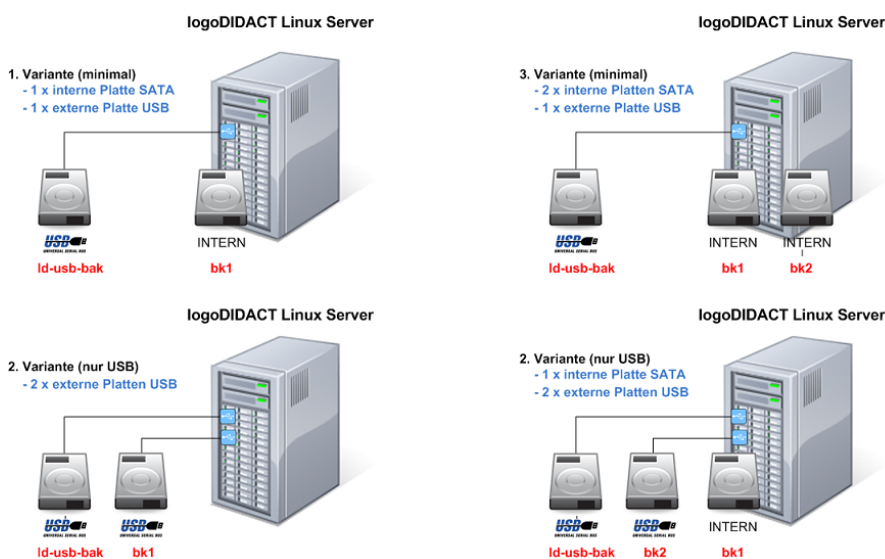


Abbildung III.2.1. Verschiedene Varianten mit internen und USB-Backup-Platten

Die Sicherungsplatten erhalten dabei je nach Funktion bestimmte Labels, d.h. fest definierte Bezeichnungen, die über entsprechend vordefinierte Skripte zum Backup genutzt werden. Entscheidend ist dabei also nicht, ob eine Platte extern oder intern angeschlossen ist, sondern welche Bezeichnung (Label) die Platte besitzt.

Tabelle III.2.1. Bezeichnung und Funktion verschiedener Backup-Medien in LogoDIDACT

Label	Funktion
bk1	Dauerhaft angeschlossene erste Backup-Platte (intern oder USB)

Label	Funktion
bk2	Dauerhaft angeschlossene zweite Backup-Platte (intern oder USB)
LD-USB-BAK	Nur temporär für den Zeitraum der Sicherung angeschlossene USB-Backup-Platte

III.2.1.1. Art und Ablauf der Sicherung

Jeden Dienstag-Samstag wird abends um 22 Uhr ein kompletter Snapshot aller Daten vorgenommen. Dabei werden jedoch nur die Daten übertragen, die sich seit dem letzten Snapshot geändert haben, das ganze ist daher sehr platzsparend und zeiteffizient. Ein kompletter Snapshot dauert, auch bei voller Platzauslastung der Festplatte, selten mehr als eine Stunde. Jeder Snapshot ist dabei jedoch in sich konsistent, d.h., im Falle eines Systemcrashes liesse sich das komplette System wiederherstellen, indem man einfach den Inhalt des jeweils letzten Snapshots zurückkopiert.

III.2.1.2. Zeitplan für Sicherungen in LogoDIDACT

Das Backup erfolgt standardmäßig jede Nacht von Montag bis Freitag um 22 Uhr. Wenn es nur eine Backupfestplatte (bk1) gibt, wird an jedem Tag ein Snapshot darauf erzeugt. Falls auch eine zweite Festplatte existiert, wird auf bk1 Montags, Mittwochs und Freitags ein Snapshot erzeugt und auf bk2 Dienstags und Donnerstags.

Die Zeiten können bei Bedarf im **ldhost** in `/etc/cron.d/backup` angepasst werden.

Es werden jeweils die letzten 20 Snapshots auf jeder Festplatte vorgehalten, wodurch man bei „BK1“ auf die letzten 6-7 Wochen und „BK2“ auf die letzten zehn Wochen täglicher Systemsicherungen zurückgreifen kann. Treten bei einer Sicherung Fehler und Warnungen auf, werden diese per eMail an den Serveradministrator gesandt.

III.2.1.3. Benachrichtigung über durchgeführte Sicherungen

Am Ende einer Sicherung erhält der Administrator eine Mail-Benachrichtigung mit Informationen zum durchgeführten Backup. Darin enthalten sind Infos zur Dauer des Backups und der Gesamtgröße der aktuellen Sicherung. Ebenso wird aufgeführt ob es Fehler gab und in einer Übersicht werden jeweils die 50 größten Dateien angezeigt die verändert wurden oder neu hinzugekommen sind.

```

[ldbackup] Backup 'daily_bk2' - OK
logoDIDACT Backup [admin@schule.local]
Gesendet: Di 02.04.2013 22:08
An: admin@schule.local

                                Snapshot 2013-04-02,22-07-49
                                =====

Dauer: 6m29s
Neue Daten: 1.26GB
Durchsatz: 4.27MB/s (Faktor: 49.81)
Gesamtgroesse des Snapshot: 62.90GB
Exit Status: 0
Anzahl der Warnungen: 0
Anzahl der Fehler: 0
Vorhandene Snapshots: 20

                                50 groesste Aenderungen
                                =====

535.74MB var/lib/mysql/logodb/surflog.MYI
410.84MB var/lib/mysql/logodb/surflog.MYD
65.75MB var/backup/mysql/logodb.sql.gz
62.31MB var/lib/clamav/dailv.cid
...

                                50 neue Dateien
                                =====

1.33MB var/log/sysstat/sar30
1.33MB var/log/sysstat/sar29
1.33MB var/log/sysstat/sar28
1.33MB var/log/sysstat/sar01
...

                                50 geaenderte Dateien
                                =====

535.74MB var/lib/mysql/logodb/surflog.MYI
410.84MB var/lib/mysql/logodb/surflog.MYD
65.75MB var/backup/mysql/logodb.sql.gz
62.31MB var/lib/clamav/daily.cid
...

```

Abbildung III.2.2. Benachrichtigung per Mail über durchgeführte Datensicherung

III.2.1.4. Dateien, die nicht gesichert werden

In der Datei `/etc/logodidact/backup.exclude` im **Ldhost** werden Dateien und Ordnerstrukturen aufgeführt, die nicht in die Datensicherung mit einbezogen werden. Neben dem Quarantäneverzeichnis für vermeintliche virenverseuchte Dateien, gehören dazu vor allem auch Log-Dateien:

```

...

/backup/*
/bd/*
/home/install/*
/var/quarantine/*
/var/spool/squid/*/*/*
/var/spool/logodidact/virus-scan/*

...

# Wechseldatentraeger, AutoMounter
/cdrom/*
/floppy/*
/media/*
/var/autofs/*/*
/mnt/*

# Temporaere Dateien
/tmp/*
/var/tmp/*

```

```

/proc/*

# Alte Logdateien
/var/log/*.gz
/var/log/*.old
/var/log/*.[0-9]
/var/log/**/*.*gz
/var/log/**/*.*old
/var/log/**/*.*[0-9]

```

Log-Dateien, die z.B. komprimiert sind (*.gz), landen somit nicht in der Datensicherung. Welche Dateien dies sind, lässt sich maßgeblich durch logrotate bestimmen (siehe Abschnitt III.4.13, „Log-Dateien“).

III.2.1.5. Internet-Surfdaten aus dem Backup ausschließen

Um auch die Internet-Surfdaten in der Datenbank aus der Sicherung auszuschließen, muss die Datei `/etc/logodidact/backup.exclude` um den folgenden Eintrag ergänzt werden, sofern nicht bereits vorhanden:

```
/var/lib/mysql/logodb/surflow*
```

III.2.1.6. Art und Anzahl der Sicherungen festlegen (Backup-Rotation)

In der Datei `/etc/logodidact/backup.conf` ist nicht nur festgelegt, wie die Backupplatten im System heißen (bk1, bk2 usw.), sondern auch, die Art und Anzahl der Backups festlegen. Der Parameter *MaxSnapshots* mit dem Standardwert 20 legt fest, wie viele Sicherungen erstellt werden, bevor die älteste Sicherung überschrieben wird. Über diese so genannte Rotation der Backups lässt sich also auch das Thema Datenschutz auf den Bereich der Datensicherung sehr genau und gezielt anwenden und anpassen.

Alternativ dazu, kann man den Parameter *MinSpaceLeft* verwenden, über den man den freien Platz definiert, der mindestens auf der Sicherungsplatte vorhanden sein muss, bevor ein Backup beginnt. Steht der Wert *MinSpaceLeft* z.B. auf *15G* wird geprüft, ob auf der Platte noch 15G frei sind. Falls nicht, wird das älteste Backup gelöscht und dann wieder geprüft, ob genug Platz ist. Das passiert so lange, bis die notwendigen 15 GB frei sind. Dann wird eine Sicherung durchgeführt. Über diesen Parameter kann man also nicht die exakte Anzahl an Sicherungen festlegen, dafür aber die gesamte Sicherungsplatte optimal ausnutzen und die maximale Anzahl an Sicherungen (für diese Plattengröße) erreichen.

Jeder der beiden Parameter hat also je nach Anforderungen und Ziel gewisse Vorteile und kann für jede einzelne Platte separat konfiguriert werden.

III.2.2. Backupfestplatte neu initialisieren

Um nächtliche Backups anzulegen, formatieren Sie zunächst die Partition einer Backupfestplatte mit dem Dateisystem EXT3 und versehen diese mit dem Label bk1.

Erstellen Sie dann auf der Partition ein Verzeichnis `snapshot`. Sie können einer zweiten Backupfestplatte das Label bk2 vergeben, dann werden die Backups abwechselnd auf die eine oder andere Festplatte vorgenommen (mit Ausweichmöglichkeit auf die jeweils andere, falls eine der beiden einmal nicht verfügbar ist).

Nachdem Sie die Partition formatiert haben, sollten Sie den Server neu starten, damit der Kernel das Label erkennt. Die Festplatte wird dann automatisch lesend eingebunden, wenn Sie nach `/backup/bk1` wechseln.

Im Beispiel wird angenommen, dass die Backupfestplatte mit dem Gerätenamen `/dev/sdx` angesprochen wird. Sie können den genauen Gerätenamen für Ihre Installation über den Befehl **fdisk -l** ermitteln.

1. Erstellen Sie eine Partition über die gesamte Backupfestplatte

```
echo '0' | sfdisk /dev/sdx
```

2. Formatieren Sie die Partition mit dem Dateisystem EXT3 und vergeben Sie das Label bk1 oder bk2

```
mkfs.ext3 -L [ bk1 | bk2 ] /dev/sdx1
```

```
mkfs.ext3 -L bk1 /dev/sdx1
```

3. Passen Sie die EXT3 Dateisystem Parameter für die Partition an

```
tune2fs -i0 -c0 /dev/sdx1
```

4. Legen Sie das `snapshot` Verzeichnis an

```
mount /dev/sdx1 /mnt
```

```
mkdir /mnt/snapshot
```

```
umount /mnt
```

5. Führen Sie `partprobe` aus oder starten Sie den Server neu

```
partprobe
```

Der Befehl veranlasst den Kernel dazu, die Partitionstabelle komplett neu einzulesen. Falls das funktioniert, können Sie nun die Platte über das Label ansprechen:

```
cd /backup/bk1
```

Sollte das nicht funktionieren, starten Sie den Server neu: **reboot**

6. Erstellen Sie einen manuellen Snapshot `daily_bk1` oder `daily_bk2` (optional)

```
ldsnapshot [ daily_bk1 | daily_bk2 ]
```

```
ldsnapshot daily_bk1
```



Tipp

Sie können auch eine Partition einer USB-Festplatte mit dem Label `LD-USB-BAK` versehen, dann wird sofort ein Backup angelegt, wenn Sie die Festplatte anstecken (durch Pieptöne bzw. eine Melodie bei Start und Ende angezeigt).

III.2.3. "Hot-Plug" Sicherung über LD-USB-BAK

Der Sinn und Zweck der Hot-Plug-Sicherung auf eine externe USB-Platte besteht vor allem darin, dass man die Sicherung des gesamten Servers an einem anderen Ort aufbewahren kann. Der große Vorteil dabei liegt in einem extrem guten Kosten/Nutzenverhältnis. Eine 2 TB große USB3-Festplatte liegt preislich inzwischen im Bereich 60.- bis 80.- €. Beim Kauf sollte man darauf achten, dass es sich um eine 2.5" Festplatte handelt, die ihren Strombedarf komplett über USB deckt und nicht umständlich mit einem separaten Netzteil betrieben werden muss.

III.2.3.1. USB-Platte für Hot-Plug neu einrichten

Die Einrichtung einer externen USB-Platte für die "Hot-Plug"-Sicherung ist denkbar einfach und ähnlich, wie bereits zuvor für eine interne Backplatte bk1 oder bk2 beschrieben.

Deshalb hier nur die Kurzform (Platte sdx wie zuvor mit **fdisk -l** ermitteln):

1. **echo '0' | sfdisk /dev/sdx**
2. **mkfs.ext3 -L LD-USB-BAK /dev/sdx1**
3. **tune2fs -i0 -c0 /dev/sdx1**
4. Verzeichnisstruktur

Im Gegensatz zu der Sicherung auf interne Backupgeräte ist das manuelle Erstellen von Ordnern beim Hot-Plug-Backup nicht notwendig. Die Ordner **snapshot** und **lost+found** werden beim Ausführen des Sicherungsskriptes automatisch erstellt, sofern sie nicht vorhanden sind.

5. Hot-Plug-Sicherung starten

Um die Sicherung auf die USB-Platte sofort zu starten gibt es zwei Möglichkeiten. Wenn man vor Ort ist, kann man die USB-Platte kurz abziehen und wieder einstecken. Wenn man die Konfiguration der USB-Platte per Fernwartung einrichtet, kann man die Erkennung der Platte durch Eingabe des Befehls **partprobe** erzwingen. In beiden Fällen wird das Skript für das Hot-Plug-Backup geladen und die Sicherung angestoßen.



Achtung

Unter LogoDIDACT 2.0 können Sie aus dem Host heraus das Backup durch den folgenden Befehl **udevadm trigger -s block -s scsi -c add -y sdx1** anstoßen, wobei x wieder durch den entsprechenden Buchstaben des Geräts zu ersetzen ist.

III.2.3.2. Sicherung mit USB Hot-Plug durchführen

Die Durchführung der Sicherung ist noch einfacher als die Einrichtung und besteht nur darin, die Platte am Server anzuschliessen, die Sicherung laufen zu lassen und die Platte später gegebenenfalls wieder abzuklemmen.



Abbildung III.2.3. Hot-Plug-Backup auf 2.5 Zoll USB-Platte mit Sicherheitscode



Wichtig

Der Ablauf bei der Sicherung ist wie folgt:

1. USB-Platte am Server mit USB-Kabel verbinden

Der Server erkennt die Platte (`/etc/udev/rules.d/55-usb-backup.rules`), prüft diese auf das Label "LD-USB-BAK" und ruft das Backup-Script `/home/bin/usb_snapshot` auf.

2. Sofern ein CD-ROM-Laufwerk vorhanden ist, bekommt dieses das Signal, die Schublade auszufahren und wieder einzuziehen, so dass man eine optische Rückmeldung hat.
3. Sofern am Server ein Lautsprecher vorhanden ist, wird der Anfang der Melodie "für Elise" ausgegeben.
4. Die Sicherung wird gestartet.
5. Wenn die Sicherung fertig ist, wird das Laufwerk (sofern vorhanden) ausgefahren, so dass man wiederum eine optische Rückmeldung für das Ende der Sicherung vorliegen hat.
6. Das Ende der Melodie "für Elise" wird ausgegeben.
7. Das Laufwerk wird nicht mehr automatisch eingezogen, sondern muss manuell eingeschoben werden. Diese Aufgabe soll zusammen mit dem Abklemmen der USB-Hot-Plug-Sicherung erfolgen.
8. Am Ende der Sicherung erhält der Administrator eine Mail mit Informationen zum durchgeführten Backup.

Hinsichtlich der Anzahl an USB-Backupplatten gibt es keine Einschränkung, d.h. man kann mehreren USB-Platten das gleiche Label **LD-USB-BAK** geben. Damit kann man z.B. eine noch höhere Sicherheit erreichen, indem man 2 Platten wechselseitig verwendet und für gerade oder ungerade Kalenderwochen verwendet.

Neben dem preislichen Vorteil der USB-Platten, gibt es vor allem auch im Falle der Wiederherstellung deutliche Vorteile gegenüber der Sicherung z.B. auf einem NAS-Laufwerk.

III.2.3.3. USB Hot-Plug im Monitoring überwachen

Um auch die Sicherung auf USB-Platte zu überwachen, muss man dies im Monitoring explizit aktivieren. Zunächst muss der Check für die Prüfung über den Befehl **ldintsall ld-usb-backup** installiert werden. Die Aktivierung erfolgt anschliessend über **icingactl enable ld-usb-backup**. Nähere Infos dazu finden sich im ????



Tipp

Sofern man ein so genanntes Hot-Plug-Backup einrichtet, sollte man die Sicherung alle 30 spätestens aber alle 60 Tage durchführen. Das Plugin im Monitoring verwendet diese Werte, um Sie entsprechend zu informieren. Wenn Sie die USB-Platte länger als 30 Tage nicht anschliessen, erhalten Sie den Status "Warning", bei mehr als 60 Tagen wechselt der Status zu "Critical".

III.2.4. Sicherung des Auslieferungszustandes

Neben der Methode der Sofortsicherung z.B. über das Anstecken einer USB-Platte oder der zyklischen Sicherung mit Rotation, gibt es selbstverständlich auch die Möglichkeit einer Grundsicherung bzw. Sicherung eines beliebigen Zustandes.

Gerade dann, wenn man keine zusätzliche Sicherung über USB als Zustand speichert, führt der Mechanismus der Backup-Rotation zwangsweise dazu, dass der älteste Backupzustand irgendwann überschrieben wird. In der Regel kann man auch aus datenschutzrechtlichen Gründen dann nur auf Backups zugreifen, die 30 Tage oder weniger in der Vergangenheit liegen.

Über das ITB-Interface (Menü Server) erfolgt auch ein Hinweis, ob ein Backup eines Auslieferungszustand erfolgt ist oder nicht.

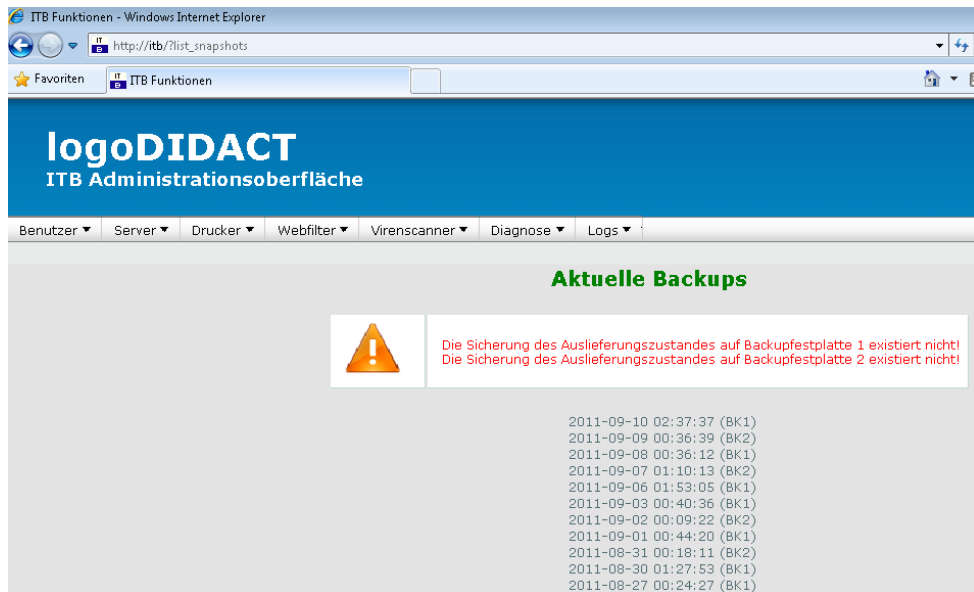


Abbildung III.2.4. Anzeige der Backups im ITB-Interface ohne Sicherung des Auslieferungszustandes

Über folgende Befehle lässt sich ein beliebiges Backup als Auslieferungszustand ablegen, so dass dieses nicht durch den Mechanismus der Rotation überschrieben wird.

```
cd /backup/bk1
mount -o remount,rw /backup/bk1
mv snapshot/DATUM_DES_SNAPSHOTS auslieferung
cd
umount /backup/bk1
```

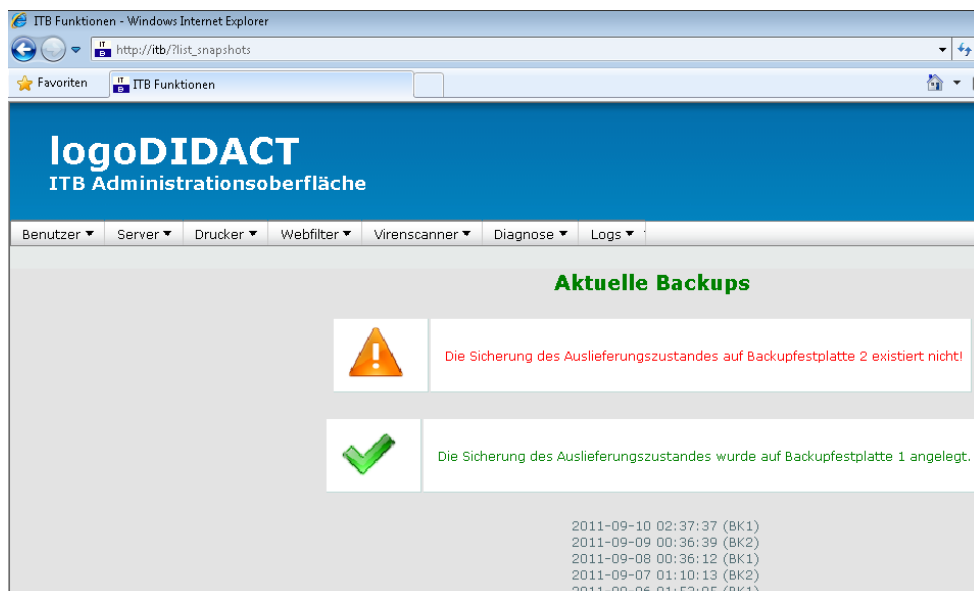


Abbildung III.2.5. Sicherung des Auslieferungszustandes auf BK1 im ITB-Interface vorhanden

III.2.5. Technischer Ablauf des Backups und mögliche Probleme

Aus Anwendersicht hat man bei jeder Sicherung in LogoDIDACT den gesamten Zustand des Servers und damit ein Kompletbackup. Auf technischer Ebene wird das Ganze aber sehr effizient über so genannte Hardlinks realisiert. Wenn ein Backup erzeugt wird, werden zuerst Links auf den jeweils vorhergehenden Snapshot angelegt. Vereinfacht ausgedrückt, können beliebig viele "harte Links" auf ein und dieselbe Datei verweisen. Solange sich diese Datei nicht ändert, wird in der Datensicherung auch bei einer Vollsicherung dafür also auch kein zusätzlicher Platz benötigt. Damit ist die Sicherung schnell und extrem speicherplatzeffizient. Zudem hat man zu jeder Zeit den kompletten Zustand des Servers in der Sicherung.

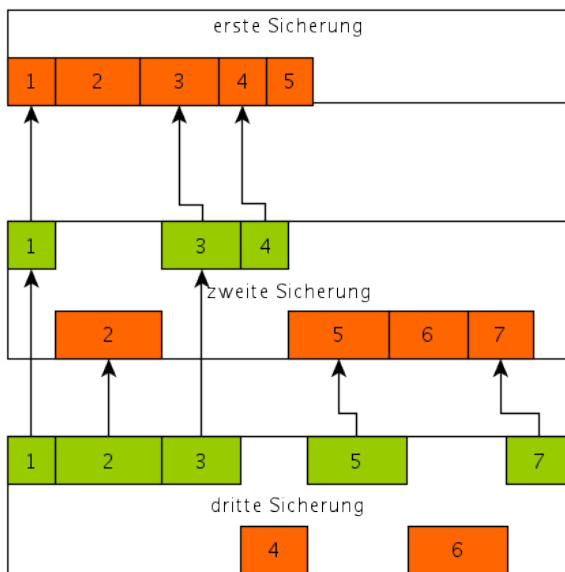


Abbildung III.2.6. Backup in LogoDIDACT über Hardlinks

Bild-Quelle <http://www.tralios.de/Managed-Server/Datensicherung/hardlink-backup.png>

Das Erzeugen von Hardlinks kann dann zu Problemen führen, wenn der Server zu voll wird und das Sicherungsmedium zu langsam reagiert, wie dies manchmal im Zusammenhang mit der Sicherung auf NAS-Laufwerken der Fall ist.

III.2.6. Backup auf NAS per iSCSI

Als NAS (Network Attached Storage) bezeichnet man ein Gerät im Netzwerk, welches über verschiedene Protokolle Speicherplatz im Netzwerk zur Verfügung stellt. Dazu gehören beispielsweise CIFS (= Windows-Freigaben), NFS (= Linux-Freigaben) und FTP.

Um das Backup eines LogoDIDACT-Server auf einem NAS-Gerät anzulegen, ist es zwingend erforderlich, dass dies per iSCSI erfolgt. Alle anderen Methoden und Protokolle sind für die zu sichernden Datenmengen zu langsam. Das entscheidende dabei ist, dass iSCSI sowohl über Gigabit als auch 10 GbE spezifiziert ist. Server in großen Umgebungen mit Hunderten Rechner verfügen in der Regel auch über 10 GbE Interfaces und entsprechende NAS-Geräte für dieses Segment ebenfalls.



Tipp

Die Sicherung auf NAS-Laufwerke ist vor allem dann sinnvoll, wenn ein zusätzliches, erhöhtes Sicherheitsbedürfnis für die Daten besteht, das man z.B. nicht täglich über die Hot-Plug-Sicherung per USB abdecken kann oder möchte.

Über die Sicherung auf ein NAS-Gerät, das sich in einem anderen Raum im Gebäude befindet, erhöht man die Sicherheit vor allem für den Fall eines Brandes im Serverraum oder den Fall des Serverdiebstahls.

III.2.6.1. Separates Netzwerkinterface für NAS einrichten

Damit die NAS nicht im normalen internen Netzwerk hängt, sondern nur direkt vom Server aus erreichbar ist, sollte diese über eine separate (physische) Netzwerkkarte in einem eigenen Netz angesprochen werden. Die Einrichtung und Konfiguration dieser Karte und des Netzwerkbereichs wäre dabei auch über Puppet möglich, jedoch mit entsprechendem Aufwand verbunden, der keine wirklichen Vorteile bietet. Deshalb wird im Folgenden die Einbindung und Konfiguration direkt im **ldhost** beschrieben.

Um eine externe Schnittstelle für den Anschluss der NAS zu konfigurieren, gehen Sie wie folgt vor:

1. Falls nötig, zusätzliche Netzwerkkarte in den Server einbauen
2. Eine Netzwerkkarte bzw. ein Interface einbinden und konfigurieren

Suchen Sie über **inxi -n** nach einem freien Netzwerkadapter und legen Sie darüber ein neues Interface an oder benennen ein vorhandenes nicht genutztes um. Detaillierte Infos dazu finden Sie in Abschnitt III.3.1, „Netzwerk-Konfiguration am Server“.

Definieren Sie einen passenden Namen wie z.B. **p_nas** über eine entsprechende Datei **80-p_nas.link**, deren Inhalt wie in folgendem Beispiel aussieht:

```
[Match]
MACAddress=98:f2:b3:e6:25:dc
[Link]
Name=p_nas
```

Damit Änderungen am Namen oder Schnittstellen übernommen werden, ist es wichtig, den folgenden Befehl auszuführen, damit das initramfs-Image neu aufgebaut wird, in welchem die Schnittstellen in Ubuntu 16.04 oder höher festgelegt sind.

update-initramfs -u

3. Netzwerkadresse für Interface definieren

Öffnen Sie im **ldhost** die Datei **interfaces** mit einem Editor Ihrer Wahl, wie z.B. Nano:

nano /etc/network/interfaces

Ergänzen Sie die Konfiguration um eine Passage, wie folgt:

```
# Interfaces für Backup direkt auf NAS
auto p_nas
iface p_nas inet static
    address 192.168.5.1
```

```
netmask 255.255.255.0
```



Achtung

Damit die Änderungen an der Zuordnung von Netzwerkschnittstellen übernommen werden, muss der Server **ldhost** neu gestartet werden!

4. Starten Sie den Server neu. Nach dem Neustart sollte die neue Schnittstelle unter dem neuen Namen verfügbar sein.

Mittels des folgenden Befehls lässt sich die Konfiguration aller Interfaces prüfen:

```
inxi -n
```

Das neue Interface prüfen Sie gezielt über:

```
ifconfig p_nas
```

III.2.6.2. Das NAS-Gerät konfigurieren

Im nächsten Schritt konfigurieren Sie Ihr Speichergerät entsprechend der Anleitung des jeweiligen Herstellers. Zu beachten ist dabei die Konfiguration im Hinblick auf iSCSI.

Für Synology ist diese Anleitung hilfreich:

```
https://www.synology.com/de-de/knowledgebase/DSM/tutorial/Virtualization/How\_to\_use\_the\_iSCSI\_Target\_service\_on\_Synology\_NAS
```

Für QNAP ist die folgende Anleitung bis zum Punkt "5. Verbindung mit einem iSCSI-Ziel mithilfe eines iSCSI-Initiators unter Windows" zu empfehlen:

```
https://www.qnap.com/de-de/how-to/tutorial/article/so-erzeugen-und-nutzen-sie-den-iscsi-zieldienst-auf-einem-qnap-turbo-nas/
```

III.2.6.2.1. Tips zur NAS-Konfiguration

Für die Grundkonfiguration Ihres NAS-Gerätes, hängen Sie dieses per Netzkabel zunächst nicht an das oben erstellte Interface **p_nas**, sondern ins interne Netzwerk.

Im internen Netzwerk bekommt das Gerät per DHCP eine IP aus dem dynamischen Bereich, d.h. im Standardfall aus dem Adressbereich 10.16.253.x. Welche Adresse das Gerät konkret bekommt, lässt sich leicht prüfen. Wechseln Sie in den Container **logosrv** und prüfen Sie die letzten log-Einträge des DHCP-Servers über folgenden Befehl:

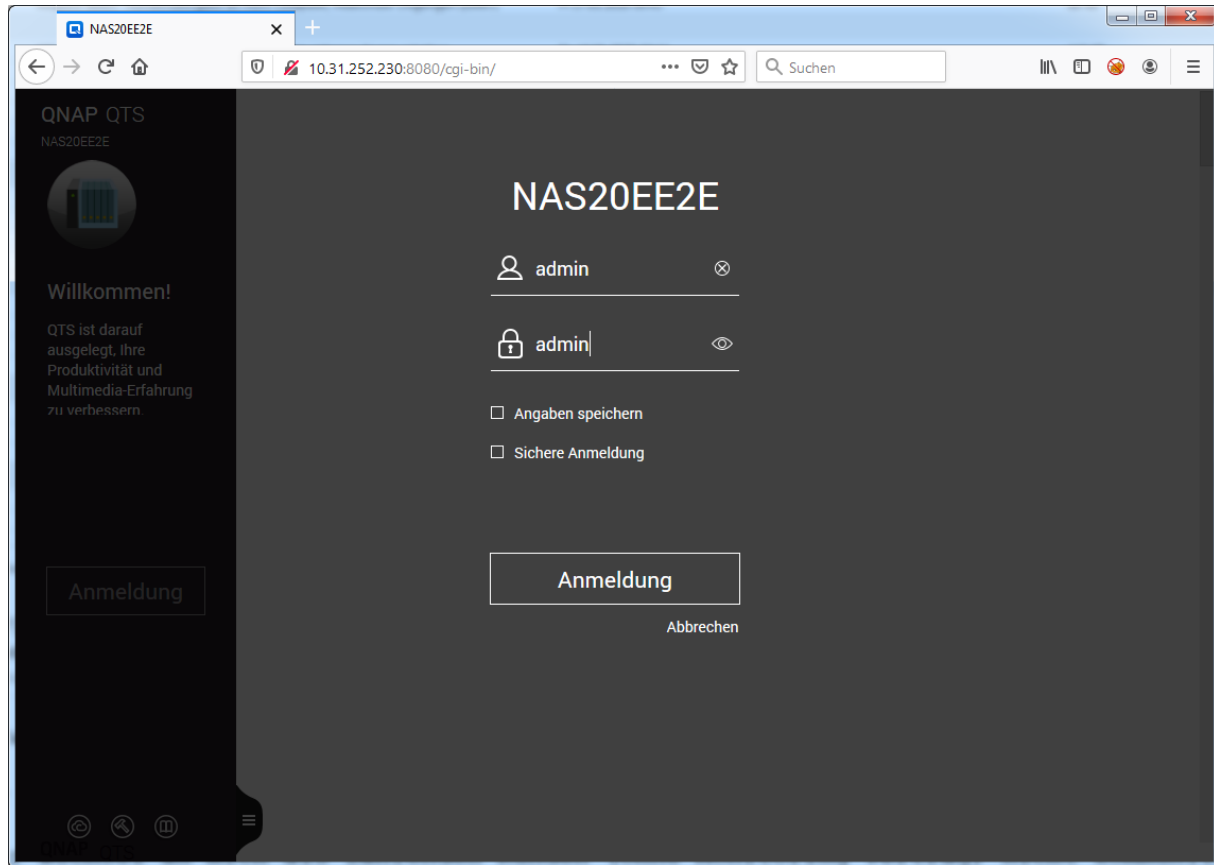
```
tail -f /var/log/dhcp.log
```

Mit der IP-Adresse gelangen Sie dann per Web-Browser auf die Konfigurationsseite Ihres NAS-Geräts.

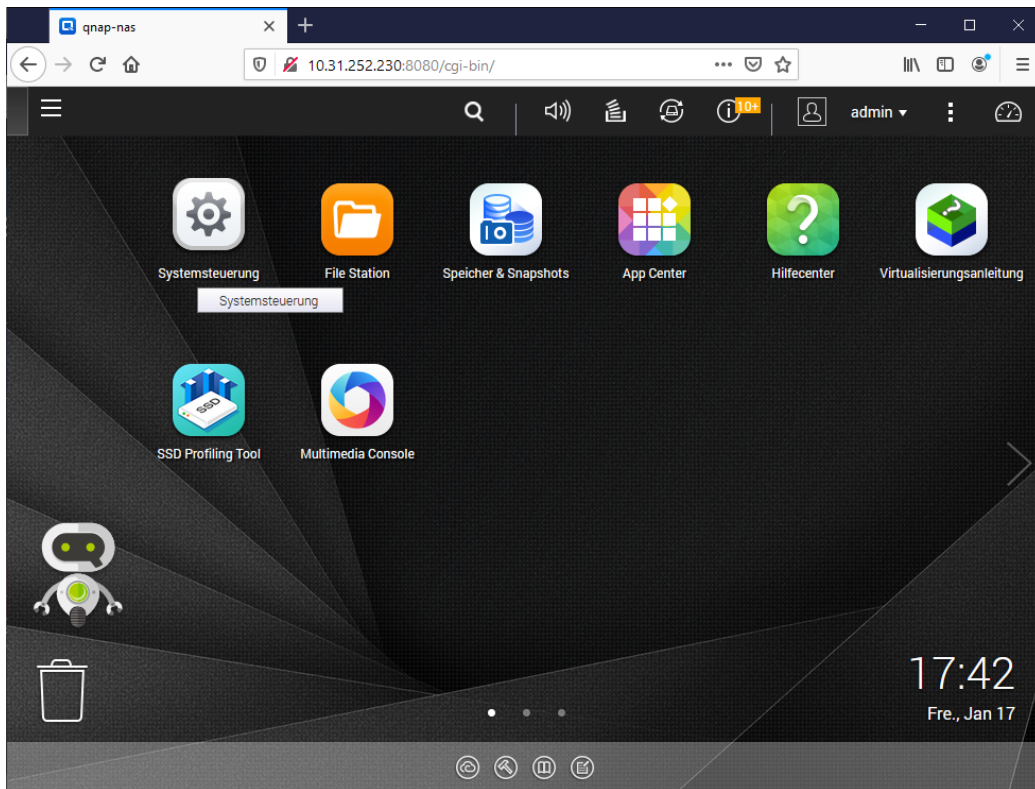
III.2.6.2.2. Konfiguration am Beispiel QNAP TS-328

Gehen Sie mit einem Webbrowser der vom Hersteller des NAS-Speichers unterstützt wird auf die oben ermittelte IP-Adresse dynamische Adresse (im Beispiel 10.31.252.230) und loggen sich dort mit dem vorgegebenen Administrator-Account ein.

Bei QNAP lautet das Standard-Kennwort für den Benutzer admin in der Regel ebenfalls **admin.** in der Regel



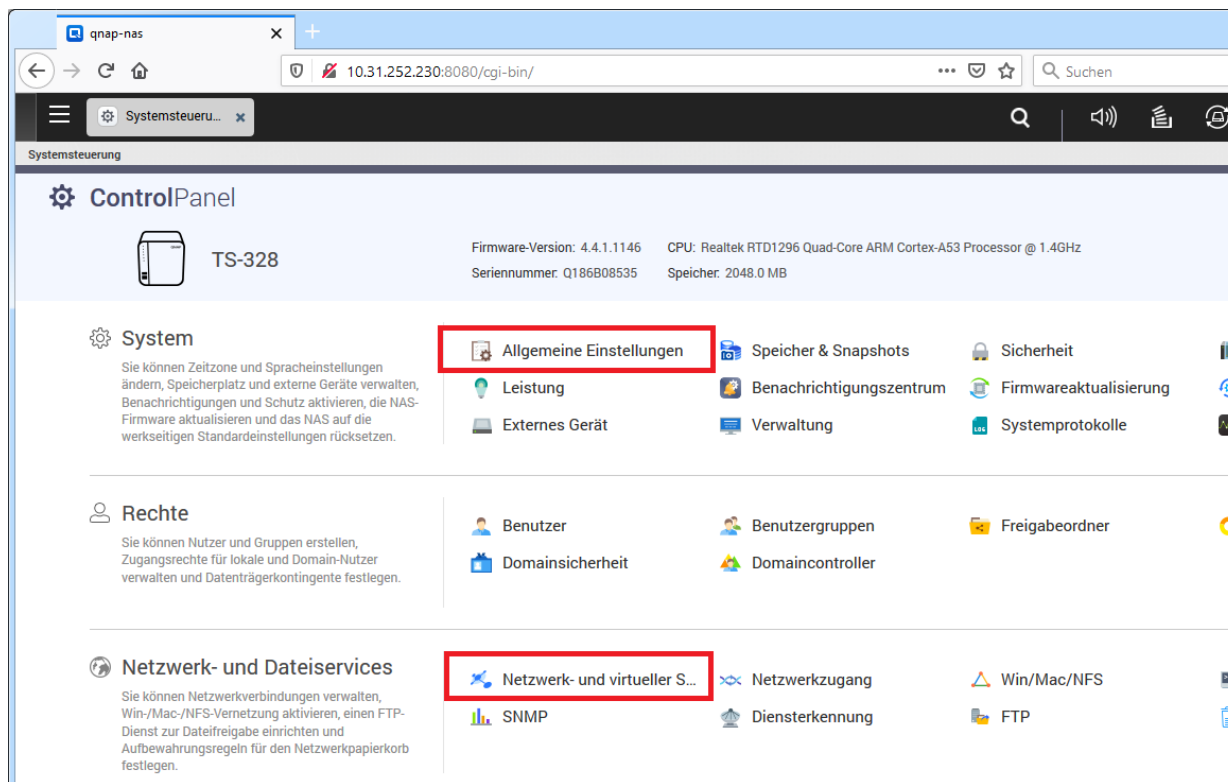
Sie sollten bzw. müssen dieses aus Sicherheitsgründen zwingend ändern. Richten Sie die NAS anschließend entsprechend Handbuch des Herstellers ein.



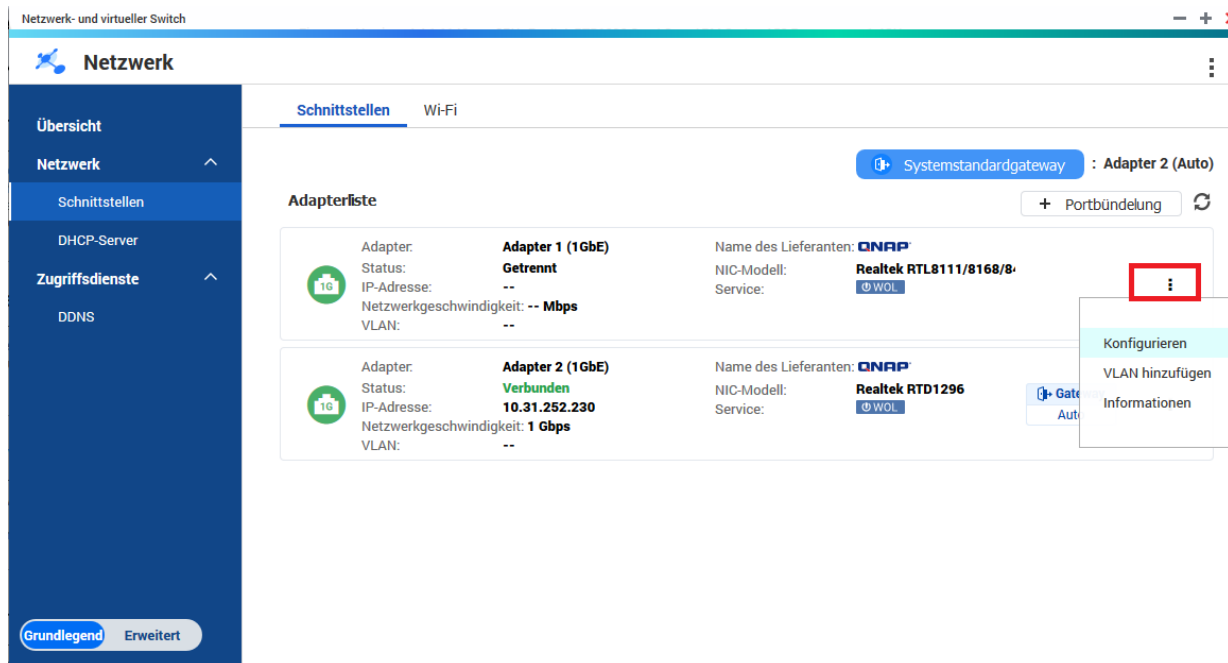
III.2.6.2.2.1. Grundkonfiguration

Über das Symbol **Systemsteuerung** gelangen Sie zum ControlPanel. Legen Sie dort zunächst über den Eintrag **Allgemeine Einstellungen** die folgenden Werte fest:

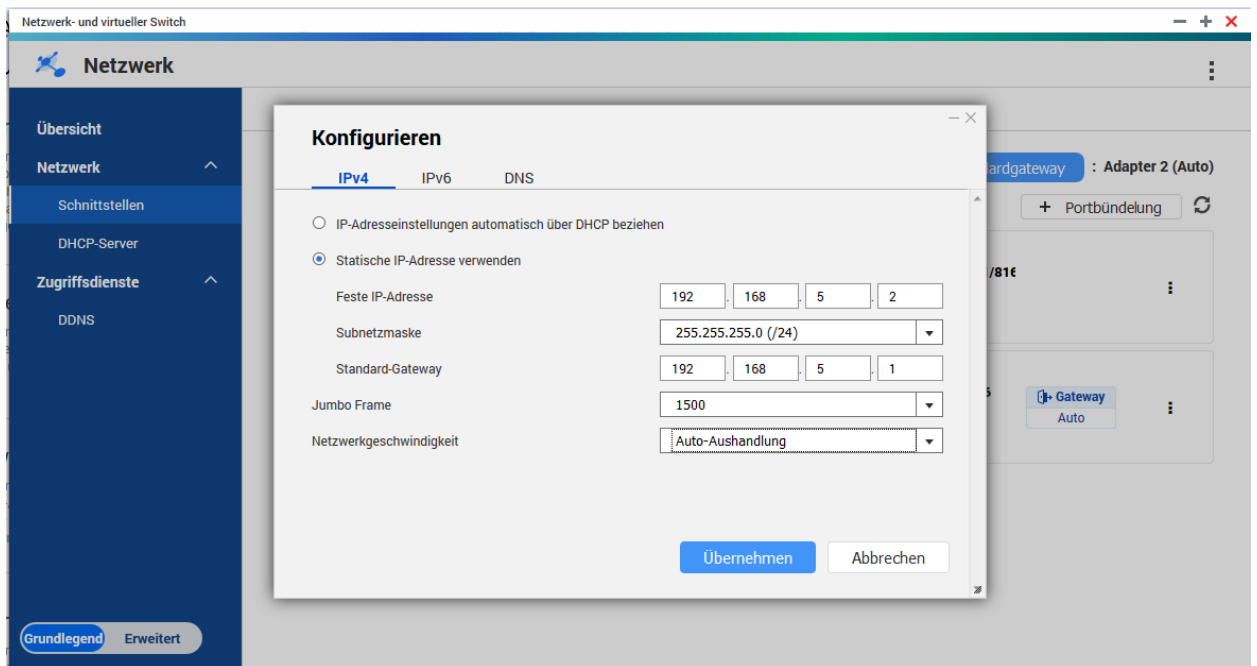
- Name des NAS-Geräts (im Beispiel qnap)
- Zeitzone (GMT + 01:00, Amsterdam, Berlin,...)



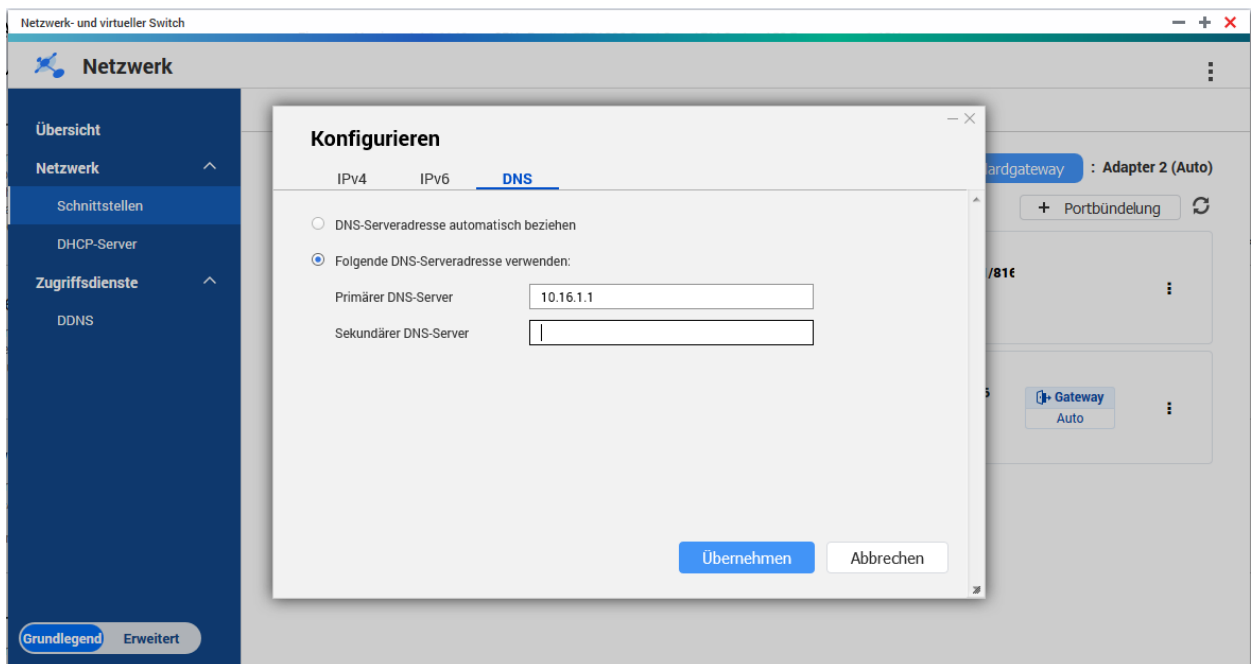
Wählen Sie danach **Netzwerk- und virtueller Switch** und legen Sie die IP-Adresse für das Interface über den Eintrag **Konfiguration** fest.



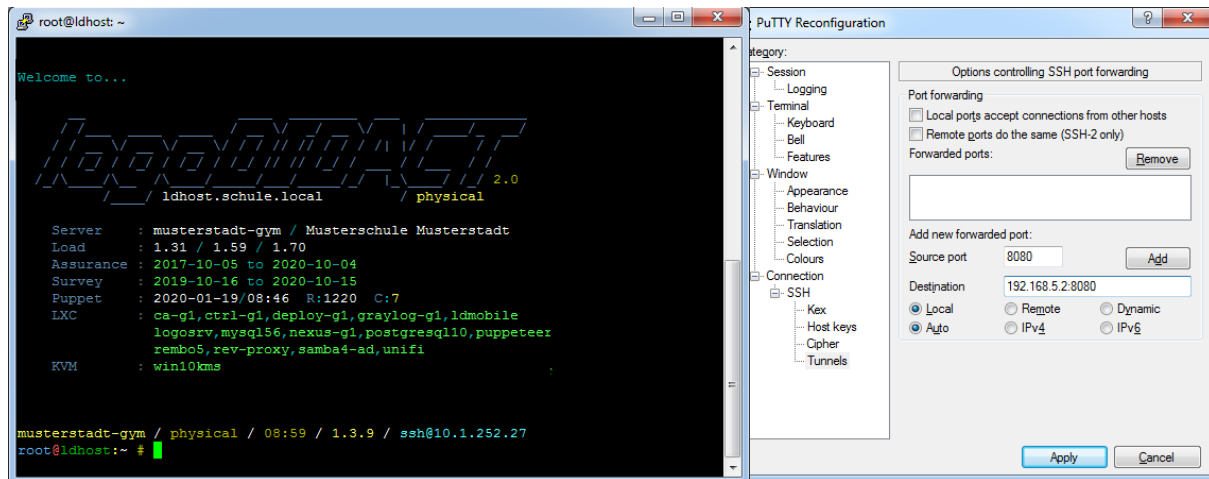
Legen Sie entsprechend des gewählten Netzwerkbereichs die IP fest z.B. auf 192.168.5.2. Deaktivieren Sie über den Reiter **IPV6** die Konfiguration für IPV6.



Geben Sie als IP des DNS-Servers die Adresse des **Logosrv** an und wählen Sie den Eintrag **Übernehmen**, damit die Einstellungen wirksam werden.



Sofern die NAS nur ein Interface hat und Sie bisher mit diesem verbunden waren, schließen Sie sich durch die Umkonfiguration in aller Regel aus. Um das Gerät von einem Client aus weiter zu administrieren, verbinden Sie sich mit dem Server und stellen Sie die Verbindung über eine Portweiterleitung her. Im gezeigten Beispiel ist das Ziel dann 192.168.5.2:8080 und über den Browser vom Client erreichbar über <http://localhost:8080>.

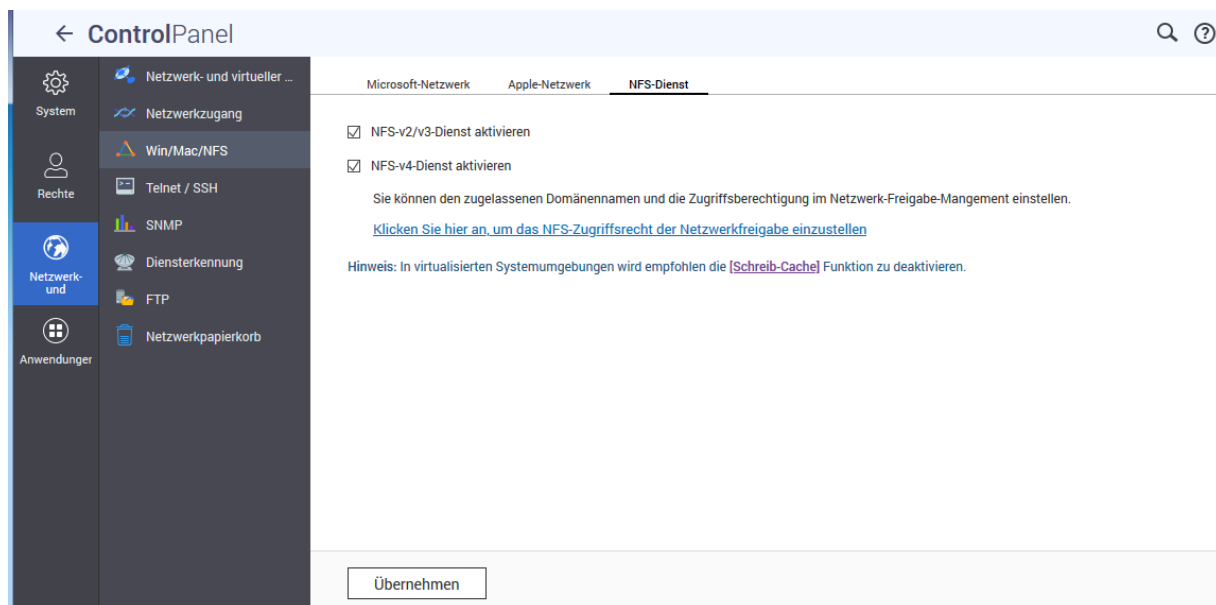


Nachdem die allgemeinen Einstellungen durchgeführt wurden, folgen die spezifischen Anpassungen.

III.2.6.2.2.2. Protokoll NFS aktivieren

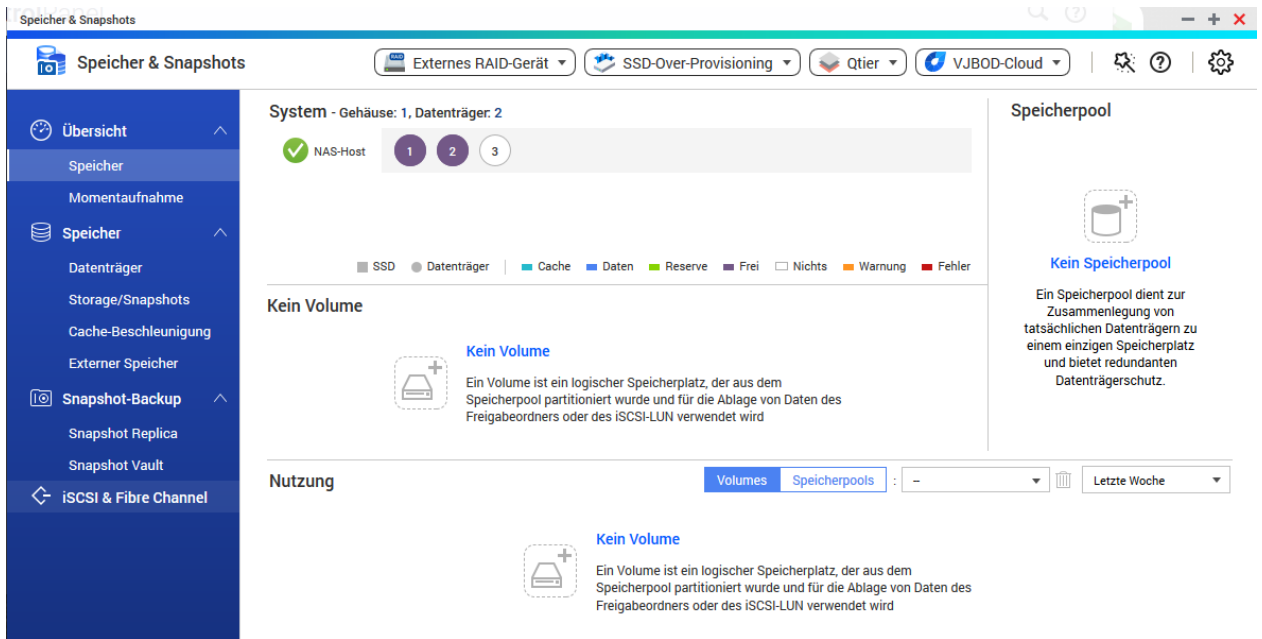
Das **Network File System**, kurz NFS, ist ein Protokoll den Zugriff auf Dateien über das Netzwerk zu ermöglichen und muss auf dem NSA-Gerät aktiviert werden. Wählen Sie den Menüpunkt **Netzwerk- und Services** und dort **Win/Mac/NFS**. Deaktivieren Sie die Dateidienste für Microsoft- und Apple Netze.

Aktivieren Sie den NFS-Dienst und klicken Sie auf **Übernehmen**.

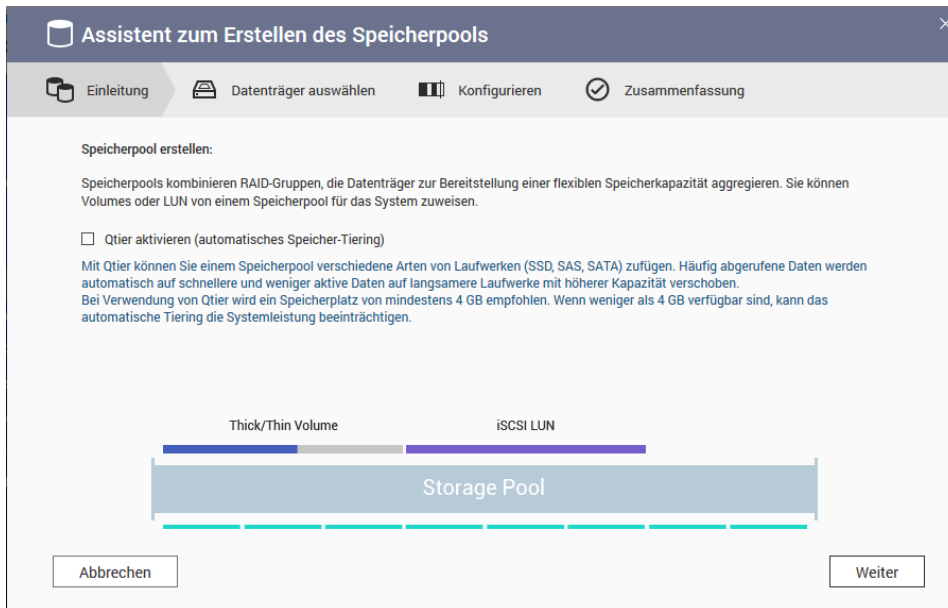


III.2.6.2.2.3. Speicherpool erstellen

Über den Menüeintrag **System** und den Menüpunkt **Speicher / Snapshots** geht es nun an die Datenträgerkonfiguration.



Erstellen Sie einen neuen Speicherpool über das "+" Symbol auf der rechten Seite.



Wählen Sie entsprechend der Anzahl der physisch vorhandenen Festplatten eine sinnvolle Konfiguration. Im Beispiel ein aus zwei jeweils 4 GB großen Platten einen RAID-1 Verbund. Klicken Sie auf **Weiter**.

Assistent zum Erstellen des Speicherpools
✕

Einleitung
Datenträger auswählen
Konfigurieren
Zusammenfassung

Datenträger auswählen und konfigurieren:

Gehäuseeinheit [insgesamt: 1 Einheit(en)]: AS-Host [verfügbare(r) Datenträger: 2/3] ▼

Sicheren SED-Speicherpool erstellen

<input checked="" type="checkbox"/>	Festplatte	Hersteller	Modell	Typ	Bustyp	Kapazität	Status
<input checked="" type="checkbox"/>	Datenträger 1	Seagate	ST4000VN00...	HDD	SATA	3.64 TB	Gut
<input checked="" type="checkbox"/>	Datenträger 2	Seagate	ST4000VN00...	HDD	SATA	3.64 TB	Gut

Ausgewählt: 2 Geschätzte Kapazität: 3.63 TB

RAID-Typ: RAID 1 ▼ Ersatzfestplatte (Hot Spare): Nichts ▼

Abbrechen
Zurück
Weiter

Übernehmen Sie den Warnschwellenwert im folgenden Dialog mit **Weiter**.

Assistent zum Erstellen des Speicherpools
✕

Einleitung
Datenträger auswählen
Konfigurieren
Zusammenfassung

Konfigurieren:

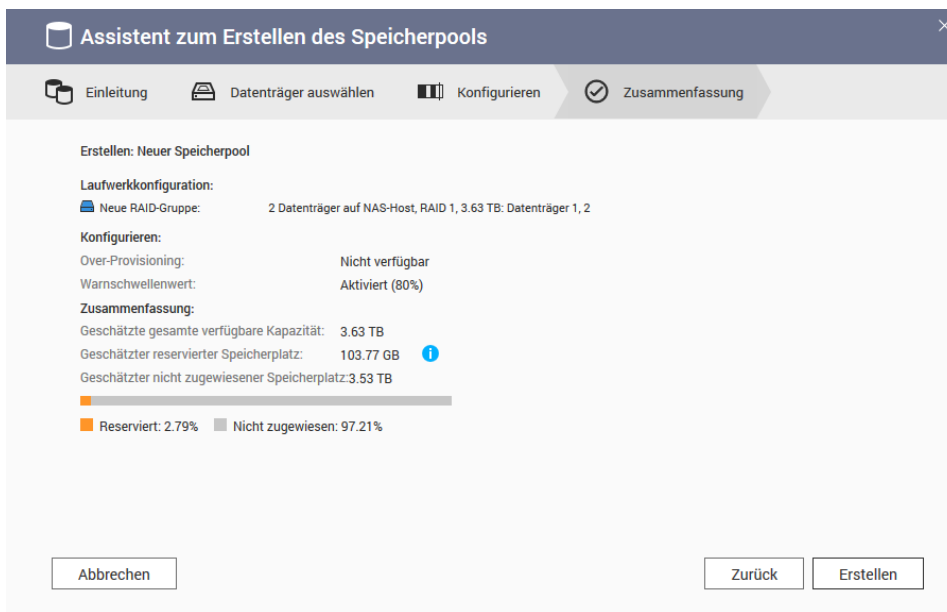
Over-Provisioning: Nicht verfügbar ▼

Erweiterte Einstellungen: ▲

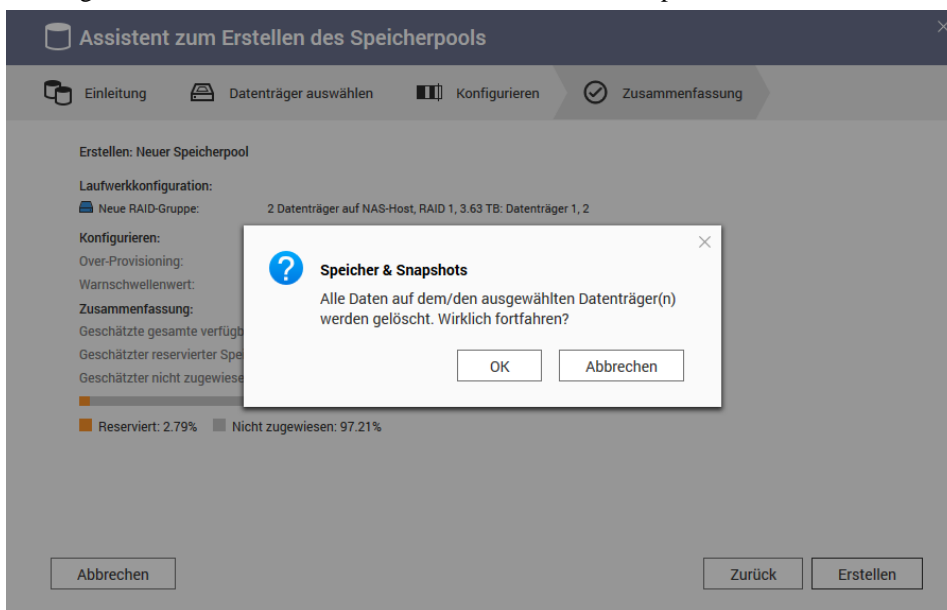
Warnschwellenwert %

Abbrechen
Zurück
Weiter

Starten Sie den Aufbau des Speicherpools im letzten Dialog über **Erstellen**.



Bestätigen Sie den Hinweis, dass Ihnen klar ist, was dadurch passiert.

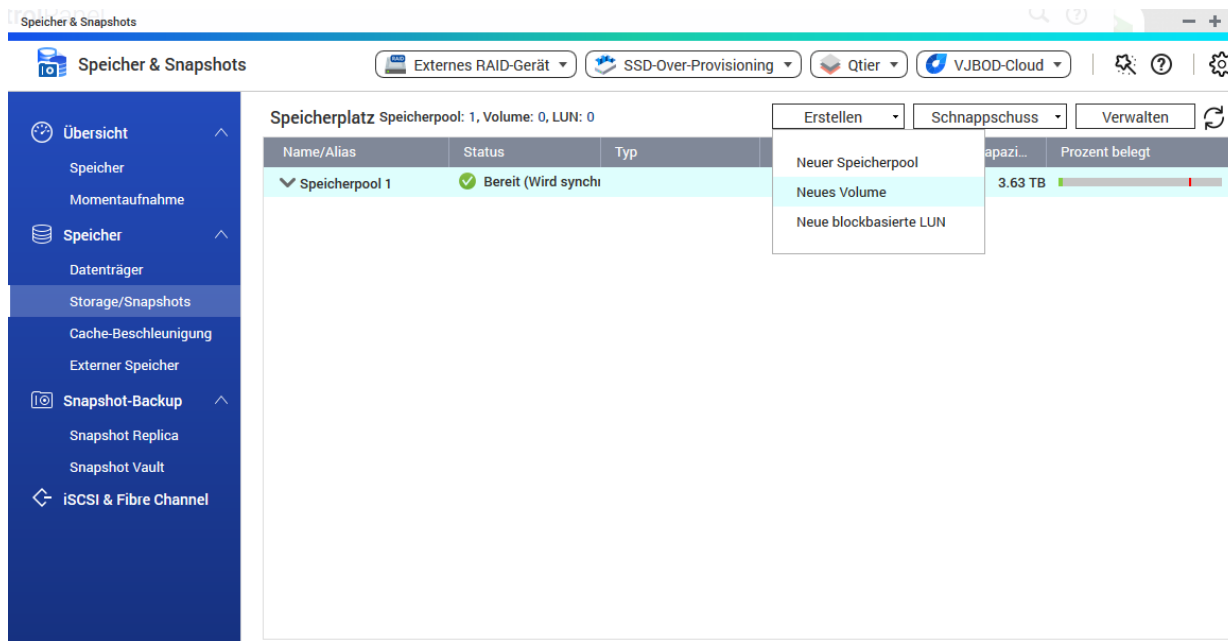


Danach wird der Speicherpool aufgebaut und im Beispielfall erfolgt die Synchronisation des RAID-1.

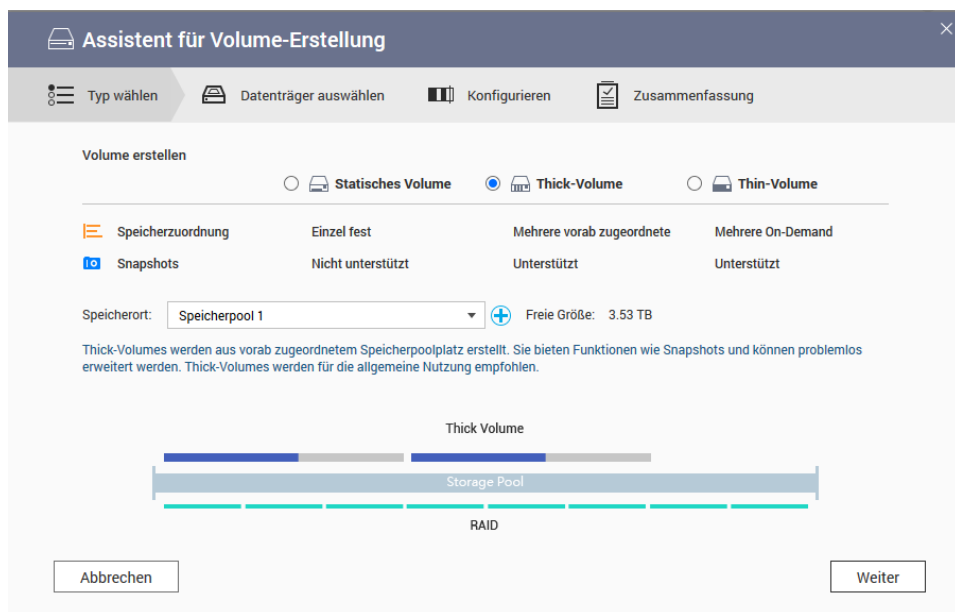
III.2.6.2.2.4. Ein Volume erstellen

Wählen Sie aus dem Menü **Erstellen** den Eintrag **Neues Volume**.

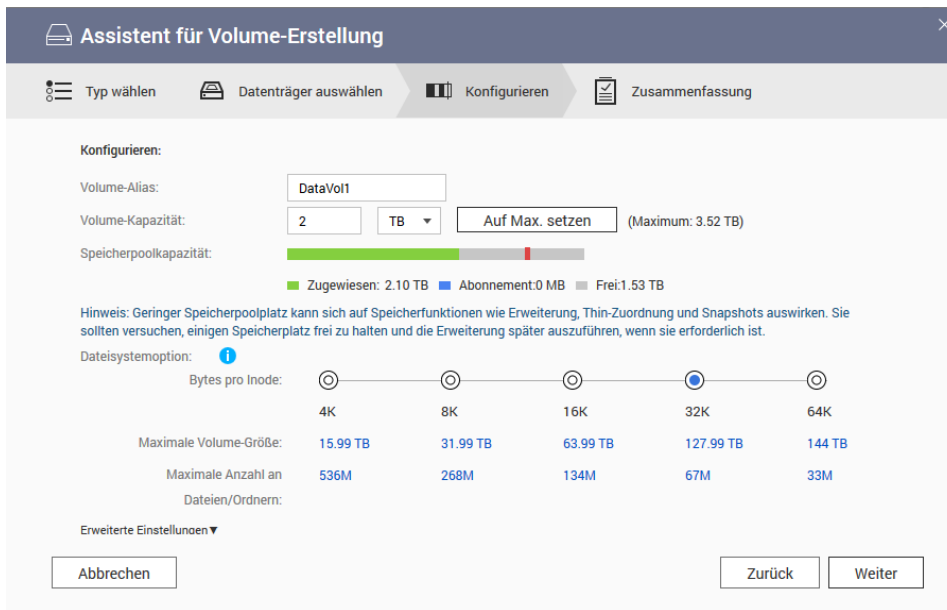
Ein solches **Volume** ist die Voraussetzung für eine Dateibasierte Sicherung.



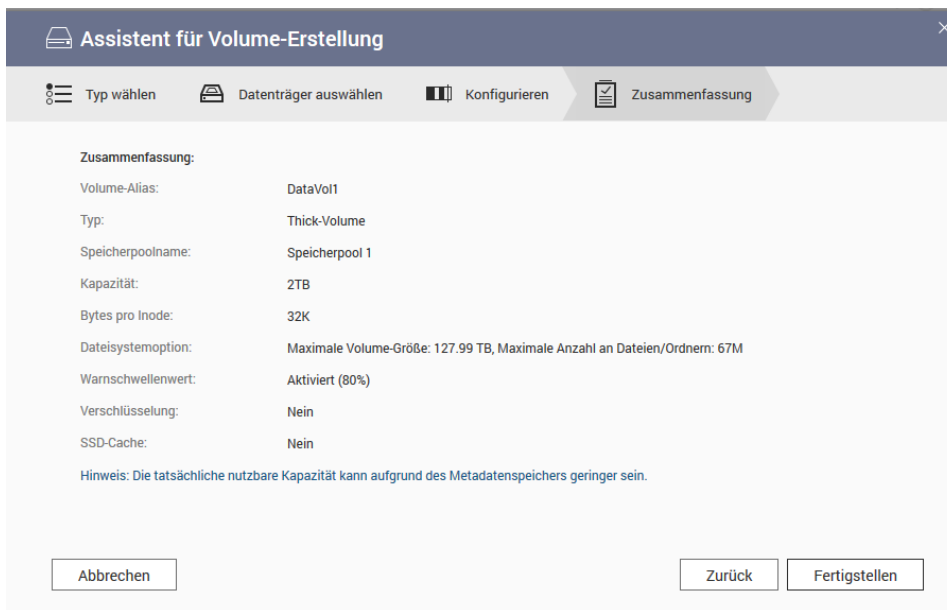
Aus Geschwindigkeitsgründen, sollte die Vorgabe "Thick-Volume" gewählt werden. Fahren Sie fort mit **Weiter**



Im folgenden Eintrag kann die Kapazität des Volumes gewählt und Optimierungen hinsichtlich des Dateisystems vorgenommen werden.



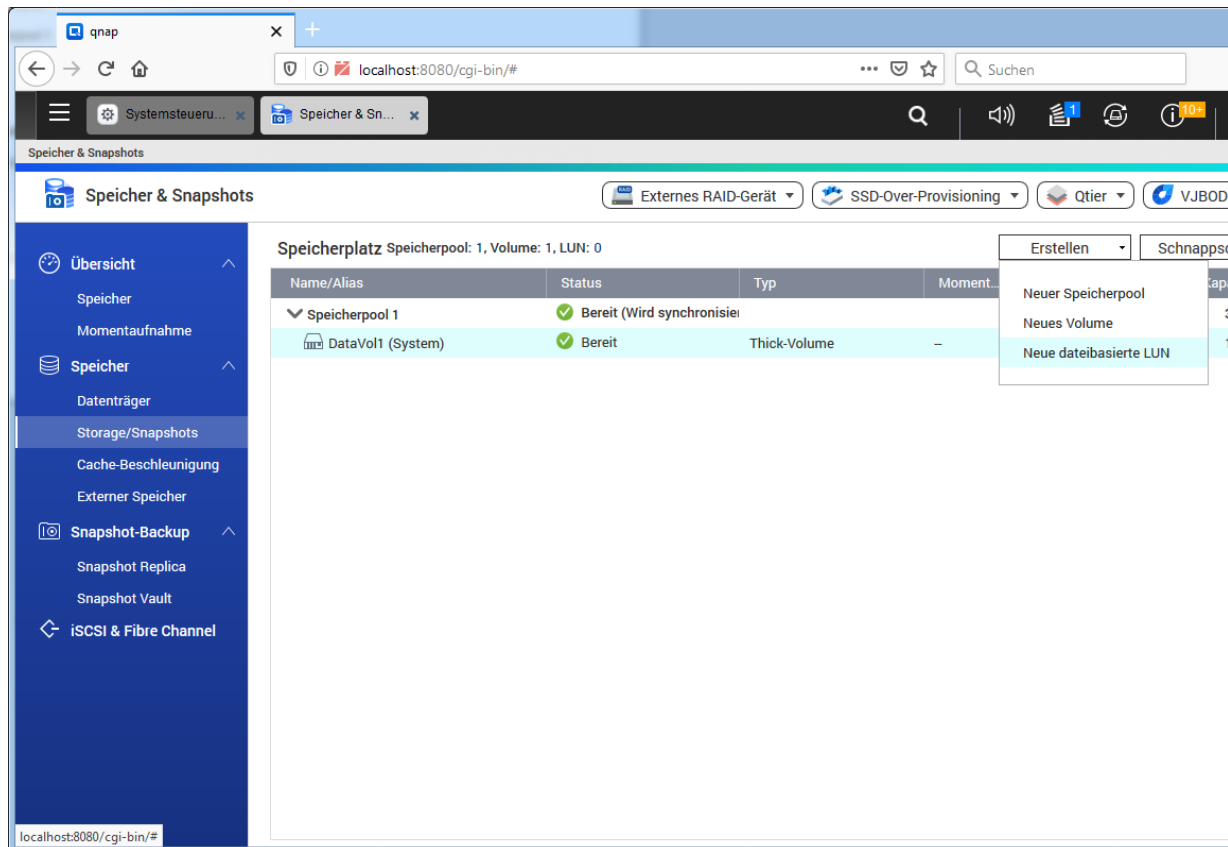
Um das Volume zu erstellen, im letzten Dialog **Fertigstellen** wählen.



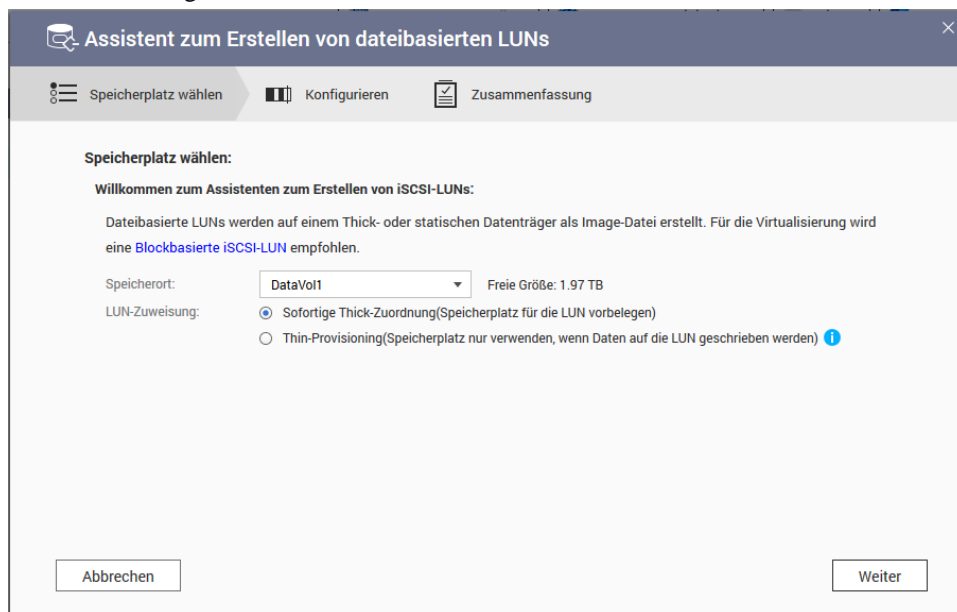
III.2.6.2.2.5. Dateibasierte LUN anlegen

Ein iSCSI-Target (NAS-Gerät) kann eine oder mehrere LU (Logical Units) haben. Diese sind nummeriert, weshalb die Abkürzung LUN eigentlich für Logical Unit Number steht.

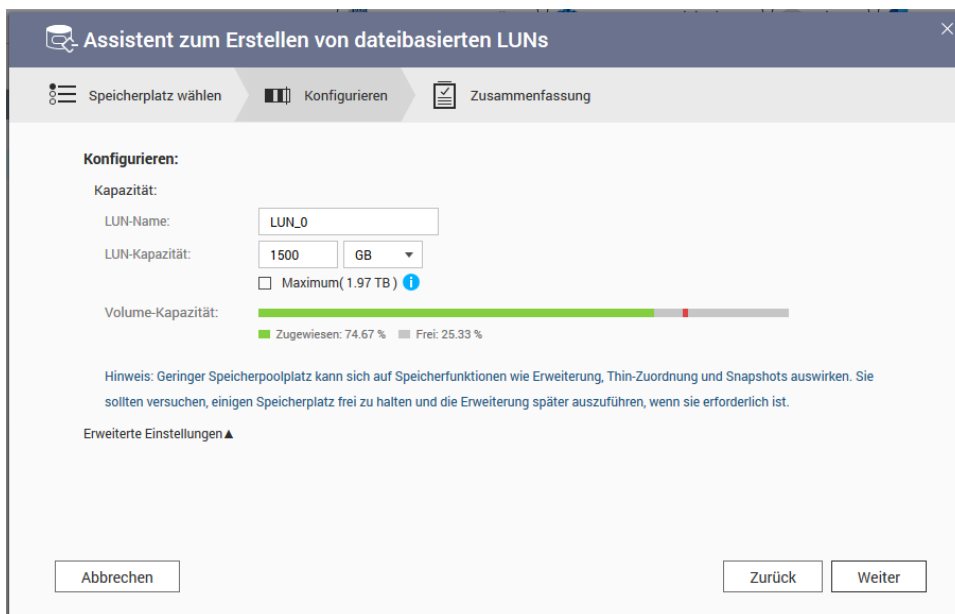
Wählen Sie über das Menü **Erstellen** im Bereich der Speicherverwaltung der NAS den Eintrag **Neues dateibasiertes LUN** aus, um ein solches zu erstellen.



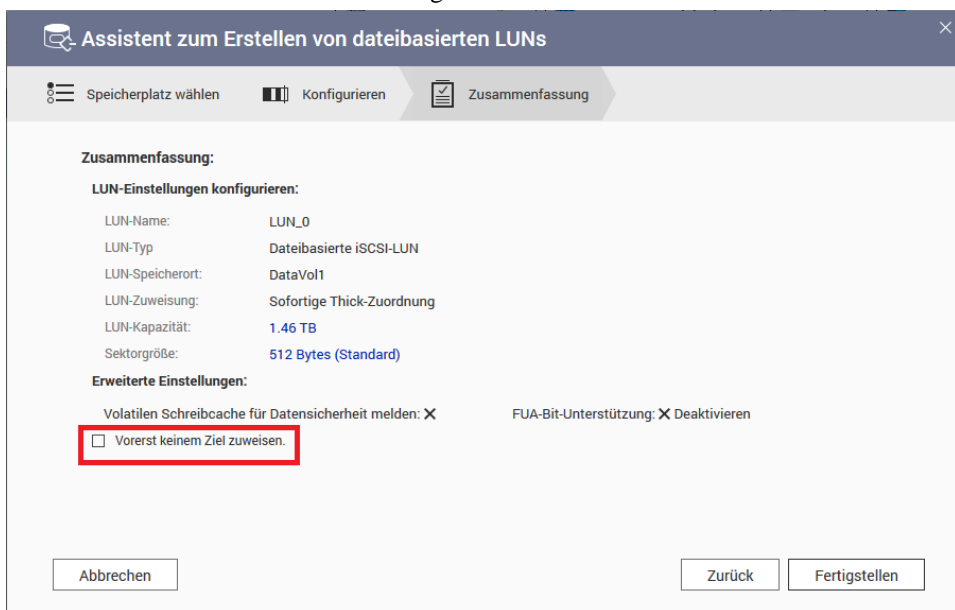
Thick-Zuordnung wählen und mit **Weiter** fortfahren.



Die LUN-Kapazität wählen

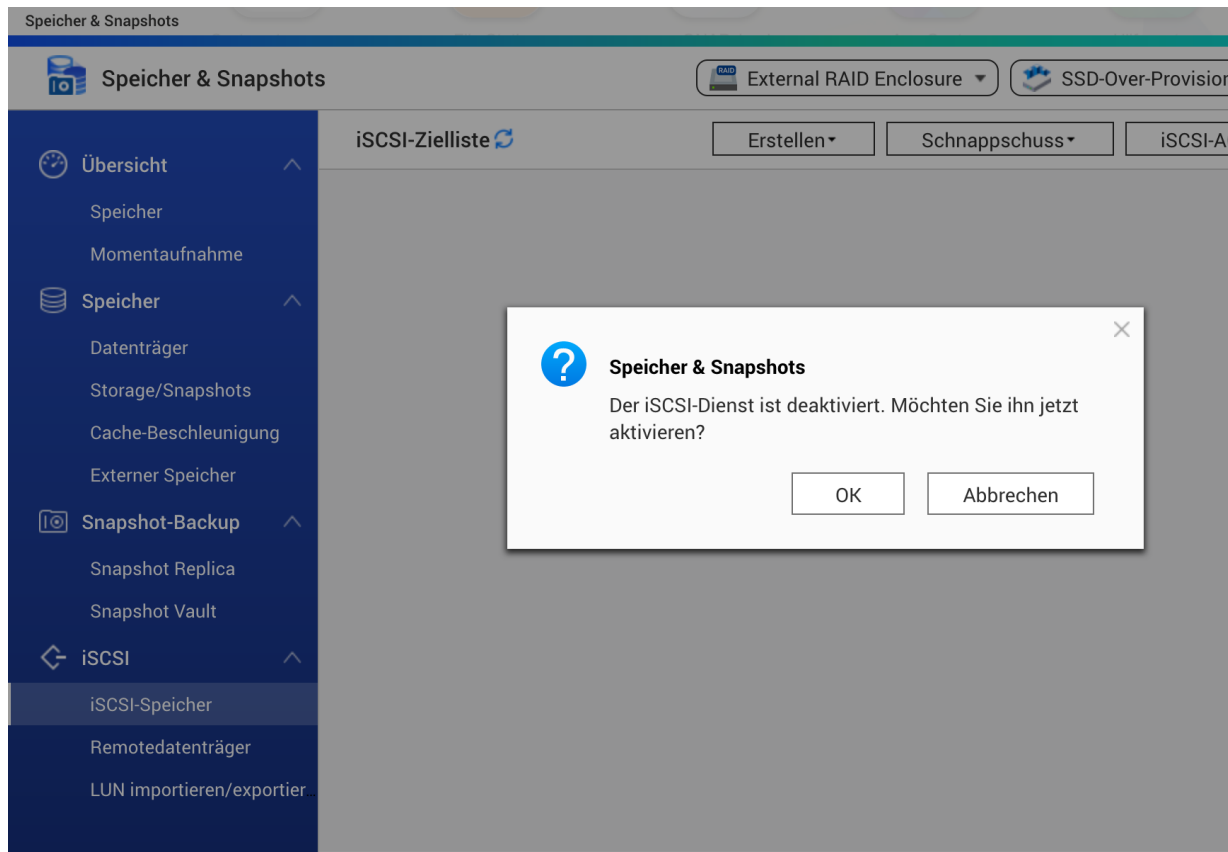


Vorerst keinem Ziel zuweisen und Fertigstellen.

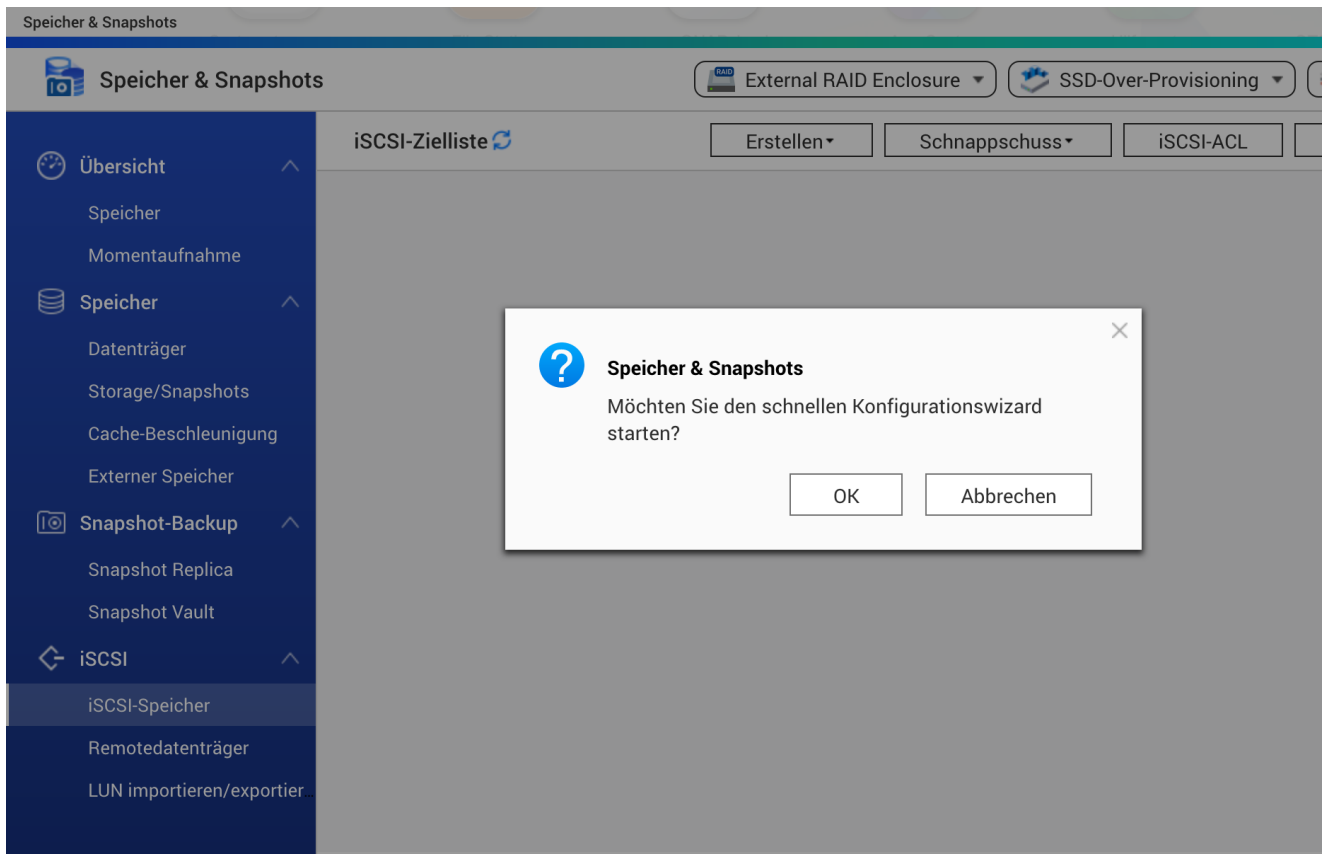


III.2.6.2.2.6. Dienst iSCSI aktivieren

Der Eintrag **iSCSI & Fibre Channel** führt zum Dialog, der die iSCSI- und Fibre Channel-Dienste aktiviert, sofern noch nicht geschehen. Diesen mit **OK** bestätigen..

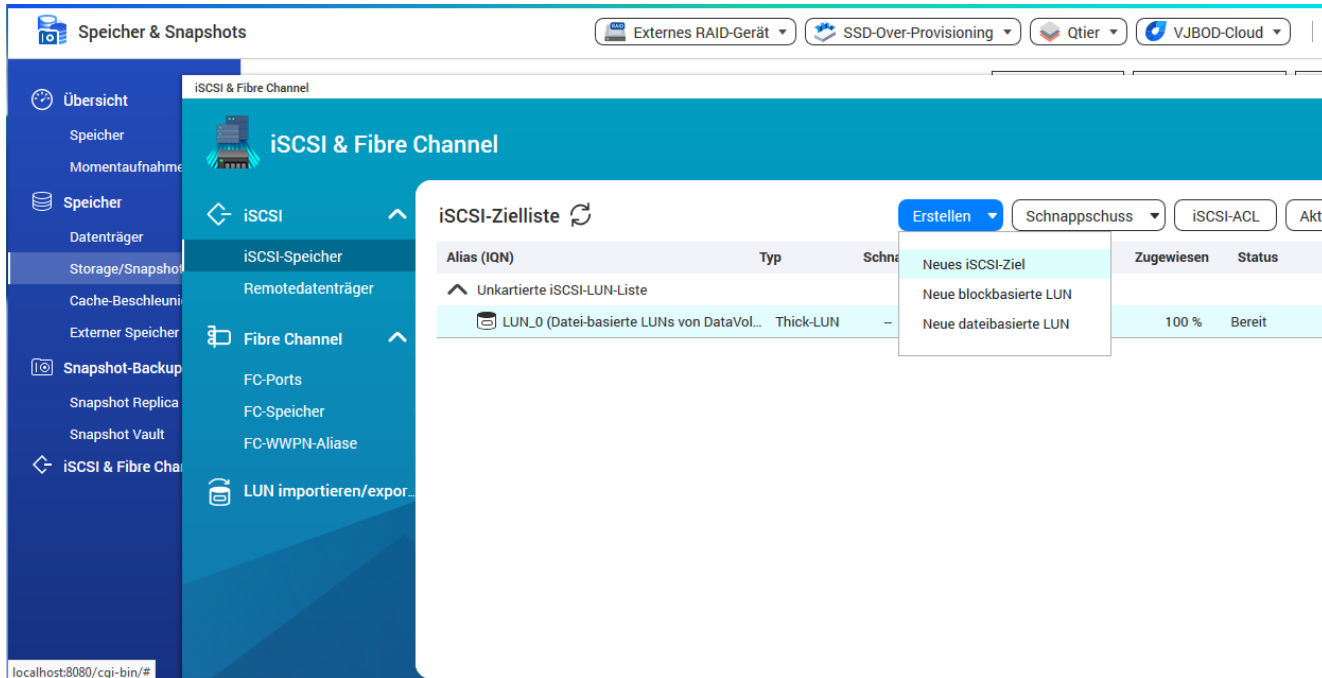


Den nachfolgenden Dialog zum Start eines Wizards bitte beenden über **Abbrechen**



III.2.6.2.7. Neues iSCSi-Ziel anlegen

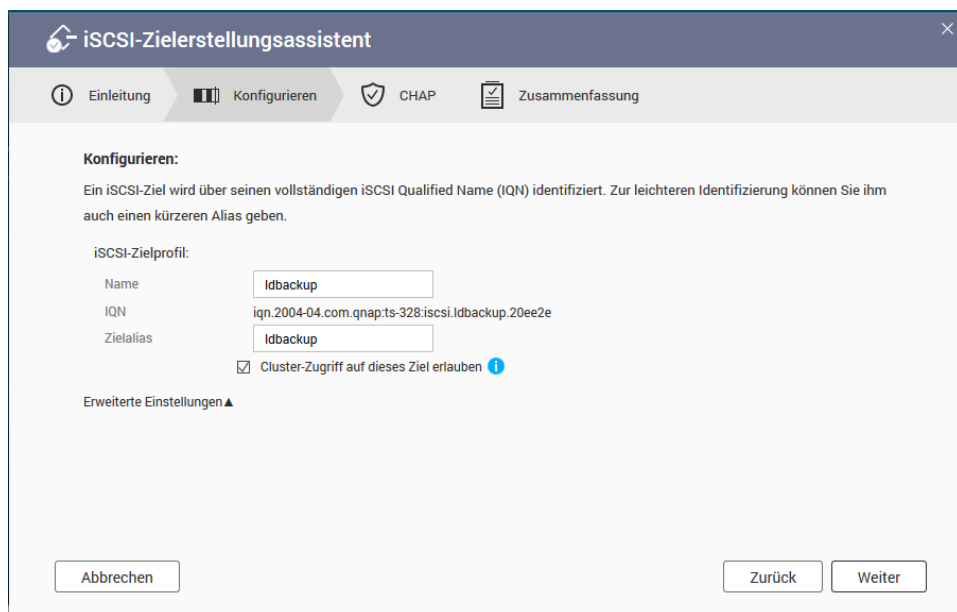
Das Ziel



Da



Da



Da

The screenshot shows the 'iSCSI-Zielerstellungsassistent' (iSCSI Target Setup Assistant) window. The 'CHAP' step is active, indicated by a shield icon. The interface includes a progress bar with steps: 'Einleitung', 'Konfigurieren', 'CHAP', and 'Zusammenfassung'. The main content area is titled 'CHAP:' and contains the following text: 'CHAP zwingt iSCSI-Initiatoren zur Authentifizierung, wenn sie sich mit diesem Ziel verbinden. Dies bietet Sicherheit, da iSCSI-Initiatoren keinen NAS-Benutzernamen und kein Kennwort benötigen.' Below this text are two sections for CHAP authentication. The first section, 'CHAP-Authentifizierung verwenden', has an unchecked checkbox and three input fields: 'Benutzername:', 'Passwort:', and 'Kennwort nochmals eingeben:'. The second section, 'Gegenseitiges CHAP', also has an unchecked checkbox and three input fields: 'Benutzername:', 'Passwort:', and 'Kennwort nochmals eingeben:'. At the bottom of the window are three buttons: 'Abbrechen', 'Zurück', and 'Weiter'.

Häkchen entfernen bei Erstellen Sie eine iSCSI-LUN ...

Da

The screenshot shows the 'iSCSI-Zielerstellungsassistent' window at the 'Zusammenfassung' (Summary) step, indicated by a document icon in the progress bar. The main content area is titled 'Zusammenfassung:' and contains the following information: 'iSCSI-Zielprofil:' with fields for 'Name' (ldbackup), 'IQN:' (iqn.2004-04.com.qnap.ts-328:iscsi.ldbackup.20ee2e), 'Abgebildet' (ldbackup), and 'Cluster-Zugriff auf dieses Ziel erlauben:' (Ja). Below this is the 'Erweiterte Einstellungen:' section, which includes: 'Daten-Digest: X Deaktivieren', 'Header-Digest: X Deaktivieren', 'CHAP-Authentifizierung: X Deaktivieren', and 'Gegenseitige CHAP-Authentifizierung: X Deaktivieren'. At the bottom, there is an unchecked checkbox with the text 'Erstellen Sie eine iSCSI-LUN, und ordnen Sie sie diesem Ziel zu.' and three buttons: 'Abbrechen', 'Zurück', and 'Übernehmen'.

III.2.6.3. Sicherung auf NAS am Server einrichten

Voraussetzung für die Einrichtung ist ein Hostsystem auf Ubuntu 16.04.

III.2.6.3.1. Einrichtung des Dienstes am Idhost

Installieren Sie im ersten Schritt die notwendigen Pakete für iSCSI:

```
apt install open-iscsi ld-iscsi-systemd-timer
```

Passen Sie die folgenden Einstellungen in der Datei `/etc/iscsi/iscsid.conf` mit einem Editor Ihrer Wahl an (etwa ab Zeile 40.):

```
node.startup = automatic
# node.startup = manual
```



Achtung

Eventuell müssen in der obigen Konfigurationsdatei weitere Anpassungen (Benutzername, Authentisierungsmethode, etc) vorgenommen werden, je nachdem wie das iSCSI-LUN konfiguriert wurde.

Geben Sie danach die folgenden Befehle ein, um die Dienste und Timer neu zu starten und dauerhaft zu aktivieren:

```
systemctl restart iscsid.service
```

```
systemctl enable --now iscsid.service
```

```
systemctl restart open-iscsi.service
```

```
systemctl enable --now open-iscsi.service
```

```
systemctl restart iscsi-reconnect.timer
```

```
systemctl enable --now iscsi-reconnect.timer
```

Durch diese Kommandos wird ein Timer aktiviert, der täglich um 21:45 Uhr (d.h. 15 Minuten vor Beginn des LogoDIDACT Backups) versucht, das iSCSI-Device neu zu verbinden. Diese Zeiteinstellung ist dabei im Paket `ld-iscsi-systemd-timer` enthalten. Dies dient der Fehlervermeidung, falls die NAS zwischenzeitlich ausgeschaltet oder kurzzeitig vom Netzwerk getrennt wurde. Zusätzlich muss folgender Befehl am `ldhost` eingegeben werden, um mögliche iSCSI-Ziele (sogenannte Nodes) erkennen zu lassen:

```
iscsiadm -m discovery -t sendtargets -p NAS-IP:3260>
```

Anschließend erstellt der Dienst `iscsid` unter `/etc/iscsi/nodes/iqn.<XYZ>/NAS-IP,3260,0/` bzw. `/etc/iscsi/nodes/iqn.<XYZ>/NAS-IP,3260,1/` eine Konfigurationsdatei namens `default`. Der Wert `<XYZ>` steht hier für den IQN-Namen, d.h. eine Kennung unter der sich die NAS im Netzwerk meldet.

Beispiele hierfür wären die folgenden:

- `iqn.2000-01.com.synology:nas-ds418.Target-1.1a4d8ce1ed`
- `iqn.2000-01.com.synology:nas.Target-1.eed43fd969`
- `iqn.2004-04.com.qnap:ts-220:iscsi.qnap.e297f5`

Die darin liegende Datei `default` muss unter anderem nachfolgende Einstellungen zur automatischen Verbindung der LUN enthalten:

```
node.startup = automatic
node.conn[0].startup = automatic
```

Falls eine Authentifizierung erforderlich ist, müssen die Zugangsdaten ebenfalls in die Datei `default` eingetragen werden. Anbei ein Beispiel mit Anmeldung nach dem CHAP-Verfahren:

```
node.session.auth.authmethod = CHAP
node.session.auth.username = admin
node.session.auth.password = xyz
```

Anschließend meldet sich das iSCSI-Target ganz normal im Dateisystem als angeschlossene Festplatte, was per Befehl **journalctl -r** oder **blkid** überprüfbar ist.

III.2.6.3.2. Startreihenfolge der Dienste unter systemd anpassen

Falls die Sicherungs-NAS nicht direkt an einem Interface am **ldhost** angeschlossen ist, sondern im internen Netzwerk, ist eine Verbindung zur iSCSI-LUN durch den **ldhost** erst möglich, nachdem die Software Open-vSwitch gestartet wurde.

In diesem Fall muss die Startreihenfolge der Dienste **open-iscsi** und **openvswitch-switch** in Abhängigkeit zueinander konfiguriert werden.

Hierzu folgenden Befehl im ldhost absenden:

```
systemctl edit open-iscsi.service
```

Es öffnet sich ein Texteditor, in dem nachfolgende Zeilen eingetragen werden müssen:

```
[Unit]
After=openvswitch-switch.service
```

Nachdem die Datei angepasst wurde, ist noch das Neuladen des systemd-Daemons notwendig, damit dieser die Anpassung mitbekommt. Ebenfalls muss der iSCSI-Dienst nochmal neugestart werden:

```
systemctl daemon-reload
```

```
systemctl restart open-iscsi.service
```

III.2.6.3.3. Konfiguration Backup im ldhost

Die Konfiguration des Backups im **ldhost** gleicht der Einrichtung einer internen Sicherungs-Festplatte. Dies ist ein Merkmal und Vorteil der Anbindung von Speichergeräten per iSCSI.

Zusammengefasst wird die verbundene iSCSI-LUN also wie eine normale Festplatte partitioniert und anschließend mit dem Ext3-Dateisystem sowie dem Label bk1/bk2 formatiert.

Bitte beachten Sie, dass in der Regel **gdisk** anstelle von **fdisk** eingesetzt werden muss, um Speicherpools größer 2 GB partitionieren zu können. Im Beispiel wird angenommen, dass die Backupfestplatte mit dem Gerätenamen **/dev/sdX** angesprochen wird. Sie können den genauen Gerätenamen für Ihre Installation über den Befehl **fdisk -l** ermitteln.

1. Installieren Sie gegebenenfalls **gdisk**

```
apt install gdisk
```

2. Erstellen Sie eine Partition über die gesamte Backupfestplatte

```
echo '0' | gdisk /dev/sdX
```

3. Formatieren Sie die Partition mit dem Dateisystem EXT3 und vergeben Sie das Label bk1 oder bk2

```
mkfs.ext3 -L bk1 /dev/sdX1
```


4. Passen Sie die EXT3 Dateisystem Parameter für die Partition an

```
tune2fs -i0 -c0 -m0 /dev/sdX1
```

5. Legen Sie das `snapshot` Verzeichnis an

```
mount /dev/sdX1 /mnt
```

```
mkdir /mnt/snapshot
```

```
umount /mnt
```

6. Führen Sie `partprobe` aus oder starten Sie den Server neu

```
partprobe
```

Der Befehl veranlasst den Kernel dazu, die Partitionstabelle komplett neu einzulesen. Falls das funktioniert, können Sie nun die Platte über das Label ansprechen:

```
cd /backup/bk1
```

Sollte das nicht funktionieren, starten Sie den Server neu: **reboot**

III.2.6.3.4. Ein Backup auf NAS

Nach der Einrichtung kann man durch den Befehl `ldsnapshot daily bk1` bzw. `ldsnapshot daily bk2` ein erstes Backup laufen lassen. Das sollte beim ersten Backup im screen laufen, da dieses für gewöhnlich etwas länger dauert.

III.2.7. Restauration im Fehlerfall

III.2.7.1. Restauration im lauffähigen System

Wenn einzelne Dateien aus dem Backup zurückgespielt werden müssen und das System noch lauffähig ist, dann können Sie direkt auf die einzelnen Dateien zugreifen, indem Sie die Backupfestplatte einbinden, nach `/backup/bk1/snapshot` wechseln, sich das jeweilige Snapshot herausuchen und die Dateien mit einem Dateimanager oder über die Kommandozeile einfach zurückkopieren.



Tipp

In den Snapshotverzeichnissen gibt es einen Link namens `latest`, der immer auf das jeweils aktuellste Snapshot verweist.

III.2.7.2. Disaster Recovery - Notfallwiederherstellung

Sofern die grundlegenden Empfehlungen für den Betrieb eines Servers befolgt werden, ist die hier beschriebene Notfallwiederherstellung ein seltener Vorgang. Grundlegend ist der Schutz des Servers und seiner Komponenten vor Überspannung durch eine USV (unterbrechungsfreie Stromversorgung). Ebenso grundlegend und wichtig ist die Redundanz bei den Festplatten über ein so genanntes RAID-System. Empfehlenswert sind im Zusammenhang mit dem LogoDIDACT-Server richtige Hardware-RAID-Controller, welche die physikalischen Gegebenheiten auch tatsächlich vor dem Betriebssystem verbergen.

Durch Berücksichtigung der beiden oben genannten Empfehlungen für USV und Redundanz durch RAID, werden 95% aller in der Praxis auftretenden Ursachen für eine Notfallwiederherstellung vermieden. Festplattenausfälle sind im Hardwarebereich die häufigste Fehlerursache in der EDV, so dass ein Server, der nur mit einer einzigen Festplatte ohne RAID betrieben wird, im Fall eines Defekts auf dieser Platte komplett ausfällt. Dort wird dann eine Notfallwiederherstellung notwendig, die im Folgenden kurz beschrieben wird.

Bei der Wiederherstellung eines Systems gibt es keine einfache pauschale Vorgehensweise, die in sämtlichen Fällen ohne tiefgehende Systemkenntnisse durchgeführt werden kann. Wichtig ist dabei vor allem auch die Ursache des Ausfalls bzw. der Wiederherstellung. Ist die Ursache ein logischer Fehler, weil man versehentlich als root am Server das gesamte System "zerschossen" hat, ist die Wiederherstellung etwas einfacher. Liegt dem Ausfall hingegen ein Hardwaredefekt einzelner Komponenten zugrunde oder gar des gesamten Servers, so dass das System auf einer ganz anderen Serverhardware wiederhergestellt werden muss, gestaltet sich die Sache etwas schwieriger.

1. Im Fall eines Festplattendefektes die Platte tauschen
2. LogoDIDACT neu installieren (nur die absolute Basisinstallation bis zum Neustart)
3. Im laufenden LogoDIDACT System folgendes ausführen

```
cd /backup/bk1/snapshot/latest
rsync -avxH --delete --numeric-ids --exclude=/etc/fstab . /
grub-install /dev/sda
reboot
```

Sowohl beim Tausch einer Festplatte als auch beim Formatieren bestehender Platten wird die Datei `fstab` neu angelegt und darf deshalb beim Zurückkopieren nicht überschrieben werden (Option **exclude**).

III.2.7.2.1. Wiederherstellung über Rescue-CD

Eine Alternative zur Wiederherstellung über eine Grundinstallation mit der LogoDIDACT CD ist über eine so genannte Rescue-CD möglich. Die hier zur Verfügung stehende CD basiert auf dem OpenSource Projekt <http://sysresccd.org>.



Achtung

Die Rescue-CD ist primär für LogoDIDACT Kunden mit Monitoring-Vertrag gedacht. Über diese spezielle CD ist auch ein Eingreifen von Außen durch den SBE Support oder einen LogoDIDACT Partner möglich, der jedoch nur funktioniert, wenn Server und Router den Anforderungen des Monitoring genügen und entsprechend installiert und konfiguriert wurden.

Die Service-Leistungen im Zusammenhang mit einer Notfallwiederherstellung sind weder Gegenstand der Softwarepflege noch des Supports!

Die RescueCD ist aber als Download frei verfügbar: <http://myshn.com/pub/logoDIDACT-Rescue.iso>

Der Ablauf beim Einsatz der RescueCD ist wie folgt

1. CD einlegen und Server von CD booten

Es erscheint ein Auswahlmenü bei dem man zwischen der 32 Bit und 64-Bit-Version wählen kann. Die Standardeinstellung ist 32 Bit und wird nach 10 Sekunden automatisch gestartet, wenn keine Eingabe erfolgt.

2. Das Rescue-Startskript `sbe-network` wird aufgerufen
3. Es wird versucht die Systempartition zu mounten. Wenn das möglich ist, wird die Netzwerkkonfiguration aus `/etc/logodidact/network.conf` ausgelesen, um die Netzwerkinterfaces im nächsten Schritt mit diesen Daten zu konfigurieren.
4. Sämtliche Netzwerk-Schnittstellen des Servers werden dynamisch ausgelesen und falls möglich mit den vorher ausgelesenen Daten konfiguriert
5. Falls der vorherige Schritt nicht funktioniert werden die Netzwerkinterfaces nacheinander automatisch mit festen IP-Adressen konfiguriert und geprüft, ob und an welchem Interface eventuell ein Router hängt:

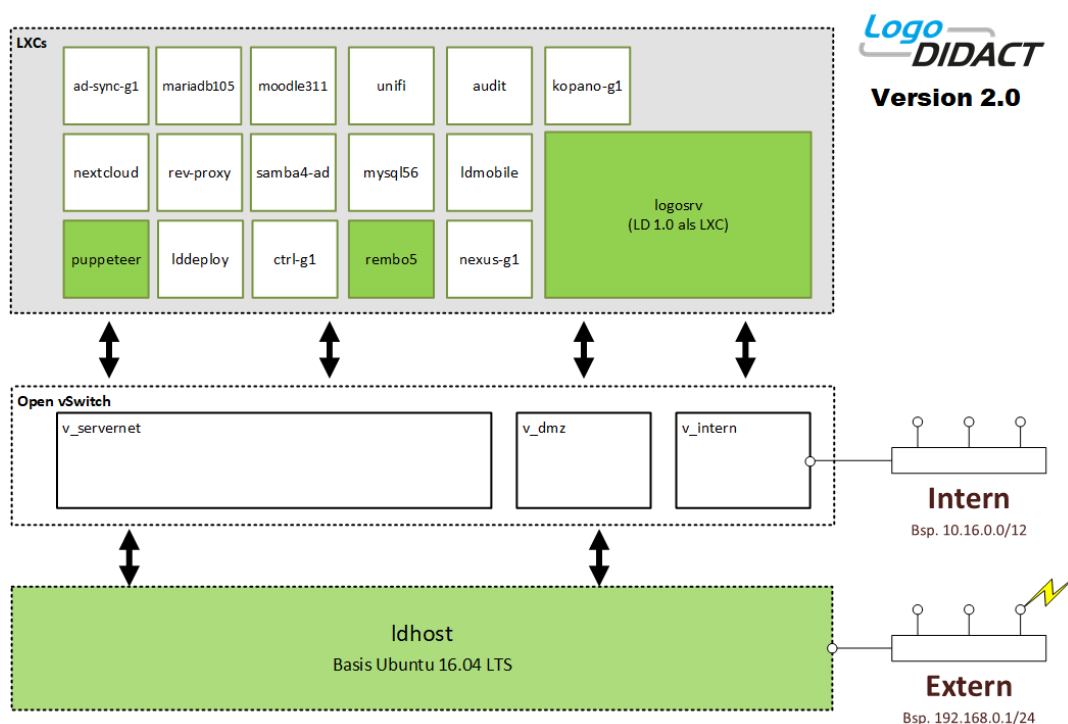
```
EXTERN: 192.168.1.254
ROUTER: 192.168.1.1
```

6. Es wird versucht den Router per ping zu erreichen und falls machbar dann auch einen SBE-Server im Internet per ping zu kontaktieren.
7. Wenn der Zugang zum Internet erfolgreich ist, wird ein SBE remote Tunnel gestartet
8. Wenn vorhanden, wird der Servername in der Datei `.id` ausgelesen und falls vorhanden verwendet. Ist das nicht möglich, wird versucht die Seriennummer über `dmidecode` auszulesen, so dass ein eindeutiger Name bildbar ist.
9. Es wird eine SBE `public_keyliste` (für den Fernzugriff per ssh) heruntergeladen. Falls die Liste nicht heruntergeladen werden kann, ist auf der RescueCD auch der Public Key von `s1.support.logodidact.com` enthalten, d.h. der SBE Support-Server `s1` wird vom "Rescue-Server" als vertrauenswürdig akzeptiert.
10. Die Live-CD meldet sich an der Webseite `notify.logodidact.com` und es wird ein cronjob ausgeführt damit die IP geupdatet wird.
11. Sobald sich eine Rescue-CD auf der Webseite meldet, erhält SBE eine Mail im Support-Postfach. Darin werden die Kommunikations-Daten des Servers mitgeteilt, d.h. IP-Adresse, Namen (sofern auslesbar) und die Portnummer für den Remote-Tunnel.
12. Es wird dynamisch ein root Kennwort generiert.

Kapitel III.3. Server und Systemdienste

Was die Serverseite von LogoDIDACT 2.0 anbelangt, unterscheidet sich diese gravierend von der Vorgängerversion und basiert auf einer zukunftsweisenden Architektur mit virtuellen Maschinen und einem System zum Management dieser Bausteine.

Der LogoDIDACT 2.0 Server besteht dabei aus einem aktuellen Hostsystem auf Basis von Ubuntu 16.04 LTS (Long Term Support) und einer „schlanken“ Virtualisierung auf Basis von LXC (Linux Containers). Durch diese Modularisierung können Lösungsbausteine extrem einfach und nach Bedarf schulspezifisch aktiviert werden. Auch die Weiterentwicklung und Einbindung neuer Bausteine geht dadurch erheblich einfacher und schneller.



Zu den vielen Neuerungen gehört auch das System- und Konfigurations-Management Puppet (deutsch = Puppe/Marionette). Dieses Open Source Werkzeug wird sowohl für das Upgrade auf LogoDIDACT 2.0 als auch im Betrieb für sämtliche Konfigurationsaufgaben genutzt. Der puppeteer (Puppenspieler) hält sinnbildlich die Fäden in der Hand und bestimmt, welche Aufgaben auf welchen physischen oder virtuellen Maschinen zu erledigen sind. Die Anweisungen werden dabei über so genannte Rezepte verteilt und über Agenten entgegengenommen.

Die Vorteile dieser zukunftsweisenden Architektur und der eingesetzten Werkzeuge münden alle in einer deutlichen Zeit- und Kosteneinsparung. Hier setzt LogoDIDACT 2.0 Maßstäbe und Sie sind damit bestens für die Zukunft gerüstet.

III.3.1. Netzwerk-Konfiguration am Server

Wie in der obigen Abbildung zu sehen, gibt es im Gegensatz zur alten Version in der neuen Version LogoDIDACT 2.0 nicht mehr den einen Server, sondern einen so genannten Host und viele virtuelle Maschinen, die selbst als Server bezeichnet werden. Der Host läuft mit seinem Basis-Betriebssystem auf der physischen Hardware und "bewirtet" die virtuellen Maschinen.

Zwischen Host und virtuellen Maschinen fungiert ein virtueller Switch auf Basis von Open vSwitch, kurz **OvS**. Dabei handelt es sich um einen virtuellen Multilayer Software Switch, der unter der Open-Source Apache 2.0 Lizenz steht. Mehr Infos unter: <http://openvswitch.org/>

Selbstverständlich lassen sich Netzbereiche, IP-Adressen und Zuordnungen der Schnittstellen auch nach der Grundinstallation anpassen. Bitte bedenken Sie jedoch, dass die Standardkonfiguration hinsichtlich der IP-Bereiche gut durchdacht ist und sich bewährt hat. Standardisierung vereinfacht vieles und sorgt immer für eine Minimierung der Kosten vor allem im Betrieb.



Tipp

Wenn Sie etwas an der Zuordnung der physischen Netzwerkadapter ändern oder das externe Interface auf einen anderen Router anpassen müssen, finden Sie hier die notwendigen Infos dazu. Sofern Sie bei der Installation keine Fehler gemacht haben und alles funktioniert, können Sie den Abschnitt überspringen und mit Abschnitt III.3.2, „Der Host und seine Container“ fortfahren.

III.3.1.1. Physische Netzwerkzuordnung

Die physisch vorhandenen Netzwerkschnittstellen des Servers, an die man ein Kabel anstecken kann, werden in LogoDIDACT 2.0 mit einem vorangestellten **p_** bezeichnet, wie z.B. **p_extern** oder auch **p_intern**.



Achtung

1. Unter Ubuntu 16.04 oder höher wird **systemd** zum Starten, Überwachen und Beenden von Prozessen verwendet.
2. Mit **systemd-networkd** wird auch die Geräteverwaltung mit **udev** abgelöst (Netzwerkarten, USB-Backup-Platten usw.)
3. Wenn Sie LogoDIDACT neu installieren, wird ausschließlich **systemd** verwendet.
4. Wenn Sie in LogoDIDACT ein Upgrade von Ubuntu 14.04 auf Ubuntu 16.04 durchführen, haben Sie zunächst einen Mischbetrieb, der zwingend beseitigt werden muss.
5. Falls noch nicht geschehen, legen Sie die Netzwerkkonfiguration wie unten gezeigt entsprechend **systemd** an und löschen Sie dann die Datei `/etc/udev/rules.d/70-persistent-net.rules`.

Bei **systemd** (Ubuntu 16.04 oder höher) finden Sie die Netzwerkkonfiguration unter `/etc/systemd/network`. Für jedes Interface muss dort eine entsprechende `.link`-Datei angelegt werden, in der im Wesentlichen die MAC-Adresse des Adapters und der Name der Schnittstelle gespeichert sind.

Die physischen Adapter kann man sich mittels des folgenden Tools anzeigen lassen:

```
inxi -n
```

Falls das Paket nicht installiert ist, kann man es über `apt-get install inxi` nachinstallieren.

Erkennbar sind über `inxi -n` die Namen von Netzwerkadaptern, Herstellerinfos, ob ein Interface UP oder DOWN ist und nicht zuletzt die MAC-Adresse der Adapter.

```
musterstadt-gym / physical / 11:24 / 1.3.5 / ssh@10.1.252.27
root@ldhost:/etc/systemd/network # inxi -n
Network: Card-1: Broadcom and subsidiaries NetXtreme BCM5719 Gigabit Ethernet PCIe driver: tg3
         IF: p_extern state: up speed: 1000 Mbps duplex: full mac: 98:f2:b3:e6:25:da
         Card-2: Broadcom and subsidiaries NetXtreme BCM5719 Gigabit Ethernet PCIe driver: tg3
         IF: p_intern state: up speed: 1000 Mbps duplex: full mac: 98:f2:b3:e6:25:db
         Card-3: Broadcom and subsidiaries NetXtreme BCM5719 Gigabit Ethernet PCIe driver: tg3
         IF: eth2 state: down mac: 98:f2:b3:e6:25:dc
         Card-4: Broadcom and subsidiaries NetXtreme BCM5719 Gigabit Ethernet PCIe driver: tg3
         IF: rename5 state: down mac: 98:f2:b3:e6:25:dd
```

Die Zuordnung zwischen MAC-Adresse des jeweiligen Netzwerkadapters und dem logischen Namen für das Interface kann an dieser Stelle mit **systemd** relativ einfach erstellt bzw. angepasst werden.



Achtung

Der Name einer Netzwerkkarte darf dabei nicht mehr als **14 Zeichen lang** sein!

Der Aufbau für das externe Interface **p_extern** findet sich folglich in der Datei **80-p_extern.link**, deren Inhalt wie in folgendem Beispiel aussieht:

```
[Match]
MACAddress=00:0c:29:0f:f1:f1
[Link]
Name=p_extern
```

Der Aufbau für das interne Interface **p_intern** findet sich entsprechend in der Datei **80-p_intern.link**:

```
[Match]
MACAddress=00:0c:29:0f:f1:dd
[Link]
Name=p_intern
```

Damit Änderungen am Namen übernommen werden, ist es wichtig, den folgenden Befehl auszuführen, damit das initramfs-Image neu aufgebaut wird, in welchem die Schnittstellen in Ubuntu 16.04 oder höher festgelegt sind.

update-initramfs -u



Achtung

Wenn Sie Änderungen an der Zuordnung von Netzwerkschnittstellen vornehmen, müssen Sie danach den Server **ldhost** neu starten.

III.3.1.2. Externe IP-Adresse des Servers anpassen

Das so genannte externe Netzwerkinterface hängt direkt am Host und wird dort konfiguriert. Die Netzwerkkonfiguration für dieses Interface findet, wie von Ubuntu her bekannt, in der Datei **/etc/network/interfaces** auf dem **ldhost** statt. Diese Datei wird **nicht** per Puppet gemanaged.

In einer Standard-Umgebung für LogoDIDACT hängt am externen Interface des Servers ein Router, dessen IP-Adresse häufig im 192er Netz liegt. Viele Routerhersteller verwenden aus Gründen der Standardisierung die IP 192.168.1.1. Das externe Interface **p_extern** muss natürlich im Netz die-

ses Routers liegen, worauf bereits bei der Installation hingewiesen wird. In der beschriebenen Beispiel-Konfiguration wird die IP für **p_extern** auf `192.168.1.254` gesetzt, was zwar nicht zwingend notwendig, aber empfehlenswert ist.

```
auto p_extern
iface p_extern inet static
    address 192.168.1.254
    netmask 255.255.255.0
    gateway 192.168.1.1

auto lo
iface lo inet loopback
    dns-domain schule.local
    dns-search schule.local
    dns-nameservers 127.0.0.1
```

Damit Änderungen greifen, muss der Server neu gestartet werden. Mit **Server** ist in diesem Fall der **ldhost** gemeint, also die physische Maschine.

III.3.1.3. Interface extern auf DHCP stellen

In bestimmten Situationen kann es auch sinnvoll oder erforderlich sein, das externe Interface am Server auf DHCP umzustellen. Wenn man z.B. einfach nur einen Anschluss zur Verfügung gestellt bekommt, auf dem ein externer Dienstleister den Zugang zum Internet oder auch einem Stadtnetzwerk bereitstellt, dann bekommt man auf diese Weise in der Regel die IP-Adresse und weitere Daten per DHCP zugewiesen.

Der Eintrag in der Datei `/etc/network/interfaces` auf dem **ldhost** ist dann wie folgt anzupassen:

```
auto p_extern
iface p_extern inet dhcp

auto lo
iface lo inet loopback
    dns-domain schule.local
    dns-search schule.local
    dns-nameservers 127.0.0.1
```

Damit Änderungen greifen, muss der Server (**ldhost**) neu gestartet werden.

III.3.1.4. Interne IP-Adresse des ldhost anpassen

Bis auf das externe Interface **p_extern**, werden alle anderen Interfaces über Puppet gemanaged und von OVS (Open vSwitch) verwaltet. Die Einstellungen landen zwar letztendlich im **ldhost** in `/etc/network/interfaces.d/ovs` werden aber im Container **puppeteer** konfiguriert.



Achtung

Bis auf das externe Interface **p_extern**, sind sämtliche Einstellungen für Netzwerkschnittstellen im Container **puppeteer** vorzunehmen.

Wechseln Sie vom **ldhost** aus in den Container **puppeteer**

lxc-attach -n puppeteer

Öffnen Sie die Datei `nic.conf` mit einem Editor Ihrer Wahl, wie z.B. Nano:

nano /etc/logodidact/hosts/ldhost/nic.conf

Eine Standard-Konfiguration sieht wie folgt aus:

```
[NIC intern]
suffix 1

[NIC p_intern]
vlan_mode access
vlan_untagged ld-intern
Type manual
ovs_type OVSPort
```

Wie unschwer zu erkennen ist, taucht dort keine IP-Adresse auf. Diese wird dynamisch aus dem gewählten Netzwerkbereich und dem Parameter **suffix** gebildet. Der Wert **suffix 1** bedeutet, dass sich der `ldhost` automatisch die erste freie IP aus seinem Netzwerkbereich (Standard `10.16.0.0`) holt, was in der Praxis der IP-Adresse `10.16.0.1` entspricht. Die dynamische Zuordnung der IP-Adresse hat den Vorteil, dass sie bei einer Änderung des Netzwerkbereichs automatisch richtig angepasst wird.

Wenn man die IP des `ldhost` statisch festlegen möchte oder muss, ersetzt man **suffix 1** durch Angabe von IP und Subnetzmaske des Servers. Hierbei kann man die Netzmaske komplett ausschreiben `255.240.0.0` oder die Kurznotation verwenden, wie sie im unten stehenden Beispiel verwendet wird:

```
[NIC intern]
IP 10.16.0.1/12

[NIC p_intern]
vlan_mode access
vlan_untagged ld-intern
Type manual
ovs_type OVSPort
```

III.3.1.5. Netzwerkbereich anpassen

Wie im vorherigen Abschnitt erwähnt, wird bei einer Standardinstallation ein `10er` Netz mit `12er` Netzmaske definiert, also `10.16.0.0/255.240.0.0`. Sofern es keine triftigen Gründe gibt, sollte man daran nichts ändern.

Ein möglicher Grund ist gegeben, wenn das externe Netzwerk unabänderlich vorgegeben ist und ebenfalls den `10er` Bereich nutzt. Dann muss man den Netzbereich von LogoDIDACT 2.0 zwangsweise abändern.

Ein mögliches Szenario im pädagogischen Netz ergibt sich, wenn viele oder alle dezentralen Schulserver an ein internes städtisches Netzwerk angeschlossen werden, um darüber auf zentrale Dienste zuzugreifen (Jugendschutzfilter, Proxy, Virens Scanner usw.) bzw. um darüber gemanagt zu werden.

Ein zweites Szenario ergibt sich beim Einsatz von LogoDIDACT im Verwaltungsnetzwerk einer Baden-Württemberger Schule, wenn man den Server an das so genannte KISS-Netz (**K**ommunikations-**I**nfrastruktur zwischen **S**chulen und **S**chulverwaltung) ankoppelt. Dieses öffentliche Netz der Schulbehörde in Baden-Württemberg ist selbst ein `10er` Netz, weshalb in diesem Fall der LogoDI-

DACT Server dann in das private 172er Netz gelegt wird (IP des logosrv 172.16.1.1 mit Subnetzmaske 255.240.0.0).

Wechseln Sie vom ldhost aus in den Container puppeteer

lxc-attach -n puppeteer

Öffnen Sie die Datei `networkscope.conf` mit einem Editor Ihrer Wahl, wie z.B. Nano:

nano /etc/logodidact/config/networkscope.conf

Eine Standard-Konfiguration sieht wie folgt aus, wobei der Netzwerkbereich für das interne Netz **ld-intern** im dritten Block definiert wird.

```
[NetworkScope ld-servernet]
Description Network for servers
GuestInterface servernet
Scope servernet
Net 172.28.28.0/24
Gateway 172.28.28.1
```

```
[NetworkScope ld-dmz]
Description DMZ
GuestInterface dmz
Scope dmz
Net 172.28.29.0/24
```

```
[NetworkScope ld-intern]
Description Network Internal
GuestInterface intern
Scope internal
Net 10.16.0.0/255.240.0.0
```

III.3.1.5.1. Ändern des Netzwerkbereichs bzw. mehrere Bereiche

Wie im obigen Abschnitt zu erkennen, gibt es in LogoDIDACT 2.0 drei Netzwerkbereiche. Neben **ld-intern**, gibt es das so genannte **ld-servernet**, dem alle virtuellen Maschinen hängen und ein DMZ-Netz **ld-dmz**. Wie bereits erwähnt, besteht in der Regel kein Grund an den Netzbereichen etwas zu ändern. Wenn es aber einen guten Grund für die Änderung eines Bereichs gibt, dann ergibt sich daraus in der Praxis eine Anpassung aller drei Netzwerkbereiche.

Im folgenden Beispiel wird die Anpassung deshalb konkret am Beispiel des so genannten KISS-Netzwerkes dargestellt.

```
[NetworkScope ld-servernet]
Description Network for servers
GuestInterface servernet
Scope servernet
Net 192.168.28.0/24
Gateway 192.168.28.1
```

```
[NetworkScope ld-dmz]
Description DMZ
GuestInterface dmz
Scope dmz
```

```
Net 192.168.29.0/24
```

```
[NetworkScope ld-intern]
Description Network Internal
GuestInterface intern
Scope internal
Net 172.16.0.0/255.240.0.0
```

Das Netzwerk ld-intern wird dabei auf ein 172.16.0.0/12 geändert.



Achtung

Die Änderung des Netzwerkbereichs bzw. der Bereiche hat gravierende Auswirkungen auf das gesamte System und sollte nur von erfahrenen Netzwerkadministratoren vorgenommen werden. Sofern man die IP-Konfiguration des ldhost auf dynamisch stehen lässt, ergibt sich dessen IP-Adresse automatisch aus dem geänderten Netzbereich von ld-intern.

In jedem Fall manuell angepasst werden muss jedoch auch die IP-Adresse des logosrv.

Damit die Änderungen im puppeteer im Host und den virtuellen Maschinen umgesetzt werden, sind die üblichen Puppet-Aktionen durchzuführen, die in Abschnitt III.3.3.2, „Puppet Tools und Befehle“ ausführlich beschrieben werden.

Wechseln Sie im Puppeteer ins Verzeichnis `/etc/logodidact` und übertragen Sie die Änderungen ins Versionierungssystem git:

```
git add .
```

```
git commit -m "Änderung des Bereichs, Ankopplung an KISS"
```

Wechseln Sie in den Host und starten Sie einen `prun`. Die neue Konfiguration steht dann im ldhost in der config-Datei von OVS unter `/etc/network/interfaces.d/`.

Damit der Open vSwitch diese übernimmt, sind unter Ubuntu 14.04 nacheinander die folgenden Befehle einzugeben:

```
service openvswitch-switch stop
```

```
rm /etc/openvswitch/conf.db
```

Unter Ubuntu 16.04 lauten die Befehle:

```
systemctl stop openvswitch-switch.service
```

```
rm /var/lib/openvswitch/conf.db
```

Zum Abschluss muss der Server (ldhost) neu gestartet werden:

```
reboot
```

III.3.1.6. IP-Adresse des logosrv anpassen

Der Container logosrv ist vereinfacht gesagt das, was als Rest vom LogoDIDACT 1.0 Server übrig geblieben ist. Stück um Stück wurden und werden daraus einzelne Software-Bausteine entfernt und

in separate Container ausgelagert oder durch komplett neue Module ersetzt. Ungeachtet der Tatsache, dass bereits mehr als ein Dutzend der Bausteine in Container ausgelagert sind, wird es den logosrv noch eine ganze Weile geben.

Ausführliche Informationen zur Konfiguration des **logosrv** finden sich in Kapitel III.4, *Konfiguration des logosrv*. Zur Anpassung der IP-Adresse des logosrv wechseln Sie in diesen Container.

lxc-ssh -n logosrv

Öffnen Sie die Datei `/etc/logodidact/network.conf` mit einem Editor Ihrer Wahl, wie z.B. Nano. Die IP-Konfiguration sieht im Standard mit `10.16.1.1` für die interne IP des logosrv wie folgt aus und kann im Abschnitt **Internal** angepasst werden.

```
[Base]
Hostname logosrv
Domainname schule.local
DNS 127.0.0.1

[Internal]
IPAddress 10.16.1.1
Netmask 255.240.0.0
Device intern
Scope internal
Comment internes Interface (Verbindung zum LAN)

[External]
Netmask 255.255.255.0
Device dmz
Comment externes Interface (Verbindung zum Internet)
IPAddress 172.28.29.2
Gateway 172.28.29.1
```

Damit die Änderung übernommen wird, muss nach dem speichern noch der folgende Befehl ausgeführt werden:

do_netconf --all



Achtung

Wenn Sie Änderungen an der IP des logosrv vornehmen, müssen Sie gegebenenfalls im Puppeteer auch die Anpassungen im Netzwerkbereich vornehmen, wie in Abschnitt III.3.1.5, „Netzwerkbereich anpassen“ beschrieben. Ebenfalls zu beachten gilt es, dass dies Auswirkungen auf die Vergabe von IP-Adressen per DHCP hat und bereits aufgenommene Geräte im Control Center angepasst werden müssen.

III.3.1.7. Trunks, Bonding und LACP

Aufgrund der Änderung in der Architektur mit vielen verschiedenen Containern und der Einführung des virtuellen Switches **OVS**, ergeben sich bestimmte Anforderungen an die Umgebung von LogoDI-DACT 2.0 und damit auch einige Einschränkungen.

Für das Bündeln von Netzwerkkarten bzw. Leitungen sind sowohl der Begriff "Trunk" oder auch "Bond" gebräuchlich. Die Bündelung findet gewöhnlich zwischen einem Server mit mehreren physi-

kalischen Schnittstellen und dem zentralen Switch statt. Hat ein Server beispielsweise 2 Netzwerkkarten mit jeweils 1 GBit Geschwindigkeit, kann man diese mittels 2 Kabeln auf dem zentralen Switch zu einer 2 GBit schnellen Leitung zusammenfassen.

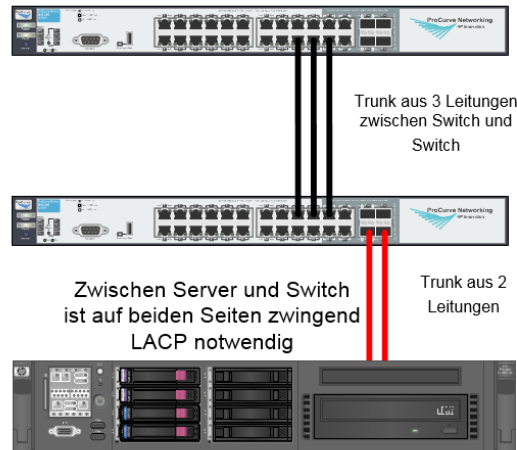


Abbildung III.3.1. Trunks erfordern unter LogoDIDACT 2.0 die Konfiguration von LACP auf beiden Seiten

In LogoDIDACT 2.0 ist es zwingend erforderlich, dass Trunks zwischen dem Server und dem zentralen Switch auf beiden Seiten per LACP (Link Aggregation Control Protocol) konfiguriert werden.

III.3.1.7.1. Ein Bonding Interface (LACP) konfigurieren

In folgendem Beispiel ist gezeigt, wie das Bonding auf Basis von 2 physischen Interfaces konfiguriert wird. Dazu sollte man zunächst auf der physischen Ebene die Netzwerkinterfaces entsprechend umbenennen, um nicht den Überblick zu verlieren.

Bitte beachten Sie, dass diese Anpassungen ab Ubuntu 16.04 oder höher entsprechend **systemd** gemacht werden. Man benennt das Interface mit der Bezeichnung **p_intern** und die zugehörige Link-Datei um im Verzeichnis `/etc/systemd/network/` um in `80-p_intern1.link`

```
[Match]
MACAddress=00:0c:29:0f:f1:dd
[Link]
Name=p_intern1
```

und definiert über `80-p_intern2.link` ein weiteres Interface über die Bezeichnung **p_intern2**

```
[Match]
MACAddress=00:0c:29:0f:f1:de
[Link]
Name=p_intern2
```

Es wird natürlich vorausgesetzt, dass dieses zweite Interface physisch vorhanden ist und noch nicht verwendet wird.

Damit die Änderungen werden, ist es zwingend erforderlich, den folgenden Befehl auszuführen, damit das `initramfs`-Image neu aufgebaut wird, in welchem die Schnittstellen in Ubuntu 16.04 oder höher festgelegt sind.

update-initramfs -u



Achtung

Wenn Sie Änderungen an der Zuordnung von Netzwerkschnittstellen vornehmen, müssen Sie danach den Server **ldhost** neu starten.

Anschließend müssen diese beiden physischen Adapter per Name dem logischen Netzwerk zugeordnet werden. Dies geschieht im Container des Puppeteer in der Datei `/etc/logodidact/hosts/ldhost/nic.conf`.

In Anlehnung an das Bonding, benennt man dazu das Interface **p_intern** um in **b_intern** (b für bond). Den Parameter **ovs_type** ändern Sie von **OVS_Port** auf **OVSBond**. Die beiden physischen Interfaces werden über den Parameter **members** zugeordnet. Über **bondlACP active** wird das zwingend notwendige Link Aggregation Control Protocol (LACP) aktiviert.

```
[NIC intern]
suffix 1

[NIC b_intern]
Type manual
ovs_type OVSBond
bondlACP active
bondmode tcp
members p_intern1 p_intern2
vlan_mode access
vlan_untagged ld-intern
```

Damit die Änderungen im Puppeteer umgesetzt werden, sind die üblichen Puppet-Aktionen durchzuführen, die in Abschnitt III.3.3.2, „Puppet Tools und Befehle“ ausführlich beschrieben werden.

Wechseln Sie im Puppeteer ins Verzeichnis `/etc/logodidact` und übertragen Sie die Änderungen ins Versionierungssystem git:

```
git add .
```

```
git commit -m "Einrichtung Bonding auf 2 Netzwerkkarten"
```

Wechseln Sie in den Host und starten Sie einen **prun**. Die neue Konfiguration steht dann im ldhost in der config-Datei von OVS unter `/etc/network/interfaces.d/`. Damit der Open vSwitch diese übernimmt, sind nacheinander die folgenden Befehle einzugeben:

```
service openvswitch-switch stop
```

```
rm /etc/openvswitch/conf.db
```

Zum Abschluss muss der Server (ldhost) neu gestartet werden:

```
reboot
```

III.3.1.8. Netzwerke und VLANs in LogoDIDACT 2.0

Einen etwas detaillierteren Blick auf das interne Netzwerk in LogoDIDACT 2.0 mit dem virtuellen Switch OVS, den logischen Netzwerken und VLANs liefert die folgende Grafik.

In der Standardausführung gibt es auf dem Server die 3 Netze **servernet**, **intern** und **dmz** und ein unabhängiges Interface **extern**.

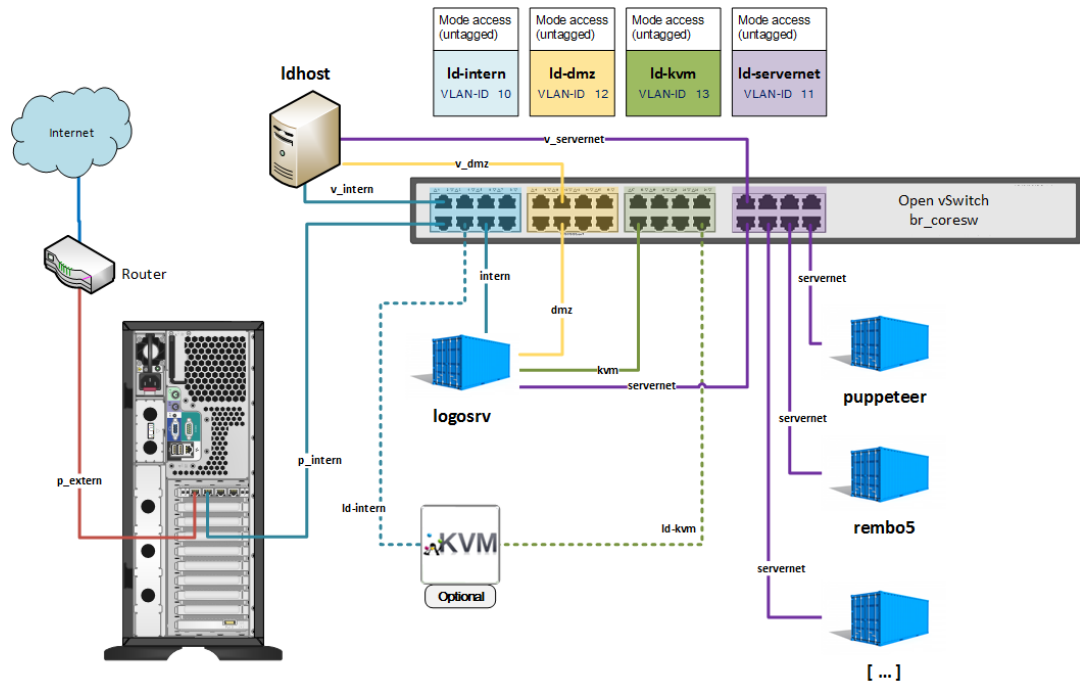


Abbildung III.3.2. Die Netzwerke und VLANs in LogoDIDACT 2.0

Die Netzwerke, VLANs und IP-Netzbereiche hier nochmals in tabellarischer Übersicht:

Tabelle III.3.1. Tabellarische Übersicht zu Netzen und VLAN-IDs

Bezeichnung:	Standard-Netz:	VLAN-ID
intern	10.16.0.0/12	10
dmz	172.28.29.0/24	11
servernet	172.28.28.0/24	12
ld-kvm		13
ld-maintenance		14

Bitte beachten Sie, dass die in LogoDIDACT vorgegebenen VLAN-IDs nicht anderweitig verwendet werden dürfen. Sofern Sie eine VLAN-ID zwingend ändern müssen, ist das über eine kundenspezifische Konfiguration in YAML prinzipiell möglich. Um z.B. die beiden VLAN-IDs der Netze ld-kvm und ld-maintenance zu ändern, ist das im Container Puppeteer in der Datei `/etc/logodidact/hiera/custom.yaml` möglich.

```

global::network:
  scopes:
    maintenance:
      ld-maintenance:
        vlan: 114
    kvm:
      ld-kvm:
        vlan: 113
    
```



Achtung

Führen Sie solche Anpassungen in und über YAML (Yet Another Markup Language) in keinem Fall durch, wenn Sie mit dieser sehr speziellen Markierungssprache nicht bestens vertraut sind. Anders als der Name vermuten lässt, handelt es sich bei YAML keinesfalls nur um irgendeine weitere Beschreibungssprache, denn auch Leerzeichen und Zeileneintrückungen haben eine Bedeutung und Auswirkung auf die Ergebnisse.

III.3.2. Der Host und seine Container

Die Technologie der Virtualisierung auf Basis von LXC (Linux Containern) hat erst mal nichts mit dem des Konfigurations-Managements per Puppet zu tun, weshalb man sich mit den Grundlagen der LXC vertraut machen sollte bzw. muss. Dass im Betrieb viele Aufgaben automatisiert erledigt werden, befreit einem nicht davon, die Grundlagen der Virtualisierung zu beherrschen.

III.3.2.1. Befehle zum Verwalten der Container (LXC)

Während der Neuinstallation von LogoDIDACT 2.0 mussten bereits einige der grundlegenden Befehle wie **lxc-attach** kennengelernt, um z.B. vom Hostsystem aus in einen Container zu wechseln oder **reboot**, um diesen neu zu starten.

Im Hostsystem gibt es eine ganze Reihe von Befehlen, die mit „lxc“ beginnen und die man sich über die Autovervollständigung („lxc eingeben und Tab-Taste drücken) ansehen kann. Den Großteil der Befehle braucht man weder zu kennen, noch sollte man diese verwenden. Zum Einstieg reichen einige wenige Befehle aus.

III.3.2.1.1. Infos zu aktiven Containern

Um vom Host aus einen Überblick über die Container zu bekommen und einige wesentliche Infos zu den aktiven LXC zu erhalten, dient der folgende Befehl:

```
lxc-ls -f
```

Mit der Option „f“ für fancy (=schick) erhält man eine praktische Ausgabe mit Infos zum Namen, dem Status und den IPs.

```
root@ldhost:~# lxc-ls -f
NAME      STATE  AUTOSTART  GROUPS          IPV4                                IPV6
logosrv   RUNNING 1          onboot, system 10.16.1.1, 172.18.18.1, 172.18.19.1, 172.28.28.1, 172.28.29.2 -
puppeteer RUNNING 1          onboot, system 172.28.28.5 -
rembo5    RUNNING 1          app             172.28.28.16 -
```

Um einen Überblick zum RAM-Bedarf aller Container zu bekommen, lässt sich der **LXC**-Befehl mit entsprechenden Optionen erweitern:

```
lxc-ls -f -F NAME, RAM
```

```
root@ldhost:~# lxc-ls -f -F NAME, RAM
NAME      RAM
ca-g1     329.66MB
ctrl-g1   1425.95MB
deploy-g1 346.05MB
icinga2   433.95MB
ldmobile  1291.19MB
logosrv   4064.88MB
mysql56   952.20MB
postgres110 411.98MB
puppeteer 1627.75MB
rembo5    1569.98MB
rev-proxy 329.67MB
samba4-ad 780.59MB
unifi     1840.90MB
```

Um weitere detaillierte Infos zu einem bestimmten Container zu bekommen, dient der Befehl:

lxc-info -n LXC-Name

wobei LXC-Name der Name des Containers ist. Mit **lxc-info -n rembo5** erhalten Sie beispielsweise detaillierte Informationen über den Container Rembo5.

```
root@ldhost:~# lxc-info -n rembo5
Name:      rembo5
State:    RUNNING
PID:      8794
IP:       172.28.28.16
CPU use:  1043.17 seconds
BlkIO use: 1.12 GiB
Memory use: 1.27 GiB
RMem use: 0 bytes
Link:     rembo5
Total bytes: 0 bytes
Link:     v_14_rembo5
TX bytes: 0 bytes
RX bytes: 0 bytes
Total bytes: 0 bytes
```

III.3.2.1.2. Einwählen in und Ausloggen aus einem Container

Um vom Host aus in einen Container zu wechseln, gibt es prinzipiell zwei verschiedene Möglichkeiten. Die Einwahl in einen Container ist per **ssh containername** möglich (z.B. **ssh rembo5**), wobei hier jedes Mal das **root** Kennwort eingegeben werden muss.

Wesentlich einfacher wechselt man deshalb in einen Container über den folgenden Befehl:

lxc-attach -n containername

Auf rein technischer Ebene ist die Umgebung dabei nicht exakt gleich, was aber in der Praxis keine Rolle spielt.

Der Befehl zum Verlassen eines Containers ist in beiden Fällen gleich:

exit

III.3.2.1.3. Neustart eines Containers

Der Befehl für den Neustart eines Containers ist denkbar einfach und wurde während der Neuinstallation ebenfalls schon mehrfach verwendet:

reboot

**Achtung**

Jeder Container bzw. LXC stellt eine virtuelle Maschine bzw. einen Server dar. Eine Aufforderung zum Neustart des Servers hat innerhalb eines Containers damit eine vollkommen andere Auswirkung, als die gleiche Aufforderung im Hostsystem.

Es ist deshalb extrem wichtig zu wissen, wo man sich befindet!

Nach Ausführung des Befehls **reboot** innerhalb eines Containers, wird man automatisch aus diesem herausgeworfen und steht wieder im Hostsystem.

III.3.2.1.4. Herunterfahren und Starten eines Containers unter Ubuntu 14.04**Achtung**

Die folgenden Befehle zum Herunterfahren und Starten von Containern gelten ausschließlich für Ubuntu 14.04!

Die entsprechenden Befehle für Ubuntu 16.04 finden Sie im nachfolgenden Abschnitt.

Dass man einen Container herunterfahren bzw. beenden muss, kommt eher selten vor und geschieht über den folgenden Befehl:

stop lxc-instance NAME=containername

wobei **containername** wieder der Name des jeweiligen Containers ist.

Um einen heruntergefahrenen Container wieder zu starten, sollte man die Befehle verwenden, die auch beim Hochfahren des Gesamtsystems zum Starten der einzelnen Container genutzt werden, da nur dort die init-Skripte mit einbezogen werden:

start lxc-instance NAME=containername

Auch ein Restart eines Containers ist möglich über **restart lxc-instance NAME=containername**. Der Neustart hat dabei eine andere Wirkung als der Befehl **reboot** innerhalb des Containers. Letzterer startet den Server innerhalb der virtuellen Maschine bzw. des LXC neu, während der **restart**-Befehl die gesamte Instanz, also den Container selbst neu startet.

Noch seltener erforderlich und nur der Vollständigkeit halber erwähnt, lassen sich **alle** Container über **stop lxc** herunterfahren und **start lxc** wieder starten.

III.3.2.1.5. Start und Stop eines Containers unter Ubuntu 16.04



Achtung

Die folgenden Befehle zum Herunterfahren und Starten von Containern gelten ausschließlich für Ubuntu 16.04!

Die entsprechenden Befehle für Ubuntu 14.04 finden Sie im vorherigen Abschnitt.

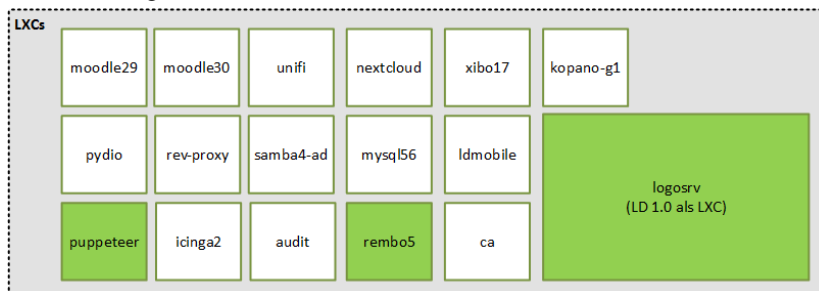
Mit Ubuntu 16.04 haben sich viele Dinge verändert und verbessert, unter anderem die Art und Weise, wie das System selbst startet und Prozesse verwaltet.

Starten eines Containers:

systemctl start lxc@CONTAINERNAME

III.3.3. Konfigurations-Management mit Puppet

In LogoDIDACT 2.0 wird ein Konfigurationsmanagement auf Basis des OpenSource-Systems Puppet (deutsch: Puppe oder Marionette) genutzt, um die große Anzahl an (virtuellen) Servern weiterhin einfach konfigurieren zu können.



Wie in der Abbildung zu erkennen stehen in LogoDIDACT 2.0 inzwischen 16 Module bzw. Bausteine als virtuelle Maschinen zur Verfügung, wenngleich es sich bei einigen davon, "nur" um verschiedene Versionen handelt, wie Moodle 2.8, Moodle 2.9 und Moodle 3.0. Verwaltet werden muss zudem der Host bzw. das Wirtssystem selbst und auch der virtuelle Switch OVS. Dass diese Systeme alle virtualisiert auf einem physischen Server laufen, ist im Hinblick auf das Management dieser Dienste unerheblich.

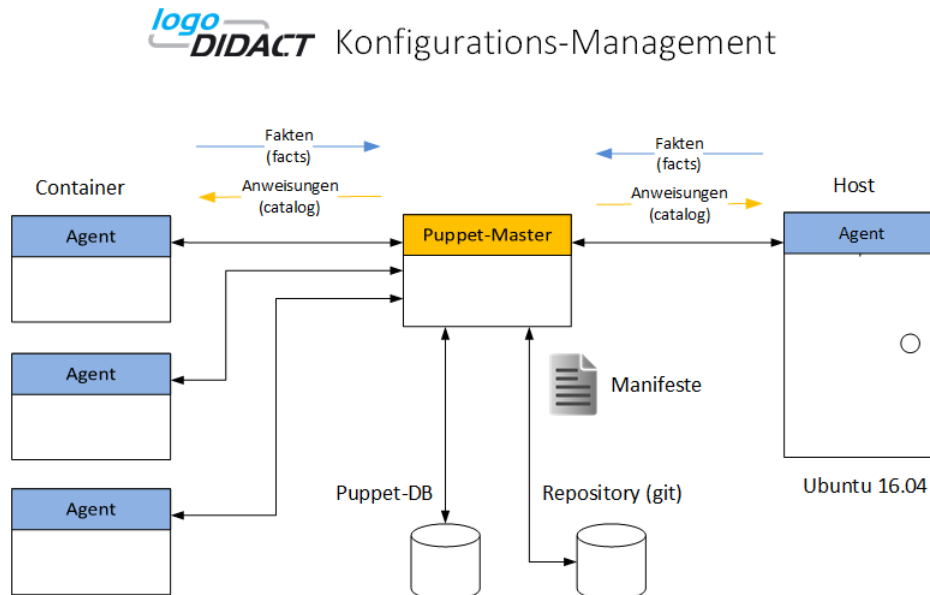
Die entscheidende Fragestellung ist, wie man all diese Server im Griff hat, d.h., wie man diese automatisiert installiert und konfiguriert und im Hinblick auf die Sicherheit auf einem aktuellen Stand hält. Genau dafür und für vieles andere mehr, wird in LogoDIDACT 2.0 das Konfigurationsmanagement Puppet eingesetzt.

Das Grundprinzip ist, dass Konfigurationen nicht innerhalb der jeweiligen Container bzw. LXC's, sondern im Konfigurations-Managementsystem durchgeführt werden. Hiervon gibt es nur wenige Ausnahmen. Die größte Ausnahme ist der LogoDIDACT (1.0) - LXC, welcher **nicht** von Puppet konfiguriert wird, da dieser LXC auf Dauer vollständig durch andere LXC's ersetzt werden wird.

III.3.3.1. Grundlagen zu Puppet

III.3.3.1.1. Puppet Komponenten

Wie oben erwähnt, hält der puppeteer (Puppenspieler) sinnbildlich die Fäden in der Hand und bestimmt, welche Aufgaben auf welchen physischen oder virtuellen Maschinen zu erledigen sind. Die Anweisungen werden dabei über so genannte **Rezepte** verteilt und über **Agenten** entgegengenommen. Neben dem puppeteer sind eine ganze Reihe weiterer Komponenten mit im Spiel, von denen nur die wichtigsten dargestellt werden sollen. Es ist aber in jedem Fall sehr wichtig zu wissen, wie die Konfiguration von Parametern in einem Container von LogoDIDACT 2.0 abläuft. Dies ist in der folgenden Abbildung dargestellt:



Die Puppet Agenten liefern dem Puppet-Master Fakten, wie z.B. über die vorhandene Hardware, d.h. die Größe des Hauptspeichers oder den Festplattenplatz. Weiterhin liefern sie ihm auch Infos zu erfolgreich erreichten Zuständen oder über Fehlschläge. Der Puppet-Master (auch kurz puppeteer genannt) verwertet diese Fakten zusammen mit Manifesten, in denen Zustände definiert sind. Aus Fakten und Manifesten generiert (compiliert) der puppeteer den Katalog. Darin befinden sich dann konkret die Anweisungen für die verschiedenen jeweiligen Agenten.

III.3.3.1.2. Arbeitsweise von Puppet

Was in und mit Puppet tatsächlich alles geschieht, lässt sich auf wenigen Seiten nur schwer erklären und viele Details sind zunächst auch eher unwichtig.

Wichtig ist hingegen, dass man einige Fakten kennt und die grundlegenden Zusammenhänge sowie die Arbeitsweise versteht.

- Sowohl im Host als auch in jedem Container (mit Ausnahme des logosrv) läuft ein Agent
- Der puppeteer wird auch Puppet-Master genannt
- Puppet arbeitet „**unsichtbar**“ im Hintergrund
- Der puppeteer ist die zentrale Stelle in LogoDIDACT 2.0 für sämtliche Konfigurationsaufgaben
- Puppet arbeitet **asynchron**, d.h. die Agenten melden sich zyklisch alle 10 bis 20 Minuten (konfigurierbar) beim puppeteer

Vor allem sorgen die Punkte "unsichtbar" und "asynchron" bei vielen Einsteigern erst mal dafür, dass man nur schwer versteht, was wann und wo passiert. Deshalb wurden von SBE einige wichtige Tools entwickelt.

III.3.3.2. Puppet Tools und Befehle

III.3.3.2.1. Das Tool pstat

Da Puppet weitestgehend im Stillen und unsichtbar arbeitet, wurde von SBE das Tool **pstat** (Abkürzung für **puppet status**) entwickelt. Dieses Tool läuft nur im Container puppeteer und gibt einen Überblick über den Status von Puppet. Vereinfacht ausgedrückt wird das sichtbar gemacht, was unsichtbar im Hintergrund abläuft.

Das Tool aktualisiert sich per Standard jede Sekunde, wobei das Intervall durch Eingabe der Zeit in Sekunden verlängert werden kann, d.h. 9 bedeutet, dass die Anzeige nur alle 9 Sekunden aktualisiert wird.

Wie bereits bei der Installation erwähnt, wechselt man vom Host aus durch **lxc-attach -n puppeteer** in den Container. Gestartet wird das Tool durch Eingabe von **pstat** und beendet durch Eingabe von **q** (für quit).

```
2017-10-08T11:27:09
Agent State | Catalog State | Node | Successes | Noops | Skips | Failures | Last run
-----|-----|-----|-----|-----|-----|-----|-----
Deactivated |  | audit |  |  |  |  |  |
Deactivated |  | icinga2 |  |  |  |  |  |
Waiting | OK | ldhost.schule.local | 198 |  |  |  | 8 minutes ago
Deactivated |  | ldmobile |  |  |  |  |  |
Deactivated |  | moodle28 |  |  |  |  |  |
Deactivated |  | moodle29 |  |  |  |  |  |
Deactivated |  | moodle30 |  |  |  |  |  |
Deactivated |  | mysql56 |  |  |  |  |  |
Waiting | OK | puppeteer.schule.local |  |  |  |  | 10 minutes ago
Deactivated |  | pydio |  |  |  |  |  |
Waiting | OK | rembo5.schule.local | 129 |  |  |  | 10 minutes ago
Deactivated |  | rev-proxy |  |  |  |  |  |
Deactivated |  | samba4-ad |  |  |  |  |  |
Deactivated |  | unifi |  |  |  |  |  |
Deactivated |  | xibol7 |  |  |  |  |  |
Press '1'-'9' to change update interval. Press 'q' to quit.
```

In der Spalte „Node“ stehen alle Module bzw. virtuelle Maschinen, die derzeit in LogoDIDACT 2.0 verfügbar sind. Ebenso taucht dort auch der Host bzw. das Basissystem auf, innerhalb dessen diese Container laufen bzw. laufen können.

In der ersten Spalte steht, ob das jeweilige Modul aktiviert ist oder nicht. Aus der letzten Spalte ist erkennbar, wann zuletzt der Agent lief und versucht hat Anweisungen auszuführen.

Die zweite Spalte gibt an, ob die Aufgaben erledigt werden konnten, die der Agent beim letzten Durchlauf versucht hat abzuarbeiten. Dass der Status der Abarbeitung hier auf FAIL steht, ist weder ungewöhnlich noch deutet es auf einen wirklichen Fehler hin. Während der Umstellung bzw. auch bei der Installation neuer Module ist das eher „normal“ und kann z.B. bedeuten, dass eine Anweisung jetzt nicht ausgeführt werden konnte, da eine Voraussetzung dafür noch nicht da ist, die über eine andere Anweisung **asynchron** abgearbeitet wird.

Beim nächsten Durchlauf (**puppet run = prun**) kann diese Voraussetzung dann vorhanden sein, so dass dann auch darauf aufbauende Anweisungen durchgeführt werden können.

III.3.3.2.2. Der Befehl prun

Die Eingabe des Befehls **prun** in einem Container oder im Host prüft zunächst, ob nicht gerade schon ein automatischer Durchlauf des Puppet Agents stattfindet. Ist das nicht der Fall, startet der Agent und verbindet sich mit dem Puppetmaster, um etwaige Änderungen sofort mitzubekommen und in Form einer Catalog-Datei abzuholen. Das ist z.B. bei der Installation eines neuen Containers hilfreich, wenn der Aufbau mehrere prun-Durchläufe benötigt und man diesen Prozess gezielt beschleunigen möchte.

Die Tools **pstat** und **prun** sind zunächst vor allem deshalb sehr nützlich, da man die asynchronen und im Hintergrund ablaufenden Vorgänge von puppet ein Stück weit sichtbar und steuerbar machen kann.

III.3.3.2.3. Agent Befehle pdis und pena

Mit Ausnahme des logosrv läuft in jedem Container und auch im lhost ein Puppet Agent und prüft in zyklischen Abständen beim Puppet Master, ob es neue Anweisungen gibt. Für Diagnose- und Testzwecke ist es hilfreich, wenn man den Agenten vorübergehend deaktivieren kann.

Dabei steht der Befehl **pdis** für puppet agent disable und deaktiviert den Puppet Agent im jeweiligen Container. Dementsprechend steht **pena** puppet agent enable und aktiviert den Puppet Agent im jeweiligen Container.

III.3.3.3. logoDIACT 2.0 mit Puppet managen

Wie bereits an verschiedenen Stellen erwähnt, spielt das System- und Konfigurations-Managements mit Puppet in LogoDIDACT 2.0 eine Zentrale Rolle. Der Puppeteer ist dabei die zentrale Komponente und Schaltzentrale. Darüber findet nicht nur die Kommunikation statt, sondern dort befindet sich auch der zentrale Speicherort für die Konfiguration. Ebenso befindet sich in diesem Container eine Versionsverwaltung, um die Konfigurationsänderungen festzuhalten.

Diese Dinge werden in den folgenden Abschnitten allgemein aber auch ganz konkret anhand eines einfachen Beispiels durchgeführt.

III.3.3.3.1. Zentrale Konfiguration

Anstelle die Konfiguration von Parametern in jedem einzelnen Modul oder Container vorzunehmen, befinden sich diese Daten an zentraler Stelle im Container puppeteer.



Tipp

Ein Großteil der Konfiguration von LogoDIDACT 2.0 wird über Dateien innerhalb der Ordnerstruktur `/etc/logodidact/` im Container puppeteer definiert.

Während der Neuinstallation wurde beispielsweise der Schulname (Longname) der Schule und der Domänenname (Kurzname) festgelegt. Diese Parameter befinden sich in der Datei `/etc/logodidact/config/customer.conf` und können dort auch angepasst bzw. geändert werden.

Wechseln Sie im Puppeteer in das Verzeichnis `/etc/logodidact/config` und öffnen Sie die Datei mit **nano customer.conf**. Ändern Sie den Namen "Musterschule Musterstadt" z.B. "Gymnasium Musterstadt".

```
GNU nano 2.2.6 File: customer.conf
[Customer]
ShortName musterstadt-gym
LongName Gymnasium Musterstadt
```

Wie auch bereits unter LogoDIDACT 1.0 muss man selbstverständlich darauf achten, dass bei den jeweiligen Variablen oder Parametern auch nur bestimmte Werte zulässig sind und die Syntax stimmt. Damit man vor solchen Fehleingaben geschützt ist bzw. zu einem vorherigen Zustand wieder zurückkehren kann, wurde mit Puppet auch gleichzeitig das Versionsverwaltungssystem git eingeführt.

III.3.3.3.2. Zentrale Versionsverwaltung mit git

Der Sinn und Zweck des Systems mit git besteht konkret darin, dass man Änderungen in der Konfiguration von LogoDIDACT 2.0 nachvollziehen und gegebenenfalls auch rückgängig machen kann. Das System umfasst dabei konkret die Dateien innerhalb der Ordnerstruktur `/etc/logodidact/` im Container **puppeteer**.



Tipp

Das Versionsverwaltungssystem mit git umfasst in LogoDIDACT 2.0 die gleiche Ordnerstruktur `/etc/logodidact/` im Container **puppeteer**, in der auch die Konfiguration zentral verwaltet wird.

Sie sollte sich daran gewöhnen, Ihre Änderungen immer sofort über die Versionsverwaltung festzuhalten. Spätestens wenn Sie ein Update in LogoDIDACT einspielen wollen und eine dabei zuvor gemachte Änderung in der Konfiguration nicht eingepflegt haben, müssen Sie das nachholen. Dieses Festhalten solcher Änderungen wird in git mittels des Befehls **commit** gemacht.

III.3.3.3.2.1. Versionsstand prüfen

Ob es Änderungen in der Konfiguration gibt, die bisher nicht übertragen (committed) wurden, lässt sich mittels des folgenden Befehls prüfen:

git status

Wenn zuvor beispielsweise der LongName oder die Domäne der Schule in der Datei `/etc/logodidact/config/customer.conf` angepasst wurde, sieht die Ausgabe wie folgt aus:

```
root@puppeteer:/etc/logodidact # git status
On branch master
Changes not staged for commit:
  (use "git add <file>..." to update what will be committed)
  (use "git checkout -- <file>..." to discard changes in working directory)

    modified:   config/customer.conf

no changes added to commit (use "git add" and/or "git commit -a")
```

Es werden alle Dateien mit Pfadangabe angezeigt, in denen es Änderungen gab (hier nur `config/customer.conf`).

III.3.3.3.2. Versionsänderung übertragen (commit)

Um Änderungen an der Konfiguration in der Versionsverwaltung festzuhalten reicht der folgenden Befehl:

```
git commit -a -m "Schulname angepasst"
```

```
root@puppeteer:/etc/logodidact # git commit -a -m "Schulname angepasst"
=> Found no license key in /etc/logodidact/config/system/system.conf
Info : Found 20 translations configurations.
Info : Found hosts [ldhost]
Info : Analyze [config,ldhost]
Info : Translated [config]
Info : Saving dependencies (/var/spool/ld-puppet/map_translate.json)
[master 2bcf362] Schulname angepasst
 1 file changed, 1 insertion(+), 1 deletion(-)
```

Die Option "-a" fügt alle Dateien hinzu, an denen Anpassungen vorgenommen wurden. Der Parameter "-m" (für message) steht dabei für den Kommentar, der dahinter in Hochkommata gesetzt wird. Hier trägt man in der Praxis zusätzlich seinen Namen und/oder einen Firmennamen oder ein Kürzel ein.



Achtung

Ohne das Übertragen (committen) in das so genannte git-Repository, passiert nichts!

III.3.3.3.3. Konfigurationsänderungen antriggern

Konfigurationsänderungen an zentraler Stelle im Puppeteer werden durch das Eingpflegen in git automatisch übersetzt zu einer neuen Catalog-Datei compiliert. Die notwendigen Aktionen für den Host oder die Container werden dann wiederum von deren Agenten bei einem zyklischen Durchlauf abgeholt und durchgeführt.

Wie bereits weiter oben beschrieben, kann man über die beiden Tools pstat und prun die Prozesse in Puppet "sichtbar" machen und in Grenzen auch beschleunigen.



Tipp

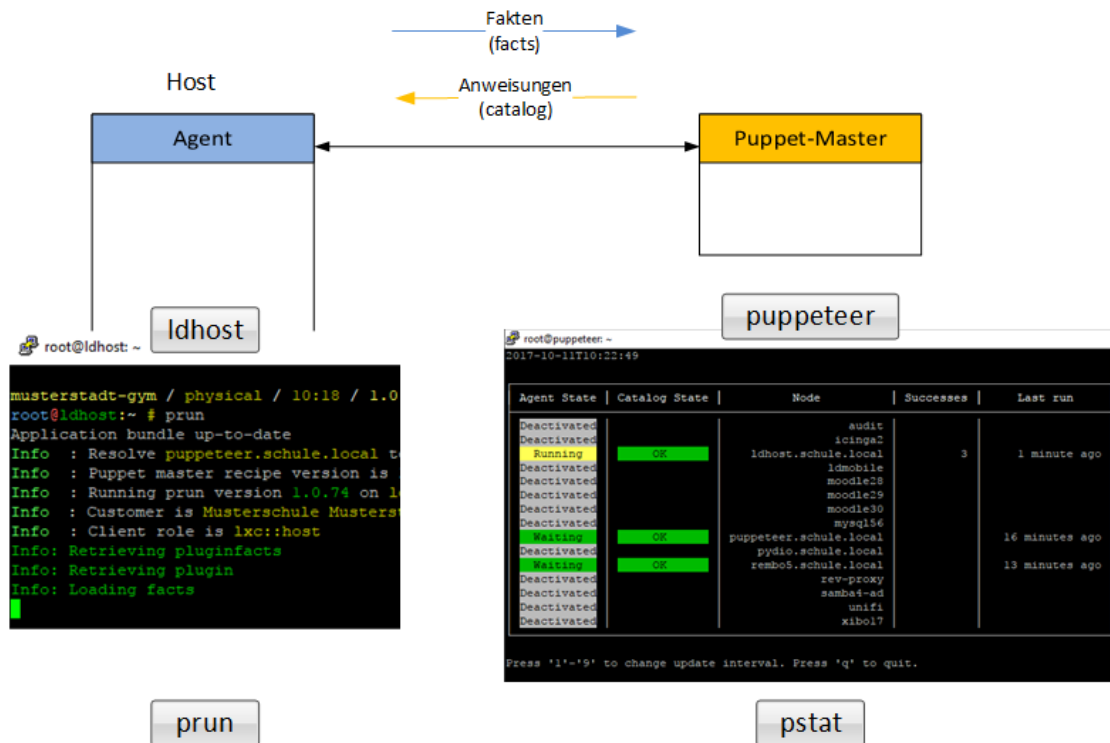
Wenn Sie direkt am Server arbeiten, können Sie mehrere Terminals gleichzeitig öffnen und zwischen diesen sehr schnell hin und herwechseln. Beim Login als root am Server befinden Sie sich im Terminal 1 (tty1) und es stehen per Standard drei weitere Terminals zur Verfügung (tty2, tty3 und tty4).

Das zweite Terminal öffnen Sie mit alt+F2 und die weiteren Terminals entsprechend. Im Terminal 2 müssen Sie sich dann zunächst wieder als root anmelden und können dann ausgehend vom Host z.B. per lxc-attach in den Container puppeteer wechseln.

Sie wechseln zwischen den Sitzungen bzw. Terminals mit dem gleichen Befehl wie beim Öffnen, d.h. mit alt+F1 schalten Sie sich auf das Terminal 1 und mit alt+F2 auf das Terminal 2.

Ähnlich können Sie natürlich vorgehen, wenn Sie mit dem Tool putty von einem Windows-Client aus auf den Server zugreifen. Dann starten Sie dieses Programm einfach zwei Mal und halten damit zwei getrennte Sitzungen und Fenster offen, mit denen Sie ebenfalls quasi parallel arbeiten können.

Das Arbeiten mit mehreren Sitzungen ist in folgender Abbildung dargestellt. Im rechten Fenster stehen Sie dabei im Container puppeteer, ändern die Konfiguration, veröffentlichen diese im git und verfolgen anschließend über **pstat**, was passiert.



Im Beispiel der Änderung des Schulnamens wird durch das Übertragen ins git-Repository im Hintergrund auch der Befehl **map_translate** aufgerufen, der die Anweisungen für den Puppeteer in dessen Sprache YAML übersetzt.

In diesem Fall gibt man im Hostsystem den Befehl **prun** ein, während man in der zweiten Konsole im Puppeteer innerhalb von **pstat** sieht, dass der Agent des Hostsystems nun läuft.

Agent State	Catalog State	Node	Successes	Noops	Skips	Failures	Last run
Deactivated		audit					
Deactivated		icinga2					
Running	OK	ldhost.schule.local	4				21 minutes ago
Deactivated		ldmobile					

Durch den **prun** im Hostsystem holt sich der Agent die Anweisungen, um den Schulnamen anzupassen und führt die notwendigen Aktionen durch. Über den Befehl **ldinfo** ist im Hostsystem das Ergebnis sofort zu sehen und der Name der Schule lautet jetzt nicht mehr "Musterschule Musterstadt" sondern "Gymnasium Musterstadt".

```

root@ldhost:~ # ldinfo
Welcome to...
  logoDIACT 2.0
  /ldhost.schule.local /physical

Server : musterstadt-gym / Gymnasium Musterstadt
Load   : 0.70 / 0.48 / 0.41
Assurance : 2018-10-04 @ 10-10 16:35
Puppet  : 2017-10-10/16:57 R:714 C:7
LXC     : logosrv,puppeteer,rembo5
    
```


III.3.3.3.4. Zentrale Aktualisierung mit ldupdate

Der Updatemechanismus unter LogoDIDACT 2.0 oder höher berücksichtigt das Updaten sämtlicher virtueller Maschinen und auch des Hosts. Eine Ausnahme dabei bildet der "alte LogoDIDACT 1.0" im Container logosrv, der nicht von Puppet gemanagt wird. Dieser muss manuell aktualisiert werden.

Der Mechanismus des neuen **ldupdate** ist kombiniert mit der Versionsverwaltung git. Solange es im Container puppeteer innerhalb `/etc/logodidact/` Konfigurationsänderungen gibt, die nicht in git eingepflegt wurden, kann das ldupdate nicht durchgeführt werden.

Sofern es keine Konfigurationsänderungen gibt bzw. alle in git eingepflegt wurden, starten Sie die Aktualisierung des Gesamtsystems mittels:

ldupdate

Ab Puppet-Rezeptstand 1.4.x bricht der Update-Prozess nicht mehr ab, wenn Änderungen in git nicht eingepflegt wurden, sondern öffnet automatisch ein Hinweifenster, das explizit zur Eingabe der Änderungen auffordert

III.3.3.3.5. Zentrales Passwortmanagement

Sofern ein Container beim automatisierten Aufbau ein administratives Konto benötigt, wird automatisch ein entsprechend komplexes Kennwort generiert und in einer kleinen **redis** Datenbank auf dem **puppeteer** zwischengespeichert. Die **redis** Datenbank fungiert dabei nur als Cacher (zudem readonly) und kann im Zweifelsfall auch gelöscht und neu aufgebaut werden. Sie eignet sich aber sehr gut, um den Namen und das Kennwort eines administrativen Benutzers für einen speziellen Dienst abzufragen.

Über den Befehl **redis-cli keys '*admin*'** lassen sich zunächst alle administrativen Konten anzeigen, sofern die Container aktiviert sind und die Dienste ein entsprechendes Konto mitbringen:

```
root@puppeteer:~ # redis-cli keys '*admin*'
1) "samba4-ad-administrator.random.pass"
2) "ldmobile::orga-admin.random.pass"
```

Gegebenenfalls führt die Suche über alle administrativen Konten schneller zum Ziel:

redis-cli keys '*' | grep pass

```
root@puppeteer:~ # redis-cli keys '*' | grep pass
rembo5.java.store.pass
nextcloud-g1.schule.local::adminpass.random.pass
ldmobile.schule.local_state.random.pass
mysql56.schule.local.random.pass
check-aggregate.random.pass
samba:ld-ldap-auth.random.pass
ldmobile::orga-admin.random.pass
nextcloud-g1.schule.local::dbpass.random.pass
samba4-ad-administrator.random.pass
audit.java.store.pass
```

Über den Befehl **redis-cli get NAME** lässt sich das Kennwort abfragen, z.B. konkret für **ldmobile**:

```
redis-cli get ldmobile::orga-admin.random.pass
```

III.3.3.4. Container aufbauen

Sämtliche Grundlagen zum Management in Puppet wurden in den vorherigen Abschnitten erläutert und die dazu notwendigen Befehle und Tools erklärt. In diesem Abschnitt wird der Aufbau eines Containers exemplarisch anhand von PYDIO beschrieben.

Welche Container auf welchem Host laufen, wird im Puppeteer über die Ordnerstruktur `/etc/logodidact/hosts` festgelegt und konfiguriert. In einem System mit nur einem physischen Server gibt es in diesem Verzeichnis auch nur einen „Host“, in unserem Fall Namens „**ldhost**“.

Sämtliche Konfigurationen für diese Standardkonstellation von LogoDIDACT 2.0 befinden sich also unter `/etc/logodidact/hosts/ldhost`.

Wechseln Sie in dieses Verzeichnis:

```
cd /etc/logodidact/hosts/ldhost
```

Öffnen Sie die Datei `quest.conf` mit einem Editor Ihrer Wahl, wie z.B. Nano:

```
nano quest.conf
```

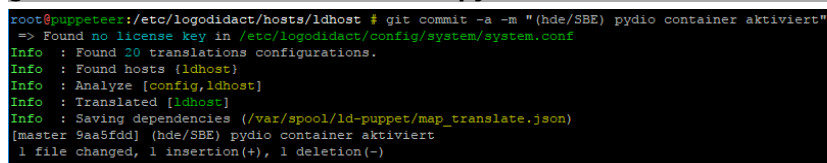
Ändern Sie dort den Eintrag für den Container `pydio` von **reserved** auf **running**.



```
GNU nano 2.2.6 File: quest.conf Modified
[Guest pydio]
Ensure running
[Guest rembo5]
Ensure running
^G Get Help ^C WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^M Exit ^O Justify ^W Where Is ^V Next Page ^U UnCut Text ^I To Spell
```

Durch Eingabe der Tastenkombination `<Strg>+<X>` verlassen Sie den Editor und geben „Y“ ein, damit die Änderung gespeichert wird. Übertragen Sie anschließend die Änderungen ins Versionierungssystem git ein:

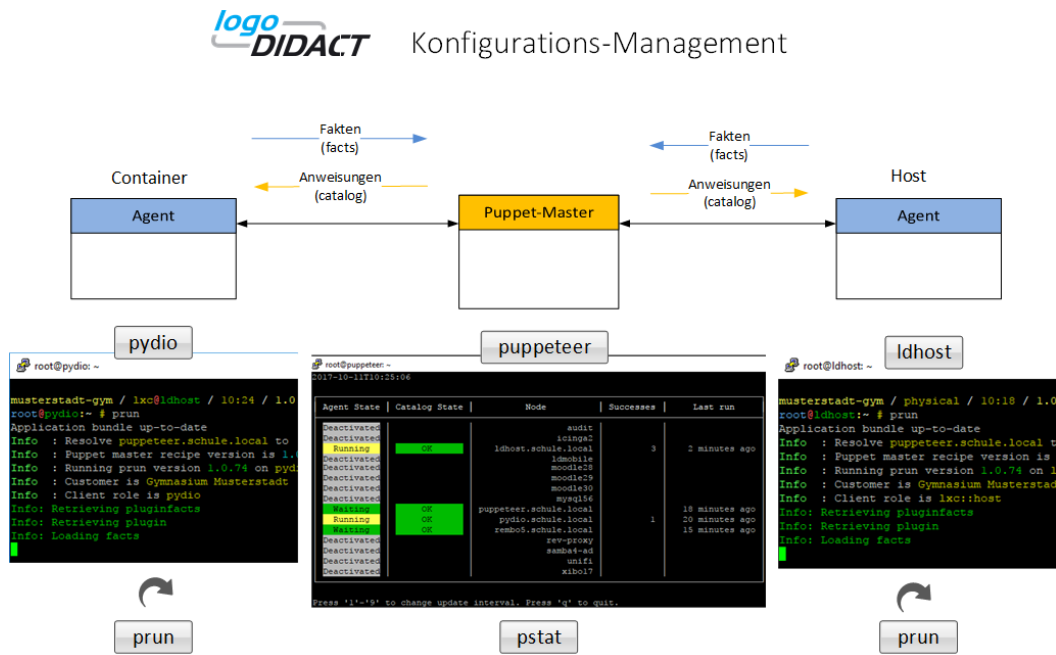
```
git commit -a -m "(hde/SBE) pydio container aktiviert"
```



```
root@puppeteer:/etc/logodidact/hosts/ldhost # git commit -a -m "(hde/SBE) pydio container aktiviert"
=> Found no license key in /etc/logodidact/config/system/system.conf
Info : Found 20 translations configurations.
Info : Found hosts {ldhost}
Info : Analyze [config,ldhost]
Info : Translated [ldhost]
Info : Saving dependencies (/var/spool/ld-puppet/map_translate.json)
[master 9aa5fdd] (hde/SBE) pydio container aktiviert
1 file changed, 1 insertion(+), 1 deletion(-)
```

Durch das Übertragen ins git-Repository wird auch automatisch `map_translate` aufgerufen, so dass die Konfigurationen in YAML übersetzt und von Puppet verarbeitet werden können.

Das Arbeiten mit mehreren Sitzungen wurde weiter oben bereits erklärt und beim Aufbau eines Containers sind in der Regel drei Sitzungen hilfreich. Das wird in der folgenden Abbildung veranschaulicht. Im mittleren Fenster stehen Sie dabei im Container puppeteer. Dort haben Sie gerade die Konfiguration geändert und in git veröffentlicht und starten jetzt **pstat**, um den Ablauf zu verfolgen.



Im rechten Fenster stehen Sie im Hostsystem und rufen dort **prun** auf. Jetzt beobachten Sie innerhalb von pstat den Durchlauf des Agenten im Host. Dieser wird mit "running" angezeigt. In der Spalte "Successes" sehen Sie, wie viele Aktionen beim letzten Durchlauf des Agenten abgearbeitet wurden.

Die folgende Abbildung des Hosts zeigt, wie sich der Agent mit dem Puppeteer in Verbindung setzt, um eine neue Catalog-Datei zu laden. In der Ausgabe erkennt man, dass der Name des Containers pydio auftaucht, der aufgebaut werden soll.

```

root@ldhost:~ # prun
Application bundle up-to-date
Info : Resolve puppeteer.schule.local to [172.28.28.5]
Info : Puppet master recipe version is 1.0.74
Info : Running prun version 1.0.74 on ldhost
Info : Customer is Gymnasium Musterstadt (musterstadt-gym)
Info : Client role is lxc:host
Info : Retrieving pluginfacts
Info : Retrieving plugin
Info : Loading facts
Info : Caching catalog for ldhost.schule.local
Info : Applying configuration version '1507657334'
Notice: /Stage[main]/Profile::Lxc::Host/Ld_lxc::Container[pydio]/File[/var/lib/puppet/scratch.d/ld_lxc/pydio]/ensure: created
Notice: /Stage[main]/Ld_ovs/Package[openvswitch-common]/ensure: ensure changed 'held' to 'present'
Notice: /Stage[main]/Ld_ovs/Package[openvswitch-switch]/ensure: ensure changed 'held' to 'present'
    
```

Es ist natürlich wenig sinnvoll jetzt mehrfach nacheinander einen **prun** durchzuführen, ohne zu wissen, was das System in etwa tut. Im Fall des Aufbaus eines neuen Containers ist es erst mal so, dass der Hosts einiges zu tun hat und das etwas Zeit in Anspruch nimmt.

Die in der obigen Abbildung gezeigte dritte Sitzung (links) ist zu diesem Zeitpunkt noch gar nicht möglich, weil der Container (in diesem Beispiel pydio) ja gerade grundlegend aufgebaut wird. Das kann je nach Größe eines Containers und Geschwindigkeit des Servers einige Minuten dauern. Erst danach ist es überhaupt erst möglich in einer dritten Sitzung per **lxc-attach -n pydio** in den Container zu wechseln.

Sobald das möglich ist, können Sie dort im Container (hier pydio) einen **prun** starten. Beim Aufbau eines Containers ist es in aller Regel so, dass mehrere dieser pruns notwendig sind, bis er fertig ist. Wie viele das sind, kann man nicht genau vorhersagen, weil es Abhängigkeiten zu anderen Containern und zum Host geben kann, die eine Vorhersage unmöglich machen.

In der Praxis ist es aber tendenziell so, dass bei jedem neuen prun in der Regel weniger Befehle abgearbeitet werden und sich der Wert in der Spalte Successes einem Endwert nähert. Dieser Endwert muss übrigens nicht 0 sein, denn es ist manchmal notwendig, dass ein bestimmter Wert im Container

oder Host bei jedem Durchlauf gesetzt werden muss, so dass der Agent diese Aktion dann auch immer als Success zurückliefert.

Waiting	OK	puppeteer.schule.local			11 minutes ago
Running	OK	pydio.schule.local	146	2	1 minute ago
Waiting	OK	rembo5.schule.local			6 minutes ago
Deactivated		rev-proxy			
Deactivated		samba4-ad			
Deactivated		unifi			
Deactivated		xibol7			

Press 'l'-'9' to change update interval. Press 'q' to quit.

III.3.3.5. Container löschen

Das Aufbauen eines Containers ist in LogoDIDACT 2.0 ein Automatismus, der mittels Puppet durchgeführt wird. Wie oben beschrieben, reicht es dazu aus, ein Modul in der Datei `/etc/logodidact/hosts/ldhost/guest.conf` als neuen "Gast" einzutragen und ihm den Parameter **Ensure running** zu geben.

```

GNU nano 2.2.6      File: guest.conf      Modified
[Guest pydio]
Ensure running

[Guest rembo5]
Ensure running
  
```

Alles andere passiert dann vollkommen automatisiert.

Dass es für das Entfernen eines Containers keinen Automatismus gibt, ist leicht verständlich, wenn man das folgende Szenario betrachtet. Stellen Sie sich vor, Sie würden versehentlich Einträge in der Datei `guest.conf` oder die gesamte Datei löschen und Puppet würde automatisch mit dem Abbau Ihres Systems beginnen. Dann hätten Sie nach wenigen Minuten nichts mehr außer ein Basissystem bestehend aus `ldhost` und dem `puppeteer`.

Das Löschen eines Containers findet deshalb manuell in mehreren Schritten statt. Zunächst muss der Eintrag aus der `guest.conf` gelöscht werden, andernfalls würde der Container erneut aufgebaut werden.

Im zweiten Schritt ist im Container `puppet` der folgende Befehle einzugeben, wobei im Beispiel der Container `pydio` entfernt wird:

puppet-master-remove-client pydio

Pflegen Sie danach die Änderung wieder in das Versionssystem `git` ein, damit klar ist, wer wann was gemacht hat.

git commit -a -m "container pydio entfernt"

Wechseln Sie danach wieder in den `ldhost` und geben Sie dort den Befehl

lxc-destroy -n pydio -f

III.3.4. Aktivierung samba4-ad

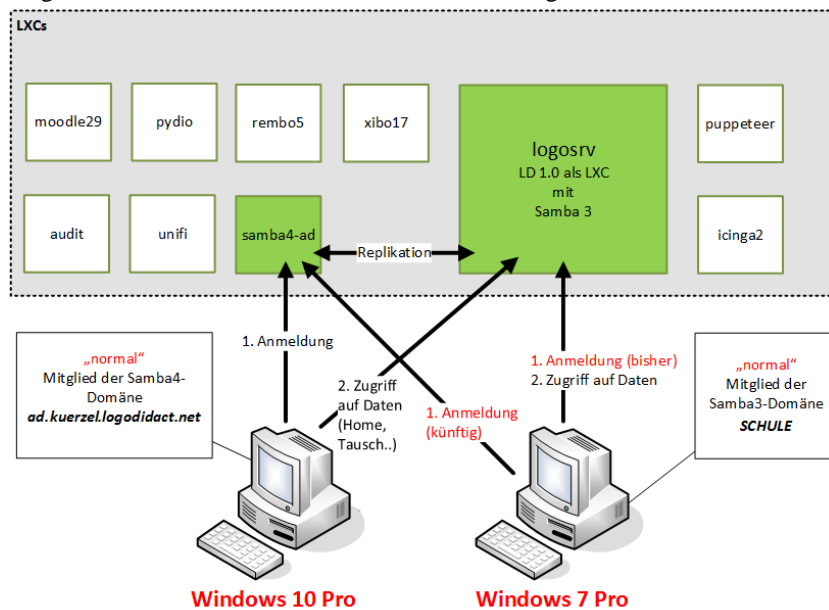
Im vorherigen Abschnitt wurde gezeigt, wie ein Container in LogoDIDACT 2.0 aktiviert wird und wie man den Aufbau eines Containers mit den Werkzeugen in und um Puppet beobachtet und steuert.

Ein essentiell wichtiger Baustein in LogoDIDACT 2.0 ist Samba 4 und damit die Emulation eines Active Directory (AD) auf Serverseite. Dieses AD wird im Container `samba4-ad` bereitgestellt und ermöglicht es beispielsweise neue PCs mit dem Betriebssystem Windows 10 in der Domäne zu betrei-

ben. Auch die Einbindung von Geräten mit Apple-Betriebssystem ist am AD deutlich einfacher als an der alten Samba3-Domäne und auch PCs mit Windows 7 lassen sich problemlos anbinden.

Ungeachtet dessen besteht die Samba3 Domäne im Container logosrv vorerst weiter und wird erst im Laufe der Zeit entfallen. Dafür gibt es einige gute Gründe. So wie es bei neuen Systemen deutlich einfacher ist, sie in das AD einzubinden, ist es bei alten Systemen wie Windows XP deutlich schwieriger und nur bedingt sinnvoll. In der Praxis erleichtert der Parallelbetrieb von Samba 3 und Samba 4 (AD) den Bestandskunden Windows 10 mit neuen PCs "sanft" einzuführen, ohne alle anderen Rechner zwangsweise ins AD nehmen zu müssen.

In der folgenden Abbildung ist der Parallelbetrieb von Samba4 AD und Samba3 dargestellt, sowie die möglichen Konstellationen der Domänenanbindung.



Tipp

Bei einer Neuinstallation von LogoDIDACT 2.0 sollten sowohl Windows 10 als auch Windows 7 Arbeitstationen an das neue Samba 4 AD angebunden werden.

III.3.4.1. Samba 4 Domännennamen festlegen

Bevor der Samba4-Container aufgebaut wird, sollte der Domännennamen festgelegt bzw. nochmals geprüft werden. Bei der Neuinstallation haben Sie diesen Namen bereits festgelegt, können ihn aber jetzt noch ändern.

Wechseln Sie in den Container puppeteer und editieren Sie die Datei `/etc/logodidact/config/customer.conf`.



Achtung

Der Eintrag ShortName bestimmt den Domännennamen! Nicht erlaubt sind Leerzeichen, Sonderzeichen, Umlaute und auch kein Unterstrich! Wir empfehlen die Verwendung von Kurzbezeichnungen, wie z.B. heilbronn-hfs oder hn-hfs als Abkürzung für „Hans-Fallada-Schule Heilbronn“ (LongName).

Wenn das AD erst einmal aufgebaut haben und Clients in die Domäne genommen haben, können und dürfen Sie den Domänennamen nicht mehr ändern. Das führt zwangsweise dazu, dass sie alles neu machen müssen!

Im weiteren Verlauf werden beispielhaft die Einträge verwendet, wie sie bereits bei der Installation festgelegt wurden.

```
[customer]
ShortName musterstadt-gym
LongName Gymnasium Musterstadt
```

III.3.4.2. Samba 4 Domäne aufbauen (lassen)

Der Samba 4 Container wird nach dem gleichen Schema aufgebaut, wie bereits in den Grundlagen zu Puppet ausführlich beschrieben. Bitte beachten Sie unbedingt die Hinweise und Erklärungen dort, um zu verstehen, wie ein Container durch Puppet automatisch aufgebaut wird und was Sie dabei machen können und was Sie dabei auf keinen Fall tun dürfen.

Wechseln Sie in den Puppeteer:

```
lxc-attach -n puppeteer
```

Wechseln Sie in das Verzeichnis zur Konfiguration von Containern:

```
cd /etc/logodidact/hosts/ldhost
```

Öffnen Sie die Datei `guest.conf` mit einem Editor Ihrer Wahl, wie z.B. Nano:

```
nano guest.conf
```

Fügen Sie dort den Eintrag für den Container `samba4-ad` hinzu.

```
[Guest samba4-ad]
Ensure running
```

Durch Eingabe der Tastenkombination `<Strg>+<X>` verlassen Sie den Editor Nano und geben „Y“ ein, damit die Änderung gespeichert wird. Wechseln Sie dann ins Stammverzeichnis der Konfiguration und übertragen Sie anschließend die Änderungen ins Versionierungssystem git:

```
cd /etc/logodidact
```

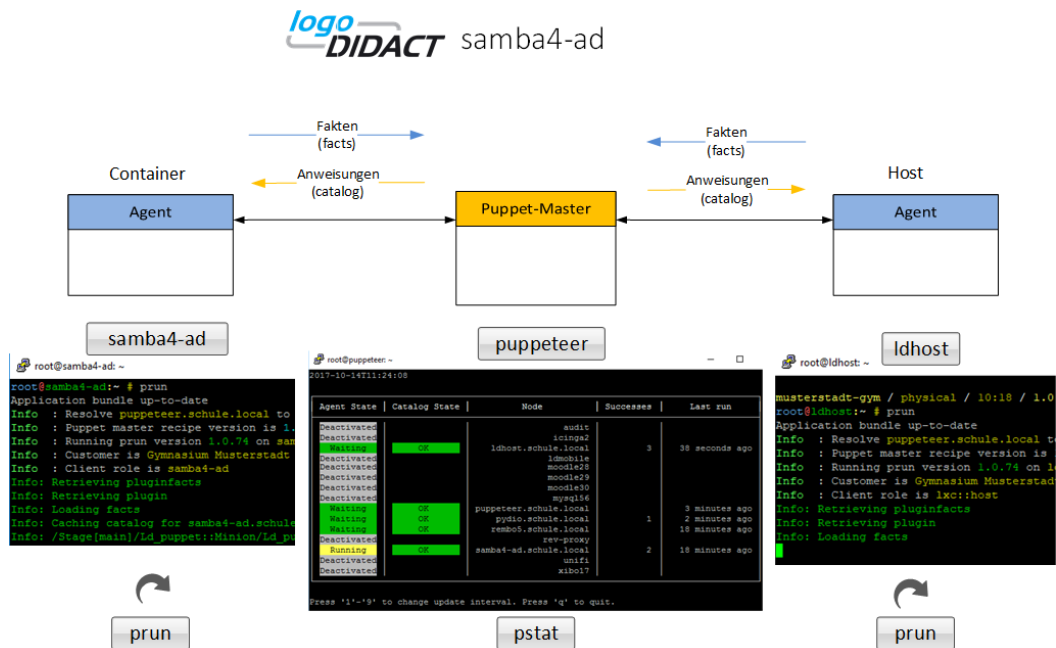
```
git add .
```

```
git commit -m "(hde/SBE) Aktivierung samba4-ad"
```

Durch das Übertragen ins git-Repository wird auch automatisch `map_translate` aufgerufen, so dass die Konfigurationen in YAML übersetzt und von Puppet verarbeitet werden können.

Wie in den Grundlagen beschrieben, gibt es nun zwei Möglichkeiten. Sie können abwarten, bis der zyklisch stattfindende Durchlauf des Puppet Agenten im Host mitbekommt, dass er einen neuen Container aufbauen soll und sein Werk verrichtet. Danach wird der Agent im `samba4-ad` Container mehrere Durchläufe benötigen, bis er das AD vollständig aufgebaut hat. Das Ganze kann je nach Konstellation in etwa einer Stunde erledigt sein.

Alternativ können Sie das Ganze kontrolliert beschleunigen, wenn Ihnen die Zusammenhänge in Puppet klar sind.



Mit einem **prun** im Host veranlassen Sie den Agenten sich beim Puppeteer zu melden. Dieser baut die Catalog-Datei für den ldhost und schickt sie ihm. Der ldhost beginnt dann mit dem Aufbau des Containers samba4-ad. Beobachten können Sie das Ganze mit pstat im Puppeteer. Nach einer Weile wird dort der Container samba4-ad auftauchen. Sofern der Container grundlegend aufgebaut ist und läuft, kann man in einer neuen Sitzung per **lxc-attach -n samba4-ad** dort hineinwechseln und sofern gerade kein prun läuft einen solchen neuen Durchlauf mit **prun** starten.

Agent State	Catalog State	Node	Successes	Noops	Skips	Failures	Last run
Deactivated		audit					
Deactivated		icinga2					
Waiting	OK	ldhost.schule.local	30				5 minutes ago
Deactivated		moodle28					
Deactivated		moodle29					
Deactivated		moodle30					
Waiting	OK	puppeteer.schule.local	10				6 minutes ago
Deactivated		pydio					
Waiting	OK	remn05.schule.local	6				4 minutes ago
Waiting	OK	samba4-ad.schule.local	136				4 minutes ago
Deactivated		unifi					
Deactivated		xibo17					

Der Container benötigt wieder mehrere Durchläufe, die sie nacheinander mit **prun** aktiv starten können. Anstelle diese zu beschleunigen, können Sie parallel dazu ein Windows 10 Image am Server vorbereiten. Auf technische Ebene können Sie über die Namensauflösung feststellen, ob die Samba4-Domäne bzw. das AD bereit ist.

Das ist der Fall, sobald man über den Befehl **nslookup ad.DOMAINNAME.logodidact.net** plausible Werte erhält, wobei der **DOMAINNAME** der Name der Domäne ist (im unserem Beispiel musterstadt-gym).

III.3.4.3. Samba 4 Administration und Tools

Im Rahmen einer Neuinstallation können Sie diese Abschnitt überspringen und es ist auch eher selten notwendig sich mit den verschiedenen Tools von Samba 4 auf Serverseite zu beschäftigen. Wie in der Grafik weiter oben dargestellt, gibt es aus Gründen der Kompatibilität zu alten Clientsystemen noch immer einen Parallelbetrieb von Samba 3 und Samba 4.

Nicht alles, was es in Samba 3 gibt, wird dabei nach Samba 4 synchronisiert.

III.3.4.3.1. Das Konto ld-su-domjoin

Im Zusammenhang mit dem Imagingsystem **lddeploy** gibt es auf Serverseite in Samba 4 (nur dort) den administrativen Benutzer **ld-su-domjoin**. Dieser ist ausschließlich für die Funktion des Domänenbeitritts zuständig und kann auf Serverseite Computerkonten erstellen, ändern und löschen.

Ab Puppet Rezeptstand 1.3.0 wird dieser Benutzer automatisch angelegt und ein komplexes Kennwort generiert. Ob der Benutzer angelegt wurde, lässt sich über das Samba-Tool `pdbedit` (Password Database) prüfen. Wechseln Sie in den Container **samba4-ad** und lassen Sie sich zunächst Infos zum Konto anzeigen:

```
pdbedit -v ld-su-domjoin
```

Sie dürfen das Kennwort dieses Kontos nicht ändern. Sollte das versehentlich doch einmal der Fall sein, wechseln Sie in den Container **ctrl-gl** und starten Sie den ControlService neu:

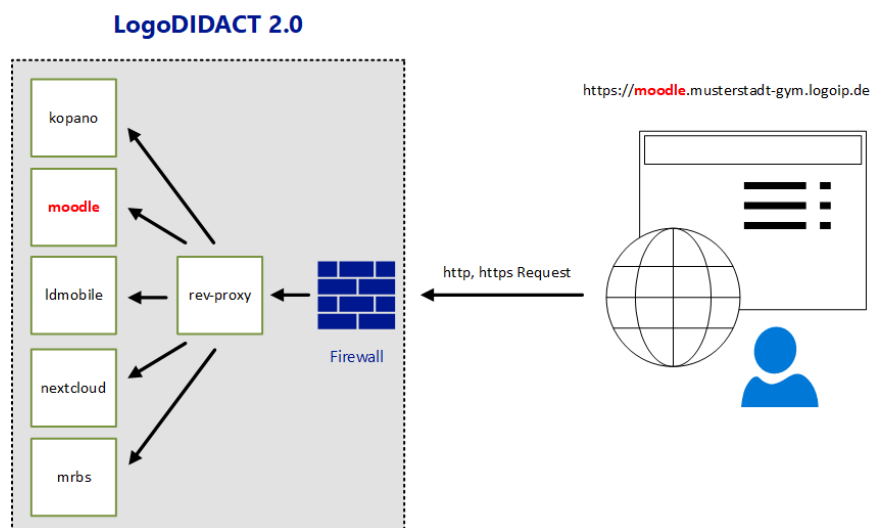
```
systemctl restart ld-control-service
```

Das Kennwort wird dadurch wieder auf einen komplexen Wert gesetzt und in die Datenbank synchronisiert.

III.3.5. Reverse-Proxy

Ähnlich wie Samba 4, gehört auch der Reverse-Proxy zu den Bausteinen bzw. Containern in LogoDIDACT 2.0, die als Standard aktiviert werden sollten.

Der Reverse-Proxy ermöglicht einen einfachen und sicheren Zugriff über das Internet von außen auf die vielen Web-Dienste des Servers. Diese Konstellation ist in der folgenden Grafik dargestellt und es geht konkret um das Freischalten von Web-Diensten.



Ein riesiger Vorteil von LogoDIDACT besteht gerade darin, dass alle Dienste zunächst lokal auf dem Server der Schule liegen. Man kann diese Dienste auch in "die Cloud" bzw. besser konkret in ein Rechenzentrum legen, aber der erste, einfachste und sicherste Weg ist zunächst der Server an der Schule. In jedem Fall sollten Sie wissen, wo die Daten von Schülern und Lehrern liegen. Im Falle von LogoDIDACT verlassen diese Daten die Schule auch nicht, wenn Sie per Web-Browser von außen darauf zugreifen. Damit sind Sie also auf der sicheren Seite. Der Reverse-Proxy sorgt dabei für eine höhere Sicherheit, weil die interne Struktur verborgen bleibt.

III.3.5.1. Vorbereitungen und Voraussetzungen

Wie anhand des obigen Beispiels zu erkennen, erfolgt der Zugriff von außen über den Reverse-Proxy auf Basis eines DNS-Namens wie z.B.

```
https://moodle.musterstadt-gym.logoip.de.
```

Damit das funktioniert, muss sich der LogoDIDACT-Server per **ldipupdate** mit dem richtigen Schulkürzel an dem von SBE bereitgestellten DynDNS **logoip.de** melden.

Die Konfiguration dafür findet sich im Container **logosrv** in der Datei `/etc/logodidact/service.conf` im Abschnitt **[IPUpdate]**. Bitte prüfen Sie den Eintrag bzw. passen diesen an, wie in Abschnitt III.4.1.1.1, „Dynamischer Rechnername“ ausführlich beschrieben.

III.3.5.2. Container rev-proxy aufbauen

Der Container rev-proxy wird nach dem gleichen Schema aufgebaut, wie bereits in den Grundlagen zu Puppet ausführlich beschrieben. Bitte beachten Sie unbedingt die Hinweise und Erklärungen dort, um zu verstehen, wie ein Container durch Puppet automatisch aufgebaut wird und was Sie dabei machen können und was Sie dabei auf keinen Fall tun dürfen.

Wechseln Sie in den Puppeteer:

```
lxc-attach -n puppeteer
```

Wechseln Sie in das Verzeichnis zur Konfiguration von Containern:

```
cd /etc/logodidact/hosts/ldhost
```

Öffnen Sie die Datei `guest.conf` mit einem Editor Ihrer Wahl, wie z.B. Nano:

```
nano guest.conf
```

Fügen Sie dort den Eintrag für den Container rev-proxy hinzu.

```
[Guest rev-proxy]  
Ensure running
```

Durch Eingabe der Tastenkombination `<Strg>+<X>` verlassen Sie den Editor Nano und geben „Y“ ein, damit die Änderung gespeichert wird. Wechseln Sie dann ins Stammverzeichnis der Konfiguration und übertragen Sie anschließend die Änderungen ins Versionierungssystem git:

```
cd /etc/logodidact
```

```
git add .
```

```
git commit -m "Aktivierung rev-proxy"
```

Durch das Übertragen ins git-Repository wird auch automatisch `map_translate` aufgerufen, so dass die Konfigurationen in YAML übersetzt und von Puppet verarbeitet werden können.

Wie in den Grundlagen beschrieben, gibt es nun zwei Möglichkeiten. Sie können abwarten, bis das Managementsystem Puppet alles automatisiert erledigt oder das Ganze kontrolliert beschleunigen, wenn Ihnen die Zusammenhänge in Puppet klar sind.

Mit einem **prun** im Host veranlassen Sie den Agenten sich beim Puppeteer zu melden. Dieser baut die Catalog-Datei für den `ldhost` und schickt sie ihm. Der `ldhost` beginnt dann mit dem Aufbau des

Containers rev-proxy. Beobachten können Sie das Ganze mit `pstat` im Puppeteer. Nach einer Weile wird dort der Container rev-proxy auftauchen. Sofern der Container grundlegend aufgebaut ist und läuft, kann man in einer neuen Sitzung per `lxc-attach -n rev-proxy` dort hineinwechseln und sofern gerade kein `prun` läuft einen solchen neuen Durchlauf mit `prun` starten.

In der Regel sind mehrere dieser Durchläufe notwendig, bis der Container vollständig aufgebaut ist.

Agent State	Catalog State	Node	Successes	Noops	Skips	Failures	Last run
Deactivated		audit					
Deactivated		ca-g1					
Deactivated		collabora-g1					
Deactivated		icings2					
Deactivated		kpano-g1					
Waiting	OK	ldhost.schule.local	17				10 minutes ago
Deactivated		ldmobile					
Unknown	OK	logosrv					a long while ago
Deactivated		moodle30					
Deactivated		mysql56					
Deactivated		nextcloud-g1					
Deactivated		postgres10					
Waiting	OK	puppeteer.schule.local					16 minutes ago
Waiting	OK	rembo5.schule.local					15 minutes ago
Waiting	OK	rev-proxy.schule.local	155				1 minute ago
Waiting	OK	samba4-ad.schule.local	1				15 minutes ago
Deactivated		unifi					
Deactivated		xibol7					

Press 'i'-'9' to change update interval. Press 'q' to quit.

Die Anzahl an durchgeführten Anpassungen in der Spalte Successes sinkt tendenziell mit jedem Durchlauf und tendiert gegen einen Wert, der nicht notwendigerweise 0 sein muss (siehe Abschnitt III.3.3.4, „Container aufbauen“)

III.3.5.3. Den Reverse Proxy für Webdienste aktivieren

Umgesetzt ist der Reverse-Proxy über `nginx`. Die Konfiguration der über den rev-proxy erreichbaren Dienste ist denkbar einfach.

Wechseln Sie in den Puppeteer:

```
lxc-attach -n puppeteer
```

Wechseln Sie in das Verzeichnis zur Konfiguration von Containern:

```
cd /etc/logodidact/hosts
```

Erstellen Sie den Ordner `rev-proxy` für die Konfiguration des Reverse-Proxy-Servers und wechseln Sie in das Verzeichnis:

```
mkdir rev-proxy
```

```
cd rev-proxy
```

Erstellen Sie mit einem Editor Ihrer Wahl die Datei `revproxy.conf` mit folgendem Inhalt:

```
[ReverseProxy mrbs.SCHULKUERZEL.logoip.de]
Url http://mrbs.schule.local
```

Das Schulkürzel entspricht dabei in der Regel wieder dem zuvor festgelegten Domännennamen, d.h., in unserer beispielhaften Umgebung `musterstadt-gym`.

Alternativ können Sie aus dem Unterordner `/usr/share/doc/ld-puppet10/hosts/rev-proxy` die Vorlagedatei `revproxy.sample` kopieren und anpassen.

Pflegen Sie die Änderungen wie gewohnt ins git ein:

```
cd /etc/logodidact
```

```
git add .
```

```
git commit -m "Konfiguration rev-proxy"
```

III.3.5.4. Ports an den Reverse Proxy weiterleiten

Nach Aufbau des Containers **rev-proxy** müssen die Ports 80 und 443 in der Firewall des Basissystems **ldhost** entsprechend zum Reverse-Proxy hin weitergeleitet werden.

Prüfen Sie zunächst im Container **rev-proxy** die IP-Adresse des Containers in der DMZ:

```
ip address show dmz
```

Im Normalfall liegt die IP im Bereich 172.28.29.x. Notieren Sie sich diese IP und wechseln Sie in den **ldhost** und dort in das Verzeichnis der Firewall:

```
cd /etc/shorewall
```

Öffnen Sie die Datei **rules** mit einem Editor Ihrer Wahl und tragen Sie dort die zuvor ermittelte IP an erster Stelle wie unten dargestellt ein:

```
#
# Shorewall version 4.0
#

DNAT ext dmz:172.28.29.3 tcp 80,443
DNAT ext dmz:172.28.29.2 tcp 1:21
DNAT ext dmz:172.28.29.2 tcp 23:2221
DNAT ext dmz:172.28.29.2 tcp 2223:65535
DNAT ext dmz:172.28.29.2 udp 1:65535
```

Speichern Sie die Datei und starten Sie die Firewall im **ldhost** neu

```
/etc/init.d/shorewall restart
```

Im Anschluss an das Neustarten der Firewall werden sämtliche HTTP-/HTTPS-Anfragen an den LogoDIDACT-Server von extern an den Container **rev-proxy** weitergeleitet. Die Voraussetzung dafür ist natürlich, dass der Router an externen Interface entsprechend konfiguriert ist. Entweder sind dort einzelne Portweiterleitungen definiert oder es ist die DMZ Host Funktion aktiviert.

III.3.6. Zertifikate mit Let's Encrypt

Dass man Webdienste heutzutage nur noch per **https** anspricht und damit verschlüsselt kommuniziert, ist hinlänglich bekannt. Um jedoch zu gewährleisten, dass man auch tatsächlich mit der richtigen Gegenstelle kommuniziert und die verschlüsselten Daten auch dort ankommen, wo sie sollen, gibt es digitale Zertifikate.

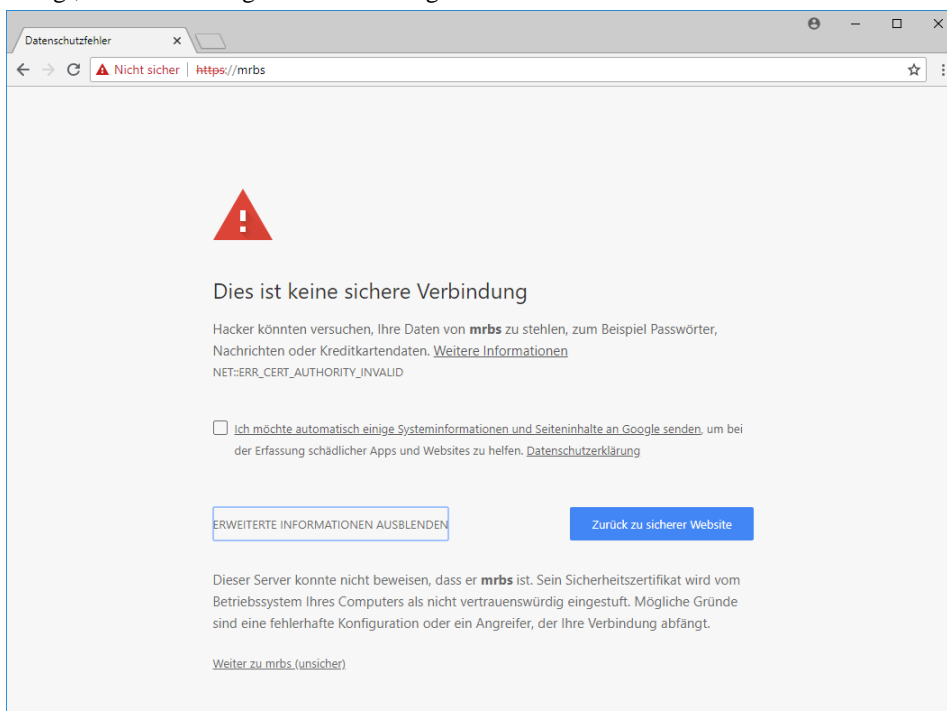
In LogoDIDACT wird dafür Let's Encrypt (deutsch „Lasst uns verschlüsseln“) als Zertifizierungsstelle genutzt, die Ende 2015 in Betrieb gegangen ist und kostenlose X.509-Zertifikate für Transport Layer Security (TLS) anbietet. Dabei ersetzt ein automatisierter Prozess die bisher gängigen komplexen händischen Vorgänge bei der Erstellung, Validierung, Signierung, Einrichtung und Erneuerung von Zertifikaten für verschlüsselte Websites.



III.3.6.1. Digitale Zertifikate

Ein digitales Zertifikat enthält identifizierende Informationen über die Webseite oder den Service für den das Zertifikat ausgestellt wurde, sowie Informationen über den Aussteller des Zertifikats, die Gültigkeitsdauer, das Ausstellungs- und Ablaufdatum und nicht zuletzt eine einzigartige Signatur. Diese Signatur ist der wichtigste Teil des digitalen Zertifikats. Die Signatur bestätigt, dass man genau mit demjenigen kommuniziert, mit dem man es möchte und dass die Kommunikation verschlüsselt übertragen wird.

Der erste Webservice, der während der Grundinstallation von LogoDIDACT sehr früh und automatisch zur Verfügung steht, ist das Raumbuchungssystem **mrbs**. Wenn man dieses vom internen Netzwerk im Browser per `https` aufruft, erhält man eine wenig vertrauenserweckende Rückmeldung, die besagt, dass es kein digitales Zertifikat gibt.



Diese Meldung würde man nun für jeden der webbasierten Dienste sowohl im internen Netzwerk erhalten, als auch beim Zugriff von außen bzw. von zu Hause. Obwohl diese Verbindungen nicht wirklich unsicher sind und man für jeden Dienst eine Ausnahme definieren und der Seite vertrauen kann, ist es besser, entsprechende Zertifikate bereitzustellen.

III.3.6.2. Let's encrypt aktivieren

Solange keine eigenen Zertifikate existieren, können und sollten Zertifikate von Let's Encrypt genutzt werden. Dies funktioniert jedoch erst, nachdem der Container **rev-proxy** vollständig aufgebaut ist Abschnitt III.3.5, „Reverse-Proxy“ .

Für Let's Encrypt gibt es keinen separaten Container, weil letztlich nur ein Zertifikat generiert und zentral bereitgestellt wird. Da der Puppeteer die zentrale Managementkomponente ist, wird Let's Encrypt in diesem Container konfiguriert.

Wechseln Sie in den Puppeteer:

```
lxc-attach -n puppeteer
```

Wechseln Sie in das Verzeichnis zur Konfiguration von Containern:

```
cd /etc/logodidact/hosts
```

Erstellen Sie den Ordner `puppeteer` für die Konfiguration von Let's Encrypt und wechseln Sie in das Verzeichnis:

```
mkdir puppeteer
```

```
cd puppeteer
```

Erstellen Sie mit einem Editor Ihrer Wahl die Datei `letsencrypt.conf` mit folgendem Inhalt:

```
[LetsEncrypt]
Ensure present
AccountMail support@sbe.de
```

Pflegen Sie die Änderungen wie gewohnt gleich ins git ein:

```
cd /etc/logodidact
```

```
git add .
```

```
git commit -m "Aktivierung von Let's Encrypt"
```

III.3.6.3. Zertifikat erstellen

Bevor Sie das Zertifikat versuchen zu erstellen, prüfen Sie kurz die Verfügbarkeit der Zertifizierungsstelle. Gehen Sie dazu mit einem Webbrowser auf die Internetseite `https://letsencrypt.status.io/` und prüfen Sie, ob die Dienste dort verfügbar sind oder es eventuell Probleme gibt.

Um die Registrierung oder Erneuerung von Zertifikaten durchzuführen, wird in LogoDIDACT bisher (Stand August 2021) die Software `acmetool` verwendet.



Achtung

Mit dem Tool `acme.sh` gibt es ab Puppet-Rezeptstand 1.4.1-x ein neueres und besser gepflegtes Werkzeug, um Zertifikate zu beantragen und erneuern.

III.3.6.3.1. Umstellung auf das Tool `acme.sh`

Im folgenden Abschnitt wird beschrieben, wie Sie auf das Tool `acme.sh` umstellen, um die Zertifikate bei Let's Encrypt darüber zu verwalten.

Gehen Sie dazu in den Container Puppeteer und wechseln in das Verzeichnis für spezifische Anpassungen:

```
lxc-ssh -n puppeteer
```

```
cd /etc/logodidact/hiera/custom.d
```

Erstellen Sie dort die Datei `puppeteer.yaml` mit folgendem Inhalt, um `acme.sh` zu verwenden:

```
ld_acme::client: 'acme.sh'
ld_acme::ensure: 'present'
```

Wenn Sie weiterhin `acmetool` nutzen wollen, sieht der Inhalt wie folgt aus:

```
ld_acme::client: 'acmetool'
ld_acme::ensure: 'present'
```

Pflegen Sie die Änderungen wie gewohnt ins git ein, um diese nachvollziehen zu können:

```
cd /etc/logodidact
```

```
git add .
```

```
git commit -m "Verwaltung der Zertifikate über acme.sh"
```

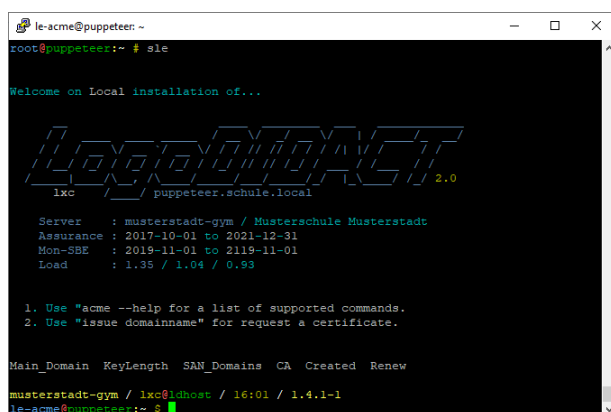
Über einen `prun` im Container Puppeteer wird das neue Tool dort installiert.

III.3.6.3.2. Die Skripting-Umgebung sle

Im Zusammenhang mit der Installation der Pakete wird im Puppeteer eine Skripting-Umgebung eingerichtet, die über den "Benutzer" `sle` gestartet wird. Wenn Sie im Puppeteer den Befehl `alias` eingeben, wird ersichtlich, dass es sich bei `sle` um die Kurzform des Befehls `su - le-acme` handelt.

`sle` steht dabei für `sudo let's encrypt environment` und beschreibt die erwähnte neue Umgebung zur Verwaltung von Let's Encrypt Zertifikaten.

Sollte die Eingabe von `sle` nicht gleich funktionieren, verlassen Sie den Container über `exit` und wählen sich neu ein. Über `sle` gelangt man in einen anderen Benutzerkontext und kann sich dort auch eine Liste der verfügbaren Befehle anzeigen lassen.



```
le-acme@puppeteer: ~
root@puppeteer:~# sle
Welcome on Local installation of...

Logodidact 2.0
lxc puppeteer.schule.local

Server : musterstadt-gym / Musterschule Musterstadt
Assurance : 2017-10-01 to 2021-12-31
Mon-SBE : 2019-11-01 to 2119-11-01
Load : 1.35 / 1.04 / 0.93

1. Use "acme --help" for a list of supported commands.
2. Use "issue domainname" for request a certificate.

Main_Domain KeyLength SAN_Domains CA Created Renew
musterstadt-gym / lxc@ldhoat / 16:01 / 1.4.1-1
le-acme@puppeteer:~#
```

Bevor ein Zertifikat beantragt werden kann, muss noch eine Konfiguration am DNS-Server vorgenommen werden.

III.3.6.3.3. Split-DNS konfigurieren

Split-DNS kann genutzt werden um eine Domain wie z.B. `www.meinedomain.de` nicht über das Internet aufzulösen, sondern lokal an den Rev-Proxy und darüber dann an den internen Dienst (z.B. Webserver) weiterzuleiten.

Diese Technik kann man sich auch bei Problemen mit Routern zu nutze machen. Wenn ein vorgeschalteter Router kein „NAT Loopback“ bzw. „NAT Hairpinning“ unterstützt, schickt er die erhaltenen Verbindungsanfragen über die Portweiterleitungen (80 / 443) auf demselben Interface wieder zurück, auf dem er sie erhalten hat.

Es gibt nur wenige Router, wie die Vigor-Modelle von Draytek, die NAT-Loopback von Hause aus ohne weiteres Zutun unterstützen.

Um solche Probleme zu vermeiden, kann man im Container `logosrv` im Nameserver `bind` die separate DNS-Zone `schulkuerzel.logoip.de` registrieren und diese Subdomain mit der IP des `Rev-Proxy` verknüpfen.

Wechseln Sie dazu in den `logosrv` und entfernen Sie die Kommentarzeichen in der Datei `/etc/bind/named.conf.local`, so dass der Inhalt wie folgt aussieht:

```
zone "schulkuerzel.logoip.de" {
    type master;
    file "/etc/bind/db.dynip";
    check-names ignore;
};
```

Öffnen Sie dann ebenfalls im `logosrv` die Datei `/etc/bind/db.dynip` und passen Sie die IP-Adresse auf diejenige des Containers `Rev-Proxy` an (im Standard ist dies `172.28.28.27`):

```
$TTL 1h
@           IN      SOA    ns1.schule.local. postmaster.schule.local. (
                                2009010101 ; serial
                                86400      ; refresh (1 day)
                                900       ; retry (15 minutes)
                                604800    ; expire (1 week)
                                900       ; minimum (15 minutes)
                                )

           NS     ns1.schule.local.
           NS     ns2.schule.local.

           A      172.28.28.27
*          A      172.28.28.27
```

Damit die Nutzung von Split-DNS sauber funktioniert, muss der DNS-Server neu gestartet werden:

```
/etc/init.d/bind9 restart
```

III.3.6.3.4. Zertifikat anfordern per acme.sh

Den eigentlichen Befehl, um ein Zertifikat von Let's Encrypt anzufordern geben Sie im Container `Puppeteer` wie folgt ein, nachdem Sie dort die Umgebung per `sle` gestartet haben:

issue webservice.schulkuerzel.logoip.de

Hierbei steht **schulkuerzel** für den bereits mehrfach verwendeten individuellen Namen (z.B. musterstadt-gym) und **webservice** für den Dienst (wie z.B. mrbs).

**Achtung**

Für jeden Webdienst wie z.B. mrbs, kopano, ldmobile und nextcloud muss nach obigem Schema ein eigenes Zertifikat erstellt werden. Ein einzelnes Wildcard-Zertifikate für die gesamte Domäne zu erstellen wäre prinzipiell machbar aber unnötig kompliziert oder eben mit Zusatzkosten verbunden.

In unserem konkreten Beispiel lautet der Befehl:

issue mrbs.musterstadt-gym.logoip.de

Der zweite wichtige Befehl liefert eine Übersicht über alle beantragten Zertifikate:

acme.sh --list

Wenn das Zertifikat erstellt und heruntergeladen wurde, landet es über Puppet irgendwann im Container **rev-proxy** im Ordner `/etc/nginx/ssl`. Das Ganze lässt sich ggf. wieder über einen **prun** im **puppeteer** und danach im **rev-proxy** beschleunigen.

III.3.6.3.5. Alle bestehenden Zertifikate erneuern über acme.sh

Wenn Sie bei einem laufenden System von **acmetool** auf **acme.sh** umstellen, sollten Sie in diesem Zusammenhang gleich alle bereits bestehenden Zertifikate erneuern.

Über **cat /data/le/acme.sh/.acmetool.domains** bekommen Sie angezeigt, für welche Web-Dienste die Zertifikate mit dem bisherigen Tool **acmetool** beantragt wurden.

Beantragen Sie auf Basis dieser Liste für jeden dort aufgeführten Webdienst das Zertifikat neu über den Befehl:

issue webservice.schulkuerzel.logoip.de

Über **acme.sh --list** können Sie nachprüfen, ob alle Zertifikate mit dem neuen Tool erzeugt wurden.

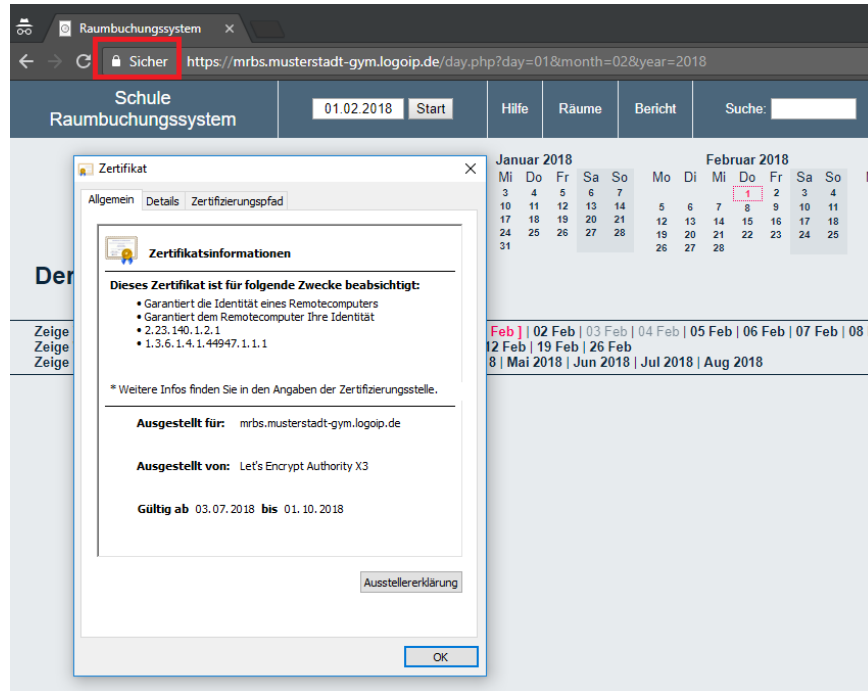
```
musterstadt-gym / lxc@ldhost / 16:58 / 1.4.1-1
le-acme@puppeteer:~$ cat /data/le/acme.sh/.acmetool.domains
collabora.musterstadt-gym.logoip.de
ldaps-ad.musterstadt-gym.logoip.de
ldaps.musterstadt-gym.logoip.de
ldmobiile.musterstadt-gym.logoip.de
mrbs.musterstadt-gym.logoip.de
nextcloud.musterstadt-gym.logoip.de
ssp.musterstadt-gym.logoip.de

musterstadt-gym / lxc@ldhost / 16:58 / 1.4.1-1
le-acme@puppeteer:~$ acme.sh --list
Main Domain      KeyLength  SAN_Domains  CA              Created                               Renew
collabora.musterstadt-gym.logoip.de  ""         no           LetsEncrypt.org  Thu Aug 19 14:56:47 UTC 2021  Mon Oct 18 14:56:47 UTC 2021
ldaps-ad.musterstadt-gym.logoip.de    ""         no           LetsEncrypt.org  Thu Aug 19 14:57:19 UTC 2021  Mon Oct 18 14:57:19 UTC 2021
ldaps.musterstadt-gym.logoip.de       ""         no           LetsEncrypt.org  Thu Aug 19 14:57:38 UTC 2021  Mon Oct 18 14:57:38 UTC 2021
ldmobiile.musterstadt-gym.logoip.de   ""         no           LetsEncrypt.org  Thu Aug 19 14:46:26 UTC 2021  Mon Oct 18 14:46:26 UTC 2021
mrbs.musterstadt-gym.logoip.de        ""         no           LetsEncrypt.org  Thu Aug 19 14:52:49 UTC 2021  Mon Oct 18 14:52:49 UTC 2021
nextcloud.musterstadt-gym.logoip.de   ""         no           LetsEncrypt.org  Thu Aug 19 14:58:04 UTC 2021  Mon Oct 18 14:58:04 UTC 2021
ssp.musterstadt-gym.logoip.de         ""         no           LetsEncrypt.org  Thu Aug 19 14:58:20 UTC 2021  Mon Oct 18 14:58:20 UTC 2021
```


III.3.6.4. Zertifikat prüfen

Sofern ein Zertifikat vorhanden ist, lässt sich dieses über den Browser von einem Client aus relativ leicht prüfen. In unserem obigen Beispiel mit dem Raumbuchungssystem **mrbs** sollte nun bereits der netzinterne Aufruf über

`https://mrbs.musterstadt-gym.logoip.de` keine Hinweise auf ein fehlendes Zertifikat mehr bringen.



Über das Schloss-Symbol und den Eintrag **Zertifikat** erhält man Infos zu dem gerade erstellten Zertifikat, wie z.B. die Laufzeit bzw. Gültigkeitsdauer.

III.3.6.5. Zertifikate aktualisieren

Ein Let's Encrypt Zertifikat hat eine Gültigkeitsdauer von 90 Tagen und muss deshalb regelmäßig erneuert werden. Das geschieht über einen entsprechenden Cron-Job automatisch, so dass Sie sich darum nicht kümmern müssen.

III.3.7. Verwendung eigener Zertifikate

Wie im vorherigen Kapitel beschrieben, ist die Nutzung von Zertifikaten mit Let's Encrypt primär aus Kostengründen die am häufigsten eingesetzte Variante.

Neben den kostenfreien LetsEncrypt-Zertifikaten können aber auch gekaufte SSL-Zertifikate eingesetzt und mit dem Rev-Proxy verknüpft werden.

Hierzu müssen die Dateien nach einem gewissen Schema im Container **Puppeteer** abgelegt werden, und zwar unter `/etc/logodidact/certs/`. Für jede öffentlich nach außen freigeschaltete Adresse muss dort ein entsprechendes Unterverzeichnis mit der Bezeichnung dieser Adresse erstellt werden.

In diese Ordner werden dann die Zertifikate (`cert . pem` und `key . pem`) kopiert. Das können einzelne SSL-Zertifikate sein oder auch ein gekauftes Wildcard-Zertifikat für die gesamte Domain. Bei einem Wildcard-Zertifikat muss dann dasselbe Zertifikat als Kopie in jedem Unterverzeichnis liegen.

```
root@puppeteer:/etc/logodidact/certs # ls *

mrbs.topleveldomain.de
cert.pem  key.pem

ldmobile.topleveldomain.de
cert.pem  key.pem

nextcloud.topleveldomain.de
cert.pem  key.pem
```

Nach diesem Schema müssen die Unterordner für alle Adressen erstellt werden, die im **puppeteer** unter `/etc/logodidact/hosts/rev-proxy/revproxy.conf` freigeschaltet sind (siehe Abschnitt III.3.5.3, „Den Reverse Proxy für Webdienste aktivieren“).

III.3.8. Interne Certification Authority (CA)

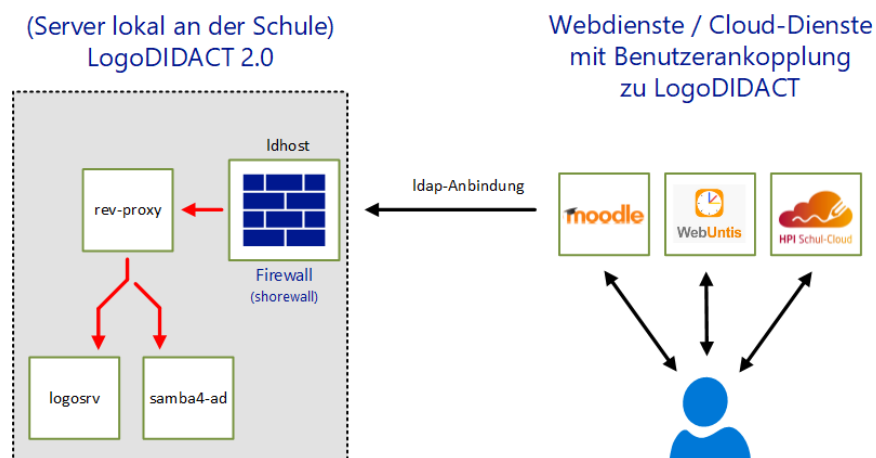
Die Verwendung digitaler Zertifikate für Webdienste, die auch von extern erreichbar sind, erfolgt über Let's Encrypt wie in Abschnitt III.3.6, „Zertifikate mit Let's Encrypt“ beschrieben. Für primär intern genutzte Webdienste wird eine andere interne Zertifizierungsstelle genutzt. Der Container **ca-g1** wird ab Puppet-Rezeptstand 1.1.15 dabei automatisch aufgebaut und muss nicht explizit in die `guest.conf` eingetragen werden.

Die CA im Container **ca-g1** hält alle notwendigen Informationen und Schlüssel aller Container im Ordner `/etc/cfssl`.

III.3.9. Zugriff auf LDAP per SSL/TLS

Der per SSL/TLS (Secure Socket Layer / Transport Layer Security) gesicherte Zugriff auf LDAP wird gemeinhin als LDAPs bezeichnet. Dank dieser gesicherten Kommunikation lassen sich Daten zwischen Sender und Empfänger verschlüsselt austauschen, so dass darüber der Zugriff von außen auf das LDAP-Verzeichnis abgesichert werden kann.

Dieser Zugriff von außen wird überwiegend dazu genutzt, um externe Systeme anzukoppeln und dort nicht separat Benutzer und Kennwörter zu pflegen, sondern auf die vorhandenen Informationen im LDAP-Verzeichnis am Schulserver zuzugreifen und diese im externen System zu nutzen.



Der Gegensatz zu den intern auf dem Server laufenden Web-Diensten (z.B. das Raumbuchungssystem MRBS), die über den Reverse-Proxy von außen zugänglich gemacht werden, geht es in diesem

Szenario um webbasierte Dienste in der Public-Cloud, die an die LogoDIDACT Benutzerverwaltung angekoppelt werden sollen.



Achtung

Ab Puppet Version 1.3.20 (Veröffentlichung am 21.09.2020) ist die Stream-Funktion im Reverse-Proxy (**nginx**) verfügbar, mit der es möglich ist, eine Verbindung an einen internen Dienst weiterzuleiten, der kein http-Dienst ist.

Ab Puppet Version 1.3.22 (Veröffentlichung am 25.01.2021) ist der Zugriff auf LDAP nur noch per Benutzer-Authentifizierung möglich und kann damit eingeschränkt und nochmals besser abgesichert werden.

III.3.9.1. Port über Firewall an Rev-Proxy leiten

Ähnlich wie bei http oder https muss der Port in der Firewall des Basissystems **ldhost** entsprechend zum Reverse-Proxy hin weitergeleitet werden, also im Fall von LDAP der Port 636.

Wechseln Sie in den **ldhost** und dort in das Verzeichnis der Firewall:

```
cd /etc/shorewall
```

Öffnen Sie die die Datei **rules** mit einem Editor Ihrer Wahl und ergänzen Sie die Liste um einen separaten Eintrag für LDAP:

```
#  
# Shorewall version 4.0  
#  
  
DNAT ext dmz:172.28.29.3 tcp 636  
  
DNAT ext dmz:172.28.29.3 tcp 80,443  
  
DNAT ext dmz:172.28.29.2 tcp 1:21  
DNAT ext dmz:172.28.29.2 tcp 23:2221  
DNAT ext dmz:172.28.29.2 tcp 2223:65535  
DNAT ext dmz:172.28.29.2 udp 1:65535
```

Speichern Sie die Datei und starten Sie die Firewall im **ldhost** neu

```
/etc/init.d/shorewall restart
```

Im Anschluss an das Neustarten der Firewall werden auch die LDAP-Anfragen von extern über die Firewall an den Container **rev-proxy** weitergeleitet. Die Voraussetzung dafür ist natürlich, dass der Router am externen Interface entsprechend konfiguriert ist. Entweder sind dort einzelne Portweiterleitungen definiert oder es ist die DMZ Host Funktion aktiviert.

III.3.9.2. Zertifikat für Rev-Proxy erstellen und prüfen

Wechseln Sie in den Container **Puppeteer** und prüfen Sie zunächst, ob Sie dort über den Befehl **sle** in die Umgebung zur Verwaltung der Zertifikate kommen. Stellen Sie dies gegebenenfalls um, wie in Abschnitt III.3.6.3.1, „Umstellung auf das Tool acme.sh“ beschrieben.

Beantragen Sie dann ein Zertifikat von Let's Encrypt wie folgt:

```
sle
```

```
issue ldaps.schulkuerzel.logoip.de
```

Wie gewohnt steht **schulkuerzel** für den bereits mehrfach verwendeten individuellen Namen (z.B. musterstadt-gym). In unserem konkreten Beispiel lautet der Befehl:

```
issue ldaps.musterstadt-gym.logoip.de
```

Die Rückmeldung an Infos ist im Fall von **acme.sh** in der Regel sehr ausführlich. Mit dem folgenden Befehl kann man sich eine Liste aller Zertifikate anzeigen lassen und damit auch den Status prüfen:

```
acme.sh --list
```

Wenn das Zertifikat erstellt und heruntergeladen wurde, landet es über Puppet irgendwann im Container **rev-proxy** im Ordner `/etc/nginx/ssl`. Das Ganze lässt sich über einen **prun** im **puppeteer** und danach im **rev-proxy** beschleunigen.

III.3.9.3. Konfiguration für LDAP im Rev-Proxy

Bleiben Sie im Container **Puppeteer** und erstellen Sie im Verzeichnis `/etc/logodidact/hiera/custom.d/` eine Konfigurationsdatei `rev-proxy.yaml` mit folgendem Inhalt:

```
---
ld_rproxy::hosts:
  ldaps.[shortname].logoip.de:
    type: stream
    template: ldap
    ensure: present
```

Diese empfohlene Standard-Konfiguration arbeitet derzeit mit **openLDAP** auf dem **Logosrv**.

Übernehmen Sie die Änderungen wie üblich ins git:

```
cd /etc/logodidact
```

```
git add .
```

```
git commit -m "LDAPs Konfiguration im Rev-Proxy"
```

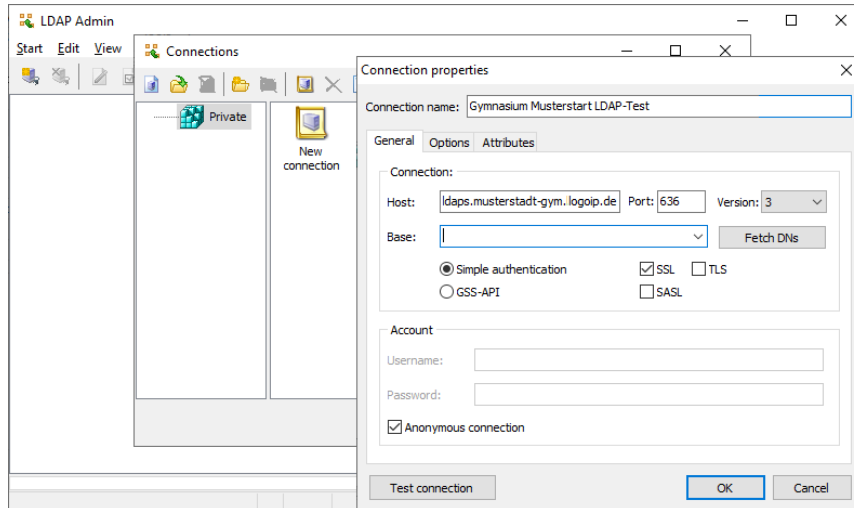
Wechseln sie anschließend in den **rev-proxy** und starten Sie dort **prun**, damit die Anpassungen von **Puppet** durchgeführt werden.

III.3.9.4. LDAP von außen testen

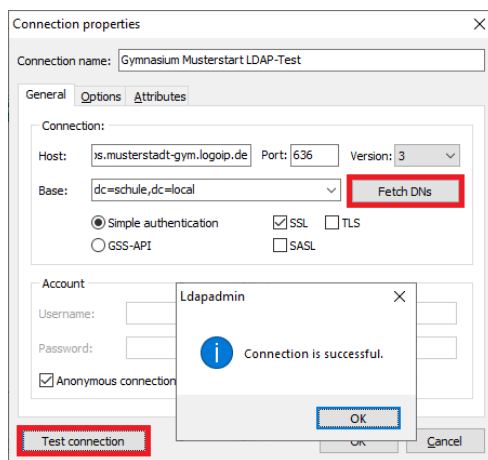
Vorausgesetzt, dass keine weitere Firewall den Zugriff verhindert und der Router mit den Portweiterleitungen richtig konfiguriert ist, kann der sichere Zugriff auf LDAP von außen getestet werden.

Von Windows aus geht das am einfachsten mittels eines graphischen LDAP-Browsers, wie z.B. dem kostenlosen Open-Source-Tool LDAP Admin, das unter der GNU General Public License lizenziert ist und hier heruntergeladen werden kann: www.ldapadmin.org oder

Die Konfiguration ist denkbar einfach und erfordert lediglich die Angabe des Hosts, in unserem Beispiel `ldaps.musterstadt-gym.logoip.de` und das Häkchen bei **SSL**, das dann automatisch den Port auf 636 setzt.



Über die Schaltfläche **Fetch DNs** werden dann bereits die Werte für **Base** automatisch ausgefüllt und im Standardfall auf `dc=schule,dc=local` gesetzt. Über die Schaltfläche **Test Connection** kann zunächst die Verbindung auf technischer Ebene explizit getestet werden.



Für den Zugriff auf Daten im Verzeichnis sind im nächsten Schritt Benutzerdaten einzutragen.



Achtung

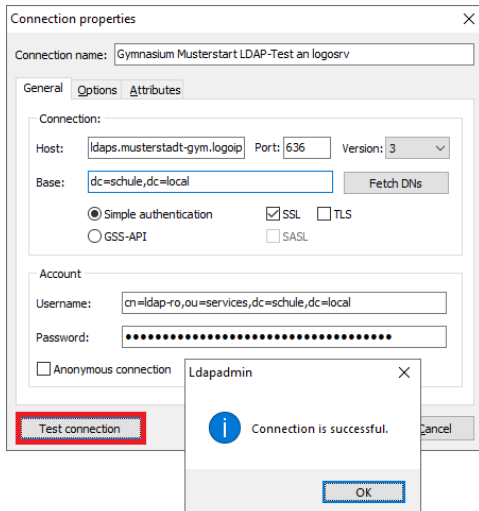
Ab Puppet-Version 1.3.22 (Veröffentlichung am 25.01.2021) ist der Zugriff auf LDAP nicht mehr anonym möglich, sondern nur noch per Benutzer-Authentifizierung und kann damit eingeschränkt und nochmals besser abgesichert werden.

Im Normalfall reicht für jede Ankopplung ein lesender Zugriff auf LDAP, wofür der neue Benutzer **ldap-ro** eingeführt wurde. Relevant für den Zugriff von außen sind folgenden Informationen:

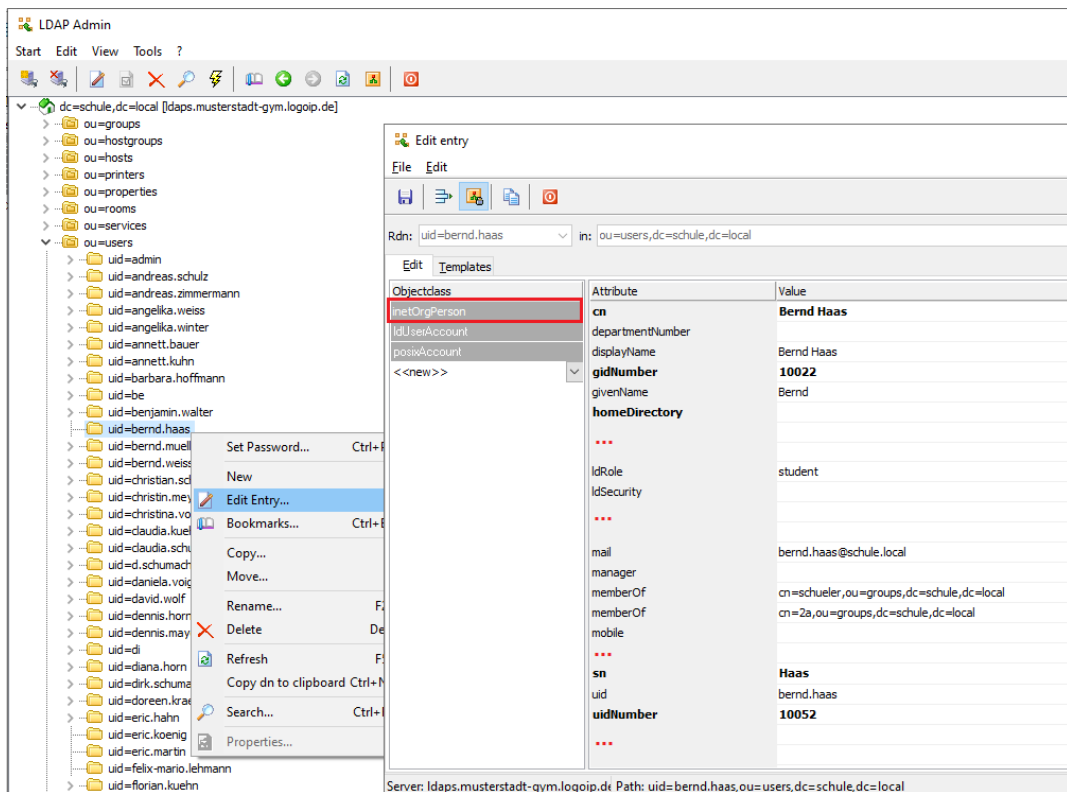
LDAP-User: `cn=ldap-ro,ou=services,dc=schule,dc=local`

Kennwort : steht im logosrv in der Datei /etc/ldap.ro.secret

Tragen Sie die Daten des Benutzers **Ldap-ro** entsprechend im Abschnitt **Account** ein und prüfen Sie die Verbindung speziell für diesen Benutzer erneut über die Schaltfläche **Test Connection**:



Danach lässt sich dann die LDAP-Verzeichnisstruktur und einen minimalen Satz an Attributen lesend abfragen.





Achtung

Bei der oben gezeigten Abfrage der LDAP-Verzeichnisstruktur wird unmittelbar klar, dass man auf diese Weise an personenbezogene Daten gelangt und dieser Zugriff deshalb nicht nur zusätzlich abgesichert werden sollte, sondern abgesichert werden muss!

III.3.9.5. Den Zugriff auf LDAP in der Firewall absichern

Der Zugriff auf die LDAP-Verzeichnisstruktur ermöglicht selbst in der nur lesenden Variante die Abfrage vieler personenbezogener Daten, wie Vor- und Nachname aller Benutzer und die Zugehörigkeit zur jeweiligen Klasse oder auch der Gruppe Lehrer.

Um den Zugriff auf diese Daten einzuschränken, sollte in jedem Fall die Firewall diesen Zugriff auf Quell-IP-Ebene zusätzlich absichern. Wenngleich auch dieser Schutz mit genügend Wissen und krimineller Energie umgangen werden kann, ist diese Absicherung sinnvoll und dringend anzuraten.

Wechseln Sie in den **ldhost** und dort in das Verzeichnis der Firewall:

```
cd /etc/shorewall
```

Öffnen Sie die die Datei **rules** mit einem Editor Ihrer Wahl und ergänzen Sie den Parameter **ext** um die IP-Adresse des Servers oder Dienstes, der von außen auf LDAP zugreifen möchte. Um Beispiel unten, ist die IP-Adresse eines Webuntis-Servers angegeben, der damit auf das LDAP des LogoDI-DACT zugreifen darf:

```
#
# Shorewall version 4.0
#

# Zugriff auf LDAP mit Absicherung über zugelassene externe IP-Adressen
# (falls mehrere IP-Adressen nötig, diese per Komma trennen)
# -----
# Beispiele:
# - BelWue-Moodle-Server IPs: 129.143.69.1,129.143.232.18,129.143.255.2
# - Webuntis Server in Österreich IP: 213.208.138.146
#
DNAT ext:213.208.138.146 dmz:172.28.29.3 tcp 636

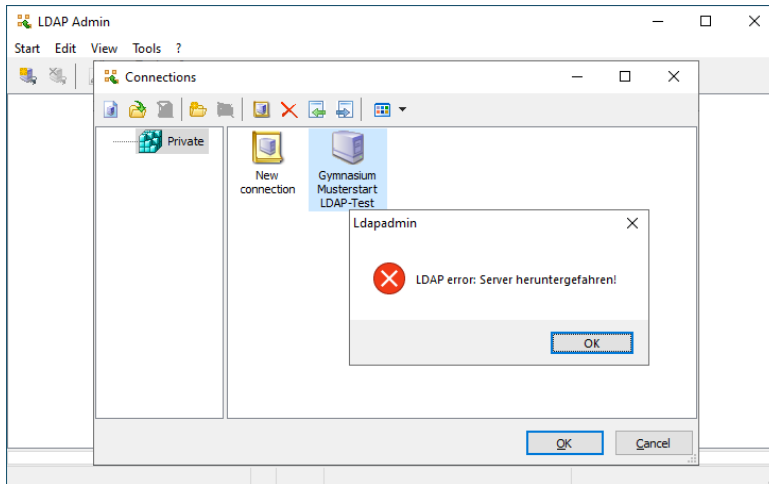
DNAT ext dmz:172.28.29.3 tcp 80,443

DNAT ext dmz:172.28.29.2 tcp 1:21
DNAT ext dmz:172.28.29.2 tcp 23:2221
DNAT ext dmz:172.28.29.2 tcp 2223:65535
DNAT ext dmz:172.28.29.2 udp 1:65535
```

Speichern Sie die Datei und starten Sie die Firewall im ldhost neu

```
/etc/init.d/shorewall restart
```

Wenn Sie nun wieder mittels des Tools LDAP Admin versuchen zuzugreifen, erhalten Sie eine entsprechende Fehlermeldung.



Über `wieistmeineip.de` können Sie natürlich auch die IP-Adresse ihrer Arbeitsstation ermitteln und für den Test bei `ext` eintragen.

III.3.9.6. Konfiguration für Samba4-AD

Optional lässt sich das Ganze auch umleiten auf das AD bzw. Samba 4, indem man im `puppeteer` eine Feature-Datei erstellt und darin einen anderen Host definiert. Die Datei `/etc/logodirect/feature.d/rev-proxy/ldap.yaml` sieht wie folgt aus:

```
---
host: 'samba4-ad'
port: 636
```

Übertragen Sie anschließend die Änderungen ins Versionierungssystem git ein:

```
git add .
```

```
git commit -m "LDAPs Zugriff auf samba4-ad"
```

Wechseln Sie anschließend in den Container `rev-proxy` und starten Sie einen `prun`.



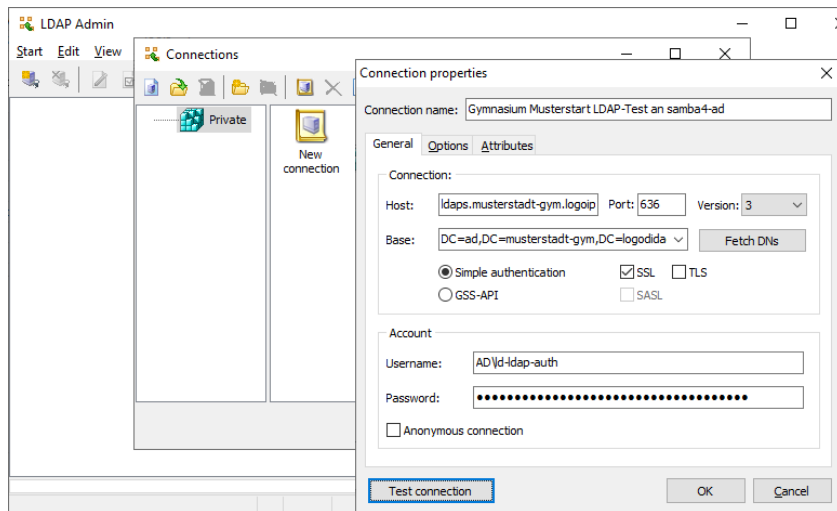
Achtung

Der Zugriff auf das LDAP-Verzeichnis in Samba4 unterscheidet sich vom Schema und den Werten her extrem vom Zugriff auf das Open-LDAP Verzeichnis in Samba3 im `logosrv`.

Die Ankopplung externer Systeme erfordert grundsätzlich entsprechend tiefgehende Kenntnisse der jeweiligen Verzeichnisstruktur.

III.3.9.6.1. LDAP Zugriff auf Samba4-ad von außen testen

Der Zugriff von außen kann wieder mittels eines LDAP-Browsers getestet werden, wie das weiter oben bereits auf Basis des Tools LDAP Admin gezeigt wurde. Hier erfolgt der Zugriff über die Authentifizierung des Benutzers `ld-ldap-auth`.



An das Kennwort bzw. Secret dieses Benutzers gelangen Sie über den Container **Puppeteer** durch die folgende Abfrage:

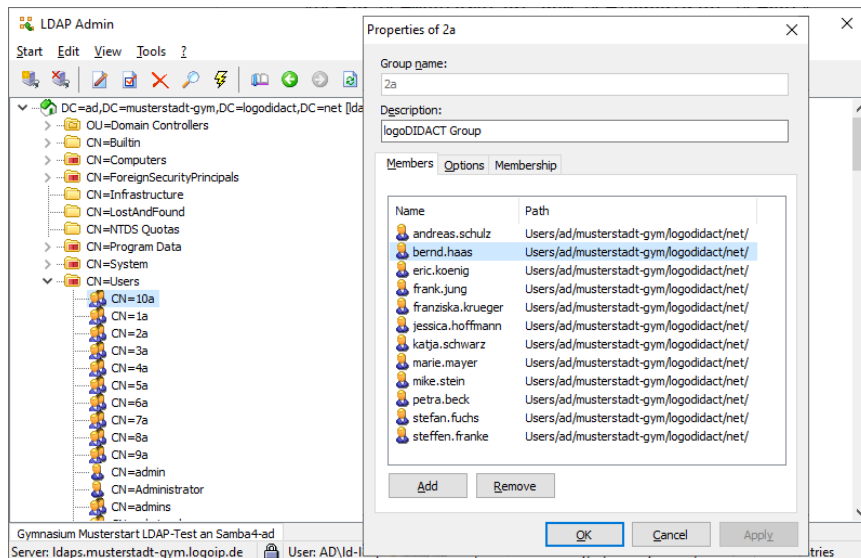
```
redis-cli GET ld_samba4::ld-ldap-auth.random.pass
```

Kopieren Sie die Ausgabe (ohne Hochkommata) in die Zwischenablage und fügen Sie diese im Feld **Password** in obigem Dialog ein.

Über die Schaltfläche **Fetch DNs** können wieder die Werte für **Base** automatisch ausgefüllt werden, wobei sich diese bei samba4-ad deutlich von der Abfrage des Open-LDAP im logosrv unterscheiden:

DC=ad,DC=musterstadt-gym,DC=logodidact,DC=net

Über die Schaltfläche **Test Connection** kann die Verbindung nochmals explizit getestet werden und die Verzeichnis-Struktur danach abfragen.



III.3.9.7. Spezielle LDAP-Benutzer und Attribute

Wie in den vorherigen Abschnitten erwähnt, ist der anonyme Zugriff auf LDAP sowohl für das LDAP im logosrv als auch im Samba4-ad gesperrt. Für den lesenden Zugriff gibt es den Benutzer **ldap-ro**, der auf einen eingeschränkten Satz an Attributen zugreifen kann.

Tabelle III.3.2. LDAP-Benutzer

LDAP-Benutzer	Zugriff auf folgende Objekte und Attribute in der Verzeichnis-Struktur
ldap-ro	lesender Zugriff: entry, cn, displayName, gidnumber, givenName, mail, member, memberOf, memberUid, o, objectClass, ou, sn, title, uid, uidnumber, uniqueMember, ldObjectType, ldRole
ldap-admin	schreibender Zugriff auf nahezu alle Attribute (minimale Einschränkungen). Primär für interne Zwecke im logosrv notwendig.
Directory Manager	Hat keine ACL Einschränkungen und ist ausschließlich für Wartungsarbeiten vorgesehen. Wichtig: Darf nie in irgend welchen Systemen weder intern noch extern verwendet werden!

Die Zugriffsrechte bzw. ACLs finden sich im Container **logosrv** in der Datei `/etc/ldap/slapd.puppet.conf`, die durch Puppet automatisch aufgebaut wird. Nicht notwendige Objektclassen (objectclasses) werden versteckt und im Detail festgelegt, welcher der obigen LDAP-Benutzer auf welche Informationen zugreifen kann.

Sind für die Anbindung eines externen Systems weitere LDAP-Attribute notwendig, können diese im Container **puppeteer** in der Datei `/etc/logodidact/hiera/custom.d/ldhost.yaml` freigegeben werden.

Dass diese Parameter in `ldhost.yaml` eingetragen werden, obwohl sie für den Container `logosrv` bestimmt sind, hängt damit zusammen, dass im `logosrv` kein `puppet agent` läuft und der Container vom `ldhost` aus verwaltet wird.

Muss aus einem speziellen Grund z.B. das Geburtsdatum (**ldBirthday**) und das Geschlecht (**ldGender**) im externen System verfügbar sein, sieht die Datei `/etc/logodidact/hiera/custom.d/ldhost.yaml` exemplarisch so aus:

```
---
ld_legacy::ldap::ldap_ro_atts:
  - ldBirtday
  - ldGender
```

Diese Anpassungen sind wie gewohnt im **puppeteer** ins git zu übernehmen und können dann durch ein **prun** im **ldhost** aktiv in Richtung **logosrv** verteilt werden.

Über das LDAP Admin Tool sind dann die freigeschalteten Attribute zugänglich, wie in folgender Grafik dargestellt.

Objectclass	Attribute	Value
inetOrgPerson	audio	
ldUserAccount	businessCategory	
posixAccount	carLicense	
<<new>>	cn	Bernd Weiss
	cn	Bernd Weiß
	departmentNumber	
	description	
	destinationIndicator	
	displayName	Bernd Weiß
	employeeNumber	
	gidNumber	10018
	givenName	Bernd
	...	
	idBirthday	30.04.1979
	idComment	
	idGender	m



Achtung

Bitte beachten Sie folgendes:

1. Die Freigabe von Attributen wirkt ausschließlich auf LDAP im **Logosrv!**
2. Der Zugriff per LDAP sollte auf die notwendigsten Daten beschränkt werden.
3. Es besteht in der Regel keine Notwendigkeit weitere als die bereits verfügbaren Attribute zugreifbar zu machen.

III.3.10. Virtuelle Maschinen mit KVM

Der LogoDIDACT 2.0 Server selbst nutzt die Technologie der Virtualisierung. Aus vielerlei Gründen wird dabei keine Vollvirtualisierung genutzt, sondern eine "schlanke" Virtualisierung auf Basis von LXC (Linux Container). Ungeachtet dessen, kann man innerhalb des Basissystems Ubuntu 16.04 LTS auch die Technologie der Vollvirtualisierung nutzen.

Hierzu ist es möglich, im Host virtuelle Maschinen auf Basis von KVM (Kernel-based Virtual Machine) einzurichten.



Achtung

1. Die Aktivierung der Vollvirtualisierung über KVM wird in LogoDIDACT ausschließlich dafür gezeigt und verwendet, um darüber die Microsoft-Produktaktivierung für Windows und Office zu realisieren.
2. Wir raten dringend davon ab auf dem Server weitere Maschinen per KVM zu betreiben.
3. Der Betrieb weiterer Server oder Clients in einer KVM ist weder Gegenstand des Supports noch der Überwachung per Server-Monitoring.
4. Es erfolgt keine Datensicherung von KVMs.

III.3.10.1. KVM am Server aktivieren

Für die Microsoft Produktaktivierung von Windows-Clients und Office, wird auf Serverseite ein Windows 10 Client innerhalb einer vollvirtualisierten KVM-Umgebung betrieben. Dazu muss die Technologie der KVM-Vollvirtualisierung am Server aktiviert werden.

Der KVM-Hypervisor wird dabei ähnlich aktiviert, wie ein Container. Wählen Sie sich auf dem Logo-DIDACT 2.0 Server und wechseln Sie per `lxc-attach -n puppeteer` in den Container, um die Konfiguration für KVM festzulegen.

Wechseln Sie dort in das Verzeichnis `/etc/logodidact/hosts/ldhost/` und erstellen Sie die Datei `puppet.conf` mit einem Editor Ihrer Wahl, wie z.B. Nano:

```
nano puppet.conf
```

Tragen Sie folgenden Inhalt ein:

```
[Puppet]
Role profile::kvm::host
```

Durch Eingabe der Tastenkombination `<Strg>+<X>` verlassen Sie den Editor und geben „Y“ ein, damit die Änderung gespeichert wird. Übertragen Sie anschließend die Änderungen ins Versionierungssystem git ein:

```
git add .
```

```
git commit -m "kvm aktiviert"
```

Wechseln Sie in den Host und starten Sie einen `prun` wodurch sämtliche für KVM-Virtualisierung benötigten Pakete installiert werden. Das geht sehr schnell und ohne große sichtbare Veränderung. Dass die Pakete eingespielt wurden, sieht man an der Ausgabe im `prun` oder auch am Vorhandensein einiger Tools, die danach zur Verfügung stehen. Wenn Sie im Host den Befehl `virsh -h` eingeben und keine Fehlermeldung erscheint, dann sind die Pakete installiert.

III.3.10.2. Virtio Treiber installieren

Zur Optimierung der Performance gibt es virtio-Treiber von Fedora, die über die folgende Seite heruntergeladen werden können:

```
https://fedoraproject.org/wiki/Windows\_Virtio\_Drivers.
```

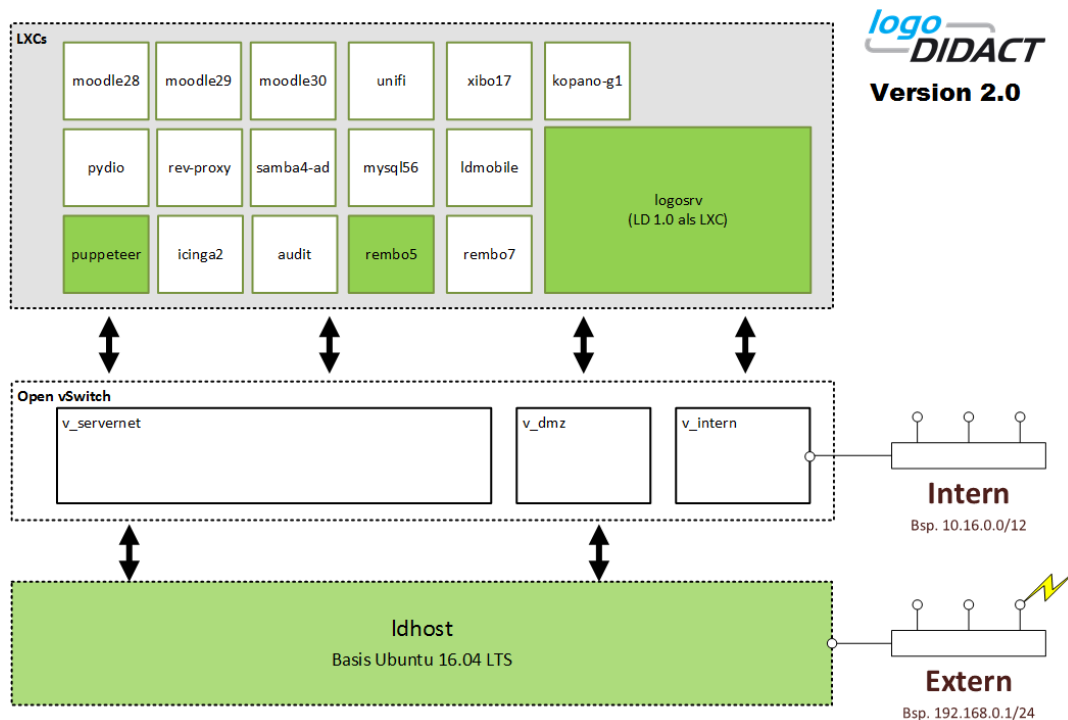
Die entscheidende Datei für Windows-Systeme ist dabei `virtio-win.iso`.

Damit das Betriebssystem in einer virtuellen Maschine auch Signale vom Wirtssystem erhält, ist es zwingend erforderlich, dass der so genannte QEMU Guest Agent installiert wird. Dieser findet sich ebenfalls auf der oben aufgeführten Seite des Fedora-Projektes.

Kapitel III.4. Konfiguration des logosrv

Wie in Kapitel III.3, *Server und Systemdienste* beschrieben, hat sich die Architektur von LogoDIDACT 1.0 zur neuen Version 2.0 gravierend verändert. Vereinfacht gesagt, wurde das gesamte Basissystem komplett neu entwickelt und der alte LogoDIDACT als virtuelle Maschine in einen Container Namens **logosrv** ausgelagert.

Stück um Stück wurden und werden daraus einzelne Software-Bausteine entfernt und in separate Container ausgelagert oder durch komplett neue Module ersetzt. Der Container **logosrv** ist vereinfacht gesagt das, was als "Rest" vom LogoDIDACT 1.0 Server übrig geblieben ist.



Ungeachtet der Tatsache, dass bereits mehr als ein Dutzend der Bausteine in Container ausgelagert sind, gibt es noch immer viele Module im **logosrv**, die im Laufe der Entwicklung ausgelagert werden. Die Konfiguration dieser Bausteine wird in diesem Kapitel beschrieben.

III.4.1. Firewall

Die Einstellungen und Anpassungen an der internen Firewall von LogoDIDACT erfolgen im Wesentlichen in der Datei `/etc/logodidact/internet.conf`

Dort wird geregelt, welche Ports intern offen und von Innen nach Außen oder umgekehrt erreichbar sind. Grundsätzlich werden die Änderungen immer erst wirksam, nachdem man die LogoDIDACT Firewall neu gestartet hat. Dies erfolgt über den Befehl: **ldfirewall restart**

III.4.1.1. Fernzugriff auf den Server

Neben dem Fernzugriff per VPN kann man auch den direkten Zugriff auf den Server ermöglichen. Dadurch ist es Benutzern möglich, über das Internet auf Dienste des Servers zuzugreifen ohne zuvor eine spezielle Software installieren zu müssen.

In den meisten Fällen wird das dazu genutzt, Benutzer von zu Hause aus den einfachen Zugriff auf Webdienste wie beispielsweise Moodle oder Webmail zu gestatten.

Im folgenden wird die Einrichtung dieses Fernzugriffs erklärt.

III.4.1.1.1. Dynamischer Rechnername

Um den Fernzugriff zu ermöglichen, muss die Möglichkeit bestehen, den Server von außen über einen festen Namen zu erreichen, auch wenn sich die IP Adresse des Routers häufig ändert. Für diesen Fall gibt es im Internet verschiedene Anbieter, die dynamische DNS Dienste anbieten. Dabei registriert der Server dort seine aktuelle IP Adresse, wenn sich diese ändert.

III.4.1.1.1.1. logolP

In LogoDIDACT ist ein dynamischer DNS Dienst integriert, der für Anwender kostenfrei verfügbar ist und keine separate Registrierung erfordert. Der Zugriff erfolgt dabei über den Namen `kuerzel.logoip.de`. Die Konfiguration ist sehr einfach:

1. Navigieren Sie in der Datei `/etc/logodidact/service.conf` zum Abschnitt `[IPUpdate]`. Dort finden Sie den Parameter `HostName`. Dieser ist standardmäßig auf den Wert `beispielhausen-gym` gesetzt. Ändern Sie diesen Parameter auf einen eigenen, beliebig von Ihnen selbst gewählten Wert. Empfehlenswert ist hier ein Name, der den Schulnamen und Ort wieder spiegelt. Beispiele:

```
HostName hamburg-mpg
```

oder

```
HostName maxplanck-hh
```

oder

```
HostName maxi
```

2. Führen Sie den folgenden Befehl aus: **ldipupdate**

Dabei sollte die folgende Ausgabe erscheinen:

```
Registrierung von hamburg-mpg.logoip.de auf 87.106.41.230... OK
Update von hamburg-mpg.logoip.de auf 87.106.41.230... OK
```

3. Beim ersten Aufruf von **ldipupdate** wird der Rechnername registriert. Wenn die Registrierung nicht erscheint sondern nur das `Update... OK`, dann ist das auch normal. Der Name wurde in dem Fall vom Server bereits zwischen Schritt 1 und 2 selbst registriert, da dieser den **ldipupdate** Befehl alle zwei Minuten aufruft um die IP Adresse aktuell zu halten. Wenn beim **ldipupdate** die folgende Meldung erscheint, existiert bereits eine Registrierung für das von Ihnen gewählte Rechnerkürzel. In diesem Fall sollten Sie ein anderes Kürzel wählen:

```
Registrierung von maxi.logoip.de auf 87.106.41.230...
Error: [EEXISTS] Host already exists
```



Achtung

Während der Registrierung wird ein zufälliges Kennwort erzeugt, das bei späteren Updates notwendig ist, um diese zu authentifizieren. Falls Sie den Server also beispielsweise neu installieren, müssen Sie die Datei `/etc/ipupdate_logoip.secret` vorher sichern und in der neuen Installation zurückspielen, anderenfalls können Sie für Ihr bestehendes Kürzel keine logoIP Updates vornehmen.

III.4.1.1.1.2. DynDNS

Der bekannteste Anbieter für dynamisches DNS ist DynDNS (<http://www.dyndns.com>). Dort kann man sich neben anderen Angeboten für den kostenlosen Dienst DynDNS Free anmelden. Dieser Dienst wird häufig von DSL Routern direkt unterstützt. In diesem Fall muss man die Konfiguration im Router selbst vornehmen und nichts am Server ändern.

Leider wurde vor einer Weile in der Free Variante der Wildcard Support für neue Accounts eingestellt und muss für einen Betrag (derzeit \$15/Jahr) zusätzlich erworben werden. Den Wildcard Support benötigt man, um auf Dienste wie <http://moodle.ihrkuerzel.dyndns.org> zuzugreifen. Ohne diese Funktionalität ist der Server nur über <http://ihrkuerzel.dyndns.org> zu erreichen, und die automatische Dienststeuerung von LogoDIDACT funktioniert nicht mehr. Aus diesem Grund empfehlen wir die Verwendung von logoIP. Sie können aber auch beide Dienste parallel verwenden.

Um die DynDNS Updates vom Server vornehmen zu lassen, können diese dort wie folgt konfiguriert werden:

1. Navigieren Sie in der Datei `/etc/logodidact/service.conf` zum Abschnitt `[IPUpdate]`. Erzeugen Sie unter diesem Abschnitt einen weiteren Abschnitt nach folgendem Schema:

```
[IPUpdate dyndns]
Type dyndns
HostName ihrdyndnshost.dyndns.org
User ihrdyndnsuser
Secret file:/etc/ipupdate_dyndns.secret
```

Bitte beachten Sie, dass Sie als `HostName` Ihren kompletten DynDNS Hostnamen angeben, da DynDNS mehrere Domänen unterstützt.

2. Schreiben Sie Ihr DynDNS Kennwort in die Datei `/etc/ipupdate_dyndns.secret` und schützen Sie diese Datei vor Lesezugriffen anderer. Beispiel:

```
echo geheim > /etc/ipupdate_dyndns.secret
chmod 600 /etc/ipupdate_dyndns.secret
```

3. Führen Sie den folgenden Befehl aus: **ldipupdate**

III.4.1.1.1.3. Andere Dienste

Bei Verwendung anderer dynamischer DNS Dienste, die von Ihrem Router nicht direkt unterstützt werden, müssen Sie die jeweiligen Updater-Skripte am Server nachinstallieren und konfigurieren. So gibt es beispielsweise die Ubuntu Pakete `ez-ipupdate` und `ddclient`, die beide verschiedene Anbieter unterstützen.



Achtung

Um die volle LogoDIDACT Funktionalität zu haben, sollte Ihr Anbieter Wildcard-DNS unterstützen und diese Option aktiviert sein, anderenfalls gibt es Probleme beim Zugriff auf LogoDIDACT Webdienste, da diese standardmäßig über ihre Rechnernamen unterschieden werden, also beispielsweise:

<http://moodle.ihrkuerzel.logoip.de/>

<http://webmail.ihrkuerzel.logoip.de/>

...

III.4.1.1.2. Portweiterleitung am Router

Damit die Verbindungen vom Internet auch auf dem Server ankommen und nicht vorher schon vom Router blockiert werden, müssen am Router Portweiterleitungen oder ein sogenannter DMZ Host eingerichtet werden.

III.4.1.1.2.1. DMZ Host

Bei Einrichtung eines DMZ Host leitet der Router alle eingehenden Verbindungen transparent an den Server durch. Diese Variante ist die einfachste. Die Firewall des Servers verhindert dabei unberechtigte Zugriffe, und das interne Netz bleibt geschützt.

Bei der Einrichtung muss am Router die DMZ Host Funktion aktiviert werden und als Ziel die IP Adresse der externen Netzwerkschnittstelle (die, die zum Router führt) des Servers eingetragen werden.

III.4.1.1.2.2. Portweiterleitung

Um gezielt einzelne Verbindungen vom Router an den Server weiterzuleiten, kann am Router eine Portweiterleitung eingerichtet werden. Wie die Konfiguration genau aussieht ist bei jedem Router etwas anders. Prinzipiell benötigen Sie jedoch die folgenden Informationen:

Welches Protokoll soll weitergeleitet werden? In den meisten Fällen ist das TCP.

Welcher Port am Router soll die Verbindungen entgegennehmen?

An welchen Port am Server soll diese Verbindung weitergeleitet werden? Die Ports in Punkt 2 und 3 sind normalerweise gleich.

An welche IP Adresse soll die Verbindung weitergeleitet werden? Hier muss die IP Adresse der externen Netzwerkschnittstelle (die, die zum Router führt) angegeben werden.

Um beispielsweise eingehenden unverschlüsselte (per http) und verschlüsselte (per https) Verbindungen an den Webserver durchzulassen, müssen Sie zwei Portweiterleitungen einrichten:

```
Protokoll: TCP
Router Port: 80
Server Port: 80
IP: 192.168.1.254 (externe IP des Servers)
```

```
Protokoll: TCP
Router Port: 443
Server Port: 443
IP: 192.168.1.254 (externe IP des Servers)
```

In der folgenden Tabelle sind nochmals diejenigen Ports aufgeführt, die typischerweise für verschiedene Zwecke und Funktionen auf dem Router als entsprechende Weiterleitungen von Außen (Internet) nach Innen (zum externen Interface des Servers hin) eingerichtet werden. Die Bezeichnung "lokaler Server" ist dabei die externe IP des Servers, d.h. per Standard ist das 192.168.1.254.

Tabelle III.4.1. Portweiterleitungen im Router für den Zugriff von Außen (Internet) nach Innen (Server)

Service	Port	Quelle	Ziel
http	80	*	lokaler Server:80
https	443	*	lokaler Server:443

Service	Port	Quelle	Ziel
ssh	2222	*	lokaler Server:2222
LogoDIDACT-Console	4284	*	lokaler Server:4284
OpenVPN	1194	*	lokaler Server:1194
OpenVPN	1195	*	lokaler Server:1195

III.4.1.1.3. Freischaltung in der Serverfirewall

Damit eingehende Verbindungen auch vom Server akzeptiert werden, müssen für diese Ausnahmen in der Firewall konfiguriert werden. Editieren Sie dazu die Datei `/etc/logodidact/internet.conf`, suchen Sie dort den Parameter `FromInternetAllowTCP` bzw. bei UDP Kommunikation den Parameter `FromInternetAllowUDP` und fügen Sie dort die betreffenden Ports ein. Im folgenden Beispiel wird SSH Zugriff von außen erlaubt, sowie HTTP und HTTPS Verkehr:

```
FromInternetAllowTCP 22 2222 http https
```

Um die Änderungen zu aktivieren, führen Sie den folgenden Befehl aus: **ldfirewall restart**

III.4.1.1.4. Besonderheiten

III.4.1.1.4.1. Moodle

Beim Fernzugriff auf Moodle ist zu beachten, dass Moodle viele Inhalte mit einer absoluten URL abspeichert. Das hat zur Folge, dass beispielsweise im Schulnetz erstellte Bildinhalte mit der internen URL abgelegt werden. Beispiel: `http://moodle.schule.local/bild.jpg`

Wenn man Moodle dann extern aufruft, wird auf die Inhalte mit der internen URL verlinkt, und da `http://moodle.schule.local/` extern keine Bedeutung hat (es sei denn man ist per VPN verbunden), ist kein Zugriff möglich.

Bei Moodle gibt es für dieses Fehlverhalten bislang keine Einstellung um eine relative Adressierung zu aktivieren.

Als Workaround empfehlen wir daher, intern und extern mit derselben Adresse auf Moodle zuzugreifen. Um das zu aktivieren, kann man wie folgt vorgehen:

1. Setzen Sie in `/etc/bind/named.conf.local` den folgenden Abschnitt (bzw. aktivieren und modifizieren Sie den Beispielabschnitt):

```
# Externe dynamische IP intern auflösen
zone "beispielhausen-gym.logoip.de" {
    type master;
    file "/etc/bind/db.dynip";
    check-names ignore;
};
```

Ersetzen Sie dabei das `beispielhausen-gym.logoip.de` durch Ihren dynamischen DNS Host, also z.B. `ihrkuerzel.logoip.de` oder `ihrhost.dyndns.org`

2. Sofern nötig, ersetzen Sie in `/etc/bind/db.dynip` die IP Adresse `10.16.1.1` durch die interne IP Adresse Ihres Servers und die Domäne `schule.local` durch Ihre interne Domäne. Beispiel:

```
cd /etc/bind
```

```
rpl 10.16.1.1 10.1.1.1 db.dynip
rpl schule.local max-planck-gymnasium.local db.dynip
```

3. Starten Sie den DNS Server neu: **/etc/init.d/bind9 restart**

Ein Ping von Client oder Server auf ihrkuerzel.logoip.de sollte dann eine Antwort von der internen IP Ihres Servers erhalten.

4. Kopieren Sie die Datei `/var/www/moodle/.htaccess.dynip` nach `/var/www/moodle/.htaccess`, und passen Sie die Datei an Ihren dynamischen DNS Namen an. Diese Datei sorgt dafür, dass beim Zugriff auf Moodle automatisch auf den richtigen Namen umgeleitet wird.

5. Falls Sie bereits Moodle-Inhalte haben und diese anpassen möchten, können Sie folgendes ausführen:

```
adm_mysqldump --add-drop-table moodle > /root/moodle.sql
cp /root/moodle.sql /root/moodle.neu.sql
```

Passen Sie `/root/moodle.neu.sql` an (z.B. durch Suchen/Ersetzen der internen URLs durch die externe URL:

```
rpl http://moodle/ http://moodle.ihrkuerzel.logoip.de/
/root/moodle.neu.sql
```

```
rpl http://moodle.schule.local/ http://moodle.ihrkuerzel.logoip.de/
/root/moodle.neu.sql
```

Importieren Sie die angepasste Datenbank:

```
adm_mysql moodle < /root/moodle.neu.sql
```



Achtung

Bitte führen Sie diese Schritte nur durch, wenn Sie wissen was dabei passiert und ein aktuelles, funktionsfähiges Backup besitzen!

III.4.1.2. Ports und Protokolle

Die Einstellung in der LogoDIDACT Firewall ist nach einer Standard- Grundinstallation bewusst so gehalten, dass Sie auch mit Ihrer anschließenden Einrichtung der Arbeitsstationen dort nicht unnötig beim Zugang ins Internet eingeschränkt werden. Konkret lässt die Firewall neben dem logischerweise immer notwendigen http-Protokoll auch das sichere https zu, ebenso ftp für Downloads (z.B. Treiber) von ftp-Servern und pop und smtp für Mail. Grundsätzlich sollte man jedoch nach der Installation prüfen, ob bestimmte Protokolle und damit Ports dicht gemacht werden können.

III.4.1.2.1. FTP-Zugang

Per Standardeinstellung ist der Zugriff per FTP im LogoDIDACT Server nicht aktiviert und muss in `/etc/logodidact/internet.conf` freigegeben werden. Für den reibungslosen Betrieb von FTP reicht es allerdings nicht aus, dass die Standard-Ports 20 und 21 erlaubt sind. Beim **passiven** FTP bestimmt der FTP Server (im Internet) die Ports, die im Verlauf der weiteren Kommunikation genutzt werden, und diese sind bei den einzelnen Servern verschieden. Daher muss man hier den kompletten Bereich freigeben, der von FTP-Servern genutzt werden kann. Die Ports sind allerdings "nur"

von Innen nach Außen hin offen, nicht für eingehende Verbindungen vom Internet. Zusammenfassend sind folgende Einstellungen in `/etc/logodidact/internet.conf` am Server notwendig:

```
ToInternetAllowTCP ftp, ftp-data, https, 22, 1024:
```

Die Portfreigaben können sowohl über die Nummer des Ports als auch die entsprechenden Namen erfolgen, d.h., ftp steht synonym für den Port 21 und ftp-data für den Port 20. Die Angabe 1024: bedeutet, dass ab Port 1024 alle Ports möglich sind. Anschließend muss die Firewall neu gestartet werden:

ldfirewall restart

Weiterhin muss bzw. sollte der FTP Client auf **Passive** FTP geschaltet werden.

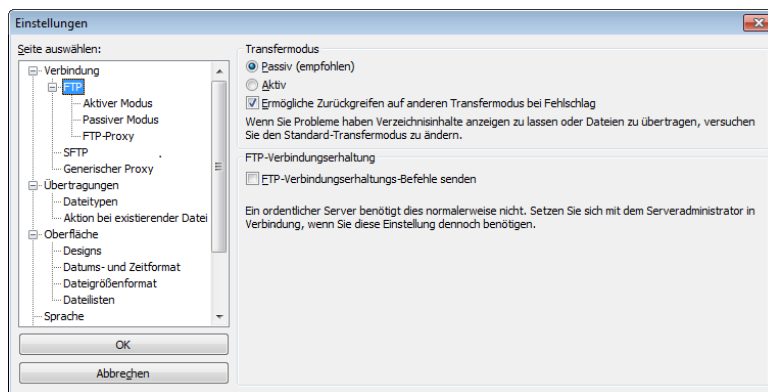


Abbildung III.4.1. Ändern des FTP-Transfermodus am Beispiel von Filezilla



Warnung

FTP ist grundsätzlich kein gutes Protokoll und hat einige Schwächen. Bitte beachten Sie vor allem, dass durch das Öffnen der Ports oberhalb 1024 auch viele Programme wie z.B. Filesharing, Instant Messenger usw. funktionieren.

III.4.1.2.2. SMTP-Zugang für ausgewählte Rechner

Vielen Schulen ist inzwischen sicherlich das so genannte Abuse-Team der Telekom bekannt, das sich um die Vermeidung vor allem von SPAM-Mails bemüht. Die Praxis zeigt, dass sich LogoDI-DACT-Schulen in aller Regel nur an solchen PCs Trojaner und Viren einhandeln, die sie nicht per Imaging betreiben. Damit auch ungeschützte oder fremde Geräte (mit Trojaner) nicht einfach den Port 25 zum Versenden von Mails benutzen oder missbrauchen können, sollte das Protokoll bzw. der Port pauschal gesperrt werden. Das geschieht dadurch, dass man das jeweilige Protokoll wie z.B. smtp aus der Datei `/etc/logodidact/internet.conf` entfernt:

```
ToInternetAllowTCP pop3, smtp, ftp, ftp-data, https
```

ändern in

```
ToInternetAllowTCP pop3, https
```

Um an einem einzelnen Rechner das Senden von Mails mit einem „richtigen“ Mailclient zu erlauben, sollte das Protokoll am Server in der Datei `/etc/logodidact/internet.conf` gezielt für die IP-Adresse dieses Rechners erlaubt werden. Die Freigabe eines Protokolls wie smtp ist gleichbedeu-

tend mit der Freigabe des verwendeten Standard-Ports (hier 25). Alternativ oder auch parallel dazu kann man auch den Port 587 verwenden, sofern es der Provider zulässt:

```
ToInternetAllow 10.16.100.101:25
ToInternetAllow 10.16.100.101:587
```

III.4.1.2.2.1. Prüfen ob Port 25 des t@school Anschlusses gesperrt ist

Wenn der Port 25 vom Abuse-Team schon gesperrt wurde, dann sieht man das bereits bei der Abfrage des Mailpostfachs über pop mittels des folgenden Befehls direkt am Server: **telnet pop.t-online.de pop3**

Die Fehlermeldung bei gesperrtem Zugang beinhaltet dann: -ERR Toid authentication disabled

III.4.1.3. Sperren von Tor-Verbindungen

Das Wort Tor steht für „The Onion Routing“ und bezeichnet ein Protokoll, mit dessen Hilfe eine Arbeitsstationen eine Verbindung zu einem Tor-Netzwerk aufbaut. Ähnlich wie bei der Nutzung eines Webproxy-Servers kann damit ein Schüler versuchen, den Jugendschutzfilter zu umgehen. Bei der Verwendung von Tor wird auf der Arbeitsstation ein Proxy-Client installiert. Dieser Client baut eine verschlüsselte Verbindung zum ersten Tor-Server auf und diese Verbindung wird dann durch zwei weitere Server derart „verlängert“, dass eine möglichst große Anonymität erreicht wird, aber die Verbindung trotzdem einigermaßen schnell bleibt. Um solche Verbindungen zu unterbinden, holt sich der LogoDIDACT Server stündlich (per Cronjob in /etc/cron.d/update_tor_nodes) eine Liste aller aktuell bekannten Tor Server von update.logodidact.com. Über die Firewall werden Verbindungen zu diesen Servern gesperrt.

Per Parameter

```
[Firewall]
BlockTor no
```

und Neustart der Firewall kann man diese Sperrung deaktivieren, standardmäßig ist diese jedoch aktiv.

III.4.2. Proxy-Server

In LogoDIDACT wird als Proxy-Server squid eingesetzt. Für HTTP Traffic auf den Ports 80, 3128 und 8080 existiert ein so genannter transparenter Proxy, d.h., es muss auf den Arbeitsstationen nicht explizit im Browser ein Proxy-Server eingetragen werden. Das ist vor allem im Hinblick auf mobile und überwiegend private Geräte sinnvoll und macht die Konfiguration sehr einfach.

Grundsätzlich ist ein Proxy ein Stellvertreter, der für einen Client eine Anfrage übernimmt und weiterleitet. In manchen Fällen kann das auch zu Problemen führen, weshalb es notwendig sein kann, den Proxy zu umgehen oder einen anderen Proxy einzutragen.

Dazu gibt es verschiedene Parameter in der Datei /etc/logodidact/internet.conf die entsprechend angepasst werden können:

```
# Clients im Intranet ohne Proxyzwang
# (umgeht transparenten Proxy)
# Beispiel:
# NoProxyClients r100-lehrer, r200-lehrer, 10.1.4.101
# NoProxyClients * (Zwangproxy abschalten)
```

```
NoProxyClients
```

```
# Websites im Internet ohne Proxyzwang
# (umgeht transparenten Proxy)
# Beispiel:
# NoProxySites www.lernraum-berlin.de, 209.85.135.99
# NoProxySites *          (Zwangsproxy abschalten)
NoProxySites
```

III.4.3. Webfilter

Als Basis für die Webfilterung wird in LogoDIDACT Dansguardian verwendet. Darüber können sowohl "bekannte" unerwünschte Seiten gefiltert werden (URL-Filter) als auch Seiten, die bestimmte unerwünschte Wörter enthalten.

Viele Einstellungen, wie z.B. das komplette Deaktivieren des Web- bzw. Jugendschutzfilters lassen sich aus Endkundensicht sehr einfach und praktikabel aus der LogoDIDACT-Console heraus einstellen. Andere Dinge, wie das Festlegen, ob ein Rechner grundsätzlich gefiltert wird oder nicht und wie die Starteinstellung nach dem Neustart eines Rechners aussehen, lassen sich für den EDV-Betreuer über das ITB-Interface ebenfalls recht einfach anpassen. Es gibt jedoch auch Anpassungen, die derzeit nur vom Administrator mit root-Zugang angepasst werden können.

III.4.3.1. Schlagwortfilter Schwellwert ändern

Ergänzend zum URL-Filter kann in LogoDIDACT-Console ein Wortfilter aktiviert werden. Zu jedem Eintrag eines Wortes gibt es eine Punktzahl. Jedes Wort auf einer Internetseite wird dabei jeweils nur ein einziges Mal bewertet. Die Punktezahlen der verschiedenen "verbotenen" Wörter werden dabei addiert und bei Erreichen eines bestimmten Schwellwertes, sperrt dann der Wortfilter die Seite. Per Standardeinstellung ist diese Schwelle mit einem Wert von 90 Punkten relativ niedrig eingestellt ("Grundschuleinstellung"). Der Wert "naughtynesslimit" kann in der Datei `/etc/dansguardian/dansguardianfl.conf` ohne Probleme auf 400 hochgesetzt werden. Anschließend muss Dansguardian neu gestartet werden: `/etc/init.d/dansguardian restart`

III.4.3.2. Vorratsdatenspeicherung für Internetauswertung anpassen

Die Dauer der Speicherung von Surfdaten für die Internetauswertung kann in LogoDIDACT entsprechend den Vorgaben des jeweiligen Bundeslandes, der Stadt oder auch der Schule angepasst werden. Dies erfolgt über die Datei `/etc/logodidact/service.conf` im Abschnitt **[Webfilter]**.

```
SurflogMaxAge 1 week
```

Per Standard ist dieser Parameter nicht vorhanden und steht auf `SurflogMaxAge 1 month`.

III.4.4. Drucker Einstellungen cups/pykota

Die Anpassungen, die in diesem Bereich aufgeführt sind, beziehen sich lediglich auf das Drucksystem cups/pykota und spiegeln einige derjenigen Dinge wider, die ja nach Kunde speziell angepasst werden sollen oder auch müssen, damit das System praktikabel nutzbar ist.

III.4.4.1. Bestätigung des Druckauftrags am Client deaktivieren

Per Standardeinstellung ist in der Datei `/etc/pykota/pykota.conf` festgelegt, dass Druckaufträge die zum Server geschickt werden nochmals vom Anwender bestätigt werden müssen, nach-

dem er angezeigt bekommt, was von seinem Druckkontingent abgezogen wird. Der Nachteil dabei ist der, dass cups/pykota die Druckaufträge auf Serverseite strikt sequentiell abarbeitet. Solange der erste Druckauftrag vom Benutzer also nicht bestätigt oder abgebrochen und verworfen wird, erhält der zweite Benutzer zu seinem Druckauftrag keinerlei Nachricht. Wenn die Unterrichtssituation so ablaufen soll, dass alle Benutzer am Ende der Stunde drucken sollen, dann führt diese Methode in der Praxis zu erheblichen Verzögerungen, die man unbedingt verhindern sollte.

Folgende Einstellung muss in `/etc/pykota/pykota.conf` durch Voranstellen des Rautezeichens deaktiviert werden.

```
#askconfirmation : /usr/bin/pykoman ask
```

Damit erfolgt keine Rückfrage mehr am Client.

III.4.4.2. Druckeragent bzw. Printagent Symbol am Client ausschalten

Im Zusammenhang mit der Druckerzuordnung und Steuerung über cups auf Serverseite, stellt LogoDIDACT-Console einen Printagent für Windows-Clients zur Verfügung. Dieser Printagent taucht auf der Windows-Symboleiste rechts Unten als EURO-Symbol auf. Der Printagent (Druckagent) wird über das Anmeldeskript `/home/samba/progs/Anmeldung/PrintAgent/start.bat` aktiviert. Wenn man die Druckquotierung über cups/pykota überhaupt nicht einsetzt, irritiert bzw. stört das Symbol des Druckagenten auf den Arbeitsstationen nur. Den Agent am Client kann man dadurch deaktivieren, dass man in dem Verzeichnis `/PrintAgent` einfach eine Datei mit Namen "disable" (keine Endung und ohne Inhalt) anlegt. Das Anmeldeskript prüft das Vorhandensein dieser Datei und bricht ab, falls die Datei vorhanden ist. Direkt am Server legt man die Datei z.B. mit dem Befehl **touch disable** an.

III.4.5. DHCP-Optionen

III.4.5.1. IP-Adress-Vergabe für fremde Rechner sperren

Die Standardeinstellung in LogoDIDACT bezüglich DHCP ist so, dass auch fremde Geräte eine IP-Adresse aus dem dynamischen Bereich des DHCP-Servers bekommen. Bekannte Geräte, die in der `wimport_data` stehen, erhalten vom DHCP-Server immer die gleichen IP-Adressen über den Mechanismus der Reservierung.

Die freie Vergabe von IP-Adressen auch an fremde Geräte hat sich in der Praxis lange Zeit bewährt, wird aber aufgrund der Verbreitung von kleinen kostengünstigen Geräten wie Netbooks und Smartphones mit integrierten Netzwerkinterfaces zunehmend kritischer. Die Geräte sind inzwischen so klein, dass der Zugang nicht mehr ohne Weiteres erkennbar und damit mehr oder weniger anonym möglich ist.

Sollen „fremde Rechner“ nicht mit IP-Adressen versorgt werden, kann dies in `/etc/dhcp3/template/dhcpd.conf.logodidact.range.intern` durch entfernen des Eintrages `$auto` deaktiviert werden. Anschließend muss noch **import_workstations** ausgeführt werden und danach werden keine Leases mehr an unbekannte Geräte vergeben.

III.4.5.2. Adressbereich für dynamische IPs anpassen

In einer Standardumgebung, liegt der Adressbereich für dynamisch vergebene IPs im 10er Netz, so dass genügend IPs zur Verfügung stehen. Der freie Bereich, bzw. die so genannte **range** wird in der Datei `/etc/dhcp3/dhcpd.conf.logodidact` auf dem logosrv festgelegt.

Bitte beachten die Information am Anfang der Datei und die Hinweise, dass die Datei dynamisch generiert und überschrieben wird. Konkret befinden sich am Ende dieser Datei die Reservierungen für alle Rechner, die mit `lddeploy` betrieben werden.

Der freie Bereich umfasst in einer Standardumgebung entsprechend 65.535-1 Adressen.

```
# Interface intern
...
range 10.31.0.1 10.31.255.254;
...
```

Wenn Sie einen anderen Netzwerkbereich gewählt haben, können entsprechend weniger Adressen zur Verfügung stehen.

III.4.6. DNS-Server

Der DNS-Server ist einer der wichtigsten Dienste im Serversystem und für die Namensauflösung (DNS = Domain Name System) zuständig. Es geht dabei um die Auflösung von Gerätenamen wie PCs, Notebooks, andere Server und Peripherie aber nicht die Namen von Benutzern im Netzwerk. Ähnlich wie auch im Internet ein Name wie `http://www.logodidact.de` in eine IP-Adresse aufgelöst wird und umgekehrt auch die IP-Adresse eine Verbindung zu einem Namen hat, ist das auch im lokalen Netzwerk beim LogoDIDACT-Server der Fall.

Der Namensdienst auf Serverseite heisst dort `bind` und ist per Standard so vorkonfiguriert, dass daran nichts geändert werden muss.

III.4.6.1. Verbotene Namen

Im LogoDIDACT-Server sind bereits etwa 40 Namen für Serverdienste und den Server selbst, die während der Installation im DNS eingetragen werden. Diese Namen dürfen deshalb auf keinen Fall an andere Geräte vergeben werden!

Vordefinierte Einträge finden sich am Server in der Datei `/etc/bind/template/db.domain.static`.



Achtung

An dieser Datei dürfen keine Veränderungen durchgeführt werden, da diese bei Updates überschrieben wird. Bei Updates kann es auch sein, dass LogoDIDACT zusätzliche Namen definiert. Man sollte also immer gewahr sein, dass Konflikte auftreten können, wenn ein neuer Systemname mit einem selbst definierten Namen übereinstimmt.

Derzeit sind dies `master`, `server`, `catalog`, `ldap`, `dhcp`, `mail`, `smtp`, `proxy`, `webfilter`, `samba`, `files`, `logon`, `gw`, `ns1`, `ns2`, `dns`, `ns`, `moodle`, `ntp`, `print`, `radius`, `rembo`, `sql`, `mysql`, `imap`, `cyrus`, `homepage`, `www`, `monitoring`, `webmail`, `cms`, `itb`, `wpad`, `mrbs`, `raumplan`, `raumbellegung`, `support`, `vpn`, `zarafa`, `portfolio`, `webclient`, `webconsole`, `console`.

III.4.6.2. DNS Rechnereintrag per `wimport_data`

Ein Großteil der Namen neuer Geräte wird automatisch über die Geräteliste (`wimport_data`) erzeugt, wenn ein Rechner dort manuell oder über die Rechneraufnahme eingetragen wird.



Achtung

Achten Sie darauf, dass Sie beim Eintragen in der Geräteliste weder verbotene Namen verwenden, noch verbotene Zeichen, wie z.B. den Unterstrich bzw. Underscore.

Die Manuelle Aufnahme über das ITB-Interface ist in Abschnitt V.2.1.3, „Geräteliste“ beschrieben, die automatische Aufnahme über den PXE-Netzwerkboot in ???. In beiden Fällen ist es so, dass durch den eigentlichen Vorgang des Importierens auf Serverseite ein Skript aufgerufen wird, das die neuen Geräte sowohl im DHCP-Server einträgt als auch im DNS-Server.

III.4.6.3. Dynamisches DNS

Dynamisches DNS oder kurz DDNS wird häufig auch als DNS Update bezeichnet und bedeutet im Umfeld des LogoDIDACT-Server, dass eine Arbeitsstation über die Kommunikation mit dem DHCP-Server seinen DNS-Namen aktualisiert.

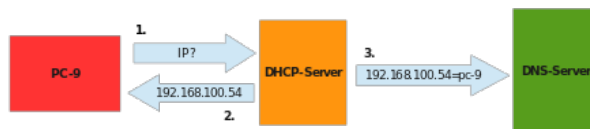


Abbildung III.4.2. Ablauf beim dynamischen DNS über den DHCP-Server (Bildquelle: wikipedia)



Achtung

In LogoDIDACT hat DDNS aufgrund des Imagings der Arbeitsstationen und der automatischen Zuweisung und Pflege von Rechnernamen über die Geräteliste in dieser Hinsicht keinen Nutzen.

Es ist sogar so, dass dadurch für bestimmte Systeme eher Probleme auftreten, wenn diese z.B. Mitglied in der Domäne sind (siehe Abschnitt MAC-Clients).

III.4.7. Laufwerke und Zugriffsberechtigungen

III.4.7.1. Zusätzliche Freigabe und Laufwerk einrichten

In LogoDIDACT gibt es verschiedene Freigaben (shares) auf dem Server, die teilweise versteckt sind und teilweise auch als offene Freigaben über die Suche von Ressourcen des Servers erkennbar sind.

Normalerweise reichen die per Standard vorhandenen und mit Freigaben verbundenen Laufwerksbuchstaben H:, T: und P: aus, um alles zu realisieren, was es an Anforderungen und Konstellationen an Schulen gibt. Es kann aber bei einem Umstieg von einer alten Lösung auf LogoDIDACT sinnvoll sein, bereits bestehende Laufwerksbuchstaben und Freigaben möglichst 1:1 zu übernehmen. Beschrieben wird dies beispielhaft an einem share "wpgm" und dem Laufwerksbuchstaben "Q:".

Legen Sie zunächst die Datei **/etc/samba/smb.conf.custom** an, bzw. fügen Sie dort einen Eintrag wie folgt ein, falls die Datei schon existiert.

```

# Share mit Vollzugriff für Jeden
[wpgm]
path = /home/samba/wprogs
admin users = @pgadmins
create mask = 0666
    
```



```
force directory mode = 0777
guest ok = yes
writeable = yes
include = /etc/samba/smb.conf.vscan
include = /etc/samba/smb.conf.wpgm
```

Danach muss die Konfigurationdatei von Samba neu eingelesen werden.

```
/etc/init.d/samba reload
```

Der nächste Schritt besteht darin festzulegen, dass über ein Anmeldeskript (Batchdatei) die Freigabe mit dem Laufwerksbuchstaben verbunden wird. Der einfachste Fall ist dabei, dass Schüler wie Lehrer die Freigabe bzw. den Buchstaben sehen sollen. Das geschieht über einen Eintrag in `/home/samba/netlogon/settings.bat`

```
REM Anpassung Laufwerksbuchstaben und Shares
set EXTRA_SHARES=Q: wpgm
```

Soll der Buchstabe nur für bestimmte Benutzergruppen verbunden werden, kann das über eine rollenbezogene Anmeldung erfolgen. Bei der Anmeldung wird geprüft, ob es eigene Anmeldeskripte gibt und diese zusätzlich aufgerufen. Der Ablauf ist hierbei wie folgt:

1. Gibt es `\\server\netlogon\role_%ROLE%.bat`, wird dieses ausgeführt. `%ROLE%` ist hierbei die Benutzerrolle, also `student`, `teacher`, `course` oder `admin`.
2. Gibt es `\\server\netlogon\group_%GROUP%.bat`, wird dieses ausgeführt. Für `%GROUP%` werden hierbei nacheinander alle Gruppen eingesetzt, in denen der Benutzer Mitglied ist.
3. Gibt es `\\server\netlogon\user_%USER%.bat`, wird dieses ausgeführt. `%USER%` ist hierbei der Benutzername des angemeldeten Benutzers.



Achtung

Bitte beachten Sie, dass Skripte nur ausgeführt werden können, wenn diese DOS-Zeilennenden besitzen (CRLF). Am Server können Sie das durch Aufruf von `flip -b -m skript.bat` sicherstellen.

Weitere Informationen dazu finden sich in der Datei `\\server\netlogon\INFO.txt`.

III.4.7.2. Zugriffsberechtigung ACLs in LogoDIDACT

Der LogoDIDACT Server unterstützt so genannte ACLs, d.h. Zugriffsberechtigungen, die auf Ordner- und Dateiebene sehr detailliert für Gruppen und Benutzer einstellbar sind. Diese Berechtigungen können grundsätzlich auch von einem Windows-Client aus auf Ordner am Server angepasst werden. Bitte bedenken Sie aber, dass es aus Gründen der Systemstabilität am Server bestimmte Ordner und dafür festgelegte Dateiberechtigungen gibt, die zwangsweise so belassen werden müssen.

Weiterhin gibt es Skripte dafür, die in einem Fehlerfall die Berechtigungen wieder korrekt zurücksetzen. Der Befehl in einer Shell am Server lautet dafür `repair_permissions` und kann gezielt für

bestimmte Ordner ausgeführt werden. Wenn man **repair_permissions** ohne Argument angibt, erhält man eine Auflistung aller unterstützten Optionen.

III.4.7.2.1. Datei und Verzeichnisrechte am Server prüfen

Bevor man die Rechte an Dateien und Ordnern ändert, sollte man sich diese am Server zunächst anschauen. Damit kann man dann konkret sowohl an Ordnern als auch an Dateien prüfen, ob sich die Rechte auch tatsächlich geändert haben. In Linux gibt es dazu den Befehl **getfacl**, mit dem sich die ACL, also die Zugriffsrechte auslesen und anzeigen lassen.

Als Beispiel, wechseln Sie dazu am Server mit **cd /home/tausch/Lehrer** in den Lehrertauschordner und erstellen dort mit dem Befehl **mkdir TEST** einen Unterordner Namens TEST. Mit dem Befehl **getfacl TEST** lesen Sie die Berechtigungen an diesem Unterordner aus und erhalten in etwa folgende Ausgabe:

```

root@ ~: /home/tausch/Lehrer# getfacl TEST
# file: TEST
# owner: root
# group: root
user::rwx
group::r-x
group:itbs:rwx
group:sysadmins:rwx
mask::rwx
other:---
default:user::rwx
default:group::r-x
default:group:itbs:rwx
default:group:sysadmins:rwx
default:mask::rwx
default:other:---
Standard-Berechtigungen für neue Ordner
oder neue Dateien im Ordner TEST (im Lehrertausch)

```

Abbildung III.4.3. Standard-Zugriffsrechte am Beispiel des Lehrertauschlaufwerkes

Ohne auf jedes Detail einzugehen, ist im unteren Bereich an den Kürzeln **rwx** (r für read, w für write, x für execute) erkennbar, dass nur verschiedene administrative Gruppen schreibenden Zugriff (Flag w) auf neu erstellte Dateien und Ordner haben. Ebenfalls hat es jeder Benutzer (user::rwx) für genau diejenigen Dateien und Ordner, die er dort selbst angelegt hat. Das ist genau die Standardeinstellung, die man von einem Tauschordner erwartet.

Wenn alle Lehrer im Tauschlaufwerk auch schreibenden Zugriff auf Dateien und Ordner anderer Kolleginnen und Kollegen haben sollen, führt man die Anpassung so durch, wie in Abschnitt III.4.7.6, „Vollzugriff der Lehrer auf Lehrer-Tausch“ beschrieben. Eine erneute Prüfung mit **getfacl TEST** macht die Änderung deutlich:

```

root@ ~: /home/tausch/Lehrer# getfacl TEST
# file: TEST
# owner: root
# group: root
user::rwx
group::r-x
group:sysadmins:rwx
group:itbs:rwx
group:lehrer:rwx
mask::rwx
other:---
default:user::rwx
default:group::r-x
default:group:sysadmins:rwx
default:group:itbs:rwx
default:group:lehrer:rwx
default:mask::rwx
default:other:---
Standard-Berechtigungen für neue Ordner
oder neue Dateien im Ordner TEST (im Lehrertausch)

NACH der Anpassung
"Vollzugriff der Lehrer auf Lehrer-Tausch"
(Gruppe lehrer::rwx)

```

Abbildung III.4.4. Zugriffsrechte im Lehrertauschlaufwerk nach der Anpassung "Vollzugriff der Lehrer auf Lehrer-Tausch"

Die Gruppe Lehrer hat nach der Anpassung Vollzugriff auf sämtliche Dokumente im Ordner Lehrertausch.

III.4.7.3. Zugriff für Lehrer auf Schüler Homelaufwerke

Per Standard hat in LogoDIDACT ein Lehrer KEINEN Zugriff auf die Homeverzeichnisse der Schüler. Abhängig von der Schulart bzw. dem Schultyp und damit auch dem Alter der Benutzer, erscheint Ihnen diese Voreinstellung logisch und richtig oder vollkommen unsinnig und nicht praktikabel.

Schüler an beruflichen Einrichtungen, die schon volljährig sind, haben ein Recht darauf, dass ihre Dateien und Daten nicht ohne Weiteres eingesehen oder gar verändert oder gelöscht werden können. Denken Sie an die Situation, dass ein elektronisches Dokument vom Lehrer bewertet wird und ein Schüler behauptet, dass das Dokument von einem Lehrer verändert und manipuliert wurde. Ebenso ist es einleuchtend, dass es bei Schülern im Grundschulalter einen anderen Maßstab für den Umgang mit Dateien geben kann.

Aus rechtlicher Sicht gibt es also verschiedene Positionen zu dem Thema, WER auf WESSEN Daten WIE zugreifen darf und im Normalfall sollte das an jeder Schule durch eine entsprechende Nutzungsordnung vor der Nutzung einmalig schriftlich geregelt werden.

Ungeachtet dieser unterschiedlichen Ansichten ist jedoch klar, dass man diese verschiedenen Einstellungen in LogoDIDACT anpassen kann.

III.4.7.4. Lesender Zugriff der Lehrer auf Schüler-Homes

Die Freigabe `classes$` ist in `/etc/samba/smb.conf.shares` vordefiniert und muss lediglich über die Datei `/home/samba/netlogon/settings.bat` zugeordnet werden.

Beispiele finden Sie auch in der Datei `example_settings.bat`. Kopieren Sie die Datei `example_settings.bat` nach `settings.bat` mit dem Befehl **cp example_settings.bat settings.bat**

Ändern Sie dann den Eintrag `set EXTRA_SHARES=Q: wpgm` um auf `set EXTRA_SHARES=S: classes$` und entfernen Sie die anderen Mappings, sofern Sie diese nicht benötigen.

III.4.7.5. Vollzugriff der Lehrer auf Schüler-Homes

Auch beim Vollzugriff, muss das vordefinierte Share wie zuvor beschrieben wieder über die `settings.bat` eingebunden werden.

Die Berechtigungen auf dieses Share sind definiert in `/etc/samba/smb.conf.shares`. Sie sollten die Berechtigungen aber NICHT direkt in dieser Datei abändern, da sie bei einem **ldupdate** überschrieben wird. Jedes Share besitzt aber eine Include-Anweisung mit konkreten Angaben zu einer benutzerdefinierten Datei:

```
[classes$]
comment = Klassen
path = /home/dynamic/Klassen
valid users = @sysadmins, @itbs, @lehrer
admin users = @sysadmins, @itbs
read only = yes
force user = root
force group = root
```

```
include = /etc/samba/smb.conf.classes$
```

Erstellen Sie also eine Datei `/etc/samba/smb.conf.classes$` (die Datei selbst hat im Dateinamen am Ende ein `$` und heisst wirklich `smb.conf.classes$`) und tragen Sie die beiden Parameter, die „überschrieben“ werden müssen, dort ein:

```
admin users = @sysadmins, @itbs, @lehrer
read only = no
```

Die Gruppe der Lehrer hat somit die Rechte der admin users und schreibenden Zugriff, d.h. man kann Dateien erstellen und löschen.

III.4.7.6. Vollzugriff der Lehrer auf Lehrer-Tausch

Per Standard haben die Lehrer im Lehrertauschlaufwerk nur lesenden Zugriff auf Dateien und Ordner anderer Kollegen und Vollzugriff auf selbst erstellte Dateien und Ordner. Soll das geändert werden, editieren Sie die entsprechende Stelle in `/etc/logodidact/service.conf`.

Standardeinstellung im Lehrer-Tausch (Vollzugriff nur auf selbst erstellte Dateien und Ordner):

```
TeachersSwapMode 01770
TeachersSwapOwner root
TeachersSwapGroup lehrer
TeachersSwapEnabled yes
TeachersSwapPermissions d:u::rwX d:g::rX d:o::- ↪
d:g:lehrer:rwX
TeachersSwapPermissions u::rwX g::rwX o::- ↪
g:lehrer:rwX
```

Vollzugriff für alle Lehrer auf Dateien und Ordner im Lehrer-Tausch:

```
TeachersSwapMode 00770
TeachersSwapOwner root
TeachersSwapGroup lehrer
TeachersSwapEnabled yes
TeachersSwapPermissions d:u::rwX d:g::rwX d:o::- ↪
d:g:lehrer:rwX
TeachersSwapPermissions u::rwX g::rwX o::- ↪
g:lehrer:rwX
```



Achtung

Damit die Berechtigungen an bereits bestehenden Ordnern und Dateien verändert werden, muss noch ein `repair_permissions --tausch` ausgeführt werden. Damit neu erzeugte Dateien und Ordner die richtigen Rechte erhalten, muss auch der ldserver neu gestartet werden: `/etc/init.d/ldserver restart`

III.4.7.7. Vollzugriff aller Benutzer auf Schulweiter Tausch

Im Bereich Schulweiter Tausch haben sowohl Lehrer als auch Schüler per Standardeinstellung nur lesenden Zugriff auf Dateien und Ordner anderer Benutzer und Vollzugriff auf die selbst erstellten

Dateien und Ordner. Soll das geändert werden, editieren Sie die entsprechende Stelle in `/etc/logodidact/service.conf`.

Standardeinstellung im schulweiten Tausch (Vollzugriff nur auf selbst erstellte Dateien und Ordner):

```
GlobalSwapMode 01777
GlobalSwapOwner root
GlobalSwapGroup root
GlobalSwapEnabled yes
GlobalSwapPermissions d:u::rwX d:g::rwX d:o::rwX ↵
d:g:lehrer:rwX
GlobalSwapPermissions u::rwX g::rwX o::rwX ↵
g:lehrer:rwX
```

Vollzugriff für alle Benutzer auf Dateien und Ordner im schulweiten Tausch:

```
GlobalSwapMode 00777
GlobalSwapOwner root
GlobalSwapGroup root
GlobalSwapEnabled yes
GlobalSwapPermissions d:u::rwX d:g::rwX d:o::rwX ↵
d:g:lehrer:rwX
GlobalSwapPermissions u::rwX g::rwX o::rwX ↵
g:lehrer:rwX
```

Entscheidend bei dieser Anpassung ist nur das so genannte Sticky Bit, d.h. die Änderung des Parameters **GlobalSwapMode 01777** auf **GlobalSwapMode 00777**.



Achtung

Damit die Berechtigungen an bereits bestehenden Ordnern und Dateien verändert werden, muss noch ein **repair_permissions --tausch** ausgeführt werden. Damit neu erzeugte Dateien und Ordner die richtigen Rechte erhalten, muss auch der Idserver neu gestartet werden: **/etc/init.d/ldserver restart**

III.4.7.8. Vollzugriff auf Klassen-Tauschlaufwerke

Standardeinstellung für Klassentauschlaufwerke (in `/etc/logodidact/service.conf`):

```
ClassesSwapMode 01770
ClassesSwapOwner root
ClassesSwapGroup $class
ClassesSwapEnabled no
ClassesSwapPermissions d:u::rwX d:g::rX d:g:$class:rwX ↵
d:o::rX d:g:lehrer:rwX
ClassesSwapPermissions u::rwX g::rwX g:$class:rwX ↵
o::rX g:lehrer:rwX
```

Vollzugriff für alle Lehrer auf Dateien und Ordner im Klassen-Tausch:

```
ClassesSwapMode 00770
```

```
ClassesSwapOwner root
ClassesSwapGroup $class
ClassesSwapEnabled yes
ClassesSwapPermissions d:u::rwX d:g::rwX d:o::rx d:g:lehrer:rwX ↵
  d:g:schueler:rwX
ClassesSwapPermissions u::rwX g::rwX o::rx g:lehrer:rwX ↵
  g:schueler:rwX
```



Achtung

Damit die Berechtigungen an bereits bestehenden Ordnern und Dateien verändert werden, muss noch ein **repair_permissions --tausch** ausgeführt werden. Damit neu erzeugte Dateien und Ordner die richtigen Rechte erhalten, muss auch der Ldserver neu gestartet werden: **/etc/init.d/ldserver restart**

III.4.7.9. Klassentauschlaufwerke deaktivieren

Die Klassentauschlaufwerke lassen sich in `/etc/logodidact/service.conf` deaktivieren:
`ClassesSwapEnabled no`

III.4.7.10. Tauschlaufwerke zyklisch löschen

Der eigentliche Grundgedanke eines Tauschlaufwerkes ist derjenige, dass Dokumente dort wirklich nur temporär eben für den Zweck des Austausches zwischengespeichert werden. Oftmals wird diese Funktion aber „missbraucht“ und das Tauschlaufwerk wird immer voller und mutiert zur zentralen Datenablage.

Ein weiteres Problem der Tauschlaufwerke besteht darin, dass die dort abgelegten Dateien die Quota des Benutzers, der sie ablegt, belasten. Ein Benutzer, der dort also viele Dateien ablegt und in seinem Homelaufwerk hingegen nur wenig speichert, kann trotzdem die Meldung erhalten, dass seine Quota erschöpft ist, was ihm in aller Regel vollkommen unerklärlich erscheinen wird. Es gibt derzeit noch keine Ansicht für den Endbenutzer, um festzustellen, wo überall Dateien liegen (außerhalb seines Homeverzeichnis), die seiner Quota zugerechnet werden.

In der `service.conf` im Abschnitt `[Usermanagement]` können folgende Parameter gesetzt werden:

- `ArchiveSwapMaxAge 14d` = Entfernte Dateien zur Sicherheit für 14 Tage archivieren (`/home/archive/Tausch`).
- `GlobalSwapPrune 1h` = Dateien älter als 1 Stunde aus dem globalen Tausch entfernen, also praktisch alle Dateien.
- `TeachersSwapPrune` = Dateien im Lehrertauschlaufwerk löschen. Ist der Parameter nicht gesetzt bzw. leer oder hat einen Wert < 60 Sekunden, dann wird das Verzeichnis NICHT gesäubert.
- `ClassesSwapPrune 4d` = Klassentauschdateien älter als 4 Tage entfernen.
- `CoursesSwapPrune 7w` = Dateien älter als 7 Wochen in Kurstauschordnern löschen.
- `ProjectsSwapPrune 1y` = Dateien älter als 1y in Projekttauschordnern löschen.

Die Parameter sollten aus optischen Gründen und zur einfacheren Erkennung am besten unter dem jeweiligen Abschnitt gesetzt werden, innerhalb dessen auch die Rechte und Berechtigungen geregelt werden.

Hier ein Beispielauszug aus der `service.conf`, wobei die fett markierten Einträge per Standard NICHT enthalten sind:

```
ArchiveHome yes
ArchiveMails yes
ArchiveSwapMaxAge 30d

GlobalSwapMode 01777
GlobalSwapOwner root
GlobalSwapGroup root
GlobalSwapEnabled yes
GlobalSwapPermissions      d:u::rwX    d:g::rwX    d:o::rwX  ↪
    d:g:lehrer:rwX
GlobalSwapPermissions      u::rwX     g::rwX     o::rwX    ↪
    g:lehrer:rwX
GlobalSwapPrune 1h
```

Die Reinigung findet nachts über `/usr/lib/logodidact/nightly/prune` automatisch statt. Manuell anzustoßen über: **`prune_swap -p`** oder Testdurchlauf mit Ausgabe, was passieren würde **`prune_swap -p -t`**

III.4.7.11. Anpassung der Dateigröße beim Austeilen

In der Datei `/etc/logodidact/service.conf` im `logosrv` finden sich viele weitere Optionen und Parameter, die angepasst werden können. In aller Regel müssen Sie daran aber nichts ändern, weil die vorgegebenen Werte für die meisten Umgebungen passend gewählt sind.

Wenn die Dateigröße beim Austeilen über die LogoDIDACT-Console angepasst werden müssen, dann können Sie dies über die folgenden beiden Werte tun.

```
DistributeFilesSoftLimit 20MB
DistributeFilesHardLimit 50MB
```

III.4.8. Cron-Jobs

So genannte cron-jobs zur zeitlichen Steuerung von Vorgängen werden in LogoDIDACT in der Datei **`/etc/crontab`** definiert.

Bitte ändern Sie auf keinen Fall etwas an den bestehenden Einträgen, sondern ergänzen Sie die vorhandenen Einträge durch Ihre spezifischen Kommandos. Im Beispiel unten wird an alle Rechner ("*") von Montags bis Freitags um 7:00 Uhr ein Wake-On-LAN Paket gesendet, so dass Sie aufgeweckt werden. Um 9:40 Uhr und um 13:20 Uhr wird dieser Vorgang wiederholt.

```
# m h dom mon dow user  command

# von Mo bis Fr. PCs wecken um 07:00 Uhr, 9:40 und 13:20
0 7 * * 1-5 root /usr/bin/ldhost -w "*" >/tmp/ldhost.log 2>&1
40 9 * * 1-5 root /usr/bin/ldhost -w "*" >/tmp/ldhost.log 2>&1
20 13 * * 1-5 root /usr/bin/ldhost -w "*" >/tmp/ldhost.log 2>&1
```

```
# von Mo bis Fr. Rechner um 18 Uhr alle PCs in den
# Räumen r0* und r2* herunterfahren
00 18 * * 1-5 root /usr/bin/ldhost -s "r0*,r2*" >/tmp/ldhost.log 2>&1

# Signal an alle Rechner um 21 Uhr, ALLE herunterfahren
00 21 * * 1-5 root /usr/bin/ldhost -s "*" >/tmp/ldhost.log 2>&1
```

Die Voraussetzung dafür, dass die Rechner tatsächlich aufwachen, müssen selbstverständlich gegeben sein und können von LogoDIDACT nicht beeinflusst werden. Die Systeme müssen sowohl vom BIOS her WOL unterstützen und entsprechend richtig konfiguriert sein, als auch durchgehend mit dem Stromnetz verbunden sein (keine Schüsselschalter und/oder nächtliche Stromabschaltung). Weiterhin funktioniert WOL in aller Regel nur, wenn die Computer sauber Heruntergefahren werden, so dass sich die Netzwerkkarten in einem definierten Zustand befinden. Weiterhin ist im Beispiel umgesetzt, dass die Rechner in den Räumen r0* und r2* um 18:00 Uhr ein Signal zum Herunterfahren erhalten und alle Rechner dann nochmals ein solches Signal um 21:00 Uhr. Voraussetzung dafür ist, dass die Rechner dem Namensschema auch folgen, d.h. die Rechner selbst heißen r01 oder r01-01 usw.. Eine zweite Voraussetzung dafür ist die, dass auf den Arbeitsstationen der LogoDIDACT-Agent installiert ist, d.h. das Herunterfahren funktioniert nicht für private Geräte oder Geräte, die ohne Rembo/mySHN® bzw. LogoDIDACT betrieben werden.

III.4.9. Befehle und Skripte am logosrv

In diesem Abschnitt werden einige Befehle und Skripte aufgeführt, die man direkt am logosrv an der Console ausführen kann und die sehr nützlich sein können. Dies ist keine vollständige Auflistung sämtlicher verfügbaren Befehle und Skripte.



Tipp

Befehle und Skripte, die man in LogoDIDACT 1.0 im monolithischen System an beliebiger Stelle aufrufen konnte, verteilen sich nun logischerweise auf die jeweiligen Container und sind nur dort verfügbar. Ein einfaches Beispiel dafür ist der Befehl **myhosts** der anzeigt, wann die Rechner zuletzt ein Image synchronisiert haben. Dieser Befehl kann nur im Container **rembo5** aufgerufen werden.

Tabelle III.4.2. Tabelle nützlicher LogoDIDACT Befehle und Skripte

Befehl/Skript	Funktion
teachers (Befehl ohne Parameter)	Zeigt alle Lehrerkonten an
students (Befehl ohne Parameter)	Zeigt alle Schülerkonten an

Die zweite Gruppe bilden die so genannten **ld**-Befehle, d.h. alle Tools, Skripte und Programme, die mit dem Namen **ld** als Abkürzung für LogoDIDACT beginnen.

Wenn man auf der Shell im Container **logosrv ld** gefolgt von TAB eingibt, erhält man eine Liste von etwas mehr als 50 LogoDIDACT spezifischen Befehlen und Tools aufgelistet. Ein großer Teil der Befehle hat eine entsprechende Anbindung an die graphische Oberfläche der LogoDIDACT-Console, so dass normalerweise keine Notwendigkeit darin besteht, das Tool auf Kommandozeilenebene auszuführen. Ein Beispiel dafür ist der Befehl **lduser**, über den man mit einem Benutzerkonto alles das machen kann, was auch graphisch machbar ist, d.h. anlegen, löschen, versetzen, Kennwort ändern usw.

Diese Tools erwarten in der Regel einen oder viele weitere Parameter, die man aufgelistet bekommt, wenn man den Befehl ohne Parameter eingibt.

An dieser Stelle sollen jedoch nur solche **ld**-Befehle aufgelistet werden, die kein entsprechendes graphisches Äquivalent haben oder die einem bei der Fehlersuche direkt am Server sehr nützlich sind.

Tabelle III.4.3. Tabelle der so genannten **ld**-Befehle und Skripte im logosrv

Befehl/Skript	Funktion
ldcheck -a (Befehl mit Parametern)	Zeigt den Status sämtlicher LogoDIDACT Dienste am Server an.
ldcheck -l (Befehl mit Parametern)	Führt eine Schleifenprüfung auf dem internen Interface durch.
ldhost -w (Befehl mit Parametern)	Weckt einen Rechner per WOL auf.

Ebenfalls an dieser Stelle eine Aufführung einiger nützlicher Linux-Befehle.

Tabelle III.4.4. Tabelle nützlicher Linux Befehle und Skripte

Befehl/Skript	Funktion
quota -s USERNAME (Befehl mit USERNAME als Parameter)	Zeigt die Quota eines Benutzers in Megabyte an.

III.4.10. Apache Webserver

Der Apache HTTP Server ist der meistbenutzte Webserver im Internet und wird auch in LogoDIDACT als interner Webserver verwendet.

III.4.10.1. Aktivierung interner Webseiten über public_html

Häufig wird von Lehrern der Wunsch geäußert, dass die Schüler intern eigene HTML-Seiten erstellen können sollen, die dann auch so getestet werden können, als würden diese im Internet liegen. Dabei soll es Seiten geben, die nur vom Schüler selbst betrachtet werden können als auch Seiten, die von anderen Benutzern aufgerufen und betrachtet werden können.

Dafür bietet Apache von Hause aus die Option eines Zugriffs über das Homeverzeichnis eines Benutzers. Der Ordner dafür heisst per Standard `public_html` für den Zugriff auch von anderen Benutzern.

Zunächst muss das Apache Modul für diesen Zugriff aktiviert werden:

```
a2enmod userdir
```

.

Dies ist möglicherweise nicht notwendig, wenn man den Standard-Ordner `public_html` verwendet. Über das folgende Skript legt man die Ordner an und setzt die Berechtigungen:

```
for dir in /home/users/*; do
[ ! -d "$dir/public_html" ] && mkdir "$dir/public_html"
[ -d "$dir/public_html" ] && chmod -R a+rX "$dir/public_html"
```

done

III.4.10.2. Schulinterne Homepage im Intranet aktivieren

Eine zweite etwas weniger problematische Art interne Webseiten bzw. eine eigene Homepage zu erstellen, besteht in der zentralen Ablage auf dem Server mit beschränktem schreibenden Zugriff nur für bestimmte Nutzer oder Gruppen.

III.4.10.2.1. Den virtuellen Host "homepage" verwenden und anpassen

Ein virtueller Host ist nichts anderes, als dass man den Webserver so konfiguriert, dass er für verschiedene Namen die man im Webbrowser eingibt, verschiedene Seiten liefert. Dies ist in LogoDIDACT für die Namen itb, moodle, cups, mrbs und viele weitere webbasierte Dienste bereits der Fall, d.h. das alles sind virtuelle Hosts (kurz vHosts). Jeder Name muss natürlich so interpretiert bzw. umgesetzt werden, dass man damit beim entsprechenden Dienst landet.



Achtung

Es gibt in LogoDIDACT auch den vordefinierten virtuellen Host (vHost) "homepage". Der Sinn und Zweck dieses virtuellen Hosts besteht allerdings allein darin, dass man auf einfache Art und Weise, den Namen "homepage" auf die reale Internetseite der Schule umleitet.

Der vHost ist nicht(!) dafür gedacht, dass man darüber ein internes Intranet aufbaut, was ja auch aufgrund des Namens missverständlich wäre.

Unter `/etc/apache2/sites-enabled/homepage` ist der Pfad zum Verzeichnis zu finden, innerhalb dessen der Apache Webserver nach Inhalten sucht (hier `/var/www/homepage`):

```
<VirtualHost *>
ServerName homepage.schule.local
ServerAlias homepage
ServerAlias homepage.*
ServerAdmin webmaster@schule.local

DocumentRoot /var/www/homepage/
...
```

Per Standard liegt dort im Verzeichnis `/var/www/homepage` die Datei `index.rhtml` in der ein sogenannter Redirect, d.h. eine Umleitung, auf `google.de` steht. Möchte man nun erreichen, dass bei Eingabe von "homepage" im Browser z.B. die Seite `http://www.logodidact.de` aufgerufen wird, muss man lediglich die Umleitung anpassen:

```
<%
require "/usr/lib/logodidact/utils.rb"
require "cgi"

cgi = CGI.new
url = SI.get("homepage.redirect") || "http://www.google.de"
```

```
cgi.header("Location" => url);
%>
```

III.4.10.2.2. Einen neuen virtuellen Host "intranet" anlegen

Wie oben erwähnt, ist der virtuelle Host "homepage" nicht dafür gedacht ein lokales Intranet aufzubauen. Deshalb wird im Folgenden beschrieben, wie man einen neuen Host "intranet" anlegt. Dazu wird die bereits bestehende Konfiguration des Hosts "homepage" als Vorlage verwendet, kopiert und angepasst:

```
cd /etc/apache2/sites-available/
cp homepage intranet
rpl homepage intranet intranet
cd /etc/apache2/sites-enabled/
ln -s /etc/apache2/sites-available/intranet /etc/apache2/
sites-enabled/intranet
mkdir /var/www/intranet
```

Anschliessend wird die Datei `.htaccess` in das Verzeichnis gelegt, über die der Zugriff auf Dateien, Ordner und Unterordner geregelt werden kann. Die Datei `index.html` dient nur für einen ersten Test des Intranets.

```
cd /var/www/intranet
echo Options +indexes > .htaccess
echo Hallo Intranet > index.html
```

Danach wird der Apache Webserver über den Befehl `apache2ctl graceful` neu gestartet werden, wobei die Option `graceful` bewirkt, dass aktive Verbindungen nicht gestört werden.

Damit der Name "intranet" aufgelöst werden kann, muss die Datei in `/etc/bind/template/db.domain.static.custom` angelegt bzw. erweitert werden mit folgendem Inhalt:

```
intranet    CNAME server
```

Abschliessend muss nur noch der DNS-Server über den Befehl `update_dns` über den neuen Alias Namen informiert werden. Die Seite sollte nun direkt am Server über den textbasierten Webbrowser `lynx` aufgerufen werden können:

```
lynx http://intranet
```

III.4.10.2.3. Zugriff auf das Verzeichnis "intranet" festlegen

Damit nun im bestehenden Verzeichnis `/var/www/intranet` Internetseiten abgelegt werden können muss über die entsprechende Samba-Konfiguration in `/etc/samba/smb.conf.custom` der Zugriff geregelt werden:

```
[intranet]
```

```
comment = Intranet Verzeichnis
path = /var/www/intranet
valid users = @sysadmins, @pgadmins, @datenschutz
admin users = @sysadmins, @pgadmins, @datenschutz
write list = @sysadmins, @pgadmins, @datenschutz
read only = no
force user = root
force group = root
```

Damit die Freigabe in Samba auch aktiviert wird, muss noch der Befehl `/etc/init.d/samba reload` ausgeführt werden. Dort können nun entsprechend den Rechten HTML-Seiten abgelegt werden. Im obigen Beispiel können nur Mitglieder der administrativen Gruppen Daten ablegen.

III.4.11. Rechte und Berechtigungen

III.4.11.1. Zugriff auf Funktionen in der LogoDIDACT-Console ändern

In der LogoDIDACT-Console hat man in seiner jeweiligen Rolle als Lehrer oder administrativer Benutzer exakt die Möglichkeiten, die im Normalfall für die jeweilige Rolle praxisgerecht sind. Ein "normaler" Lehrer kann also im Bereich des Moduls Benutzerverwaltung genau das an Funktionen durchführen, was er für den Unterricht tun können muss. Alle anderen Funktionen sind ausgegraut und damit nicht aufrufbar.

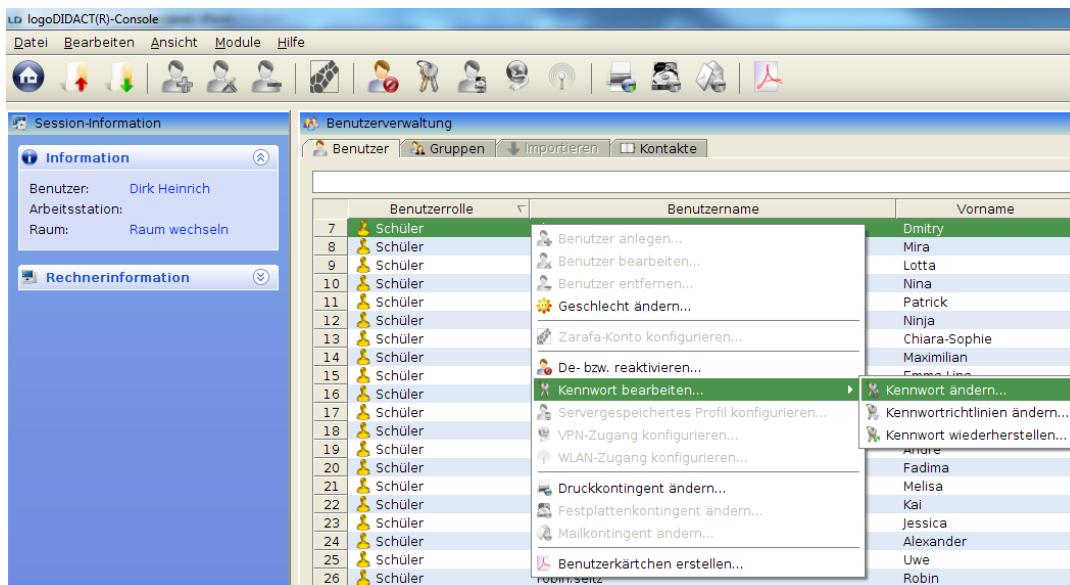


Abbildung III.4.5. Funktionen die in der Rolle Lehrer in der LogoDIDACT-Console nutzbar sind.

Andere Aufgaben im Bereich des Benutzermanagements sind der Rolle der administrativen Benutzer zugeordnet (Benutzer **admin**).

III.4.11.1.1. Zugriff für Lehrer auf Funktionen in der LogoDIDACT-Console anpassen

Es gibt jedoch bestimmte Funktionen und Steuerungsmöglichkeiten, die man abhängig vom Kollegium bzw. der Schule vielleicht allen oder auch einzelnen Lehrern erlauben möchte.

Solche Anpassungen für die LogoDIDACT-Console sind auf Serverseite im Pfad `/etc/logodidact/acl` machbar. Im Falle der Gruppe Lehrer, legen Sie dort eine Datei `/etc/logodidact/acl/role/teacher/custom.allow` an. Um z.B. allen Lehrern das Ändern der Quotas zu ermöglichen, muss in der Datei `custom.allow` folgende Zeile hinzugefügt werden:

```
user modify attrs=lddiskquota,ldmailquota,diskquota,mailquota
```

Damit die Änderungen wirksam werden, muss der Befehl **ldserver restart** ausgeführt werden. Danach sind die Einträge zur Änderung der Quota-Einstellungen auch für Lehrer verfügbar und nicht mehr ausgegraut.

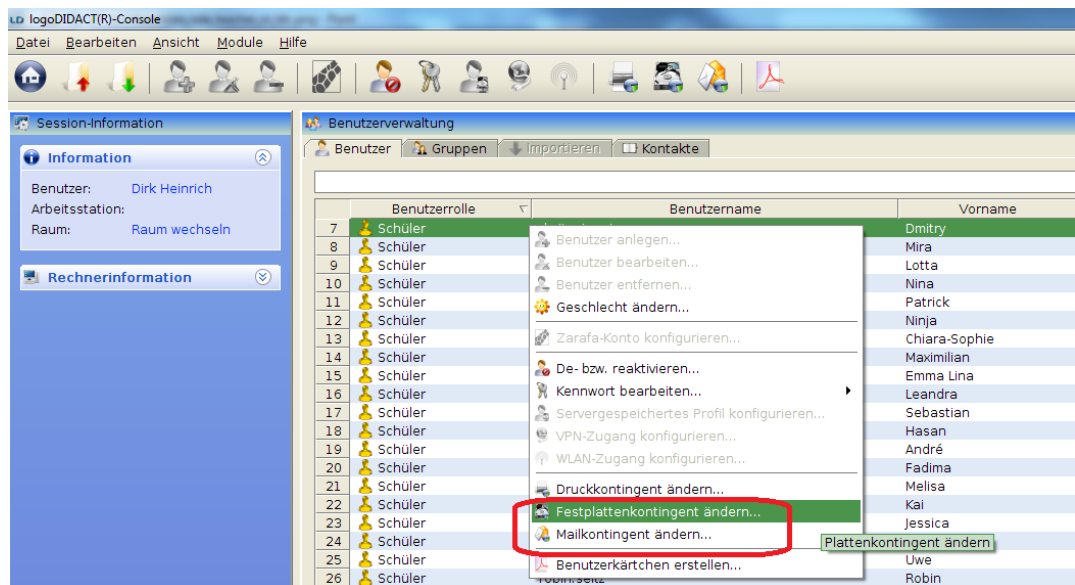


Abbildung III.4.6. Erweiterte Funktionen der Rolle Lehrer in der LogoDIDACT-Console.

III.4.11.1.2. Zugriff für einen speziellen Benutzer auf Funktionen in der LogoDIDACT-Console anpassen

Soll der Zugriff nur für einen bestimmten Benutzer erlaubt werden, ist das Vorgehen, wie bereits zuvor beschrieben. Der Pfad für die entsprechende Datei ist jedoch wie folgt: `/etc/logodidact/acl/user/BENUTZERNAME/custom.allow`.

Damit z.B. der Lehrer Dirk Heinrich (Benutzername "hei") den WLAN-Zugriff in der LogoDIDACT-Console für Schüler aktivieren oder deaktivieren kann, sind folgende Schritte notwendig:

```
cd /etc/logodidact/acl/user
mkdir hei
cd hei
echo 'user modify rcpt_role=student attrs=ldallowwlan' > custom.allow
```

Es werden dabei die zuvor auf Gruppenebene definierten Zugriffsrechte mit den auf Benutzerebene definierten Rechten so kombiniert, wie man dies erwartet, d.h. im obigen Beispiel hat nur der Lehrer Dirk Heinrich das Recht in der LogoDIDACT-Console wlan bei den Schülern zu steuern. Als Mitglied der Gruppe Lehrer hat er aber auch das Recht, die verschiedenen Quotas anzupassen.

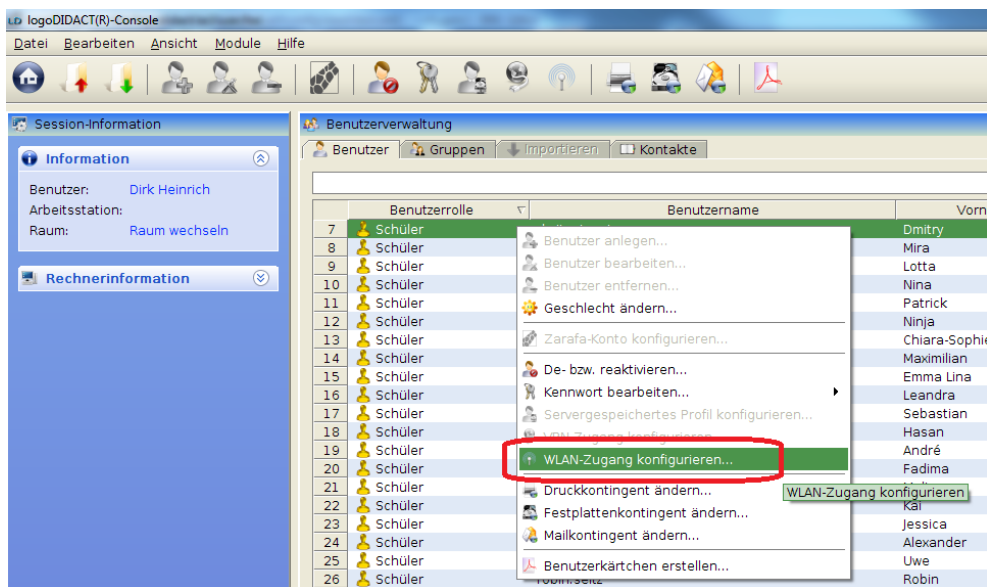


Abbildung III.4.7. Erweiterte Funktionen für einen einzelnen Benutzer in der LogoDIDACT-Console.

III.4.11.1.3. Zugriff für Schüler auf die LogoDIDACT-Console

Prinzipiell besteht die Möglichkeit, dass auch Schüler auf die LogoDIDACT-Console zugreifen können. Dies wurde im Hinblick auf die Weiterentwicklung von LogoDIDACT von Anfang an berücksichtigt.



Achtung

Der Zugriff auf die LogoDIDACT-Console durch Schüler bietet derzeit keinen realen Mehrwert und wird hier nur der Vollständigkeit halber erwähnt.

In Anlehnung an die obigen Beschreibungen muss die Datei `custom.allow` mit den Zugriffsberechtigungen dabei in das Verzeichnis `/etc/logodidact/acl/role/student`.

```
#group list
host list
#room list
user list rcpt_user_uid=$user
user modify rcpt_ldrole=student attrs=password,ldinitialpassword
ldc run
ldc user view rcpt_user_uid=$user
```

III.4.11.2. Gruppe Datenschutz und Verwaltung

In LogoDIDACT gibt es neben den vordefinierten speziellen Benutzern, wie z.B. `pgmadmin`, `admin` und `itb` auch vordefinierte spezielle Gruppen wie z.B. die Gruppe `Datenschutz und Verwaltung`. Diese beiden Gruppen sind primär dafür da, das Thema Internetauswertung bzw. Auswertung des Surfverhaltens datenschutzrechtlich sauber abzubilden.

Das Thema `Datenschutz und Logauswertung` ist in den jeweiligen Bundesländern sehr unterschiedlich geregelt und es gibt leider keine einheitlichen übergreifenden Regelungen, geschweige denn ein Gesetz, das dieses Thema zuverlässig und rechtssicher behandelt.

Wenn man das Thema Auswertung der Internetzugriffe von der praktischen Seite her betrachtet, ist für jeden leicht nachvollziehbar, dass dies auch von der Schulart abhängt. Was bei einer Grundschule eher unkritisch ist (z.B. alle Lehrer dürfen Auswerten), geht bei volljährigen Schülern einer Berufsschule natürlich gar nicht. Nicht zuletzt ist das Thema auch davon abhängig, ob es eine Schulordnung gibt, bzw. das Thema EDV und Auswertung darin geklärt wird.

Deshalb wurde dieses Thema, wie so vieles in LogoDIDACT so umgesetzt, dass man die Auswertung der Internetzugriffe an die Gegebenheiten des Landes, der regionalen Vorschriften oder auch der jeweiligen Schule anpassen kann.

III.4.11.2.1. Lehrer zur Gruppe Datenschutz hinzufügen

Damit ein Lehrer in der LogoDIDACT-Console das Surfverhalten der Schüler einsehen kann (siehe Abschnitt V.1.3.1, „Auswertung der Internetzugriffe“), muss er Mitglied in der Gruppe Datenschutz sein.

Diese Zuordnung eines Benutzers zu einer Gruppe ist bewusst nicht über die LogoDIDACT-Console machbar, weil man sich sonst temporär als Benutzer "admin" kurzfristig in jede beliebige Gruppe stecken und damit das Thema Datenschutz ad absurdum führen könnte. Deshalb ist diese Zuordnung nur auf einer anderen Ebene und zwar als Benutzer root direkt am Server machbar. Damit ist also eine Trennung von Aufgaben, Rechten und Verantwortungsbereichen so möglich, wie sie von vielen Schulen, Schulträgern oder externen Firmen nicht nur gewünscht, sondern oftmals zwingend erforderlich ist. Verfügt ein Lehrer über alle Kennwörter, inkl. root, so ist mit diesem Zugang am Server ohnehin alles möglich.

Über den folgenden Befehl direkt am Server wird der Benutzer **anmeldename** der Gruppe **datenschutz** hinzugefügt.

```
ldprivacy -a datenschutz anmeldename
```

Anschliessend kann mit dem Befehl **ldprivacy -l** geprüft werden ob die Zuordnung funktioniert hat und wer sonst noch alles in der Gruppe **datenschutz** Mitglied ist.



Achtung

Ist ein Lehrer Mitglied der Gruppe Datenschutz, hat er "nur" Zugriff auf das Surfverhalten von Schülern. Um auch auf Log-Dateien von Lehrern Zugriff zu erhalten, ist eine weitere Person aus der Gruppe Schulleitung notwendig.

III.4.12. Benutzer und Kennwörter

In diesem Abschnitt wird beschrieben welche Konfigurationsmöglichkeiten es auf Serverseite für den Administrator hinsichtlich der Festlegung von Anmeldenamen und Kennwörtern gibt.

III.4.12.1. Benutzer

III.4.12.1.1. Namenskonvention

Beim Anlegen von Benutzern in LogoDIDACT (siehe Abschnitt V.1.1, „Benutzerverwaltung“ werden die Anmeldenamen nach einer bestimmten Konvention in der Regel aus Vornamen und Nachname gebildet.

Die Standardeinstellung für Schüler ist dabei **Vorname.Nachname**, d.h. die Schülerin "Lieschen Müller" würde entsprechend dieser Konvention den Anmeldenamen **Lieschen.Mueller** erhalten.

Umlaute und Sonderzeichen werden automatisch so gewandelt, dass diese den technischen Regeln und Richtlinien der Betriebssysteme und des Internets entsprechen, d.h., keine Umlaute in Anmeldenamen und E-Mails und Beschränkung der Länge von Anmeldenamen.



Achtung

Die Konvention **Vorname.Nachname** für Schülerkonten hat sich in der Praxis bewährt und sollte wenn möglich beibehalten werden. Mit dieser Konvention gibt es nur dann einen minimalen Mehraufwand für Schüler mit identischem Vor- und Nachnamen.

Soll die Namenskonvention trotzdem angepasst werden, so ist diese am Server in `/etc/logodidact/user.conf` im Abschnitt **[Role]** möglich. Sollte ein Benutzername bereits belegt sein, gibt es eine zweite, dritte einige weitere Konventionen die so angewandt werden, wie sie in ihrer Reihenfolge von oben nach unten in der Datei `user.conf` stehen:

```
UserName %firstname.%lastname
UserName %firstname-%middlename.%lastname
UserName %initial.%lastname
UserName %initial%lastname
UserName %firstname(2)%lastname(6)
UserName %firstname(2)%lastname(6)%num
```



Achtung

Was Sie auf keinen Fall machen dürfen:

Das ändern der Anmeldekonzvention (für Schüler) im laufenden Betrieb mündest bei den meisten Schulen zwangsweise in einem Chaos. So etwas sollte man nur zum Schuljahresende bzw. Beginn durchführen und dann komplett für alle Benutzer. Am besten löscht man dazu alle Schüler und legt diese neu an.

Die Konvention spielt für Lehrerkonten dabei keine Rolle, weil dort in der Regel das Lehrerkürzel des jeweiligen Benutzers als Anmeldeame verwendet wird.

Beim Bilden von Benutzeramen werden verschiedene andere Dinge berücksichtigt, die in der Praxis eine Rolle spielen. Bei Vornamen mit Bindestrich wird der gesamte Name verwendet Bei mehreren durch Leerzeichen getrennte Vorname wird nur der erste Vorname verwendet Bei mehreren durch Leerzeichen getrennte Nachnamen (z.B. "van Helsing") werden diese durch Bindestrich zu einem Nachnamen verbunden. So gebildete Namen werden grundsätzlich auf die Einhaltung einer Länge von 20 Zeichen geprüft und gegebenenfalls die Konvention geändert.

III.4.12.1.2. Servergespeichertes Benutzerprofil

Jeder Administrator, der sich intensiv mit dem Thema servergespeicherte Profile beschäftigt hat, kennt die Probleme, die damit in der Praxis mehr oder weniger regelmäßig auftreten.

Gerade an Schulen ist die Aktivierung eines individuellen servergespeicherten Profils für jeden Schüler genau das, was man nicht haben will, denn damit ist das Chaos vorprogrammiert. Auch die meisten der unerfahrenen Kolleginnen und Kollegen bescheren dem Administrator damit eher viel unnötige Zusatzarbeit.



Tipp

Deshalb ist es in LogoDIDACT empfehlenswert die bewährte Lösung des DefaultUser-Profiles zu verwenden, bei der über das Profil des Benutzers `pgmadmin` die Vorlage für alle Benutzer definiert wird (siehe ???).

In bestimmten Ausnahmesituationen kann es allerdings doch gewünscht oder sogar notwendig sein, dass einzelne Benutzer ein servergespeichertes Profil erhalten. Das ist z.B. in einem Verwaltungsnetzwerk der Fall, wenn wenige Benutzer Ihren Desktop individuell anpassen wollen oder für bestimmte Anwendungen wie z.B. Outlook in Kombination mit dem Zarafa-Server anpassen müssen. Bei Outlook lassen sich dann über das servergespeicherte Profil unabhängig vom Image benutzerspezifische Einstellungen aktivieren, wie z.B. welche anderen Postfächer eingebunden werden.

Sie können über die LogoDIDACT-Console als Benutzer `admin` ein servergespeichertes Profil aktivieren, wie in der folgenden Abbildung dargestellt. Wie jedoch ersichtlich, ist diese Option per Standard ausgegraut und damit nicht aktivierbar.

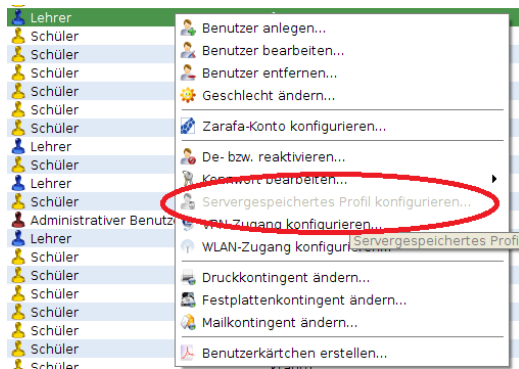


Abbildung III.4.8. Servergespeichertes Profil über LogoDIDACT-Console zur Sicherheit nicht aktivierbar

Der Grund liegt einfach darin, dass man in 99% der Fälle auf servergespeicherte Profile verzichten kann und damit in der Praxis deutlich weniger Probleme hat.

Um die ausgegraute Option zu aktivieren, muss man am Server in der Datei `/etc/logodidact/service.conf` den folgenden Parameter hinzufügen:

```
...
# --- Benutzermanagement -----
[Usermanagement]
AllowServerProfiles yes
...
```

Damit die Änderung übernommen wird, muss der Befehl `ldserver restart` ausgeführt und die LogoDIDACT-Console neu gestartet werden.

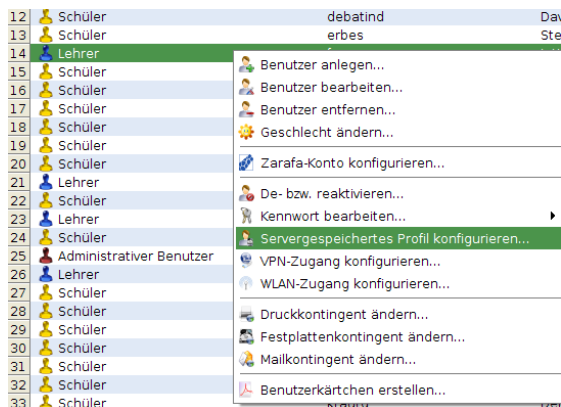


Abbildung III.4.9. Servergespeichertes Profil nach Anpassung in `service.conf` über LogoDIDACT-Console aktivierbar

Im zweiten Dialog setzt man zur Aktivierung des servergespeicherten Profile einfach das entsprechende Häkchen.

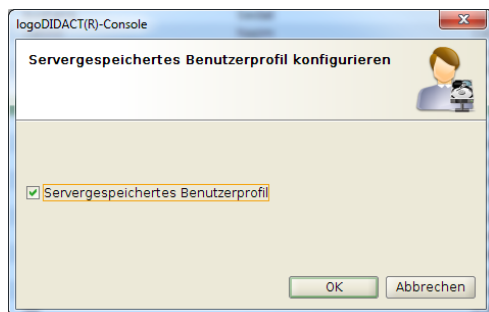


Abbildung III.4.10. Servergespeichertes Profil für einen Benutzer aktivieren

Im Homverzeichnis des Nutzers wird dann beim nächsten An- und Abmelden im Unterordner `Profile` ein Ordner für das Windows-Profil erstellt. Bei Windows XP heisst dieser Ordner einfach `Windows`, bei Windows 7 heisst er `Windows.v2`.

III.4.12.2. Kennwörter

Beim massenweisen Anlegen von Benutzern über die Impotfunktion in der LogoDIDACT-Console werden per Standardeinstellung ausreichend komplexe und dennoch leicht zu merkende Kennwörter generiert. Bei vielen Schulen hat es sich bewährt, den Schülern das Ändern dieser "guten" Kennwörter gar nicht zu erlauben. Solche Einstellungen lassen sich in der LogoDIDACT-Console pro Benutzer oder auch pro Klasse ändern (siehe Abschnitt VI.2.4.4, „Kennwortrichtlinien in der LogoDIDACT-Console ändern“). Nicht ändern lässt sich dort allerdings, wie komplex das Passwort ist, d.h. wie viele Zeichen, Sonderzeichen oder welche Länge das Passwort haben darf oder haben muss.

III.4.12.2.1. Komplexität für generierte Kennwörter

Erfahrungsgemäß haben zu komplexe Kennwortrichtlinien oft einen gegenteiligen Effekt und machen das System unsicher, da die Kennwörter überall notiert werden. Dem Administrator oder den Lehrerinnen und Lehrern bereitet das ständige Zurücksetzen vergessener Kennwörter unnötig viel Arbeit. Dennoch ist es möglich, die Standardrichtlinie, die eine Kennwortlänge von 5 Zeichen verlangt, zu verändern. Auch diese Anpassung ist am Server in der Datei `/etc/logodidact/user.conf` im Abschnitt `[Role]` möglich.

Die Standardvorgabe `phonemic(5)` liefert dabei ein aussprechbares Kennwort, das aus 2 Silben mit je 2 Kleinbuchstaben besteht, gefolgt von einer Zahl, also z.B. `rubu4` oder `kose2`.

```
[Role]
...
Password ${phonemic(5)}
...
```

Für Umgebungen, in denen Dienste auch von außen zugänglich sind oder eine Cloud-Ankopplung erfolgt, sollten entsprechend komplexere Kennwörter gebildet werden. Denkbar ist z.B. eine Anpassung bestehend aus zwei durch ein Sonderzeichen (im Beispiel ein Doppelpunkt) getrennte phonemische Blöcke:

```
[Role]
...
Password ${phonemic(5)}:${phonemic(5)}
...
```

Da die Vorgabe `phonemic(5)` aber nur Kleinbuchstaben liefert und viele Portale neben der Mindestlänge, einer Zahl, und einem Sonderzeichen auch einen Großbuchstaben verlangen, ist folgende Anpassung möglich:

```
[Role]
...
# Kennwort beginnend mit Großbuchstaben "BS" und Sonderzeichen ":"
# gefolgt von einem aussprechbaren Wort wie z.B. "rubu4" aus
# 4 Buchstaben und einer Zahl
Password BS:${phonemic(5)}

# Zufalls-Kennwort bestehend aus 8 Zeichen alle in Kleinbuchstaben,
# jedoch nicht über Silben aussprechbar, gefolgt von einer Zahl am Ende.
Password ${random(8)}
...
```

Damit die Änderung übernommen wird, muss der Serverprozess im **Logosrv** neu gestartet werden:

ldserver restart



Achtung

Die obige Festlegung der Komplexität für Kennwörter greift ausschließlich in zwei Situationen. Die Richtlinie findet Anwendung, wenn ein Benutzer neu angelegt und das Kennwort erstellt wird oder wenn Sie es das Kennwort über die LogoDIDACT Console neu vergeben.

Diese Richtlinie hat nichts damit zu tun, welches Kennwort sich ein Benutzer geben kann, wenn er es selbst z.B. vom Windows Client aus ändert (sofern er es darf).

III.4.12.2.2. Kennwort für alle Schüler neu generieren

Will oder muss man für alle Schüler neue Kennwörter vergeben, so ist dies über den folgenden Befehl auf Kommandozeile möglich:

```
for user in $(students); do ldapass -i $user -; done
```

III.4.12.2.3. Kennwort bei mehrmaliger Falscheingabe sperren

Soll das Kennwort bei mehrfacher Falscheingabe gesperrt werden, so ist das über das Samba-Tool `pdbedit` (Password Database) aktivierbar. Der Parameter `C` bestimmt dabei die Anzahl Fehlversuche für die Eingabe des Kennwort. Der dazugehörige Wert beträgt im folgendem Beispiel 3, d.h. nach der dritten Fehleingabe wird das Konto gesperrt:

```
pdbedit -P "bad lockout attempt" -C 3
```

Weitere Optionen von `pdbedit` finden sich unter http://www.linuxcommand.org/man_pages/pdbedit8.html.

III.4.13. Log-Dateien

Im Hinblick auf das Thema Datenschutz ist es wichtig zu wissen, wo und wie lange Benutzerspezifische Informationen im System gespeichert werden. Nahezu jeder Prozess oder Dienst in LogoDIDACT speichert Informationen über sein Verhalten in so genannten LOG-Dateien.

Log-Dateien liegen in LogoDIDACT im Verzeichnis `/var/log/`, wie z.B. die Datei `user.log` oder `dhcp.log`.

III.4.13.1. Rotieren und Komprimieren von Log-Dateien

Damit Log-Dateien nicht unkontrolliert groß werden und eventuell das System lahm legen, werden diese mit `logrotate` rotiert. Zudem lassen sich kleinere Log-Dateien wesentlich schneller durchsuchen, was die Fehlersuche vereinfacht. Alte Log-Dateien können dabei komprimiert werden, was in LogoDIDACT auch der Normalfall ist. Wie Log-Dateien dabei behandelt werden, lässt sich für jeden Dienst separat konfigurieren und anpassen.

Für Pakete erfolgt die Konfiguration in der jeweiligen Datei innerhalb des Verzeichnisses `/etc/logrotate.d/`. Am Beispiel des Imagingsystems `rembo` werden demnach Log-Dateien wöchentlich (*weekly*) rotiert. Der Parameter bestimmt damit in welchem Intervall eine neue Log-Datei angelegt wird. Ohne weitere spezielle Parameter wird eine Log-Datei dabei zunächst umbenannt und eine neue Log-Datei wird angelegt. Wenn das zu Problemen führt, kann man mit dem Parameter *copytruncate* auch zuerst eine Kopie der Log-Datei erstellen und dann die originale Log-Datei "abschneiden". Der Parameter *rotate 5* legt dabei fest, wie viele Versionen an Log-Dateien vorgehalten werden (Rotationszyklus), bevor die älteste Version überschrieben wird. Die Logdateien werden zudem beim Rotieren komprimiert (*compress*):

```
/usr/lib/rembo5/files/logs/*.log {
rotate 5
weekly
olddir archive
dateext
missingok
compress
delaycompress
sharedscripts
}
```

Mit der aktuellen Log-Datei und den 5 komprimierten Versionen hat man somit Log-Informationen über 5 bis 6 Wochen.

Komprimierte Log-Dateien werden nicht in die Datensicherung mit einbezogen (siehe Abschnitt III.2.1.4, „Dateien, die nicht gesichert werden“).

III.4.14. Radius-Server

Im Container `logosrv` läuft per Standardkonfiguration automatisch auch ein Radius-Server. Sollte der Radius-Server nicht installiert sein, lässt sich das über folgenden Befehl im Container `logosrv` erreichen:

```
apt-get install ld-radius-server
```

Für die Ankopplung eines WLAN-Controllers, wie z.B. Unifi, wird im Wesentlichen der Sicherheitsschlüssel des Radius-Servers benötigt. Dieser findet sich ebenfalls im Container `logosrv` in der Datei `/etc/radius.secret`.

Kapitel III.5. Softwareverteilung mit LD Deploy

Für die Softwareverteilung wurde in LogoDIDACT viele Jahre lang Rembo/mySHN® eingesetzt. Im Laufe der Zeit ergaben sich aber neue Herausforderungen, die mit dem bisherigen System und speziell dem Rembo-Kern nicht mehr zu lösen waren.

Mit der Eigenentwicklung der Komponente **LD Deploy** und der Freigabe in 2018 wurden nicht nur die aufgelaufenen Probleme der Vergangenheit gelöst, sondern jede Menge neue Technologien und Konzepte genutzt, um die Verteilung von Software noch einfacher, schneller und zuverlässiger zu machen.

III.5.1. Vorteile von LD Deploy

Die Vorteile von **LD Deploy** im Überblick:

- BIOS und UEFI Support
- Optimale Hardware Unterstützung auf PXE-Ebene (USB- Maus & Tastatur, Festplattengeschwindigkeit, Netzwerkdurchsatz)
- Unterstützung aller Windows 10 Versionen
- Schnellere und dezentrale Verteilung mittels Torrent
- Zentrale Steuerung über Webinterface im Control Center
- Imageerstellung unter Windows über Menü
- Automatischer und individueller Domänenbeitritt
- Einfachere Produktaktivierung über Microsoft KMS
- Background-Deployment unter Windows
- WLAN Imaging

III.5.2. Voraussetzungen und Einschränkungen

Hier sind die aktuellen Voraussetzungen (Stand 8/2020) und bekannten Einschränkungen sowohl für die Installation von **LD Deploy** auf Serverseite als auch für die Nutzung innerhalb einer bestimmten Netzwerkkumgebung aufgeführt:

III.5.2.1. Voraussetzungen

- Ubuntu 16.04 LTS (gegebenenfalls Aktualisierung entsprechend Handbuch durchführen)
- Aufgebauter Container **samba4-ad**
- Puppet Rezeptstand 1.1.34 oder höher

Gegebenenfalls im Container **puppeteer** die Aktualisierung per **ldupdate** durchführen

- Aufgebauter Container **ca-g1** (Certificate Authority - kurz CA = Zertifizierungsstelle)

Dieser Container wird über den Puppet-Rezeptstand ab 1.1.15 automatisch aufgebaut. Zwischen CA und den Containern sind mehrere **prun** notwendig, bis die Zertifikate auf allen Seiten vorhanden sind.

III.5.2.2. Einschränkungen

- **LD Deploy** unterstützt Windows 10 in 64 Bit (**keine 32 Bit**-Unterstützung!)
Windows 7 kann weiterhin mit Rembo/mySHN® betrieben werden.
- Bitte keinen Virenschanner installieren, da die diversen Clientkomponenten noch nicht signiert sind und ggf. blockiert werden.
- **LD Deploy** unterstützt kein SecureBoot und keine Verschlüsselung mit BitLocker.
- Seit Windows 10 Version 1903 gibt es diverse Bugs in Windows hinsichtlich der Ansteuerung und Konfiguration von Druckern, sowohl im AuditMode (Sysprep-Phase) als auch im normalen Betriebsmodus. Diese Bugs in Windows 10 können zu seltsamen Effekten führen, wie z.B. Fehlern beim Ausdruck einer Testseite im AuditMode.

III.5.2.3. Dringende Empfehlungen

In den beiden folgenden Punkten geht es um Funktionen und Technologien, die möglicherweise in Ausnahmefällen und bei hinreichend Know-how auf Seiten des Kunden und des Partners funktionieren. Wir raten aber grundsätzlich vom Einsatz dieser Funktionen vor allem in einer pädagogischen Netzwerkumgebung mit Hunderten Benutzern und Rechnern ab und leisten dafür keinen Support:

- Verzichten Sie auf die Verwendung von Gruppenrichtlinien
- Verzichten Sie auf die Verwendung von servergespeicherten Profilen

Die Anpassungen, die über Gruppenrichtlinien möglich sind, werden in **LD Deploy** über **AutoConf** umgesetzt. Einzig für die Herstellung der Netzlaufwerke wird eine Gruppenrichtlinie bereitgestellt.

III.5.3. Parallelbetrieb von LD Deploy und Rembo/mySHN®

Mit **LD Deploy** wird ausschließlich Windows 10 unterstützt, was primär daran liegt, dass Technologien genutzt werden, die es unter Windows 7 nicht gibt. Sie sind jedoch nicht gezwungen, alle alten Windows 7 Clients auf Windows 10 umzustellen, sondern können diese weiterhin mit Rembo/mySHN® betreiben.

Die Entscheidung, ob sich ein Rechner über den Netzwerkboot zu **LD Deploy** oder Rembo/mySHN® verbindet, wird auf der DHCP-Ebene getroffen.



Achtung

Unabhängig davon, ob man Rembo tatsächlich noch parallel zu **LD Deploy** betreiben möchte, muss der Container **rembo5** noch laufen und darf in keinem Fall entfernt werden.

Abhängig davon, was für eine Installation man durchführt, gibt es zwei verschiedene Möglichkeiten, das Standard-Imagingsystem festzulegen.

III.5.3.1. Neuinstallationen nur mit LD Deploy

Bei einer LogoDIDACTNeuinstallation ist es verbindlich und ebenso sinnvoll ausschließlich das neue Modul **LD Deploy** zur Verteilung von Software und zum Schutz der Rechner zu verwenden. Damit lassen sich neue PCs, Notebook und auch Windows Tablets mit einem topaktuellen Windows 10 in der Version 1909 oder höher betreiben.

Es gibt daher keinen wirklichen Parallelbetrieb mit Rembo, wenngleich der Container noch laufen muss!

In diesem Szenario muss **LD Deploy** als Standard Imaging-System festgelegt werden. Wechseln Sie dazu in den Puppet-Container und in das entsprechende Verzeichnis `/etc/logodidact/hiera`.

```
lxc-ssh -n puppeteer
```

```
cd /etc/logodidact/hiera
```

Prüfen Sie, ob es in dem Verzeichnis bereits eine Datei `custom.yaml` gibt. Falls diese **nicht** existiert, gibt es in der vorliegenden Umgebung keine kundenspezifische Anpassungen und Sie können die Anpassung für die Paketquellen gefahrlos herunterladen:

```
wget https://files.sbe.de/ld-deploy/custom.yaml
```

Öffnen Sie die Datei `custom.yaml` mit einem Editor Ihrer Wahl und entfernen Sie dort das Kommentarzeichen in der Zeile, so dass der folgende Eintrag aktiv geschaltet wird:

```
ld_legacy::dhcp::lddeploy_enabled: true
```

Wechseln Sie auf die passende Verzeichnisebene und tragen Sie Ihre Änderungen im Versionsverwaltungssystem git ein:

```
cd /etc/logodidact
```

```
git add .
```

```
git commit -m "aktiviere LD Deploy als Standard-Imagingsystem"
```

Das Management-System Puppet entfernt daraufhin im Wesentlichen die für Rembo/mySHN® notwendigen Einträge in der DHCP-Konfiguration.

III.5.3.2. Ergänzung bestehender Rembo-Installationen mit LD Deploy

Für Bestandskunden, die bisher Rembo/mySHN® verwenden, besteht die Möglichkeit neue oder auch vorhandene Geräte auf **LD Deploy** umstellen. Alte Geräte, die noch mit Rembo/mySHN® z.B. unter Windows 7 laufen müssen nicht sofort entsorgt werden, sondern können wie bisher weiterbetrieben werden.

In diesem Szenario ist also ein sanfter Umstieg auf Windows 10 mit **LD Deploy** möglich. In vielen Fällen ergibt sich dieses Szenario konkret dann, wenn z.B. die Hardware eines EDV-Raumes erneuert wird aber eben keinesfalls alle Rechner und oder Notebooks einer Schule. Das gleiche gilt, wenn z.B. Windows-Tablets beschafft wurden oder werden. Diese können jetzt mit **LD Deploy** betrieben werden.

In dieser Konstellation bleibt Rembo/mySHN® deshalb für die Altgeräte das Default-Imaging-System. Ob das so ist, wird über die Optionen in der DHCP-Serverkonfiguration bestimmt.

Das ist der Fall, wenn die folgenden beiden Zeilen im Container **logosrv** in der Datei `/etc/dhcp3/template/dhcpd.conf.logodidact` vorhanden sind:

```
option vendor-class-identifizier "PXECient";  
include "/etc/dhcp3/options/default.conf";
```

Damit sich neue Clients gezielt zum neuen **LD Deploy** verbinden, muss im ersten Schritt eine passende DHCP-Konfiguration erstellt werden. Gehen Sie dazu im Container **logosrv** in das Verzeichnis `/etc/dhcp3/options` und erstellen Sie einfach die Datei `lddeploy.conf`:

nano lddeploy.conf

Fügen Sie die folgende Zeile ein und speichern Sie die Datei ab.

```
option vendor-class-identifizier "";
option vendor-encapsulated-options "";
```

Für alte Clients ist es notwendig eine entsprechende Konfiguration für **rembo5** zu erstellen. Wechseln Sie dazu im Container **Logosrv** in das Verzeichnis `/etc/dhcp3/options`. Dort gibt es eine durch Puppet verwaltete Datei `r5.conf`. In dieser Datei ist die IP-Adresse des Rembo-Servers als HEX-Wert im Parameter `vendor-encapsulated-options` kodiert. Im Standardfall ist das die IP-Adresse `172.28.28.16` (= `ac:1c:1c:10` in HEX).

Kopieren Sie diese Datei wie folgt:

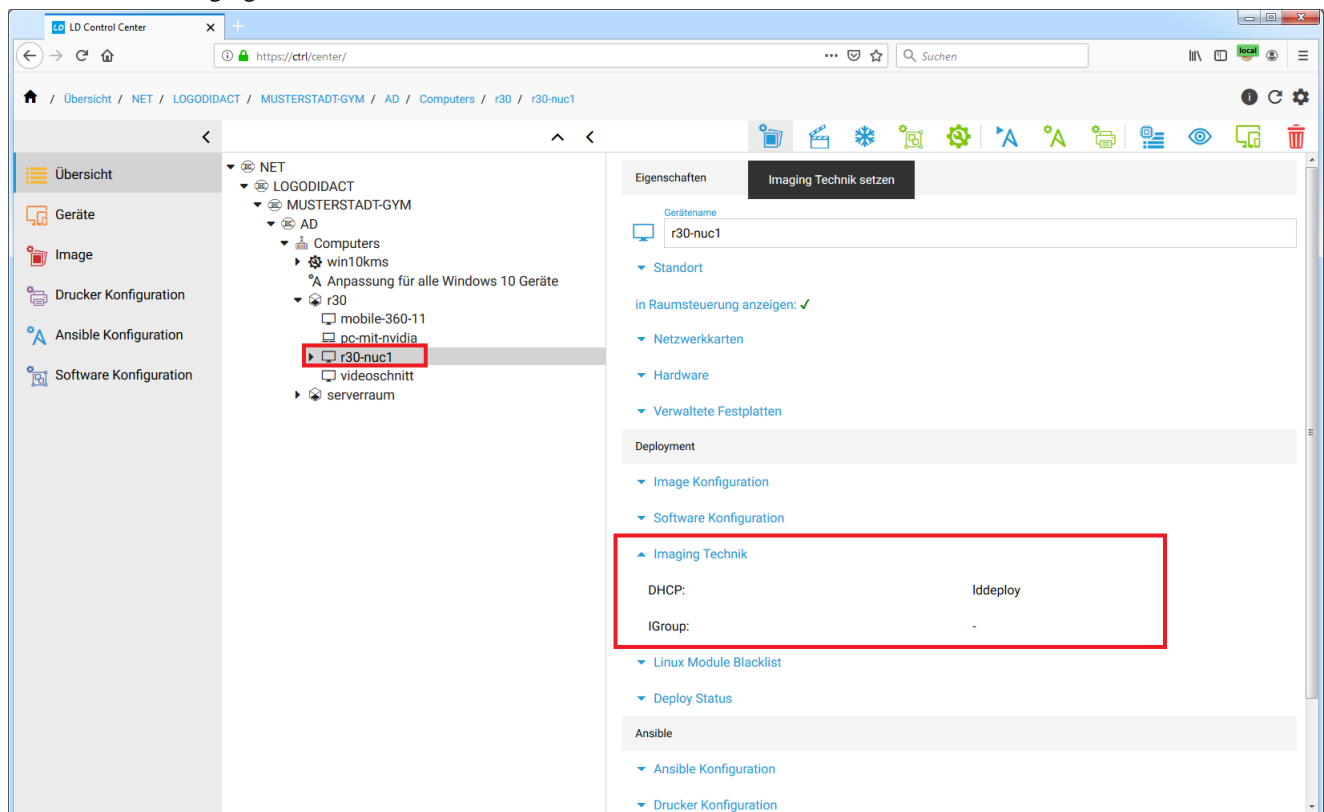
cp r5.conf rembo5.conf

Ergänzen Sie die Datei anschließend noch um den Eintrag in Zeile 1 und speichern Sie diese ab.

```
option vendor-class-identifizier "PXECClient";
option vendor-encapsulated-options 06:01:07:08: ...
```

Ob sich ein Client dann zum alten Rembo-Server verbindet oder zum neuen LD Deploy-Server wird über den DHCP-Server geregelt, bzw. die Option "tag 43", die der DHCP-Server einem Client mitgibt.

Diese Zuweisung kann im Control Center pro Rechner oder Rechnergruppe festgelegt werden über den Parameter Imaging-Technik.



III.5.4. Installation von LD Deploy

Die Installation von **LD Deploy** besteht aus den vier Containern **ctrl-g1**, **postgresql10**, **deploy-g1** und **nexus-g1**. Diese werden wieder auf die gleiche Weise aktiviert und konfiguriert, wie das bereits bei den Bausteinen zuvor gezeigt wurde.

Wechseln Sie in den Puppeteer:

```
lxc-ssh -n puppeteer
```

Wechseln Sie in das Verzeichnis zur Aktivierung von Containern:

```
cd /etc/logodidact/hosts/ldhost
```

Öffnen Sie die Datei `guest.conf` mit einem Editor Ihrer Wahl, wie z.B. Nano:

```
nano guest.conf
```

Fügen Sie dort die Einträge für die vier Container hinzu:

```
[Guest ctrl-g1]  
Ensure running
```

```
[Guest postgresql10]  
Ensure running
```

```
[Guest deploy-g1]  
Ensure running
```

```
[Guest nexus-g1]  
Ensure running
```

Durch Eingabe der Tastenkombination `<Strg>+<X>` verlassen Sie den Editor Nano und geben „Y“ ein, damit die Änderung gespeichert wird. Wechseln Sie dann ins Stammverzeichnis der Konfiguration und übertragen Sie anschließend die Änderungen ins Versionierungssystem git:

```
cd /etc/logodidact
```

```
git add .
```

```
git commit -m "Aktivierung der 4 Container für LD Deploy"
```

Analog zu der bisherigen Vorgehensweise wird der Aufbau der Container durch einen **prun** im `ldhost` angestoßen. Über **pstat** im Puppeteer kann man den Installationsverlauf wieder beobachten und die Durchläufe in den drei Containern durch gezielte Aufrufe von **prun** beschleunigen.

Agent State	Catalog State	Node	Successes	Noops	Skips	Failures	Last run
Deactivated		audit					
Waiting	OK	ca-gl.schule.local	6				2 minutes ago
Deactivated		collabora-gl					
Running	OK	ctrl-gl.schule.local	146		2		4 minutes ago
Running	OK	deploy-gl.schule.local	146		2		4 minutes ago
Deactivated		icinga2					
Deactivated		kopano-gl					
Waiting	OK	ldhost.schule.local	34				6 minutes ago
Waiting	OK	ldmobile.schule.local	6				1 minute ago
Unknown	OK	logosrv					a long while ago
Deactivated		moodle30					
Waiting	OK	mysql56.schule.local	4				3 minutes ago
Deactivated		nextcloud-gl					
Running	OK	postgresql10.schule.local	146		2		4 minutes ago
Waiting	OK	puppeteer.schule.local					7 minutes ago
Deactivated		pydio					
Waiting	OK	rembo5.schule.local	5				1 minute ago
Waiting	OK	rev-proxy.schule.local	6				3 minutes ago
Waiting	OK	samba4-ad.schule.local	6				2 minutes ago
Waiting	OK	unifi.schule.local					7 minutes ago
Deactivated		xiboi7					

Press 'l'-'9' to change update interval. Press 'q' to quit.

Sobald alle Container vollständig aufgebaut sind, können Sie mit der Bereitstellung des Windows 10 Images beginnen.

III.5.5. Freigegebene und Entwickler-Pakete

III.5.5.1. Offizielle Pakete

Über die offiziellen Paketquellen, werden alle für **LD Deploy** notwendigen Debian-Pakete aus dem jeweiligen "stable release" geladen und installiert. Für den Test neuer Funktionen oder auch die Behebung von Fehlern kann es auch neuere Debian-Pakete geben, die in Abstimmung mit dem Support eines LogoDIDACT-Partners eingespielt werden können.

Im Folgenden eine Auflistung der offiziellen Pakete mit einer Kurzbeschreibung, dem Versionsstand und dem Container, in dem diese installiert werden.

Um sich beispielsweise 5 relevante Pakete im Container **deploy-g1** anzeigen zu lassen, kann man das über **dpkg -l ld-d*** tun.

Paketname:	Datum:	Container:	Beschreibung:
ld-deploy-linpe_31~200320.173113_all.deb	20.03.20	deploy-g1	LD Deploy linpe-Komponente mit Linux Fedora 31 und Kernel 5.x
ld-deploy-winpe_1903~191125.083045_all.deb	25.11.19	deploy-g1	LD Deploy winpe-Komponente
ld-deploy-agent_70.4_all.deb	22.07.20	deploy-g1	LD Deploy Kernsoftware am Client (sowohl in PXE als auch Windows)
ld-deploy-windows-qbittorrent_4.2.0.0~2_all.deb	28.01.19	deploy-g1	qbittorrent Client
ld-deploy-ipxe_1.0.0~200703.003505_all.deb	03.07.20	deploy-g1	Open Source Boot Firmware
ld-control-service_42.4_amd64.deb	23.06.20	ctrl-g1	Controller-Logik Server/Client
ld-control-center_41.8_all.deb	25.06.20	ctrl-g1	Control Center graphische Oberfläche
ld-control-client_13_amd64.deb	22.05.20	ctrl-g1	Kommunikationsdienst auf Serverseite in deploy-g1, ctrl-g1 und postgresql10

Paketname:	Datum:	Container:	Beschreibung:
ld-control-client_13_i386.deb	22.05.20	logosrv	Kommunikationsdienst auf Serverseite im logosrv
ld-deploy-windows-tools_11_i386.deb	05.12.19	logosrv	Tools für Anpassungen (Drucker, WLAN, Gruppenrichtlinien, KMS, KVM)
ld-nexus-upload_3_all.deb	19.12.19	nexus-gl	Upload von Paketen in Nexus
ld-choco-install_4_all.deb	18.12.19	nexus-gl	Chocolatey Client
ld-sysinternals_2019.12.11~1_all.deb	18.12.19	nexus-gl	Tools für Clientanpassungen per Ansible
ld-vc-redis_14.24.28127.4~1_all.deb	18.12.19	nexus-gl	Tools für Clientanpassungen per Ansible

III.5.5.2. Entwickler-Pakete für Testzwecke

Sowohl für die Problembehandlung in Fehlerfällen als auch den Test von Weiterentwicklungen ist es möglich, gezielt einzelne Debian-Pakete in **LD Deploy** zu aktualisieren. Da der Baustein aber nicht unabhängig vom Puppet-Versionsstand betrachtet werden kann, ist gegebenenfalls auch dafür ein Paket explizit einzuspielen.



Achtung

SBE stellt diese Pakete nur gezielt einzelnen Partnern und Endkunden für Tests von Funktionen oder zur Beseitigung von Problemen zur Verfügung. Bitte spielen Sie diese Pakete nicht grundlos ein, auch wenn diese vorhanden und neuer sind, als die Pakete der Paketquelle bzw. des aktuellen Repositories!

III.5.5.2.1. LD Deploy Entwicklerpakete

Um solche Pakete gezielt einzuspielen, wechseln Sie in den Puppet-Container und dort in das zum Paket passenden Verzeichnis:

```
lxc-ssh -n puppeteer
```

```
cd /srv/repos/xenia1
```

Die zu ladenden Pakete für Testzwecke liegen im Pfad `https://files.sbe.de/ld-deploy/beta` und können über folgenden Befehl geladen werden:

```
wget https://files.sbe.de/ld-deploy/beta/PAKETNAME.deb .
```

Prüfen Sie anschließend, ob die Debian-Pakete die richtigen Rechte und Besitzverhältnisse haben und ändern Sie diese gegebenenfalls:

```
chown root:root *
```

```
chmod 0644 *
```

Sollte es Aktualisierungen der Pakete für den Container logosrv geben, müssen diese vom Ordner xenial nach hardy verschoben werden:

```
mv ld-control-client_X_i386.deb /srv/repos/hardy/
```

```
mv ld-deploy-windows-tools_X_all.deb /srv/repos/hardy/
```

Der nächste Schritt besteht darin, das Repository in Puppet aufzubauen:

```
puppet-repo-build
```

Die Aktualisierung der Pakete in den jeweiligen Containern ist nachfolgend beschrieben. Sollte sich ein Paket trotzdem nicht aktualisieren, kann es notwendig sein, den repo-Cache zu löschen und nochmals komplett neu aufbauen zu lassen.

```
cd /var/cache/repos
```

```
rm *.db
```

```
puppet-repo-build
```

III.5.5.2.2. Puppet Entwicklerpakete

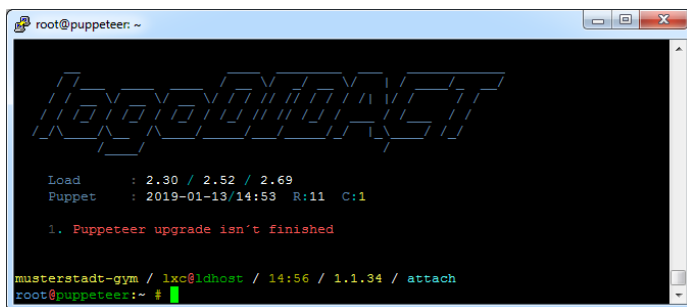
Um Puppet selbst zu aktualisieren, wird das entsprechende Debian-Paket über den gleichen Mechanismus wie oben beschrieben geladen. Zusätzlich muss das Paket im Puppeteer selbst explizit installiert werden.

```
dpkg -i ld-puppet10_1.1.35_all.deb
```

```
cd /root/p/update.d
```

```
./update
```

Bitte beachten Sie unbedingt, dass das Upgrade von Puppet relativ lange dauern kann. Sie sehen das, wenn Sie den Container verlassen und sich erneut einwählen.



Während diese Upgradephase funktioniert auch das Tool **pstat** nicht bzw. liefert nicht die gewohnte Ausgabe. Ab und an kann es dabei vorkommen, dass die Puppet-Datenbank aus nicht näher bekannten Gründen nicht mehr läuft und neu gestartet werden muss:

```
service puppetdb restart
```

Ob das der Fall ist, sieht man beispielsweise über **htop** und etwas mehr als einem Dutzend vordefinierter Datenbankverbindungen von puppetdb. Wenn diese vorhanden sind, ist alles in Ordnung.

III.5.6. Aktualisierung von LD Deploy Paketen

Durch die Einbindung zusätzlicher Paketquellen werden neue Pakete für die Container **ctrl-g1**, **postgres10** und **deploy-g1** über den normalen Updatemechanismus aktualisiert. Wechseln Sie in den Container **puppeteer** und starten Sie die Aktualisierung über den Befehl **ldupdate**:

```
lxc-ssh -n puppeteer
```

```
ldupdate
```

Den gleichen Vorgang führen Sie im Container **logosrv** durch:

```
lxc-ssh -n logosrv
```

```
ldupdate
```

Die Aktualisierung der Pakete in den Containern lässt sich gezielt über den Befehl **prun** beschleunigen. Hierbei sollte man jedoch warten, bis die Updates im Container **puppeteer** durchgelaufen sind.

```
lxc-ssh -n ctrl-g1
```

Sofern im Puppeteer zusätzliche individuelle Pakete in `/srv/repos/xenial` bereitgestellt und ein lokales Repository aufgebaut wurde (siehe oben), müssen diese Pakete in den jeweiligen Containern auch explizit installiert werden:

```
apt update ; apt -y upgrade
```

```
prun
```

Das Gleiche Vorgehen gilt für den Container **deploy-g1**:

```
lxc-ssh -n deploy-g1
```

```
apt update ; apt -y upgrade
```

```
prun
```



Tipp

Um zu prüfen welche Version eines Paketes eingespielt ist, kann man folgenden Befehl nutzen

```
dpkg -l KOMPONENTE also konkret z.B.
```

```
dpkg -l ld-control-client (im Container logosrv)
```

III.5.7. Windows 10 bereitstellen

Die Softwareverteilung mittels **LD Deploy** unterstützt ausschließlich die Version Windows 10. Das Vorgehen bei der Installation von Windows 10 auf den Clients ist ähnlich wie bisher und erfolgt ausschließlich über die Bereitstellung einer ISO-Datei bzw. der darin befindlichen Datei `install.wim` am Server als Ausgangsbasis.

Neu ist dabei, dass **LD Deploy** die aktuellste Windows 10 Version 1909 unterstützt und auch alle künftigen neuen Releases in der 64 Bit Ausführung unterstützen wird. Aufgrund der normalen Ausstattung von 4 GB und mehr auf den Arbeitsstationen ist die 64 Bit-Version auch die sinnvollste Variante.

III.5.7.1. Die richtige Windows 10 Variante bereitstellen

Sobald alle notwendigen Container vollständig aufgebaut sind, kopieren Sie die Datei `install.wim` auf den Server.

Bitte beachten Sie, dass in einer `install.wim` in der Regel alle verschiedenen Windows 10 Varianten enthalten sind und der **LD Deploy** Client per Standard den ersten Eintrag aus einer `wim`-Datei verwendet.

Um Verwirrungen zu vermeiden, sollten Sie deshalb das System extrahieren, welches Sie tatsächlich lizenziert haben und einsetzen dürfen. Das ist in den meisten Fällen Windows 10 Professional.

III.5.7.1.1. Windows 10 Professional bereitstellen

Für die am häufigsten eingesetzte Variante Windows 10 Professional, können Sie eine bereits extrahierte `wim`-Datei herunterladen. Zum Herunterladen der Datei, wechseln Sie in den Container **deploy-g1** und dort in das Ziel-Verzeichnis für die Images:

```
lxc-ssh -n deploy-g1
```

```
cd /var/lib/deploy/qBittorrent/
```

Laden Sie die `wim`-Datei herunter und die dazu passende Prüfsummendatei:

```
wget https://files.sbe.de/ld-deploy/win10pro1909.wim
```

```
wget https://files.sbe.de/ld-deploy/win10pro1909_sha512sum.txt
```



Achtung

Überprüfen Sie über den folgenden Befehl, ob die Prüfsumme der heruntergeladenen `wim`-Datei mit der MD5-Prüfsummendatei übereinstimmt:

```
sha512sum -c win10pro1909_sha512sum.txt
```

Wenn die Prüfsumme nicht übereinstimmt, löschen Sie die `wim`-Datei und laden diese erneut herunter.

Sofern die `wim`-Datei vollständig heruntergeladen wurde (Ausgabe `win10pro1909.wim: OK`), können Sie mit dem Importieren fortfahren, wie in Abschnitt III.5.7.2, „Image importieren“ beschrieben.

III.5.7.1.2. Spezielle Windows 10 Version bereitstellen

Um eine andere Variante von Windows 10 zu extrahieren (z.B. Education), nutzen Sie das in Windows 10 eingebauten Tool **dism**.



Achtung

Das Anzeigen und Extrahieren über die im Folgenden aufgeführten Befehle funktioniert nur unter Windows 10.

Ausgehend von einer Datei `Windows10.iso` ist das Vorgehen auf einem Rechner mit Windows 10 wie folgt:

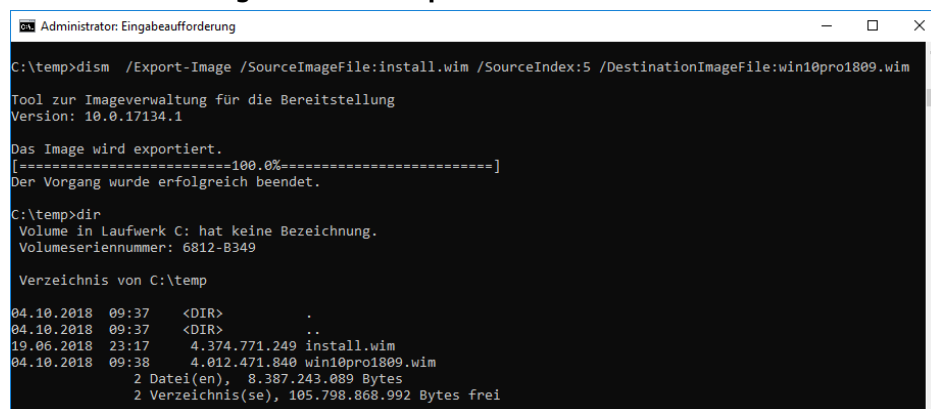
1. Entpacken Sie die ISO-Datei mit den Bordmitteln unter Windows 10 z.B. in den Ordner `C:\Windows10`.
2. Navigieren Sie in den Ordner `C:\Windows10\sources`.
3. Öffnen Sie eine Kommandozeile und listen Sie alle Systeme auf

```
dism /Get-WimInfo /WimFile:install.wim
```

Notieren Sie sich die Nummer des gewünschten Systems (z.B. Index 5 für Windows 10 Pro)

4. Exportieren Sie eine `wim`-Datei, welches nur das von Ihnen gewünschte System enthält. Der entscheidende Parameter ist dabei **SourceIndex**:

```
dism /Export-Image /SourceImageFile:install.wim /SourceIndex:5 /DestinationImageFile:win10pro1909.wim
```



```
Administrator: Eingabeaufforderung
C:\temp>dism /Export-Image /SourceImageFile:install.wim /SourceIndex:5 /DestinationImageFile:win10pro1809.wim
Tool zur Imageverwaltung für die Bereitstellung
Version: 10.0.17134.1
Das Image wird exportiert.
[=====100.0%=====]
Der Vorgang wurde erfolgreich beendet.
C:\temp>dir
Volume in Laufwerk C: hat keine Bezeichnung.
Volumeseriennummer: 6812-B349

Verzeichnis von C:\temp

04.10.2018  09:37  <DIR>          .
04.10.2018  09:37  <DIR>          ..
19.06.2018  23:17      4.374.771.249  install.wim
04.10.2018  09:38      4.012.471.840  win10pro1809.wim
                2 Datei(en),  8.387.243.089 Bytes
                2 Verzeichnis(se), 105.798.868.992 Bytes frei
```

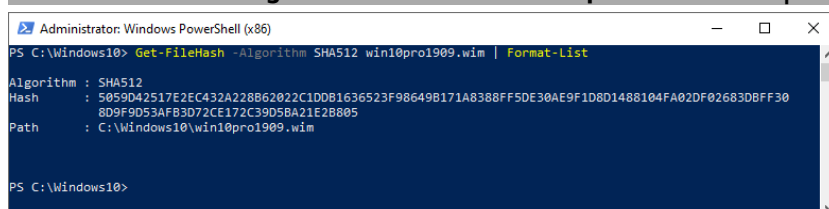
5. Sollte sich in der `iso`-Datei keine `install.wim`, sondern eine `install.esd` befinden, so ist diese lediglich komprimiert, so dass der Befehl beim Extrahieren des richtigen Systems etwas anders aussieht:

```
dism /Export-Image /SourceImageFile:install.esd /SourceIndex:5 /DestinationImageFile:win10pro1909.wim /Compress:max /CheckIntegrity
```

Diese Installationsdatei ist damit Ihr Ausgangssystem für die weiteren Schritte.

Wenn Sie die `wim`-Dateien auf eigenen Servern zum Download bereitstellen wollen, sollten Sie unbedingt mit Prüfsummen arbeiten. Über Powershell können Sie auch unter Windows 10 eine entsprechende Prüfsumme bilden und auf dem Zielsystem mit den entsprechenden Tools gegenprüfen:

```
Get-FileHash -Algorithm SHA512 win10pro1909.wim | Format-List
```



```
Administrator: Windows PowerShell (x86)
PS C:\Windows10> Get-FileHash -Algorithm SHA512 win10pro1909.wim | Format-List
Algorithm : SHA512
Hash      : 5059042517E2EC432A228862022C1D081636523F986498171A8388FF5DE30AE9F1D801488104FA02DF02683DBFF30
           8D9F9D53AFB3D72CE172C39D5BA21E28805
Path      : C:\Windows10\win10pro1909.wim

PS C:\Windows10>
```

Im folgenden Beispiel befindet sich die Datei für das Betriebssystem Windows 10 auf einem USB-Stick und soll auf den Server in das passende Verzeichnis übertragen werden. Gehen Sie dazu an den Server in den lhost und geben den Befehl **blkid** ein. Stecken Sie danach den USB-Stick ein auf dem sich das ISO-Abbild befindet und geben Sie erneut **blkid** ein. Anhand der unterschiedlichen Ausgabe sollte auch der Laie erkennen, als welches Gerät (device) der USB-Stick erkannt wurde.

Mounten Sie den USB-Stick mit **mount /dev/sdb1 /mnt** wenn sdb1 ihr device ist. Wechseln Sie danach in das Ziel-Verzeichnis für die Images im Container **deploy-g1**:

```
cd /var/lib/lxc/deploy-g1/rootfs/var/lib/deploy/qBittorrent
```

Setzen Sie von hier aus den Kopierbefehl entsprechend der von Ihnen benannten Datei ab:

```
cp /mnt/win10pro1909.wim .
```

III.5.7.2. Image importieren

Für die Bereitstellung eines Windows 10 Images in Form einer wim-Datei müssen für Torrent noch entsprechende Metainfos generiert werden.

Wechseln Sie in den Container **deploy-g1**:

```
lxc-ssh -n deploy-g1
```

Wechseln Sie in den Ordner für die zu verteilenden Images:

```
cd /var/lib/deploy/qBittorrent/
```

Importieren Sie die entsprechende wim-Datei und vergeben Sie dabei einen Namen, der zum Inhalt des Images passt.

```
ld-control-client image add --description win10pro1909 --file win10pro1909.wim
```

Die wim-Datei wird in den Ordner **downloads** verschoben und sofern dieser noch nicht existiert wird er zuvor angelegt. Alle weiteren Schritte und Konfigurationsarbeiten erfolgen per Browser über das Control Center.



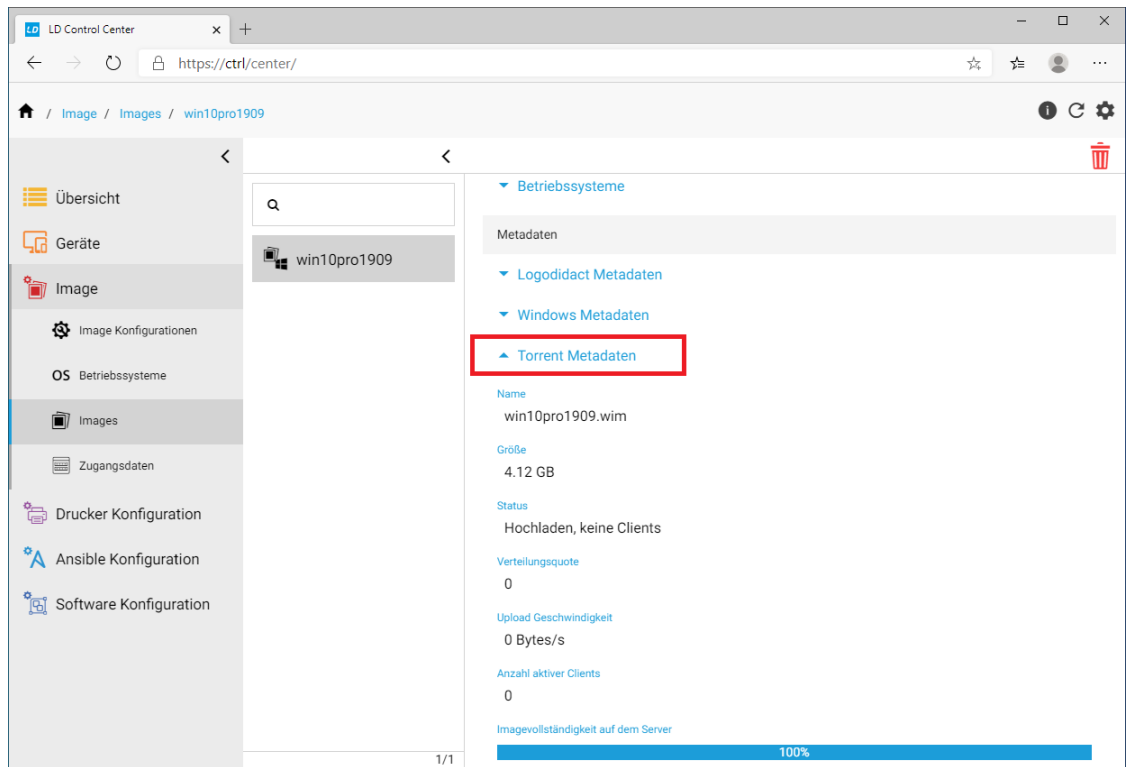
Tipp

Sie können jedes mit **LD Deploy** erstellte Image bzw. jede Installation auf diese Weise von einem Server A auf einen anderen Server B portieren.

III.5.7.3. Import eines Images prüfen

Beim Importieren eines Images bzw. dem Generieren der Torrent-Metainfos gibt es eine Phase der Überprüfung durch Torrent, der trotz korrektem Import in einer Art Endlosschleife hängen bleibt. Dies ist ein softwareseitiger Fehler in der Torrent-Implementierung, der von SBE an die Torrent-Entwickler gemeldet wurde (Sept. 2018).

Prüfen Sie unmittelbar nach dem Import im Control Center, ob das Image im Bereich **Torrent Informationen** 100% vollständig geladen wurde.



Wenn der Ladebalken bei 100% steht, ist alles okay und Sie brauchen nichts zu unternehmen. Wenn der Ladebalken über mehrere Minuten zwischen 0% und anderen Werten "springt", handelt es sich um die oben beschriebene Endlosschleife.

Deaktivieren Sie in diesem Fall auf dem Server im Container **deploy-g1** den Parameter zur Überprüfung durch Torrent.

```
lxc-ssh -n deploy-g1
```

Wechseln Sie in das Verzeichnis zur Konfiguration von Parametern:

```
cd /var/lib/lddeploy/qBittorrent/config/
```

Öffnen Sie die Datei `qBittorrent.conf` mit einem Editor Ihrer Wahl, wie z.B. Nano:

```
nano qBittorrent.conf
```

Setzen Sie den Parameter zur Überprüfung des Images auf **false** und speichern Sie die Änderung.

```
Advanced\RecheckOnCompletion = false
```



Tipp

Die Überprüfung eines Images ist grundsätzlich sinnvoll und wird bei jeder Imageerzeugung mit **LD Deploy** angewandt. Dafür dient genau der gerade geänderte Parameter.

Sie brauchen diesen Parameter nicht wieder auf **true** zu setzen, weil dies durch das Systemmanagement mittels Puppet automatisch gemacht wird.

Damit die Parameteränderung greift, muss der Dienst neu gestartet werden

systemctl restart qbittorrent-nox.service

III.5.7.4. Torrent Infos

Ein Bestandteil der **LD Deploy** Umgebung ist das Protokoll Torrent, das sich für die schnelle und effiziente Verteilung großer Datenmengen eignet. Die Verwendung ist beim so genannten FileSharing deshalb sehr verbreitet. Die Impelementierung, die in **LD Deploy** derzeit dafür eingesetzt wird, ist **qBittorrent**.

Das Webinterface von **qBittorrent** ist über folgende URL erreichbar:

<http://deploy:8080>



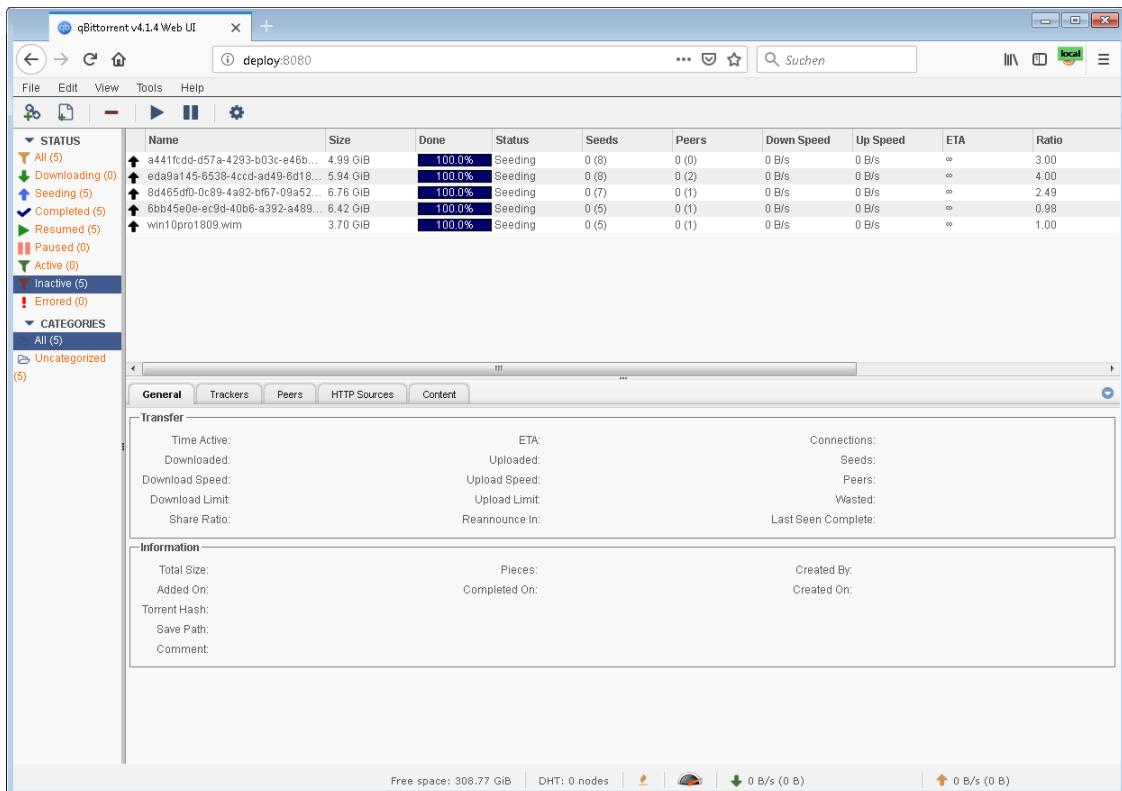
Achtung

Verwenden Sie auf keinen Fall die Browser InternetExplorer oder Edge!

Sie erhalten darüber fehlerhafte Anzeigen und absurde Darstellungen, die zu vollkommen falschen Schlussfolgerungen führen.

Nutzen Sie bitte die Browser Chrome oder Firefox.

Das Kennwort für den Benutzer **qadmin** findet sich im Container **ctrl-g1** unter `/etc/ld-control-service/application.properties`.

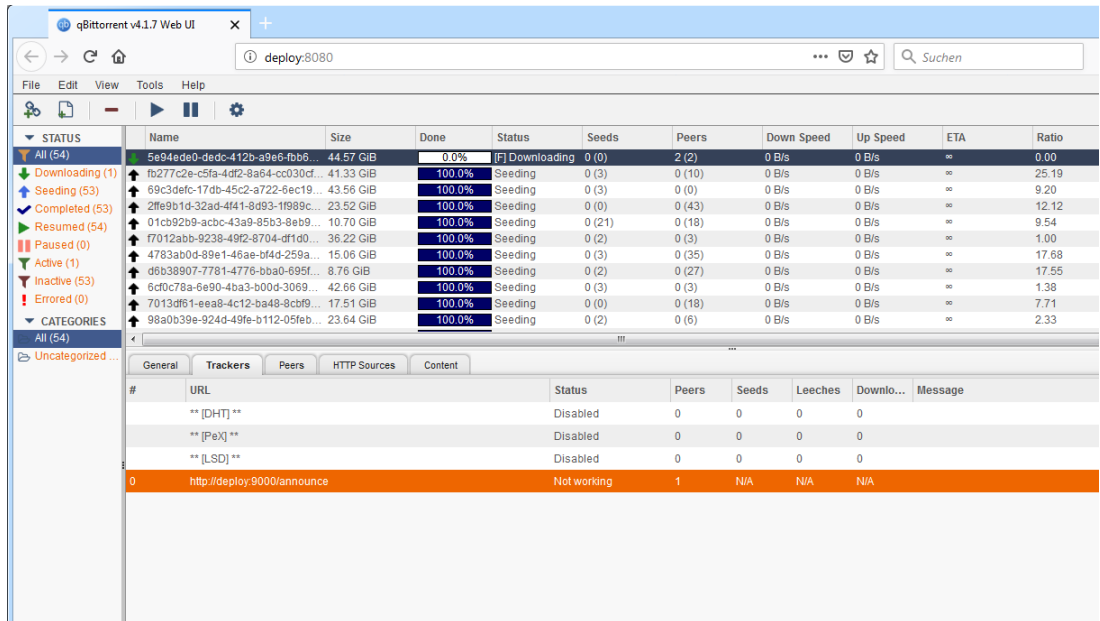




Achtung

Es besteht selten die Notwendigkeit in dieses Webinterface zu schauen und die darin enthaltenen Informationen über Seeder und Leacher sind sehr speziell und primär für den 3rd Level Support und die Softwareentwicklung von Interesse.

Wenn der Upload eines Images hängt oder Clients beim Download nicht fortfahren, kann dies am Tracker liegen, der gegebenenfalls nicht läuft. Der Tracker übernimmt die gesamte Koordination in der Verteilung von Dateien. Genaugenommen handelt es sich um zwei Tracker, die auf IPv4 und IPv6 laufen.



Sollte der Tracker nicht laufen, kann man versuchen diesen über das Webinterface neu zu starten. Eventuell ist es aber notwendig den gesamten qBittorrent-Service neu zu starten. Wechseln Sie dazu in den Container **deploy-g1** und geben Sie den folgenden Befehl **systemctl restart qbittorrent-nox.service** ein.

III.5.8. Das Control Center starten

Im Vergleich zu Rembo/mySHN ist das Softwareverteilungssystem **LD Deploy** deutlich flexibler und einfacher und die gesamte Konfiguration wird von zentraler Stelle aus per Webbrowser durchgeführt.

Das Control Center ist über einen Webbrowser erreichbar unter <https://ctrl>, wobei die Verwendung von Chrome empfohlen wird.. Noch schneller geht es im Browser über `ctrl/`.

Melden Sie sich dort mit dem Benutzer **admin** und dessen Kennwort an.

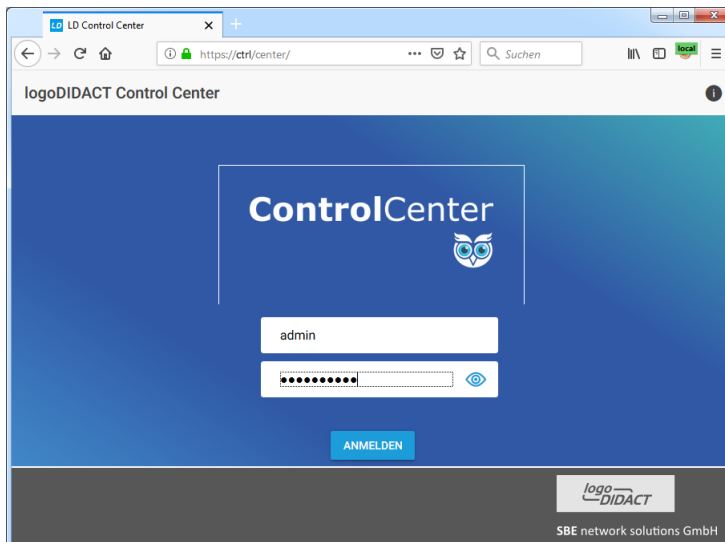


Achtung

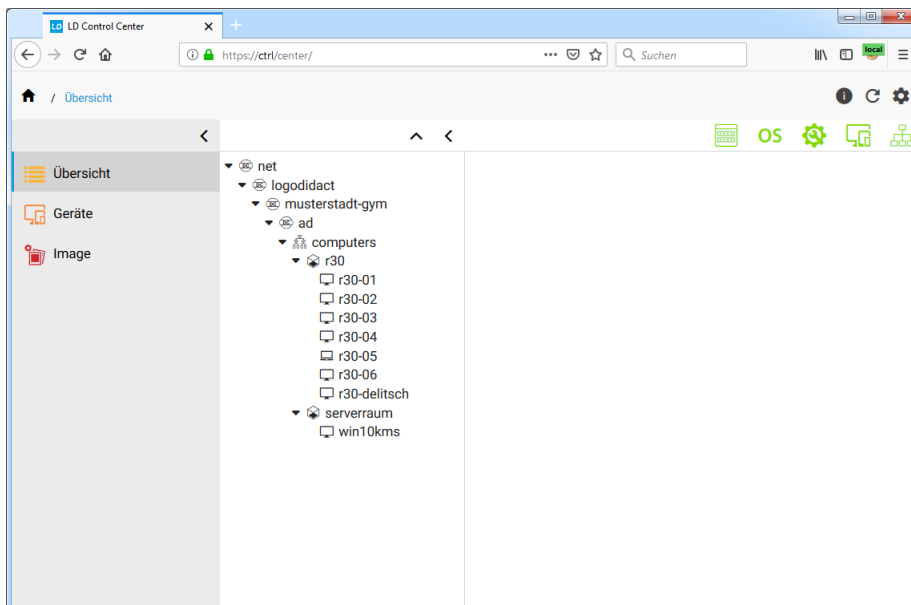
Verwenden Sie auf keinen Fall den Internet Explorer oder die alte Version des Edge Browsers!

Sie erhalten darüber fehlerhafte Anzeigen und absurde Darstellungen, die zu vollkommen falschen Schlussfolgerungen führen. Nutzen Sie bitte die Browser Firefox, Chrome oder den neuen Edge-Browser, der auf Chromium basiert. Wenn der Login nicht klappt, verwenden Sie bitte den FQDN:

`https://ctrl.schule.local/center`



Das Control Center startet in einem übersichtlichen Modus mit aufgeklappter Baumstruktur in Anlehnung an die Struktur im AD (Active Directory) mit der OU (organizational unit) computers, Räumen und Rechnern.



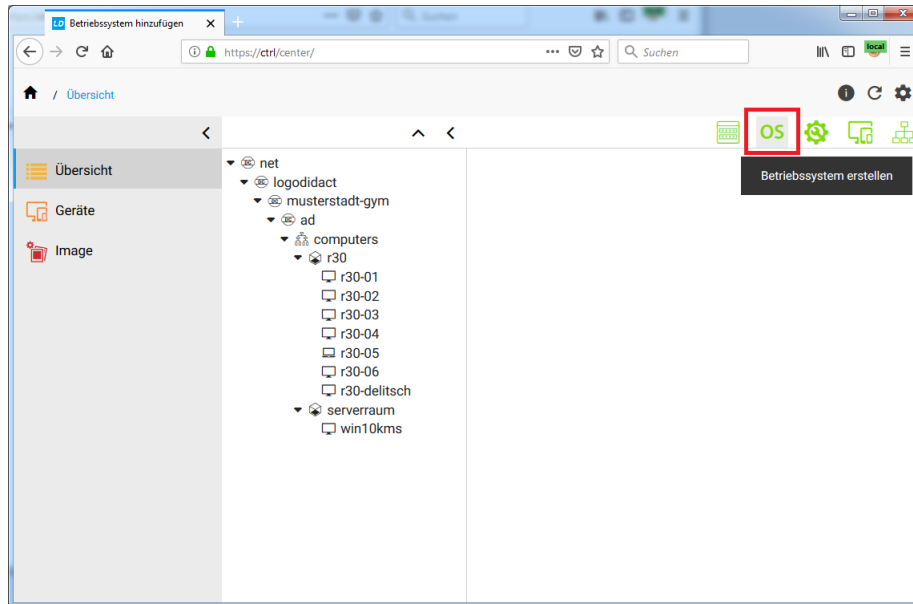
III.5.9. Eine Windows 10 Umgebung erstellen

Im Vergleich zu Rembo/mySHN gibt es in der Konfiguration einige Unterschiede und viele Vereinfachungen. Grundsätzlich erfolgt die Konfiguration per Webbrowser, wobei es das **Control Center** auch als WebApp gibt.

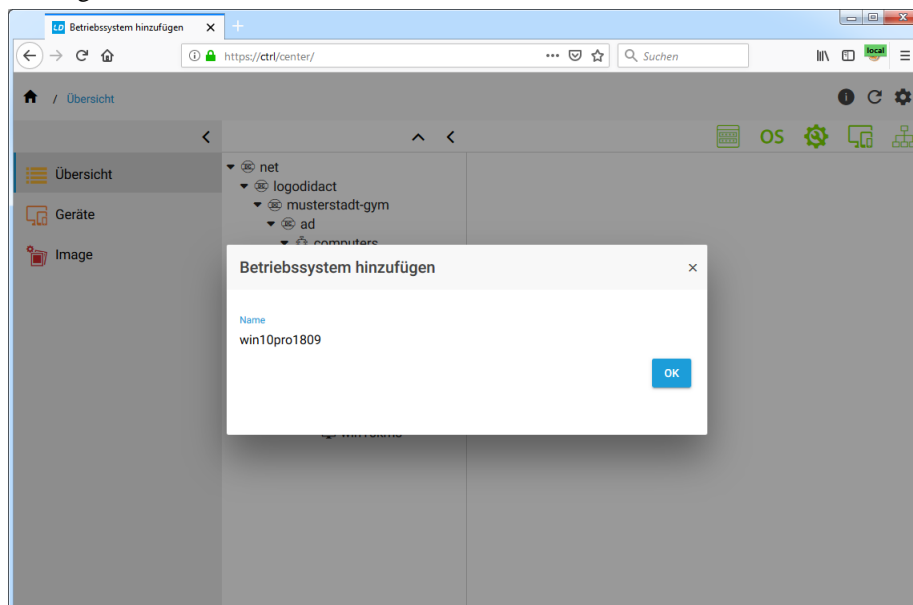
Führen Sie einfach die folgenden Schritte nacheinander durch.

III.5.9.1. Ein Betriebssystem erstellen

Wählen Sie im Hauptmenü den Eintrag **OS Betriebssysteme**. Wählen Sie aus dem Symbolmenü am rechten oberen Bereich das Symbol **OS** um ein neues Betriebssystem anzulegen.



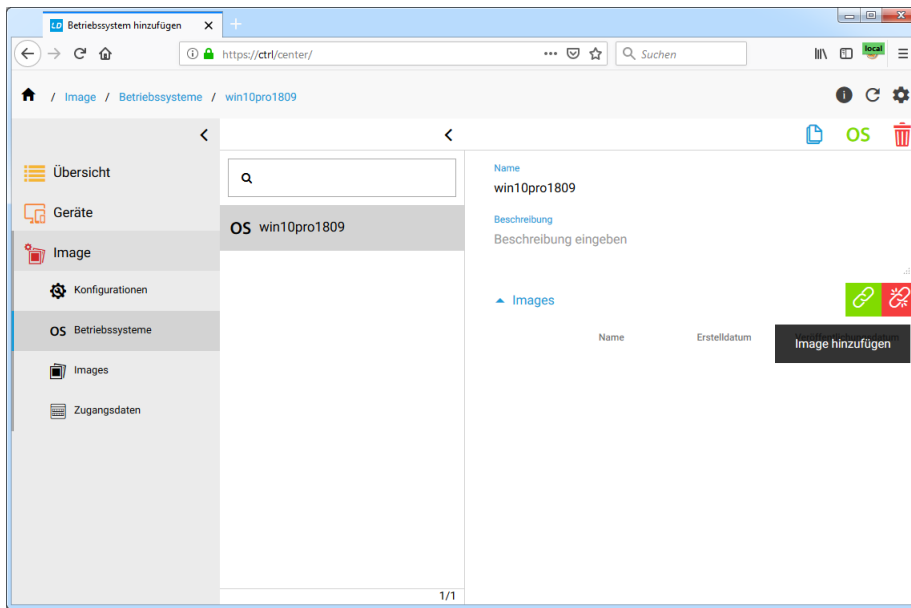
Geben Sie einen aussagekräftigen Namen für das Betriebssystem an, wie z.B. **win10pro1909** und bestätigen Sie mit **OK**.



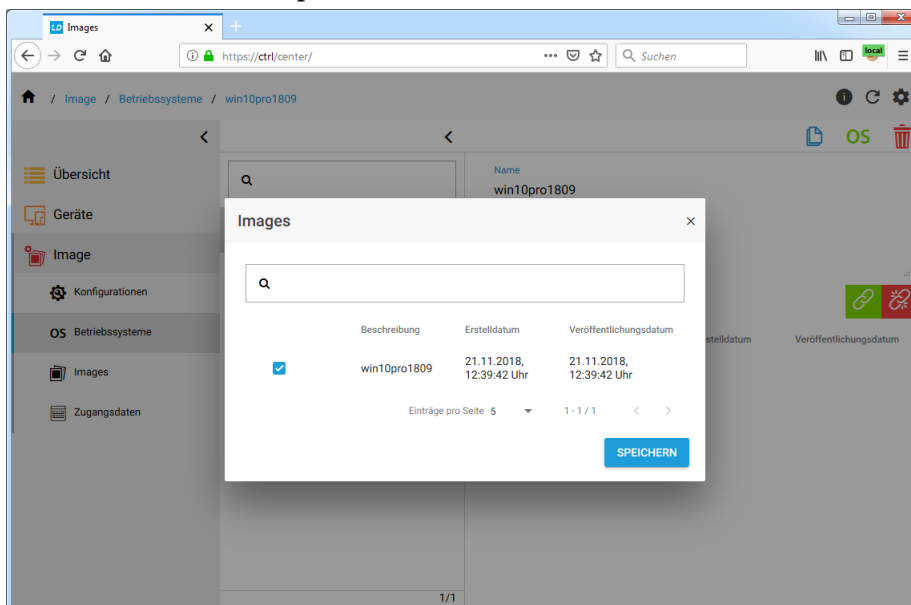
III.5.9.2. Dem Betriebssystem ein Image zuordnen

Navigieren Sie im linken Menübaum zum Modul **Imaging** und dort zum Menüeintrag **OS Betriebssysteme**. In der zweiten Spalte wird das gerade erstellte Betriebssystem angezeigt. Da es zunächst nur dieses eine System gibt, braucht man es nicht explizit auszuwählen, sondern kann die Imagezuordnung auf der rechten Seite im Abschnitt **Images** über das grüne Verknüpfungssymbol zuordnen.

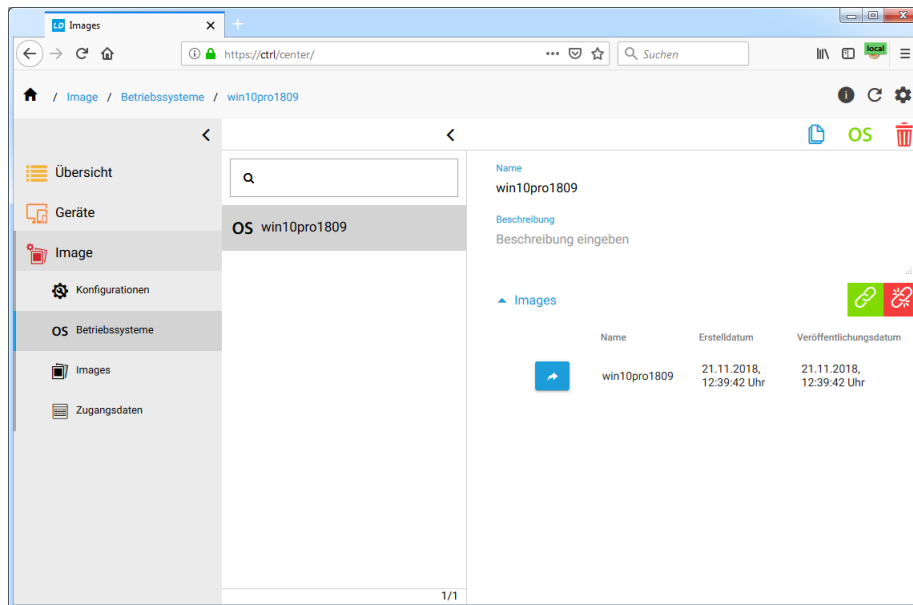
Dem Betriebssystem ein Image zuordnen



Klicken Sie auf das grüne Symbol auf der rechten Seite und markieren Sie das gewünschte Image. Wählen Sie anschließend **Speichern**.



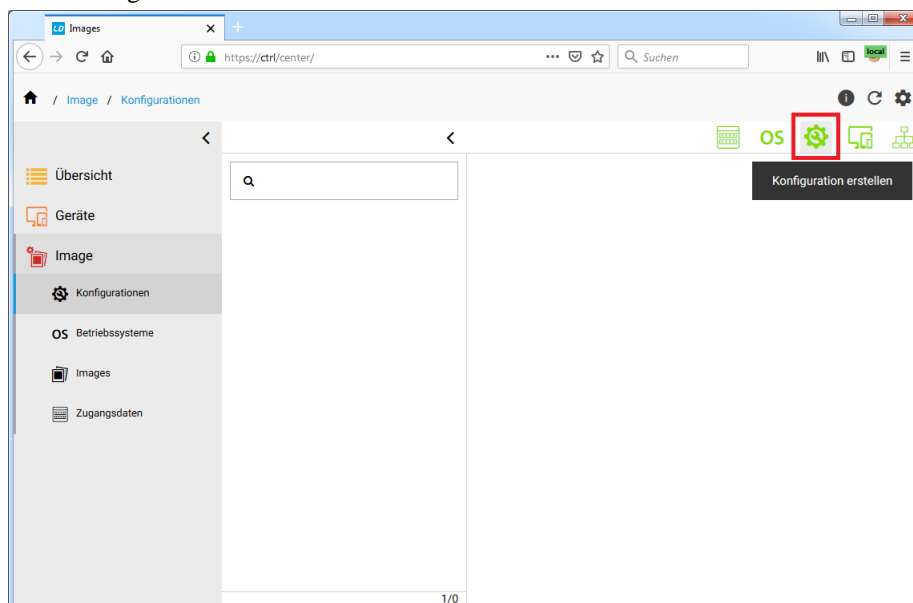
Das Betriebssystem ist jetzt mit dem Image verbunden.



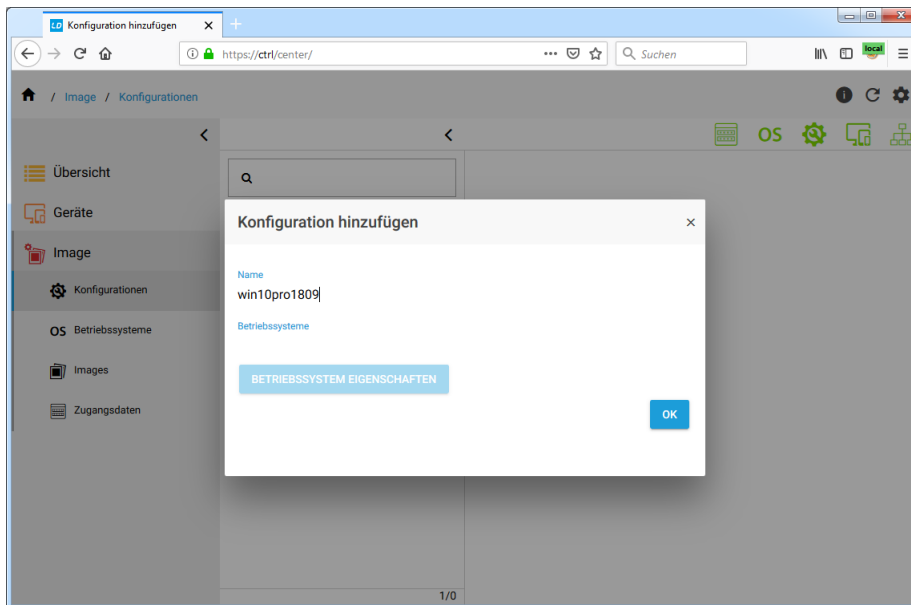
III.5.9.3. Konfiguration erstellen und Betriebssystem verknüpfen

Einen sehr großen Unterschied zwischen Rembo/mySHN® und **LD Deploy** gibt es im Bereich der Konfiguration von Partitionen. Diese ist nun deutlich einfacher und es besteht keine Notwendigkeit spezielle Größen für das Betriebssystem oder die Cache-Partition zu definieren. Alles erfolgt dynamisch und die gesamte Festplatte wird optimal ausgenutzt.

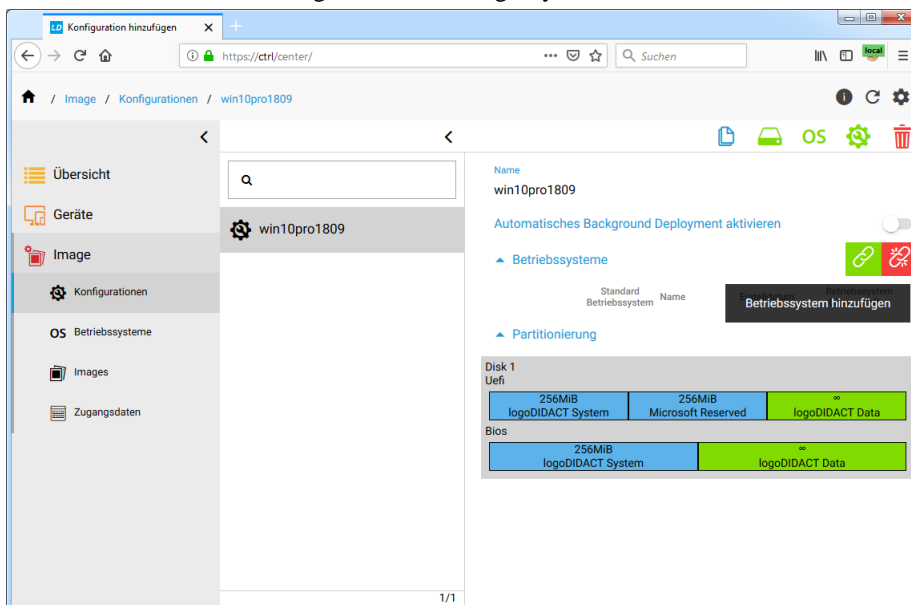
Navigieren Sie im linken Menübaum zum Modul **Imaging** und dort zum Menüeintrag **Konfigurationen**. Wählen Sie aus dem Symbolmenü im rechten oberen Bereich das Zahnrad-Symbol aus, um eine neue Konfiguration zu erstellen.



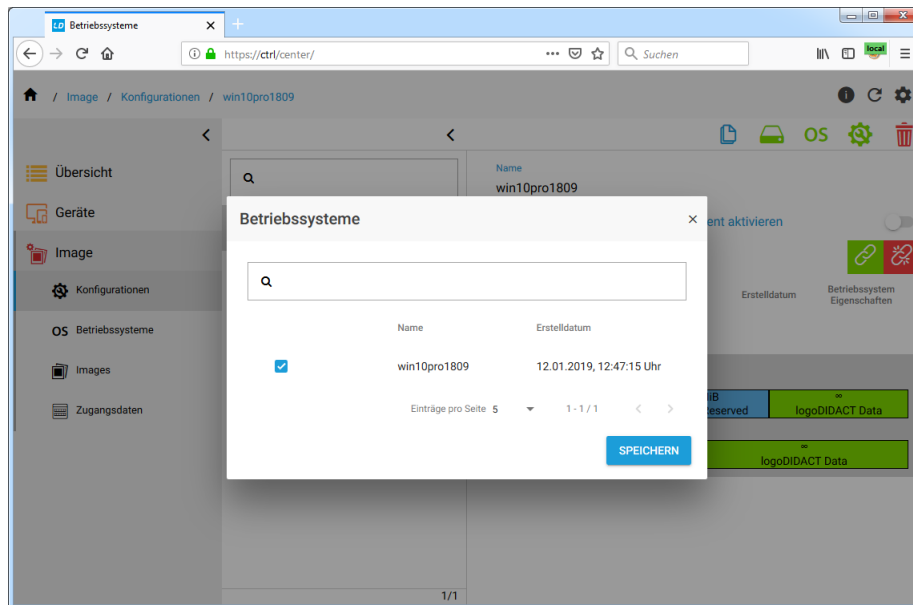
Geben Sie einen aussagekräftigen Namen für die Konfiguration an, wie z.B. **win10pro1909** und bestätigen Sie mit **OK**.



Verknüpfen Sie nun das zuvor erstellte Betriebssystem mit dieser Konfiguration. Wählen Sie dazu auf der rechten Seite wieder das grüne Verbindungssymbol.



Markieren Sie das gewünschte Betriebssystem und klicken auf **Speichern**.



III.5.9.4. Den Domänenbeitritt konfigurieren

Bei Rembo/mySHN® musste man mit seinem Master-Client auf manuellem Weg in Windows der Domäne beitreten. Auch dieser Mechanismus ist in **LD Deploy** automatisiert, einfacher und trotzdem flexibler und wird über das Control Center vorab konfiguriert. Wählen Sie dazu links im Menü den Eintrag **Image** und dort den Eintrag **Zugangsdaten**.

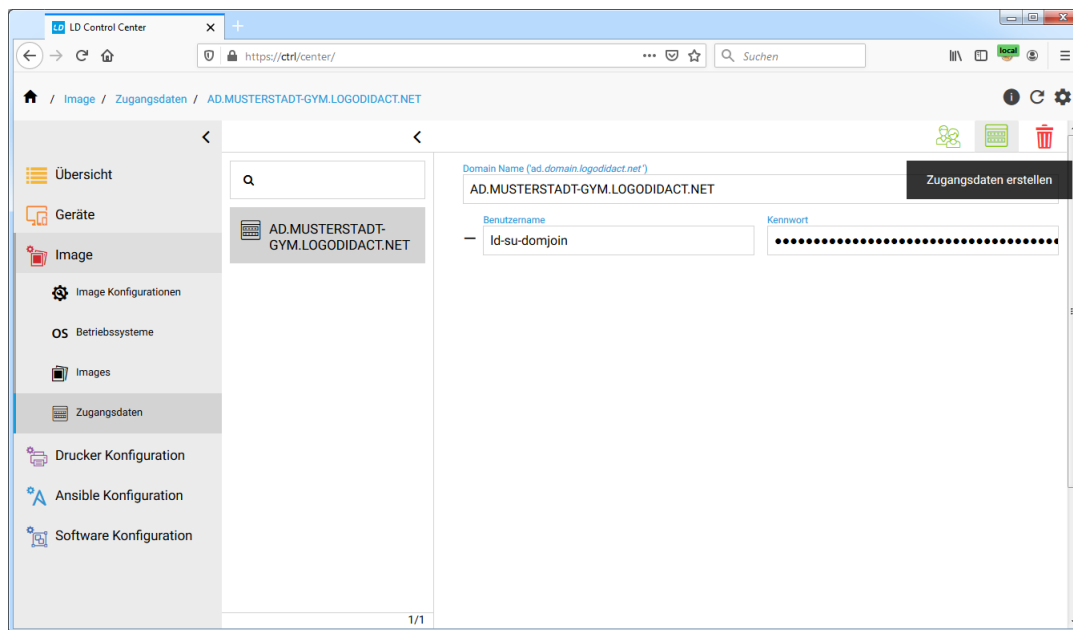


Achtung

Ab Puppet Rezeptstand 1.3.0 brauchen Sie an dieser Stelle keine manuelle Anpassung mehr!

Speziell für den automatisierten Domänenbeitritt mit **LD Deploy** gibt es ab dieser Version auf Serverseite in Samba 4 den neuen administrativen Benutzer **ld-su-dom-join**. Dieser ist ausschließlich für die Funktion des Domänenbeitritts zuständig und kann Computerkonten erstellen, ändern und löschen.

Bitte ändern Sie das Kennwort dieses Benutzers im ControllCenter auf keinen Fall, da dieses auf Gegenseite am Server nur vom **root** geändert werden kann (siehe Abschnitt III.3.4.3.1, „Das Konto ld-su-domjoin“)



Bisher wurde für den Domänenbeitritt der Benutzer **admin** verwendet, was weiterhin möglich ist. Der **admin** wird jedoch für die Benutzerverwaltung, die Softwareverteilung und verschiedene andere administrative Aufgaben genutzt und dessen Kennwort ab und an geändert. Das führt dann zu Problemen in **LD Deploy**, wenn man das Kennwort dort nicht ändert.

Der Beitritt von Windows 10 zur Samba4-Domäne (AD) ist im Prinzip unverändert zu der von Windows 7. Einzig der Domänenname ist nicht mehr ein NetBIOS-Name wie SCHULE, sondern ein FQDN (Fully Qualified Domain Name), aufgebaut nach dem folgenden Schema: **ad.domain.logodidact.net**

An diesem Namensschema dürfen Sie nichts ändern, bis auf den zweiten Teil im FQDN, d.h. den Eintrag „domain“, der weiter oben bereits angepasst wurde.

In der automatisch angelegten Konfiguration der Beispielumgebung lautet der FQDN: **ad.musterstadt-gym.logodidact.net**

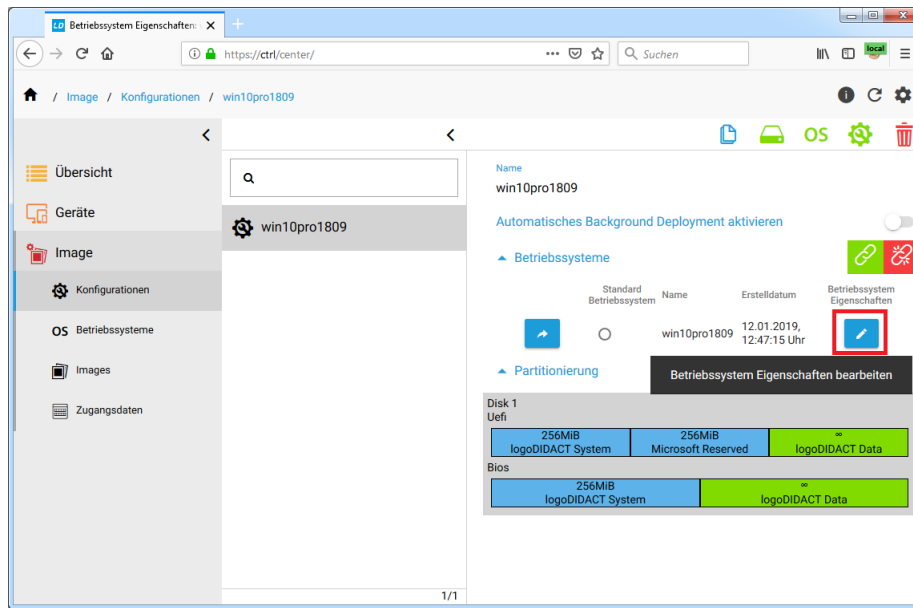
III.5.9.4.1. Einer fremden Domäne beitreten

Mit "fremder Domäne" sind alle Domänen oder Domaincontroller gemeint, die nicht am LogoDI-DACT-Server laufen. An dieser Stelle können Sie dann den Domänennamen und die Daten eines Domänen-Benutzers eingeben, der auf der fremden Domäne das Recht hat Computerkonten anzulegen, zu löschen und zu ändern..

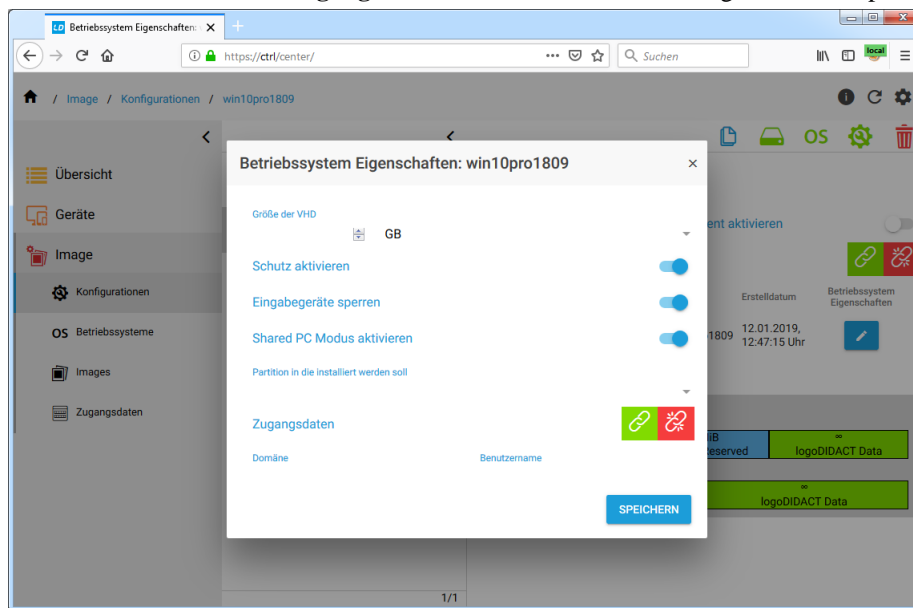
III.5.9.5. Das Betriebssystem mit der Domäne verknüpfen

Mit **LD Deploy** können von zentraler Stelle aus viele verschiedene Standorte und Domänen verwaltet werden. Der im vorherigen Schritt konfigurierte Domänenbeitritt muss deshalb einem System innerhalb einer Konfiguration zugeordnet werden, bzw. Sie müssen für das System festlegen, welcher Domäne es beitreten soll.

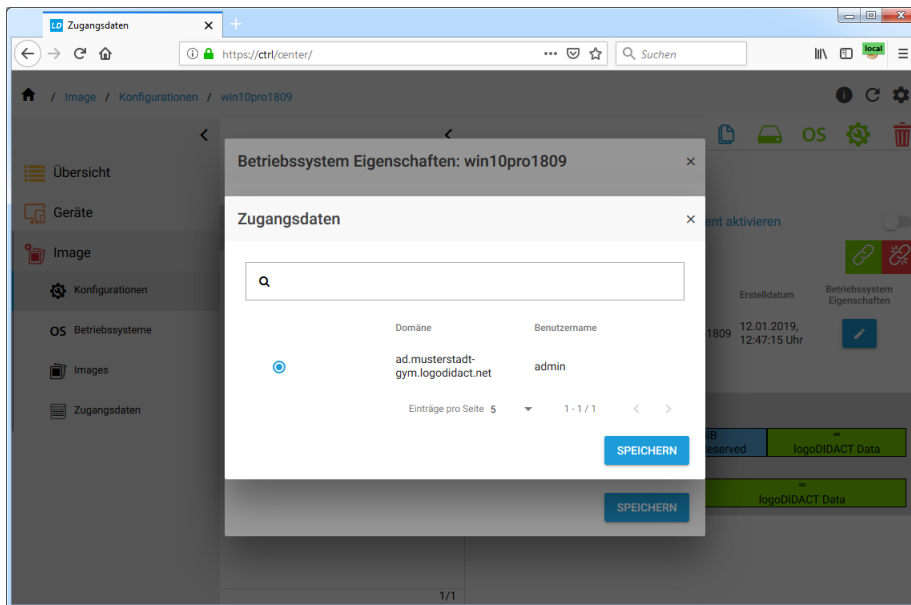
Dazu wählt man im Menübaum den Eintrag **Konfiguration** und in der zweiten Menüspalte die jeweilige Konfiguration. Im rechten Bereich beim Eintrag **Betriebssysteme** wählen Sie das blaue Editieren-Symbol.



Wählen Sie im Abschnitt **Zugangsdaten** auf der rechten Seite das grüne Verknüpfungs-Symbol.



Markieren Sie im Dialog **Zugangsdaten** den Eintrag für die passende Konfiguration des Domänenbeitritts und bestätigen Sie mit **SPEICHERN**.

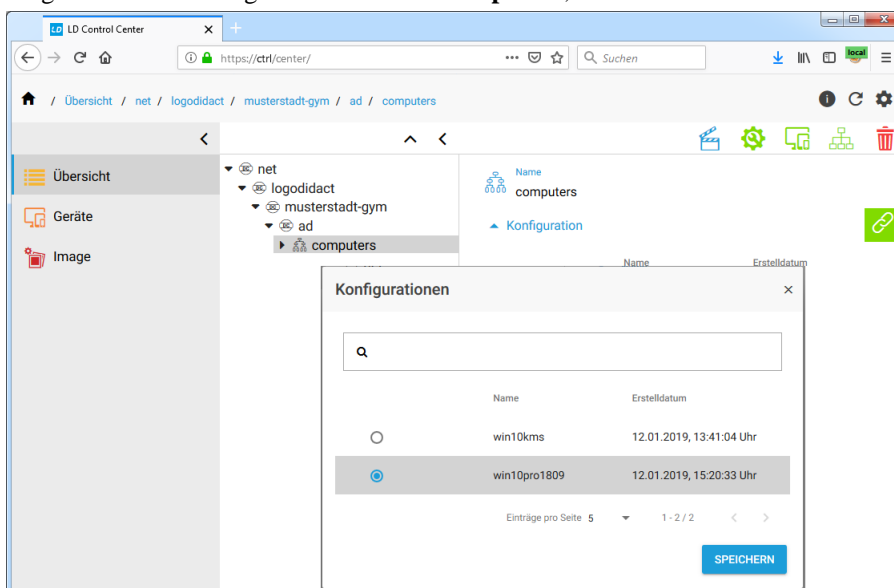


Wählen Sie erneut **SPEICHERN** um wieder im Fenster der Konfiguration zu landen. Konfiguration, Betriebssystem und Domäne sind nun miteinander verbunden, so dass Sie mit der Aufnahme des ersten Clients beginnen können.

III.5.9.6. Die Konfiguration mit der OU Computers verknüpfen

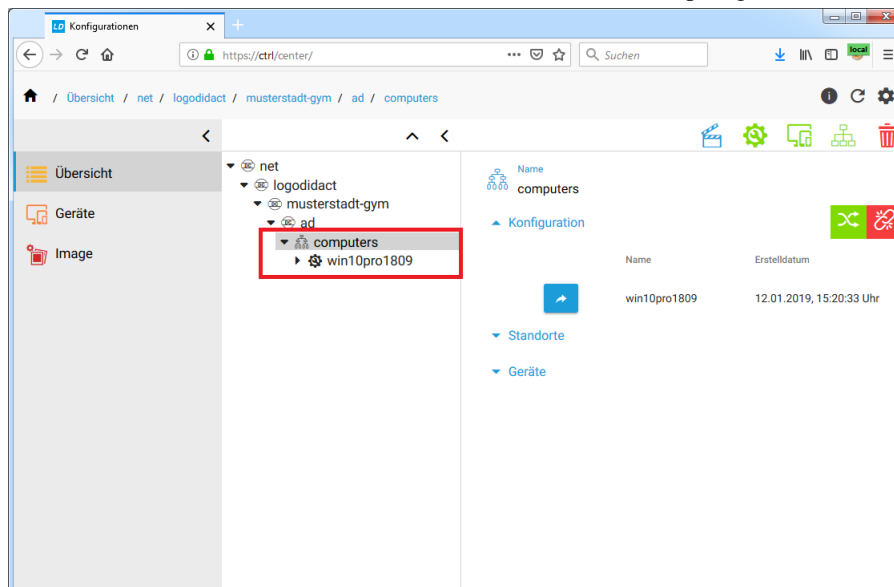
Der letzte Schritt in der Grundkonfiguration einer **LD Deploy** Umgebung besteht darin, einem Rechner oder einer Gruppe von Rechnern die jeweilige Konfiguration zuzuweisen.

Dazu wählt man in der Menübaum den Eintrag **Übersicht** und in der zweiten Menüspalte die jeweilige Gruppe bzw. den Raum oder Rechner. Bei einer Standardkonfiguration empfiehlt sich die Verknüpfung auf Ebene der Organisationseinheit **computers**, da diese an alle Räume vererbt wird.



Markieren Sie im Dialog **Konfiguration** den Eintrag für die passende Konfiguration und bestätigen Sie mit **SPEICHERN**. Danach steht diese Konfiguration als Standard-Umgebung allen Rechnern und

Räumen zur Verfügung. Das ist sowohl in der Baumstruktur der Organisation in der zweiten Spalte erkennbar als auch auf der rechten Seite im Bereich der Verknüpfung.



III.5.10. Background Deployment

Die grundlegende Funktionalität für das Background-Deployment steht seit 30.01.2019 im Pilotprogramm zur Verfügung! Die dafür notwendigen Versionsstände sind Control Center 19, ControlService 26 auf Serverseite und Iddeploy-agent 42 auf Clientseite.



Achtung

Führen Sie die Verteilung von Images oder Software niemals im laufenden Schulbetrieb durch, weder per PXE noch über Background-Deployment.

Der Server aber vor allem das Netzwerk wird dabei an seine maximal verfügbare Leistung gebracht, so dass andere Dienste dabei nur eingeschränkt oder gar nicht verfügbar sein können.

III.5.10.1. Hintergrund-Verteilung in Windows 10

Background-Deployment bedeutet, dass die Imageverteilung nicht "klassisch" über den Netzwerkboot per PXE erfolgt, sondern innerhalb des Betriebs von Windows 10 im Hintergrund.

Das funktioniert natürlich nur, nachdem ein Image per PXE verteilt wurde und der **Iddeploy-agent** am Client in der Version 42 oder höher installiert ist.

III.5.10.1.1. Background Deployment per WLAN

Das Background-Deployment wurde primär für Geräte entwickelt, die normalerweise nicht per Kabel am Netzwerk angeschlossen sind. Das sind neben Notebooks und Netbooks auch Windows 10 Tablets. Damit erspart man sich das "Betanken" per LAN-Kabel und jede Menge Zeit.



Achtung

Images oder Softwarepakete per WLAN verteilen zu können ist der Traum aller Administratoren und mit dem Background-Deployment und einer performanten WLAN-Infrastruktur prinzipiell auch möglich!

Genau dafür darf das Background-Deployment derzeit aber noch nicht eingesetzt werden!

Es sind noch intensive Tests notwendig, um das Verhalten in der Praxis beurteilen zu können.

Einsetzen lässt sich die Funktion aber bereits bei Clients, die dauerhaft per LAN-Kabel angeschlossen sind.

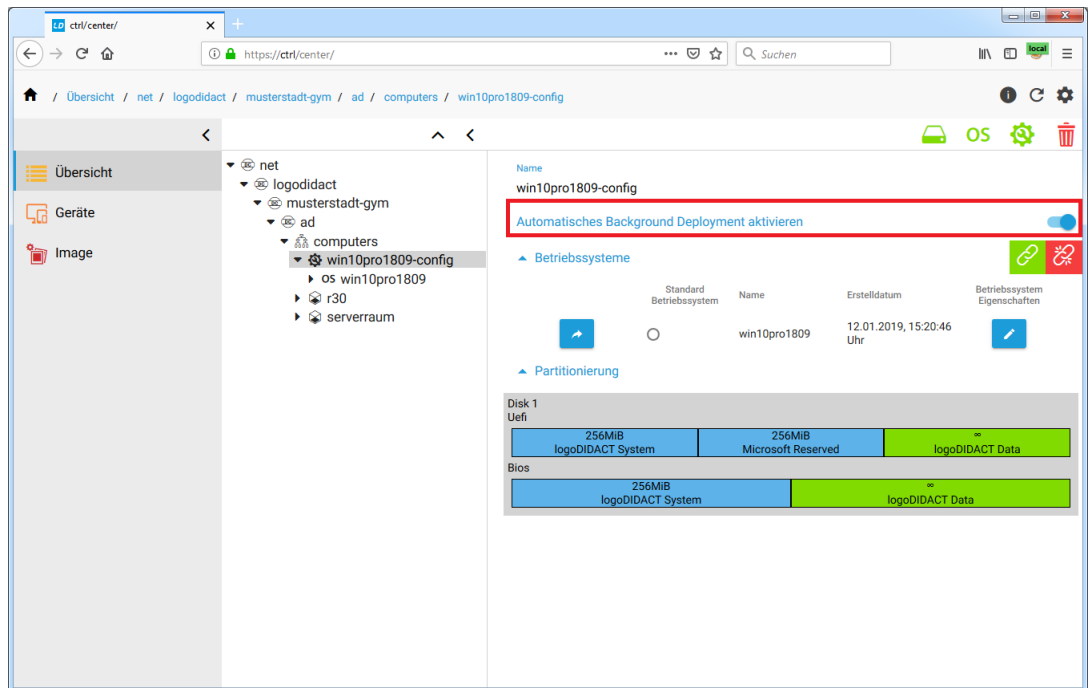
III.5.10.1.2. Background Deployment per LAN

Die Funktion Background-Deployment bietet auch für "normale" PCs, die dauerhaft per Kabel am Netzwerk angeschlossen sind, viele Vorteile:

- Die Verteilung ist schneller, da weder in LinPE noch WinPE gebootet werden muss.
- Die Verteilung verursacht **weniger Server- und weniger Netzlast**, da der 500 MB große LinPE-Client nicht über Netzwerk verteilt werden muss. Dies spielt insbesondere in großen Umgebungen eine Rolle, weil die Verteilung des LinPE-Clients nicht per Torrent erfolgt und der Server bei 100 Clients dafür 50 GB an Daten alleine für den PXE-Bootvorgang durchs Netzwerk schickt.
- Die Verteilung umgeht Probleme auf PXE-Ebene. Es gibt immer wieder Rechner, die auf PXE-Ebene Probleme mit der Implementierung der Treiber oder der Umsetzung der PXE-Spezifikation haben, so dass der Netzwerkdurchsatz nicht optimal ist. Solche Probleme gibt es beim Background-Deployment unter Windows nicht, da dort die Netzwerktreiber sehr aktuell gehalten werden können.
- Es gibt UEFI-Implementierungen, bei denen sich die Bootreihenfolge ändert, wenn Windows 10 beim ersten Deployment installiert wurde. Der Windows Boot-Manager wird dabei in der Bootreihenfolge an die erste Stelle geschoben, so dass solche Rechner überhaupt nicht mehr per PXE starten und eine Imageverteilung auf diesem Weg nur durch manuellen Eingriff möglich ist. Auch solche Geräte können über das Background-Deployment mit neuen Imageständen versorgt werden.

III.5.10.2. Background Deployment aktivieren

Die Aktivierung der Funktion Background Deployment findet im Control Center auf der Konfigurationsebene statt. Wählen Sie in der Baumstruktur den Eintrag für die jeweilige Konfiguration und aktivieren Sie im Fenster auf der rechten Seite den Schieberegler für den Eintrag **Automatisches Background Deployment aktivieren**.



III.5.10.3. Verhalten an den Windows 10 Clients

Wie der Name der Funktion bereits erahnen lässt, findet beim Background-Deployment die Verteilung im Hintergrund statt. Sichtbar wird der Prozess derzeit nur dann, wenn ein Rechner hochgefahren ist und an der Windows Anmeldemaske steht. Sobald es ein neues Image gibt, bzw. dem Rechner im Control Center ein anderes Image zugewiesen wird, startet das Background-Deployment und das Hintergrundbild im Anmeldebildschirm ändert sich.



Solange der Rechner in der Anmeldemaske stehen bleibt, laufen alle Prozesse automatisch ab, d.h. das Image wird im Hintergrund vom Server per Torrent geladen und anschließend in die VHD entpackt. Danach startet der Rechner automatisch neu und durchläuft die dritte Phase, wie auch beim "normalen" Verteilen über das Netzwerk.

III.5.11. Synchronisation der Geräteliste wimport_data

Für den Parallelbetrieb mit Rembo/mySHN® ist es weiterhin erforderlich, dass die alte Geräteliste `wimport_data` im System vorhanden ist. Diese liegt im Container `logosrv` und wird auch weiterhin von anderen älteren Komponenten im System genutzt.



Achtung

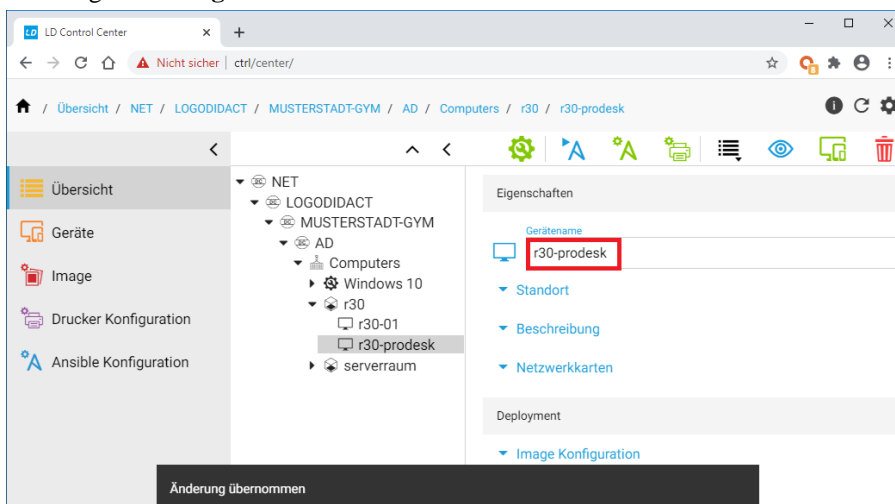
1. Die Rechneraufnahme in `LD Deploy` erfolgt nicht in der `wimport_data`, sondern direkt in der Datenbank.
2. Neue Geräte dürfen **NICHT** in der Geräteliste angelegt werden, sondern ausschließlich im Control Center
3. Die Datenbank ist die zentrale Stelle zur Speicherung aller Informationen und hat Priorität.
4. Die Geräteliste `wimport_data` wird aus den Einträgen aus der Datenbank erstellt.

III.5.11.1. Automatischer Abgleich beim Anlegen oder Löschen

Änderungen an den Einträgen im Control Center bzw. der Datenbank werden über eine teilautomatisierte Synchronisation zur Geräteliste `wimport_data` übertragen, inklusive einem Geräteimport (`import_workstations`). Bevor die Geräteliste dabei neu geschrieben wird, wird ein Backup angelegt.

Die Kommunikation zwischen dem Control Center und der Geräteliste erfolgt dabei über den Dienst `ld-control-service` im Container `ctrl-g1` und dem Dienst `ld-control-client` im `logosrv`.

Wird beispielsweise der Name eines Gerätes angepasst und gespeichert, indem man das Eingabefeld verlässt und auf einen anderen Bereich klickt, erfolgt kurze Zeit später am unteren Fensterrand die Meldung **Änderung übernommen**.



Bei folgenden Änderungen im Control Center wird die Synchronisation in Richtung der Geräteliste ausgelöst:

- IP-Adresse
- MAC-Adresse
- Subnet-Mask
- Rechnername
- Raumname
- Imagingtechnik (LD Deploy oder rembo5)

Es gibt dabei eine zeitliche Verzögerung von ca. 10 Sekunden, um gegebenenfalls gleichzeitige Änderungen zusammenzufassen und die Liste nicht permanent zu synchronisieren.

III.5.11.2. Fehler in der Synchronisation zwischen Control Center und Geräteliste

Wie oben erwähnt, ist die Datenbank bzw. das Control Center die primäre Stelle, in der alle Geräte und Konfigurationen zu **LD Deploy** gepflegt werden. Die Geräteliste (wimport_data) wird lediglich aus den Werten der Datenbank aufgebaut!

Wenn sich z.B. der Rechnername in der Geräteliste nicht ändert, obwohl er im Control Center geändert wurde, lässt sich die Ursache wie folgt prüfen:

Wechseln Sie auf Serverseite in den Container **logosrv** und prüfen Sie die Logs nach Einträgen des Dienstes:

```
tail -f /var/log/syslog | grep -i ldcli
```

Führen Sie nun im Control Center einer der obigen Änderungen durch, welche die Synchronisation auslösen, wie z.B. die Änderung eines Raumnamens. Wenn die Kommunikation zwischen den Diensten in Ordnung ist, sieht die Ausgabe so aus, dass man die Synchronisation zur Geräteliste und dem anschließenden Import erkennen kann:

```
root@logosrv:~ # tail -f /var/log/syslog | grep -i ldcli
..." level=info msg="Getting '/etc/logodidact/wimport_data' from 'https://ct
..." level=info msg="Renaming '/etc/logodidact/wimport_data' to '/var/backup
..." level=info msg="Writing '/etc/logodidact/wimport_data'..."
..." level=info msg="Running '/usr/bin/import_workstations'..."
```

III.5.11.2.1. Fehlerhaftes Zertifikat im logosrv

Sollte das Zertifikat im Container **logosrv** falsch bzw. ungültig sein, erscheinen entsprechende Fehlermeldungen. Die Ursache für dieses Problem kann darin liegen, dass Zertifikate erneuert werden müssen, was auch bei allen durch Puppet gemanageten Container problemlos funktioniert, nur eben beim **logosrv** nicht.

Die Fehlerbehebung besteht darin, die Zertifikate neu generieren zu lassen.

Im **logosrv** Zertifikat löschen:

```
rm /usr/share/ca-certificates/ld10/ca-g1.crt
```

Im lhost Erstellung eines neuen Zertifikates für logosrv anstoßen:

```
prun
```

Im logosrv den Dienst neu starten:

```
invoke-rc.d ld-control-client restart
```

III.5.11.3. Fehler durch doppelten dhcpd Prozess im logosrv

Sollte die Synchronisation zwischen Control Center und Geräteliste funktionieren und z.B. die Änderung eines Rechner- oder Raumnamens auch in der Geräteliste stehen, besteht trotzdem noch die Möglichkeit, dass sich am Client selbst nichts ändert.

Die Ursache dafür kann ein zweiter Prozess des dhcp-Servers im **Logosrv** sein. Prüfen Sie das, indem Sie in den Container wechseln und prüfen, ob es eventuell zwei oder mehr Prozesse gibt:

```
ps aux | grep dhcpd
```

Der erste dhcp-Prozess liefert damit weiterhin die alten Daten an die Clients, so dass die Fehlerursache nur schwer erkennbar ist. In einer solchen Situation lassen sich die Prozesse selten normal beenden, sondern müssen mit Priorität über ihre Prozess-ID (PID) "abgeschossen" werden:

```
kill -9 PID
```

III.5.11.4. Manueller Abgleich der Geräteliste bei Namensänderung

Ein automatischer Abgleich ist aus verschiedenen Gründen nicht bei allen Änderungen über das Control Center sinnvoll. So werden beispielsweise Änderungen am Rechnernamen nicht automatisiert in die `wimport_data` geschrieben.

Die Namensänderung kann über folgenden Befehl vom Container **Logosrv** aus synchronisiert werden:

```
ld-control-client sync hosts
```

```
root@logosrv:~# ld-control-client sync hosts
INFO[0000] Reading '/etc/logodidact/wimport_data'...
INFO[0000] Posting '/etc/logodidact/wimport_data' to 'https://ctrl...'
INFO[0000] Getting '/etc/logodidact/wimport_data' from 'https://ctrl...'
INFO[0001] Renaming '/etc/logodidact/wimport_data' to '/var/backups/wimport_data/2018-08-23,20-33-42'...
INFO[0001] Writing '/etc/logodidact/wimport_data'...
```

III.5.12. Client-Konfiguration mit AutoConf

Anfang 2019 wurde das Open-Source Werkzeug Ansible zur automatisierten Client-Konfiguration eingeführt und war zu Beginn eine gute Wahl. Im Laufe der Zeit stieg aber die Anzahl an komplexen Anpassungen und Rollen immer mehr an, so dass die negativen Eigenschaften von Ansible immer mehr ins Gewicht fielen.

Vor allem im Hinblick auf Geschwindigkeit und Stabilität konnte Ansible in keiner Weise die Anforderungen erfüllen. Mit **AutoConf** wurde deshalb Anfang 2020 eine Eigenentwicklung angestoßen und mit Puppet Rezeptstand 1.3.22-6 im Januar 2021 freigegeben.

Alle von SBE entwickelten Rollen in Ansible wurden nach Autoconf portiert und sind 1:1 im ControlCenter so zu verwenden.

III.5.12.1. Vordefinierte Rollen für AutoConf

Der Umgang mit **AutoConf** für Windows 10 Clients wird im Kapitel Abschnitt IV.1.7, „Systemanpassung in LD Deploy mit AutoConf“ ausführlich beschrieben. Was dabei im Einzelnen passiert

und wie diese Rollen aufgebaut sind, lässt sich im Container **ctrl-g1** prüfen und mit hinreichend YAML-Kenntnissen nachvollziehen.



Achtung

Ändern Sie in keinem Fall etwas an vordefinierten Anpassungen. SBE leistet dafür in keiner Weise Support.

Vordefinierte Rollen liegen im Container **ctrl-g1** im Verzeichnis `/usr/lib/ld-auto-conf/logodidact/roles`.

Infos zu einer Rolle, sowie der prinzipielle Aufbau werden beispielhaft an der Funktion gezeigt, wie Microsoft Office Updates über die Rolle `ld_win_office_disable_updates` verhindert werden. Wenn man in das Verzeichnis einer Rolle wechselt, sieht man in der Regel die Unterordner `meta` und `win`. Sofern es eine Rolle für Linux-Clients gibt, existiert auch ein Ordner `lin`.

Wenn man wissen möchte, in welcher Phase bzw. in welchen Phasen eine Rolle greift, hilft ein Blick in die Datei `/meta/logodidact.yml`. Die tags `AUDIT` und `CUSTOM` bedeuten, dass die Rolle in diesen Phasen von **LD Deploy** aktiv sind und eine Anpassung vornehmen.

Was dort für einen Windows-Client gemacht wird, findet man im Verzeichnis `win` in verschiedenen `.ps1`-Dateien. Diese Power-Shell-Dateien sind so benannt, wie die **LD Deploy** Phasen, in denen sie aufgerufen, also z.B. `audit.ps1`, `setup.ps1` oder `user.ps1`.

III.5.12.2. Aktualisieren eines Playbooks

Ein Playbook ist etwas vereinfacht dargestellt nichts anderes als eine Ansammlung von Tätigkeiten, die ein Client in verschiedenen Phasen ausführen soll. Sofern es im Control Center für einen Rechner irgendeine Anpassung über AutoConf gibt, wird für diesen Rechner ein Playbook in Form einer Datei erstellt.



Achtung

Das Playbook für einen Rechner wird ausschließlich dann erstellt oder aktualisiert, wenn:

- der Rechner automatisch in eine Phase läuft und sein Playbook vom Server anfordert
- die Ausführung eines Playbooks über das Control Center für den Rechner oder den Raum aktiv angestoßen wird

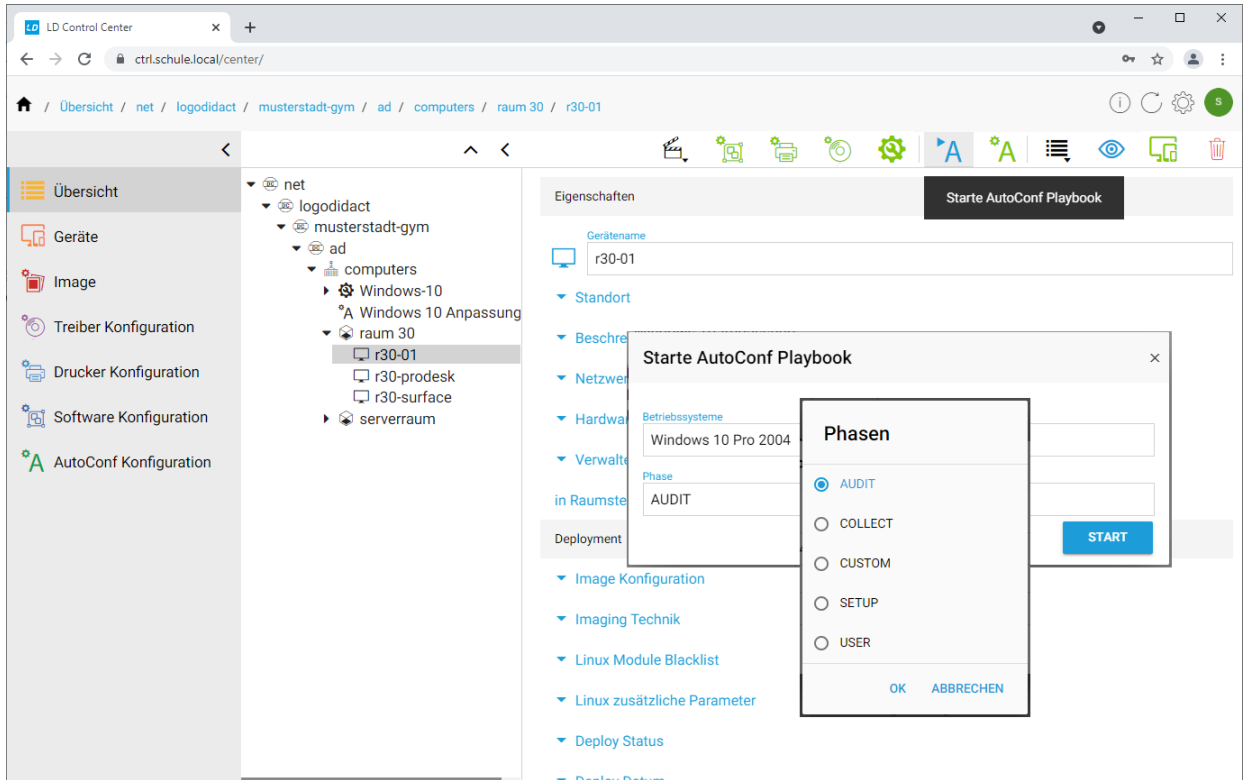
Wenn Sie eine Änderung im Control Center an der Konfiguration in AutoConf vornehmen, passiert am Playbook auf Dateiebene also zunächst nichts!



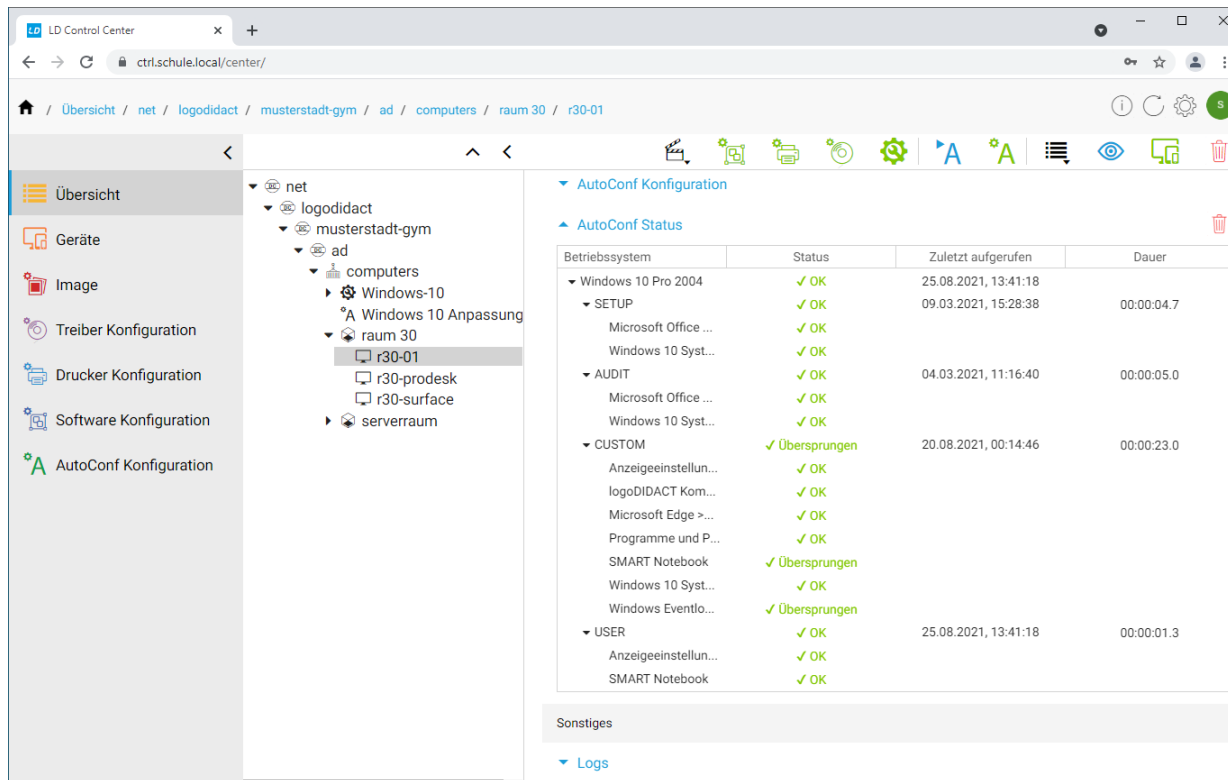
Tipp

Für die Fehlersuche und Analyse ist es extrem wichtig, dass man das Playbook aktualisiert, bevor man es auf Kommandozeile ausführt. Es spielt dabei keine Rolle, für welche Phase man die Aktualisierung über das Control Center anstößt. Es wird immer das gesamte Playbook für alle Phasen aktualisiert aber nur die ausgewählte Phase über AutoConf am Client abgearbeitet!

Am einfachsten und schnellsten ist es deshalb, die Aktualisierung des Playbooks über die Phase USER anzustoßen!



Die Abarbeitung des Playbooks geschieht dann "unsichtbar" im Hintergrund und im Control Center sind im Abschnitt **AutoConf Status** für die ausgewählte Phase ausführliche Infos zu sehen. Neben Datum und Uhrzeit der letzten Ausführung wird auch die Zeitdauer für die jeweilige Phase aufgeführt. Innerhalb einer Phase wird für jede einzelne Rolle der Status angezeigt. Neben Erfolg oder Missrfolg gibt es auch "Übersprungen", sofern eine Rolle bereits in einer anderen Phase angewandt wurde.



III.5.13. Protokollierung mit graylog

Mit der Verteilung vieler Dienste und Module auf Container und virtuelle Maschinen, verteilen sich auch die jeweiligen log-Dateien bzw. Dateien zur Protokollierung auf viele verschiedene Systeme. Protokolldateien gibt es jedoch nicht nur am Server und den vielen verschiedenen Diensten, sondern auch auf den Arbeitstationen.

Log-Dateien sind im allgemeinen sehr hilfreich, wenn es um die Suche und Behebung von Fehlern geht. Um hierbei in LogoDIDACT eine zentrale Stelle für Protokolle zu schaffen, wird die Open Source Software graylog genutzt und über einen Container bereitgestellt (<https://www.graylog.org/>).

III.5.13.1. Installation Container graylog

Auch der Container **graylog-g1** wird wieder auf die gleiche Weise aktiviert und konfiguriert, wie das bereits den Bausteinen zuvor gezeigt wurde.

Wechseln Sie in den Puppeteer:

```
lxc-ssh -n puppeteer
```

Wechseln Sie in das Verzeichnis zur Aktivierung von Containern:

```
cd /etc/logodidact/hosts/ldhost
```

Öffnen Sie die Datei `guest.conf` mit einem Editor Ihrer Wahl, wie z.B. Nano:

```
nano guest.conf
```

Fügen Sie dort den Eintrag für den Container `ldmobile` hinzu.

```
[Guest graylog-g1]
Ensure running
```

Durch Eingabe der Tastenkombination `<Strg>+<X>` verlassen Sie den Editor Nano und geben „Y“ ein, damit die Änderung gespeichert wird. Wechseln Sie dann ins Stammverzeichnis der Konfiguration und übertragen Sie anschließend die Änderungen ins Versionierungssystem git:

```
cd /etc/logodidact
```

```
git add .
```

```
git commit -m "Aktivierung der Protokollierung mit graylog"
```

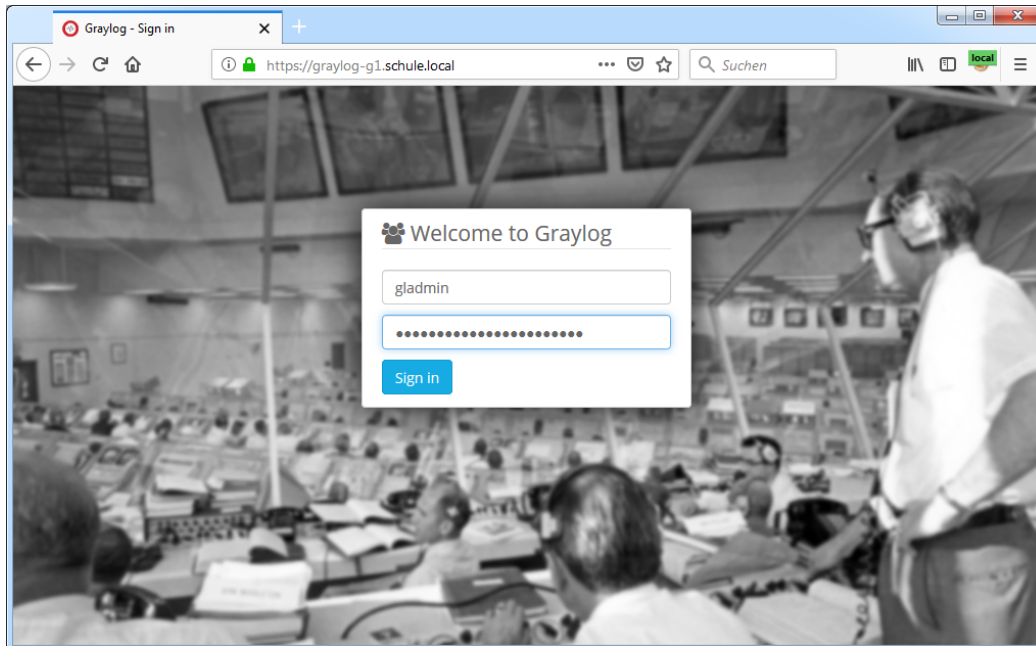
Analog zu der bisherigen Vorgehensweise wird der Aufbau des Containers durch einen `prun` im `ldhost` angestoßen. Über `pstat` im Puppeteer kann man wieder beobachten und die Durchläufe im Container `graylog-g1` durch Aufrufe von `prun` beschleunigen.

III.5.13.2. Webinterface von graylog

Im Normalfall besteht kein Grund, sich über das Webinterface von graylog die Protokolle anzuschauen. Der Sinn und Zweck von graylog besteht in LogoDIDACT vor allem darin, eine zentrale Stelle und Schnittstelle für Log-Dateien zu haben.

Die Anzeige bzw. Aufbereitung von Logs erfolgt z.B. über das Control Centergr.

```
https://graylog-g1.schule.local
```



Das Kennwort für den Benutzer `gladmin` holt man sich am besten aus dem Container `puppeteer`, in dem Kennwörter für diverse Dienste zentral abgerufen werden können (siehe Index redis).

Kapitel III.6. Microsoft Produktaktivierung mit LD Deploy

Die Produktaktivierung wurde von Microsoft bereits in Windows XP eingeführt und sollte vor allem die Piraterie verhindern, d.h. das unrechtmäßige Kopieren und Installieren auf vielen Rechnern. Während es bei Windows XP noch spezielle Volumen-Lizenz-Keys (VLKs) gab, über die man eine unbeschränkte Anzahl an gleicher oder auch komplett unterschiedlicher Hardware aktivieren konnte, gibt es diese „Flatrate-Keys“ bei Windows 7 und Windows 10 nicht. Ebenfalls hat Microsoft die Aktivierung auch für das Büropaket Microsoft Office 2010 eingeführt. Volumenlizenzkeys gibt es weiterhin, jedoch ist die Aktivierung deutlich komplexer und fehleranfälliger geworden und erfordert Expertenwissen.

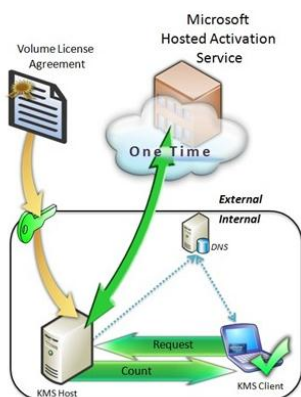
Das Thema Produktaktivierung ist vor allem deshalb nicht trivial und einfach zu beantworten, weil es viele verschiedene Lizenzierungs- und Aktivierungsformen gibt, die selbst für viele erfahrene Administratoren unbekannt sind. Zudem gibt es in diesem Bereich Unterschiede zwischen Lizenzrecht und Lizenztechnik und die wenigsten Anwender lesen die EULA (End User License Agreement), geschweige denn, dass sie diese verstehen.



Achtung

Im Zuge der Verbreitung von Windows 10 und Office 2016 ändert sich die Methode der Aktivierung in LogoDIDACT 2.0 grundlegend und erfolgt per Microsoft KMS.

Die neue Konstellation sieht wie folgt aus.



III.6.1. Neue Produktaktivierung in LogoDIDACT 2.0

Das Thema Produktaktivierung von Microsoft Windows und Office wurde in der Vergangenheit überwiegend mit dem von SBE selbst entwickelten LogoDIDACT Key-Management-Server realisiert.

Dieser Dienst stand ab 01.10.2010 zur Verfügung, als die ersten Schulen das Betriebssystem Windows 7 (erschieden im Oktober 2009) einsetzen wollten und eine Lösung für die Aktivierung benötigten. Die Aktivierung mittels des **Microsoft KMS (Key-Management-Service)** war nur sehr schwer bis gar nicht möglich, weil dieser Dienst bekanntermaßen eine minimale Anzahl an 25 Windows 7 PCs benötigt, um mit der Aktivierung zu beginnen. Zu dieser Zeit nutzte der Großteil der Schulen noch XP, so dass es schwierig war, auf die benötigte Anzahl an 25 PCs mit Windows 7 zu kommen.

Der von SBE entwickelte LogoDIDACT Key-Management-Server war deshalb so ausgelegt, dass er Volumenkeys vom Typ MAK und auch Einzelproduktkeys verarbeiten konnte. Ein weiteres Kriterium

für diese Eigenentwicklung war, dass für den Microsoft KMS ein zusätzlicher Windows 7 Rechner oder Windows 2008 Server notwendig gewesen wäre, auf dem der Dienst läuft.



Achtung

In LogoDIDACT 2.0 ist der **Microsoft KMS (Key-Management-Service)** die neue und dringend empfohlene Standardmethode zur Aktivierung von Windows 7/8/10 und Office 2013/2016.

Beim Einsatz der neuen Softwareverteilungslösung **LD Deploy** ist diese Methode sogar verbindlich, d.h., die Aktivierung von Windows und Office erfolgt ausschließlich per Microsoft KMS.

Der Microsoft KMS läuft dabei in einer virtuellen Maschine auf dem LogoDIDACT-Server entweder unter Windows 10 oder Windows 2016 Server.

Der bisher eingesetzte LogoDIDACT Key-Management-Server kann für alte Geräte verwendet werden, die noch mit Rembo/mySHN® laufen.

Zur Aktivierung von Windows und Office wird zwingend ein Lizenzkey vom Typ KMS benötigt.

III.6.2. Grundlagen der Lizenzierung und Aktivierung

Für die Produktaktivierung von **Windows** und auch **Office** gibt es zahlreiche Varianten, die im Laufe der Zeit auch immer wieder verändert, ergänzt oder deaktiviert wurden. Viele dieser Varianten sind alles andere als leicht zu verstehen und lassen sich zudem noch kombiniert einsetzen, so dass der Laie überhaupt nicht begreift, warum ein Produkt mal aktiviert ist und dann wieder nicht.

Wir beschränken uns deshalb sowohl in diesem Handbuch als auch generell in LogoDIDACT 2.0 auf eine Methode der Lizenzierung und Aktivierung von Microsoft Produkten, die verständlich, einfach, zuverlässig und kostengünstig ist.

III.6.2.1. Der Microsoft KMS (Key Management Service)

Mit dem Key Management Service stellt Microsoft einen Dienst bereit, über den sowohl **Windows** als auch **Office** auf den Arbeitsstationen im Netzwerk aktiviert werden kann.

Für den praktischen Einsatz des Microsoft KMS-Server sind einige grundlegende Voraussetzungen zu beachten, sowohl was die technische Seite der Aktivierung betrifft, als auch die lizenzrechtliche Seite. Auf technischer Ebene beginnt der Microsoft KMS mit seiner Aktivierung für Windows, wenn er mindestens 25 Aktivierungsanfragen vorliegen hat. Sofern die Menge an Anfragen nicht erreicht werden kann, ist auch eine Konstellation mit Proxy-KMS möglich. Für die Aktivierung von Office reichen hingegen 5 Anfragen, die auch in einem sehr kleinen Netzwerk problemlos erreichbar sind.

Die zweite wichtige Voraussetzung, ist das Vorhandensein eines Volumenlizenzkeys vom Typ KMS, den man ausschließlich innerhalb verschiedener Microsoft Volumenlizenz-Verträge erhält.

III.6.2.2. Lizenzrecht und Lizenztechnik

Für das Betriebssystem Windows gibt es von Seiten Microsoft schon "immer" ein so genanntes Reimaging-Recht, das regelt, wie man ein Windows-Image auf viele Geräte kopieren bzw. verteilen (Deployment) kann und darf. In diesem Zusammenhang ist man berechtigt, für alle Rechner mit OEM- oder

Retail-Lizenz die Aktivierung mit Volumenlizenzkeys (VL Keys) durchzuführen. Erlaubt sind dabei sowohl MAK als auch KMS.

Die lizenzierte Windows-Version muss aber gleich sein, d.h., für Rechner mit Windows 10 OEM Lizenzn dürfen Sie einen Volumenlizenzkey für Windows 10 nutzen und für die Aktivierung von Geräten mit Windows 7 OEM-Lizenz den entsprechenden VL-Key für Windows 7.



Achtung

Es ist unabdingbar, dass Sie das Lizenzrecht von Microsoft einhalten. Verfügt ein Computer über eine legale Windows Professional Lizenz (COA-Aufkleber, digitale Signatur, SLIC-Eintrag im BIOS, Lizenzvertrag usw.), dann besteht das Recht, darauf ein Windows in der zur Lizenz passenden Version mit einem Key vom Typ MAK oder KMS zu betreiben und zu aktivieren.

In dieser Hinsicht gibt es also zwei vollkommen verschiedene lizentechnische Möglichkeiten, die lizenzrechtlich explizit erlaubt sind.

Beim Einsatz von Volumenlizenzkeys sind folgende weitere Bedingungen unbedingt zu beachten:

- Der Einsatz der Keys ist ausschließlich auf schuleigenen Geräten erlaubt
- Die Lizenzkeys sind sicher aufzubewahren und nicht an Dritte weiterzugeben
- Die Aktivierung darf nur auf Geräten erfolgen, für welche die Schule eine Lizenz besitzt
- Die Verantwortung für die Einhaltung des Lizenzrechts obliegt alleine der Schule

III.6.2.3. Der richtige Volumenlizenzvertrag für KMS

Um an einen Volumenlizenzkey vom Typ KMS (Key Management Service) oder MAK (Multiple Activation Key) zu kommen, benötigt man einen entsprechenden Volumenlizenzvertrag. Dabei gibt es viele verschiedene Formen und Modelle, sowohl auf Kauf- als auch Mietbasis, von denen wir hier nur die zwei Wichtigsten benennen wollen.

III.6.2.3.1. FWU 2.0 Vertrag auf Mietbasis

Bei den Verträgen auf Mietbasis findet der so genannte **FWU**-Vertrag zunehmend Verbreitung. „FWU“ ist kein Lizenzmodell von Microsoft, sondern eine Kurzbezeichnung für einen Vertrag, den das Medieninstitut der Länder der Bundesrepublik Deutschland (FWU = Institut für Film und Bild in Wissenschaft und Unterricht) mit Microsoft geschlossen hat. Abgebildet wird „FWU“ bei Microsoft über das Lizenzprogramm „Open Value Subscription“. Bei „Open Value Subscription“ handelt es sich um Mietlizenzen.

Über FWU können Schulen und Schulträger die Lizenzierung von Windows und Office für eine einzelne oder auch alle Schulen abwickeln. Darüber hinaus bietet der Vertrag FWU 2.0 auch sehr umfangreiche Möglichkeiten mit Office365. Alle Lehrer und Schüler dürfen über den Student/Teacher Benefit das Produkt Office 2016 als Vollversion herunterladen und im Privatbereich an bis zu 15 verschiedenen Geräten einsetzen.

Jeder Microsoft AEP (Authorized Education Partner) kann Schulen und Schulträger in dieser Hinsicht beraten und die entsprechenden Verträge anbieten. Bitte wenden Sie sich bei Fragen dazu an Ihren LogoDIDACT-Partner.

III.6.2.3.2. Open License Vertrag

Der Großteil der Schulen verfügt bisher über keine entsprechenden Volumenlizenz-Verträge auf Mietbasis und somit auch nicht über einen KMS-Key. Viele Lizenzen wurden und werden noch immer auf Kaufbasis als Update oder Upgrade erworben. Speziell im Bereich von Windows wird das Betriebssystem im Zusammenhang mit dem Kauf von neuen Computern weiterhin als so genannte OEM-Lizenz mitgeliefert. Viele Schulen verfügen also sehr wohl über gültige Lizenzen für Windows 7 oder Windows 10, haben aber keinen KMS-Key für die Aktivierung. Diesen erhält man nur im Zusammenhang mit einem Volumenlizenzvertrag.

Die Vertragsart OPEN License bietet dabei den günstigsten Einstieg in das Volumenlizenzprogramm und wurde von SBE auch in der Vergangenheit schon immer empfohlen und verwendet, um die Aktivierung mit Volumenlizenzkeys vom Typ MAK durchzuführen.

Ein eigener individueller Open License Vertrag pro Schule hat viele Vorteile:

- er beinhaltet individuelle Produktkeys für Windows 7 und Windows 10
- die Aktivierung ist sicher, zuverlässig und einfach
- der Vertrag (nach obigem Schema) ist sehr günstig
- der Vertrag beinhaltet Keys vom Typ MAK und auf Anfrage auch KMS

Ein minimaler Open License Vertrag muss mindestens 5 Lizenzen eines Microsoft Produktes beinhalten. Da Sie Keys für Windows 10 benötigen, muss verständlicherweise mindestens ein Mal das Produkt Windows 10 enthalten sein, das es bei Open License schon immer (also auch bei Windows 7, Windows Vista oder Windows 8) nur als Upgrade-Lizenz gab.

Tabelle III.6.1. Minimaler Open License Vertrag mit 5 Lizenzen

Microsoft	Produkt	Menge
FQC-09512	Microsoft Windows 10 Pro Upgrade Open License Academic EDU Schulversion	1
R18-05089	WinSvrCAL 2016 ALNG OLP NL Acdmc Stdnt DvcCAL	4
Gesamtmenge an Lizenzen (min. 5 für Open License Vertrag)		5

Der Artikel R18-05089 wird nicht wirklich benötigt und es handelt sich dabei um "Fülllizenzen" oder "Dummylizenzen", deren Preis im Centbereich liegt und die lediglich benötigt werden, um die Mindestanzahl an 5 Lizenzen zu erreichen. Wenn Sie 5 oder mehr Upgrade-Lizenzen für Windows 10 benötigen, brauche Sie diese Fülllizenzen selbstverständlich nicht.

Sobald Sie über einen solchen Open License Vertrag verfügen, erhalten Sie darin zunächst "nur" Lizenzkeys vom Typ MAK für diverse Windows-Versionen.

The screenshot shows the Microsoft Volume Licensing Service Center interface. At the top, there are navigation tabs: Home, Lizenzen, Onlinedienstaktivierung, Downloads und Schlüssel, Software Assurance, Abonnements, Verwaltung, and Hilfe. Below this is the 'Lizenz-Details' section, which includes fields for 'Open License-Details', 'Status: Active', 'Organisation', 'Übergeordnetes Programm: OPEN S...', 'Startdatum: 2016-07-05', 'Ort', 'Visual Studio-Abonnements: klicken Sie hier', and 'Enddatum: 2018-07-31'. There are also buttons for 'Kontakte', 'Lizenzen', 'Product Keys', and 'Bestellbestätigungen'. Below the buttons is a 'Product Keys filtern' section with dropdown menus for 'Kategorie auswählen' and 'Wert auswählen', and a 'Los' button. At the bottom, there is a table of product keys with columns for 'Produkt', 'Product Key', 'Typ', 'MAK-Aktivierungen Verwendet/Verfügbar*', 'Arbeitsplätze', and 'Status'.

Produkt	Product Key	Typ	MAK-Aktivierungen Verwendet/Verfügbar*	Arbeitsplätze	Status
Win 7 - MAK	6	MAK	50/50		
Windows 10 Pro for Workstations MAK	K	MAK	0/50		
Windows 10 Pro for Workstations N/KN MAK	V	JG MAK	0/50		
Windows 10 Pro MAK	P	MAK	50/50		
Windows 10 Pro N/KN MAK	V	MAK	0/50		
Windows 10 S MAK	N	MAK	0/50		
Windows 10 S N MAK	T	D MAK	0/50		
Windows 8.1 MAK	D	D MAK	0/50		

Um auch einen KMS-Key für das jeweils eingesetzte Produkt zu erhalten, schreibt man eine entsprechende Mail an das Microsoft KMS Support Team (<kmsadd@messages.microsoft.com>).

III.6.3. Windows 10 KMS-Host mit LD Deploy aufsetzen

Um die Aktivierung von Windows und Office noch einfacher, schneller und zuverlässiger zu machen, wird in LogoDIDACT 2.0 mit **LD Deploy** eine virtuelle Maschine auf Basis von Windows 10 aufgesetzt. Dieser Rechner wird im Szenario der Produktaktivierung von Microsoft als KMS-Host bezeichnet.

III.6.3.1. Voraussetzungen

Damit eine virtuelle Maschine angelegt werden kann, muss der Hypervisor KVM aktiviert sein. Dies ist in Abschnitt III.3.10, „Virtuelle Maschinen mit KVM“ ausführlich beschrieben.

Eine lizenzrechtliche Voraussetzung für den Betrieb von Windows 10 in einer virtuellen Umgebung ist eine bestehende Softwarepflege (Software Assurance, kurz SA). Wenn Sie über einen Microsoft-Lizenzvertrag vom Typ FWU verfügen, dann beinhaltet dieser bereits die Software Assurance. Beim Open-License Vertrag, müssen Sie zusätzlich das Produkt Software Assurance für Windows 10 bestellen.

Tabelle III.6.2. Open License Vertrag mit 5 Lizenzen und Software Assurance für Windows 10

Microsoft	Produkt	Menge
FQC-09512	Microsoft Windows 10 Pro Upgrade Open License Academic EDU Schulversion	1
R18-05089	WinSvrCAL 2016 ALNG OLP NL Acdmc Stdnt DvcCAL	4
KW5-00363	Windows 10 Software Assurance OPEN-NL Academic	1

III.6.3.2. Windows 10 Professional 1903 für KMS bereitstellen

Für die Installation des KMS-Hosts wird ebenfalls die aktuellste Windows 10 Pro Version 19.03 als Ausgangsbasis verwendet. Falls Sie diese Version bereits für die Clients verwenden und heruntergeladen haben, können Sie diesen Schritt überspringen. Zum Herunterladen der Datei, wechseln Sie in den Container **deploy-g1** und dort in das Ziel-Verzeichnis für die Images:

```
lxc-attach -n deploy-g1
```

```
cd /var/lib/overlay/qBittorrent/
```

Laden Sie die `wim`-Datei herunter und die dazu passende Prüfsummendatei:

```
wget https://files.sbe.de/ld-deploy/win10pro1903.wim
```

```
wget https://files.sbe.de/ld-deploy/win10pro1903_sha512sum.txt
```



Achtung

Überprüfen Sie über den folgenden Befehl, ob die Prüfsumme der heruntergeladenen `wim`-Datei mit der MD5-Prüfsummendatei übereinstimmt:

```
sha512sum -c win10pro1903_sha512sum.txt
```

Wenn die Prüfsumme nicht übereinstimmt, löschen Sie die `wim`-Datei und laden diese erneut herunter.

Sofern die `wim`-Datei vollständig heruntergeladen wurde (Ausgabe `win10pro1903.wim: OK`), importieren Sie diese wie folgt:

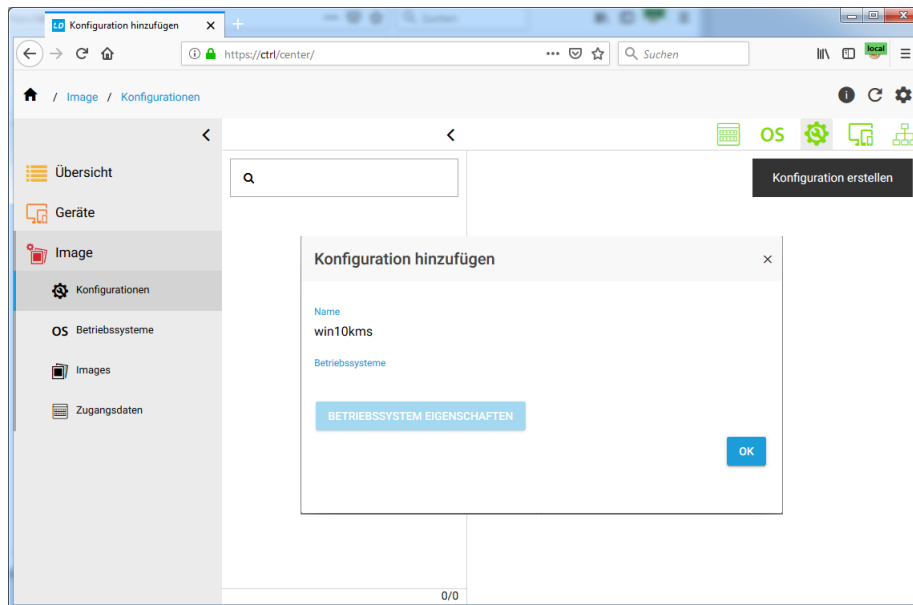
```
ld-control-client image add --description win10pro1903 --file win10pro1903.wim
```

Die `wim`-Datei wird in den Ordner `downloads` verschoben und sofern dieser noch nicht existiert wird er zuvor angelegt. Alle weiteren Schritte und Konfigurationsarbeiten erfolgen per Browser über das ControlCenter.

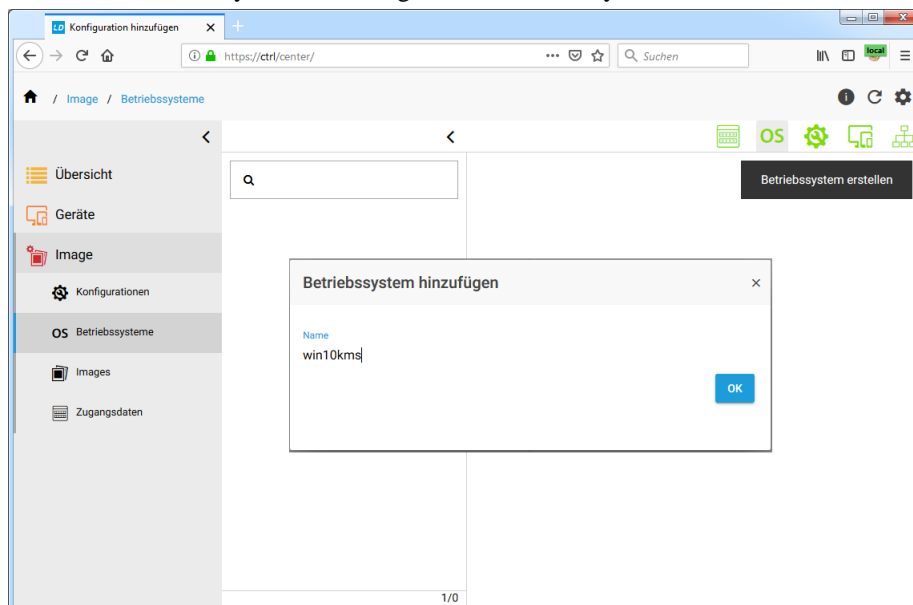
III.6.3.3. Eine win10kms Umgebung im Control-Center erstellen

Starten Sie das ControlCenter über einen Webbrowser `https://ctrl.schule.local/center` und melden Sie sich mit den Zugangsdaten des Benutzers **admin** an.

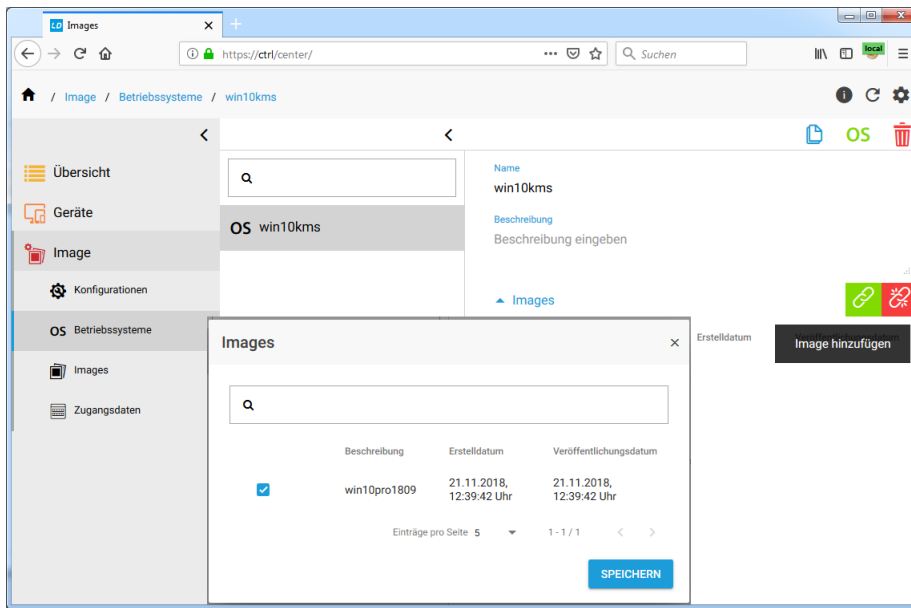
Wählen Sie den Menüeintrag **Konfigurationen** und klicken Sie auf das grüne Zahnrad-Symbol aus dem rechten oberen Symbol-Menü, um eine neue Konfiguration zu erstellen. Geben Sie dieser den Namen **win10kms**. Übernehmen Sie die Eingabe mit **OK**.



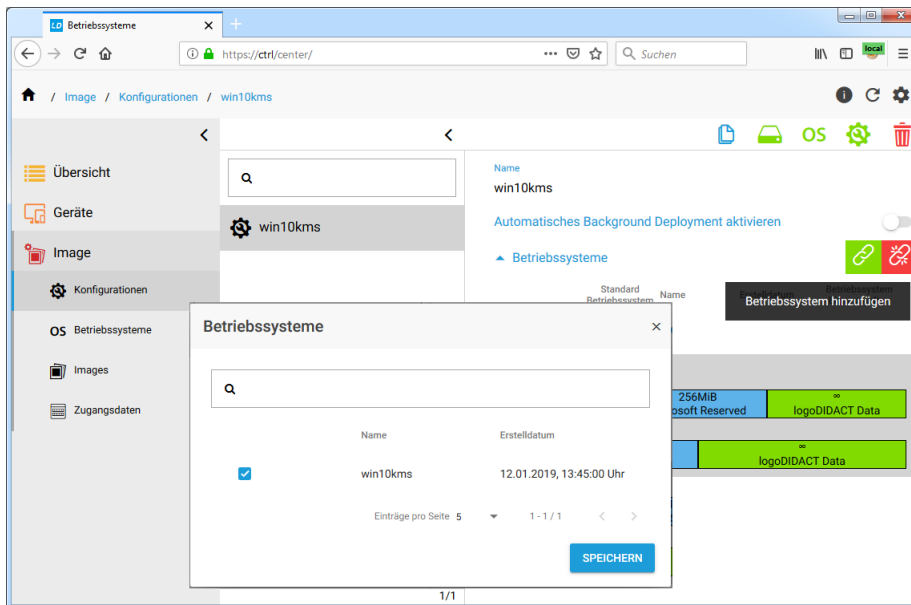
Wählen Sie im Hauptmenü den Eintrag **OS Betriebssysteme** und aus dem Symbolmenü im rechten oberen Bereich das Symbol **OS**. Vergeben Sie für das System den Namen **win10kms**.



Wählen Sie auf der linken Seite das gerade erstellte Betriebssystem **win10kms**. Verbinden Sie das System über das grüne Verknüpfungssymbol mit einem Image. Wählen Sie dazu das Image **win10pro1903**, das auch die Ausgangsbasis für alle anderen Arbeitsstationen darstellt. Schließen Sie die Zuweisung über **SPEICHERN** ab.



Wählen Sie den Menüeintrag **Konfigurationen** um die Partitionierung für die erstellte Konfiguration anzupassen. Markieren Sie auf der linken Seite das System **win10kms**. Verknüpfen Sie die Konfiguration über das grüne Verknüpfungssymbol auf der rechten Seite im Abschnitt Betriebssysteme mit dem zuvor erstellten Betriebssystem **win10kms**. Übernehmen Sie die Eingabe mit **SPEICHERN**.



III.6.3.4. Die Datenträgerverwaltung starten

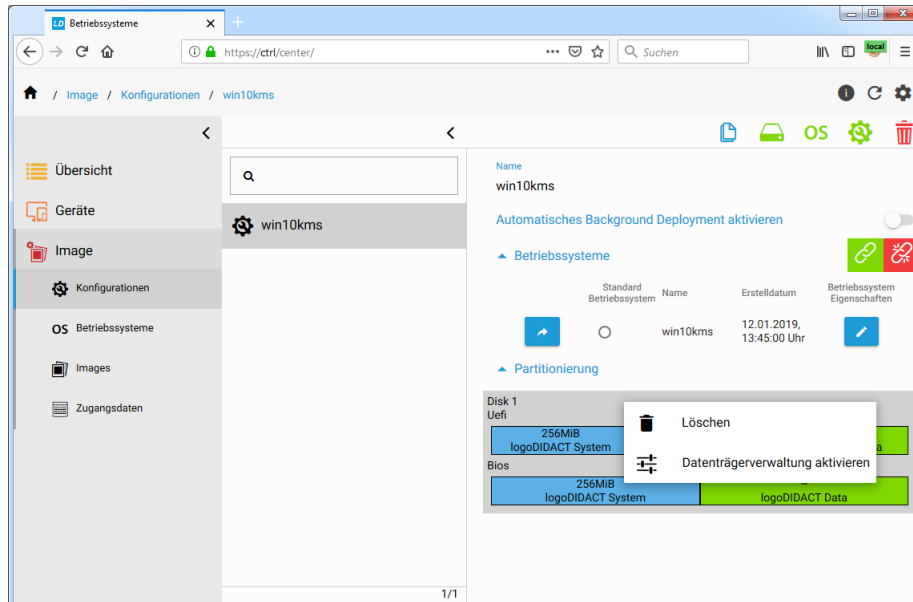
Die Verwaltung des Datenträgers ist immer dann notwendig, wenn spezielle Anpassungen vorgenommen werden sollen. Im Falle des KMS-Hosts soll das System nicht in eine virtuelle Partition gespielt werden, da es bereits vollvirtualisiert in einer KVM-Umgebung läuft. Ebenfalls soll es nicht "geheilt" betrieben werden, so dass das Betriebssystem über Windows-Updates immer auf einem aktuellen Stand gehalten werden kann.

Um die Datenträgerverwaltung zu starten, klicken Sie auf der rechten Seite mit der Maus auf eine Stelle des grau hinterlegten Bereiches im Abschnitt **Partitionierung**. Halten Sie die linke Maustaste so lange gedrückt, bis ein Auswahlménü mit dem Eintrag **Datenträgerverwaltung aktivieren** erscheint.



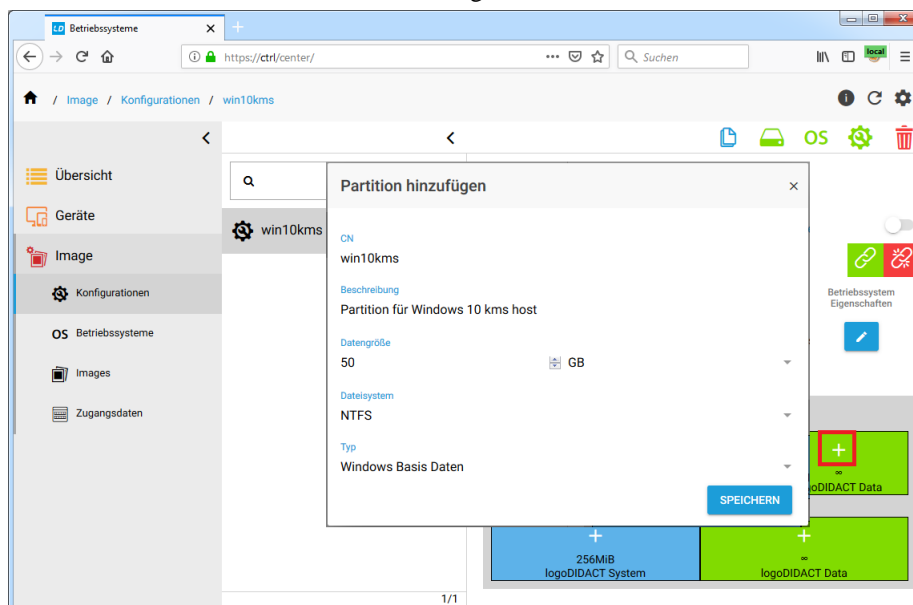
Achtung

Falls das Auswahlmü nicht erscheint, kann das an einem zu kleinen Browserfenster liegen. Maximieren Sie in diesem Fall das Fenster des Browsers.

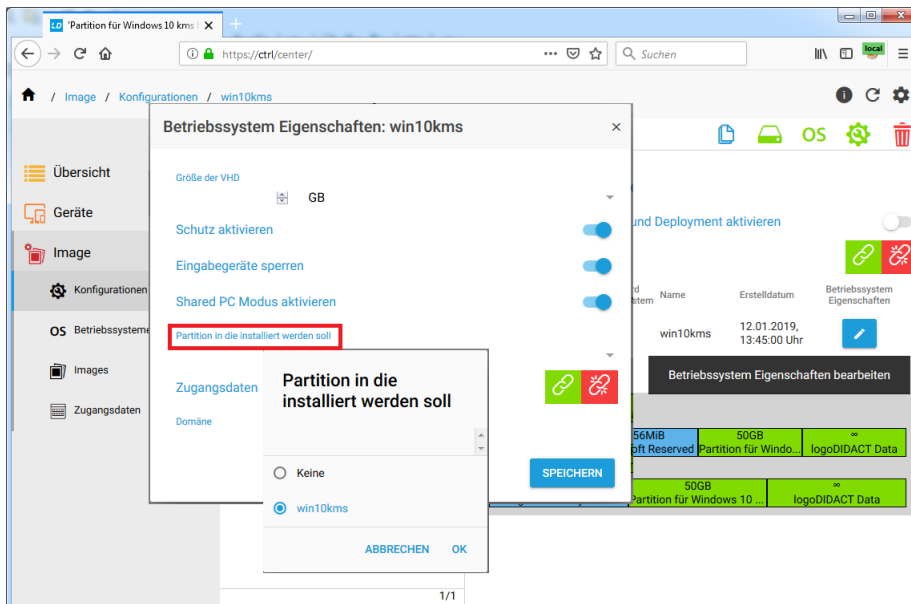


Wählen Sie den Eintrag **Datenträgerverwaltung aktivieren** aus.

Erstellen Sie dann eine neue Partition, durch Klick auf das + Symbol auf der grün hinterlegten Partition. Tragen Sie im Dialog die entsprechenden Werte ein, wie in der Abbildung dargestellt. Vergeben Sie zunächst einen Namen (CN) wie z.B. **win10kms** und eine Beschreibung. Die Partitiongröße muss mindestens 50 GB betragen und mit dem Dateisystem NTFS formatiert werden. Als Typ müssen Sie **Windows Basis Daten** wählen und alle Angaben dann über **SPEICHERN** übernehmen.

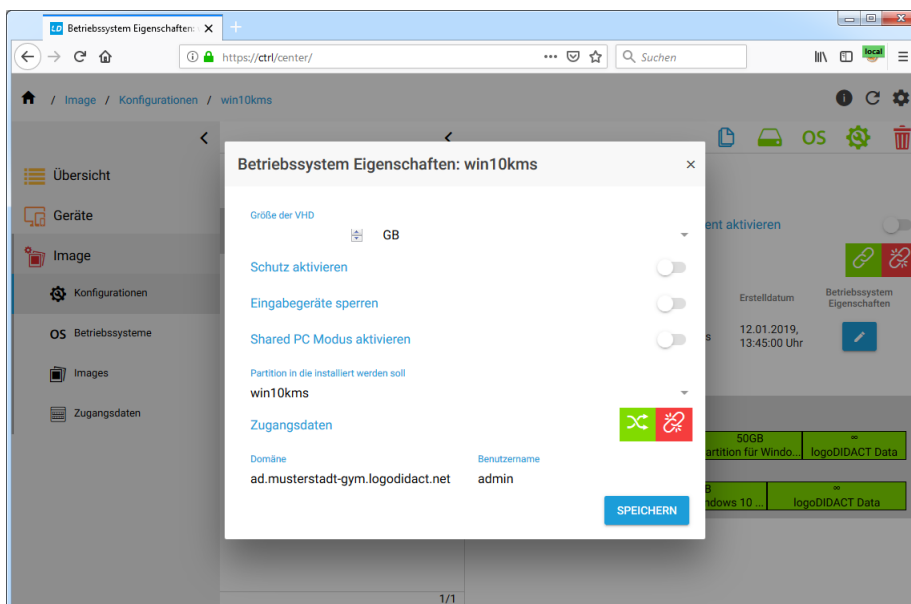


Legen Sie im nächsten Schritt fest, dass die eben erstellte Partition genutzt wird. Wählen Sie dazu rechts unten das blaue Editiersymbol. Klicken Sie auf den Eintrag **Partition in die installiert werden soll**, wählen Sie die zuvor erstellte Partition und übernehmen diese mit **OK**.



Deaktivieren Sie danach die drei Schieberegler mit den Optionen **Schutz deaktivieren**, **Eingabegeräte sperren** und **Shared PC Modus aktivieren**. Alle diese Optionen sind für den KMS-Host unnötig bzw. störend.

Verknüpfen Sie im letzten Schritt die Konfiguration für den KMS-Host mit den Zugangsdaten für die Domäne. Das ist zwingend erforderlich, damit man über diese virtuelle Maschine z.B. auch Gruppenrichtlinien setzen kann.

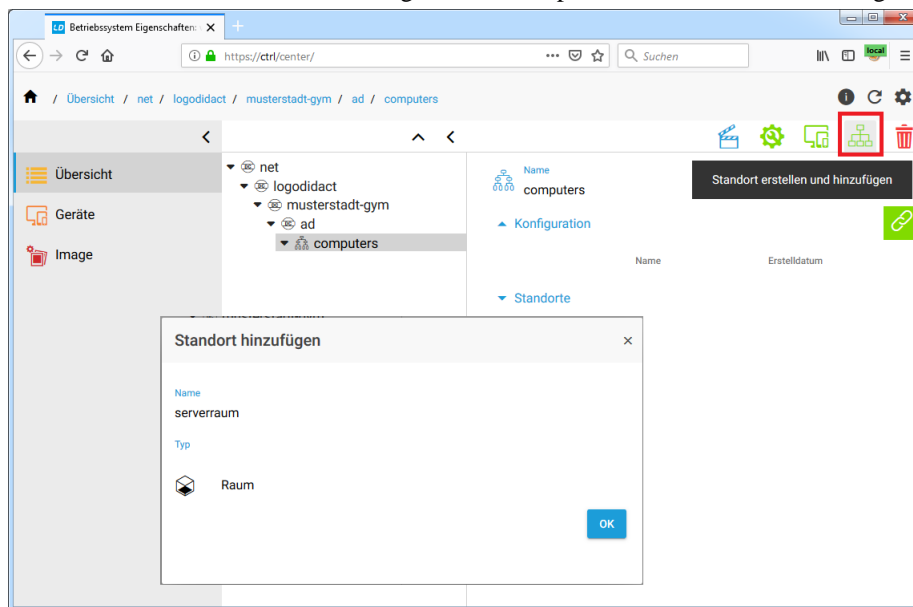


III.6.3.5. Virtuelle Maschine win10kms im Control Center eintragen

Bevor Sie die virtuelle Maschine starten, tragen Sie diese zunächst im Control-Center ein, damit der Rechner immer die gleiche IP-Adresse erhält und im Gesamtsystem per Name und IP bekannt ist.

Die MAC-Adresse der virtuellen Maschine win10kms ist ebenfalls virtuell und vom **Ldhost** aus in der XML-Datei `/etc/libvirt/qemu/win10kms-template.xml` definiert. Sie sollten diese nicht ändern, sondern können den Standardwert übernehmen: **52:54:00:5c:5f:d9**

Öffnen Sie das Control-Center und erstellen Sie zunächst einen Raum, wie z.B. **serverraum**, in dem sich der Server und der darauf virtualisierte kms-Host befindet. Wählen Sie dazu auf der linken Seite die Organisationseinheit (ou) **computers** und klicken Sie auf das grüne Symbol zum Anlegen von Standorten bzw. Strukturen. Vergeben Sie den passenden Namen und bestätigen Sie mit **OK**.



Navigieren Sie anschließend auf der linken Seite zum gerade erstellten Eintrag **serverraum** und erweitern Sie rechts unten dann die Symbolleiste über das blaue Pfeilsymbol. Klicken Sie dann auf das grüne Symbol zum Anlegen eines Gerätes.



Achtung

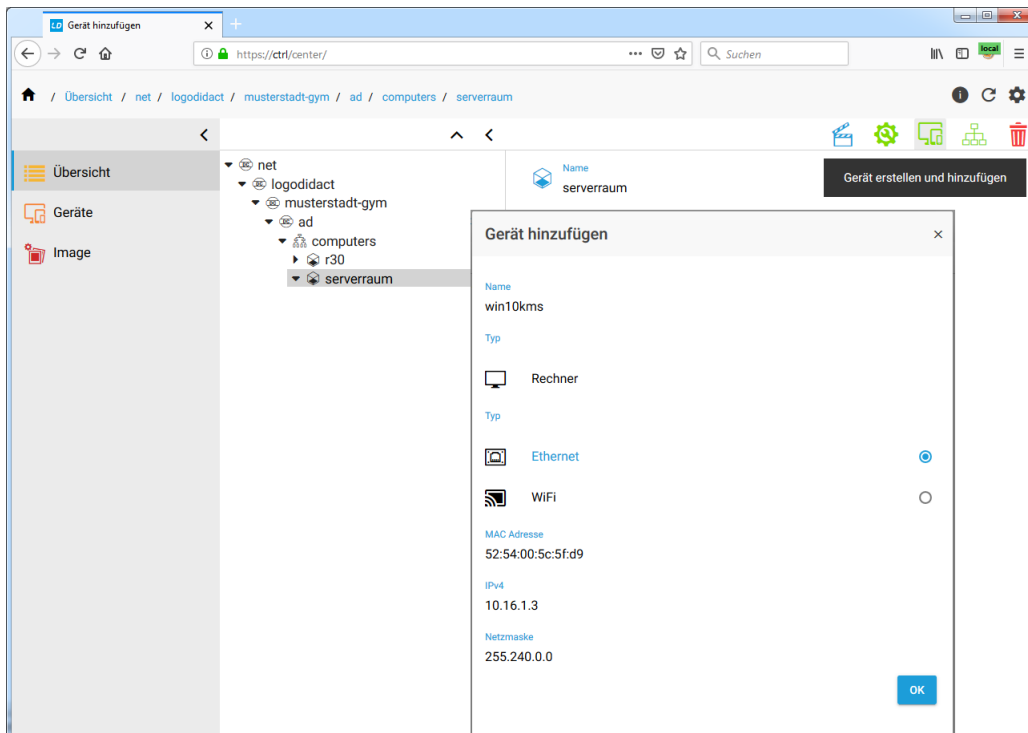
Es ist zwingend erforderlich, dass Sie die folgenden Daten für den KMS-Host verwenden:

Name: win10kms

MAC-Adresse: 52:54:00:5c:5f:d9

IPv4: 10.16.1.3

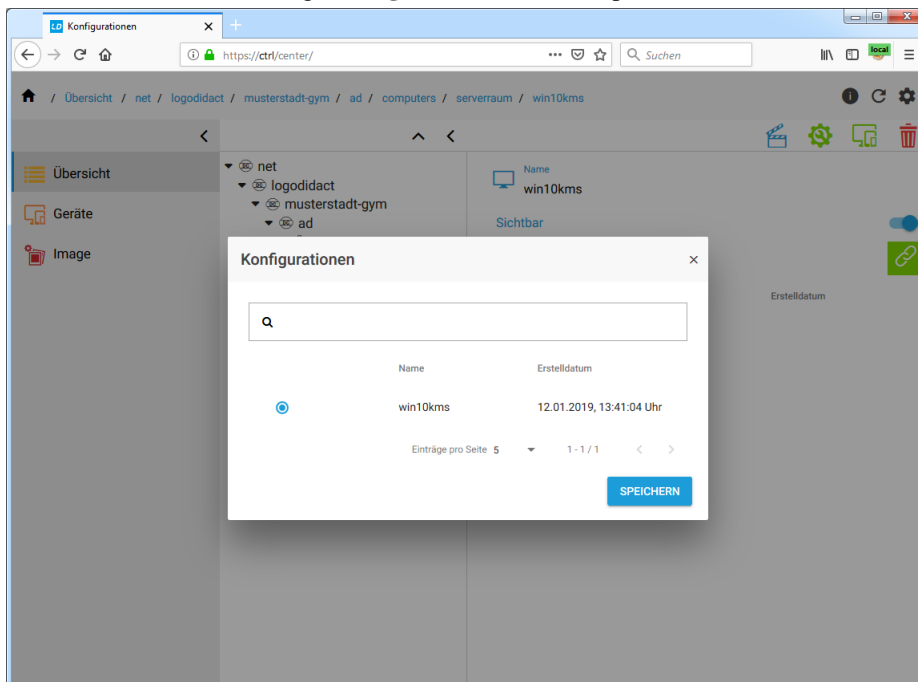
Netzmaske: 255.240.0.0



Damit die Einträge ins System übernommen werden, übernehmen Sie die Konfiguration mit **OK**.

III.6.3.6. Virtuelle Maschine win10kms mit Konfiguration verknüpfen

Im letzten Schritt verbinden Sie die vorher erstellte Konfiguration mit dem Rechner. Navigieren Sie dazu im linken Baum über den Eintrag **serverraum** zum Eintrag **win10kms**. Erweitern Sie auf der rechten Seite den Eintrag **Konfiguration** und verknüpfen Sie den Rechner mit **win10kms**.



III.6.3.7. Virtuelle Maschine aktivieren

Damit die virtuelle Maschine am Server installiert werden kann, muss zunächst eine leere `qcow2`-Datei am Server mit passender Größe erstellt angelegt werden.



Achtung

Die `qcow2`-Datei am Server muss verständlicherweise immer ein wenig größer sein, als die im ControlCenter festgelegte Partitionsgröße für das Betriebssystem.

Im Beispiel des KMS-Hosts mit seiner 50 GB Systempartition, wird die Größe der `qcow2`-Datei auf 55 GB festgelegt.

Wenn vom KMS-Host am Server per LD Deploy ein Image erstellt werden soll, muss die Größe der `qcow2` noch deutlich höher gewählt werden, weil das Image beim Erstellen zunächst lokal gespeichert werden muss, bevor es auf den Server geladen wird. Geben Sie der `qcow2`-Datei in diesem Fall eine Größe von 70 GB

Wechseln Sie im `ldhost` in das Verzeichnis, in dem die Images für die virtuellen Maschinen abgelegt werden:

```
cd /var/lib/libvirt/images/
```

```
qemu-img create -f qcow2 -o preallocation=full, lazy_refcounts=on win10kms.qcow2 70G
```

Das `preallocation=full` sorgt dafür, dass die Datei sofort den Speicherplatz vorreserviert und mit Zero-Bytes befüllt wird, was im Betrieb dann wiederum einen Performance-Boost in der KVM bewirkt.

Das Aktivieren der virtuellen Maschine erfolgt durch Import einer XML-Datei, in der die notwendigen Parameter für den KMS-Host definiert sind. In der XML-Datei sind sämtliche Infos enthalten, wie die virtuelle Maschine konfiguriert wird. Laden Sie die XML-Vorlagedatei über den folgenden Befehl von der SBE-Homepage herunter. Wechseln Sie auf dem `ldhost` in das Verzeichnis, in dem die Konfigurationsdateien der KVMs liegen müssen:

```
cd /etc/libvirt/qemu
```

Laden Sie dann die Vorlage-Datei herunter:

```
wget https://files.sbe.de/ld-deploy/win10kms-template.xml
```

Mit dem folgenden Befehl wird die virtuelle Maschine danach angelegt und dauerhaft (persistent) gemacht.

```
virsh define win10kms-template.xml
```

Löschen Sie die Vorlage-Datei wieder, damit es zu keinen Verwechslungen kommt, denn Sie benötigen diese nicht mehr:

```
rm win10kms-template.xml
```

Im Verzeichnis `/etc/libvirt/qemu` liegt nun nur die Datei `win10kms.xml`.

Mit dem folgenden Befehl sorgt man nochmals explizit dafür, dass die virtuelle Maschine mit dem Host gestartet wird.

```
virsh autostart win10kms
```

III.6.3.8. Virtuelle Maschine starten

Nachdem Sie den Namen und die IP-Adresse der VM festgelegt haben, können Sie diese vom **ldhost** aus über folgenden Befehl starten:

```
virsh start win10kms
```

Anschließend können Sie sich von einer Windows Arbeitstation per Remote Desktop darauf verbinden.

III.6.3.9. Die wichtigsten virsh Befehle

Hie eine kurze Zusammenfassung der wichtigsten virsh-Befehle und ihrer Bedeutung:

Befehl:	Bedeutung:
virsh list --all	Listet alle virtuellen Maschinen auf (laufende und abgeschaltete)
virsh destroy domain	Stoppt die virtuelle Maschine mit dem Namen domain (wird nicht sauber heruntergefahren, sondern "Stecker gezogen").
virsh shutdown domain	Führt die virtuelle Maschine mit dem Namen domain sauber herunter (funktioniert nur, wenn in der VM die virtio-Treiber installiert sind).
virsh reboot domain	Startet die virtuelle Maschine mit dem Namen domain neu (funktioniert nur, wenn in der VM die virtio-Treiber installiert sind).
virsh start domain	Startet die virtuelle Maschine mit dem Namen domain
virsh autostart domain	Sorgt dafür, dass die virtuelle Maschine mit dem Namen domain automatisch mit dem Hostsystem neu gestartet wird.
virsh define name.xml	Mit diesem Befehl legt man eine neue virtuelle Maschine an, deren Definition sich in der Datei name.xml befindet.
virsh edit domain	Ermöglicht die Änderung der Konfiguration einer virtuellen Maschine.



Achtung

Der Umgang mit virsh und KVM ist **nicht** Gegenstand des Supports. Bitte wenden Sie sich bei Unklarheiten oder Problemen an den Support des jeweiligen Herstellers.

III.6.3.10. Aufbau der virtuellen Maschine per Virt-Viewer beobachten

Die Installation der virtuellen Maschine am Server lässt sich über eine entsprechende Portweiterleitung und das Tool Virt-Viewer beobachten. Dieses kann auf der folgenden Seite heruntergeladen werden.

<https://virt-manager.org/download/>

Suchen Sie nach der Datei `virt-viewer-x64-7.0.msi`.

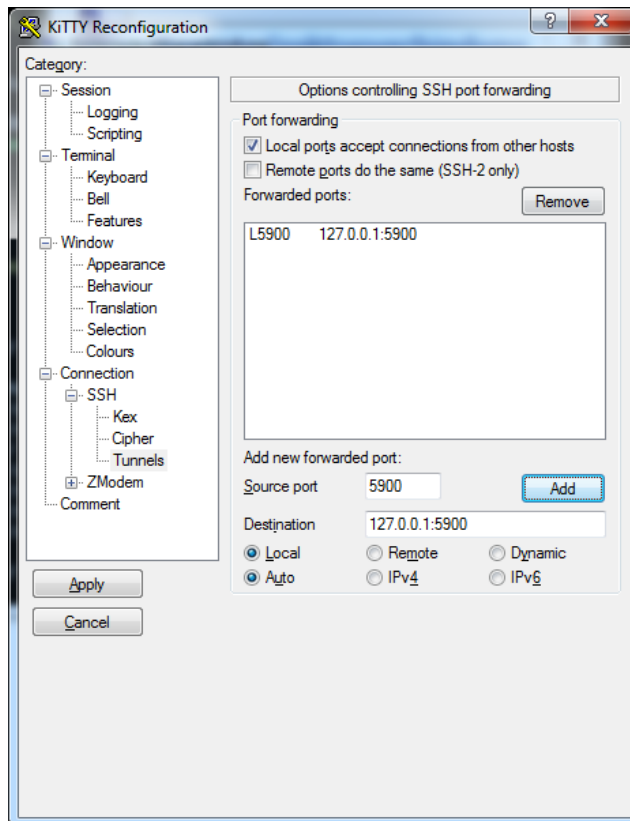
Um die Verbindung aufzubauen, sind zwei Informationen notwendig und wichtig:

1. Der Konsolenport am IHost wird pro gestarteter virtueller Maschine hochgezählt

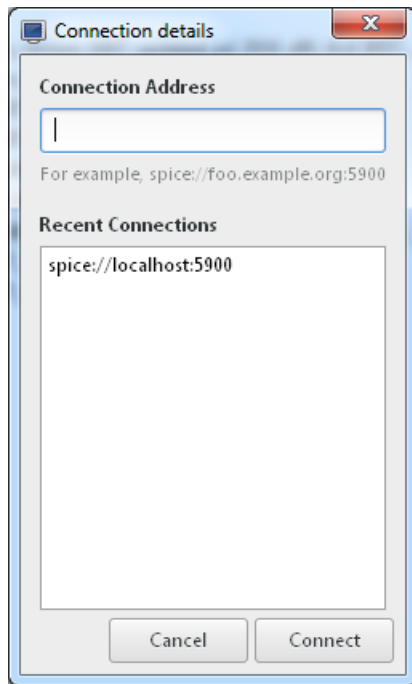
- VM #1 erhält TCP-Port 5900
- VM #2 erhält TCP-Port 5901
- usw.

2. In Putty muss man einen entsprechenden SSH Tunnel für den Fernzugriff definieren

Als Ziel wird immer 127.0.0.1 angeben, wohingegen der Zielport abhängig ist von der VM in Schritt 1



3. Im Virt-Viewer (Spice Remote Viewer) wird nach folgendem Schema die Zieladresse eingeben (siehe Recent Connections)



III.6.3.11. Tools installieren

Nachdem der Rechner neu gestartet wurde, melden Sie sich wieder mit dem Benutzer **admin** an der Domäne an.

Kopieren Sie den gesamten Ordnerinhalt `\\server\pgm\install\logoDIDACT Deploy \tools` lokal auf den KMS-Host ins Verzeichnis `C:\tools`.



Achtung

Der Umgang mit den verschiedenen Tools wird hier nicht im Detail erklärt und ist auch **nicht** Gegenstand des Supports. Bitte wenden Sie sich bei Unklarheiten oder Problemen an den Support des jeweiligen Herstellers bzw. bei Open Source Projekten an die Community und die einschlägigen Wikis.

Die Installation der Tools und deren Bedeutung wird hier deshalb nur kurz erläutert:

1. Virtio-Treiber

Diese Treiber sind notwendig, damit die Kommunikation zwischen Hostsystem und Windows funktioniert und die virtuelle Maschine herunterfährt oder neu startet, wenn das Wirtssystem herunterfährt bzw. neu startet.

Legen Sie die ISO-Datei `C:\Tools\KVM\virtio-windows-drivers-0.1.160` in ein virtuelles CD-Laufwerk. Unter Windows 10 reicht dazu normalerweise ein Doppelklick auf diese Datei.

Öffnen Sie den Gerätemanager und wählen Sie aus dem Menü **Aktion** den Eintrag **Treiber aktualisieren** aus.

Wählen Sie im nächsten Dialog **Auf dem Computer nach Treibersoftware suchen** und geben Sie danach als Ziel das durch Windows eingebundene CD-Laufwerk mit den Virtio-Treibern an. In unserem Beispiel ist das Laufwerk D:. Bestätigen Sie mit **OK** und **Weiter**.

Die Suche nach den Treibern liefert den VirtIO Balloon Driver. Wählen Sie **Installieren**.

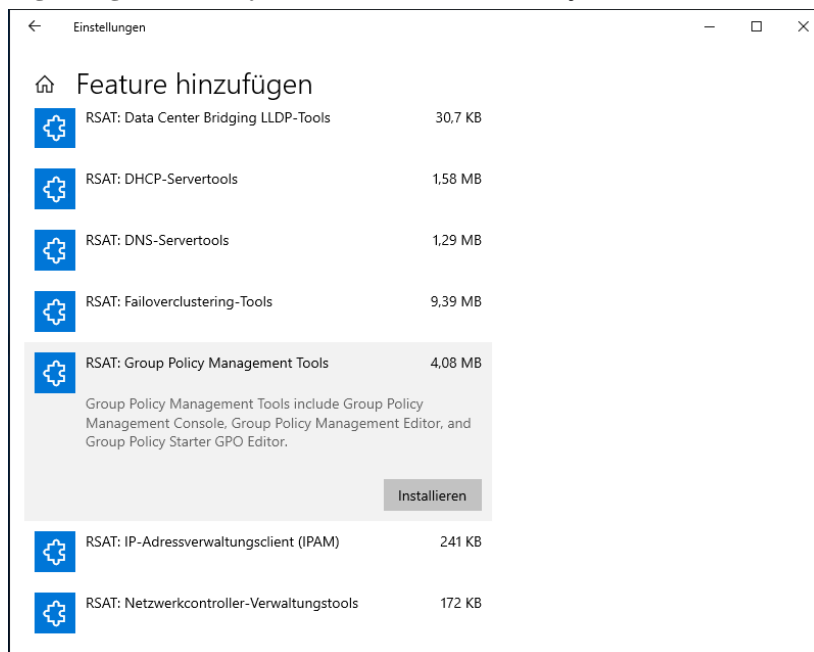
Führen Sie die Aktion für die zweite unbekannte Komponenten durch und installieren Sie auf diese Weise den VirtIO Serial Driver.

Ob die Kommunikation zwischen Hostsystem und der virtuellen Maschinen funktioniert, können Sie im **ldhost** prüfen, indem Sie dort den Befehl **virsh shutdown win10kms** eingeben und das Verhalten im Virt-Viewer oder per RemoteDesktop beobachten. Nachdem die Maschine sauber heruntergefahren wurde, können Sie diese auch wieder per **virsh start win10kms** starten.

2. Remote Server Administration Tools (RSAT)

Doppelklicken Sie auf die MSI-Datei `C:\Tools\KMS\RSAT_Windows_1803-x64` und installieren Sie Werkzeuge für die Serveradministration, wie z.B. den Gruppenrichtlinien-Editor und die Active Directory Benutzer- und Computer Verwaltung.

Alternativ können Sie auch gezielt nur die beiden Komponenten installieren, die wirklich notwendig sind. Wählen Sie aus dem Windows Hauptmenü das Zahrad-Symbol für **Einstellungen** und dort den Eintrag **Optionale Features verwalten**. Über **Feature hinzufügen** suchen Sie nach **RSAT: Group Policy Management Tools** und **RSAT: Tool für Active Directory Domain Services und Lightweight Directory Services**. Wählen Sie dabei jeweils die Schaltfläche **Installieren**.



Die Installation dauert eine Weile und findet ohne erkennbare Rückmeldung statt. Dass die Features installiert sind, erkennt man aber daran, dass diese in der Liste auftauchen oder auch am Link für den Verlauf. Ebenso natürlich, dass es Einträge im Hauptmenü von Windows unterhalb von **Windows-Verwaltungsprogramme** gibt.

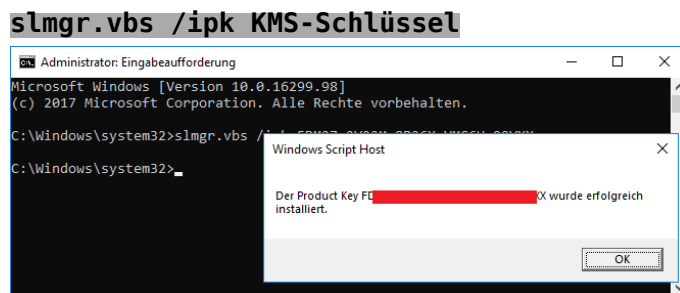
3. Gruppenrichtlinie für Netzlaufwerke aktivieren

Das Verbinden der Netzlaufwerke **H:**, **T:** und **P:** erfolgt für Windows 10 jetzt zusätzlich per Gruppenrichtlinie. Um diese Einstellungen nicht manuell über den Gruppenrichtlinie-Editor erstellen zu müssen, wird eine vordefinierte Richtlinie importiert.

Wechseln Sie in den Ordner `C:\Tools\GPO\ld-networkdrives`, markieren Sie dort die CMD-Datei `ld-networkdrives` und wählen Sie über die rechte Maustaste aus dem Kontextmenü den Eintrag **Als Administrator ausführen**.

III.6.3.12. Windows 10 Key am KMS-Host eingeben und aktivieren

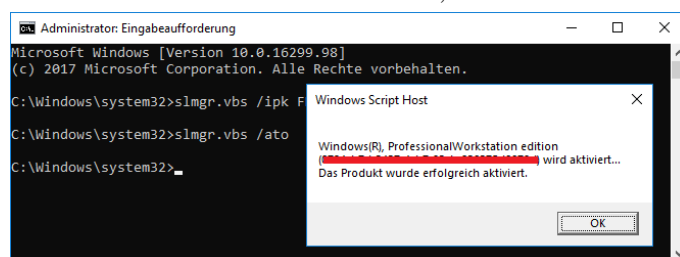
Durch das Installieren des KMS-Schlüssels unter Windows 10 wird der Computer zum KMS-Host. Öffnen Sie dazu eine Eingabeaufforderung mit erhöhten Rechten (als Administrator ausführen). Zum Installieren des KMS-Schlüssels geben Sie den folgenden Befehl ein, wobei Sie für **KMS-Schlüssel** die Daten des KMS-Keys aus Ihrem Volumenlizenzvertrag angeben.



Über die Eingabe des KMS-Schlüssels erfolgt zunächst auch die Aktivierung des Windows 10 Hosts selbst. Anschliessend wird die Onlineaktivierung des Rechners zum KMS-Host über folgenden Befehl gestartet:

slmgr.vbs /ato

Sofern der Rechner ins Internet kommt, kann auch der KMS-Host aktiviert werden.



III.6.3.13. Probleme mit KMS-Keys und mögliche Ursachen

Das gesamte Thema Microsoft Produktaktivierung hat mit LogoDIDACT wenig bis nichts zu tun, wird aber immer wieder zum Gegenstand von Support-Anfragen. Bitte beachten Sie deshalb die folgenden Einschränkungen und sich daraus ergebenden Probleme.

1. Der gleiche **KMS-Schlüssel** kann bis zu 10 Mal auf bis zu 6 verschiedenen Computern zur Aktivierung des **kms-Host** eingesetzt werden.
2. Die Anzahl der Aktivierungen wird dabei bei Microsoft über einen Online-Dienst gezählt.
3. Bei jedem Funktions-Upgrade von Windows 10 auf dem **kms-Host** geht die KMS-Funktionalität verloren und wird "zerstört".

Microsoft wirft dabei den KMS-Key aus dem System und ersetzt diesen durch einen GVLK-Key. Dies ist kein Fehler von LogoDIDACT!

4. Nach jedem Funktions-Upgrade von Windows 10 auf dem **kms-Host** muss die KMS-Funktionalität neu eingerichtet und über den **KMS-Schlüssel** neu aktiviert werden.
5. Der Lizenzzähler wird also durch jedes Funktions-Upgrade beeinflusst.
6. Wird die maximale Anzahl an Aktivierungen erreicht, erhält man den Fehlercode 0xC004C008

Ausführliche Informationen zu den Fehlercodes im Zusammenhang mit der Produktaktivierung finden Sie hier:

<https://docs.microsoft.com/en-us/windows-server/get-started/activation-error-codes>



Achtung

Bei Problemen mit der Produktaktivierung wenden Sie sich an Ihren Microsoft-Partner oder direkt an Microsoft!

III.6.3.14. Office Volume License Pack installieren

Die Aktivierung der Microsoft-Produkte aus dem Office-Paket erfolgt ähnlich, wie für Windows 10, erfordert aber einige zusätzliche Schritte.

Installieren Sie zunächst das Office Volume License Pack für die eingesetzte Office-Version. Wenn Sie der obigen Anleitung gefolgt sind, finden Sie diese im Ordner C:\Tools\KMS für Office 2010, Office 2013, Office 2016 und Office 2019.

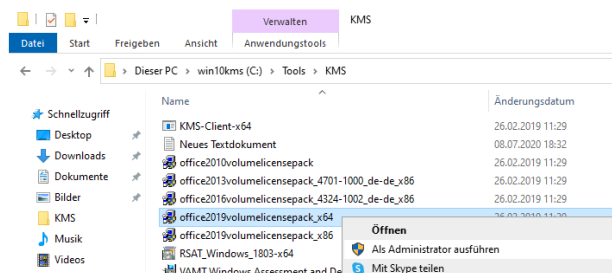
Klicken Sie die gewünschte Version mit der rechten Maustaste an und wählen Sie aus dem Kontextmenü **Als Administrator ausführen**.



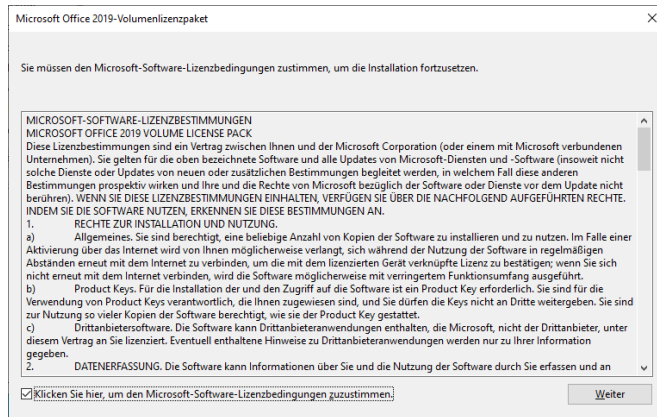
Achtung

Im Gegensatz zur Aktivierung von Windows, wo der Windows 10 KMS-Key auch ältere Windows-Versionen wie z.B. Windows 7 auf Clientseite aktiviert, gilt das für Office nicht!

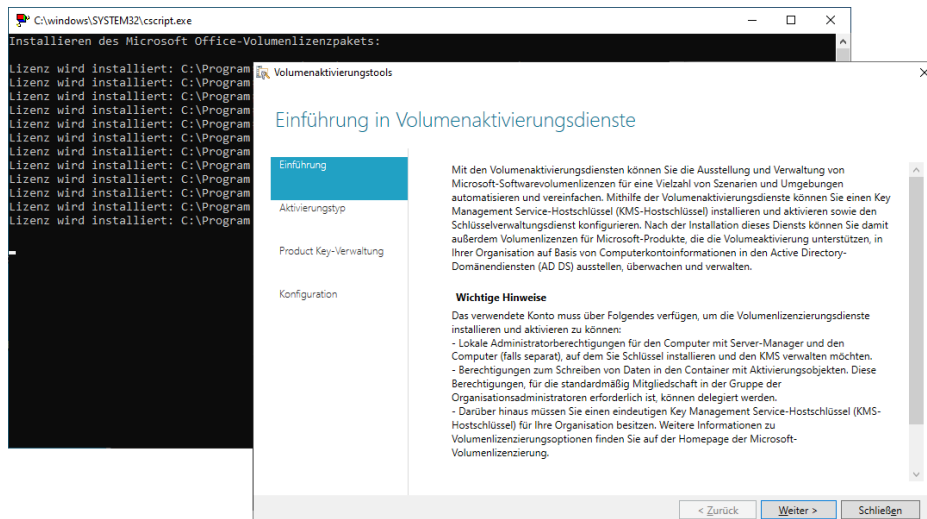
Sie benötigen für jede Office-Version am Client sowohl das spezifische Volume License Pack am KMS-Host, als auch den dazu passenden Office KMS-Key.



Akzeptieren Sie die Lizenzbedingungen und fahren Sie fort mit **Weiter**.



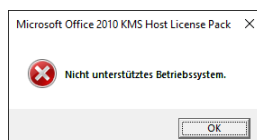
Warten Sie bis der Dialog des Volumenaktivierungstools startet und wählen Sie **Weiter**.



Diese Methode funktioniert für Office 2013, Office 2016 und Office 2019 und Sie können den Dialog fortführen und den Key über das Volumenaktivierungstool eingeben, wie im nächsten Abschnitt beschrieben. Alternativ können Sie die graphische Variante über **Schließen** beenden und alles weitere per Kommandozeile erledigen, wie im übernächsten Abschnitt dokumentiert.

III.6.3.14.1. Volume License Pack für Office 2010 installieren

Bei der Installation des Volume License Pack Office 2010 unter Windows 10 erhalten Sie nach kurzer Zeit eine entsprechende Fehlermeldung.

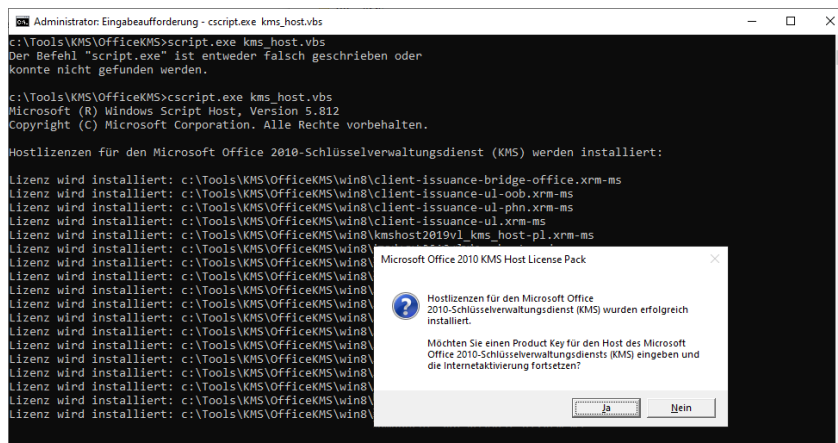


Dieses alte License Pack wird von Microsoft offiziell nicht für Windows 10 unterstützt, lässt sich aber über Umwege trotzdem noch einsetzen. Kopieren Sie dazu auf dem KMS-Host den Ordner C:\Programme (x86)\MSECache\OfficeKMS nach C:\Tools\KMS\OfficeKMS.

Laden Sie anschließend eine für Windows 10 angepasste Version des Visual-Basic-Scripts herunter und speichern Sie diese im kopierten Verzeichnis ab: https://files.sbe.de/ld-deploy/kms_host.vbs

Öffnen Sie eine Kommandozeile mit erhöhten administrativen Rechten, wechseln in das kopierte Verzeichnis und führen folgenden Befehl aus:

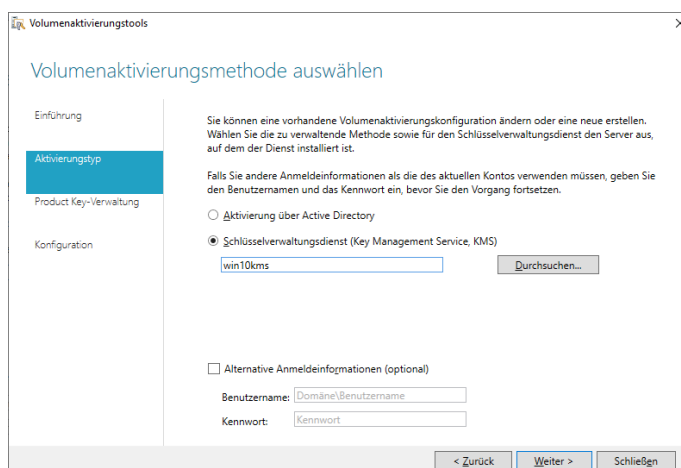
cscript.exe kms_host.vbs



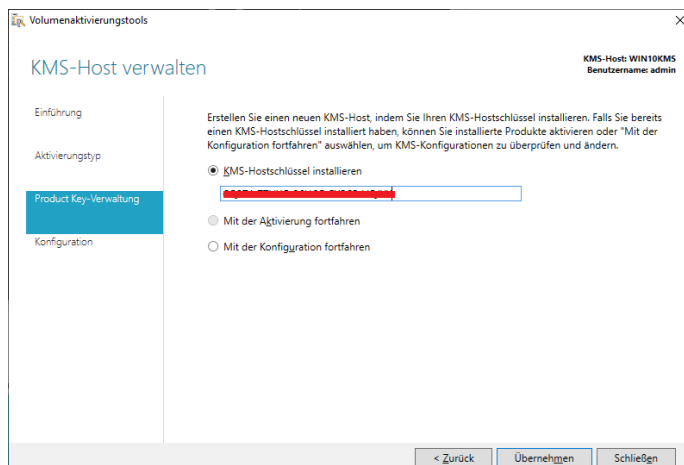
Auch hier können Sie graphisch fortfahren oder per Kommandozeile, wie weiter unten beschrieben.

III.6.3.15. Office Key über Volumenaktivierungstool eingeben und aktivieren

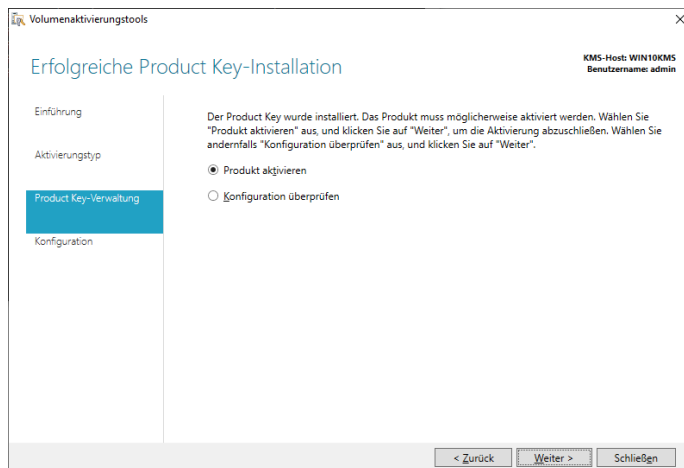
Geben Sie als Namen für den Schlüsselverwaltungsdienst den KMS-Host an, in unserem Fall **win10kms**.



Tragen Sie den KMS-Key ein und beachten Sie, dass er zu dem gestarteten License-Pack passen muss (im Beispiel für Office 2019). Klicken Sie auf **Übernehmen**, damit der Produktkey installiert wird.



Führen Sie anschließend die Aktivierung durch, indem Sie die Auswahl **Produkt aktivieren** übernehmen und mit **Weiter** fortfahren.



Übernehmen Sie die Aktivierung online und beachten Sie, dass der Internetzugang dazu offen sein muss. Deaktivieren Sie gegebenenfalls Filter oder Portsperrern und wenden Sie sich bei Problemen an ihren Administrator.



Achtung

Aktivierungsprobleme zwischen KMS-Host und der Microsoft-Infrastruktur haben nichts mit LogoDIDACT zu tun und sind nicht Gegenstand des Supports. Bitte wenden Sie sich bei Problemen an die Microsoft-Hotline!

Wählen Sie **Übernehmen**.

Office Key über Volumenaktivierungstool eingeben und aktivieren

Produkt aktivieren

KMS-Host: WIN10KMS
Benutzername: admin

Einführung

Aktivierungstyp

Produkt Key-Verwaltung

Konfiguration

Aktivieren Sie den Key Management Service-Hostschlüssel (KMS-Hostschlüssel). Ein KMS-Hostschlüssel muss vor der Verwendung zunächst aktiviert werden. Wählen Sie das Softwareprodukt aus, das aktiviert werden soll. Wählen Sie anschließend ggf. die Aktivierungsmethode und den Ort aus.

Produkt auswählen
Office 19, VOLUME_KMS channel

Online aktivieren
 Telefonisch aktivieren

Standort auswählen
Afghanistan

< Zurück Übernehmen Schließen

Sofern die Aktivierung erfolgreich war, erhalten Sie eine entsprechende Übersicht und können fortfahren mit **Weiter**.

Erfolgreiche Aktivierung

KMS-Host: WIN10KMS
Benutzername: admin

Einführung

Aktivierungstyp

Produkt Key-Verwaltung

Konfiguration

Dies sind die aktuellen KMS-Konfigurationsoptionen. Klicken Sie zum Ändern der KMS-Konfiguration auf "Weiter". Klicken Sie zum Akzeptieren dieser Konfiguration auf "Schließen".

Name: Windows(R) Operating System, VOLUME_KMS_W10 channel
SKU-ID: 0724cb7d-3437-4cb7-93cb-830375d0079d
App-ID: 55c92734-d682-4d71-983e-d6ec3f16059f
Lizenzierungsstatus: Lizenziert

Name: Office 19, VOLUME_KMS channel
SKU-ID: 70512334-47b4-44db-a233-be5ea33b914c
App-ID: Office15-a989-479d-af46-f275c6370663
Lizenzierungsstatus: Lizenziert

Konfiguration

Intervall der Volumenlizenzaktivierung: 2 Stunden
Intervall der Volumenlizenzerneuerung: 7 Tage

KMS-TCP-Überwachungsport: 1688
KMS-Firewallausnahmen: Privat: [] Öffentlich: []
DNS-Informationen veröffentlichen: [x]

In benutzerdefinierten DNS-Zonen veröffentlichen:

< Zurück Weiter > Schließen

Falls noch nicht anderweitig per LD Deploy angepasst, wird über den folgenden Schritt dafür gesorgt, dass entsprechende Firewall-Regeln erstellt werden und der KMS-Host über die die vorgesehenen Ports erreicht werden kann. Klicken Sie auf **Übernehmen**.

Optionen des Schlüsselverwaltungsdiensts konfigurieren

KMS-Host: WIN10KMS
Benutzername: admin

Einführung

Aktivierungstyp

Produkt Key-Verwaltung

Konfiguration

Die KMS-Konfigurationsoptionen bestimmen die Leistung und die Erkennbarkeit des KMS-Hosts. Bearbeiten Sie zum Ändern der Konfiguration die Felder unten, und klicken Sie auf "Übernehmen". Klicken Sie zum Akzeptieren der aktuellen Konfiguration auf "Abbrechen". Weitere Informationen zum Konfigurieren der KMS-Optionen finden Sie in der QuickInfo oder der Hilfe zur Volumenaktivierung.

Intervall der Volumenlizenzaktivierung (St): 2

Intervall der Volumenlizenzerneuerung (T): 7

KMS-TCP-Überwachungsport: 1688

KMS-Firewallausnahmen: Privat Domäne Öffentlich

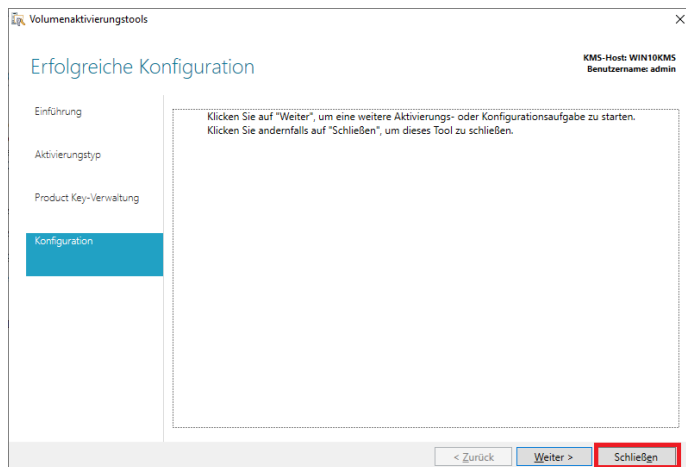
DNS-Datensätze: Veröffentlichen

In benutzerdefinierten DNS-Zonen veröffli:

Hinzufügen... Entfernen...
Wiederherstellen

< Zurück Übernehmen Abbrechen

Damit ist der KMS-Key für Office 2019 am KMS-Host erfolgreich installiert und aktiviert. Beenden Sie mit **Schließen**.



III.6.3.16. Office KMS-Key per Kommandozeile einspielen und aktivieren

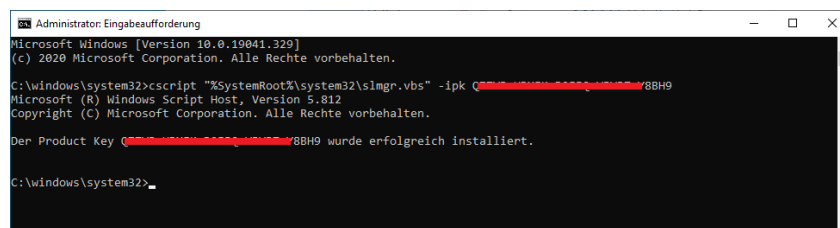
Alternativ zur graphischen Variante, gibt es auch eine verkürzte Möglichkeit auf Ebene der Kommandozeile:

1. Das passende Office License Pack installieren

Als Administrator ausführen (wie oben dargestellt), dann aber den graphischen Dialog abbrechen.

2. **cmd.exe** als Administrator ausführen
3. Produktkey installieren

```
cscript "%SystemRoot%\system32\slmgr.vbs" -ipk [PRODUKT-KEY]
```



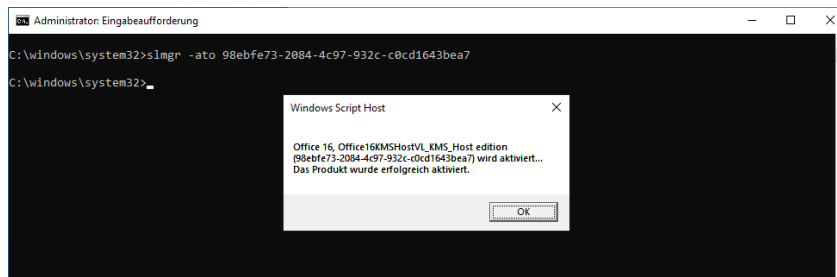
4. Produktkey aktivieren

```
slmgr -ato [Aktivierungs-ID]
```

Für jede Office-Version gibt es eine spezielle Aktivierungs-ID:

```
slmgr -ato bfe7a195-4f8f-4f0b-a622-cf13c7d16864 # MS Office 2010
slmgr -ato 2e28138a-847f-42bc-9752-61b03fff33cd # MS Office 2013
slmgr -ato 98ebfe73-2084-4c97-932c-c0cd1643bea7 # MS Office 2016
slmgr -ato 70512334-47b4-44db-a233-be5ea33b914c # MS Office 2019
```

Ohne Angabe einer Aktivierungs-ID für ein spezielles Produkt, erfolgt diese für Windows. Im folgenden Screenshot ist die Aktivierung beispielhaft für Office 2016 und der entsprechenden ID dargestellt.



III.6.3.17. KMS-Client-Emulator starten und Aktivierung prüfen

Wie in der Einführung beschrieben, gibt es beim Einsatz des Microsoft KMS-Servers einige technische und lizenzrechtliche Dinge zu beachten, die in der Praxis durchaus schwierig sein können. Auf technischer Ebene ist es leider so, dass der KMS-Server mit seiner Aktivierung für Windows-Clients real erst dann beginnt, wenn 25 Anfragen von Arbeitsstationen vorliegen. Das bedeutet, dass man an einer kleinen Grundschule mit weniger als 25 Computern mit Windows 10 diese Schwelle oftmals gar nicht erreicht.

Es wäre nun technisch möglich, dass man verschiedene KMS-Server über einen zentralen KMS-Server im Internet verbindet und hierbei mehrere kleine Schulen in der technischen Aktivierung zusammenfasst. Abgesehen davon, dass dies einen zusätzlichen technischen Aufwand darstellt und das Risiko von Fehllizenzierungen nicht unbedingt verringert, ist auch diese Zusammenfassung mehrerer Kunden lizenzrechtlich nicht "sauber".

Um Fehlaktivierungen zu vermeiden und gleichzeitig die Funktionsfähigkeit der KMS-Aktivierung bereits beim ersten Client überprüfen zu können, dient ein KMS-Client-Emulator. Dass es Situationen gibt, in denen man auf ein solches Tool zurückgreifen muss, ist Microsoft bekannt und wird "toleriert". Eine schriftliche Aussage dazu gibt es verständlicherweise nicht.



Achtung

Um hier Missverständnisse zu vermeiden, sei darauf hingewiesen, dass es solche "Graubereiche" sehr häufig gibt und man selbstverständlich das Lizenzrecht einhalten muss. Dies war auch in der Vergangenheit beim Thema MAK so und ist es auch bei KMS und wird von allen LogoDIDACT Kunden so verstanden und eingehalten.

Der KMS-Client-Emulator entstammt folgendem Git-Projekt <https://github.com/kkkgo/vlmcsd>.

Download für **win10kms**:

<https://files.sbe.de/ld-deploy/vlmcs-Windows-x64.exe>

Kopieren Sie das Tool auf den KMS-Host ins Verzeichnis: `C:\Tools\KMS\`. Öffnen Sie die Kommandozeile mit erhöhten administrativen Rechten. Über die folgenden Befehl können Sie ermitteln, welche Produkte unterstützt werden und welche Parameter Sie für das jeweilige Produkt angeben müssen.

```
vlmcs-Windows-x64.exe -x
```

Die wichtigsten Produkte und IDs sind:

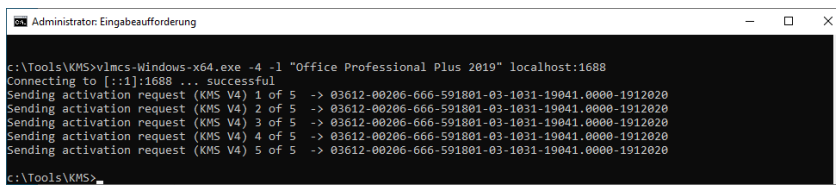
Tabelle III.6.3.

Name	ID
Windows 10 Education	18
Windows 10 Professional	26
Office Professional Plus 2019	194
Office Professional Plus 2016	174
Office Professional Plus 2013	143
Office Professional Plus 2010	125

Um z.B. die Aktivierung von Office 2019 gegen den KMS-Host anzutriggern, ist der folgende Befehl notwendig.

```
vlmcs-Windows-x64.exe 127.0.0.1:1688 -l "Office Professional Plus 2019"
```

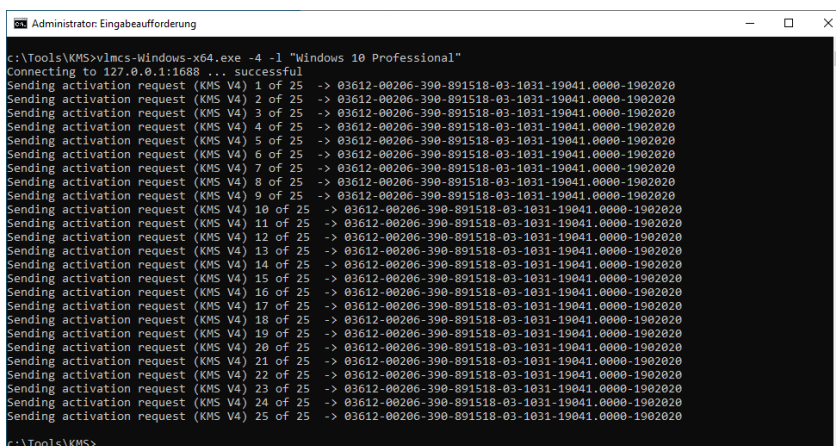
Der Emulator erzeugt dann für das jeweilige Produkt die entsprechende Anzahl an Anfragen (bei Microsoft Office 5, bei Windows 25) beim KMS-Host, so dass die Aktivierungsschwelle erreicht wird und dieser mit seiner Aktivierung beginnt.



```
Administrator: Eingabeaufforderung
c:\Tools\KMS>vlmcs-Windows-x64.exe -4 -l "Office Professional Plus 2019" localhost:1688
Connecting to [::1]:1688 ... successful
Sending activation request (KMS V4) 1 of 5 -> 03612-00206-666-591801-03-1031-19041.0000-1912020
Sending activation request (KMS V4) 2 of 5 -> 03612-00206-666-591801-03-1031-19041.0000-1912020
Sending activation request (KMS V4) 3 of 5 -> 03612-00206-666-591801-03-1031-19041.0000-1912020
Sending activation request (KMS V4) 4 of 5 -> 03612-00206-666-591801-03-1031-19041.0000-1912020
Sending activation request (KMS V4) 5 of 5 -> 03612-00206-666-591801-03-1031-19041.0000-1912020
c:\Tools\KMS>
```

Für die Aktivierung von Windows 10 Professional lautet der Befehl wie folgt:

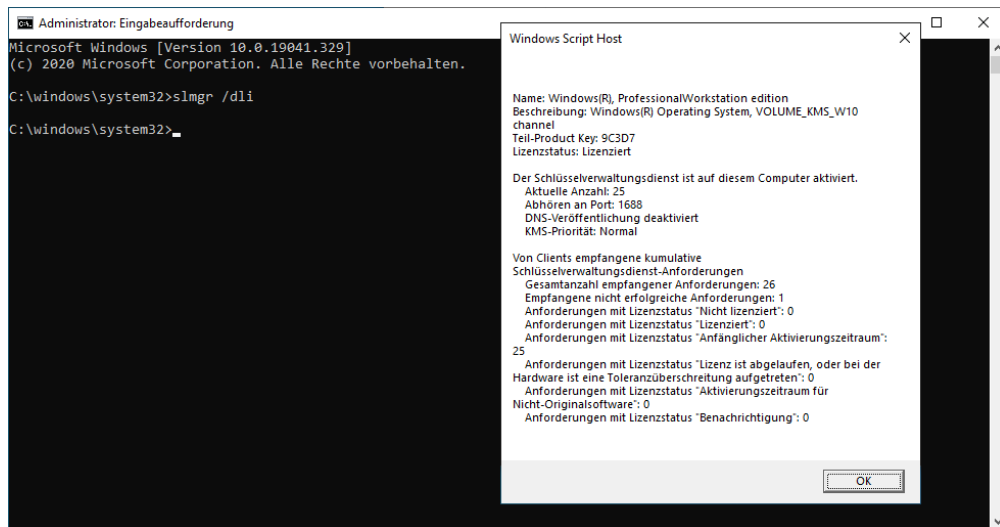
```
vlmcs-Windows-x64.exe 127.0.0.1:1688 -l "Windows 10 Professional"
```



```
Administrator: Eingabeaufforderung
c:\Tools\KMS>vlmcs-Windows-x64.exe -4 -l "Windows 10 Professional"
Connecting to 127.0.0.1:1688 ... successful
Sending activation request (KMS V4) 1 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 2 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 3 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 4 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 5 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 6 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 7 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 8 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 9 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 10 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 11 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 12 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 13 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 14 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 15 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 16 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 17 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 18 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 19 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 20 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 21 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 22 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 23 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 24 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
Sending activation request (KMS V4) 25 of 25 -> 03612-00206-390-891518-03-1031-19041.0000-1902020
c:\Tools\KMS>
```

Anschließend kann die Aktivierung des KMS-Hosts geprüft werden:

```
slmgr.vbs /dli
```



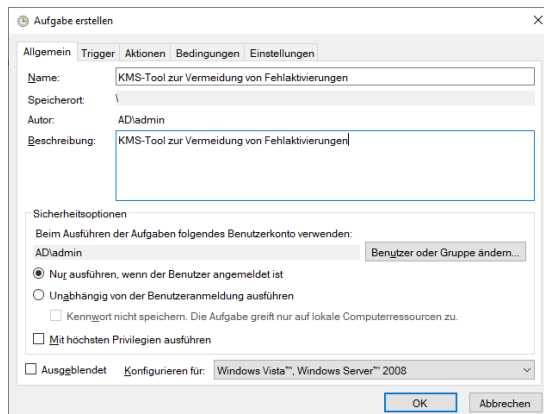
Mit dem einmaligen Ausführen des Client-Emulators sorgen Sie dafür, dass der Microsoft-KMS-Server die Aktivierungsanfragen sofort und am Client bzw. dem Produkt sichtbar und prüfbar beantwortet.

Um im laufenden Betrieb Fehlaktivierungen zu vermeiden, ist es zwingend erforderlich, den Emulator wiederkehrend auszuführen, damit der KMS-Host immer an der Aktivierungsschwelle arbeitet.

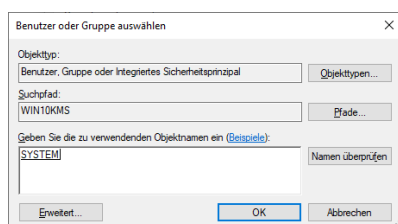
III.6.3.18. Emulator wiederkehrend als Aufgabe ausführen

Um Fehlaktivierungen zu vermeiden, sollte das Tool zur Vermeidung von Fehlaktivierungen zyklisch ausgeführt werden. Starten Sie dazu auf dem KMS-Host über **Windows Verwaltungsprogramme** die Aufgabenplanung und wählen Sie aus dem Kontextmenü **Neue Aufgabe erstellen...**

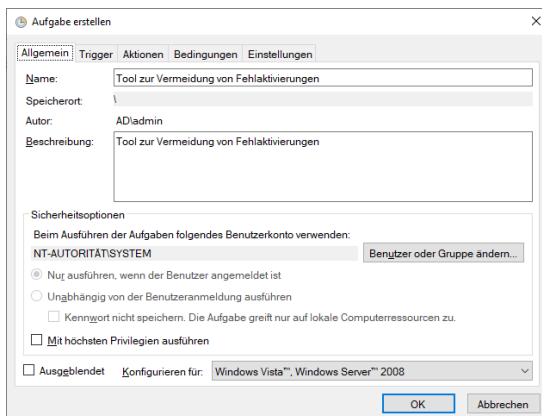
Geben Sie der Aufgabe eine aussagekräftige Bezeichnung und klicken danach auf **Benutzer oder Gruppe ändern...**



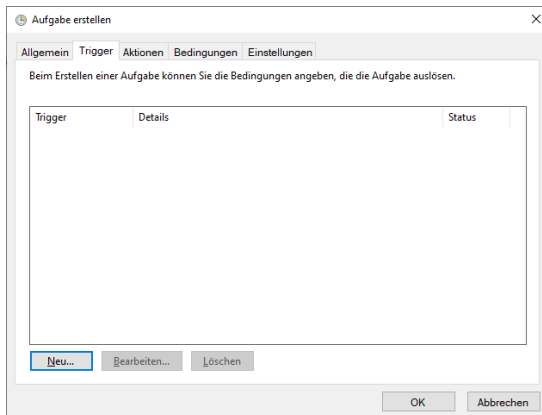
Geben Sie als Objektname **SYSTEM** ein und übernehmen Sie mit **OK**.



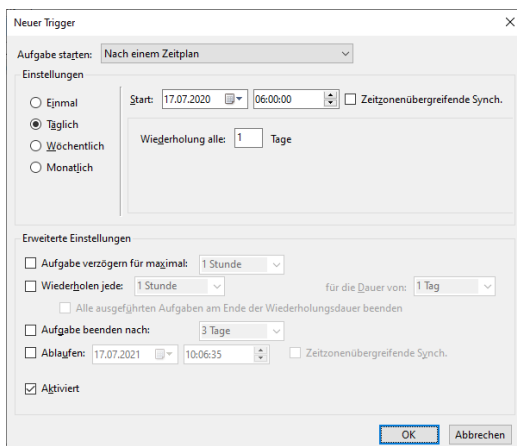
Die Aufgabe wird damit unter dem Systemkontext ausgeführt.



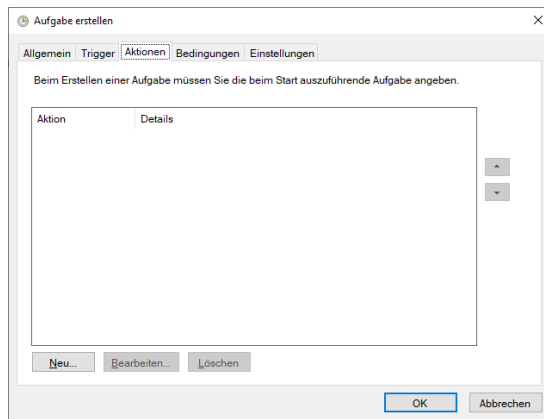
Wechseln Sie auf die Registerkarte **Trigger** und wählen Sie **Neu...**



Definieren Sie das Ausführen täglich zu einem passenden Zeitpunkt, z.B. um 6:00 Uhr am Morgen.



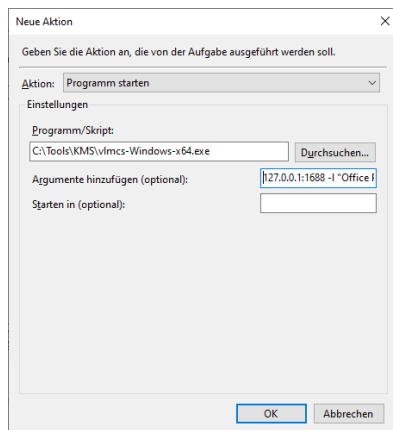
Wechseln Sie auf die Registerkarte **Aktionen** und wählen Sie **Neu...**



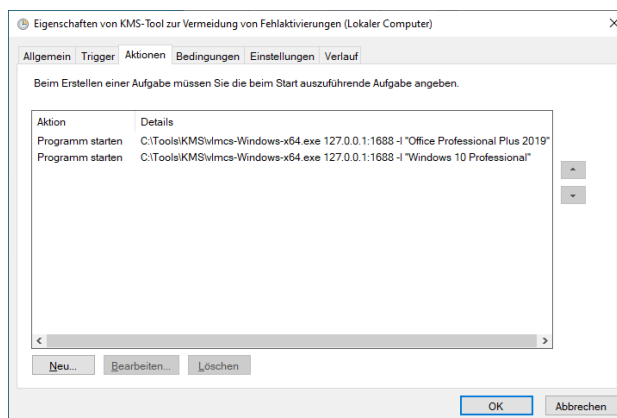
Wählen Sie über **Durchsuchen** den Client-Emulator aus, den Sie zuvor ins Verzeichnis C:\Tools\KMS kopiert haben. Sofern Sie im Namen des Tools keine Leerzeichen verwenden, braucht das Skript nicht in Hochkommata zu stehen.

Wählen Sie als Argument die bereits oben beschriebenen Angaben für das jeweilige Produkt, wie z.B. Office 2019. Beachten Sie, dass der Text exakt so geschrieben sein muss, wie er vom Tool vorgegeben wird!

127.0.0.1:1688 -l "Office Professional Plus 2019"



Legen Sie auf die gleiche Art und Weise im Reiter **Aktionen** für jedes zu aktivierende Produkt einen entsprechenden Eintrag an und übernehmen Sie mit **OK**.



Bevor Sie die Aktivierung von Windows 10 oder Office am Client prüfen, muss der KMS-Server noch über DNS im Netzwerk bekannt gemacht werden.

III.6.4. Umgebung für Microsoft KMS konfigurieren

III.6.4.1. DNS-Eintrag im logosrv erstellen

Damit die Arbeitsstationen den Microsoft KMS-Host finden, muss dafür im **logosrv** ein entsprechender DNS-Eintrag erstellt werden. Dazu wechselt man zunächst in den Container des logosrv und dort in das Verzeichnis des DNS-Servers.

```
lxc-attach -n logosrv
```

```
cd /etc/bind/template
```

Im zweiten Schritt muss ein Eintrag am DNS-Server "Bind" erstellt bzw. angepasst werden. Erstellen Sie dazu mit einem Editor Ihrer Wahl die Datei `db.domain.static.custom`, sofern sie nicht existiert.

Fügen Sie dort den folgenden Eintrag ein bzw. passen Sie diesen an:

```
_vlmcs._tcp.schule.local. SRV 0 0 1688 HOSTNAME.schule.local.
```

Der Eintrag **HOSTNAME** ist dabei der Name des Rechners auf dem der KMS läuft. Im Falle einer Standard-Installation mit LogoDIDACT 2.0, erfolgt die Aktivierung über eine per KVM virtualisierte Windows 10 Maschine mit Namen **win10kms**, so dass der Eintrag wie folgt aussieht:

```
_vlmcs._tcp.schule.local. SRV 0 0 1688 win10kms.schule.local.
```



Achtung

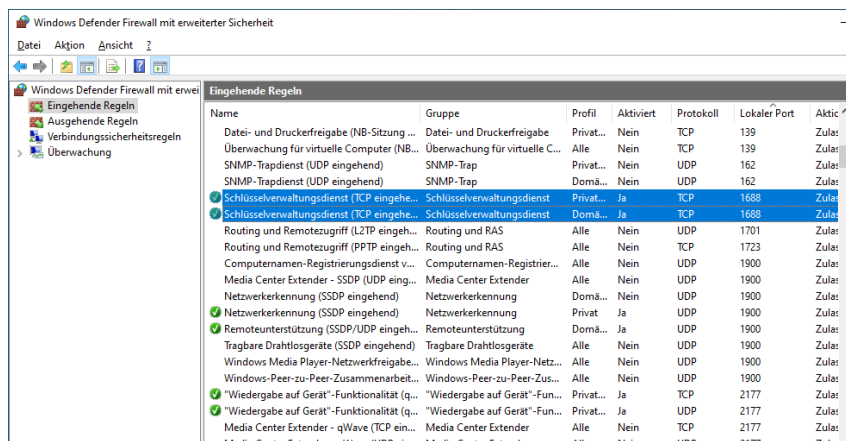
Es wird dringend empfohlen für die Aktivierung über die virtuelle Maschine **win10kms** auf Basis von Windows 10 zu verwenden!

Damit der DNS-Server die Konfiguration übernimmt, muss die Konfiguration neu geladen werden:

```
update_dns
```

III.6.4.2. Ports am KMS-Host öffnen

Sofern die entsprechenden Ports 1688 nicht bereits beim Aufsetzen des KMS-Host per LD Deploy geöffnet wurden, kann bzw. muss das direkt über die Windows Firewall am KMS-Host nachgeholt werden. Aktivieren Sie dazu die beiden Regeln für eingehende Verbindungen für den Schlüsselverwaltungsdienst.



III.6.4.3. GVLK am Windows Client eintragen

Für die Aktivierung per Microsoft-KMS ist es notwendig, dass am Client ein so genannter GVLK (Generic Volume Licenses Key) eingetragen ist. Für jedes Microsoft Betriebssystem gibt es solche GVLKs, die zudem öffentlich zugänglich und bekannt sind. Im Gegensatz zu einem MAK-Key veranlasst ein GVLK das Windows Betriebssystem sich gegenüber einem KMS-Dienst zu aktivieren.

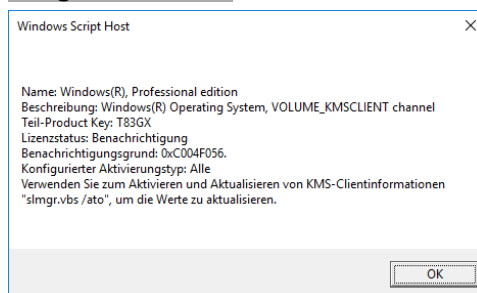
Am Windows 10 Client muss man bei einer Neuinstallation normalerweise gar nichts eintragen, denn der dort eingetragene Key ist bereits vom Typ GVLK. Sie finden die Liste der Entsprechenden Keys auf den Seiten von Microsoft.

[https://msdn.microsoft.com/de-de/library/jj612867\(v=ws.11\).aspx](https://msdn.microsoft.com/de-de/library/jj612867(v=ws.11).aspx)

Im Fall von Windows 10 Professional ist der GVLK: W269N-WFGWX-YVC9B-4J6C9-T83GX

Um herauszufinden, ob der Windows 10 Client auf der Aktivierungsmethode KMS steht, dient der folgenden Befehl:

slmgr.vbs /dli



Zum Installieren eines anderen KMS-Schlüssels nutzen Sie am Windows 10 Client diesen Befehl:

slmgr.vbs /ipk <KMS-Schlüssel>

Entsprechende Schlüssel gibt es nicht nur für die Windows Betriebssysteme, sondern auch die diversen Microsoft Office-Versionen. Bei Office heißt das Tool zur Volumenaktivierung jedoch ospp.vbs.

III.6.4.4. Aktivierungsskript für Clients

Über die Kombination des GVLK am Client und dem zuvor erstellten DNS-Eintrag suchen und finden die Windows-Clients im Netzwerk den Microsoft-KMS auf Serverseite und aktivieren sich in regelmäßigen Abständen. Per Standardeinstellung versucht ein Windows 10 Client dies z.B. alle 2 Stunden.

Im Zusammenhang mit dem Zurückspielen eines Images bzw. der Heilungsfunktion reicht es aber nicht, dass man auf diese dynamische Aktivierung wartet, weil die Anwender zwischenzeitlich mit Meldungen über ein nicht aktiviertes Windows oder Office konfrontiert werden.

Um unnötige Support-Anfragen zu vermeitlichen Fehlern bei der Aktivierung zu vermeiden, gibt es ein entsprechendes Skript, das die Aktivierung nach dem Hochfahren und vor der Anmeldung "antriggert".



Achtung

Das Skript muss kundenspezifisch angepasst werden und funktioniert nur, wenn man die entsprechende Software standardkonform in die vorgegebenen Pfade installiert hat. Bitte beachten Sie, dass die rot markierten Zeilenumbrüche # im Skript nicht vorhanden sind und auch nicht vorhanden sein dürfen!

```
@echo off
echo.
echo
echo          -----
echo          * KMS Produktaktivierung *
echo          -----
echo.
if "%OS%"=="Windows_NT" goto :start
echo Fehler: Dieses Skript benoetigt Windows NT oder hoeher!
goto :eof

:start
REM Konfiguration Office-Installationsverzeichnis
SET OFFICEPATH=C:\Programme\Microsoft Office\Office16

:act_win
for /F "tokens=1,2 delims= " %%a in ('cscript "%SystemRoot%\System32\slmgr.vbs" -dli') do IF %%b==Lizenziert (
echo Windows bereits aktiviert.
goto :act_office )

echo Aktiviere Windows ...
cscript "%SystemRoot%\System32\slmgr.vbs" /ato

:act_office

if /i not exist "%OFFICEPATH%\ospp.vbs" (
echo Office-Programmpfad nicht gefunden.
goto :eof )

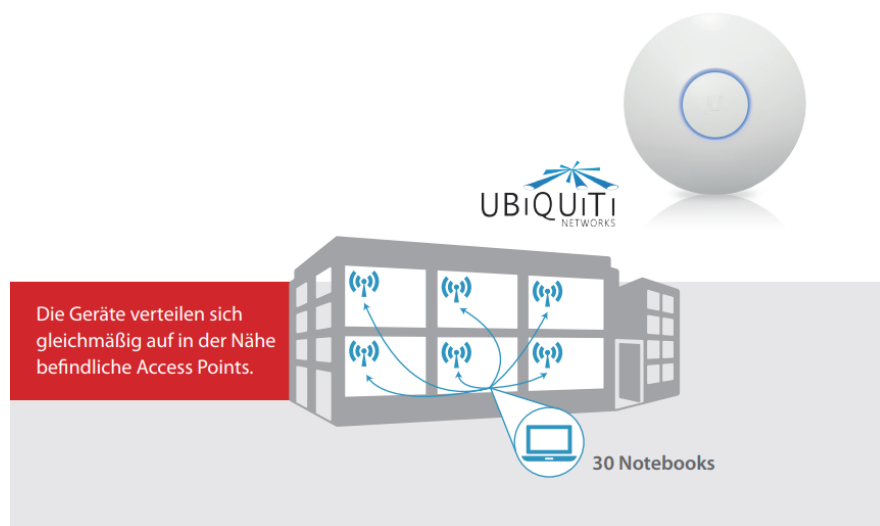
for /F "tokens=1,2,3 delims= " %%a in ('cscript "%OFFICEPATH%\ospp.vbs" /dstatus') do IF %%c===---LICENSED--- (
echo MS Office bereits aktiviert.
goto :eof )

echo Aktiviere Microsoft Office ...
cscript "%OFFICEPATH%\ospp.vbs" /act
```

Kapitel III.7. Unifi WLAN-Lösung

Für den modernen Unterricht benötigt jede Schule eine funktionierende und technisch perfekte WLAN-Infrastruktur, die zentral verwaltet werden kann. Mit einem Softwarecontroller und den dazu passenden Access Points haben Sie mit LogoDIDACT genau eine solche WLAN-Lösung.

Die automatische Lastverteilung sorgt für eine gleichmäßige Verteilung vieler mobiler Geräte auf verschiedene Access Points.



Entscheidend dabei ist, dass es sich um eine flexible Softwarelösung handelt, die sowohl lokal als auch cloudbasiert betrieben werden kann. Dies bietet Ihnen deutliche Vorteile gegenüber einer nur cloudbasierten Lösung oder Systemen mit teurem Hardwarecontroller.

Der RADIUSserver, ein vorgeschalteter Authentifizierungsdienst für sich einwählende Benutzer, ist ein weiterer fester Bestandteil von LogoDIDACT und die passende Lösung für das Einbinden privater Geräte (BYOD = bring your own device).

III.7.1. Installation Container Unifi

Die Installation des Unifi WLAN-Controllers ist wieder denkbar einfach, da der Container per Systemmanagement Puppet automatisiert aufgebaut und konfiguriert wird.

Wechseln Sie in den Puppeteer:

```
lxc-attach -n puppeteer
```

Wechseln Sie in das Verzeichnis zur Konfiguration von Containern:

```
cd /etc/logodidact/hosts/ldhost
```

Öffnen Sie die Datei `guest.conf` mit einem Editor Ihrer Wahl, wie z.B. Nano:

```
nano guest.conf
```

Fügen Sie dort den Eintrag für den Container Unifi hinzu.

```
[Guest unifi]  
Ensure running
```

Durch Eingabe der Tastenkombination <Strg>+<X> verlassen Sie den Editor Nano und geben „Y“ ein, damit die Änderung gespeichert wird. Wechseln Sie dann ins Stammverzeichnis der Konfiguration und übertragen Sie anschließend die Änderungen ins Versionierungssystem git:

```
cd /etc/logodidact
```

```
git add .
```

```
git commit -m "Aktivierung Container unifi"
```

Durch das Übertragen ins git-Repository wird auch automatisch map_translate aufgerufen, so dass die Konfigurationen in YAML übersetzt und von Puppet verarbeitet werden können.

Wie bereits beim Aufbau anderer Container mehrfach beschrieben, veranlasst ein **prun** im Host den Agent dazu, mit dem Aufbau des Containers unifi zu beginnen. Beobachten können Sie das Ganze wieder mit **pstat** im Puppetter. Nach einer Weile wird dort der Container **unifi** auftauchen. Sofern der Container grundlegend aufgebaut ist und läuft, kann man in einer neuen Sitzung per **lxc-attach -n unifi** dort hineinwechseln und sofern gerade kein prun läuft einen solchen neuen Durchlauf mit **prun** starten.

In der Regel sind mehrere dieser Durchläufe notwendig, bis der Container vollständig aufgebaut ist. Mit jedem **prun** im Container **unifi** nähert sich der Wert in der Spalte Successes einem Endwert, der nicht Null sein muss.

Agent State	Catalog State	Node	Successes	Noops	Skips	Failures	Last run
Deactivated		audit					
Deactivated		ca-g1					
Deactivated		collabora-g1					
Deactivated		icinga2					
Deactivated		kopano-g1					
Waiting	OK	ldhost.schule.local	17				3 minutes ago
Unknown	OK	ldmobile.schule.local					a long while ago
Deactivated		logosrv					
Deactivated		moodle30					
Deactivated		mysql56.schule.local					20 minutes ago
Deactivated		nextcloud-g1					
Deactivated		postgresq110					
Waiting	OK	puppeteer.schule.local					25 minutes ago
Deactivated		pydio					
Waiting	OK	rembo5.schule.local					25 minutes ago
Waiting	OK	rev-proxy.schule.local	1				18 minutes ago
Waiting	OK	samba4-ad.schule.local	1				26 minutes ago
Running	OK	unifi.schule.local	146		2		1 minute ago
Deactivated		xibol7					

Press 'l'-'9' to change update interval. Press 'q' to quit.

Auch die WLAN-Controller Software wird per Weboberfläche administriert und kann damit prinzipiell von überall aus aufgerufen werden. Wenn Sie das tun möchten, aktivieren Sie den Dienst im Reverse Proxy und erzeugen Sie ein Zertifikat, wie in den nächsten beiden Abschnitte erläutert.

III.7.2. Unifi im Rev-Proxy freischalten

Wechseln Sie in den Puppeteer:

```
lxc-attach -n puppeteer
```

Wechseln Sie in das Verzeichnis zur Konfiguration des Reverse-Proxy:

```
cd /etc/logodidact/hosts/rev-proxy
```

Öffnen Sie die Datei revproxy.conf und ergänzen Sie diese mit einem Eintrag für ldmobile. Achten Sie vor allem darauf, dass für Unifi zwingend https verwendet werden muss, sowie die Portangabe 443.

```
[ReverseProxy mrbs.musterstadt-gym.logoip.de]
```

Url `http://mrbs`

[ReverseProxy `unifi.musterstadt-gym.logoip.de`]
 Url `https://unifi.schule.local:443`

Das Schulkürzel entspricht dabei Ihrem individuell festgelegten Namen.

Pflegen Sie die Änderungen wie gewohnt ins git ein:

```
cd /etc/logodidact
```

```
git add .
```

```
git commit -m "wlan controller unifi über rev-proxy freischalten"
```

III.7.3. Zertifikat für Unifi aktivieren

Bevor Sie das Zertifikat versuchen zu erstellen, prüfen Sie kurz die Verfügbarkeit der Zertifizierungsstelle. Gehen Sie dazu mit einem Webbrowser auf die Internetseite `https://letsencrypt.status.io/` und prüfen Sie, ob die Dienste dort verfügbar sind oder es eventuell Probleme gibt.

Wechseln Sie in den Container **Puppeteer** und prüfen Sie zunächst, ob Sie dort über den Befehl **sle** in die Umgebung zur Verwaltung der Zertifikate kommen. Stellen Sie dies gegebenenfalls um, wie in Abschnitt III.3.6.3.1, „Umstellung auf das Tool `acme.sh`“ beschrieben.

Starten Sie dann in die Umgebung zur Verwaltung der Let's Encrypt Zertifikate und stellen für den Dienst einen entsprechenden Antrag:

```
sle
```

```
issue unifi.SCHULKUERZEL.logoip.de
```

Hierbei steht **schulkuerzel** für den bereits mehrfach verwendeten individuellen Namen (z.B. `musterstadt-gym`).

Die Rückmeldung an Infos ist im Fall von **acme.sh** in der Regel sehr ausführlich. Mit dem folgenden Befehl kann man sich eine Liste aller Zertifikate anzeigen lassen und damit auch den Status prüfen:

```
acme.sh --list
```

Wenn das Zertifikat erstellt und heruntergeladen wurde, landet es über Puppet irgendwann im Container **rev-proxy** im Ordner `/etc/nginx/ssl`. Das Ganze lässt sich ggf. wieder über einen **prun** im **puppeteer** und danach im **rev-proxy** beschleunigen.

III.7.4. Unifi Erstanmeldung

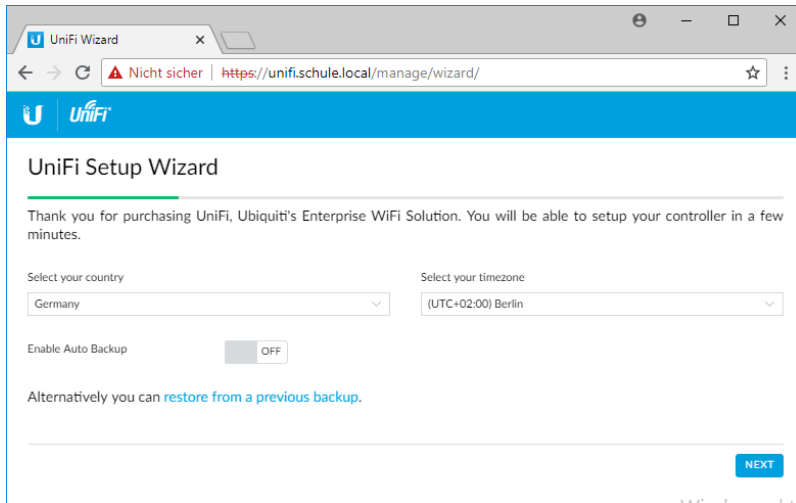
Die Administration von **unifi** erfolgt über ein Webinterface, das aus dem internen Netzwerk über die folgende Seite direkt erreichbar ist:

`http://unifi.schule.local`

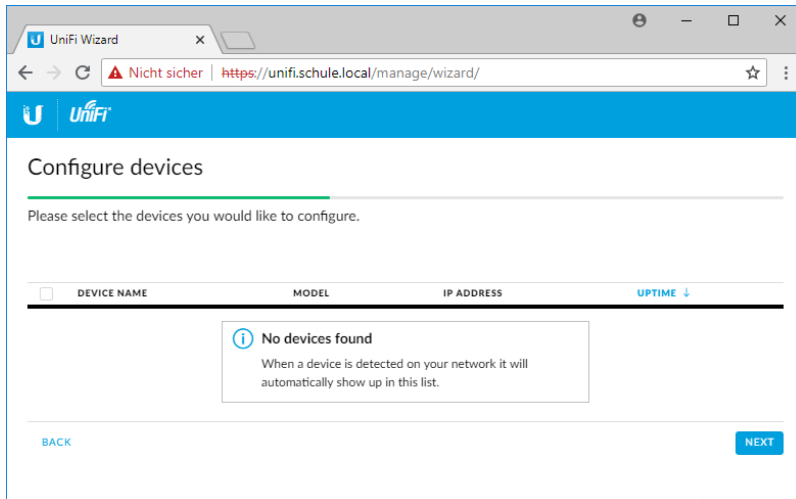
oder von intern aber auch extern über den Reverse-Proxy:

`https://unifi.musterstadt-gym.logoip.de`

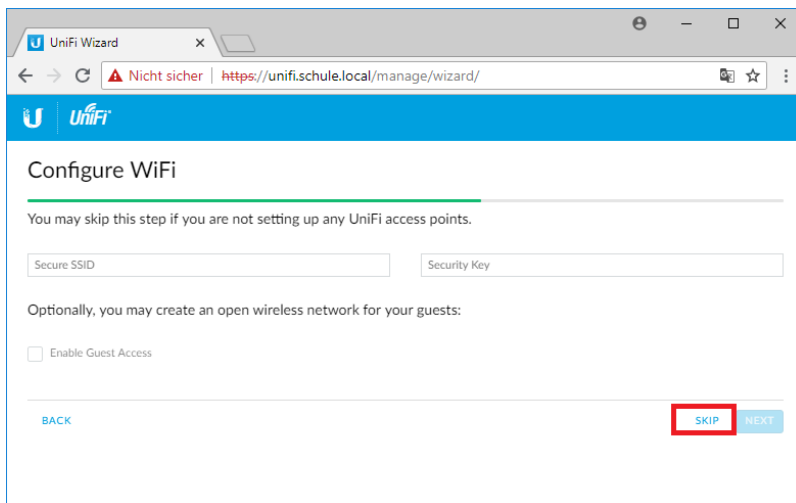
Rufen Sie diese Seite über einen Browser auf. Wählen Sie die passende Sprache und Zeitzone aus, deaktivieren Sie die Option **Enable Auto Backup**, in Sie den Schieberegler auf OFF setzen und fahren Sie fort mit **NEXT**.



Die Grundkonfiguration können Sie auch vornehmen, wenn noch keinen UniFi Access Point im Netz angeschlossen ist. Fahren Sie fort mit **NEXT**.



Da wir an dieser Stelle noch kein WLAN einrichten wollen, überspringen Sie diese Möglichkeit bitte durch Auswahl der Schaltfläche **SKIP**.



Setzen Sie im nächsten Dialog das Kennwort für den Benutzer **admin**, sowie dessen Mailadresse. Verwenden Sie dazu bitte nur diesen Benutzer und verwenden Sie als Mailadresse das interne Postfach **admin@schule.local**.



Achtung

Der Unifi-Softwarecontroller bietet derzeit leider keine Anbindung an LDAP.

Der Benutzer **admin** und damit auch sein Kennwort haben mit dem in LogoDIDACT vordefinierten gleichnamigen Benutzer nichts zu tun.

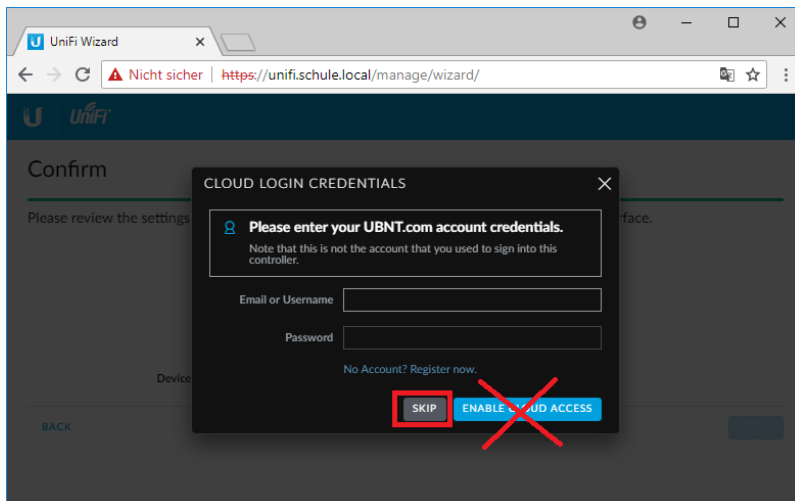
Bitte notieren Sie sich deshalb die hier gemachten Kennworte separat!

Bitte definieren Sie entsprechend komplexe Kennwörter. Lassen Sie das Feld **Device Authentication** unbedingt leer, damit für den SSH-Zugang auf die AccessPoints die gleichen admin-Daten übernommen werden.

Fahren Sie fort mit **NEXT**.

Bestätigen Sie die gemachten Angaben mit **FINISH**.

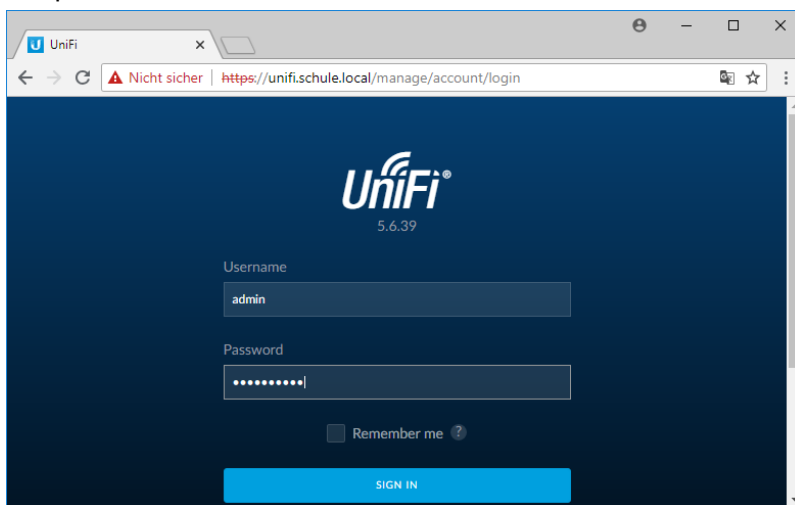
Überspringen Sie die Möglichkeit der Cloud-Anmeldung durch **SKIP**.



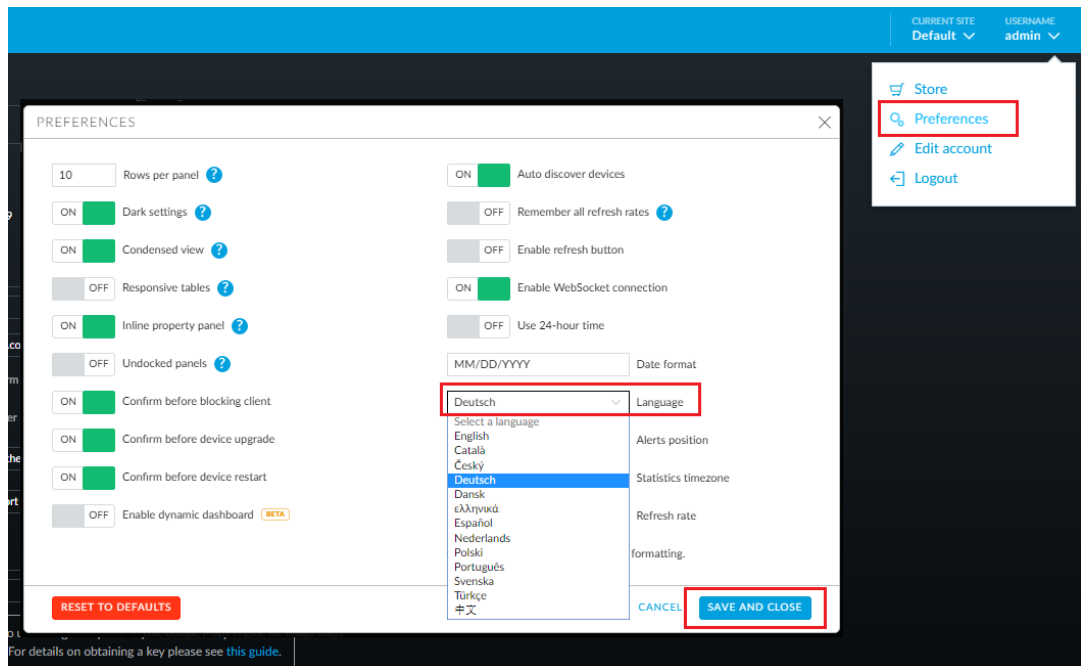
III.7.5. Admin-Anmeldung und Spracheinstellung

Nachdem die Grundkonfiguration abgeschlossen ist, melden Sie sich mit den dabei festgelegten Daten des Benutzers **admin** an. Rufen Sie dazu im Browser im internen Netzwerk die folgende Seite auf:

<http://unifi.schule.local>




Ändern Sie zunächst im Menü rechts oben über **Preferences** die Spracheinstellung der Web-Oberfläche und übernehmen Sie die Änderung durch **SAVE AND CLOSE**.



III.7.6. Unifi Konfiguration von Hostname und Mail

Sämtliche Konfigurationseinstellungen werden in der Weboberfläche über das Zahnradsymbol **Einstellungen** auf der linken Seite ganz unten vorgenommen. Klicken Sie auf dieses Symbol und wählen Sie aus dem Menü den Eintrag **Controller**.

Tragen Sie die folgenden Werte ein:

 **Achtung**

Controller-Hostname/IP: unifi.schule.local

SMTP-Server: localhost

The screenshot displays the UniFi web interface with the following configuration details:

- Controller-Einstellungen:**
 - Controller-Name: UniFi
 - Controller-Hostname/IP: unifi.schule.local
 - Hostnamen für Rückmeldungen mit Controller-Hostname/IP überschreiben:
 - Netzwerk-Erkennung:
 - Controller in Layer-2-Netzwerken sichtbar:
 - Geschäft: Geschäft nur für den Super-Administrator aktivieren
 - Messaging-Support: Live-Support nur für den Super-Administrator aktivieren
- Karten-Einstellungen:**
 - Google Maps API-Key: [Empty field]
 - Um Google Maps zu verwenden, ist ein gültiger API-Key erforderlich. Details und Hilfe zum API-Key erhalten Sie hier. Der API-Key sollte der Domäne oder der IP-Adresse des Controllers zugewiesen werden.
 - Nutzung der Google Maps Engine für Ihre Kartenbilder:
- E-MAIL SERVER:**
 - SMTP-Server: E-Mail Server aktivieren
 - Hostname: localhost
 - Port: 25
 - SSL aktivieren:
 - Authentifizierung aktivieren: Benutzername: [Empty field] Passwort: [Empty field]
 - Absenderadresse angeben: [Empty field]
 - SMTP-Server testen: Test-E-Mail senden an [Empty field] [SENDEN]

Buttons at the bottom: **ÄNDERUNGEN ANWENDEN** and **ZURÜCKSETZEN**.

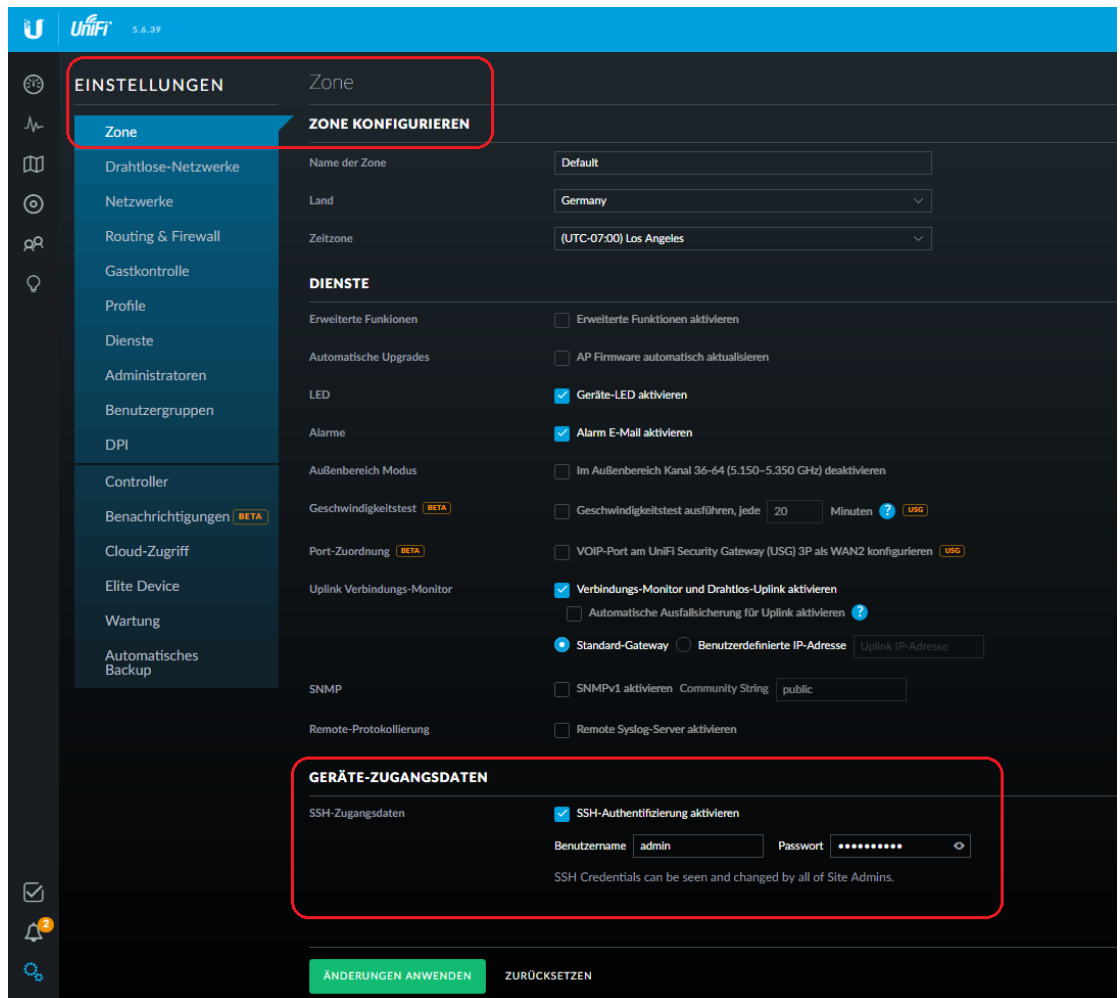
Sollten Sie das Passwort des UniFi-Administrators **admin** vergessen, kann über die Funktion "Passwort vergessen" eine Mail an den LogoDIDACT **admin** gesendet werden, um dieses wieder zurückzusetzen.

III.7.7. SSH-Zugang für Unifi Access Points

Bei der Ersteinrichtung des Softwarecontrollers gab es den Eintrag **Device Authentication**, der nicht ausgefüllt werden sollte, damit die gleichen admin-Daten übernommen werden, wie für die Administration des Controllers selbst.

Der SSH-Zugang direkt auf die Access Points kann hilfreich sein, wenn der Probleme zwischen dem Softwarecontroller und den Access Points auftreten, deren Ursache unklar ist. Dann kann man sich per SSH direkt auf einen AP einwählen.

Die Konfiguration dafür findet sich in **Einstellungen** → **Zone** → **Geräte-Zugangsdaten**.



III.7.8. WLAN Konfiguration

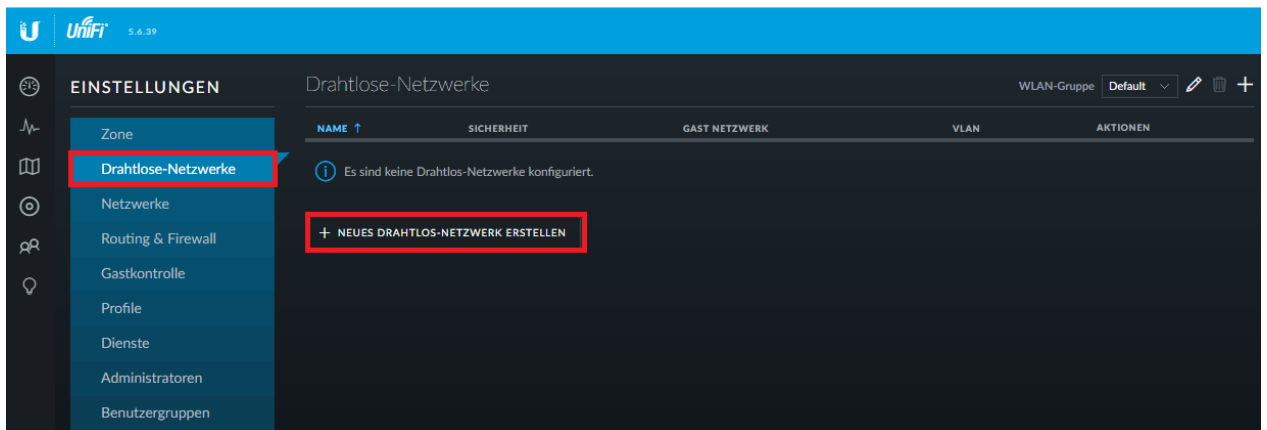
Für die Konfiguration eines WLANs gibt es sehr viele Möglichkeiten. In den meisten Fällen legt man mindestens 2 separate WLAN-Netzwerke an. Eines davon für schulinterne Geräte mit klassischer WPA2-Verschlüsselung und ein weiteres Netzwerk für private Geräte mit WPA2-Enterprise Verschlüsselung bzw. Radius-Authentifizierung.

Sofern Sie auch Tablets einsetzen wollen, empfiehlt sich für den Zeitraum der Erstaufnahme ein weiteres WLAN-Netz mit einfachem Kennwort. Dieses WLAN aktiviert man zum Zweck der Aufnahme und deaktiviert es danach wieder.

Es gibt viele weitere Möglichkeiten, wie z.B. ein separates Lehrer-WLAN oder Schüler-WLAN, für das man zudem auch die Bandbreite begrenzen kann. Lesen Sie dazu die Doku von UniFi oder Ihrem entsprechenden WLAN-System.

III.7.8.1. WLAN mit WPA2-Verschlüsselung

Wählen Sie in der UniFi-Oberfläche wieder das Zahnradsymbol auf der linken Seite ganz unten. Wählen Sie dann **Drahtlose-Netzwerke** und klicken Sie **NEUES DRAHTLOS-NETZWERK ERSTELLEN**.



Wählen Sie einen passenden Namen für das WLAN-Netzwerk und legen Sie die Art der Verschlüsselung fest.

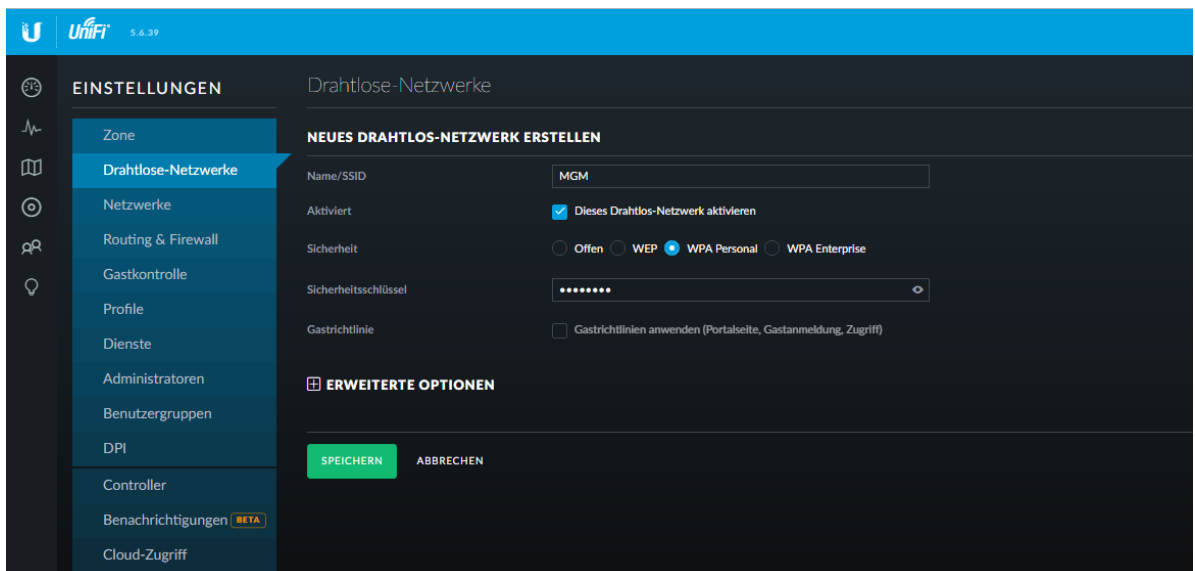


Achtung

Für iPads wird zwingend ein Netzwerk vom Typ WPA2-PSK benötigt, da sonst über iOS die Zertifikate immer wieder verworfen werden. Der dafür passende Eintrag in Unifi ist WPA Personal.

Wählen Sie ein hinreichend komplexes Kennwort. Dieses können Sie im Container **Logosrv** mit Hilfe des Befehls **pwgen 32** generieren.

Geben Sie die Daten und und sichern Sie das Ganze durch **SPEICHERN**.



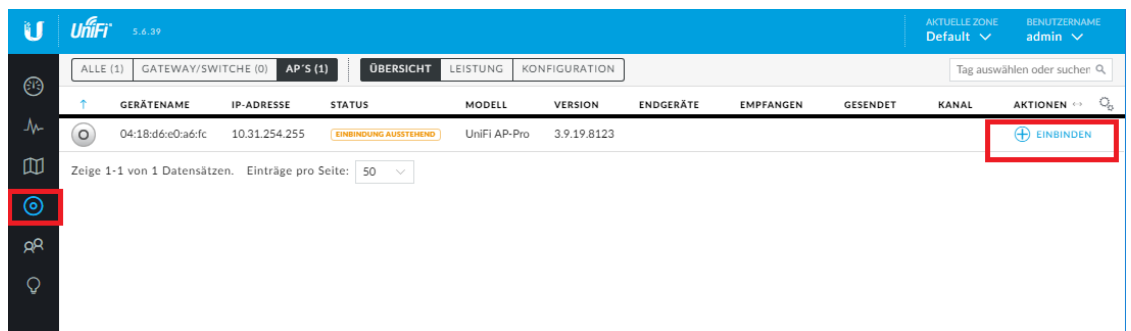
Diese logische Konfiguration eines WLAN-Netzwerkes wird nun auf ein oder mehrere Unifi Access-Points übertragen.

III.7.8.2. WLAN für die Aufnahme von Tablets

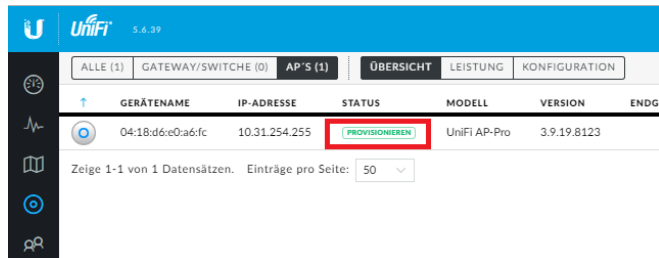
Nach dem gleichen Schema wie im Kapitel zuvor, kann man z.B. ein WLAN "Tablet-Aufnahme" mit einem einfachen Kennwort "12345678" erstellen und dieses nur für den Zeitraum der Aufnahme der mobilen Geräte aktivieren.

III.7.8.3. AccessPoints einbinden

Schließen Sie einen geeigneten Unifi AccessPoint per LAN-Interface an das LogoDIDACT Netzwerk an. Neue Geräte werden automatisch vom WLAN-Controller erkannt und angezeigt. Über die graphische Oberfläche ist es relativ einfach und intuitiv, wie ein neuer AccessPoint einzubinden ist. Klicken Sie dazu bei dem erkannten Gerät auf der rechten Seite auf **EINBINDEN**.



Sobald dieser Vorgang gestartet wurde, beginnt der Controller damit das Gerät mit der WLAN-Konfiguration zu versorgen. Der Vorgang wird auch in der Weboberfläche angezeigt und als **PROVISIONIEREN** bezeichnet.



Sobald dieser Vorgang abgeschlossen ist, erscheint als neuer Status **VERBUNDEN**.

AccessPoints einbinden

The screenshot displays the UniFi management interface in a web browser. The browser's address bar shows the URL: `https://unifi.schule.local/manage/site/default/devices/1/50/uap?pp=W3siaS16lmRldmJjZXwwNDoxODpkNjplMDphNjpmYyYsln...`. The interface features a blue header with the UniFi logo and version 5.6.39. Below the header, there are navigation tabs for 'ALLE (1)', 'GATEWAY/SWITCHE (0)', and 'AP'S (1)'. The 'AP'S (1)' tab is active, showing a table of devices. The table has columns for 'GERÄTENAME', 'IP-ADRESSE', 'STATUS', 'MODELL', 'VERSION', and 'ENDGERÄTE'. One device is listed with MAC address '04:18:d6:e0:a6:fc', IP address '10.31.254.255', status 'VERBUNDEN', model 'UniFi AP-Pro', and version '3.9.19.8123'. To the right of the table, there is a sidebar for 'EIGENSCHAFTEN' (Properties) for the selected device. This sidebar includes tabs for 'Details', 'Clients', 'Konfiguration', and 'Alerts'. The 'Details' tab is active, showing a summary of the device's information: MAC-Adresse (04:18:d6:e0:a6:fc), Modell (UniFi AP-Pro), Version (3.9.19.8123), Revisionsnr. Leiterplatte (34), IP-Adresse (10.31.254.255), and Betriebszeit (2m 12s). Below the summary, there are three expandable sections: 'FUNK (11B/G/N)', 'FUNK (11A/N)', and 'LEISTUNG (LETZTEN 24 STUNDEN)'.

GERÄTENAME	IP-ADRESSE	STATUS	MODELL	VERSION	ENDGERÄTE
	04:18:d6:e0:a6:fc	10.31.254.255	VERBUNDEN	UniFi AP-Pro	3.9.19.8123

Zeige 1-1 von 1 Datensätzen. Einträge pro Seite: 50

EIGENSCHAFTEN

ÜBERSICHT

- MAC-Adresse: 04:18:d6:e0:a6:fc
- Modell: UniFi AP-Pro
- Version: 3.9.19.8123
- Revisionsnr. Leiterplatte: 34
- IP-Adresse: 10.31.254.255
- Betriebszeit: 2m 12s

Benutzer
Gäste

FUNK (11B/G/N)
FUNK (11A/N)
LEISTUNG (LETZTEN 24 STUNDEN)

Kapitel III.8. Tablet-Management mit LD Mobile

Der Einsatz von Tablets und mobilen Geräten in Schulen gehört schon heute zum Alltag des modernen digitalen Unterrichts. Mit der MDM/MAM (Mobile-Device- bzw. Mobile Application Management) Lösung **LD Mobile** als Bestandteil von LogoDIDACT können Sie beruhigt den Schritt in die digitale Bildungszukunft gehen.

Mit **LD Mobile** lassen sich iPads und Android-Tablets zentral verwalten und mit APPs versorgen. Auch die sichere Nutzung privater Geräte (BYOD) ist in einer LogoDIDACT Umgebung spielend leicht umzusetzen. Hinter **LD Mobile** steht dabei die Software Relation des SBE-Kooperationspartners m-way.

Einer der größten Vorteile von **LD Mobile** besteht in der Integration in LogoDIDACT und der Automatisierung der dafür notwendigen Softwarebausteine für einen reibungslosen Betrieb. Neben der LDAP-Anbindung zählen hierzu unter anderem die Komponenten Rev-Proxy, Let's Encrypt-Zertifikate, MariaDB-Datenbank, Nextcloud und wpad-Konfiguration, die als Container bereitgestellt und vollautomatisiert verwaltet werden.

III.8.1. Vorteile von LD Mobile

Eine praktikable Tablet-Lösung für Schulen erfordert deutlich mehr, als irgendein MDM-System irgendeines Herstellers, irgendwo in der Cloud zu hosten. Erst mit der Einführung der DSGVO (Datenschutz Grundverordnung) Ende Mai 2018 wird Schulen und Schulträgern und den Verantwortlichen klar, dass viele vermeintlich günstige und hübsche MDM-Systeme nicht nur ungeeignet sondern schlichtweg unzulässig sind für den Einsatz an deutschen Schulen.

Gerade in dieser Hinsicht, gehen Sie mit **LD Mobile** auf Nummer sicher!

Die Vorteile von **LD Mobile** im Überblick:

- perfekte Integration in LogoDIDACT
- Betrieb lokal auf dem Schulserver oder im Rechenzentrum
- Integration von Nextcloud (Speichern lokal auf dem Schulserver und z.B. nicht in der iCloud)
- Integration in Zertifikatsumgebung mit Let's Encrypt
- Unterstützung von DEP/VPP
- Unterstützung von iPads und Android-Tablets
- Datenschutzkonform nach DSGVO
- Secure Shared iPad Modus

III.8.2. Voraussetzungen für LD Mobile

Die Voraussetzung für die Installation von **LD Mobile** wurden in den vorherigen Kapiteln geschaffen und die notwendigen Komponenten bzw. deren Installation und Konfiguration dokumentiert:

1. Samba4 (Abschnitt III.3.4, „Aktivierung samba4-ad“)
2. Reverse-Proxy (Abschnitt III.3.5, „Reverse-Proxy“)

3. Zertifikatsverwaltung (Abschnitt III.3.6, „Zertifikate mit Let's Encrypt“)
4. MariaDB Datenbank (wird hier beschrieben)

Sofern eine oder mehrere dieser Komponenten nicht korrekt installiert und konfiguriert sind, holen Sie das jetzt nach und beachten Sie dabei auch die Reihenfolge.

III.8.3. Installation der MariaDB-Datenbank

Eine weitere Voraussetzung aber eher konkreter Bestandteil von **LD Mobile** ist eine SQL-Datenbank in einem eigenen Container. Dieser Container muss zwingend vor dem Container mit LD Mobile aktiviert und installiert werden.

Für eine aktuelle Neuinstallation mit **LD Mobile 5** ist es verbindlich, dass als Datenbank **mariadb105** zum Einsatz kommt. Aus Geschwindigkeits- und Kompatibilitätsgründen war der Einsatz von **mariadb105** auch schon ab **LD Mobile 4.72** (08/2020) möglich und ratsam aber nicht zwingend erforderlich.

Sowohl für eine Neuinstallationen als auch ein Upgrade auf **LD Mobile 5**, muss zunächst der Container **mariadb105** aktiviert werden.

Wechseln Sie in den Puppeteer:

```
lxc-ssh -n puppeteer
```

Wechseln Sie in das Verzeichnis zur Konfiguration von Containern:

```
cd /etc/logodidact/hosts/ldhost
```

Öffnen Sie die Datei `guest.conf` mit einem Editor Ihrer Wahl, wie z.B. Nano:

```
nano guest.conf
```

Fügen Sie dort den Eintrag für den Datenbank-Container hinzu.

```
[Guest mariadb105]  
Ensure running
```

Durch Eingabe der Tastenkombination `<Strg>+<X>` verlassen Sie den Editor Nano und geben „Y“ ein, damit die Änderung gespeichert wird. Wechseln Sie dann ins Stammverzeichnis der Konfiguration und übertragen Sie anschließend die Änderungen ins Versionierungssystem git:

```
cd /etc/logodidact
```

```
git add .
```

```
git commit -m "Aktivierung MariaDB 10.5 für LD Mobile"
```

Durch das Übertragen ins git-Repository wird auch automatisch `map_translate` aufgerufen, so dass die Konfigurationen in YAML übersetzt und von Puppet verarbeitet werden können.

Wie bereits beim Aufbau anderer Container mehrfach beschrieben, veranlasst ein **prun** im Host den Agent dazu, mit dem Aufbau des Containers **mariadb105** zu beginnen. Beobachten können Sie das Ganze wieder mit **pstat** im Puppeteer. Nach einer Weile wird sich dort der Container auftauchen. Sofern der Container grundlegend aufgebaut ist und läuft, kann man in einer neuen Sitzung per **lxc-attach -n mariadb105** dort hineinwechseln und sofern gerade kein **prun** läuft einen solchen neuen Durchlauf mit **prun** starten.

In der Regel sind mehrere dieser Durchläufe notwendig, bis der Container vollständig aufgebaut ist. Mit jedem **prun** im Container **mariadb105** nähert sich der Wert in der Spalte Successes einem Endwert, der nicht Null sein muss.

Agent State	Catalog State	Node	Successes	Noops	Skips	Failures	Last run
Waiting	OK	ad-sync-gl.schule.local	2				16 minutes ago
Deactivated		audit					
Waiting	OK	ca-gl.schule.local	2				15 minutes ago
Waiting	OK	collabora-gl.schule.local	2				15 minutes ago
Waiting	OK	ctrl-gl.schule.local	2				14 minutes ago
Waiting	OK	deploy-gl.schule.local	2				14 minutes ago
Waiting	OK	graylog-gl.schule.local	2				13 minutes ago
Deactivated		kopano-gl					
Waiting	OK	ldhost.schule.local	4				1 minute ago
Deactivated		ldmobile					
Unknown	OK	logosrv			2		a long while ago
Running	OK	mariadb105.schule.local	161				1 minute ago
Deactivated		moodle30					
Waiting	OK	moodle311.schule.local	10				10 minutes ago
Deactivated		mysql56					
Waiting	OK	nextcloud-gl.schule.local	5				11 minutes ago
Waiting	OK	nexus-gl.schule.local	2				10 minutes ago
Waiting	OK	pgsql13.schule.local	5				18 minutes ago
Waiting	OK	pgsql10.schule.local	5				8 minutes ago
Waiting	OK	puppeteer.schule.local	3				9 minutes ago
Waiting	OK	rembo5.schule.local	1				9 minutes ago
Waiting	OK	rev-proxy.schule.local	2				8 minutes ago
Waiting	OK	samba4-ad.schule.local	3				7 minutes ago
Waiting	OK	ssp-gl.schule.local	2				7 minutes ago
Waiting	OK	unifi.schule.local	1				6 minutes ago
Deactivated		unifi-g2					
Deactivated		xibol7					

Press 'l'-'9' to change update interval. Press 'q' to quit.

Führen Sie zum Abschluss nochmals gezielt einen **prun** im Container **ca-gl** durch, so dass die Zertifikate für den Container **mariadb105** erstellt werden. Ein letzter **prun** im Container **mariadb105** holt sich diese und installiert sie.

III.8.4. Prüfung der Verzeichnisstruktur

Im Rahmen der Installation und Konfiguration von **LD Mobile** sind Anpassungen notwendig, die per Systemmanagement Puppet vorgenommen werden.



Achtung

Prüfen Sie im Container **puppeteer** über das nachfolgende Skript, ob die Verzeichnisstruktur zur Ablage von benutzerdefinierten YAML-Dateien korrekt ist.

Konkret muss der Ordner **custom.d** ein so genannter Symlink sein.

Das folgende Skript können Sie komplett in eine Shell kopieren und mit der Eingabetaste bestätigen:

```
if [ -h "/var/lib/ld-puppet/hiera.d/custom.d" ]; then
  echo "custom.d Ordner ist Symlink, alles in Ordnung."
else
  echo "Fehlerhafte Umgebung, bitte custom.d Ordner manuell korrigieren."
  # rmdir /var/lib/ld-puppet/hiera.d/custom.d
  # ln -s /etc/logodidact/hiera/custom.d /var/lib/ld-puppet/hiera.d/custom.d
fi
```

Falls bei diesem Kommando ein Fehler ausgegeben wird, muss zur Korrektur ein Symlink angelegt werden, so wie in den auskommentierten Zeilen des Skriptes beschrieben.

Sofern der Ordner ein Symlink ist, lässt sich über **ls -l** prüfen, wohin der symbolische Link für den Ordner **custom.d** zeigt:

```

root@puppeteer: /var/lib/ld-puppet/hiera.d
musterstadt-gym / lxc@ldhost / 17:31 / 1.4.1-1 / ssh@172.28.28.2
root@puppeteer:/var/lib/ld-puppet/hiera.d # ls -l custom.d
lrwxrwxrwx 1 root root 30 May  5 2018 custom.d -> /etc/logodidact/hiera/custom.d

```

III.8.5. Festlegung von MariaDB als Datenbank

Sowohl für eine Neuinstallation als auch eine Umstellung von MySQL auf die neue Datenbank, muss im System festgelegt werden, dass Maria DB verwendet wird.

Erstellen Sie dazu im Container **Puppeteer** im Pfad `/etc/logodidact/hiera/custom.d` die Datei `ldmobile.yaml` mit folgendem Inhalt und dem Verweis auf die MariaDB als Datenspeicher:

```

---
ld_mobile::db_server: mariadb105

```

III.8.6. Datenbank-Migration auf MariaDB 10.5

Bei einer Neuinstallation von **LD Mobile** überspringen Sie diesen Abschnitt!

Wenn Sie **LD Mobile** schon länger einsetzen, können Sie dieses per `ldupdate` maximal auf die Version **LD Mobile 4.72** aktualisieren, solange die Datenbank mit **MySQL 5.6** betrieben wird. Im ersten Schritt ist deshalb eine Migration auf die neue Datenbank im Container **mariadb105** notwendig.

Wechseln Sie in den Container **ldmobile** und führen Sie nacheinander die folgenden Befehle durch:

```
prun
```

```
pdis
```

```
systemctl stop relation.service
```

Nachdem der LD Mobile Dienst damit vorübergehend gestoppt wurde, wechseln Sie in den Container **mariadb105** und führen dort den folgenden Befehl durch:

```
prun
```

Nachdem LD Mobile (Relation) die Datenbank im Container **mariadb105** erstellt hat, wechseln Sie in den **ldhost**. Führen Sie dort einen **prun** aus und starten dann das Migrations-Skript für die Datenbankumstellung:

```
prun
```

```
mariadb-migrate -c -d relation -s mysql56 -t mariadb105 -y
```

```

# -c, --[no-]cleanup      Delete database dump after import (default: no)
# -d, --database=DATABASE Database to be migrated
# -s, --source=CONTAINER  Source container from which the database is to be migrat
# -t, --target=CONTAINER  Target container into which the database is to be migrat
# -y, --assume-yes        Assume "yes" as answer to all prompts and run non-intera

```

Sofern die Datenbankübertragung erfolgreich war, wechseln Sie in den Container **ldmobile** und starten den Dienst wieder:

```
lxc-ssh -n ldmobile
```



```
pena
```

```
systemctl start relation.service
```

Wenn der Container **mysql56** von keinem anderen System verwendet wird, können Sie diesen entfernen. Falls Sie die Groupware **Kopano** einsetzen, dürfen Sie das auf keinen Fall tun, da dieses System seine Datenbank ebenfalls in **mysql56** anlegt!

III.8.7. Installation Container LD Mobile

Voraussetzung für die Neuinstallation von **LD Mobile** ist der zuvor vollständig aufgebaute Container **mariadb105**, sowie die Datei **ldmobile.yaml** mit dem entsprechenden Eintrag zur Verwendung der Datenbank (siehe Abschnitt III.8.5, „Festlegung von MariaDB als Datenbank“).

Der Container **ldmobile** selbst wird wieder auf die gleiche Weise aktiviert und konfiguriert, wie das bereits bei den Bausteinen zuvor gezeigt wurde.

Wechseln Sie in den Puppeteer:

```
lxc-ssh -n puppeteer
```

Wechseln Sie in das Verzeichnis zur Konfiguration von Containern:

```
cd /etc/logodidact/hosts
```

Erstellen Sie den Ordner **ldmobile** für die Konfiguration dieses Dienstes und wechseln Sie in das Verzeichnis:

```
mkdir ldmobile
```

```
cd ldmobile
```

Erstellen Sie mit einem Editor Ihrer Wahl die Datei **ldmobile.conf** mit folgendem Inhalt:

```
[LdMobile]
PublicAddress ldmobile.SCHULKUERZEL.logoip.de
```

Das Schulkürzel entspricht dabei in der Regel wieder dem zuvor festgelegten Domänennamen, d.h., in unserer beispielhaften Umgebung **musterstadt-gym**.

Wechseln Sie anschließend in das Verzeichnis zur Aktivierung von Containern:

```
cd /etc/logodidact/hosts/ldhost
```

Öffnen Sie die Datei **guest.conf** mit einem Editor Ihrer Wahl, wie z.B. Nano:

```
nano guest.conf
```

Fügen Sie dort den Eintrag für den Container LD Mobile hinzu.

```
[Guest ldmobile]
Ensure running
```

Durch Eingabe der Tastenkombination **<Strg>+<X>** verlassen Sie den Editor Nano und geben „Y“ ein, damit die Änderung gespeichert wird. Wechseln Sie dann ins Stammverzeichnis der Konfiguration und übertragen Sie anschließend die Änderungen ins Versionierungssystem git:

```
cd /etc/logodidact
```

```
git add .
```

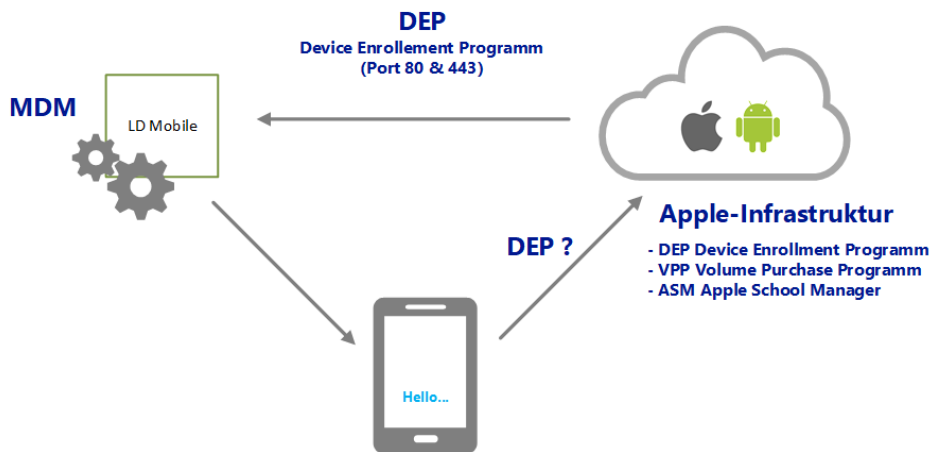
```
git commit -m "Aktivierung und Konfiguration LD Mobile"
```

Analog zu der bisherigen Vorgehensweise wird der Aufbau des Containers durch einen `prun` im `ldhost` angestoßen. Über `pstat` im Puppeteer kann man wieder beobachten und die Durchläufe im Container `ldmobile` durch Aufrufe von `prun` beschleunigen.

III.8.8. Router für Zugriff von außen konfigurieren

Für das Management der Tablets ist es unabdingbar, dass die Apple-Infrastruktur über `http` und `https` bzw. die Ports `80` und `443` mit dem MDM kommunizieren kann. Wenn LD Mobile cloudbasiert betrieben wird, sind keine Anpassungen notwendig, weil die Server mit öffentlicher IP direkt im Netz hängen und über Port `80` und `443` erreichbar sind.

Wenn LD Mobile aber auf einem lokalen Server an der Schule läuft, müssen auf dem dazwischen liegenden Router bzw. der Firewall zwingend entsprechende Portweiterleitungen eingerichtet werden.



In der folgenden Tabelle sind nochmals die Ports aufgeführt, die auf dem Router als entsprechende Weiterleitungen von Außen (Internet) nach Innen (zum externen Interface des Servers hin) eingerichtet werden. Die Bezeichnung "lokaler Server" ist dabei die externe IP des Servers, d.h. per Standard ist das `192.168.1.254`.

Tabelle III.8.1. Portweiterleitungen am Router für den Zugriff der Apple-Infrastruktur von Außen (Internet) nach Innen (Server)

Service	Port	Quelle	Ziel
http	80	*	lokaler Server:80
https	443	*	lokaler Server:443

Weitere Infos zu Ports und deren Nutzung finden sich in Abschnitt III.4.1.1.2, „Portweiterleitung am Router“.

III.8.9. LD Mobile im Rev-Proxy freischalten

Wechseln Sie in den Puppeteer:

```
lxc-ssh -n puppeteer
```

Wechseln Sie in das Verzeichnis zur Konfiguration des Reverse-Proxy:

```
cd /etc/logodidact/hosts/rev-proxy
```

Öffnen Sie die Datei `revproxy.conf` und ergänzen Sie diese mit einem Eintrag für LD Mobile:

```
[ReverseProxy mrbs.musterstadt-gym.logoip.de]
Url http://mrbs
```

```
[ReverseProxy unifi.musterstadt-gym.logoip.de]
Url https://unifi:443
```

```
[ReverseProxy ldmobile.musterstadt-gym.logoip.de]
Url http://ldmobile:8080
Template ldmobile
```

Das Schulkürzel entspricht dabei Ihrem individuell festgelegten Namen. Bitte beachten Sie bei **LD Mobile** die zusätzliche Angabe des Ports 8080 und Zeile mit dem Eintrag `Template ldmobile`.

Pflegen Sie die Änderungen wie gewohnt ins `git` ein:

```
cd /etc/logodidact
```

```
git add .
```

```
git commit -m "LD Mobile über rev-proxy freischalten"
```

III.8.10. Zertifikat für LD Mobile aktivieren

Bevor Sie das Zertifikat versuchen zu erstellen, prüfen Sie kurz die Verfügbarkeit der Zertifizierungsstelle. Gehen Sie dazu mit einem Webbrowser auf die Internetseite `https://letsencrypt.status.io/` und prüfen Sie, ob die Dienste dort verfügbar sind oder es eventuell Probleme gibt.



Achtung

Ab Puppet-Release 1.4.1-x steht für das Beantragen und Erneuern von Let's Encrypt Zertifikaten das modernere Tool **acme.sh** zur Verfügung.

Bitte beachten Sie, dass **acme.sh** nicht automatisch aktiviert wird, sondern Sie dies einmalig manuell umstellen und danach alle Zertifikate neu beantragen müssen.

Infos dazu finden Sie in Abschnitt III.3.6.3.1, „Umstellung auf das Tool `acme.sh`“

III.8.10.1. Zertifikat mit `acme.sh` beantragen

Wechseln Sie in den Container `Puppeteer` und geben dort den Befehl **sle** ein, um in die Umgebung zur Verwaltung der Zertifikate über **acme.sh** zu gelangen:

```
sle
```

Beantragen Sie dort das Zertifikat über folgenden Befehl:

```
issue ldmobile.schulkuerzel.logoip.de
```

Hierbei steht **schulkuerzel** für den bereits mehrfach verwendeten individuellen Namen (z.B. `musterstadt-gym`). Bei **acme.sh** erhält man eine sehr ausführliche Rückmeldung mit vielen Informationen.

Einen Überblick der darüber verwalteten Zertifikate erhält man per:

```
acme.sh --list
```

Wenn das Zertifikat erstellt und heruntergeladen wurde, landet es über Puppet irgendwann im Container **rev-proxy** im Ordner `/etc/nginx/ssl`. Das Ganze lässt sich ggf. wieder über einen **prun** im **puppeteer** und danach im **rev-proxy** beschleunigen.

III.8.10.2. Zertifikat mit acmetool beantragen

Sofern noch das alte Tool genutzt wird, fordern Sie ein Zertifikat von Let's Encrypt für den Container `ldmobile` wie folgt an:

```
acmetool want ldmobile.schulkuerzel.logoip.de
```

Wenn keine Rückmeldung erfolgt, läuft der Antrag. Mit dem folgenden Befehl kann man den Status prüfen:

```
acmetool status
```

III.8.11. Ports für Apple- und Google-Server freischalten

Damit sich die Tablets an den Servern von Apple bzw. Google auch anmelden können, müssen bestimmte Ports in der Firewall des **logosrv** nach außen geöffnet werden.

Wechseln Sie in den Container `logosrv`:

```
lxc-ssh -n logosrv
```

Wechseln Sie in das Verzeichnis `/etc/logodidact/` und editieren Sie die Datei `internet.conf` mit einem Editor Ihrer Wahl, wie z.B. Nano:

```
cd /etc/logodidact
```

```
nano internet.conf
```

Navigieren Sie zum Eintrag `ToInternetAllowTCP` und ergänzen Sie die Einträge um die jeweiligen Ports für die eingesetzten Geräte.

Plattform:	Port:	Richtung:	Beschreibung:
iPad/Apple	2195	ausgehend	Apple Push
	2196	ausgehend	Apple Push
	2197	ausgehend	Apple Push
	5223	ausgehend	iOS Client Verbindung zu Apple Push Notification Service
Andro- id/Google	5228	ausgehend	Android Tablet Verbindung zu Google Cloud Messaging
	5229	ausgehend	Android Tablet Verbindung zu Google Cloud Messaging
	5230	ausgehend	Android Tablet Verbindung zu Google Cloud Messaging

Je nachdem, ob Sie iPads oder Android-Geräte nutzen oder beide Plattformen, tragen Sie die Ports für den Zugriff auf die Server von Apple und Google ein. Im folgenden Beispiel ist die per Standard vorhandene Zeile um zwei weitere Zeilen ergänzt und es werden alle notwendigen Ports sowohl für iPads als auch Android-Tablets geöffnet. Speziell für das Management von iPads sollte der gesamte

Adressblock 17.0.0.0/8 für die Apple-Server in der Firewall freigeschaltet und auch der Port 2197 geöffnet werden (Quelle: <https://support.apple.com/de-de/HT203609>).

```
ToInternetAllowTCP ftp, ftp-data, https
ToInternetAllowTCP 2195, 2196, 2197, 5223, 5228, 5229, 5230
ToInternetAllow 17.0.0.0/8
```

Durch Eingabe der Tastenkombination <Strg>+<X> verlassen Sie den Editor und geben „Y“ ein, damit die Änderung gespeichert. Anschließend muss der Befehl **ldfirewall restart** im Container logosrv eingegeben werden, um die Firewall neu zu starten.

Im Zusammenhang mit der Freischaltung der Ports, sollten auch der Webfilter angepasst werden, so dass die beiden Seiten **apple.com** und **aaplimg.com** auf der Allowlist stehen und problemlos erreichbar sind. Dies können Sie ebenfalls direkt im **logosrv** auf Kommandozeilebene über die folgende Eingabe erledigen:

```
ldwebfilter -w apple.com
```

```
ldwebfilter -w aaplimg.com
```

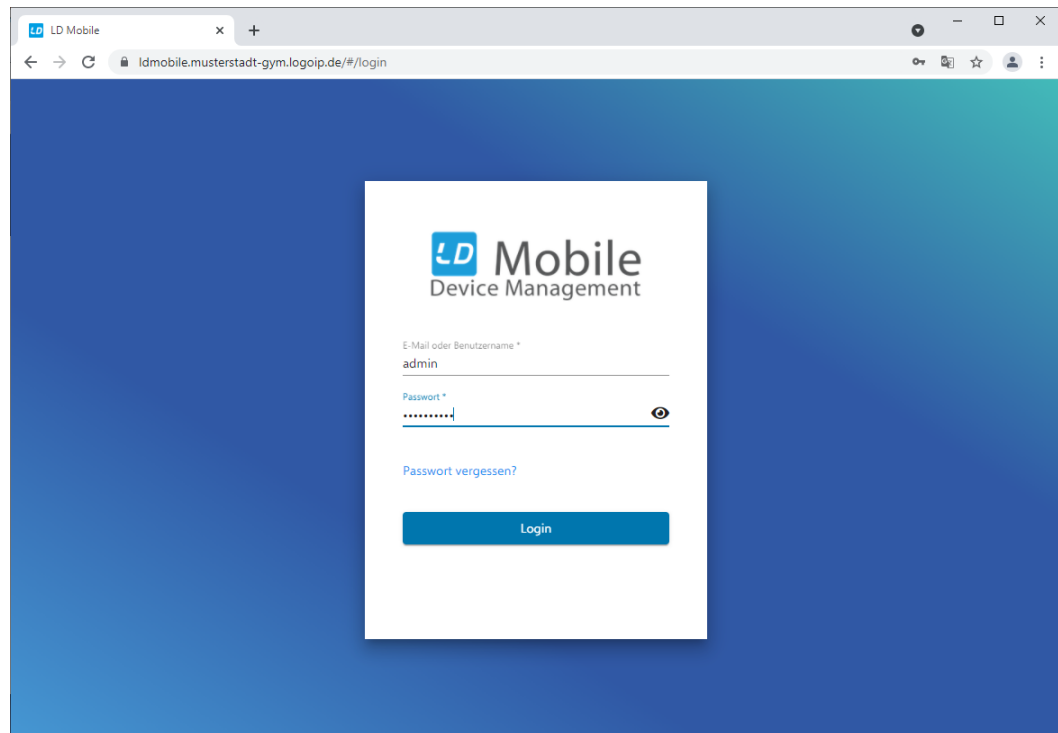
III.8.12. Admin-Anmeldung in LD Mobile

Die Administration von **LD Mobile** erfolgt über ein Webinterface, das entsprechend sowohl intern als auch über den **Reverse-Proxy** von extern zu erreichen ist. In unserer Beispielumgebung über

<https://ldmobile.schule.local> (schulintern)

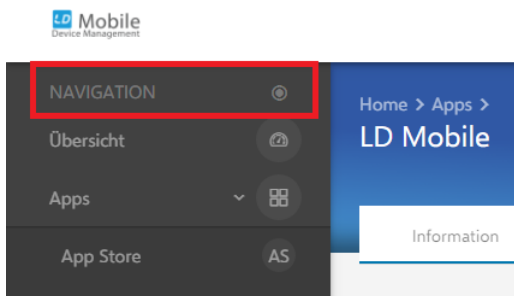
<https://ldmobile.musterstadt-gym.logoip.de> (von außen)

Rufen Sie diese Seite über einen Browser auf und melden Sie sich mit den Zugangsdaten des Benutzers **admin** an.

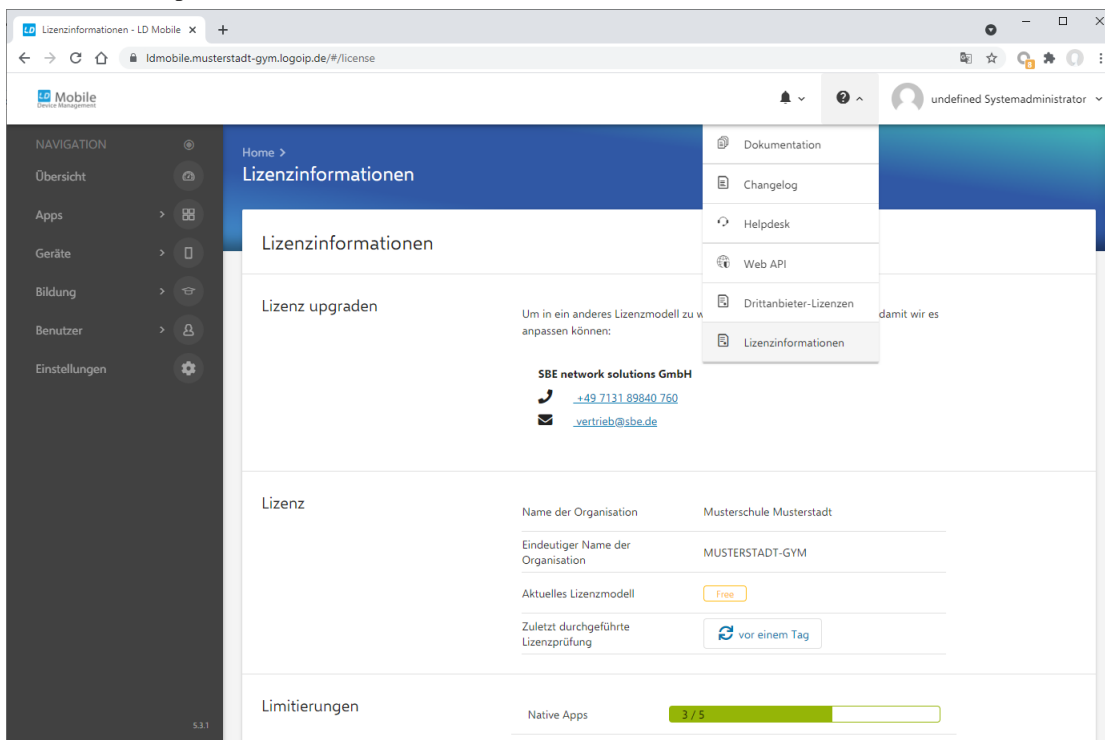


III.8.13. Lizenzen prüfen und anfordern

Im ersten Schritt sollten Sie links oben im Menü die Option **NAVIGATION** aktivieren, damit das Menü aufgeklappt stehen bleibt, was in der Regel deutlich übersichtlicher ist.



Prüfen Sie zunächst, ob eine LD Mobile-Lizenz bereits aktiviert wurde oder der MDM-Server im Lizenzmodus Free läuft. Das können Sie entsprechend über den Menüpunkt ? und den Eintrag **Lizenzinformationen** prüfen.



Achtung

Im Free-Modus können Sie mit **LD Mobile** nichts anfangen. Es gibt diesen Modus nur, damit das Basissystem über das Systemmanagement Puppet automatisiert konfiguriert und betriebsfertig installiert werden kann.

Die Zuordnung der Lizenz zum MDM-Server erfolgt nicht über einen Lizenzkey, den man selbst einspielen könnte, sondern einen Aktivierungsmechanismus auf Herstellerseite.

Die Aktivierung kann erst erfolgen, wenn **LD Mobile** und die dazugehörigen Komponenten fertig installiert sind.

Wenden Sie sich bezüglich der Aktivierung der Lizenz deshalb nun an Ihren LogoDI-DACT Partner über den Sie die **LD Mobile** Lizenzen bezogen haben.

Bitte beachten Sie, dass die Aktivierung der Lizenz unter Umständen auch einige Stunden dauern kann, da sie noch nicht automatisiert ist.

Sobald Sie Rückmeldung haben, dass die Lizenz aktiviert würde, prüfen Sie dies bitte nochmals über das oben beschriebene Vorgehen.

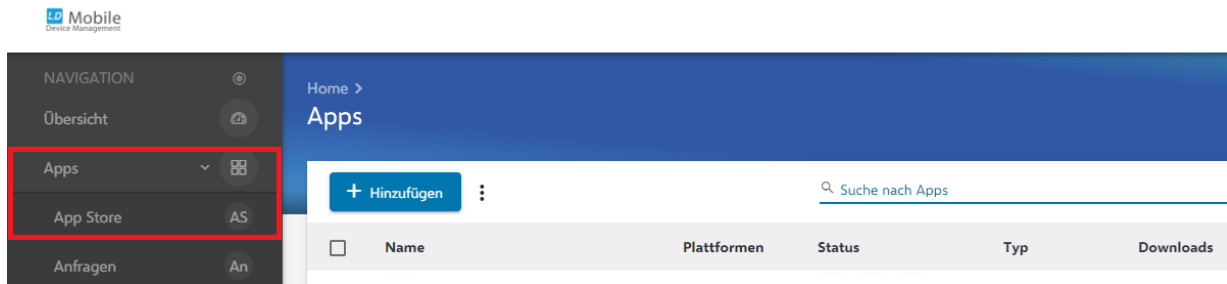
III.8.14. Die LD Mobile APPs zuweisen

Im ersten Schritt laden Sie die aktuellsten **LD Mobile**-APPs für Android und iOS über die folgenden URLs herunter, um diese danach im lokalen App Store abzulegen:

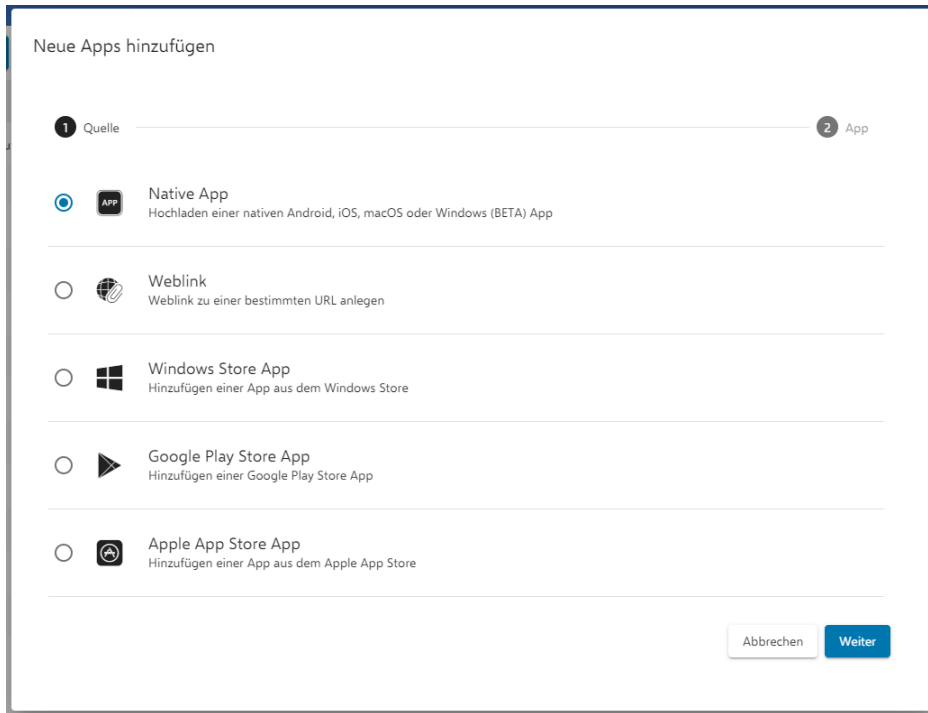
`http://repo.relution.io/apps/android/latest/Relution-sbe-release.apk`

`http://repo.relution.io/apps/ios/latest/Relution_SBE.ipa`

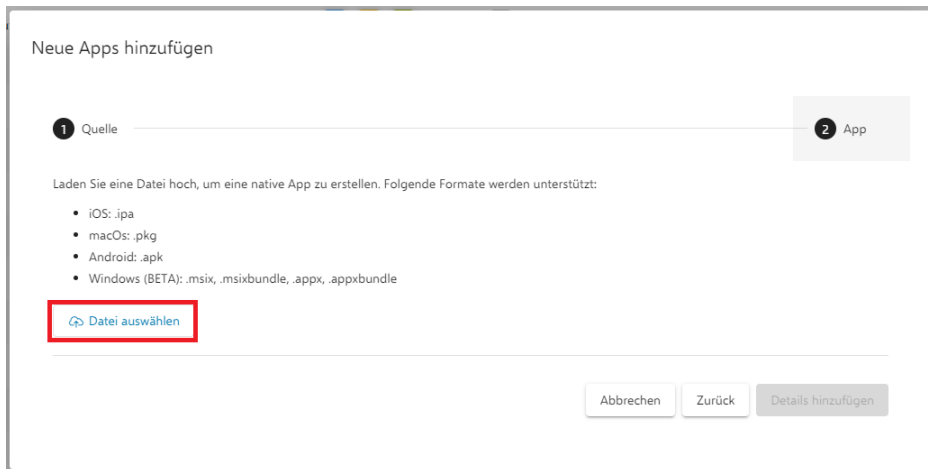
Melden Sie sich als Benutzer admin an der Weboberfläche von LD Mobile an. Über das Menü **Apps** und den Eintrag **App Store** wechseln Sie zum internen **LD Mobile** AppStore.



Wählen Sie dort die Schaltfläche **Hinzufügen** und im darauf folgenden Dialog den Eintrag **Native App**.

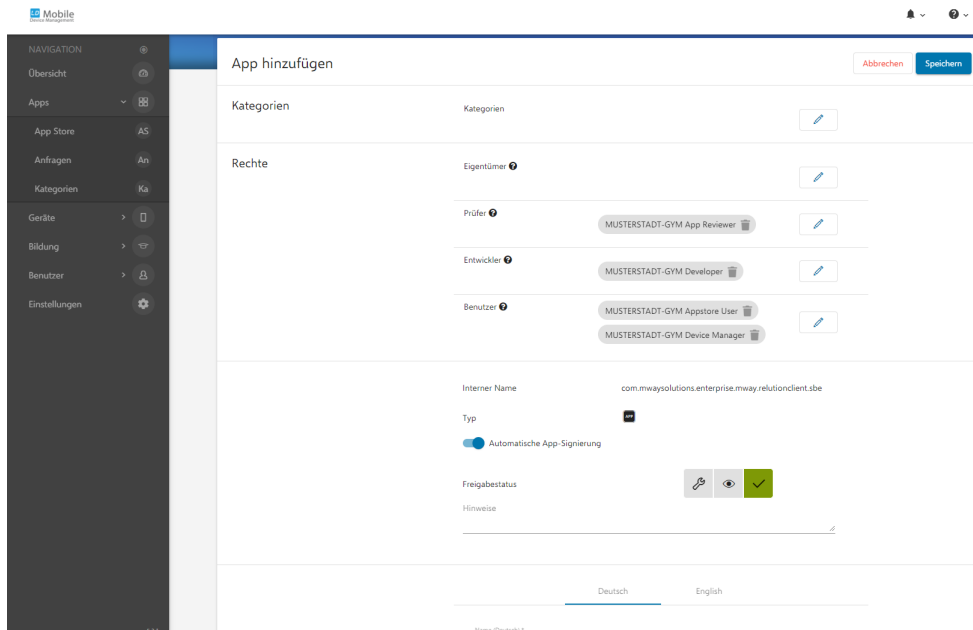


Bestätigen Sie mit **Weiter** und wählen Sie im darauf folgenden Dialog den Eintrag **Datei auswählen**.

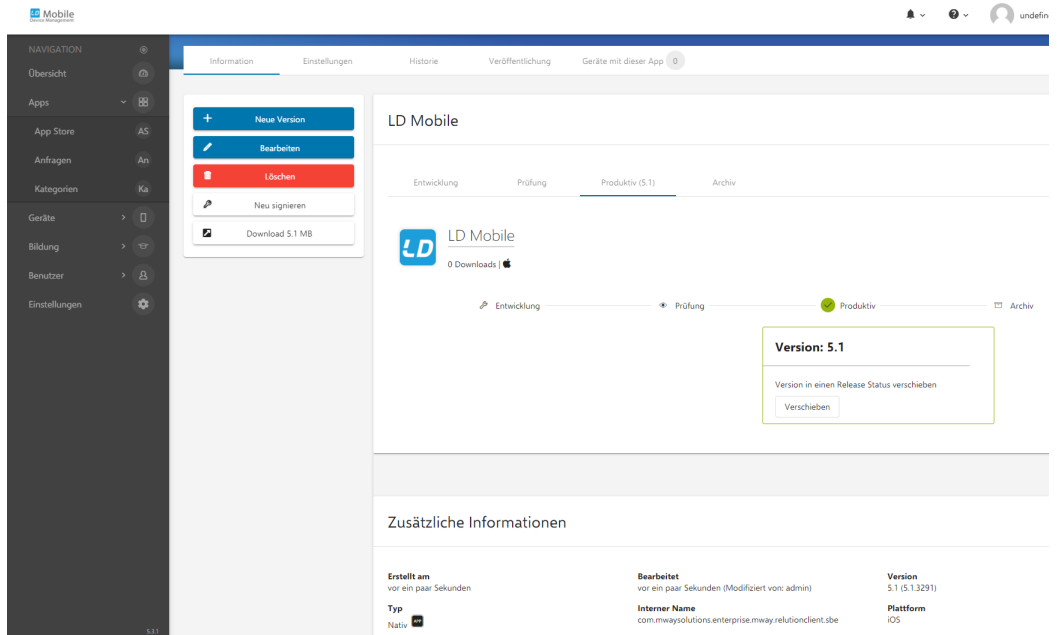


Wählen Sie über die Dateiauswahl die zuvor heruntergeladene Datei **Relution_SBE.ipa**. Diese wird in das System geladen und der Dialog wechselt automatisch zurück.

Scrollen Sie mit der Maus nach Unten bis zum Eintrag **Freigabestatus**. Ändern Sie dort den Freigabestatus über das grüne Häkchen-Symbol auf **produktiv** und wählen Sie anschließend **Speichern**.

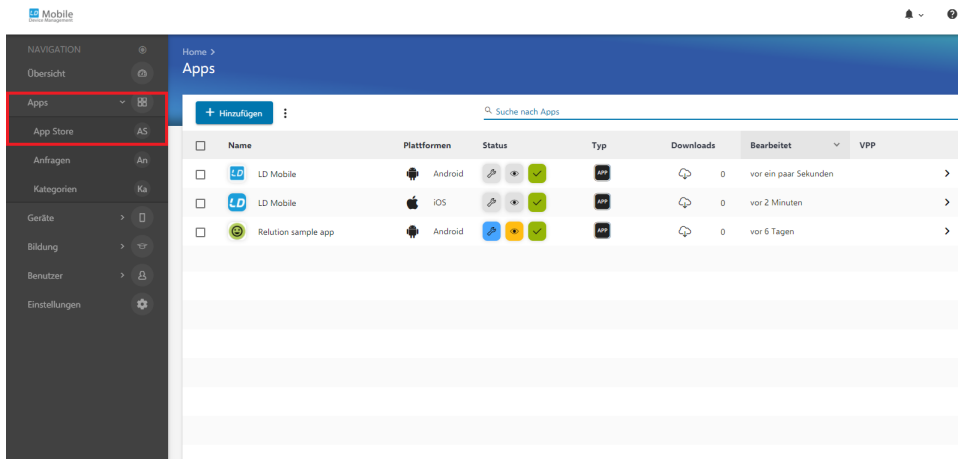


Im Anschluss sehen Sie die Infos zu der gerade geladenen **LD Mobile** App.



Wiederholen Sie diesen Vorgang für die zweite APP bzw. die Datei `Relation-sbe-release.apk`.

Wenn Sie nun wieder das Menü **Apps** und den Eintrag **App Store** aufrufen, sehen Sie die beiden **LD Mobile** APPs für die Plattformen Android und iOS.



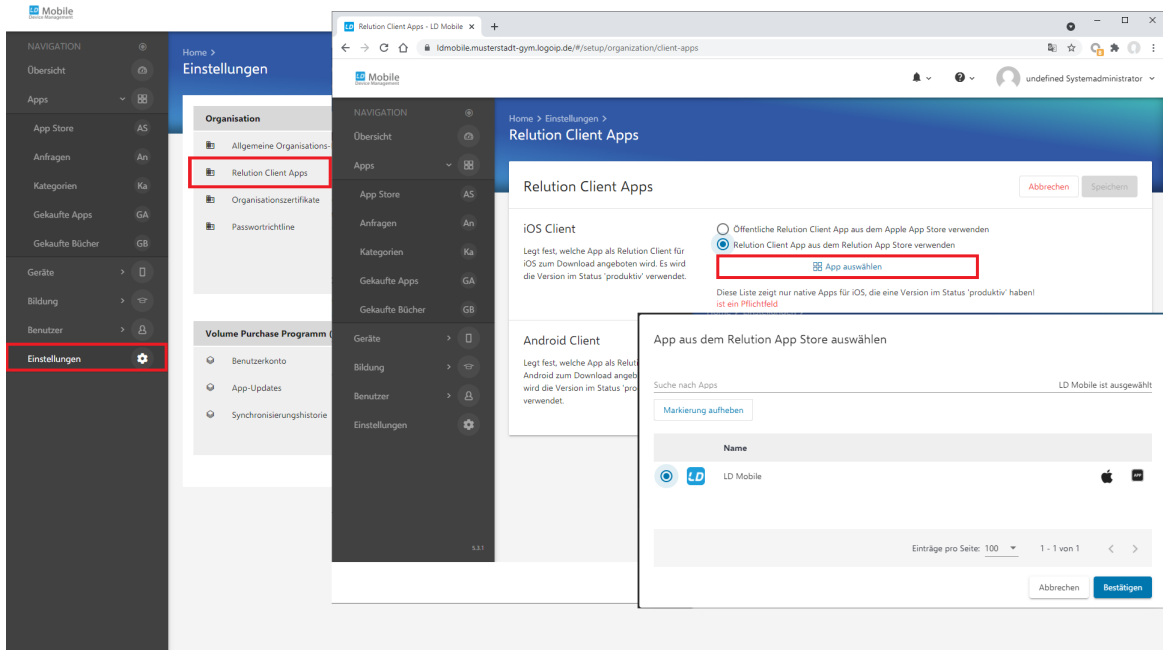
Achtung

Unabhängig davon, ob Sie nur iPads oder Android-Geräte einsetzen, müssen beide **LD Mobile** APPs in den lokalen App-Store geladen werden.

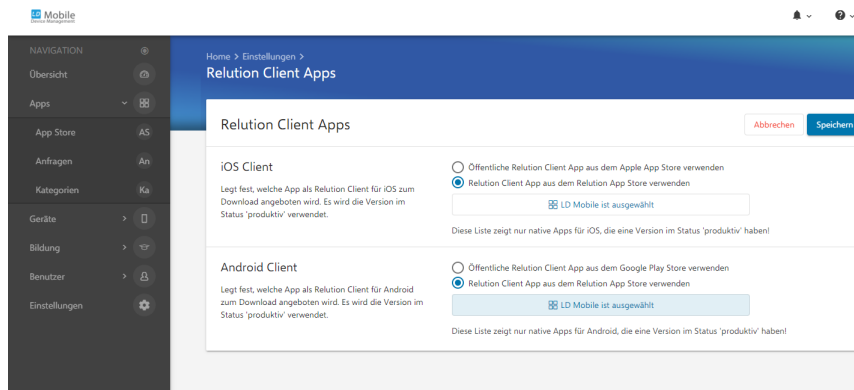
Beide **LD Mobile** APPs müssen ebenso zwingend im Freigabestatus auf produktiv gesetzt werden.

Im letzten Schritt muss noch eingestellt werden, dass das MDM-System diese beiden APPs standardmäßig auf den entsprechenden Tablet-Plattformen nutzt.

Wählen Sie dazu im Menü **Einstellungen** im Bereich **Organisation** den Eintrag **Relution Client Apps** aus. Im Abschnitt iOS Client klicken Sie auf die Option **Relution Client App aus dem Relution App Store verwenden**. Über die Schaltfläche **App auswählen** weisen Sie anschliessend die **LD Mobile** APPs für Apple-Tablets zu. Übernehmen Sie mit **Bestätigen**.



Führen Sie die gleichen Schritte dann auch für Android Clients durch.

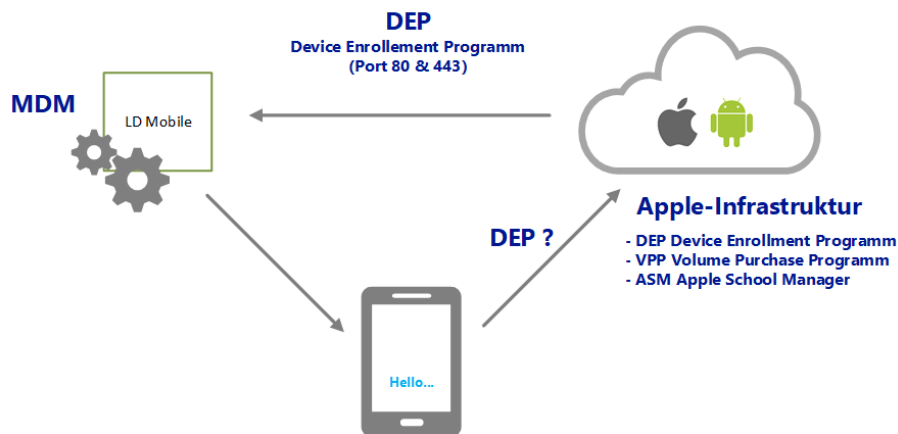


Schliessen Sie den Vorgang ab mit **Speichern**.

III.8.15. Device Enrollment Program - DEP

Das Device Enrollment Program (DEP) ist die Grundlage, um neue Tablets einfach und schnell zu konfigurieren und gleichzeitig im Betrieb durch Manipulationen der Schüler zu schützen. DEP ist dabei ein Programm, das der Hersteller der Plattform bereitstellt und sowohl von Google für Android als auch von Apple für iOS zur Verfügung steht.

In **LD Mobile** werden beide DEP Umgebungen von Apple und Google unterstützt. Wenn ein Gerät sein initiales Setup durchläuft, wie z.B. bei jeder Ersteinrichtung oder auch nach einem Reset, nimmt es (WLAN vorausgesetzt) Verbindung mit seiner jeweiligen Betriebssystem-Plattform auf und fragt im ersten Schritt nach, ob es per DEP verwaltet wird. Falls ja, leitet Apple oder Google die Anfrage des Geräts an das zugeordnete MDM-System weiter.



Damit das Ganze funktioniert, sind zwei Dinge notwendig:

- LD Mobile (das MDM) muss mit der DEP-Infrastruktur von Apple bzw. Google verbunden werden
- Die Endgeräte (iPads/Android) müssen im DEP der jeweiligen Plattform registriert werden

DEP beruht auf einer so genannten Vertrauenskette vom Hersteller über den DEP-Händler (Verkäufer) und den MDM-Anbieter bis hin zum Kunden.

III.8.16. Anbindung an Apple DEP

Bei Apple ist das DEP seit Ende 2017 zusammen mit dem VPP (Volume Purchase Program) für Bildungseinrichtungen im so genannten Apple School Manager (ASM) integriert und über ein Web-

Portal erreichbar. Seit Juli 2018 sind die beiden Bereitstellungsprogramme auch für Unternehmen im Apple Business Manager in einem Portal zusammengefasst.



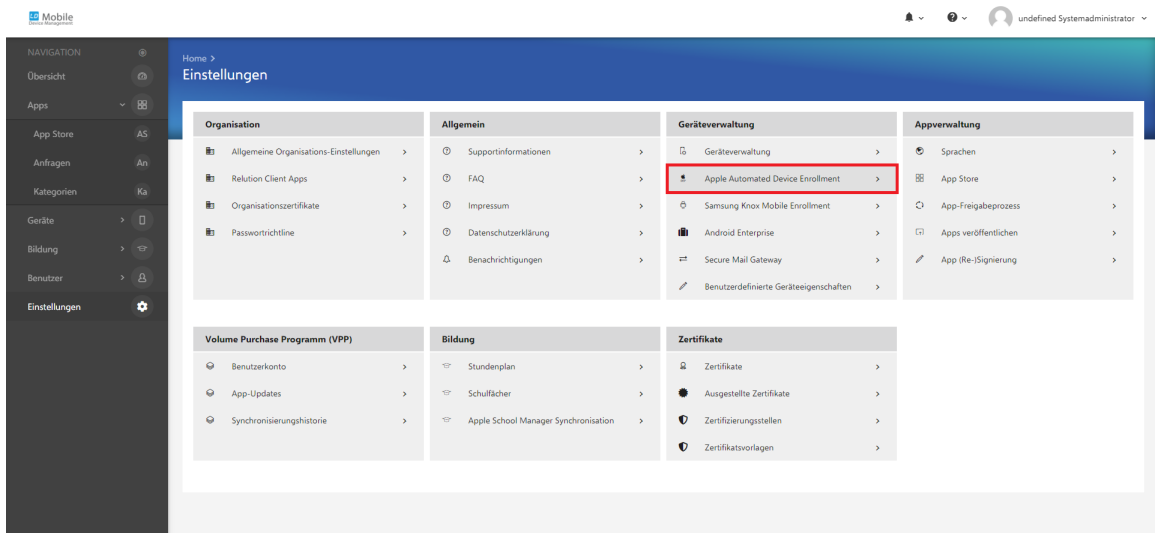
Achtung

Um die Verbindung zwischen LD Mobile und DEP einer Schule herstellen zu können, benötigen Sie Zugriff auf das Apple School Manager Portal der Schule. Wenn Sie als Systemhaus bzw. externer Administrator die Anbindung einrichten und betreuen, kann bzw. muss Ihnen die Schule dazu ein administratives Konto im ASM erstellen.

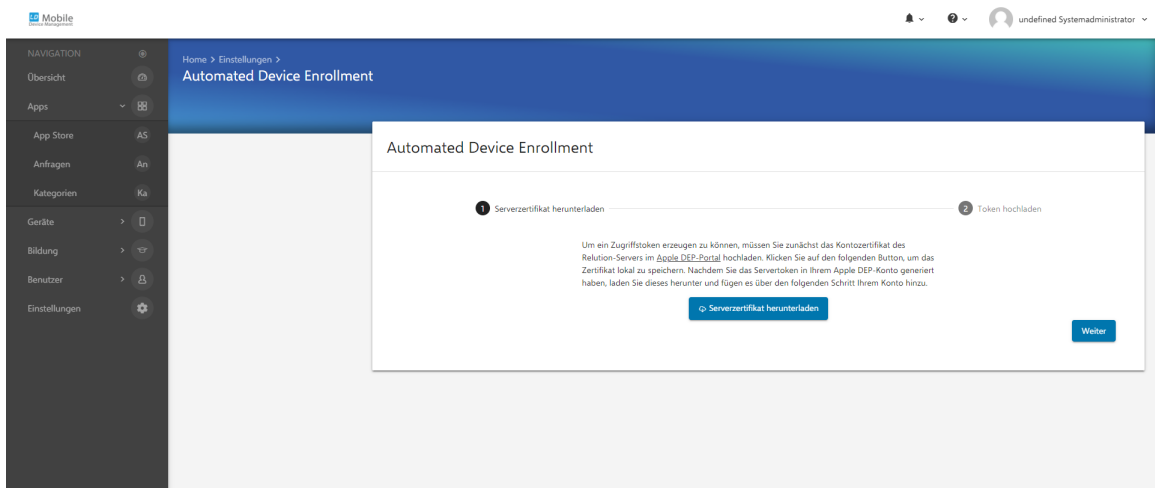
Für weitere Informationen wenden Sie sich an Ihren Fachhändler.

III.8.16.1. Serverzertifikat speichern

Zur Anbinung von LD Mobile an das Apple DEP wählen Sie im Hauptmenü **Einstellungen** und daraus den Eintrag **Apple Automated Device Enrollment**.



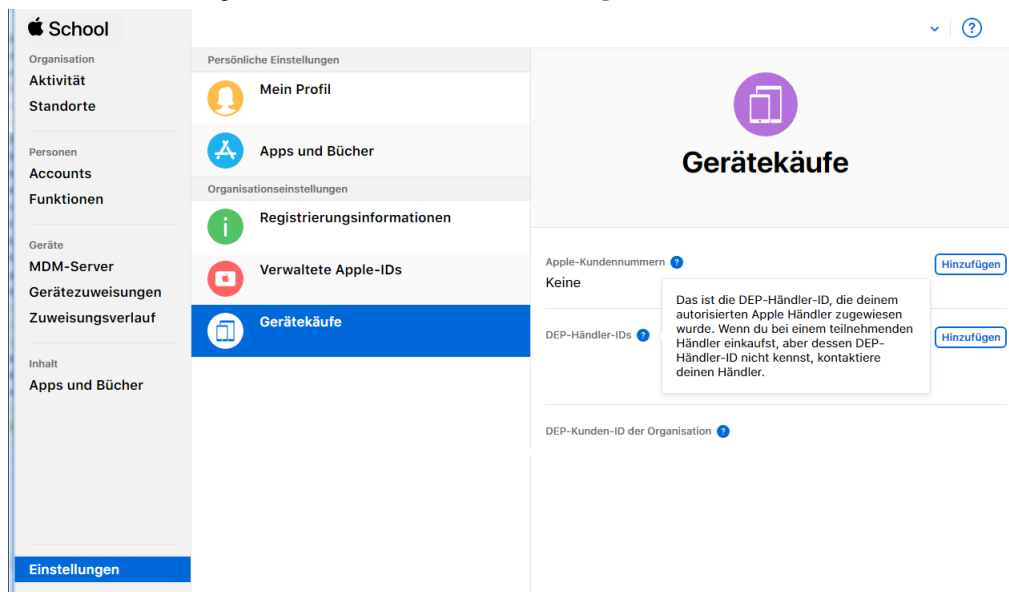
Um den LD Mobile Server mit dem Apple DEP verbinden zu können, wird zunächst ein Konto mit entsprechendem Zertifikat erstellt. Klicken Sie auf die Schaltfläche **Serverzertifikat herunterladen**.



Speichern Sie das Zertifikat lokal ab und merken Sie sich den Speicherort.

III.8.16.2. Im Apple School Manager Portal anmelden

Melden Sie sich am Apple School Manager auf <https://school.apple.com/> an. Prüfen Sie, ob im Portal bereits eine DEP-Händler-ID hinterlegt ist. Gehen Sie dazu über das Menü **Einstellungen** und den Eintrag **Gerätekäufe** in der mittleren Spalte. Falls auf der rechten Seite noch keine DEP-Händler-ID hinterlegt ist, klicken Sie bitte auf **Hinzufügen**.



Achtung

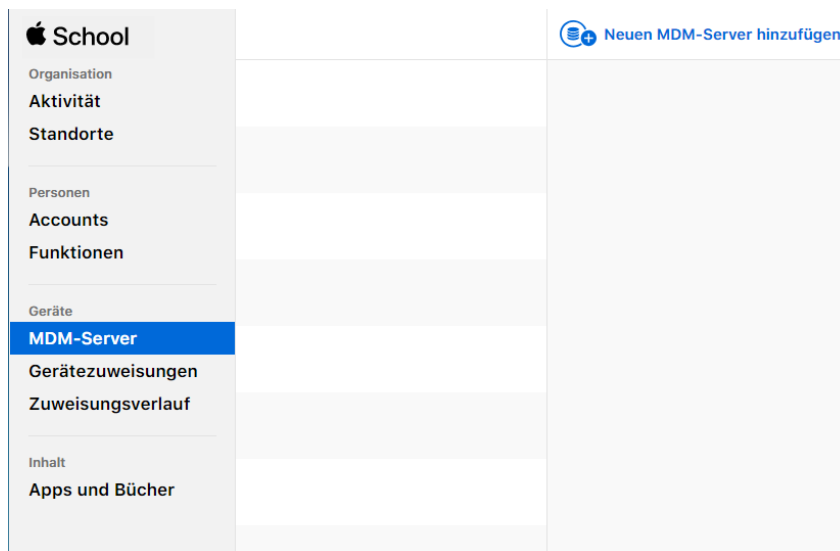
Ohne Angabe einer DEP-Händler-ID, ist die Aufnahme eines MDM Servers nicht möglich.

Falls bisher noch keine Händler-ID eingegeben wurde und Sie keine kennen, tragen Sie in diesen Fall die folgende Nummer ein: **26C9AF0**.

Sie können jeder Zeit weitere DEP-Händler-IDs eintragen.

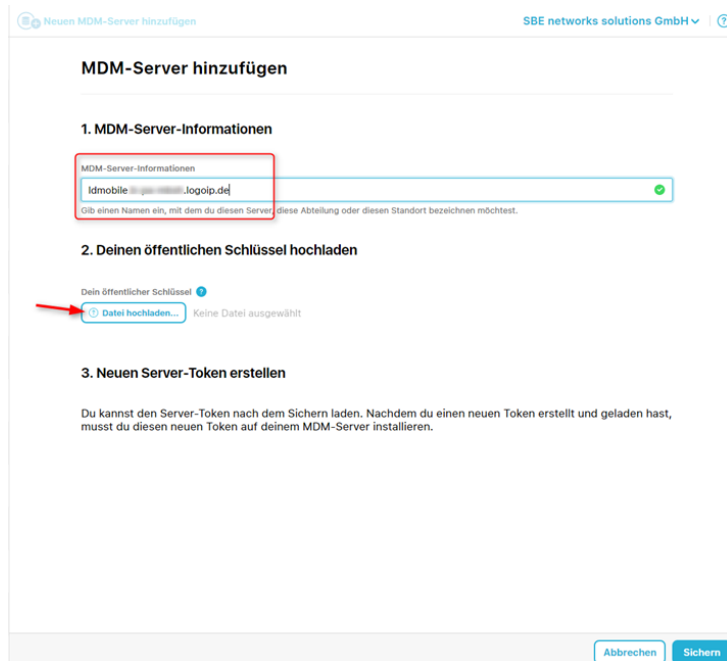
III.8.16.3. MDM-Server hinzufügen und Zertifikat laden

Sobald eine Händler-ID hinzugefügt wurde, ist es auch möglich einen MDM-Server hinzuzufügen. Wählen Sie dazu aus der Menüleiste links den Eintrag **MDM-Server** und dann **Neuen MDM-Server hinzufügen**.

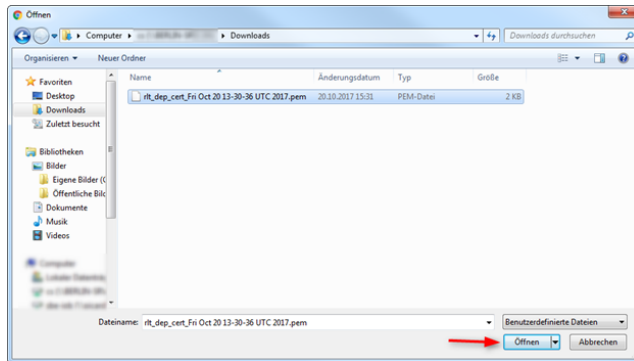


Bitte tragen Sie unter Punkt 1 die öffentliche Adresse Ihrer LD Mobile Installation ein. Diese lautet in der Regel `ldmobile.Schulkürzel.logoip.de`, wobei Schulkürzel wieder dem bereits mehrfach verwendeten Namen entspricht.

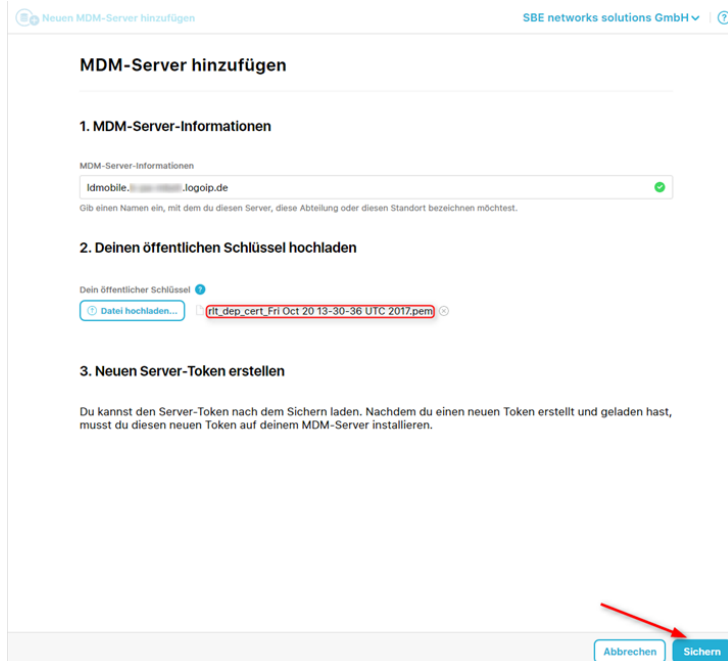
Wählen Sie anschließend unter Punkt 2. die Schaltfläche **Datei hochladen**.



Laden Sie das zuvor aus LD Mobile gespeicherte Zertifikatsdatei und klicken Sie auf **Öffnen**.



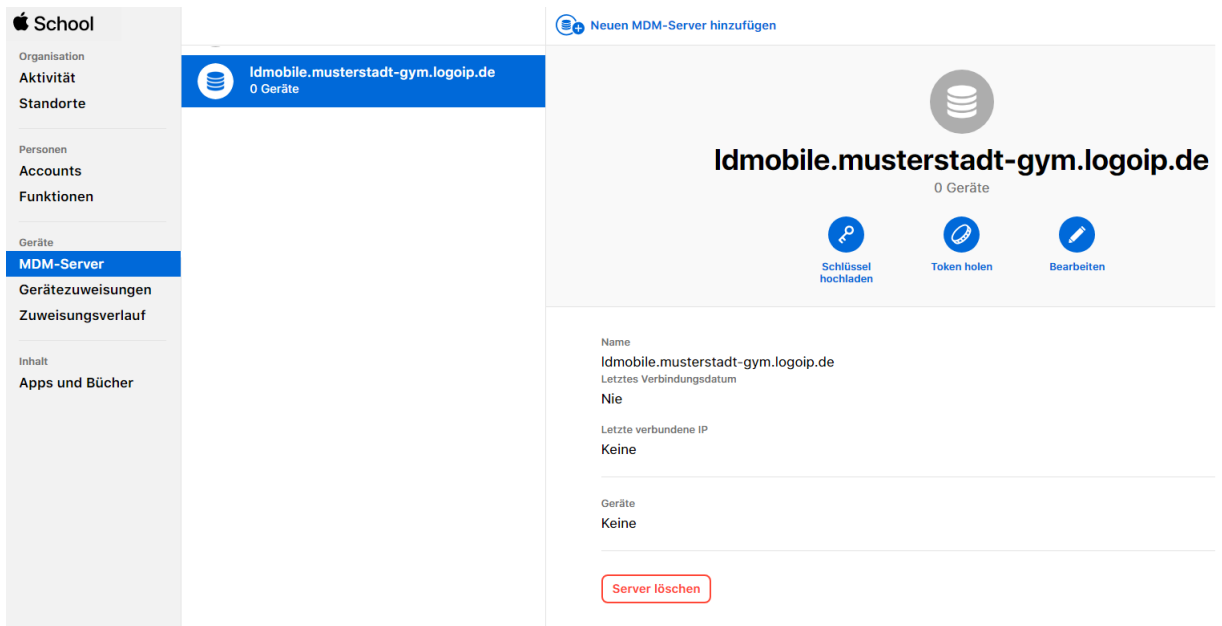
Die ausgewählte Zertifikatsdatei ist nun unter Punkt 2 zu sehen. Speichern Sie das Ganze über die Schaltfläche **Sichern**.




III.8.16.4. Server Token erzeugen

Nachdem die Einstellungen gesichert wurden, ist der LD Mobile Server dem Apple School Manager Account der Schule zugeordnet. Um die Verbindung zwischen Apple School Manager und dem LD Mobile Server auf technischer Ebene herzustellen, muss in LD Mobile ein Token des Apple School Manager eingespielt werden.

Wählen Sie im Menü auf der linken Seite den Eintrag **MDM-Server** und aus der Spalte rechts daneben den gerade erstellten Eintrag für den MDM-Server. Klicken Sie auf **Token holen**, um das Token auf Ihrem Rechner abzuspeichern.




 **Achtung**

Das Erstellen eines neuen Server-Tokens ist denkbar ungeeignet fürs "Herumspielen".

Wenn Sie ein neues Token erstellen, wird das bestehende überschrieben, wodurch die Verbindung zwischen Apple School bzw. DEP und LD Mobile unmittelbar verloren geht.

Unabhängig davon ob bewusst oder versehentlich müssen Sie ein neu erstelltes Token zwingend sofort auch in LD Mobile einspielen.

Beachten Sie den Hinweis und wählen Sie die Schaltfläche **Server-Token laden**.

 **Mit dem Laden eines neuen Server-Token wird dein bestehender Token zurückgesetzt.**

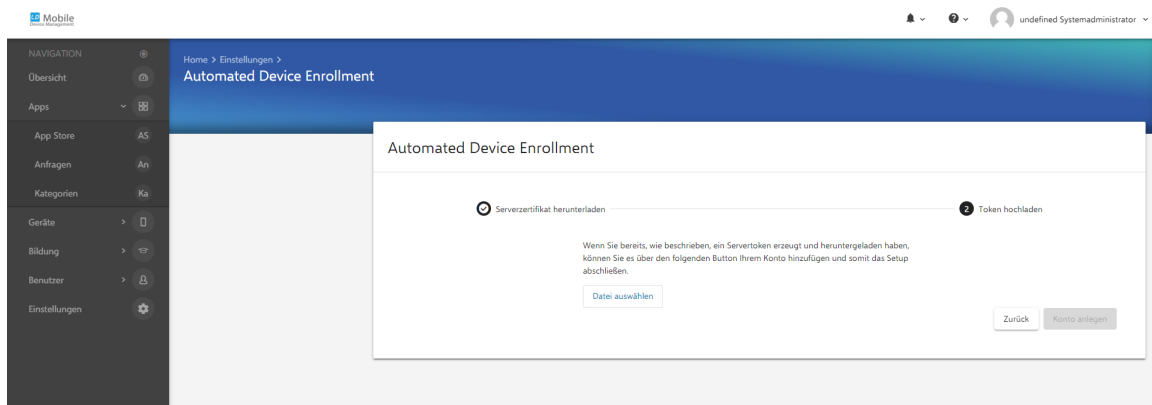
Nachdem du einen neuen Server-Token geladen hast, musst du ihn auf deinen MDM-Server hochladen.

Speichern Sie die Datei lokal ab und merken Sie sich den Speicherort.

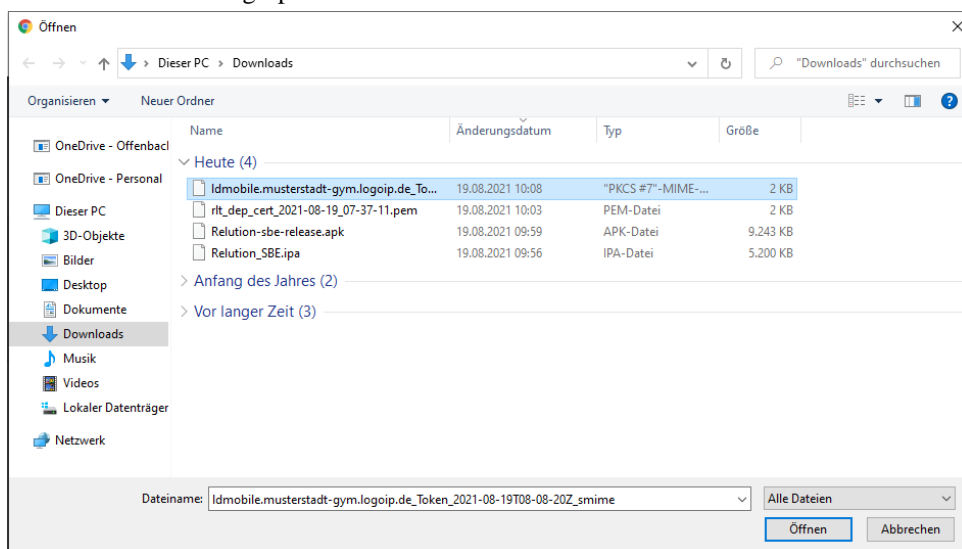
III.8.16.5. Server-Token in LD Mobile laden

Wechseln Sie nun wieder in die Weboberfläche von LD Mobile, um das gespeicherte Token des Apple School Managers hochzuladen.

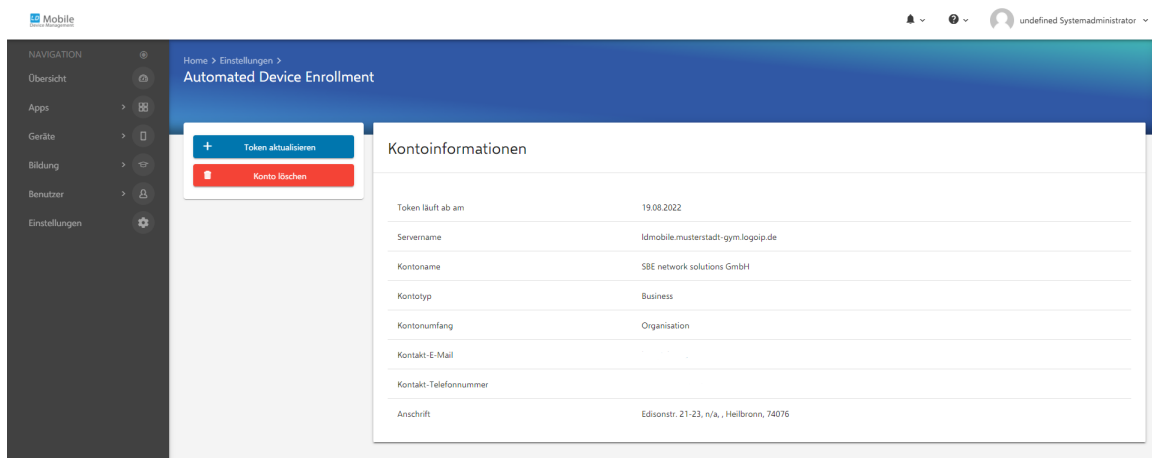
Laden Sie das Token über die Schaltfläche **Datei auswählen**.



Wählen sie das zuvor gespeicherte Token aus.



Abschließend sehen Sie das soeben hochgeladene Token und die Kontoinformationen. Die Informationen zum Konto werden sich automatisch mit dem im Apple School Manager hinterlegten Daten füllen.



Damit ist die Verbindung zwischen DEP und LD Mobile hergestellt.

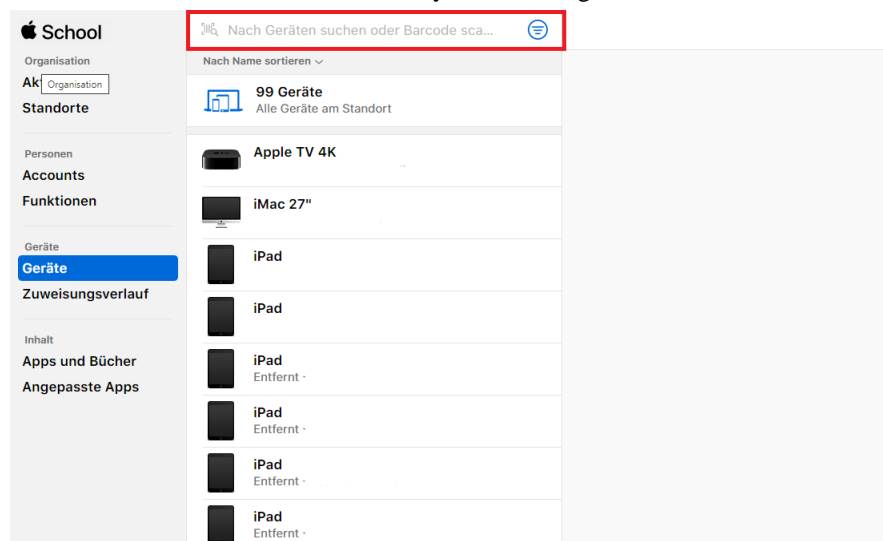
III.8.17. Anbindung an Apple VPP

Wie oben erwähnt ist sowohl das DEP (Device Enrollment Program) als auch das VPP (Volume Purchase Program) seit Ende 2017 für Bildungseinrichtungen im so genannten Apple School Manager (ASM) integriert und über ein Web-Portal erreichbar.

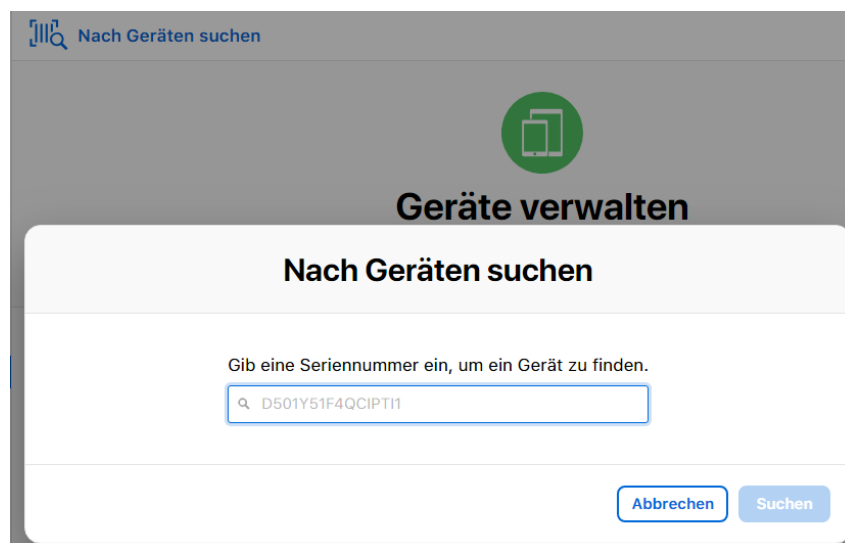
III.8.18. Geräte im ASM zuweisen

Geräte die über den DEP-Fachhandel beschafft wurden, sind über die DEP-Infrastruktur dem jeweiligen Apple School Konto der Schule zugeordnet.

Damit die Geräte aber sichtbar sind, müssen Sie diese über ihre Seriennummer oder Bestellnummer dem jeweiligen MDM zuordnen. Wählen Sie im linken Menü den Eintrag **Geräte**. Wenn Sie viele Geräte auf ein Mal bei einem autorisierten DEP-Fachhändler gekauft haben, ist es am effizientesten, diese über die **Bestellnummer** ins System zu bringen.



Die Bestellnummer erhalten Sie von Ihrem DEP-Fachhändler, von dem Sie die Geräte bezogen haben. Alternativ können Sie die Bestellnummer aber auch über die Eingabe der Seriennummer eines einzelnen Gerätes ermitteln. Gehen Sie auf den Menüeintrag oben **Nach Geräten suchen**, geben Sie die Seriennummer eines Gerätes ein und klicken Sie auf **Suchen**.

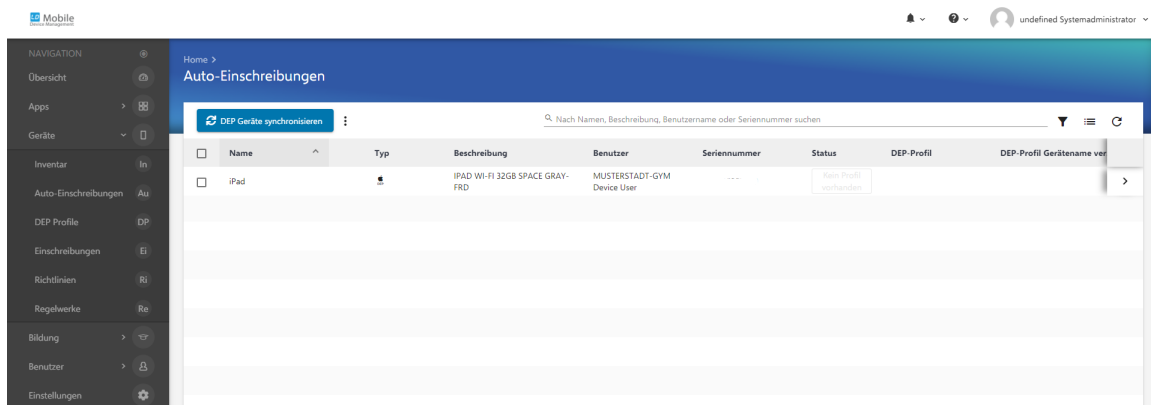


Sofern die Seriennummer existiert, können Sie das Gerät Ihrem MDM zuweisen, falls noch nicht geschehen. Wie oben erwähnt, kommen Sie über die Suche nach einem einzelnen Gerät auch an die Bestellnummer, so dass Sie darüber dann auch alle dabei gekauften Geräte dem MDM zuordnen können.



III.8.19. DEP-Geräte in LD Mobile synchronisieren

Nach der Serverzuweisung der Geräte im Apple School Manager müssen die Geräte ins MDM synchronisiert werden. Wählen Sie dazu in LD Mobile im Hauptmenü den Eintrag **Geräte** und dann **Auto-Einschreibungen**. Klicken Sie auf die Schaltfläche **DEP Geräte synchronisieren**. Anschließend sind die DEP-Geräte in LD Mobile verfügbar.

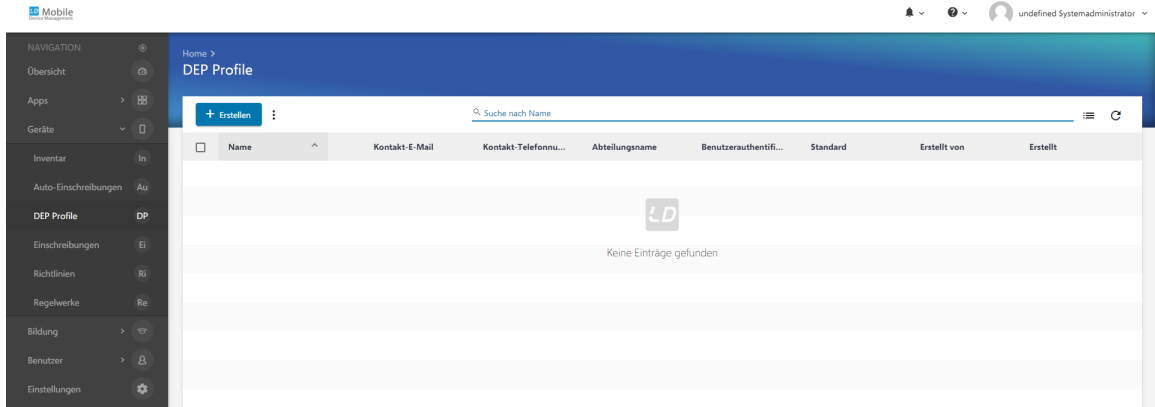


Für die bisherigen Schritte war es nicht notwendig ein iPad real vor Ort zu haben und die gesamte Konfiguration erfolgt letztlich über die Seriennummer eines Gerätes, die Zuordnung diverser IDs und Verbindung zwischen LD Mobile und der DEP-Infrastruktur von Apple.

III.8.20. DEP-Profil erstellen

Der nächste Schritt besteht darin, für die Geräte ein Profil anzulegen. In einem Profil wird festgelegt, wie sich die per DEP registrierten Geräte beim Erstkontakt oder nach einem Reset verhalten.

Wählen Sie aus dem Hauptmenü den Eintrag **Geräte** und dort **DEP-Profile**. Klicken Sie auf die Schaltfläche **Erstellen**.



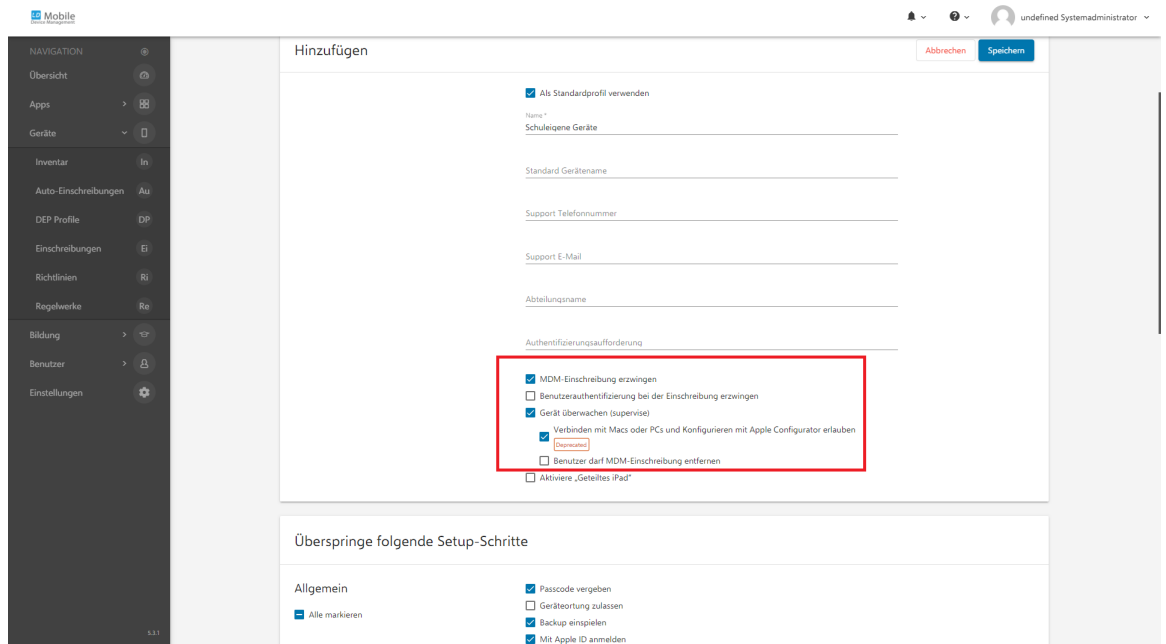
Für die Einstellungen des Profils gibt es im wesentlichen zwei unterschiedliche Einsatzszenarien. Die meisten Schulen fangen beim Einsatz von Tablets mit gemeinsam genutzten Geräten an, was dem Szenario "shared Device" entspricht. Das zweite und von vielen gewünschte Szenario wäre die "1:1" Ausstattung, bei der jeder Schüler sein eigenes Tablet hat, das er auch mit nach Hause nehmen kann und soll.

Abhängig von diesem Szenario gibt es Funktionen, die man im Profil aktiviert oder deaktiviert. Im 1:1 Szenario soll jeder Benutzer individuelle Einstellungen, wie z.B. die eigene Apple ID verwenden, was man beim gemeinsamen genutzten Gerät natürlich explizit nicht will.

III.8.20.1. DEP-Profil für gemeinsam genutzte iPads

Geben Sie dem Profil einen aussagekräftigen Namen und setzen Sie die Markierungen bei **MDM-Einschreibung erzwingen** und **Gerät überwachen (supervise)**

Im Bereich **Überspringe folgende Setup Schritte** legen Sie fest, welche Abfragen und Dialoge am iPad bei der Erstkonfiguration bzw. nach einem Reset erscheinen. Bei gemeinsam genutzten iPads ist es wichtig, dass der Dialog **Geräteortung zulassen** beim Setup erscheint und dann explizit erlaubt bzw. aktiviert werden kann. Die Geräteortung muss zugelassen werden, damit man das iPad im Falle eines Verlusts orten kann. Alle anderen Abfragen können deaktiviert bzw. übersprungen werden.



Wählen Sie rechts oben den Eintrag **Speichern**.

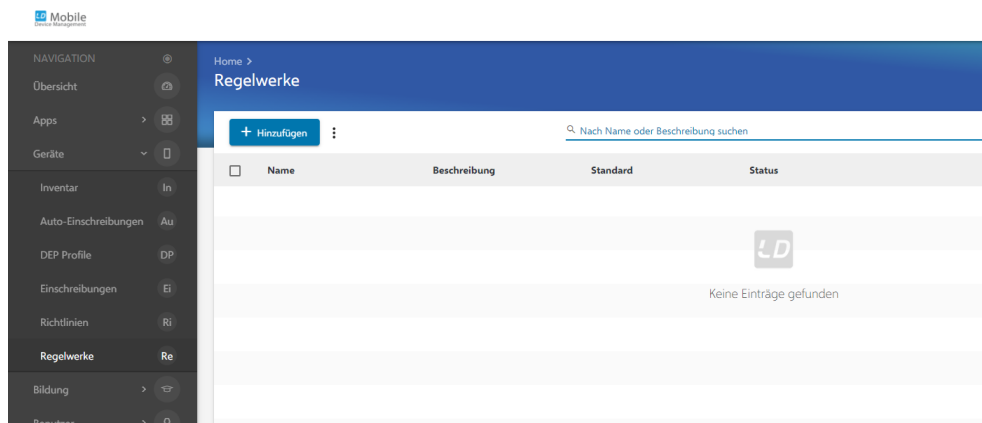
III.8.21. Regelwerk anlegen

Ähnlich wie Profile, sind auch die Regelwerke etwas, was man einmalig bei der Ersteinrichtung von LD Mobile festlegt und im laufenden Betrieb eigentlich nicht mehr verändert. Die Regeln funktionieren nach dem WENN → DANN Prinzip, d.h. es wird festgelegt, welche Aktion ausgeführt werden soll, wenn ein bestimmtes Ereignis auftritt.

Man könnte über eine Regel z.B. ein iPad sperren, wenn die APP-Konformität verletzt ist, d.h., wenn nicht alle APPs auf dem Gerät installiert sind, die es entsprechend der Richtlinie in LD Mobile sein sollen.

Wir empfehlen aber, zunächst nur eine einzige Regel zu definieren und die Konformitätsverletzungen nur informativ an den Administrator per Mail weiterzuleiten.

Um eine Regel zu erstellen, wählen Sie aus dem Menü **Geräte** den Eintrag **Regelwerke** und dann **Hinzufügen**.



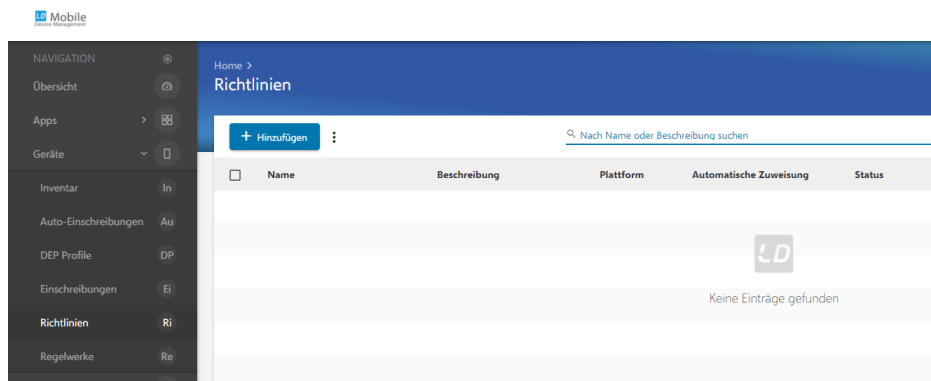
Vergeben Sie für die Regel einen sinnvollen Namen und wählen Sie bei **Ereignistyp** den **Gerätestatus**. Lassen Sie das Feld Konformitätsverletzungen leer, so dass alle Ereignisse informativ gemeldet werden. Legen Sie als **Aktionstyp** fest, dass ausgewählte Benutzer oder Gruppen benachrichtigt werden. Klicken Sie auf die Schaltfläche **Benutzer auswählen und/oder Gruppen auswählen** und wählen sie den Benutzer **admin**.

Als Zeitdauer für die Meldung einer Regelverletzung haben sich 6 Stunden bewährt. Schließen Sie das Ganze ab durch **Speichern** rechts oben.

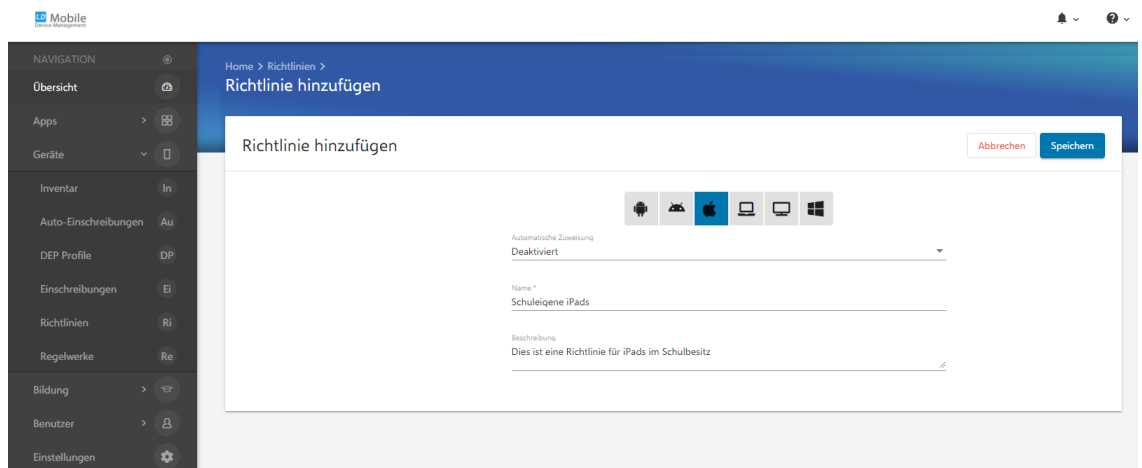
Als letzte Aktion wählen Sie **Veröffentlichen**.

III.8.22. Richtlinien anlegen

Die meisten Änderungen im laufenden Betrieb werden über Richtlinien erstellt. Um eine Richtlinie zu erstellen, wählen Sie aus dem Menü **Geräte** den Eintrag **Richtlinien** und dann **Hinzufügen**.

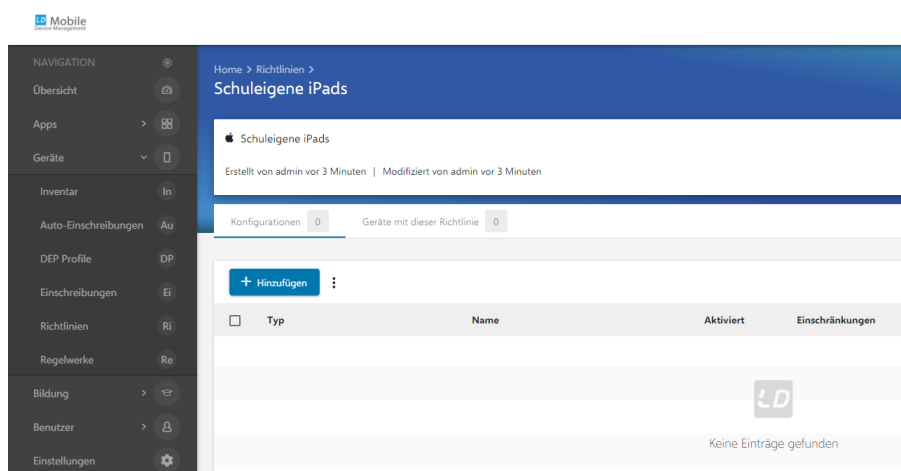


Wählen Sie die Plattform (hier Apple) und vergeben Sie einen aussagekräftigen Namen. Aktivieren Sie den Eintrag **Als Standard-Richtlinie verwenden**, tragen Sie eine Beschreibung ein und wählen Sie **Speichern**.

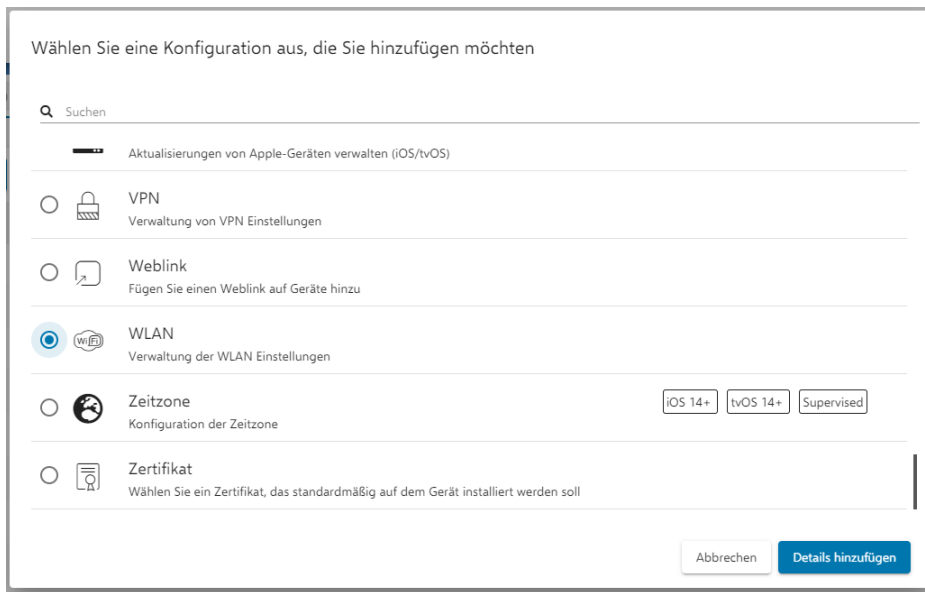


III.8.22.1. WLAN-Richtlinie

Klicken Sie auf die Schaltfläche **Hinzufügen**, um der gerade erstellten Richtlinie "Schuleigene iPads" beispielhaft eine WLAN-Konfiguration zuzuordnen.



Scrollen Sie im Dialog zum Eintrag **WLAN** und klicken Sie auf **Details Hinzufügen**.



Tragen Sie die Daten Ihres WLANs ein, das Sie zuvor z.B. im Unifi-Controller angelegt haben.

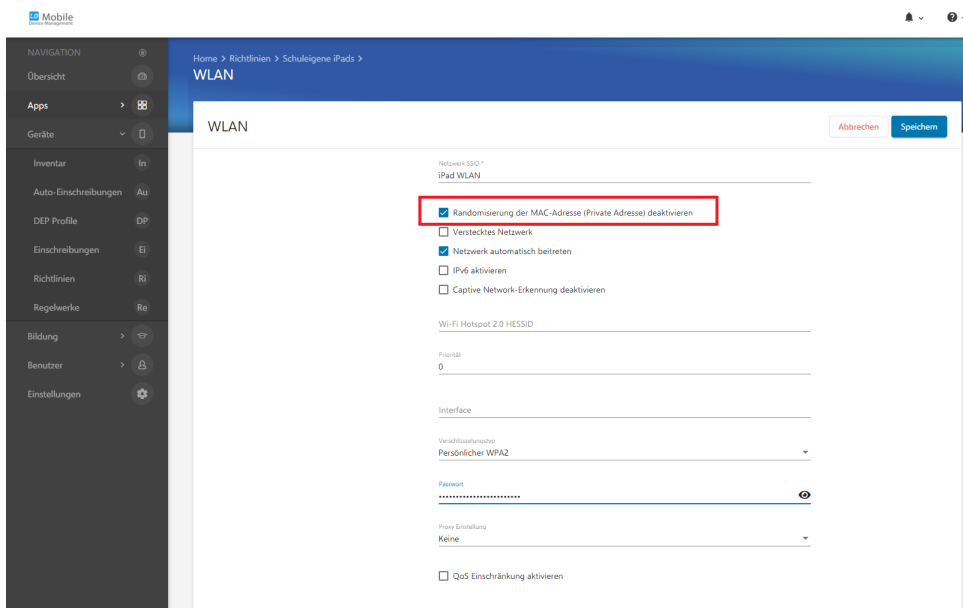


Achtung

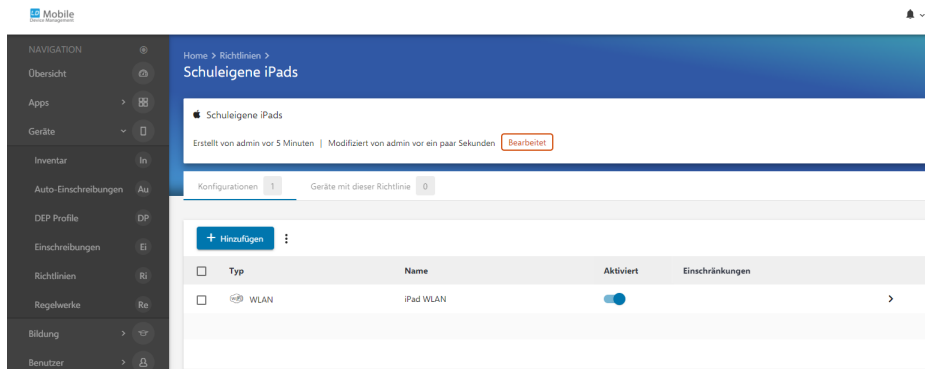
Für iPads wird zwingend ein Netzwerk vom Typ WPA2-PSK benötigt, da sonst über iOS die Zertifikate immer wieder verworfen werden.

Wählen Sie ein hinreichend komplexes Kennwort. Dieses können Sie im Container **Logosrv** mit Hilfe des Befehls **pwgen 32** generieren.

Setzen Sie unbedingt das Häkchen **Randomisierung der MAC-Adresse deaktivieren!**



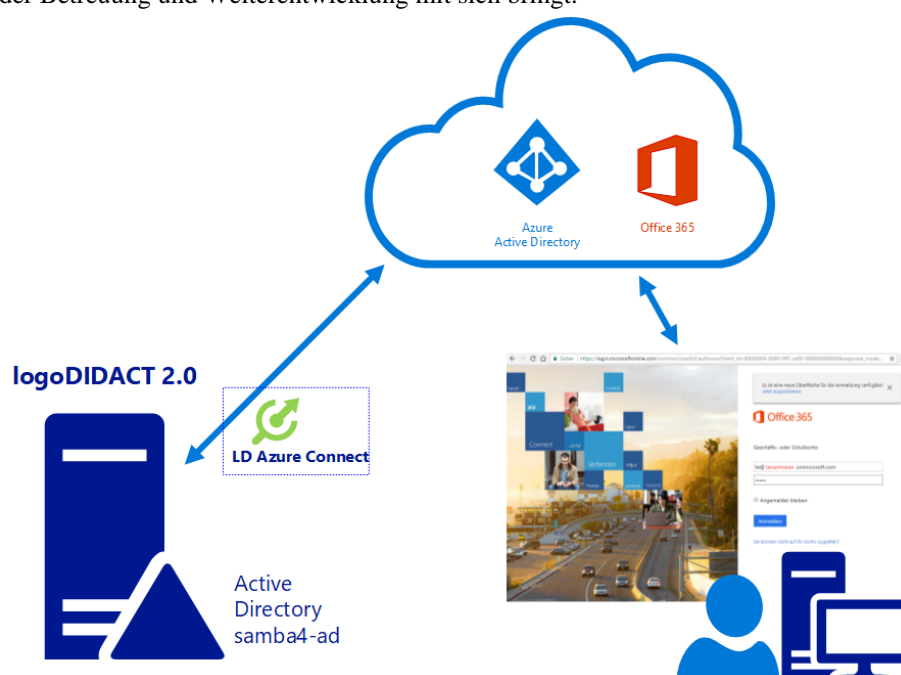
Sichern Sie die Konfiguration durch **Speichern**.



Kapitel III.9. LogoDIDACT an Office 365 ankoppeln

Bereits in 2017 gab es für kurze Zeit eine Möglichkeit der Ankopplung von LogoDIDACT an Azure-AD und die Microsoft Cloud samt Office 365. Für die Anbindung waren jedoch viele Komponenten notwendig, die nicht nur Kosten für die Lizenzierung mit sich brachten, sondern vor allem viel Pflegeaufwand im Betrieb. Zudem wurden für den Betrieb des Windows 2016 Servers in einer KVM deutlich mehr Systemressourcen belegt und notwendig.

Mit dem Modul LD Azure Connect gibt es seit April 2020 nun eine direkte Ankopplung von LogoDIDACT 2.0 an die Microsoft-Cloud, die deutlich schneller, performanter und stabiler ist. Zudem stammt die Entwicklung komplett von SBE, so dass diese Umgebung deutliche weniger Aufwand in der Betreuung und Weiterentwicklung mit sich bringt.



Bei der Ankopplung an die Microsoft-Cloud gibt es aber trotzdem vieles zu beachten und die Kopplung ist weder trivial noch wartungsfrei. Das wird leider allzu häufig vergessen, wenn es um das Thema Cloud geht. Damit die Lösung aus Endkundensicht einfach und zuverlässig funktioniert, entstehen sowohl für die Ersteinrichtung als auch für den laufenden Betrieb entsprechende Kosten für Dienstleistungen. Darüber sollte man sich insbesondere auch bei der Ankopplung von Office365 im Klaren sein.

III.9.1. Office 365 Konfiguration

Bevor man Office 365 beantragt, muss man sich ein paar grundlegende Gedanken zur Nutzung und mit einigen Grundbegriffen vertraut machen.

III.9.1.1. Tenant und Domainname

Der Zugang zu Office365 erfolgt über das Portal `portal.office.com` und die Anmeldung dort nach dem Schema einer Mailadresse:

`benutzername@tenantname.onmicrosoft.com`

Sehr vereinfacht ausgedrückt ist dabei der Tenant erst mal nichts anderes als ein Namensraum, den Sie festlegen müssen, wenn Sie mit Office 365 bzw. Azure AD arbeiten wollen. Bei der Wahl dieses Namens muss man sich bereits im Klaren darüber sein, welche Bedeutung dieser hat und dass man diesen im Nachhinein nicht mehr ändern kann.



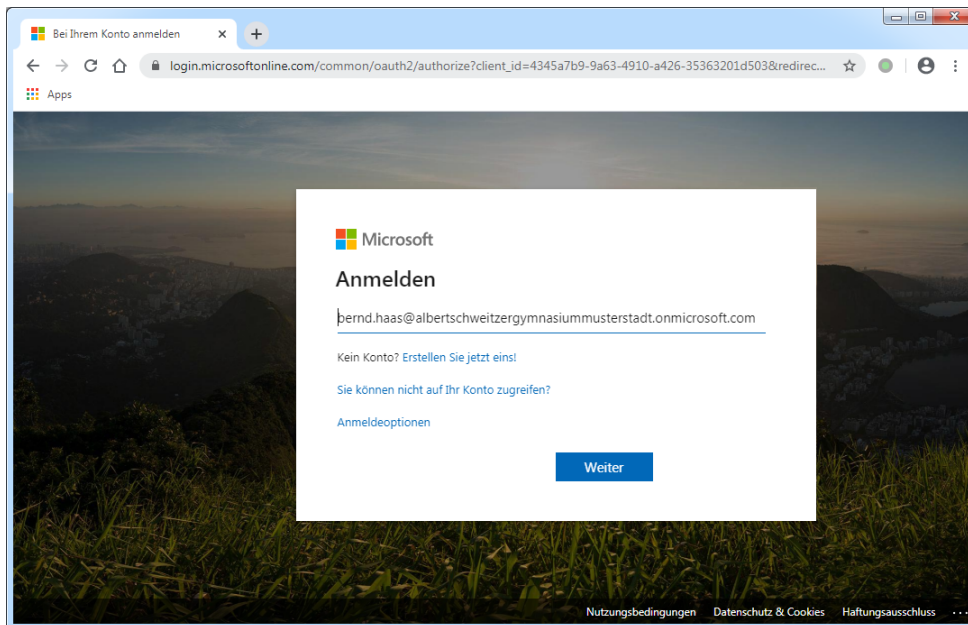
Achtung

Diese Festlegung der Anmeldung an Azure AD bzw. Office 365 über eine eigene Domäne muss man am Anfang als allerersten Schritt treffen und einrichten, noch bevor man mit dem Tenant anfängt zu arbeiten oder eine Ankopplung an LogoDIDACT vornimmt.

Weniger wichtig ist der Tenantname, wenn man diesen ohnehin nicht zur Anmeldung verwendet, sondern eine eigene Domäne nutzt. Dies ist auch die klare Empfehlung, so dass der Anmeldename kürzer und verständlicher wird:

benutzername@ihredomain.de

Je nach Domänenname, kann aber auch dies alles andere als praktikabel sein und Nachteile haben, wie das folgende Beispiel verdeutlicht. Verfügen Sie beispielsweise über die Domäne **Albert-Schweitzer-Gymnasium-Musterstadt.de**, dann wäre damit eine Anmeldung an Office 365 für die Benutzer extrem umständlich, da in Tenantnamen keine Trennzeichen erlaubt sind und das Ganze mit viel Schreibarbeit verbunden und damit fehleranfällig ist.



Ein zweiter Nachteil besteht darin, dass die Anmeldung über die Form einer Mail-Adresse den Benutzern suggeriert, dass sie über die Plattform automatisch auch E-Mail-Funktionalität erhalten. Das ist aber nicht zwingend so. Es ist zwar grundsätzlich möglich, setzt aber voraus, dass die Schule dies nicht bereits an anderer Stelle nutzt., z.B. in einem Verwaltungsnetzwerk, in dem die Schulleitung und eventuell auch das Kollegium Mailadressen nach dem gleichen Schema für genau diese Domäne nutzen.

III.9.1.2. Eine neue Domäne anlegen

Um Konflikte sowohl auf technischer Ebene als auch für die Anwender zu vermeiden, empfehlen wir in jedem Fall eine neue zusätzliche Domäne `*.schule` oder `*.online` anzulegen und diese zu verwenden.

Folgendes Vorgehen ist empfehlenswert:

1. Neue Domäne mit gleichem Namen aber der Endung `*.online`

Wenn Sie an Ihrer Schule eine Homepage haben und eine entsprechende `de`-Domäne besitzen, dann empfehlen wir Ihnen zunächst, eine gleichlautende Domäne mit der Endung `*.online` anzulegen.

Damit ist für alle Benutzer leicht zu erkennen, dass die Anmeldung in Form einer Mail-Adresse nichts mit der Mailfunktionalität zu tun hat, die es für die `de`-Domäne möglicherweise bereits gibt.

Beispiel

- Vorhandene Domäne für Homepage / E-Mail für Verwaltung und eventuell Dienstmail Lehrer

`DOMAINNAME.de`

- Neue Domäne für Office 365 / Videokonferenz / Chat / Lernplattform

`DOMAINNAME.online`

2. Neue Domäne mit kurzem Namen und der Endung `*.online`

Ist Ihre bisherige `de`-Domäne aber ungewöhnlich lange, dann sollten Sie für die `*.online`-Domäne eine praktikable Kurzform davon verwenden.

Beispiel

- Vorhandene Domäne für Homepage / E-Mail für Verwaltung und eventuell Dienstmail Lehrer

`Albert-Schweitzer-Gymnasium-Musterstadt.de`

- Neue Domäne für Office 365 / Videokonferenz / Chat / Lernplattform

`asg-musterstadt.online`

oder

`asgm.online`

Für die Auswahl des Kurznamens ist entscheidend, dass die entsprechende Domäne `*.online` oder `*.schule` noch frei und vor allem auch bezahlbar ist (Prüfung z.B. über `inwx.de`).

III.9.1.3. Tenant und Domäne für Schulträger

Alle im vorherigen Abschnitt aufgeführten Überlegungen sind auch und erst recht auf Schulträgererebene wichtig.



Achtung

Mit der neuesten Version von **LD Azure Connect** lassen sich alle Schulen eines Schulträgers in einem einzigen Tenant in separaten Domains betreiben und die dezentralen LogoDIDACT-Server daran ankoppeln.

Wenden Sie sich bei Interesse an Ihren LogoDIDACT-Partner und erfahrenen Microsoft Cloud Solution Provider.

Vorteile eines Tenants auf Schulträgerebene:

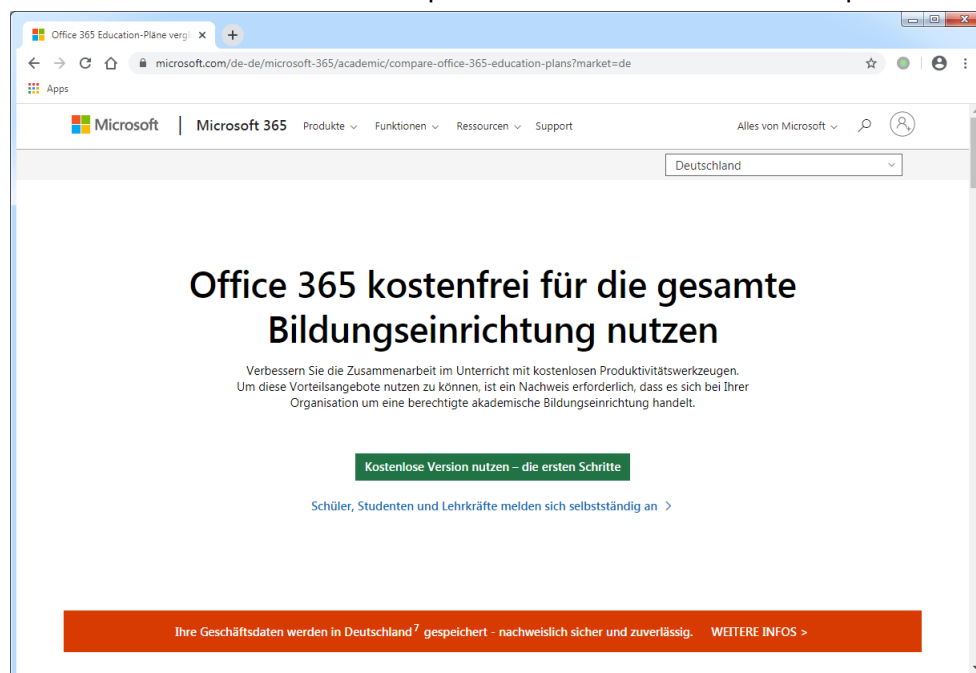
- einfacher und übersichtlicher da alle Schulen zentral in einem Tenant zusammengefasst sind
- Lizenzierung zentral
- geringere Kosten für Ersteinrichtung (1 Tenant für alle anstelle pro Schule ein Tenant)
- geringere Betriebskosten
- erhebliche Kostenersparnis für Microsoft-Vertrag FWU 4.0

III.9.1.4. Das kostenfreie Office 365 A1 beantragen

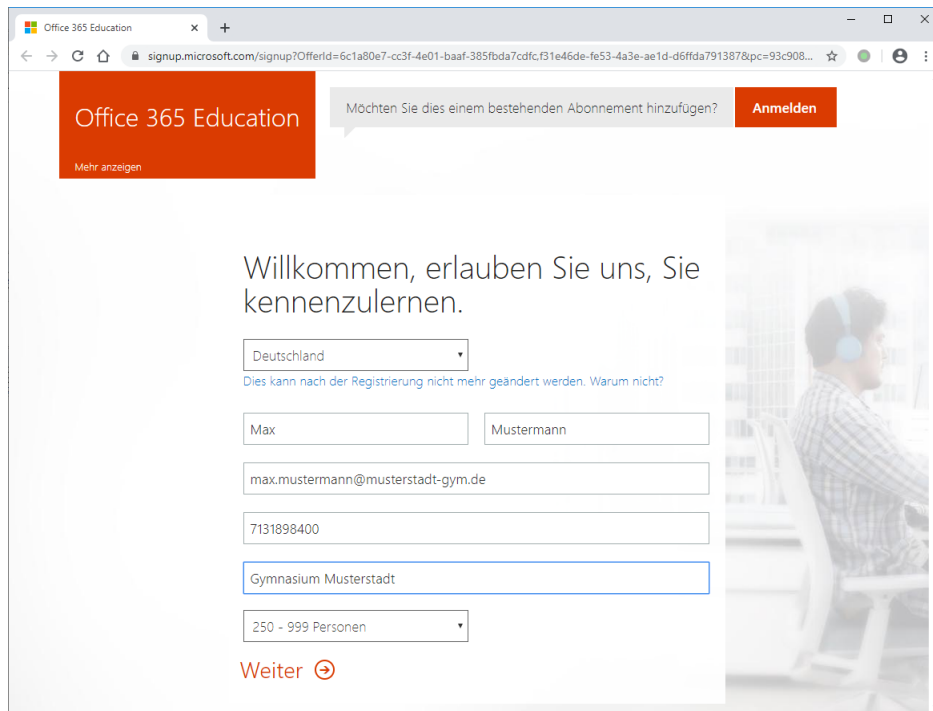
Sie erhalten Office 365 über verschiedene Wege mit unterschiedlichen Leistungen entweder kostenpflichtig (z.B. FWU Vertrag auf Mietbasis) oder auch kostenfrei. Wir behandeln in diesem Abschnitt nur die kostenfreie Variante.

Beantragen können Sie das kostenfrei Office 365 über folgenden Link:

<https://www.microsoft.com/de-de/microsoft-365/academic/compare-office-365-education-plans>

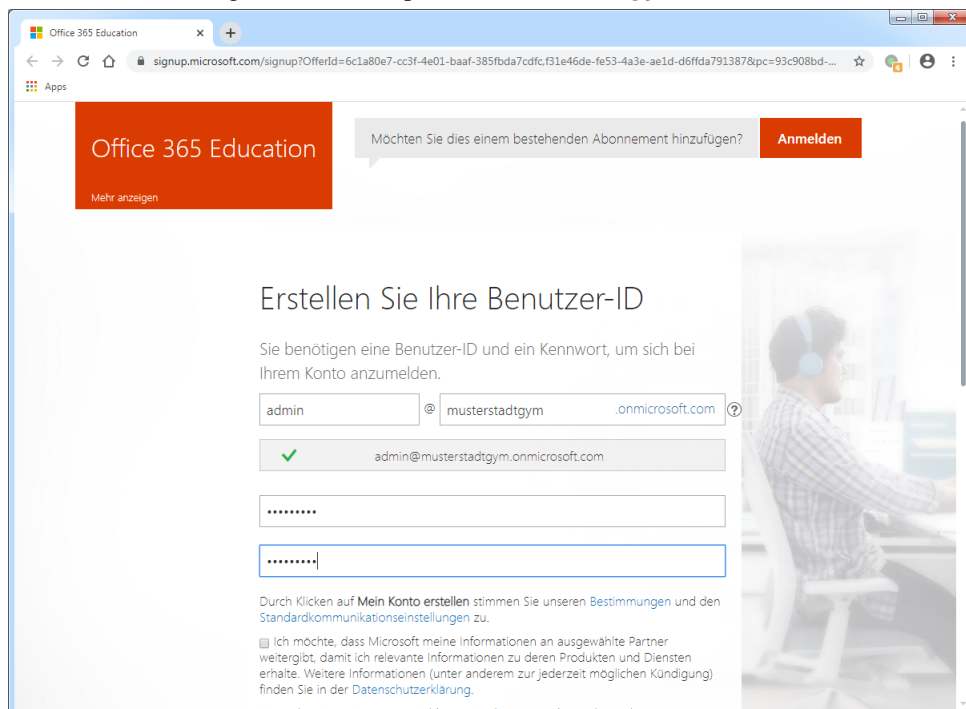


Geben Sie die Daten des Ansprechpartners an der Schule ein, sowie die Telefonnummer und den Namen der Schule. Treffen Sie über das Feld **Größe der Organisation** noch eine zur Schule passende Auswahl.



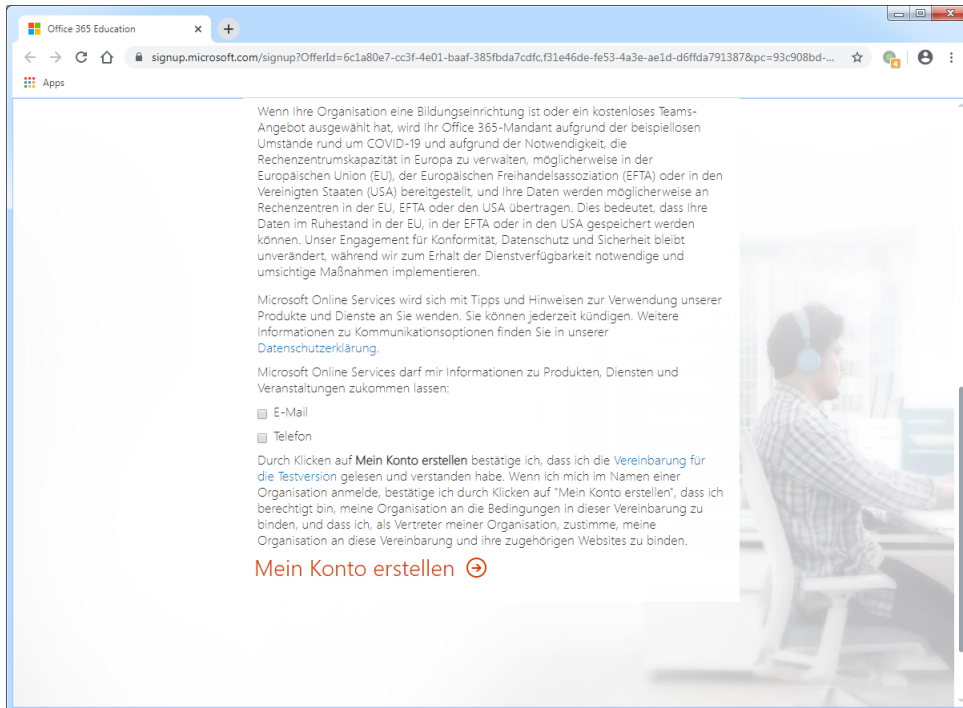
The screenshot shows the Office 365 Education sign-up page. At the top, there is a navigation bar with the Office 365 Education logo and a button labeled 'Anmelden'. Below the navigation bar, the main heading reads 'Willkommen, erlauben Sie uns, Sie kennenzulernen.' The form contains the following fields: a dropdown menu for 'Deutschland', a text input for 'Max', a text input for 'Mustermann', an email input for 'max.mustermann@musterstadt-gym.de', a text input for '7131898400', a text input for 'Gymnasium Musterstadt', and a dropdown menu for '250 - 999 Personen'. A 'Weiter' button with a right arrow icon is located at the bottom of the form.

Im nächsten Schritt wird der Admin-Zugang eingerichtet und der Name des Tenants festgelegt. Beachten Sie hierbei die oben gemachten Empfehlungen. Was den Tenantnamen anbelangt, sollten Sie sich am Namen orientieren, den Sie auch für den Dienst **logoip.de**. Im Beispiel unserer Musterschule wäre dies **musterstadt-gym**. Da im Tenantnamen allerdings keinerlei Bindestriche erlaubt sind, muss man diesen weglassen (im Beispiel **musterstadtgym**).

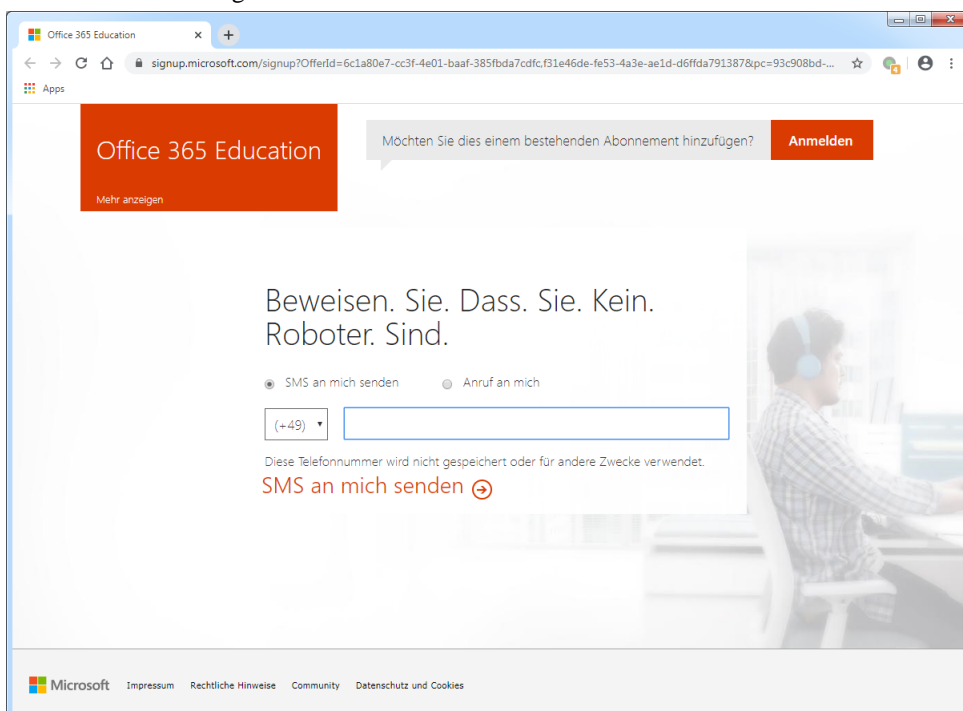


The screenshot shows the Office 365 Education sign-up page at the 'Erstellen Sie Ihre Benutzer-ID' step. The main heading reads 'Erstellen Sie Ihre Benutzer-ID'. Below the heading, the text states: 'Sie benötigen eine Benutzer-ID und ein Kennwort, um sich bei Ihrem Konto anzumelden.' The form contains the following fields: a text input for 'admin', a dropdown menu for '@ musterstadtgym', and a dropdown menu for '.onmicrosoft.com'. A green checkmark icon is visible next to the email address 'admin@musterstadtgym.onmicrosoft.com'. Below the email input, there are two password input fields, both masked with dots. At the bottom of the form, there is a checkbox for 'Ich möchte, dass Microsoft meine Informationen an ausgewählte Partner weitergibt, damit ich relevante Informationen zu deren Produkten und Diensten erhalte. Weitere Informationen (unter anderem zur jederzeit möglichen Kündigung) finden Sie in der Datenschutzerklärung.' and a 'Mein Konto erstellen' button.

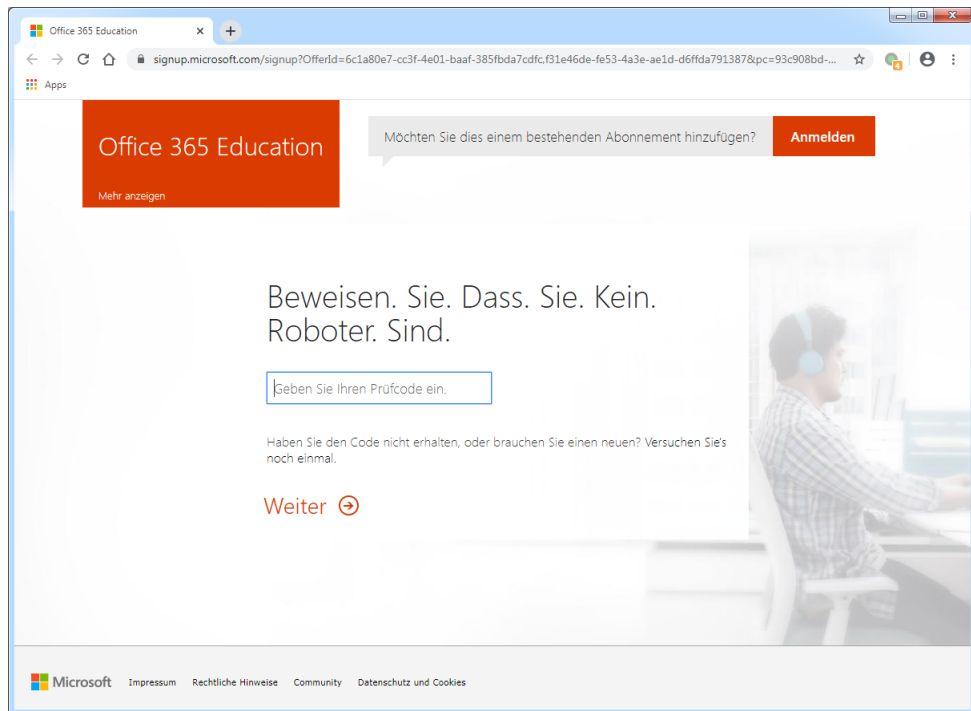
Bestätigen Sie mit Mein Konto erstellen.



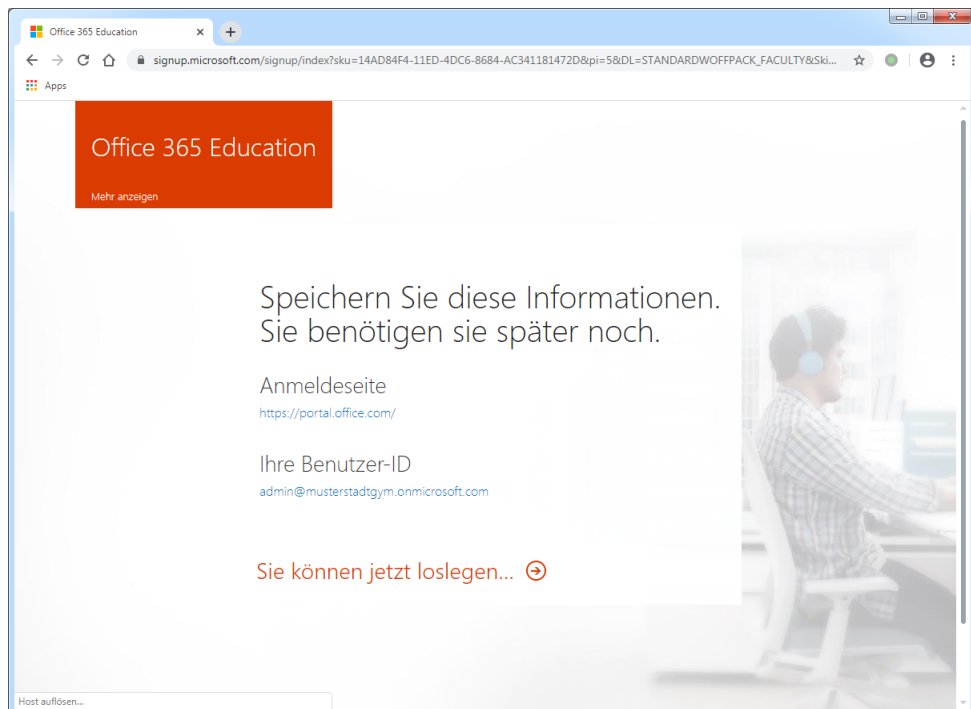
Über die Angabe der Telefonnummer erhalten Sie einen Code, den Sie im nächsten Schritt benötigen. Klicken Sie nach Eingabe der Nummer auf SMS an mich senden.



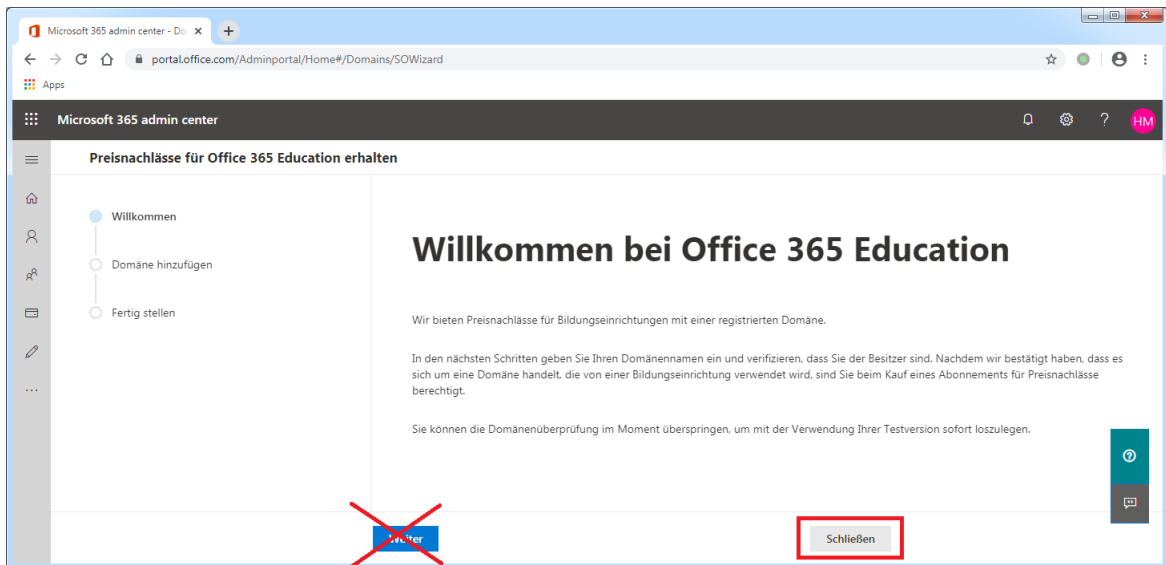
Geben Sie den per SMS erhaltenen Prüfcode ein und klicken Sie auf Weiter.



Die Einrichtung des Tenants dauert einige Augenblicke und sobald verfügbar, wählen Sie **Sie können jetzt loslegen.**



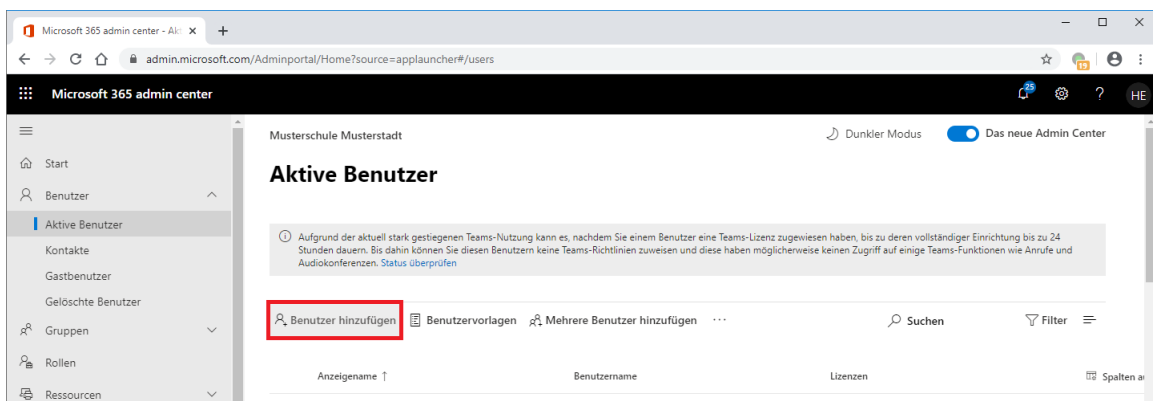
Wählen Sie im nächsten Schritt den Eintrag **Schließen**, denn die weitere Konfiguration soll gerade nicht für den Tenant mit dem etwas sperrigen Namen `musterstadtgym.onmicrosoft.com` erfolgen, sondern für die neu anzulegende Domäne.



III.9.1.5. Ein administratives Konto anlegen

Damit ihr Tenant auf technischer Ebene sauber eingerichtet und konfiguriert wird und auch während des Betriebs fachkundig betreut wird, sollten Sie im ersten Schritt einen administrativen Account für Ihren LogoDIDACT-Partner anlegen.

Öffnen Sie das Microsoft 365 Admin Center mit Ihrem Administratoraccount und wählen Sie aus dem Menü auf der linken Seite **Benutzer** und daraus den Eintrag **Aktive Benutzer** und auf der rechten Seite dann **Benutzer hinzufügen**.

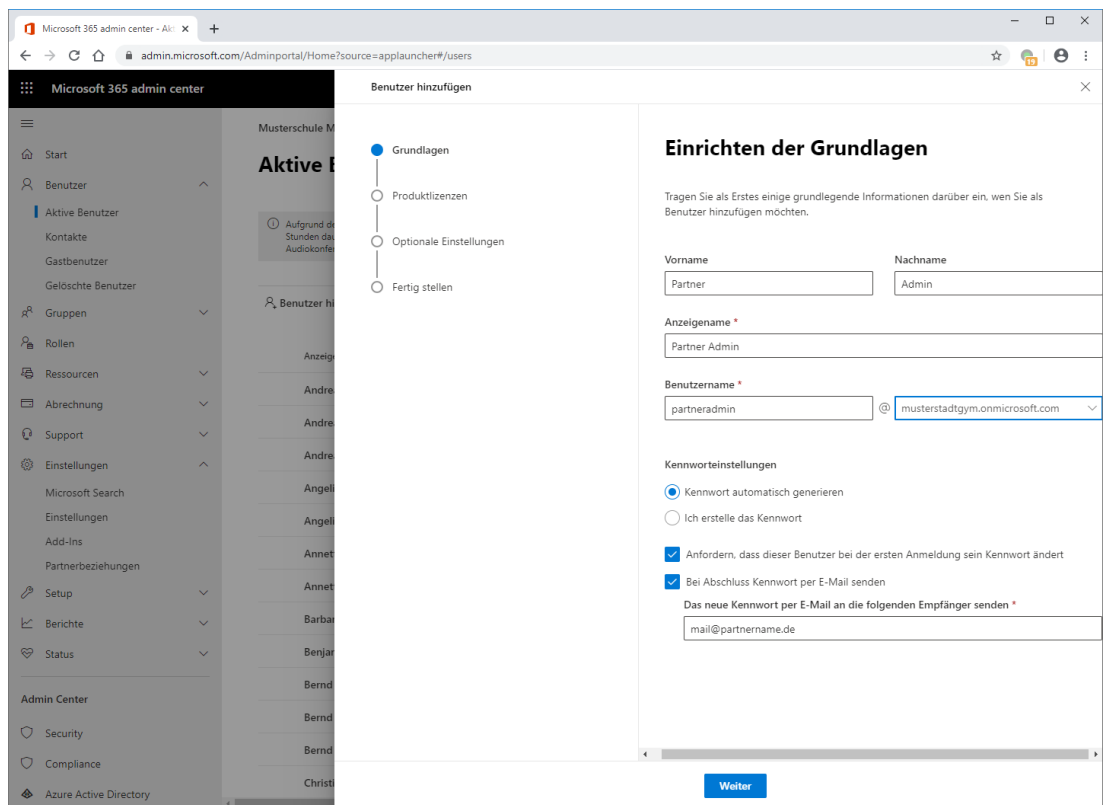


Tragen Sie die Daten für Ihren LogoDIDACT-Partner ein, der Ihren Tenant betreut. Lassen Sie für den Zugang automatisch ein Kennwort generieren und setzen Sie die beiden Häkchen bei **Anfordern, dass dieser Benutzer bei der ersten Anmeldung sein Kennwort ändert** und **Bei Abschluss Kennwort per E-Mail an die folgenden Empfänger senden**. Fahren Sie fort mit **Weiter**.

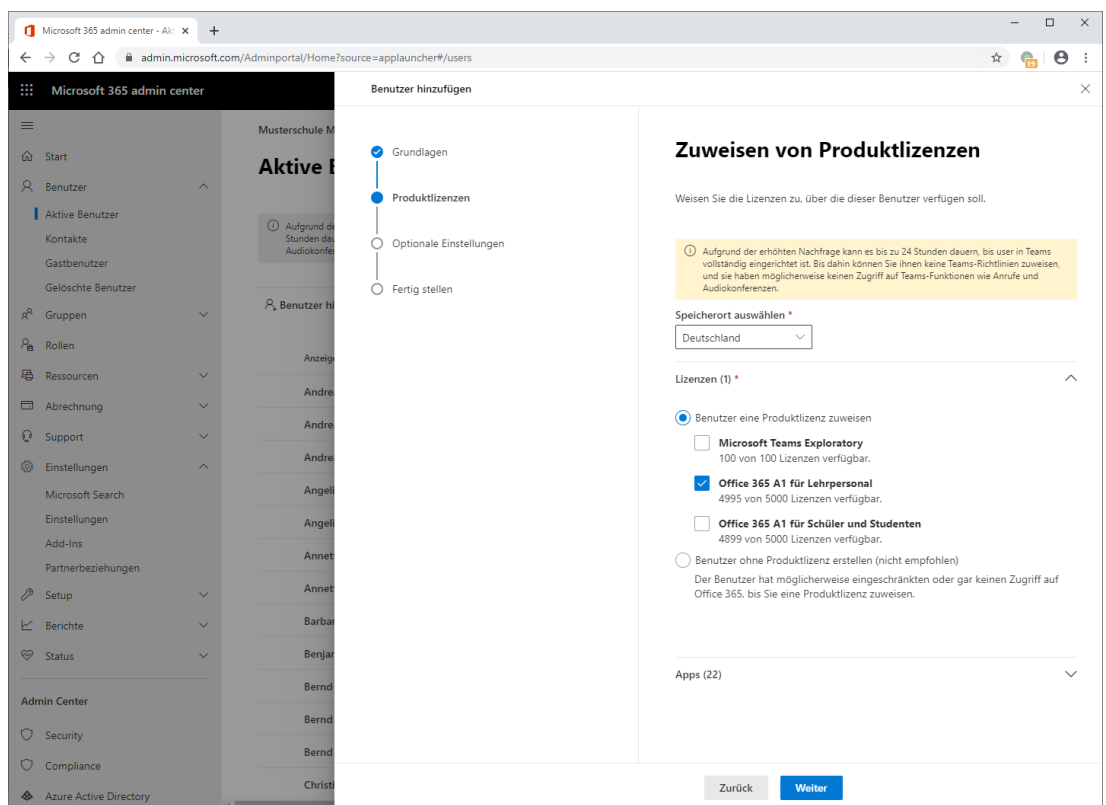


Achtung

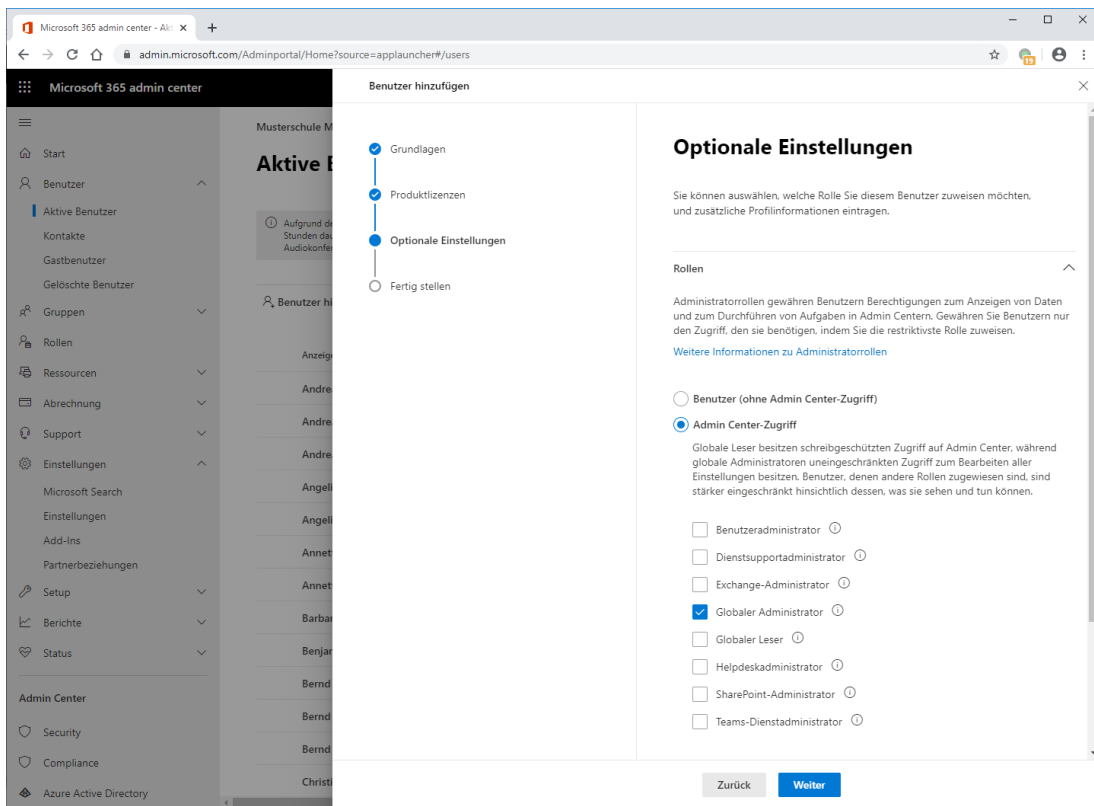
Stimmen Sie die zu verwendenden Daten für **Benutzernamen** und **E-Mail** mit Ihrem Partner ab.



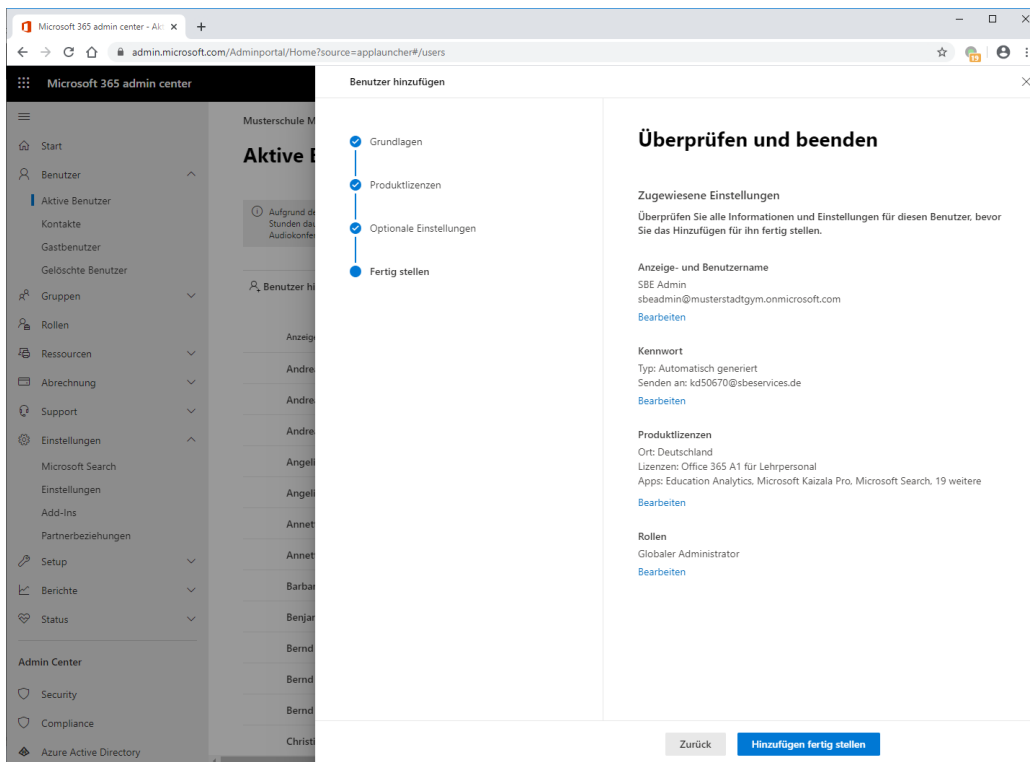
Wählen Sie den Eintrag **Benutzer eine Produktlizenz zuweisen** und setzen das Häkchen bei **Office 365 A1 für Lehrpersonal**. Fahren Sie fort mit **Weiter**.



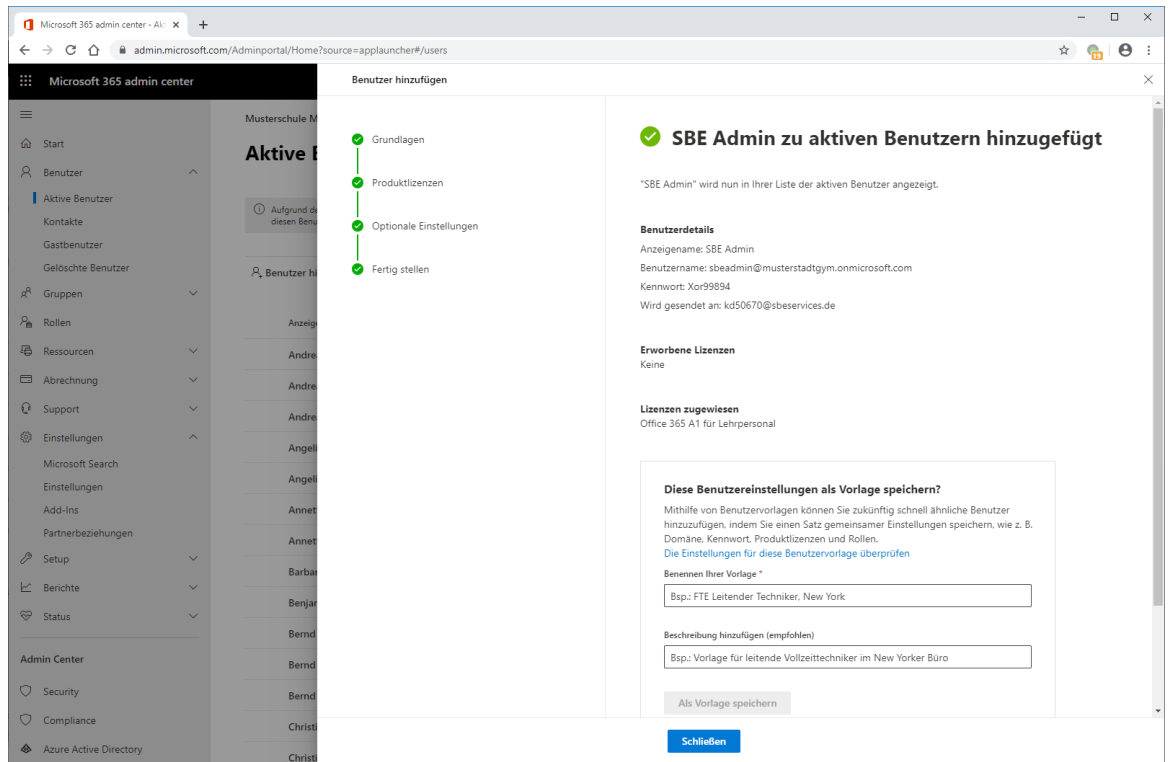
Erweitern Sie die Menüauswahl **Rollen** auf der rechten Seite und setzen den Eintrag **Admin Center-Zugriff** und das Häkchen bei **Globaler Administrator**. Fahren Sie fort mit **Weiter**.



Überprüfen Sie Ihre Eingaben und sofern alles richtig ist, bestätigen Sie mit **Hinzufügen fertig stellen**.



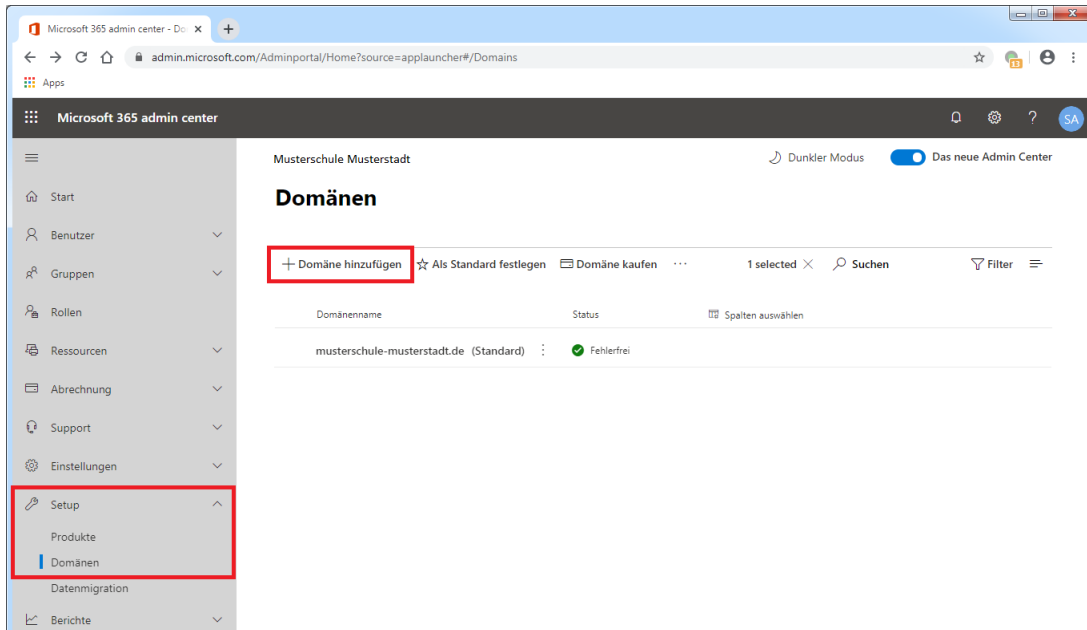
Wenige Augenblicke später ist das Konto angelegt und die Zugangsdaten an Ihren Partner versandt, der dann die Einrichtung zwischen Office 365 Tenant, Domain beim Provider und dem LogoDI-DACT-Server vervollständigen kann. Beenden Sie mit **Schließen**.



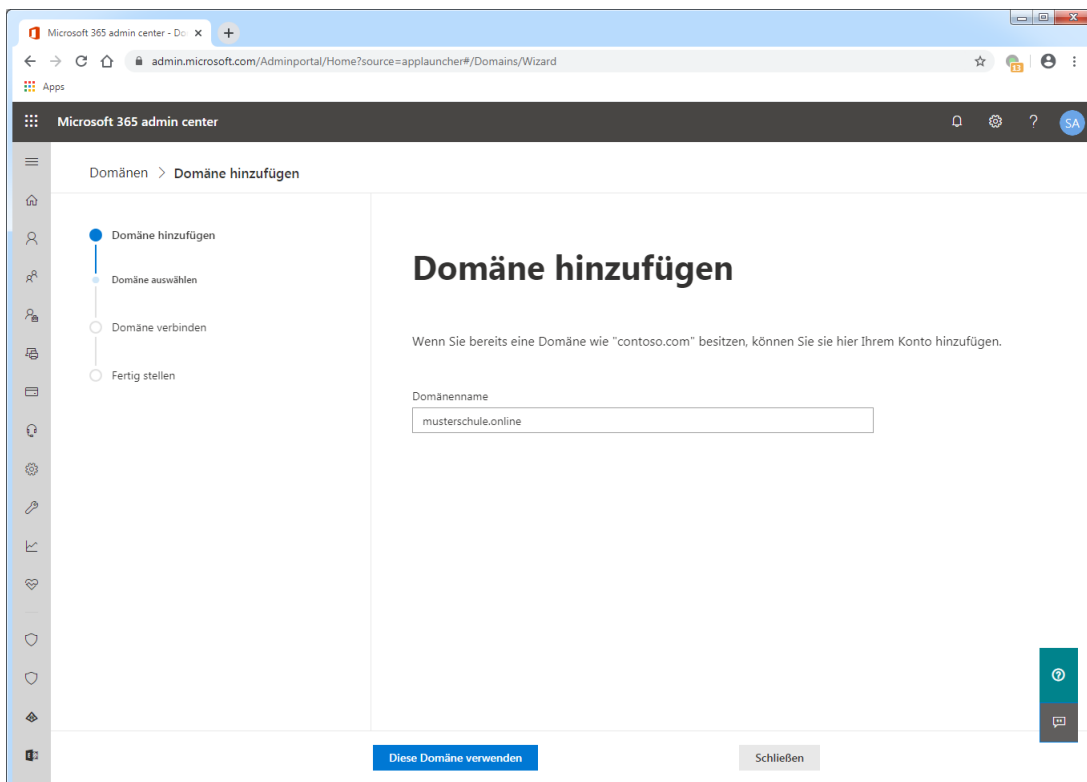
III.9.1.6. Den Tenant mit der Domäne verbinden

Das Vorgehen wird im weiteren Verlauf exemplarisch für die Musterschule Musterstadt beschrieben, für die beim Provider INWX eine neue Domäne `musterschule.online` angelegt wurde, die nun mit dem Tenant verbunden wird.

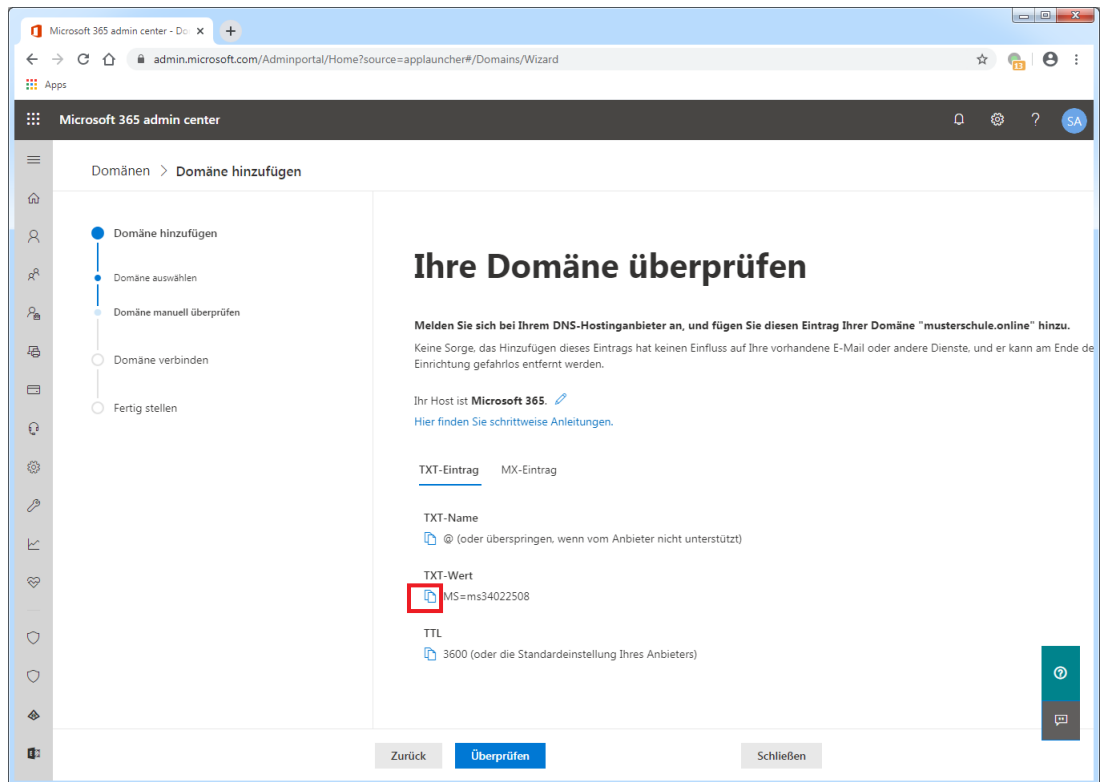
Erweitern Sie das Menü auf der linken Seite durch die Klick auf den Eintrag **... Alle anzeigen**. Wählen Sie dann aus dem linken Menübaum den Eintrag **Setup** und daraus **Domänen**. Dort sehen Sie nun Ihren Tenantnamen, so wie Sie diesen bei Microsoft beantragt haben. In unserem Fall der Name `musterschule-musterstadt.onmicrosoft.com`. Wählen Sie dort den Eintrag **+ Domäne hinzufügen**.



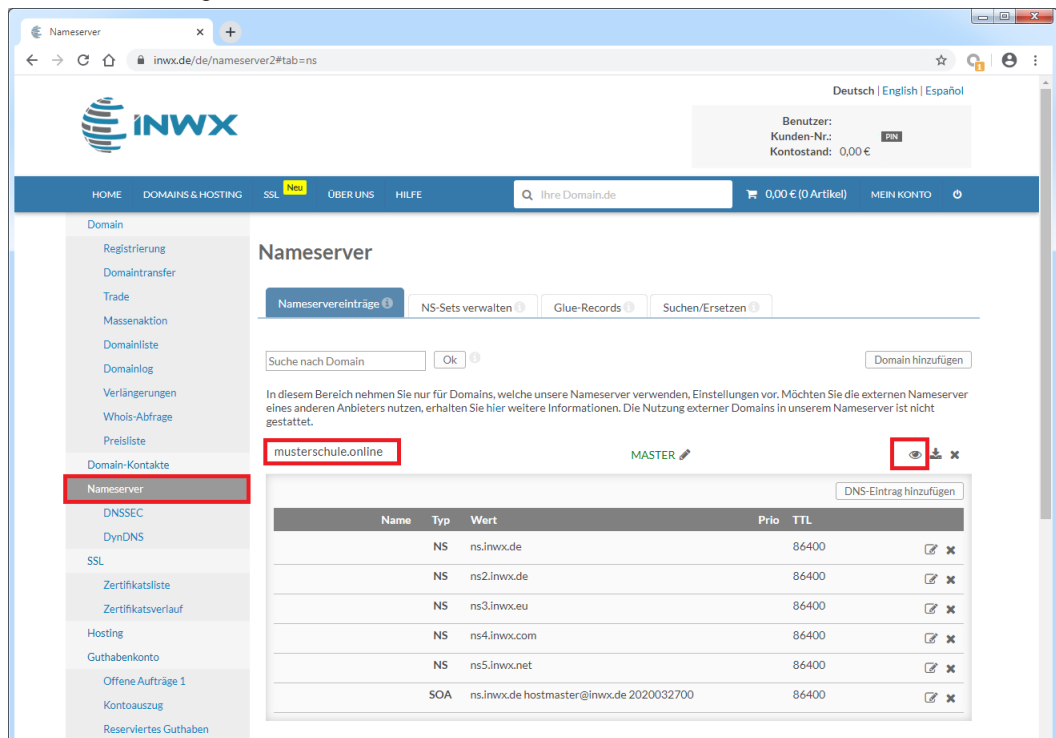
Geben Sie im folgenden Dialog den Namen der neu angelegten Domäne ein. Dieser lautet in unserem Fall `musterschule.online` und fahren Sie fort mit **Diese Domäne verwenden**.



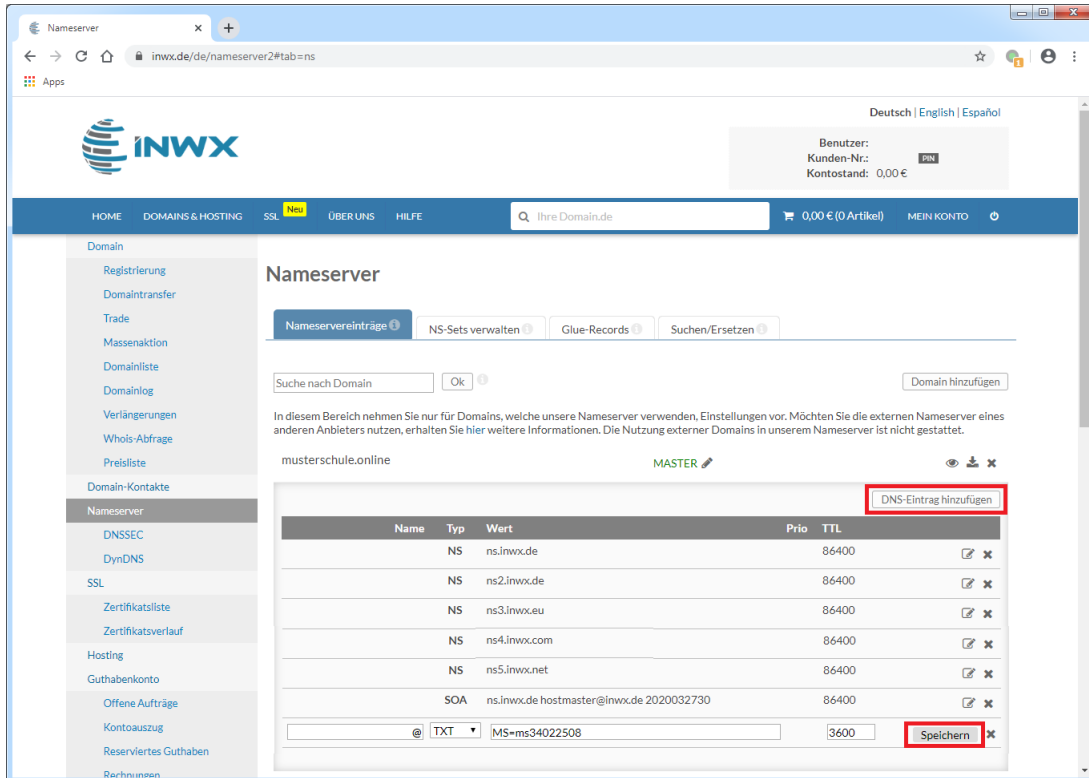
Damit Sie in der Microsoft-Cloud eine Domäne wie z.B. `musterschule.online` nutzen können, muss sichergestellt sein, dass Sie Besitzer dieser Domäne sind. Dies wird über einen entsprechenden TXT-Eintrag umgesetzt, der in Office erstellt wird und den Sie auf Ihrer Domäne in der DNS-Konfiguration eintragen müssen.



Wechseln Sie an dieser Stelle nun zur Konfiguration Ihrer Domäne, die in unserem Beispiel beim Provider INWX verwaltet wird. Die Konfiguration kann bei jedem Provider sehr unterschiedlich sein. Wenden Sie sich bei Fragen dazu bitte an Ihren Provider oder an Ihr kompetentes Systemhaus. Entfernen Sie im ersten Schritt auf keinen Fall die Nameservereinträge des Providers, damit die Domäne von Microsoft aufgelöst und verifiziert werden kann.

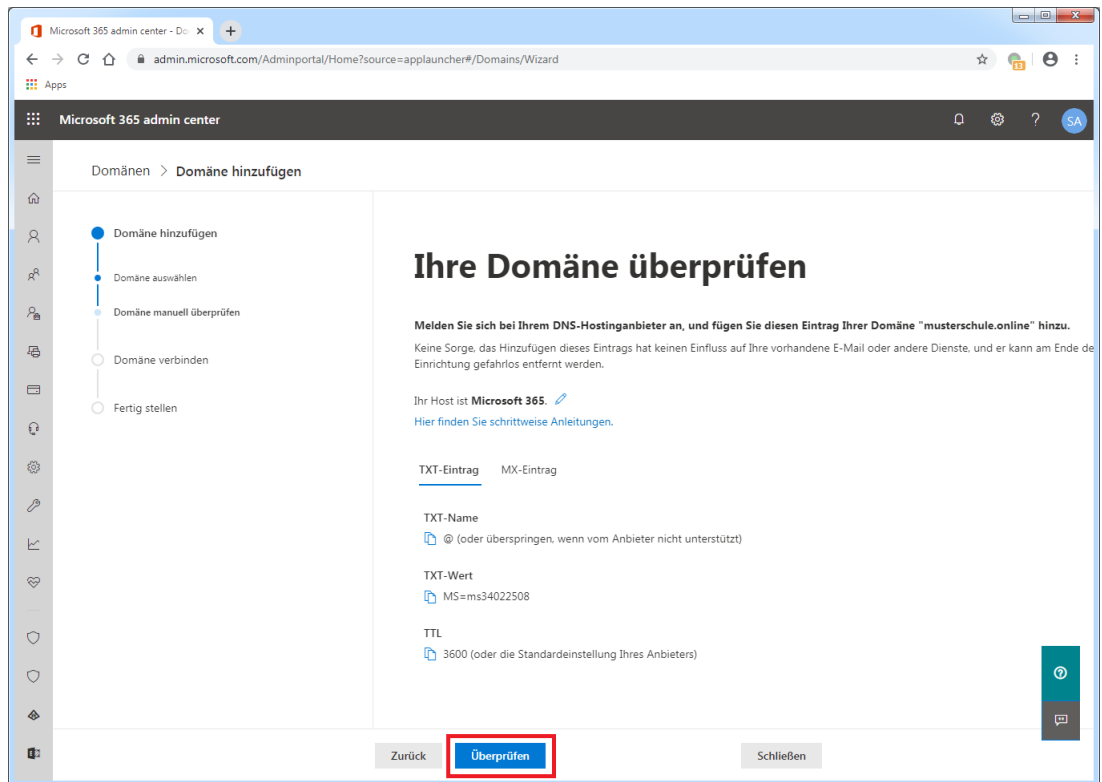


Erstellen Sie den dafür notwendigen TXT-Eintrag, indem Sie die Daten aus dem Office-Portal kopieren. Tragen Sie die Daten an den entsprechenden Stellen ein und übernehmen Sie mit **Speichern**.



Es kann bis zu 72 Stunden dauern, bis dieser Eintrag über das DNS-System verfügbar ist. Gerade deshalb ist es an dieser Stelle sehr von Vorteil, wenn Sie sowohl die Verwaltung Ihres Tenants als auch die Verwaltung der Domäne in professionelle Hände geben und beides am besten in eine Hand!

Im Fall von INWX sind die DNS-Einträge nach wenigen Minuten verfügbar, so dass die Prüfung im Office-Portal getestet werden kann.

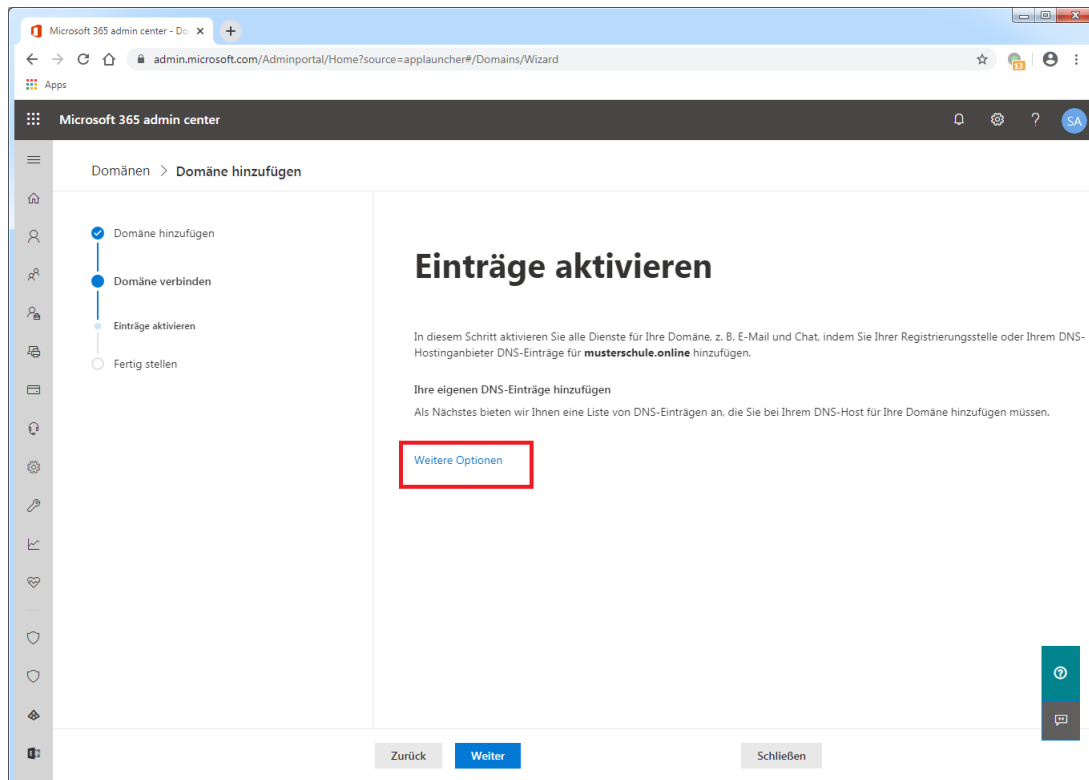


Bei erfolgreicher Prüfung gelangt man unmittelbar zum nächsten Dialog. In diesem wird erläutert, welche Möglichkeiten es bezüglich der DNS-Konfiguration gibt. Wählen Sie **Weiter**.

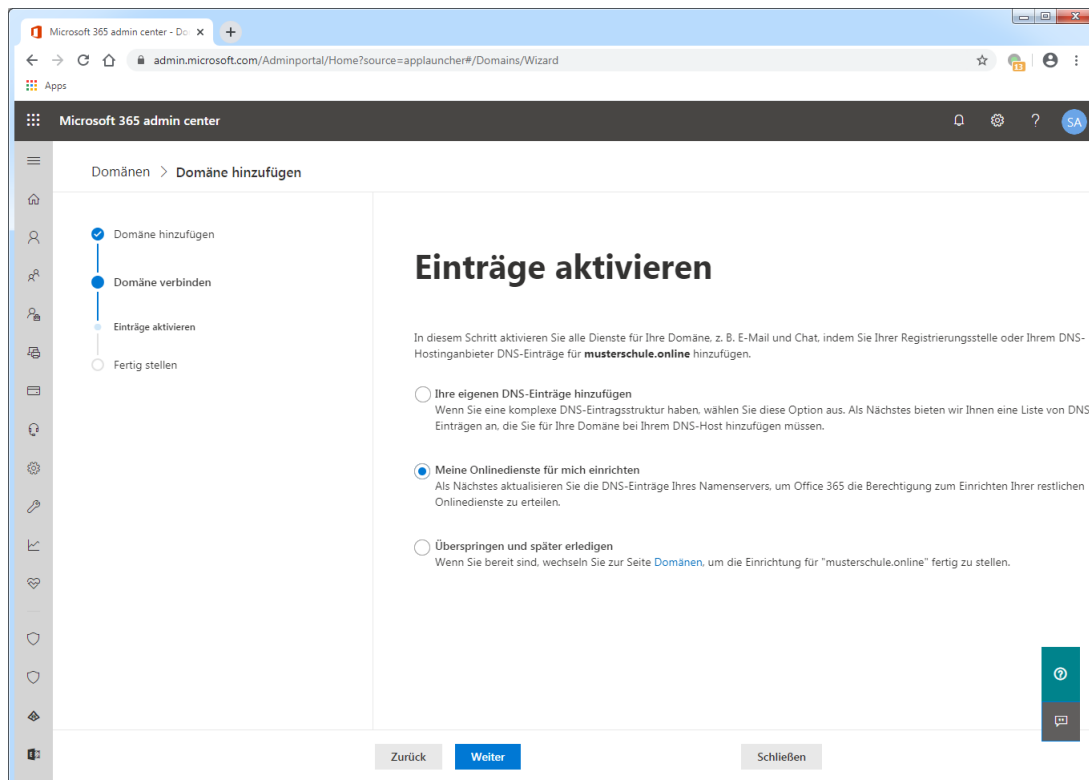
III.9.1.7. DNS-Konfiguration für weitere Dienste

Mit dem TXT-Eintrag beim Provider wird zunächst dafür gesorgt, dass die Anmeldung an Office 365 deutlich einfacher an Ihrer eigenen und kürzeren Domäne möglich ist.

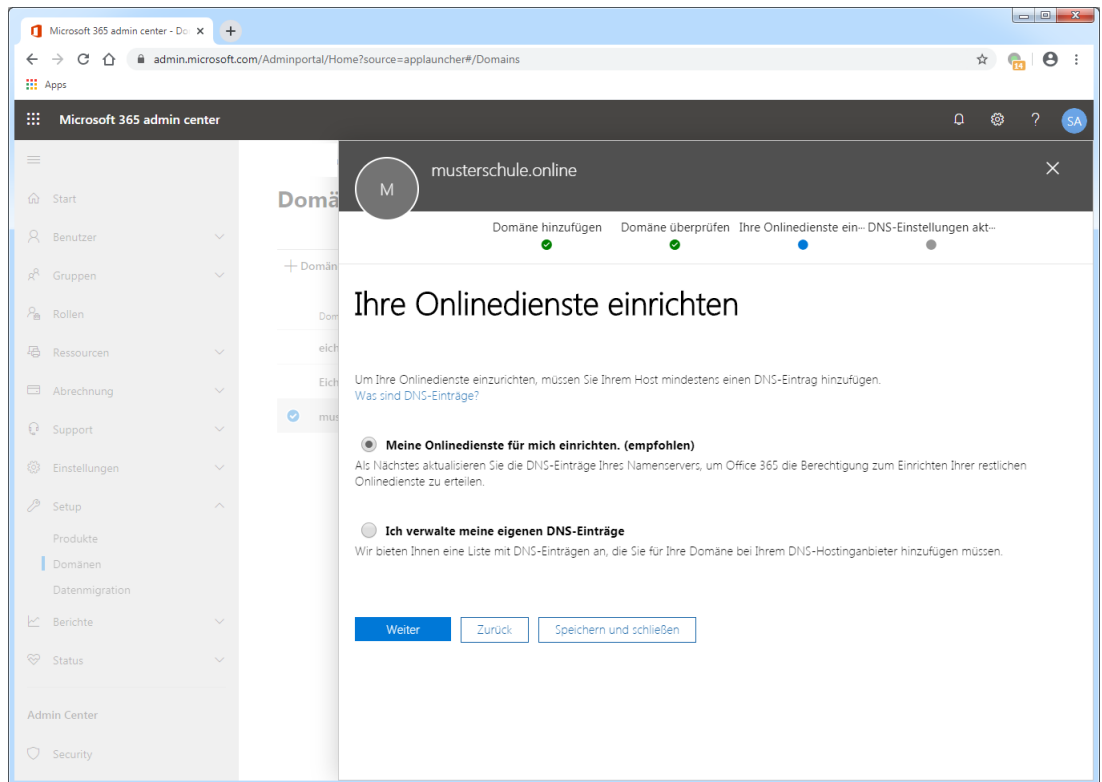
Klicken Sie auf **Weitere Optionen**.



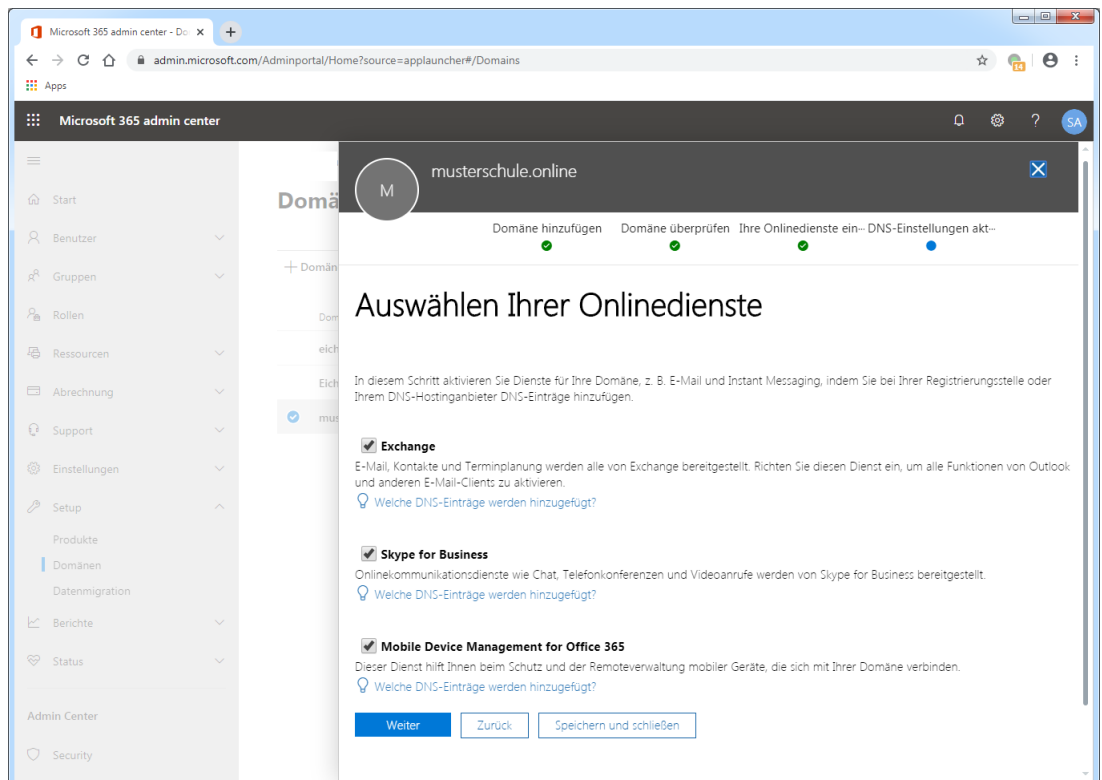
Wählen Sie im nächsten Schritt die Option **Meine Onlinedienste für mich eintragen** und fahren Sie fort mit **Weiter**.



Wählen Sie im folgenden Dialog ebenfalls **Weiter**.

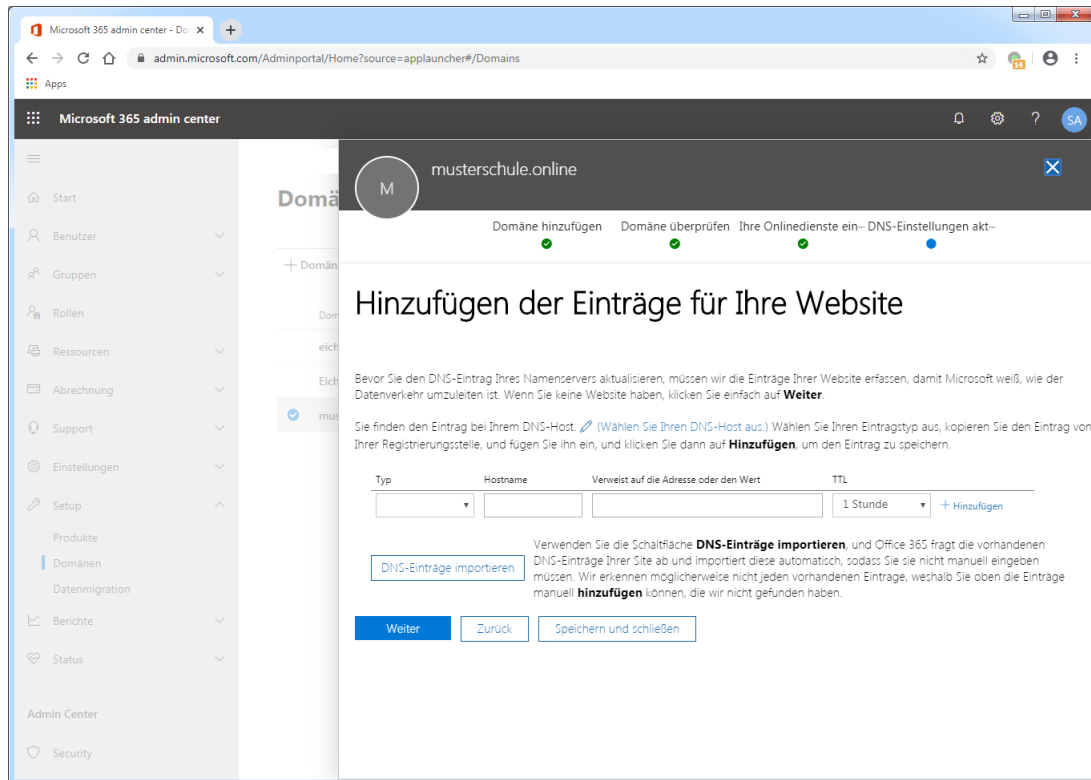


Im nächsten Schritt wählen Sie alle Dienste aus, für die Sie entsprechende DNS-Einträge erstellen wollen und klicken dann auf **Weiter**.

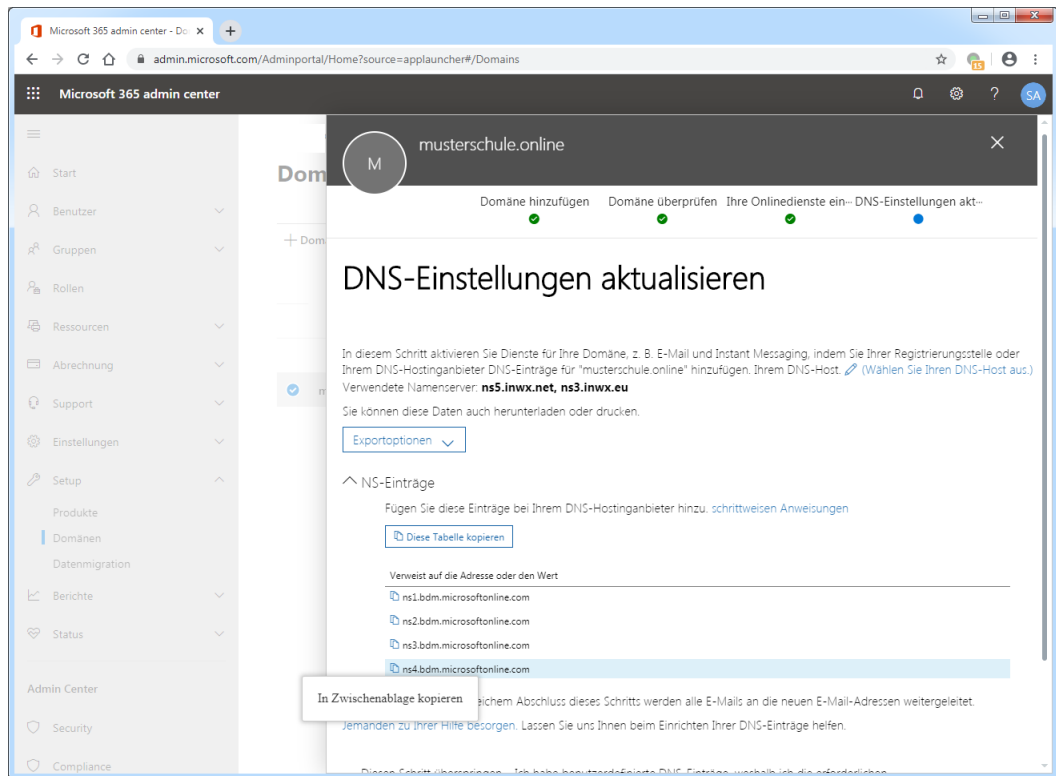


III.9.1.8. DNS-Server von Microsoft beim Provider eintragen

Der nächste Dialog weist darauf hin, dass für die diversen Microsoft-Dienste weitere DNS-Einträge vorzunehmen sind. In unserem Fall sollen alle notwendigen Einträge der Dienste auf den DNS-Servern von Microsoft erfolgen und nicht auf der Webseite des Domain-Providers. Überspringen Sie dies deshalb mit **Weiter**.

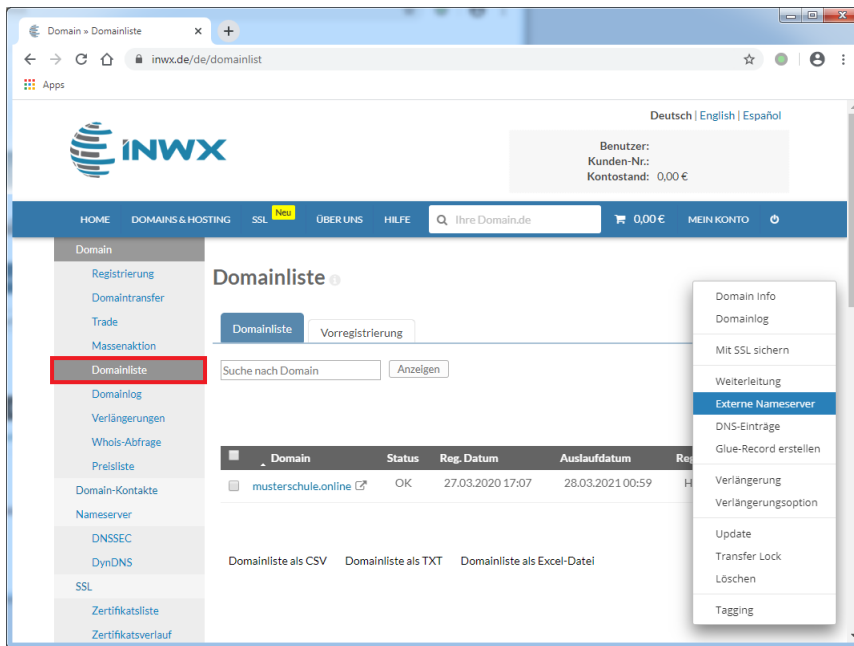


Im folgenden Abschnitt werden nun die Microsoft DNS-Server aufgeführt, die beim Provider einzutragen sind. Wie bereits beim TXT-Eintrag, lassen sich diese aus dem Office-Portal kopieren und dem Portal des Providers einfügen.

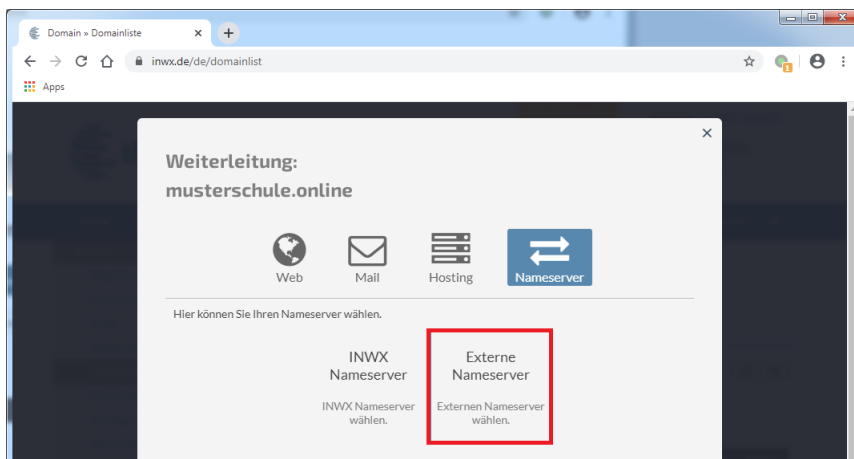


Auf Seiten des Providers (im Beispiel INWX) sollten nun die vorhandenen DNS-Einträge durch diejenigen DNS-Server von Microsoft ersetzt werden, denn alle Einträge über die verschiedenen Dienste wurden dort automatisch erstellt, so dass Dienste wie Microsoft Teams, Skype oder Exchange Online problemlos erreichbar sind.

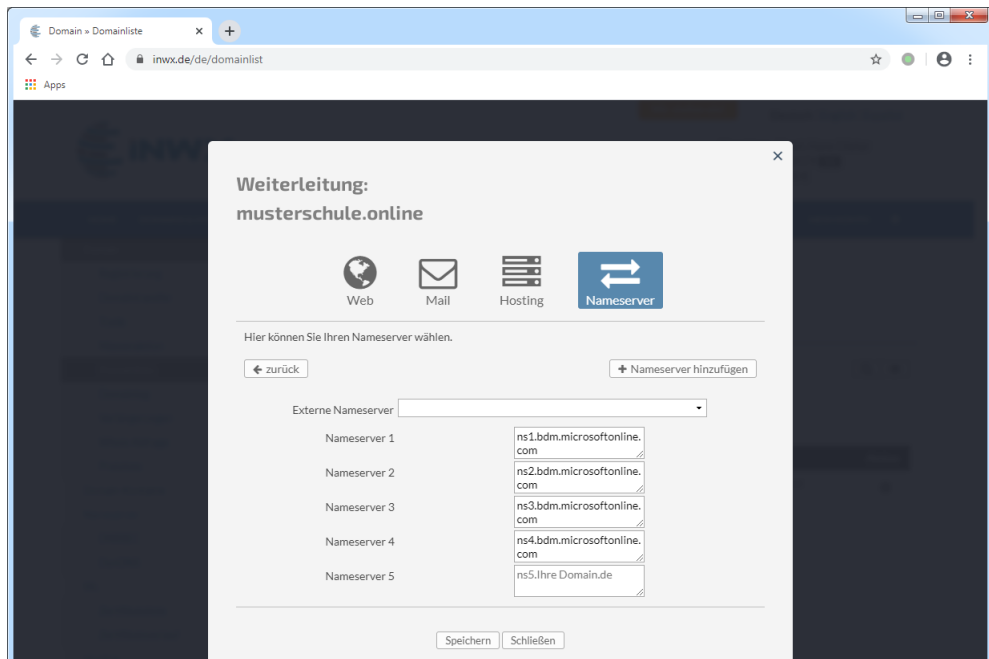
Die beste Methode ist dafür die Eintragung von externen Nameservern, die für die Domäne zuständig sind. Wählen Sie dazu aus dem Menü auf der linken Seite den Eintrag **Domainliste** und dann auf der rechten Seite das Konfigurationssymbol. Klicken Sie aus dem Kontextmenü auf den Eintrag **Externe Nameserver**.



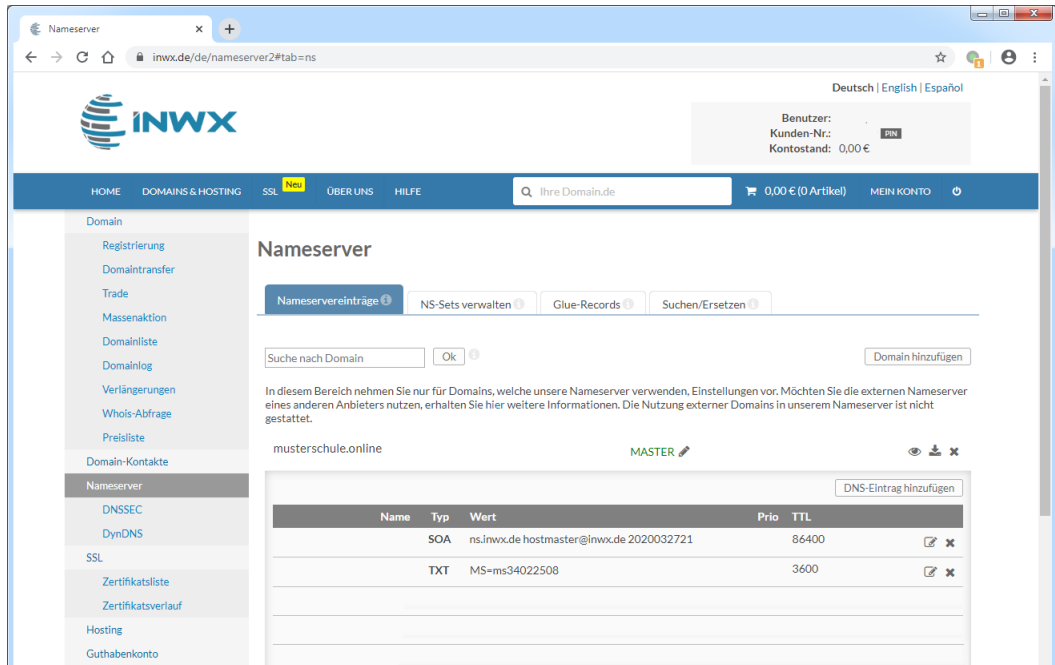
Wählen Sie dann **Externe Nameserver**.



Tragen Sie im letzten Schritt die Microsoft-Nameserver ein, die Ihnen im Tenant angezeigt werden und übernehmen Sie die Anpassung durch **Speichern**.



Wie die individuelle DNS-Konfiguration aussieht, spielt damit keine Rolle mehr, weil sämtliche Anfragen durch die obige Eintragung der externen DNS-Server auf einer Ebene höher abgefangen bzw. weitergeleitet werden. Auch der Eintrag **SOA**, der den Provider INWX als Startpunkt der Zuständigkeit (Start of Authority) ausweist, spielt keine Rolle.



Achtung

Bis diese Einträge global auf allen DNS-Servern verteilt sind, kann es bis zu 72 Stunden dauern.

Eine Abfrage **nslookup -type=SOA musterschule.online** liefert zunächst sicherlich noch eine ganze Zeit lang **ns.inwx.de** zurück.

```
Administrator: C:\Windows\system32\cmd.exe
C:\>nslookup -type=SOA musterschule.online
Server: Unknown
Address: 10.1.0.20

Nicht autorisierende Antwort:
musterschule.online
primary name server = ns.inwx.de
responsible mail addr = hostmaster.inwx.de
serial = 202903912
refresh = 10800 (3 hours)
retry = 3600 (1 hour)
expire = 604800 (7 days)
default TTL = 3600 (1 hour)

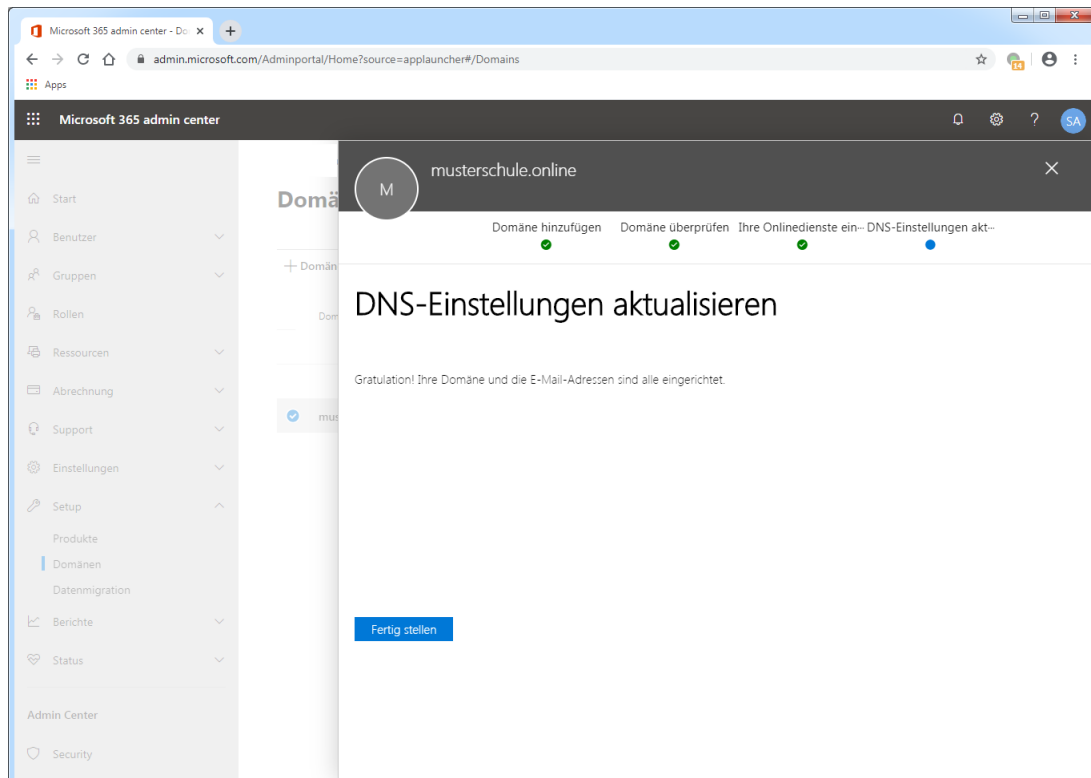
ns.inwx.de internet address = 192.174.68.104
ns.inwx.de AAAA IPv6 address = 2001:67c:1bc::104
C:\>_
```

Die gleich Abfrage an die Google-DNS-Infrastruktur **nslookup -type=SOA musterschule.online 8.8.8.8**, liefert aber bereits nach wenigen Minuten das gewünschte Ergebnis **ns1.bdm.microsoftonline.com**.

```
Administrator: C:\Windows\system32\cmd.exe
C:\>nslookup -type=SOA musterschule.online 8.8.8.8
Server: dns.google
Address: 8.8.8.8

Nicht autorisierende Antwort:
musterschule.online
primary name server = ns1.bdm.microsoftonline.com
responsible mail addr = azuredns-hostmaster.microsoft.com
serial = 1
refresh = 3600 (1 hour)
retry = 300 (5 mins)
expire = 2449200 (28 days)
default TTL = 300 (5 mins)
C:\>_
```

Die DNS-Konfiguration auf Seiten des Providers ist damit abgeschlossen. Auch auf Seite von Office 365 ist nichts mehr weiter zu unternehmen. Klicken Sie auf **Fertig stellen**.



Die notwendigen DNS-Einträge für die verschiedenen Microsoft-Dienste sieht man, wenn man im Office 365 Portal direkt auf den Namen einer fertig eingerichteten Domäne klickt.

The screenshot shows the Microsoft 365 Admin Center interface for the domain 'musterschule.online'. The left sidebar contains navigation options like 'Start', 'Benutzer', 'Gruppen', 'Rollen', 'Ressourcen', 'Abrechnung', 'Support', 'Einstellungen', 'Setup', 'Produkte', 'Domänen', 'Datenmigration', 'Berichte', 'Status', 'Admin Center', 'Security', 'Compliance', 'Azure Active Directory', 'Exchange', 'SharePoint', and 'Teams'. The main content area displays the domain name and a 'Als Standard festlegen' button. Below this, there are sections for 'DNS-Einstellungen', 'Benutzerdefinierte Einträge', 'Exchange Online', 'Skype for Business', and 'Mobile Device Management for Office 365', each containing a table of DNS records.

DNS-Einstellungen

Benutzerdefinierte Einträge

Exchange Online

Typ	Priorität	Hostname	Verweist auf die Adresse oder den Wert	TTL	Aktionen
MX	0	@	musterschule-online.mail.protection.outlook.com	1 Stunde	
TXT	-	@	v=spf1 include:spf.protection.outlook.com -all	1 Stunde	
CNAME	-	autodiscover	autodiscover.outlook.com	1 Stunde	

Skype for Business

Typ	Hostname	Verweist auf die Adresse oder den Wert	TTL	Aktionen
CNAME	lyncdiscover	webdir.online.lync.com	1 Stunde	
CNAME	sip	sipdir.online.lync.com	1 Stunde	

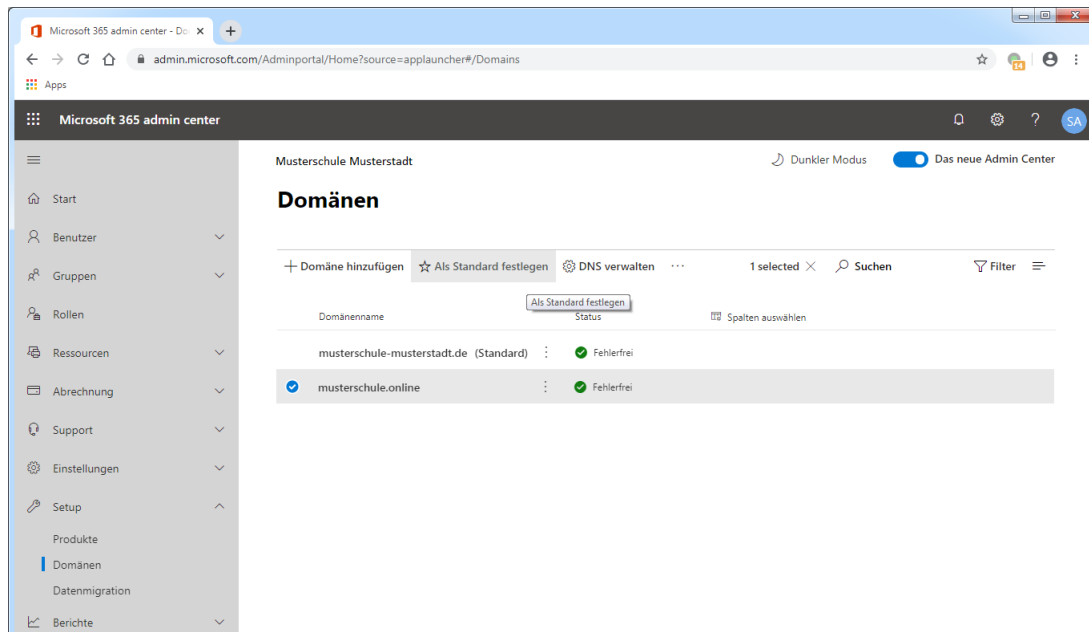
Typ	Dienst	Protokoll	Port	Gewichtung	Priorität	TTL	Name	Ziel	Aktionen
SRV	_sipfederationtls	_tcp	5061	1	100	1 Stunde	@	sipfed.online.lync.com	
SRV	_sip	_tls	443	1	100	1 Stunde	@	sipdir.online.lync.com	

Mobile Device Management for Office 365

Typ	Hostname	Verweist auf die Adresse oder den Wert	TTL	Aktionen
CNAME	enterpriseenrollment	enterpriseenrollment.manage.microsoft.com	1 Stunde	
CNAME	enterpriseregistration	enterpriseregistration.windows.net	1 Stunde	

III.9.1.9. Domäne als Standard festlegen

Eine neu angelegte Domäne wird normalerweise automatisch zum Standard, so dass Sie nichts anpassen müssen. Sollte das nicht der Fall sein, markieren Sie diese und wählen aus dem Auswahlmü den Eintrag **Als Standard festlegen**. Damit werden Objekte und Strukturen immer auf diese Domäne angelegt.



III.9.2. Der LogoDIDACT Connector für Azure-AD

Der neue LogoDIDACT Connector für Azure-AD kurz **LD Azure Connect** besteht im Wesentlichen aus zwei Teilen. Der lokale Teil auf dem Server an der Schule vor Ort befindet sich dabei wie üblich in einem eigenen Container. Der zweite Teil bildet eine entsprechenden APP in Azure-AD.

III.9.2.1. Entwicklerpakete für Azure-AD einspielen

Bevor Sie die Entwicklerpakete für Azure-AD einspielen, aktualisieren Sie den Server auf den aktuellen Puppet-Rezeptstand. Wechseln Sie dazu in den Container **puppeteer** und führen Sie ein **ldupdate** durch. Aktualisieren Sie die Container gezielt über **prun** und starten Sie den physischen Server gegebenenfalls neu, wenn dies im lhost angezeigt wird.



Achtung

Zur fachgerechten Installation von Entwicklerpaketen wenden Sie sich bitte an Ihren zertifizierten LogoDIDACT-Partner, der Ihren Server per Monitoring überwacht und administriert.

III.9.2.2. Den Connector für Azure-AD installieren

III.9.2.2.1. Voraussetzungen

Der neue Connector setzt zwingend voraus, dass sowohl Samba4, als auch die Postgres-Datenbank und der Controller aktiviert sind. Es muss aber keine komplette **lddeploy**-Umgebung vorhanden sein.



Achtung

Für den Azure-AD müssen folgende Container bereits laufen oder noch aktiviert werden:

```
[Guest samba4-ad]
Ensure running
```

```
[Guest postgresql10]
Ensure running
```

```
[Guest ctrl-g1]
Ensure running
```

Nicht notwendig sind die Container **deploy-g1**, **nexus-g1** und **graylog-g1**!

Bitte prüfen Sie im Zusammenhang mit der Aktivierung des neuen Connectors für Azure-AD, dass die oben aufgeführten Container aktiviert sind und aktivieren Sie diese gegebenenfalls.

Eine zweite grundlegende Voraussetzung betrifft die Kennwortsynchronisation.



Achtung

Die Kennwörter dürfen im bestehenden **logosrv** nicht verschlüsselt vorliegen!

Diese müssen über einen neuen Synchronisations-Mechanismus in die neue Benutzerdatenbank zum Container **postgresql10** übertragen und dort verschlüsselt abgelegt werden können.

Prüfen Sie dies im **logosrv** über folgenden Befehl, wobei die Ausgabe selbsterklärend ist:

```
less /etc/logodidact/service.conf | grep PasswordHash
```

Eine dritte Voraussetzung betrifft das Thema Kennwortkomplexität. Von Office 365 werden verschiedene Kriterien vorgegeben, die nicht veränderbar sind. Damit die Benutzer auch von zu Hause aus ihr Kennwort abändern können, wird über den Container **ssp-g1** ein Kennwortportal zur Verfügung gestellt, das zusammen mit dem Connector aktiviert werden muss.

III.9.2.2.2. Aktivierung der Container **ad-sync-g1** und **ssp-g1**

Die Container für den Connector **ad-sync-g1** und das Kennwortportal **ssp-g1** werden nach dem gleichen Schema aufgebaut, wie bereits in den Grundlagen zu Puppet ausführlich beschrieben. Bitte beachten Sie unbedingt die Hinweise und Erklärungen dort, um zu verstehen, wie ein Container durch Puppet automatisch aufgebaut wird und was Sie dabei machen können und was Sie dabei auf keinen Fall tun dürfen.

Wechseln Sie in den Puppeteer:

```
lxc-ssh -n puppeteer
```

Wechseln Sie in das Verzeichnis zur Konfiguration von Containern:

```
cd /etc/logodidact/hosts/ldhost
```

Öffnen Sie die Datei **guest.conf** mit einem Editor Ihrer Wahl, wie z.B. Nano:

nano guest.conf

Fügen Sie dort den Eintrag für den Container **ad-sync-g1** und **ssp-g1** hinzu.

```
[Guest ad-sync-g1]
Ensure running
```

```
[Guest ssp-g1]
Ensure running
```

Durch Eingabe der Tastenkombination <Strg>+<X> verlassen Sie den Editor Nano und geben „Y“ ein, damit die Änderung gespeichert wird. Wechseln Sie dann ins Stammverzeichnis der Konfiguration und übertragen Sie anschließend die Änderungen ins Versionierungssystem git:

cd /etc/logodidact

```
git add .
```

```
git commit -m "Aktivierung Azure-AD Connector und Kennwortportal"
```

Durch das Übertragen ins git-Repository wird auch automatisch map_translate aufgerufen, so dass die Konfigurationen in YAML übersetzt und von Puppet verarbeitet werden können.

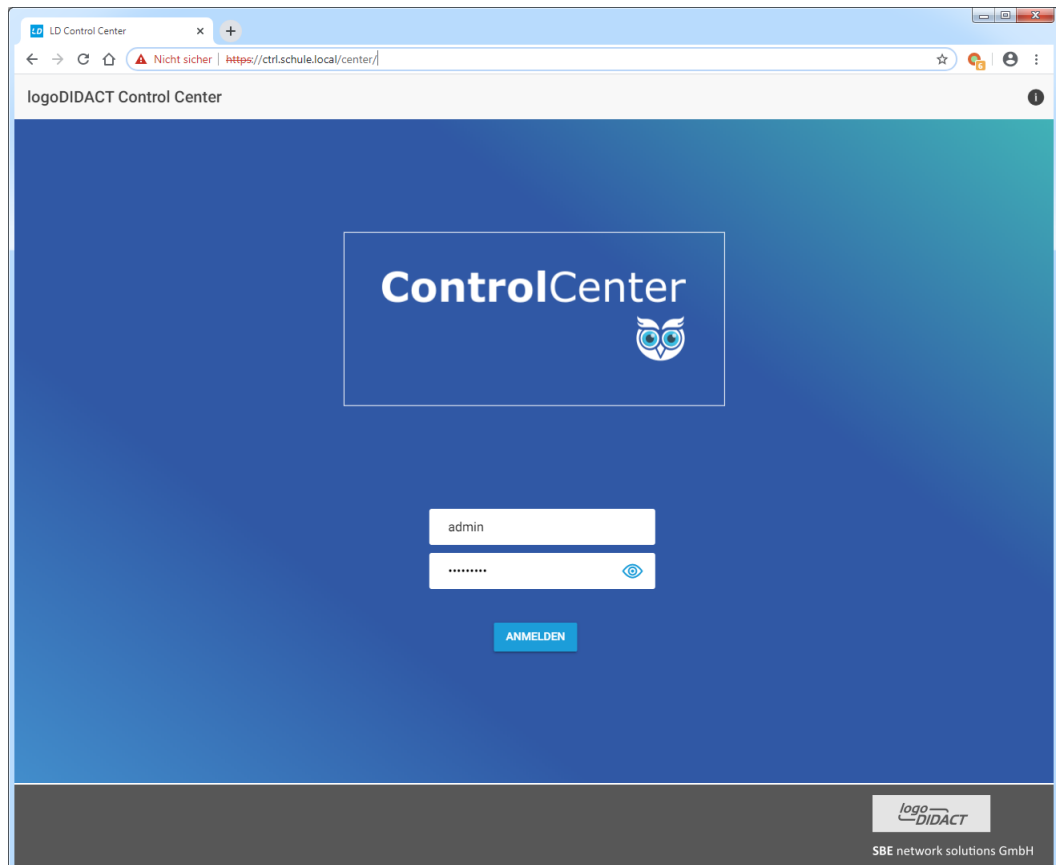
Wie in den Grundlagen beschrieben, führen Sie den Aufbau gezielt und kontrolliert durch.

Mit einem **prun** im Host veranlassen Sie den Agenten sich beim Puppetter zu melden. Dieser baut die Catalog-Datei für den Idhost und schickt sie ihm. Der Idhost beginnt dann mit dem Aufbau der Container **ad-sync-g1** und **ssp-g1**. Beobachten können Sie das Ganze mit pstat im Puppetter. Nach einer Weile werden die Container auftauchen. Sofern ein Container grundlegend aufgebaut ist und läuft, kann man in einer neuen Sitzung per **lxc-ssh -n ad-sync-g1** dort hineinwechseln und sofern gerade kein prun läuft einen solchen neuen Durchlauf mit **prun** starten.

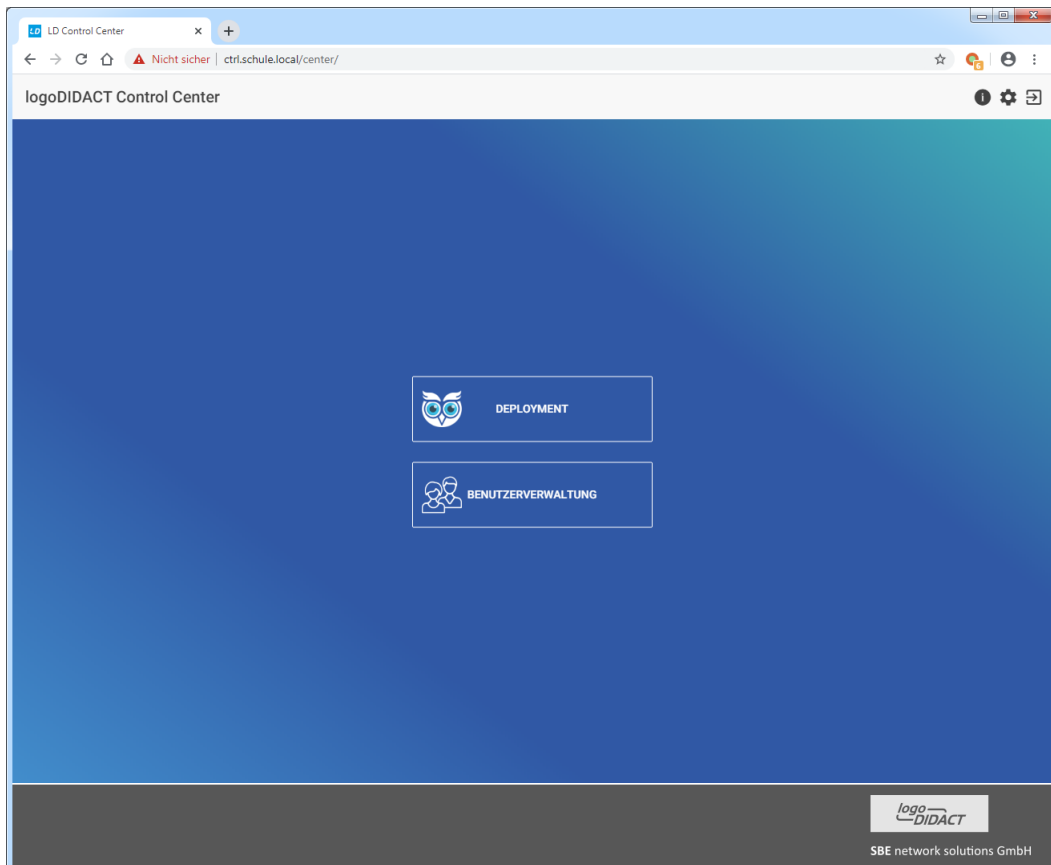
III.9.2.3. Den Connector für Azure-AD konfigurieren

Die Konfiguration des Connectors für Azure-AD ist denkbar einfach. Melden Sie sich per Web-Browser im Control Center mit den Zugangsdaten des Benutzers **admin** an.

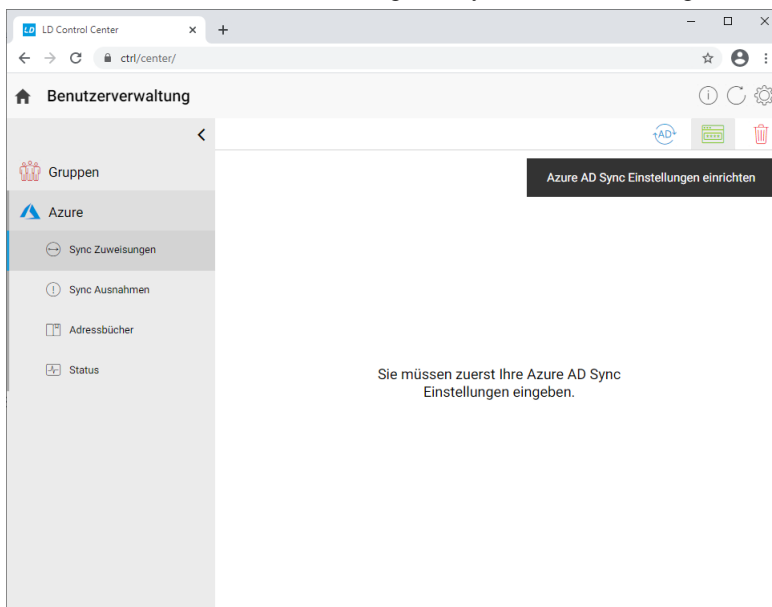
Verbinden Sie sich über das Control Center mittels `https://ctrl.schule.local/center` bzw. über die schnelle Variante `ctrl/`



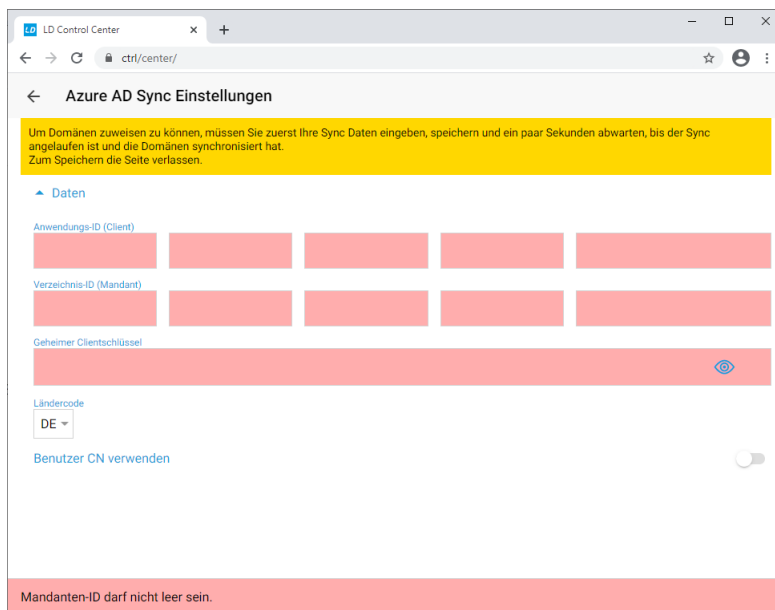
Wählen Sie den neuen Bereich **BENUTZERVERWALTUNG** aus.



Wählen Sie im linken Menü der Benutzerverwaltung den Eintrag **Azure**. Wenn der Connector noch nicht eingerichtet wurde, wird dies im rechten Fensterbereich angezeigt. Zur Einrichtung klicken Sie im oberen rechten Menübereich das grüne Symbol für die Konfiguration von **LD Azure Connect**.



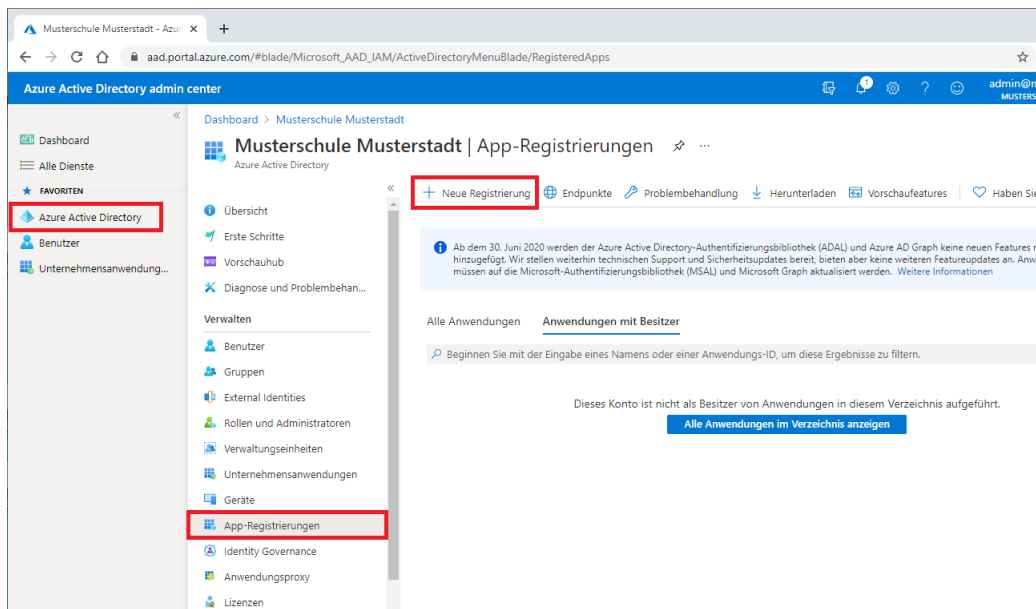
Es öffnet sich ein Dialog, in den die Daten aus Office 365 bzw. Azure-AD eingetragen werden müssen.



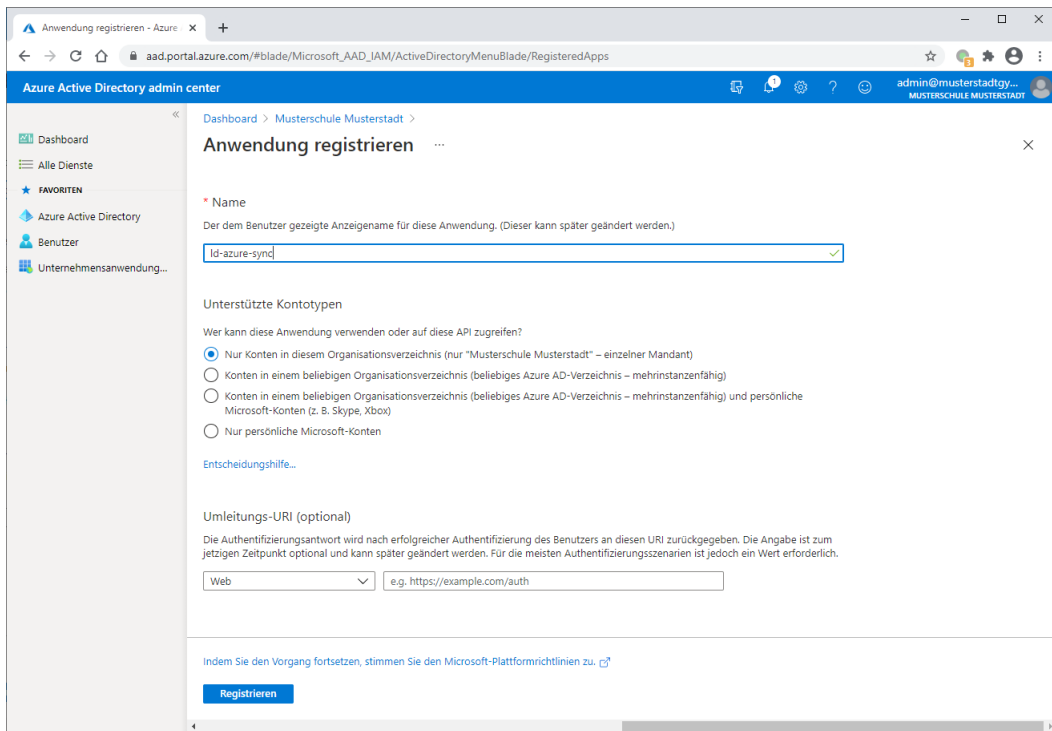
Um an diese Daten zu gelange, muss nun zunächst in Azure-AD eine APP registriert werden.

III.9.2.4. Eine APP in Azure-AD registrieren

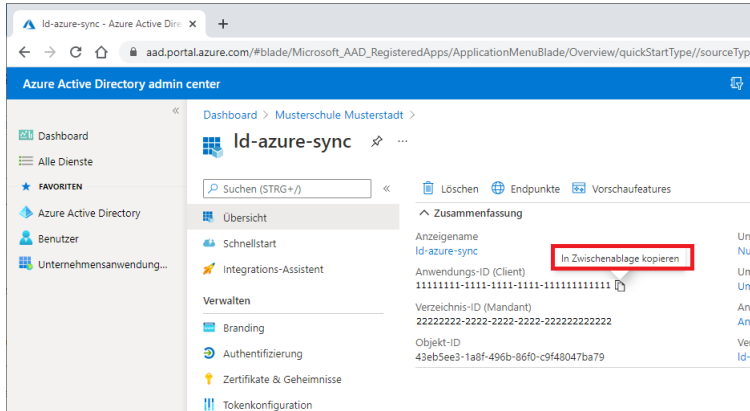
Melden Sie sich im Azure Active Directory admin center `add.portal.azure.com` mit dem administrativen Konto für Ihren Tenant an. Wählen Sie aus der linken Verzeichnisstruktur **Azure Active Directory** und aus dem mittleren Menü den Eintrag **APP-Registrierungen**. Aus der Menüleiste oben starten Sie die Registrierung über **+ Neue Registrierung**.



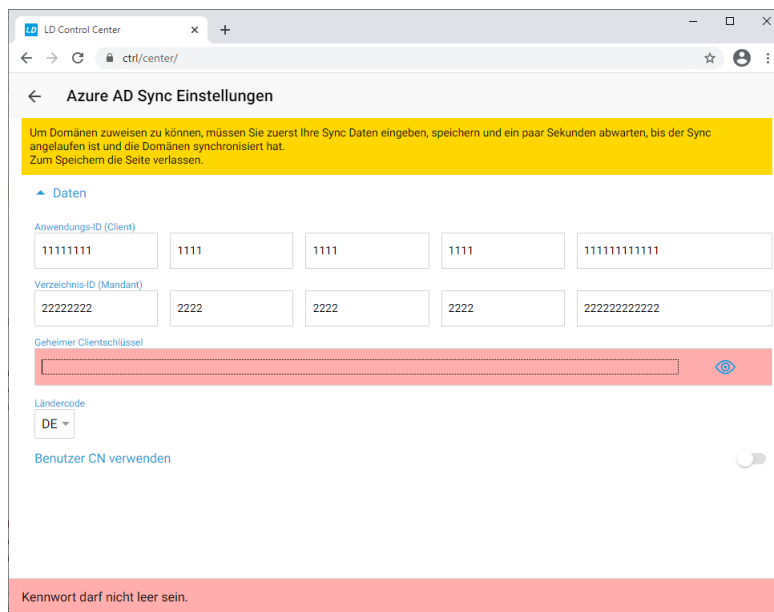
Registrieren Sie die Anwendung unter dem Namen **ld-azure-sync** und klicken Sie auf **Registrieren**.



Kopieren Sie aus der folgenden Seite zunächst die **Anwendungs - ID** in die Zwischenablage und fügen Sie diese im Control Center ein und wiederholen Sie den Vorgang für die **Verzeichnis - ID** des Mandanten.

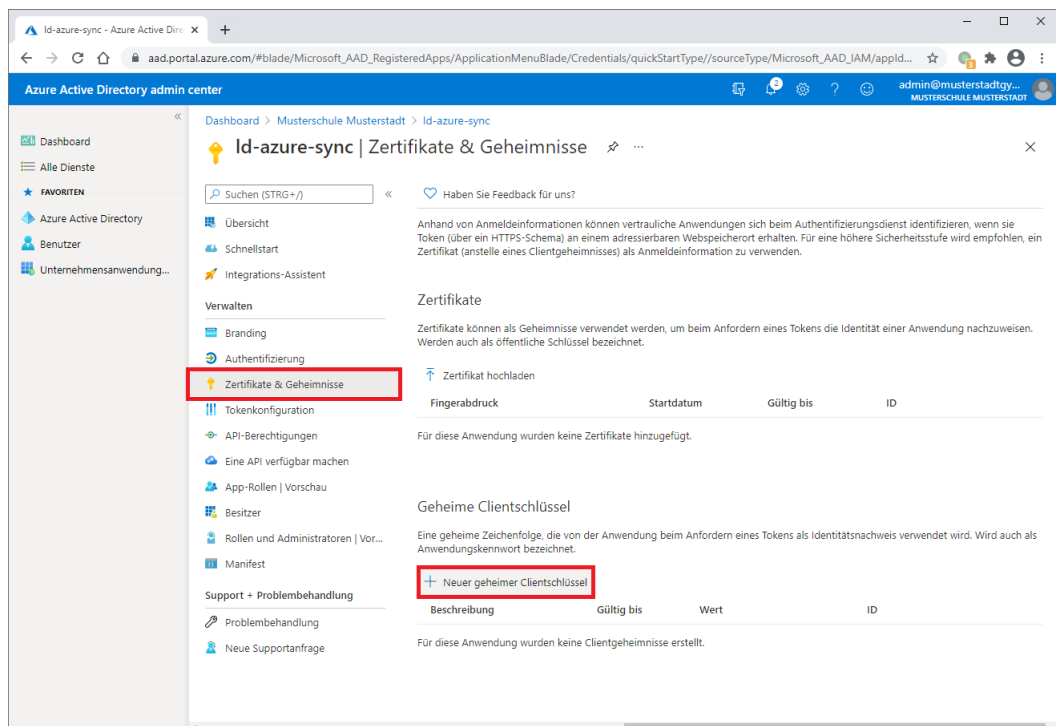


Im Control Center sieht die Konfiguration dann wie folgt aus.



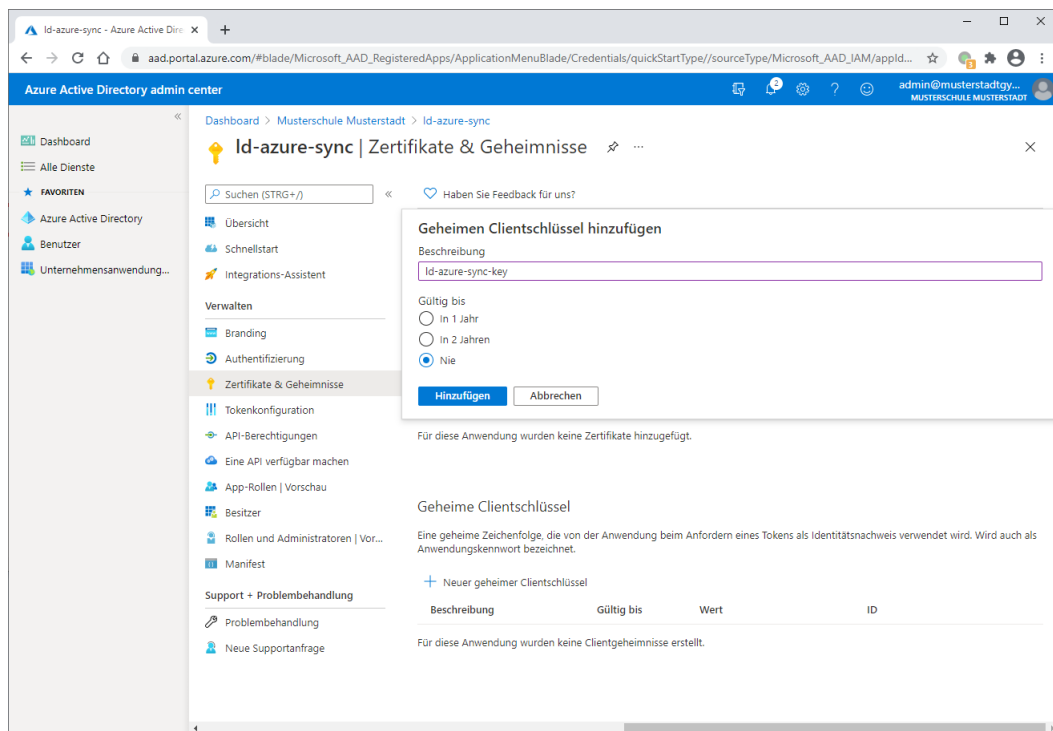
III.9.2.5. Einen geheimen Clientschlüssel in Azure-AD anlegen

Für die Synchronisation zwischen dem Connecotr für Azure-AD und der Microsoft-Cloud ist ein geheimer Clientschlüssel notwendig. Wählen Sie aus dem mittleren Menü den Eintrag **Zertifikate und Geheimnisse** und auf der rechten Seite im unteren Bereich den Eintrag **+ Neuer geheimer Clientschlüssel**.

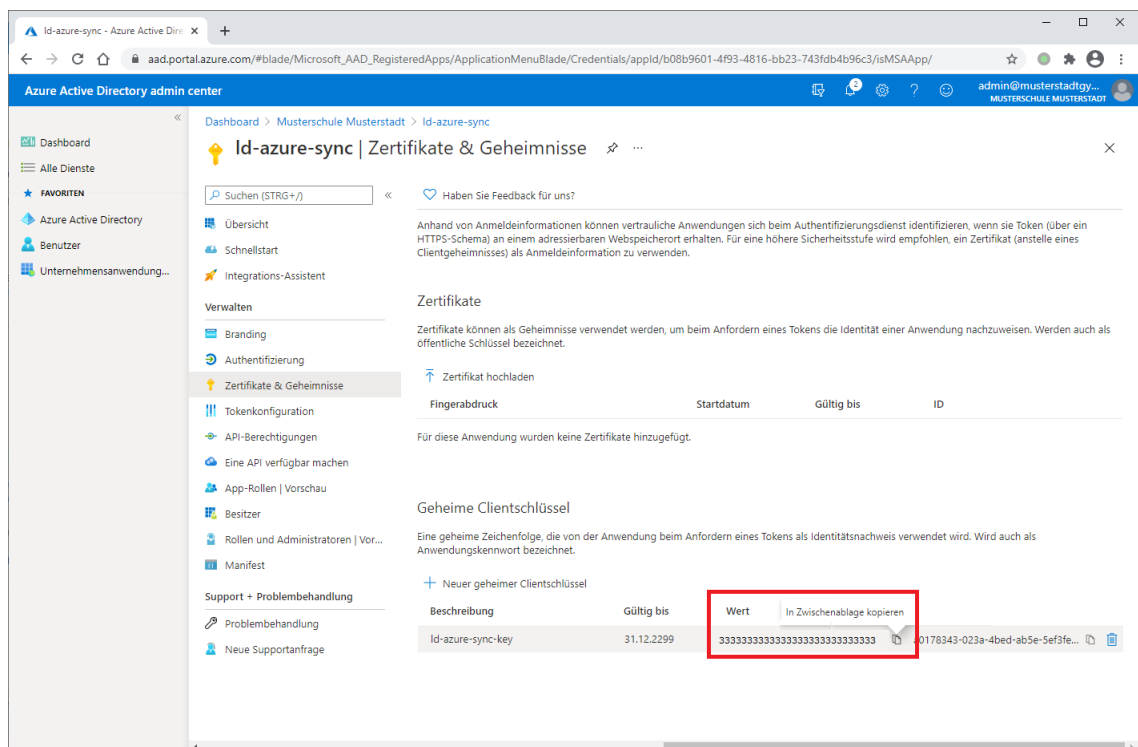


Geben Sie den neue Schlüssel im Feld **Beschreibung** den Namen **ld-azure-sync-key** und setzen Sie den Radio-Button für die Gültigkeit auf **Nie**, was in der Praxis bedeutet, dass der Key nicht abläuft.

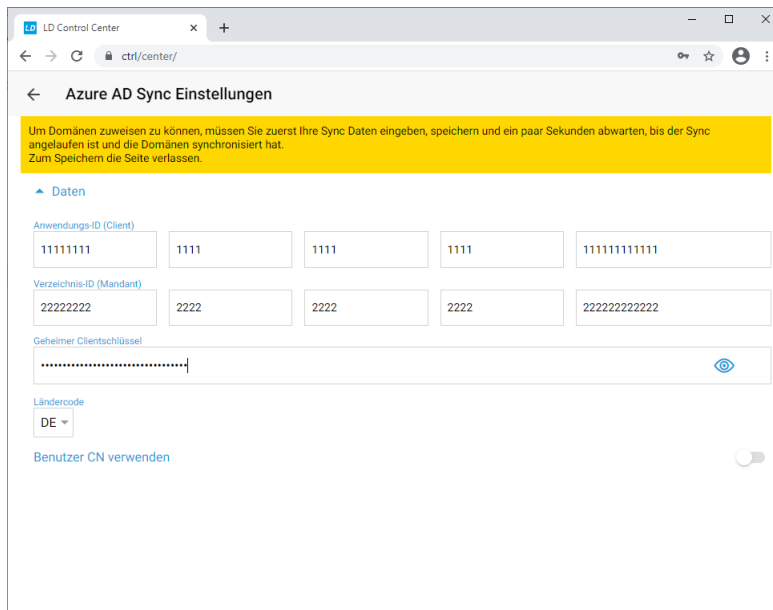
Einen geheimen Clientschlüssel in Azure-AD anlegen



Kopieren Sie anschließend den **Wert** des geheimen Clientschlüssels in die Zwischenablage und wechseln Sie ins Control Center.




Fügen Sie den Wert aus der Zwischenablage im Feld **Geheimer Clientschlüssel** ein.



ALT->VERSCHIEBEN

Tragen Sie im Feld **Domain Name** in jedem Fall den Namen der neu erstellen Domäne ein, in unserem Beispiel ist dies **musterschule.online**. Wenn Sie keinen Namen angeben, werden die Daten automatisch zu der Domäne synchronisiert, die auf Standard steht. Das kann insbesondere dann zum Chaos führen, wenn jemand in Azure-AD eine weitere Domäne anlegt und diese versehentlich zur Standard-Domäne macht.



Achtung

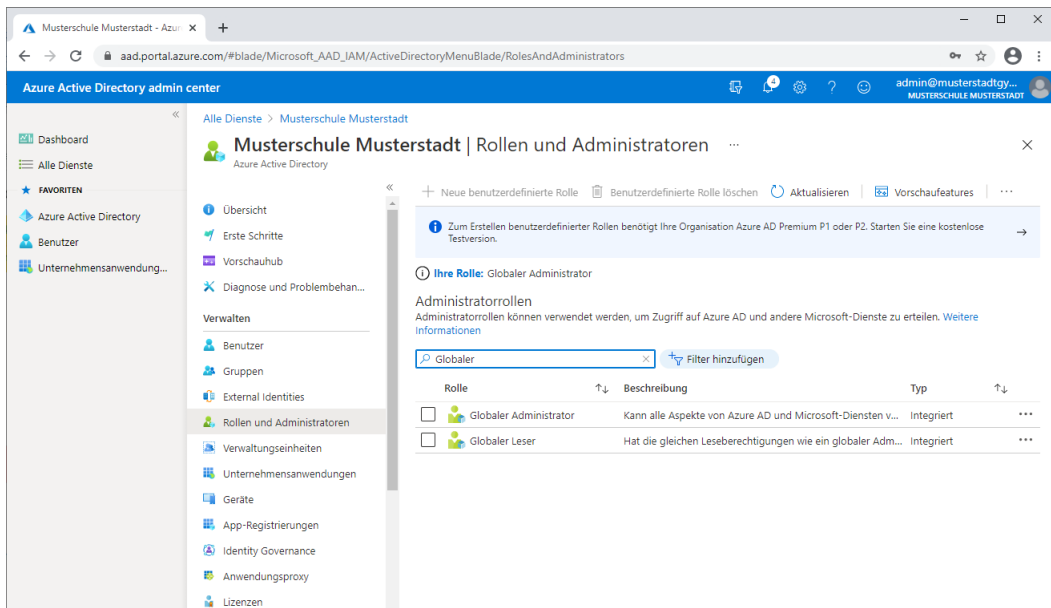
Tragen Sie immer die Domäne ein, zu der der Connector die Daten synchronisieren soll!

ALT->VERSCHIEBEN

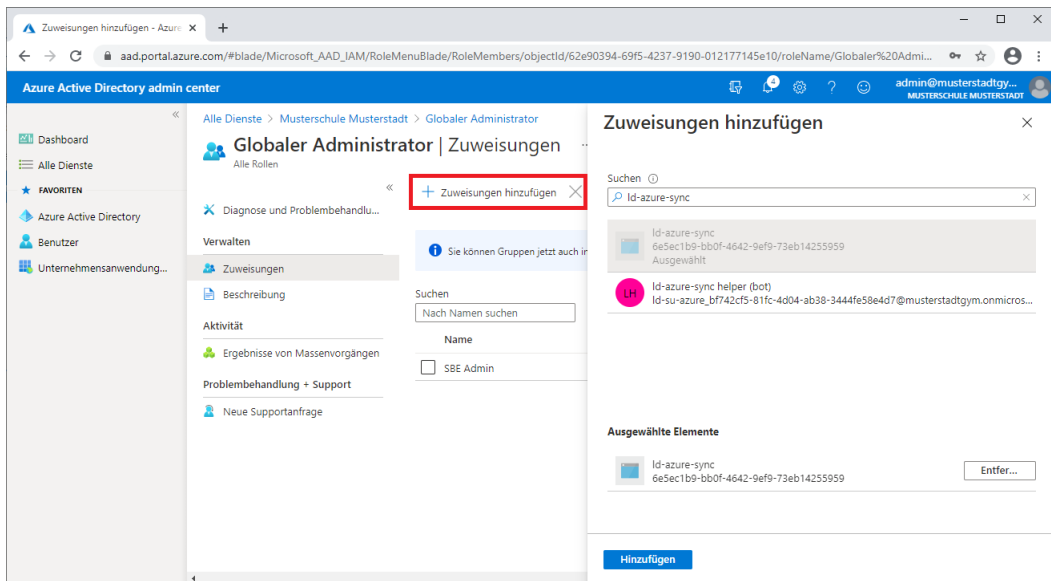
III.9.2.6. Der APP administrative Rechte zuweisen

Im nächsten Schritt müssen auf der Azure-Seite der Synchronisations-APP noch entsprechende Rechte zugewiesen werden. Gehen Sie dazu auf die Menüauswahl **Rollen und Administratoren** und geben Sie in das Feld **Suchen** das Wort **Global**, um die Auswahl auf das Wesentliche zu beschränken.

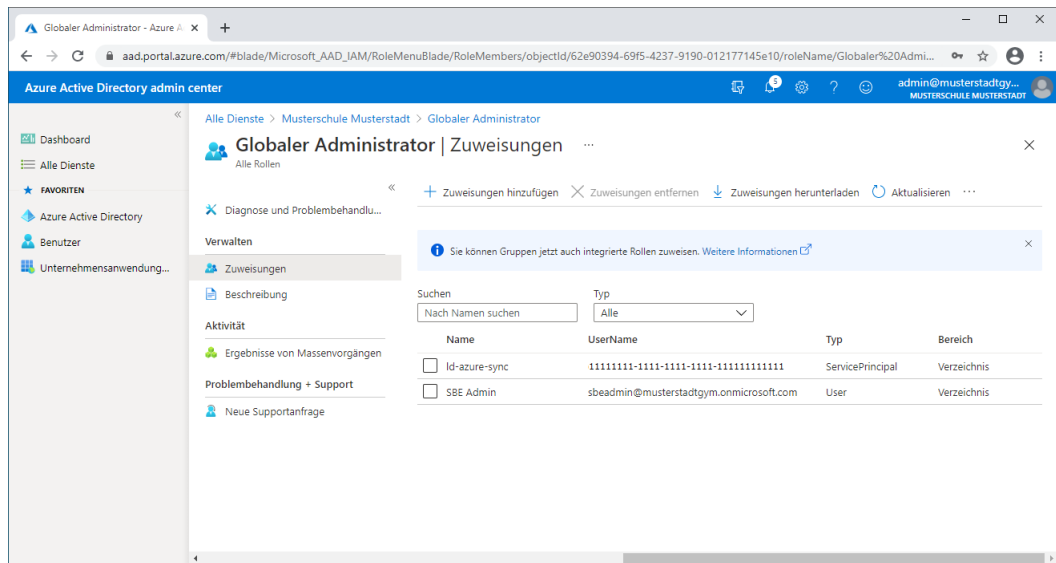
Klicken Sie dann auf den Benutzer **Globaler Administrator**.



Wählen Sie den Eintrag + **Zuweisungen hinzufügen** und geben Sie im Suchfeld den Namen **Id-azure-sync** der APP ein. Durch Auswahl der gefundenen APP und Drücken der Schaltfläche **Hinzufügen** wird die Berechtigung abgeschlossen.



Damit verfügt die APP über die notwendigen Rechte in Azure-AD Objekte anzulegen, zu verändern oder zu löschen.



Damit ist die Verbindung zwischen dem LogoDIDACT-Server und Azure-AD hergestellt.

III.9.2.7. Connector an ID koppeln

Ab Puppet-Release-Stand 1.3.22-9 (März 2021) wird von **LD Azure Connect** der Multi-Domain-Betrieb unterstützt, d.h. mehrere Schulen bzw. LogoDIDACT-Server können sich an einen Tenant koppeln und dort getrennt voneinander in verschiedenen Domains Benutzerkonten automatisch anlegen.

Es gibt damit also mehrere Quellen und damit mehrere Konnektoren. Damit die vom jeweiligen **LD Azure Connect** generierten Objekte eindeutig voneinander separierbar sind und auf Azure-Seite immer klar ist, welcher Konnektor welches Objekt erstellt hat, gibt es eine eindeutige **Sync-ID**.

Diese **Sync-ID** wird automatisch generiert, sofern dies in Puppet aktiviert wird. Wechseln Sie dazu in den Container **puppeteer** und dort in das entsprechende Verzeichnis `/etc/logodidact/hiera/custom.d`.

```
lxc-ssh -n puppeteer
```

```
cd /etc/logodidact/hiera/custom.d
```

Prüfen Sie, ob es in dem Verzeichnis bereits eine Datei `ad-sync-g1.yaml` gibt und falls nicht, erstellen Sie diese mit einem Editor Ihrer Wahl und tragen Sie dort folgende Angaben ein:

```
---
profile::host::ad_sync::enable_sync_id: true
```

Wechseln Sie auf die passende Verzeichnisebene und tragen Sie Ihre Änderungen im Versionsverwaltungssystem git ein:

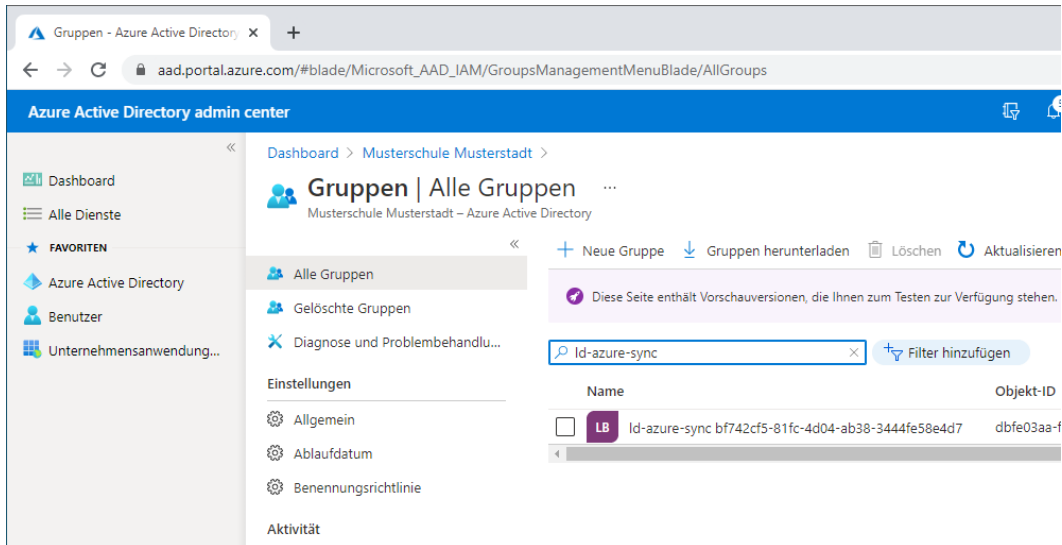
```
cd /etc/logodidact
```

```
git add .
```

```
git commit -m "aktiviere Sync-ID für LD Azure Connect"
```

Ein **prun** im Container **ad-sync-g1** sorgt dafür, dass die Veränderung beim Connector ankommt und aktiviert wird. Die von Puppet dynamische vergebene ID für den Konnektor findet sich auch

auf dem Tenant selbst und wird dort als Gruppe nach der Konvention `ld-azure-syncSYNC-ID` angelegt.

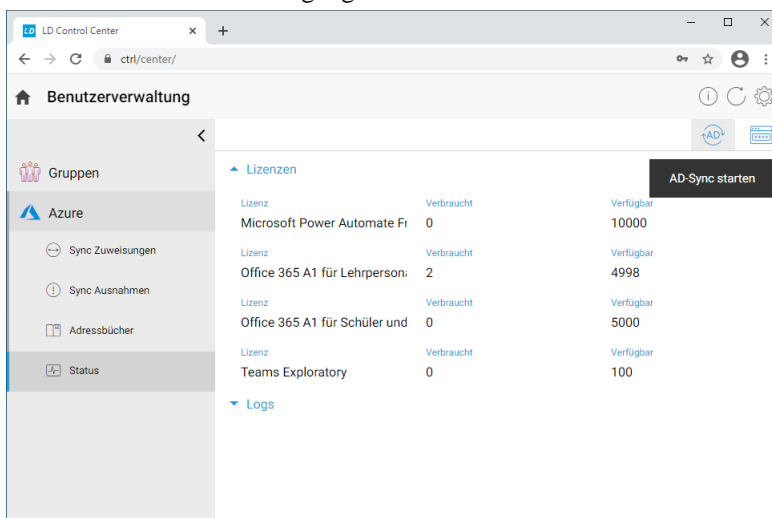


Für jeden angekoppelten LogoDIDACT-Server und jeden Konnektor wird dort eine Gruppe nach obigem Schema angelegt.

III.9.2.8. Benutzern im Control Center Office 365 Lizenzen zuweisen

Nachdem die **Sync-ID** per Puppet aktiviert wurde, kann die Kommunikation zwischen **LD Azure Connect** und dem Microsoft Tenant hergestellt werden. Über die Auswahl **Status** aus dem Menü **Azure** auf der linken Seite sieht man auf der rechten Seite grundlegende Infos zur Lizenzierung. Wählen Sie das AD-Symbo im rechten oberen Bereich, um eine manuelle neue Synchronisation von **LD Azure Connect** anzustoßen.

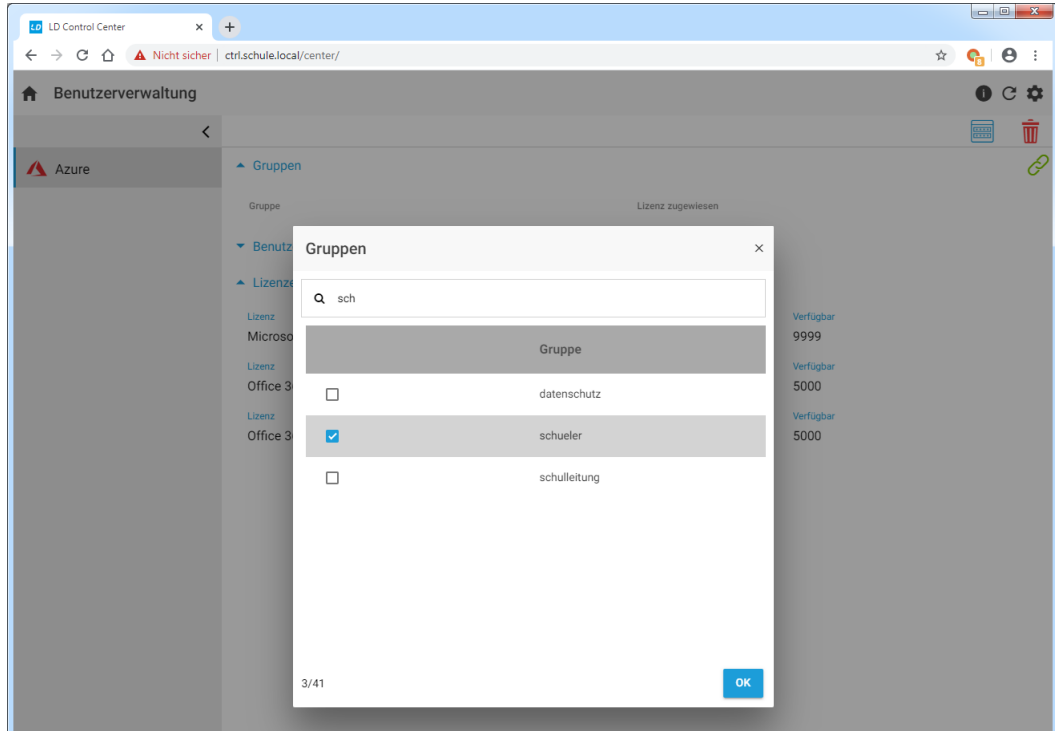
Die angezeigten Einträge hängen entscheidend vom so genannten Plan ab. Beim kostenfreien Office 365 A1 sehen die zur Verfügung stehenden Lizenzen in etwa so aus.



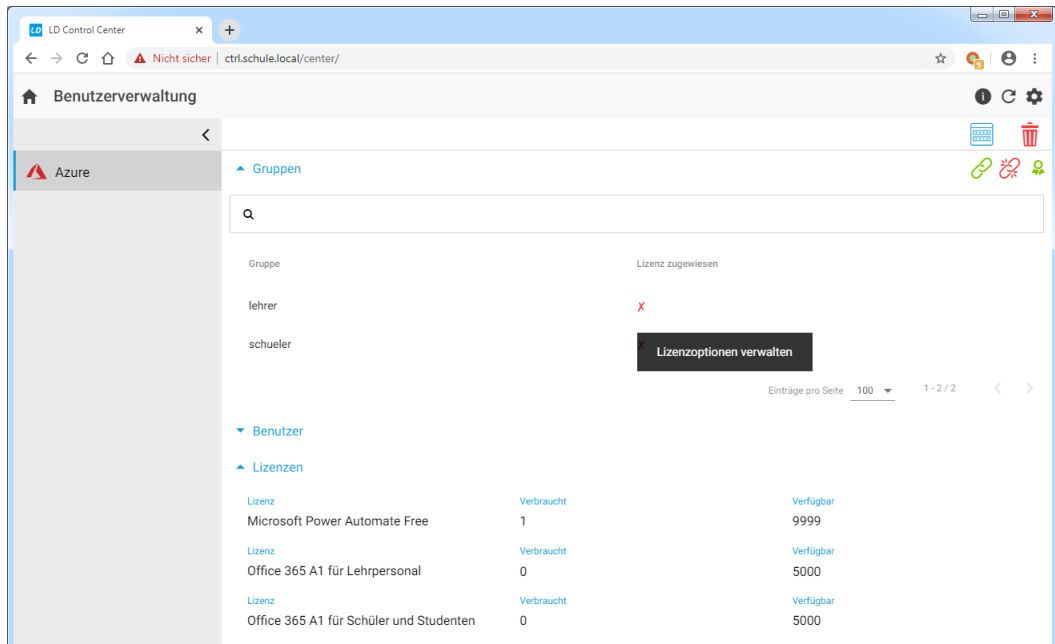
Damit nicht nur Benutzerkonten synchronisiert, sondern auch gleich Lizenzen automatisch zugewiesen werden, verknüpfen Sie die Azure-Gruppe mit einer bestehenden lokalen Gruppe. Markieren Sie

den Eintrag **Gruppe** und klicken Sie auf der rechten Seite auf das große Verknüpfungssymbol (Büroklammer). Geben Sie im Suchfeld die Buchstaben **sch** ein, um möglichst schnell die Gruppe der Schüler angezeigt zu bekommen.

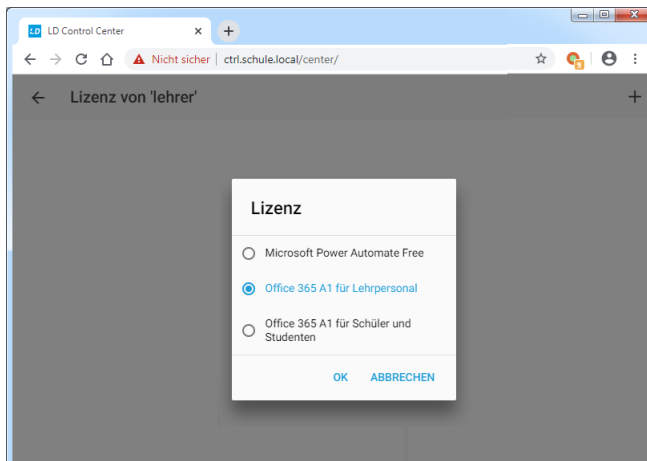
Wählen Sie die Gruppe aus, indem Sie das Häkchen im Auswahlfeld setzen und bestätigen Sie mit **OK**.



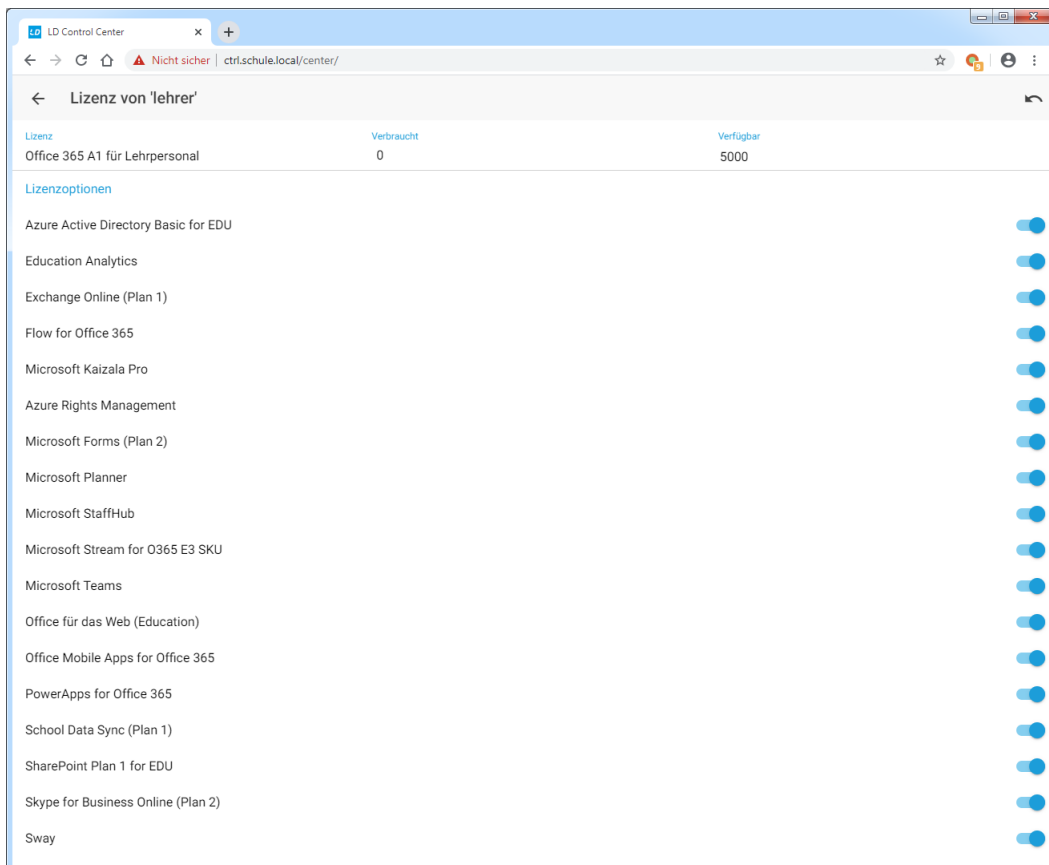
Verfahren Sie analog mit der Gruppe Lehrer und fügen Sie auch diese Gruppe hinzu. Starten Sie dann die Lizenzzuweisung, indem Sie auf das rote x in der Spalte **Lizenzen zuweisen** klicken.



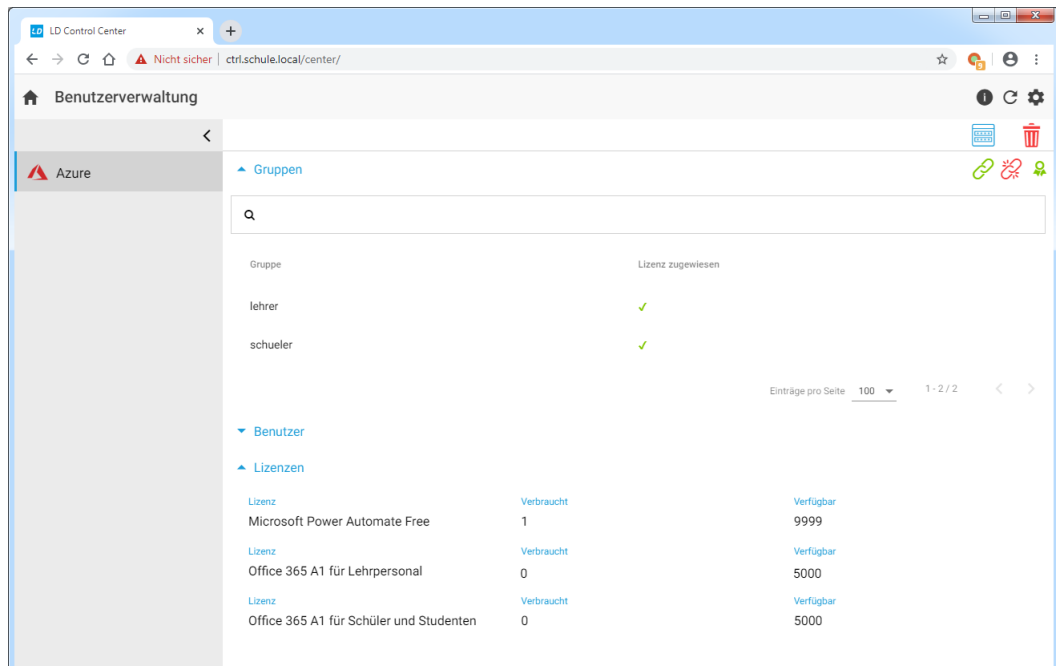
Ordnen Sie den Lehrern die passenden Lizenzen für das Lehrpersonal zu bestätigen Sie mit **OK**



Über den nächsten Dialog können Sie sehr detailliert auf Ebene beliebiger Gruppen in LogoDIDACT oder auch für einzelne Benutzer festlegen, welche Anwendungen lizenziert und damit in der Cloud verfügbar sein sollen.



Verfahren Sie danach analog mit der Lizenzzuweisung für Schüler, so dass beiden Gruppen die entsprechenden Produkte und Lizenzen zugewiesen sind.



III.9.2.9. Benutzer zu Azure AD synchronisieren

Die Synchronisation vom lokalem AD des LogoDIDACT Servers zum Azure Active Directory in der Cloud läuft voll automatisch und zyklisch über den Connector ab.

Folgende Funktionen werden dabei bisher durchgeführt:

- Alle Benutzer, die im Control Center der Azure-Konfiguration hinzugefügt wurden, werden synchronisiert
- Alle Gruppen (Klassen und Projekte) sowie Rollen für die Benutzer in der Azure-Konfiguration werden synchronisiert
- Alle Kennwörter für Benutzer werden synchronisiert
- Benutzer, die in der lokalen LogoDIDACT Umgebung gelöscht werden, werden auch aus Azure-AD gelöscht und zuvor die Lizenz entzogen, so dass diese anderen Benutzer automatisch wieder zugewiesen werden kann
- Benutzer werden nicht nach Azure-AD synchronisiert, wenn das Kennwort in LogoDIDACT nicht den Kennwortrichtlinien von Azure-AD entspricht.



Achtung

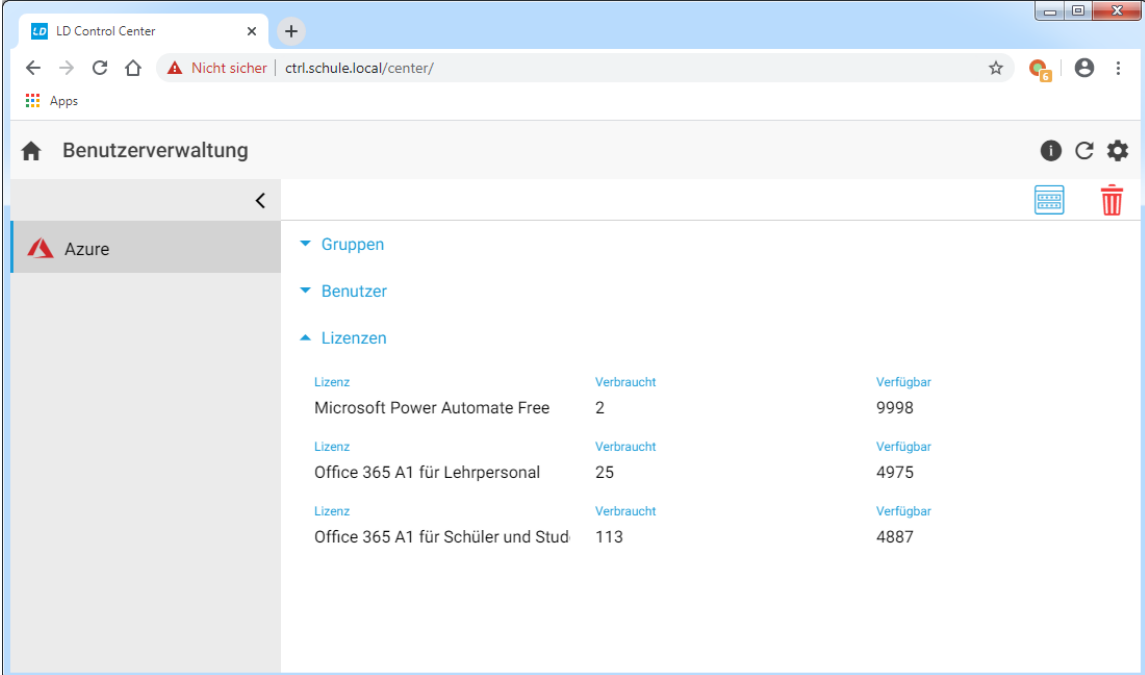
Das Anlegen von Benutzern mit zu kurzen oder zu einfachen Kennwörtern, wird von Azure-AD durch eine Kennwortrichtlinie verhindert.

Ein Kennwort in Azure-AD muss mindestens 8 Zeichen lang sein, einen Großbuchstaben, eine Zahl und ein Sonderzeichen enthalten.

Die Kennwortrichtlinien im lokalen pädagogischen LogoDIDACT -Netz wurden in der Vergangenheit bewusst niedriger gewählt mit einer Länge von 5 Zeichen, in der minde-

stens eine Zahl enthalten sein musste. Diese Kennwortrichtlinie sollte beim Einsatz von Office 365 bzw. dem Freischalten von Diensten per Web nach außen angepasst werden.

Auf graphischer Ebene im Control Center gibt es derzeit (März 2020) noch keine detaillierten Informationen über die Synchronisation von Benutzern und Objekten. Indirekt sichtbar ist die Anzahl der erfolgreich synchronisierten Benutzer über die Lizenzierung. Im unten aufgeführten Beispiel wurden 25 Lizenzen für Lehrerinnen und Lehrer zugewiesen und 113 für Schülerinnen und Schüler. Daraus lässt sich schließen, dass diese 138 Benutzer ein hinreichend langes und komplexes Kennwort hatten.



The screenshot shows the 'Benutzerverwaltung' (User Management) section of the LD Control Center. Under the 'Azure' tab, the 'Lizenzen' (Licenses) section is expanded, displaying a table of license usage:

Lizenz	Verbraucht	Verfügbar
Microsoft Power Automate Free	2	9998
Office 365 A1 für Lehrpersonal	25	4975
Office 365 A1 für Schüler und Stud	113	4887

Um festzustellen, bei welchen Benutzer das Kennwort nicht passt oder ob es andere Gründe gibt, warum das Konto nicht nach Azure-AD synchronisiert werden konnte, muss man sich am Server einwählen.

Wechseln Sie diesbezüglich auf den LogoDIDACT Server und dort in den Container des neuen Connectors:

```
lxc-ssh -n ad-sync-g1
```

Über den folgenden Befehl können Sie die Synchronisation beobachten und vor allem auch Fehler und deren Ursache erkennen:

```
journalctl -f -u ld-azure-sync.service
```

Der häufigste Grund, warum ein Benutzer nicht nach Azure-AD synchronisiert wird, hängt mit den Kennwortrichtlinien ab, die auf Seiten der Microsoft-Cloud sinnvollerweise etwas höher gewählt sind, als im lokalen LogoDIDACT Netzwerk.

```
root@ad-sync-g1:~# journalctl -f -u ld-azure-sync.service
Mar 29 17:50:43 ad-sync-g1 LdAzureSync[47]: 2020-03-29 17:50:43,357 [120] WARN LdAzureSync.Rest.AzureAdClient - Failed to create user: null|Benutzername
Mar 29 17:50:43 ad-sync-g1 LdAzureSync[47]: {
Mar 29 17:50:43 ad-sync-g1 LdAzureSync[47]:   "error": {
Mar 29 17:50:43 ad-sync-g1 LdAzureSync[47]:     "code": "Request_BadRequest",
Mar 29 17:50:43 ad-sync-g1 LdAzureSync[47]:     "message": "The specified password does not comply with password complexity requirements. Please provide a different password.",
Mar 29 17:50:43 ad-sync-g1 LdAzureSync[47]:     "innerError": {
Mar 29 17:50:43 ad-sync-g1 LdAzureSync[47]:       "request-id": "836af800-8edc-4e01-b695-b386129aee4f",
Mar 29 17:50:43 ad-sync-g1 LdAzureSync[47]:       "date": "2020-03-29T15:50:40"
Mar 29 17:50:43 ad-sync-g1 LdAzureSync[47]:     }
Mar 29 17:50:43 ad-sync-g1 LdAzureSync[47]:   }
```

Damit die Benutzer ihr Kennwort ändern können, gibt es ein Web-Portal, über das die Benutzer ihr Kennwort ändern können.

III.9.3. Das Kennwortportal SSP konfigurieren

Im Zusammenhang mit Office 365 müssen die Kennwörter der Benutzer den Kennwortrichtlinien von Microsoft entsprechen. Damit die Benutzer auch von zu Hause aus ihr Kennwort abändern können, wird über den Container **ssp-gl** ein Kennwortportal zur Verfügung gestellt, das zusammen mit dem Connector aktiviert wurde. Das Kennwortportal wird kurz als SSP-Portal (Self-Service-Passwort) bezeichnet.

Damit das Kennwortportal von außen zugänglich ist, muss es über den Reverse-Proxy erreichbar und entsprechend konfiguriert werden. Wechseln Sie dazu in den Puppeteer:

```
lxc-attach -n puppeteer
```

Wechseln Sie in das Verzeichnis zur Konfiguration des Reverse-Proxy:

```
cd /etc/logodidact/hosts/rev-proxy
```

Ergänzen Sie die Datei `revproxy.conf` mit folgendem Inhalt für das Kennwortportal. Das Schulkürzel entspricht dabei in der Regel wieder dem zuvor festgelegten Domänennamen, d.h., in unserer beispielhaften Umgebung `musterstadt-gym`.

```
[ReverseProxy ssp.SCHULKUERZEL.logoip.de]  
Url https://ssp.schule.local
```



Achtung

Bitte beachten Sie, dass das SSP-Portal aus Sicherheitsgründen ausschließlich verschlüsselt erreichbar ist, sowohl extern als auch intern. Die **Url** muss deshalb auf **https** zeigen!

Pflegen Sie die Änderungen wie gewohnt ins git ein:

```
cd /etc/logodidact
```

```
git add .
```

```
git commit -m "Konfiguration Kennwortportal ssp im rev-proxy".
```

Führen Sie danach ein **ldupdate** im Puppeteer durch gefolgt von einem **prun**. Führen Sie danach einen Neustart von nginx durch: **/etc/init.d/nginx restart**.

Wenn man danach von außen auf das Kennwort-Portal zugreift (im Beispiel über `https://ssp.musterstadt-gym.logoip.de` erhält man, je nach Browser, die typische Rückmeldung für eine vermeintlich unsichere Seite.



Prüfen Sie im Container **Puppeteer** zunächst, ob Sie dort über den Befehl **sle** in die Umgebung zur Verwaltung der Zertifikate kommen. Stellen Sie dies gegebenenfalls um, wie in Abschnitt III.3.6.3.1, „Umstellung auf das Tool acme.sh“ beschrieben.

Starten Sie dann in die Umgebung zur Verwaltung der Let's Encrypt Zertifikate und stellen für den Dienst einen entsprechenden Antrag:

```
sle
```

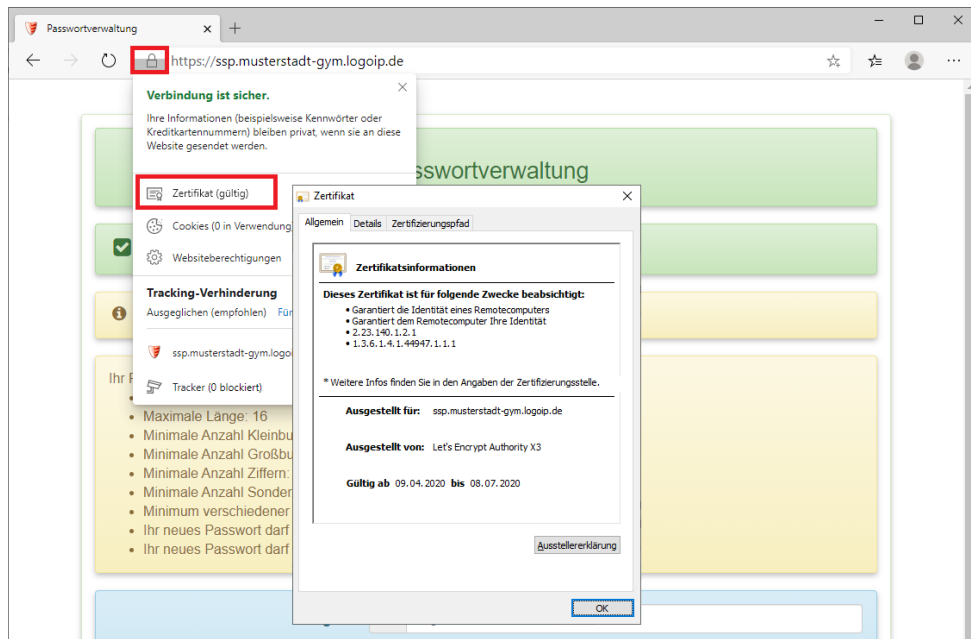
```
issue ssp.SCHULKUERZEL.logoip.de
```

Hierbei steht **schulkuerzel** für den bereits mehrfach verwendeten individuellen Namen (z.B. musterstadt-gym).

Die Rückmeldung an Infos ist im Fall von **acme.sh** in der Regel sehr ausführlich. Mit dem folgenden Befehl kann man sich eine Liste aller Zertifikate anzeigen lassen und damit auch den Status prüfen:

```
acme.sh --list
```

Wenn das Zertifikat erstellt und heruntergeladen wurde, landet es über Puppet irgendwann im Container **rev-proxy** im Ordner `/etc/nginx/ssl`. Das Ganze lässt sich ggf. wieder über einen **prun** im **puppeteer** und danach im **rev-proxy** beschleunigen.



III.9.4. Die Zwei-Faktor-Sicherheit in Azure-AD deaktivieren




Achtung

Die erhöhte Sicherheit über die so genannte Zwei-Faktor-Authentifizierung (kurz 2FA) ist grundsätzlich eine sehr sinnvolle Sache. Für die meisten Benutzer stellt dies jedoch beim Einstieg in die Nutzung von Office 365 eine entsprechende Hürde da, weil der zweite Faktor in der Regel eine Smartphone-Nummer ist.

Nicht jeder Benutzer muss zwangsweise ein Mobiltelefon besitzen.

Melden Sie sich über portal.azure.com mit dem administrativen Konto für Ihren Tenant an. Wählen Sie aus der linken Verzeichnisstruktur **Azure Active Directory** und aus dem mittleren Menü den Eintrag **Eigenschaften**. Im unteren Bereich klicken Sie dann auf den Link **Sicherheitsstandards verwalten**. Darauf öffnet sich ein Fensterbereich auf der rechten Seite. Setzen Sie den Schieberegler beim Eintrag **Sicherheitsstandards aktivieren** auf **Nein**. Aktivieren Sie ein passendes Häkchen, warum Sie die Zweifaktor-Sicherheit deaktivieren und bestätigen Sie alles mit **Speichern**.



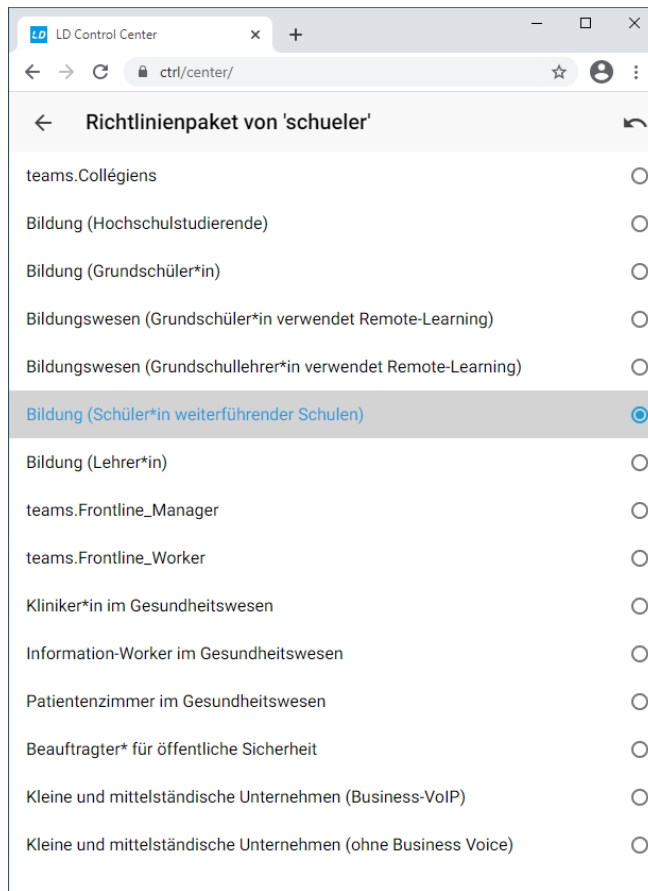
Tipp

Alle Informationen zur Anmeldung an Office 365, sowie den Umgang mit Kennwörtern finden sich im Anwenderteil der Doku!

III.9.5. Besprechungs-Richtlinien in Teams anpassen

Über das **ControlCenter** kann man pro Klasse, Gruppe oder auch einzelнем Benutzer ein Richtlinienpaket zuweisen. In aller Regel erfolgt das separat für die Rolle Schüler und Lehrer mit den von Microsoft dafür vorgesehenen Paketen, deren Namen und damit die Zuordnung selbsterklärend sind.

Dies ist für unser beispielhaftes Gymnasium Musterstadt in folgender Grafik veranschaulicht und dort die Richtlinie **Bildung (Schüler*in weiterführender Schulen)** für die Rolle **schueler** die "richtige" Wahl.



Was sich hierbei hinter diesen Richtlinien verbirgt, wird von Microsoft festgelegt und muss nicht zwangsweise das sein, was man für seine Schülerinnen und Schüler festlegen möchte.



Tipp

Die Besprechungs-Richtlinien für Teams können detailliert über **Puppet** angepasst werden!

Wechseln Sie dazu in den Container **puppeteer** und dort in das entsprechende Verzeichnis `/etc/logodidact/hiera/custom.d`.

```
lxc-ssh -n puppeteer
```

```
cd /etc/logodidact/hiera/custom.d
```

Prüfen Sie, ob es in dem Verzeichnis bereits eine Datei `ad_sync-g1.yaml` gibt und falls nicht, erstellen Sie diese mit einem Editor Ihrer Wahl und tragen Sie dort folgende Angaben ein:

```
---  
profile::host::ad_sync::options:  
  Teams:  
    MeetingPolicy:  
      AutoAdmittedUsers: "EveryoneInCompany"
```

```
AllowPSTNUsersToBypassLobby: true
DesignatedPresenterRoleMode: "OrganizerOnlyUserOverride"
```

Die Werte für **AutoAdmittedUsers** bestimmen, wer automatisch zu einem Meeting zugelassen wird und nicht in den Wartebereich bzw. in die Lobby muss:

```
Everyone
EveryoneInCompany
EveryoneInSameAndFederatedCompany
EveryoneInCompanyExcludingGuests
OrganizerOnly
```

Die Werte für **AllowPSTNUsersToBypassLobby** bestimmen, ob "Einwahlbenutzer" (Telefon) automatisch zu einem Meeting zugelassen werden und den Wartebereich umgehen dürfen:

```
true
false
```



Achtung

Wenn **AutoAdmittedUsers** auf Everyone bzw. OrganizerOnly steht, muss **AllowPSTNUsersToBypassLobby** true bzw. false sein.

Wenn Sie die Kombination in der Config falsch angeben, wird der falsche Wert für **AllowPSTNUsersToBypassLobby** ignoriert.

Die Werte für **DesignatedPresenterRoleMode** legen fest, welche Personen in Teams präsentieren bzw. ihren Bildschirm teilen dürfen:

```
EveryoneUserOverride
EveryoneInCompanyUserOverride
OrganizerOnlyUserOverride
```

Wechseln Sie auf die passende Verzeichnisebene und tragen Sie Ihre Änderungen im Versionsverwaltungssystem git ein:

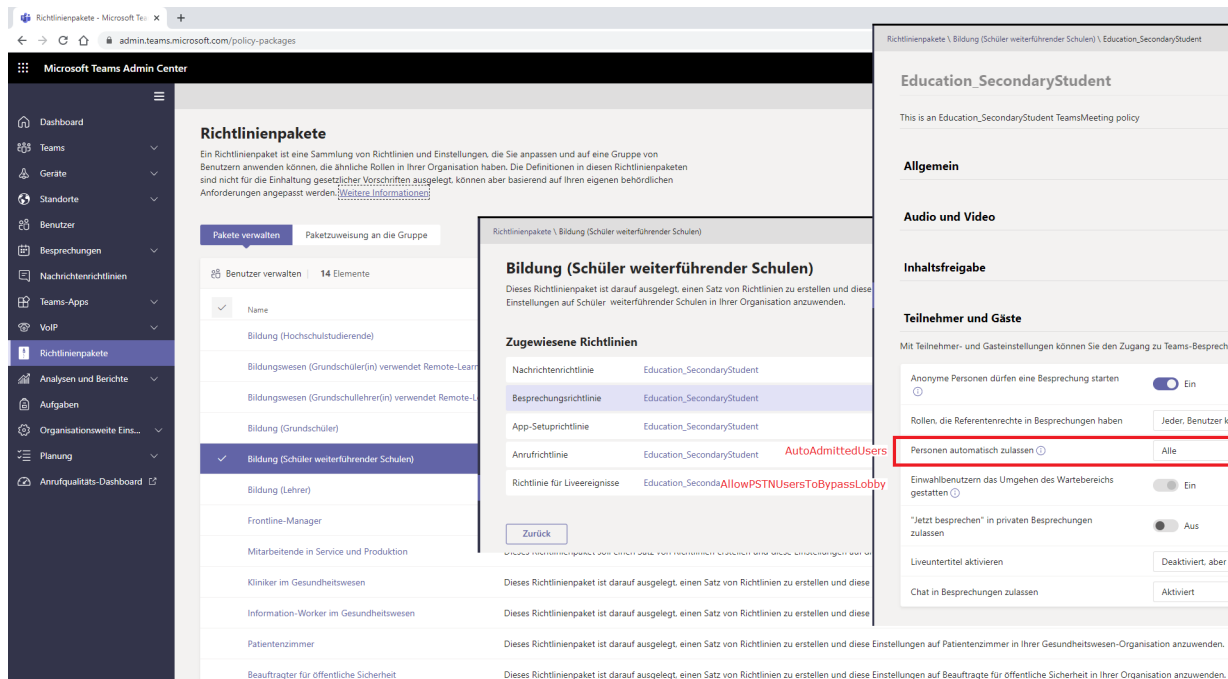
```
cd /etc/logodidact
```

```
git add .
```

```
git commit -m "Anpassung für Teams Besprechungs-Richtlinien"
```

Ein **prun** im Container **ad-sync-g1** sorgt dafür, dass die Veränderung beim Connector ankommt und aktiviert wird.

Auf graphischer Oberfläche im Teams-Admin-Center finden sich die Einträge wie in folgender Grafik gezeigt.



III.9.6. Richtlinien in Teams unberührt lassen

Sofern eine Schule über einen administrativen Zugang zu Microsoft Teams verfügt und über tiefgehendes Know-how in der Konfiguration, können individuelle Anpassungen auch im Teams Admin-Center vorgenommen werden.

Dann ist es sinnvoll, die Konfiguration von **LD Azure Connect** so anzupassen, dass der Konnektor die Richtlinien in Teams unberührt lässt. Dies erfolgt über die folgende Anpassung in der Datei `ad-sync-g1.yaml`:

```
---
profile::host::ad_sync::options:
  Teams:
    MeetingPolicy: null
```

Mit dieser Einstellung wird verhindert, dass der AzureSync die MeetingPolicies überhaupt anfasst.

III.9.7. Benutzer und Rechte anpassen

In den folgenden Abschnitten werden spezielle Szenarien und Anpassungen erläutert, die mit **LD Azure Connect** derzeit möglich sind.

III.9.7.1. Umgang mit bestehenden Benutzern in Azure

Sofern eine Schule bereits über einen eigenen Tenant verfügt und diesen erst im Nachgang über **LD Azure Connect** an LogoDIDACT anknüpft, gibt es möglicherweise auch schon bestehende Benutzerkonten und Daten in der Microsoft Cloud.

Bei der Anknüpfung kann über den Parameter **ConflictingUsers** bestimmt werden, wie der Konnektor mit bereits bestehenden manuell angelegten Benutzerkonten umgehen soll. Wie alle obigen Anpassungen, erfolgt auch diese über die Datei `/etc/logodidact/hiera/custom.d/ad-sync-g1.yaml` im Puppeteer:

```
---
profile::host::ad_sync::options:
  ConflictingUsers: null
```

Der Parameter bestimmt, was passieren soll, wenn **LD Azure Connect** ein Benutzerkonto in der Microsoft-Cloud anlegen will, es dort aber bereits ein manuell angelegtes Konto mit gleichem Account-Namen gibt.

Wert	Bedeutung
null	Es werden keine bestehenden manuell angelegten Benutzer konvertiert (Standard)
CHECK	Listet die User im azure-sync log auf, die konvertiert werden würden (entspricht einem "Probelauf")
CONVERT	Konvertiert manuell angelegte Benutzer

III.9.7.2. Benutzern Admin-Rollen zuweisen

Sofern eine Schule über Personen mit tiefgehendem Know-how in der Administration von Microsoft Teams verfügt, kann es sinnvoll sein, einem oder mehreren Benutzern in Azure-AD eine administrative Rolle zuzuweisen.

Dies ist über die folgende Anpassung in der Datei `/etc/logodidact/hiera/custom.d/ad-sync-g1.yaml` im Puppeteer möglich:

```
---
profile::host::ad_sync::options:
  Roles:
    Global Administrator:
      - te
    Teams Communications Administrator:
      - be
```

In obigem Beispiel wurde unserem fiktiven Lehrer Tom Engel über sein Konto **te** die Rolle als Globaler Administrator zugewiesen und seinem Kollegen Marco Becker über sein Konto **be** die Rolle Teams Communications Administrator.

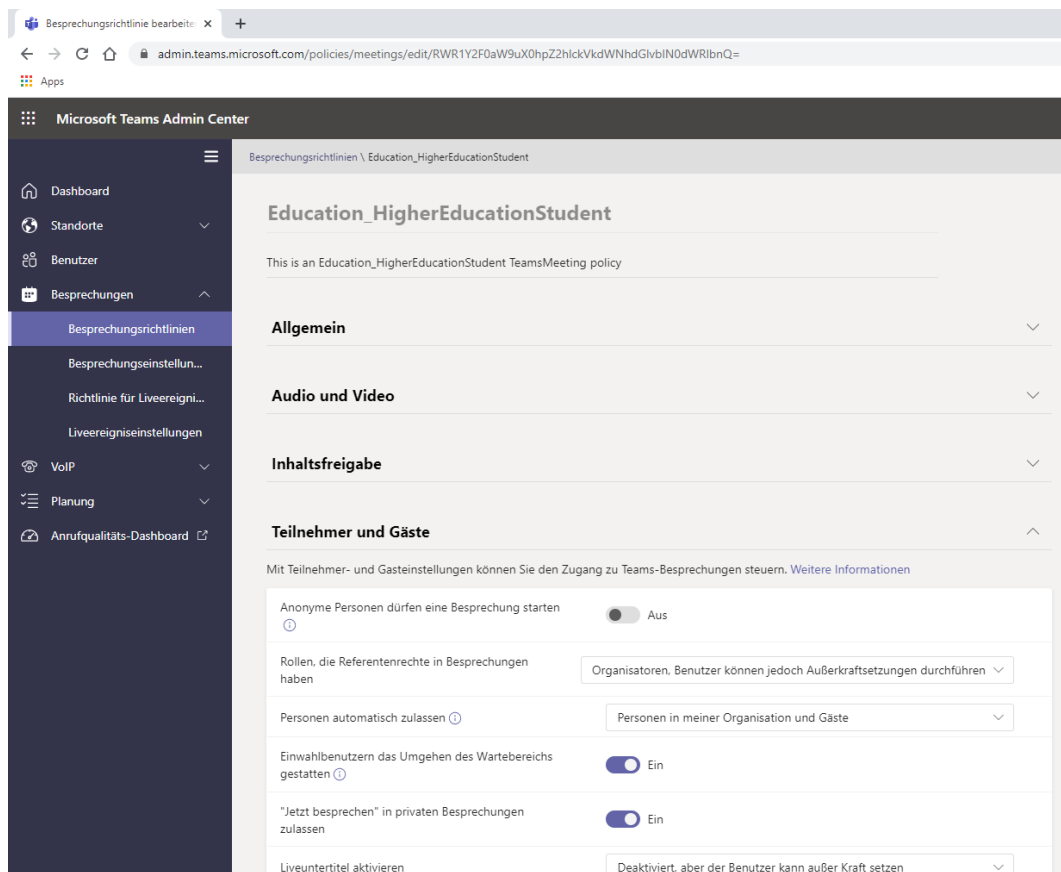


Achtung

Rollen können selbstverständlich nur Benutzern zugewiesen werden, die von **LD Azure Connect** synchronisiert und damit verwaltet werden.

Die Liste an aktuell verfügbaren Rollen, findet sich unter `/etc/ld-azure-sync/AllAvailableRoles.txt` im Container **ad-sync-g1**. Der AzureSync erstellt diese Datei dynamisch mit allen verfügbaren Rollen des Tenants zusammen mit einer kleinen Beschreibung.

Als Teams Communications Administrator können Sie über den folgenden Link alle wesentlichen Anpassungen für Teams vornehmen: <https://admin.teams.microsoft.com/>



Sollten Sie bereits über einen administrativen Zugang verfügen, besteht auch wieder die Möglichkeit, den Konnektor so zu konfigurieren, dass er keinerlei Anpassungen von Benutzern und Rollen vornimmt.

```
profile::host::ad_sync::options:
  Roles: null
```

III.9.7.3. Erstellen manueller Teams verbieten

Eine der grundlegenden Aufgaben von **LD Azure Connect** besteht darin, in LogoDIDACT bereits vorhandene Gruppen, also Klassen und Projekte automatisiert in Azure und auch Teams anzulegen.

Dazu gibt es im Anwenderteil für Teams klare Empfehlungen und Vorgaben, was die Lehrerinnen und Lehrer dabei zu beachten haben. Leider werden diese Vorgaben nicht immer beachtet und deshalb mit einem riesigen Zeitaufwand manuelle Strukturen aufgebaut, meist verbunden mit falschen Einstellungen.

Um zu verhindern, dass Lehrerinnen und Lehrer das tun, können Sie das Anlegen von Gruppen über folgende Parameter verhindern:

```
profile::host::ad_sync::options:
  AllowGroupCreationForTeachers: false
  AllowGroupCreationForUnmanagedUsers: true
```

Mögliche Werte für **AllowGroupCreationForTeachers** sind true oder false. Darüber wird bestimmt, ob Lehrer*innen Gruppen/Teams erstellen können oder nicht.

Über **AllowGroupCreationForUnmanagedUsers** wird festgelegt, ob nicht gemanagte, also von Hand erstellte Benutzer Gruppen/Teams erstellen können oder nicht.

Kapitel III.10. Nextcloud

Bei Nextcloud handelt es sich um eine freie Cloud-Software zur Speicherung von Daten auf einem eigenen Server in der Cloud oder lokal. Der Zugriff erfolgt dabei in der Praxis überwiegend per Webbrowser über ein anwenderfreundliches Portal. In diesem Zusammenhang ersetzt Nextcloud von der Funktionalität den Open-Source-Baustein PYDIO als Modul für den webbasierten Dateizugriff in LogoDIDACT.



Achtung

Die Entwicklung von Nextcloud ist sehr dynamisch und wird einzig durch die Firma Nextcloud GmbH bestimmt.

SBE ist nicht für fehlerhafte Versionen und deren Folgen verantwortlich und stellt die Software innerhalb von LogoDIDACT so bereit, wie sie ist.

Bitte beachten Sie in diesem Zusammenhang die beiden grundlegend verschiedenen Modi des Betriebs, wenn es um die Wahl des Datenspeichers geht! Ebenso wichtig ist das Thema der Deaktivierung von Apps und Plugins.

III.10.1. Voraussetzungen

In einer Standard-Umgebung befindet sich der LogoDIDACT-Server an der Schule und das Modul Nextcloud wird dort wie üblich als Container aktiviert und als Webdienst über den Revproxy im Internet nach außen freigeschaltet. Der Zugriff erfolgt schulintern über das LAN oder WLAN und extern von außen über den DSL-Zugang der Schule.



Achtung

Ein häufig auftauchendes Problem, das im Zusammenhang mit der Verwendung von Nextcloud auftritt, betrifft die schlechte Performance bei entsprechender Last. Die Ursachen dafür sind häufig technische Beschränkungen zwei Bereichen:

- lahme Speichersysteme und unzureichende Dimensionierung der Serverhardware
- zu geringe Bandbreite des Internet-Anschlusses

1. Alte Serverhardware und langsame Speichersysteme

Der Einsatz performanter Serverhardware ist eine zwingend notwendige Voraussetzung für den funktionierenden Betrieb! Bei auftauchenden Performance-Problemen wird in diesem Zusammenhang von "Experten" gerne darauf hingewiesen, wie performant und problemlos eine in der Cloud betriebene Variante von Nextcloud funktioniert.

Wenn man sich dann diese Server näher anschaut, stellt auch der "Experte" fest, dass es sich um Systeme mit SSD- oder NVMe Speicher handelt, während man den lokalen Server an der Schule krampfhaft seit Jahren mit veralteter Technik am Laufen hält.

2. Schneller synchroner Internet-Anschluss

Eine zweite Voraussetzung betrifft die Bandbreite des Internetzugangs. Auch im Jahr 2021 ist leider vielen Anwendern noch immer nicht klar, welche Bedeutung ein schneller Internetzugang im

Betrieb hat und dass DSL-Anschlüsse leider oftmals nicht die gleiche Geschwindigkeit in beide Richtungen haben. Bei einem asymmetrischen 50 MBit DSL-Anschluss, hat man an der Schule direkt eine Downloadrate von bis zu 50 MBit/s, während der Zugriff von außen auf den Server mit maximal 10 MBit/s läuft.

Auch hier sollte klar sein, wo das Kernproblem liegt, wenn man eine in der Public-Cloud gehostete Instanz mit einer über 10 MBit angekoppelten Nextcloud-Variante vergleicht.

III.10.2. Die Container für Nextcloud und Collabora aktivieren

Wie üblich wird auch die Nextcloud in LogoDIDACT in einem separaten Container aufgebaut, der in diesem Fall den Namen **nextcloud-g1** trägt und ebenfalls nach dem üblichen Schema aktiviert wird. Gemeinsam mit **nextcloud-g1** wird in der Regel auch **collabora-g1** aktiviert, um das gemeinsame und zeitgleiche Bearbeiten von Dokumenten zu ermöglichen.

Wechseln Sie dazu in den Container **puppeteer** und dort ins Verzeichnis zur Konfiguration von Containern:

```
lxc-ssh -n puppeteer
```

```
cd /etc/logodidact/hosts/ldhost
```

Öffnen Sie die Datei `guest.conf` mit einem Editor Ihrer Wahl, wie z.B. Nano:

```
nano guest.conf
```

Ergänzen Sie die Datei um den Eintrag für den Container **nextcloud-g1** und **collabora-g1**. Zwingende Voraussetzung für Nextcloud ist das Vorhandensein der Container **postgres10** und **rev-proxy**.

```
[Guest nextcloud-g1]
Ensure running
```

```
[Guest collabora-g1]
Ensure running
```

Durch Eingabe der Tastenkombination `<Strg>+<X>` verlassen Sie den Editor Nano und geben „Y“ ein, damit die Änderung gespeichert wird. Wechseln Sie dann ins Stammverzeichnis der Konfiguration und übertragen Sie anschließend die Änderungen ins Versionierungssystem git:

```
cd /etc/logodidact
```

```
git add .
```

```
git commit -m "Aktivierung nextcloud und collabora"
```

Durch das Übertragen ins git-Repository wird auch automatisch `map_translate` aufgerufen, so dass die Konfigurationen in YAML übersetzt und von Puppet verarbeitet werden können.

Wie in den Grundlagen beschrieben, führen Sie den Aufbau gezielt und kontrolliert durch.

Mit einem **prun** im Host veranlassen Sie den Agenten, sich beim Puppeteer zu melden. Dieser baut die Catalog-Datei für den ldhost und schickt sie ihm. Der ldhost beginnt dann mit dem Aufbau der Container **nextcloud-g1** und **collabora-g1**. Beobachten können Sie das Ganze mit `pstat` im Puppet-

ter. Nach einer Weile werden die Container auftauchen. Sofern ein Container grundlegend aufgebaut ist und läuft, kann man in einer neuen Sitzung per `lxc-ssh -n nextcloud-g1` dort hineinwechseln und sofern gerade kein `prun` läuft einen solchen neuen Durchlauf mit `prun` starten. Zertifikate

III.10.3. Templates kopieren und anpassen

Um Dienste wie Nextcloud oder auch Collabora über Puppet anzupassen, gibt es entsprechende Vorlagen bzw. Templates in .YAML-Dateien, die als Grundlage für die Anpassung dienen. Zum Kopieren dieser Vorlagen wechseln Sie auf dem Puppeteer in das Verzeichnis zur Konfiguration von solcher Anpassungen:

```
cd /etc/logodidact/hiera/custom.d/
```

Prüfen Sie, ob es dort evtl. bereits eine `nextcloud-g1.yaml` oder `collabora-g1.yaml` gibt und falls nicht kopieren Sie die Vorlagen von dort:

```
cd /usr/share/doc/ld-puppet10/templates/cloud/with_collabora/custom.d/
```

```
cp * /etc/logodidact/hiera/custom.d/
```

Passen Sie die beiden Dateien an, wobei die Anpassungen im Wesentlichen wieder darin besteht, den Hostnamen an Ihre Umgebung anzupassen, was bei der `collabora-g1.yaml` wie folgt aussieht:

```
---
ld_collabora::config::allowed_hosts:
  - nextcloud.SCHULKUERZEL.logoip.de
```

und bei der `nextcloud-g1.yaml` so:

```
---
ld_nextcloud::config::app:
  richdocuments.wopi_url:
    value: 'https://collabora.SCHULKUERZEL.logoip.de'

ld_nextcloud::config::system:
  trusted_domains:
    - nextcloud.SCHULKUERZEL.logoip.de
```

Auch diese Anpassungen müssen wieder ins Versionierungssystem git übertragen werden:

```
cd /etc/logodidact
```

```
git add .
```

```
git commit -m "Anpassungen für nextcloud und collabora"
```

III.10.4. Nextcloud im Rev-Proxy eintragen

Um auf die Nextcloud von überall aus per Browser zuzugreifen, kann der Dienst von außen über den Reverse-Proxy im Internet erreichbar gemacht werden. Wechseln Sie dazu in den Puppeteer:

```
lxc-ssh -n puppeteer
```

Wechseln Sie in das Verzeichnis zur Konfiguration des Reverse-Proxy:

```
cd /etc/logodidact/hosts/rev-proxy
```

Ergänzen Sie die Datei `revproxy.conf` mit folgendem Inhalt für Nextcloud und Collabora. Das Schulkürzel entspricht dabei in der Regel wieder dem zuvor festgelegten Domänennamen, d.h., in unserer beispielhaften Umgebung `musterstadt-gym`. Wenngleich Collabora nicht über kein eigenes Webinterface verfügt, ist der Eintrag zwingend erforderlich!

```
[ReverseProxy nextcloud.SCHULKUERZEL.logoip.de]
Url https://nextcloud
```

```
[ReverseProxy collabora.musterstadt-gym.logoip.de]
Url https://collabora
```

Pflegen Sie die Änderungen wie gewohnt ins git ein:

```
cd /etc/logodidact
```

```
git add .
```

```
git commit -m "Konfiguration nextcloud und collabora im rev-proxy".
```

Führen Sie danach ein `ldupdate` im Puppeteer durch gefolgt von einem `prun`. Führen Sie danach einen Neustart von nginx durch: `/etc/init.d/nginx restart`.

III.10.5. Zertifikate für Nextcloud und Collabora beantragen

Damit der Zugriff auf die Dienste von außen keine Fehlermeldungen auf eine vermeintlich unsichere Seite zurückgibt, sollten entsprechende Zertifikate beantragt werden.

Wechseln Sie in den Container `Puppeteer` und prüfen Sie zunächst, ob Sie dort über den Befehl `sle` in die Umgebung zur Verwaltung der Zertifikate kommen. Stellen Sie dies gegebenenfalls um, wie in Abschnitt III.3.6.3.1, „Umstellung auf das Tool `acme.sh`“ beschrieben.

Starten Sie dann in die Umgebung zur Verwaltung der Let's Encrypt Zertifikate und beantragen diese für die beiden Dienste:

```
sle
```

```
issue nextcloud.SCHULKUERZEL.logoip.de
```

```
issue collabora.SCHULKUERZEL.logoip.de
```

Wenn die Zertifikate erstellt und heruntergeladen wurden, landen sie über Puppet irgendwann im Container `rev-proxy` im Ordner `/etc/nginx/ssl`. Das Ganze lässt sich ggf. wieder über einen `prun` im `puppeteer` und danach im `rev-proxy` beschleunigen. Ausführliche Infos zu Let's Encrypt finden Sie in Abschnitt III.3.6, „Zertifikate mit Let's Encrypt“.

Nachdem die Zertifikate eingespielt sind, ist der sichere Zugriff von außen möglich über:

```
https://nextcloud.SCHULKUERZEL.logoip.de
```



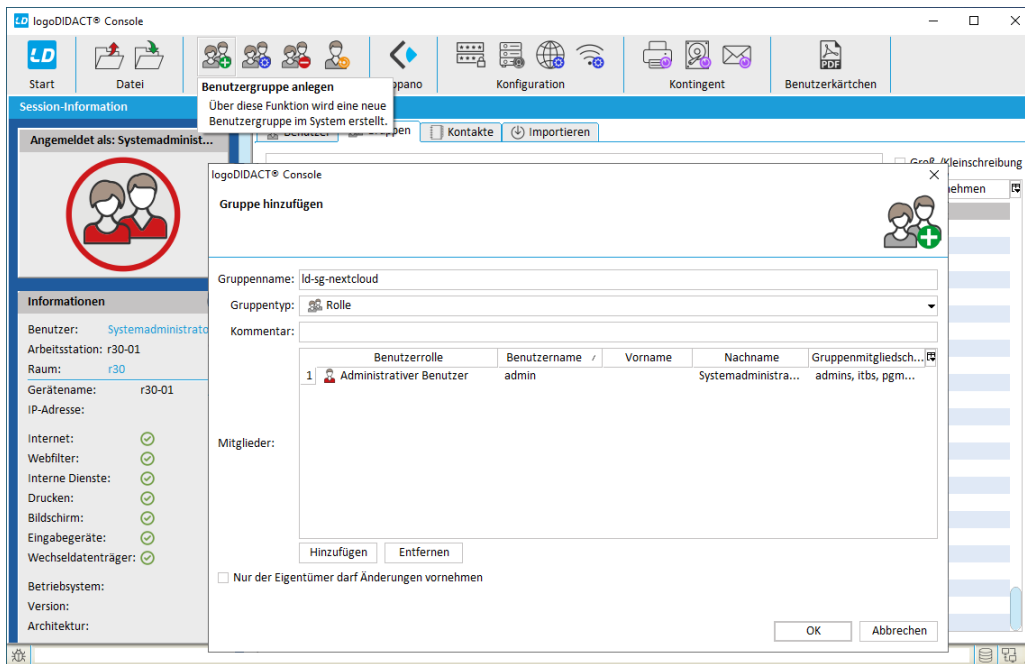

Bevor man sich dort anmelden kann, muss aber dieses Recht den Benutzern zunächst erteilt werden.

III.10.6. Zugriff auf Nextcloud erlauben

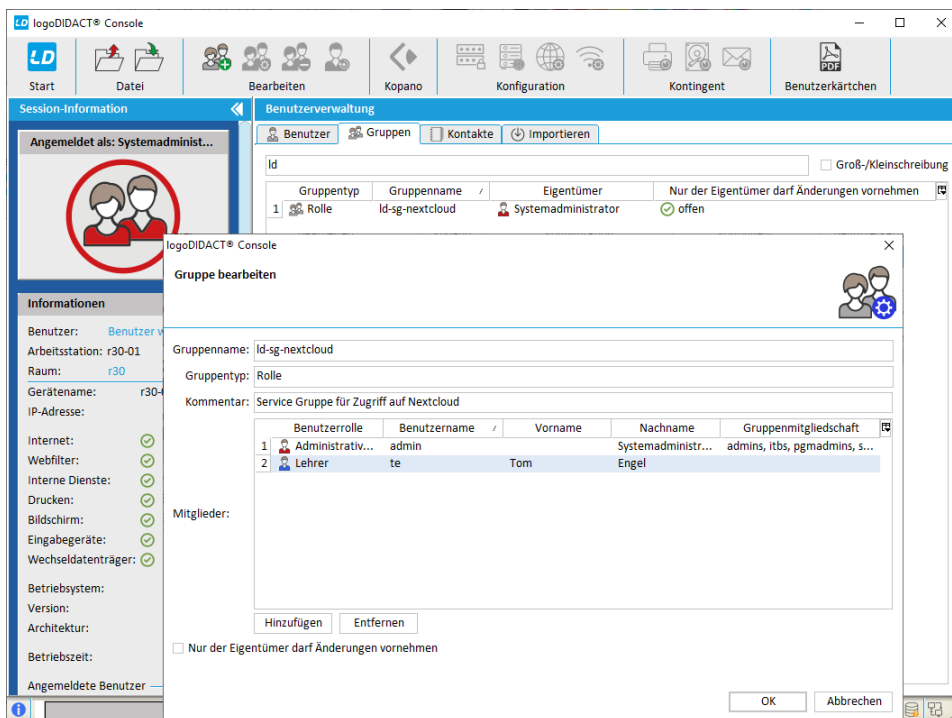
Um Benutzern den Zugriff auf die Nextcloud zu ermöglichen, muss in der LogoDIDACT-Console zunächst die Rolle **ld-sg-nextcloud** ("sg" steht für "service group") erstellt werden. Melden Sie sich dazu mit dem Konto des Benutzers **admin** an und wechseln Sie in das Modul der Benutzerverwaltung.

Wählen Sie das entsprechende mit einem grünen + versehene Benutzer-Symbol **Benutzergruppe anlegen** in der oberen Menüleiste. Wählen Sie als **Gruppentyp** den Eintrag **Rolle** und als **Gruppenname** **ld-sg-nextcloud**. Wie gewohnt, können Sie über das Häkchen **Nur der Eigentümer darf Änderungen vornehmen** regeln, ob auch Kolleginnen und Kollegen sich selbst oder Schülern der Zugriff auf Nextcloud gewähren oder entziehen können.

Um die neue Servicegruppe zu erstellen, klicken Sie auf **OK**.



Ebenfalls wie gewohnt, können Sie anschließend über Doppelklick auf die neu erstellte Servicegruppe **ld-sg-nextcloud** die Gruppe um weitere Mitglieder über die Schaltfläche **Hinzufügen** ergänzen.



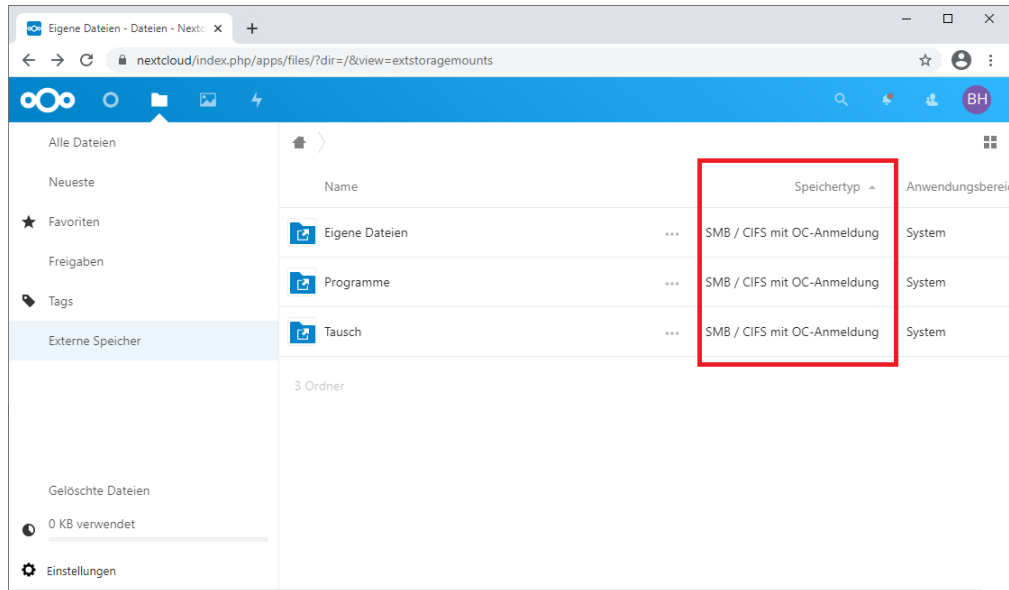
III.10.7. Änderung des Objektspeichers

Grundsätzlich lässt sich in Nextcloud der primäre Speicherbereich auf alle möglichen internen und externen Systeme anpassen. Infos dazu finden sich in der Doku zu Nextcloud: https://docs.nextcloud.com/server/latest/admin_manual/configuration_files/primary_storage.html

III.10.7.1. Ankopplung an Samba4

In LogoDIDACT wird per Standard eine Ankopplung an Samba4 per SMB/CIFS als Objektspeicher konfiguriert. Somit werden die intern an der Schule vorhandenen Freigaben (Samba Shares) so in Nextcloud abgebildet, dass den Anwendern eine relativ einfache Zuordnung möglich ist. Alles was lokal im Laufwerk H:\ lag bzw. liegt, findet sich in Nextcloud unter **Eigene Dateien**.

Entsprechendes gilt für das Laufwerk T:\ mit der Freigabe **Tausch** und P:\ mit der Freigabe **Programme**.



Eine solche Ankopplung ist zunächst für die Anwender sehr einfach, kann aber auch gravierende Nachteile haben. Webbasierte Dateizugriffe sind in der Regel nicht so performant und problemlos, wie man dies vom jeweiligen Betriebssystem her kennt.

Alle Zugriffe auf SMB sind über `http://` und weitere Protokolle und Subsysteme gekapselt.

Um in diesem Bereich die Komplexität durch Einbindung der Netzlaufwerke zu reduzieren, besteht die Möglichkeit auf die Nextcloud interne Speicherstruktur umzustellen und auf die Einbindung von Shares zu verzichten.

III.10.7.2. Umstellung auf Nextcloud files

In dieser Variante wird der Nextcloud interne Speicher verwendet und keine externen Shares. Diese Variante ist vor allem dann sinnvoll, wenn der LogoDIDACT-Server in der Cloud betrieben wird und es gar keinen klassischen direkten Zugriff von Clients auf die Shares über die Netzlaufwerke gibt.

III.10.7.2.1. Konfiguration auf lokalen Speicher

Um den Speicherort auf `nextcloud-files` umzustellen, wechseln Sie in den Puppeteer.

```
lxc-ssh -n puppeteer
```

Wechseln Sie in das Verzeichnis zur Konfiguration von Features und sofern noch nicht vorhanden, erstellen Sie einen Ordner für Nextcloud und wechseln in diesen Ordner:

```
cd /etc/logodidact/feature.d
```

```
mkdir nextcloud
```

```
cd nextcloud
```

Erstellen Sie in diesem Ordner die Datei `storage.yaml` mit folgendem Inhalt:

```
---  
storage: local
```

Pflegen Sie die Änderungen wie gewohnt ins git ein:

```
cd /etc/logodidact
```

```
git add .
```

```
git commit -m "Storage umgestellt auf Nextcloud interne files".
```

Führen Sie danach gezielte `pruns` im Container `nextcloud-g1` durch, bis die Umstellung greift.



Achtung

Per Standard wird Nextcloud in LogoDIDACT für die Verwendung von shares in Samba per SMB/CIFS als Objektspeicher konfiguriert.

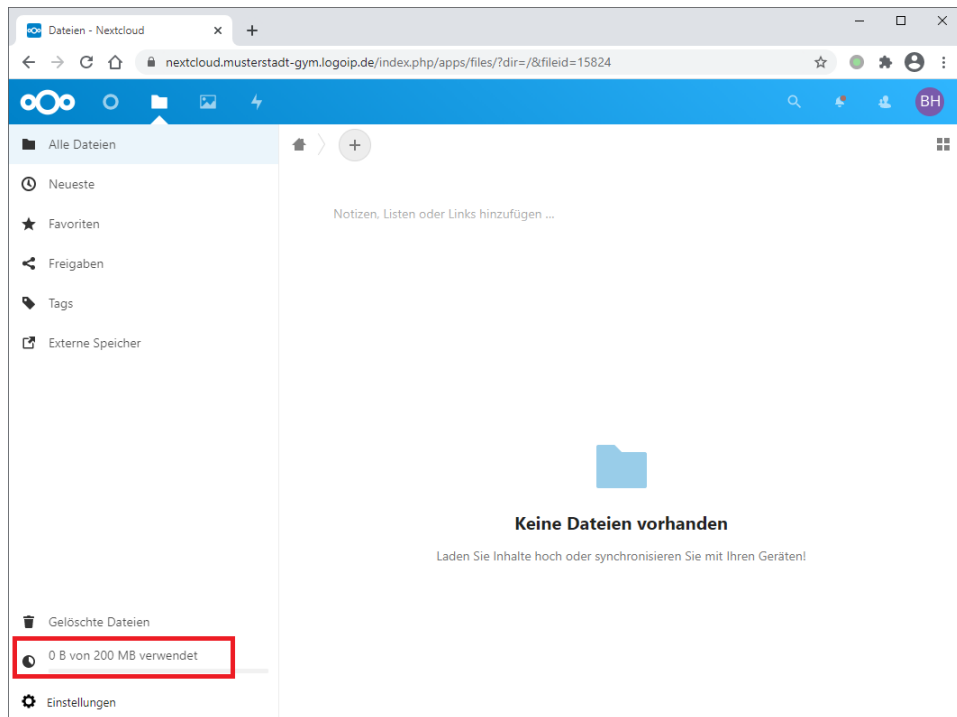
Damit man auf den lokalen Speicher innerhalb von Nextcloud nicht zugreifen kann, wird dafür die Quota auf 0 Bytes gesetzt.

Unmittelbar nach einer Umstellung wird man deshalb in Nextcloud die Meldung erhalten, dass man keine Berechtigung hat, dort Dateien anzulegen, weil die Quota noch nicht angepasst wurde.

Die Prüfung und ggf. Anpassung der Quota wird alle 4 Stunden über einen Timer in systemd durchgeführt. Wenn man dies beschleunigen möchte, lässt sich das Skript im Container `nextcloud-g1` über folgenden Befehl starten:

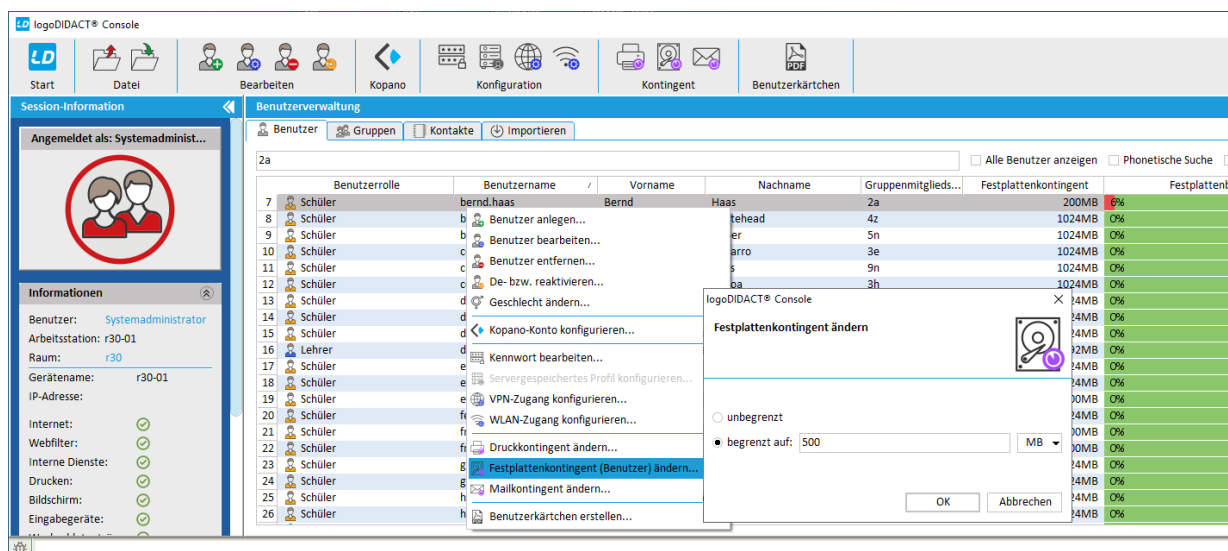
```
sudo -u www-data /opt/puppet-cm/bin/ld-nextcloud-reset-quota
```

Nachdem der Speicherpunkt auf Nextcloud interne files geändert wurde, sind keine Shares mehr zu sehen. Der zur Verfügung stehende Speicherplatz beträgt für jeden Benutzer 200 MB, was links unten in nachstehender Grafik erkennbar ist.



III.10.7.2.2. Anpassung der Quota für lokalen Speicher

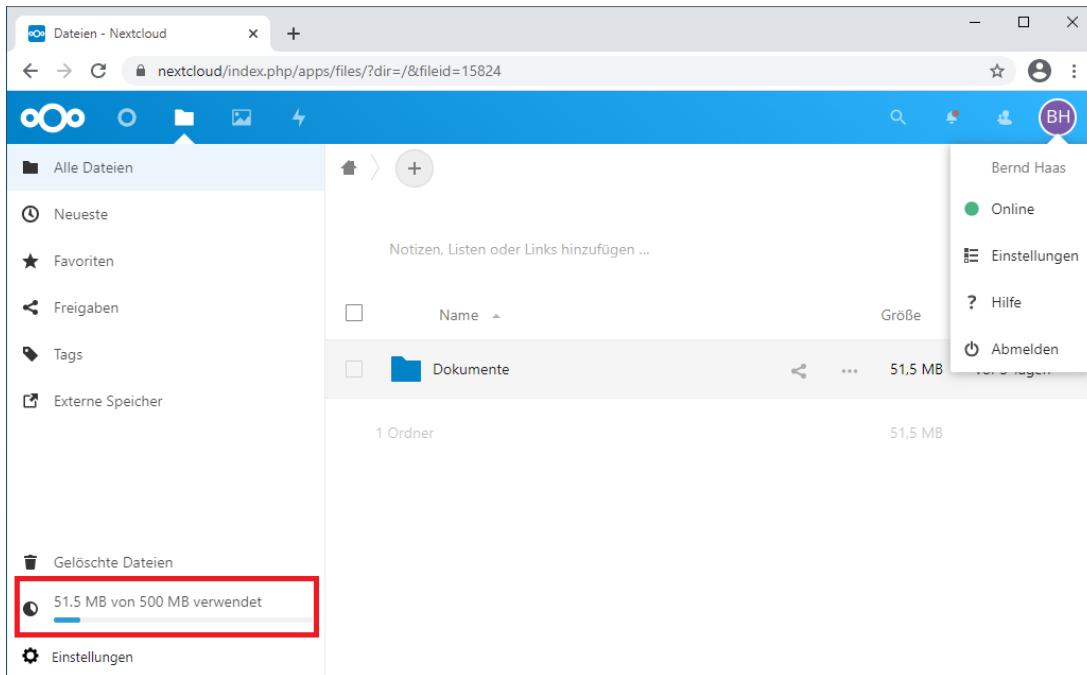
Der Speicherplatz von 200 MB für den oben aufgeführten Benutzer wird aus den Benutzereinstellungen heraus gelesen und gilt wie bei den klassischen Netzwerklaufwerken auch für **nextcloud-files**. Die Anpassung dieser Quota erfolgt damit analog über die LogoDIDACT-Console, wie in der folgenden Abbildung exemplarisch für den Schüler **bernd haas** dargestellt.



Damit diese Anpassung der Quota nicht erst in 4 Stunden wirksam wird, kann das dafür notwendige Skript im Container **nextcloud-g1** auch manuell aufgerufen werden:

```
sudo -u www-data /opt/puppet-cm/bin/ld-nextcloud-reset-quota
```

Danach ist die erhöhte Quota dann auch im Nextcloud internen Speicher sofort gesetzt und auf Benutzerebene sichtbar.



en Sie danach gezielte **pruns** im Container **nextcloud-g1** durch, bis die Umstellung greift.

III.10.8. Deaktivierung von Plugins

Viele Probleme in Nextcloud können daraus resultieren, dass es unzählige Erweiterungen in Form von Plugins gibt, über die sich die Nextcloud "in die Breite" entwickeln lässt. Abgesehen davon, dass diese Erweiterungen häufig nicht ausgereift sind, leidet darunter in der Regel die Performance und Stabilität.

Deshalb ist es dringend anzuraten, diese "Spielwiese" abzuschalten und die Installation von Plugins zu unterbinden. Wer eine Spielwiese haben möchte, kann sich dazu in der Cloud einen Server buchen und die Nextcloud dort in einer beliebigen Konfiguration betreiben.

Wechseln Sie im Puppeteer in das Verzeichnis zur Konfiguration von Features und sofern noch nicht vorhanden, erstellen Sie einen Ordner für Nextcloud und wechseln in diesen Ordner:

```
cd /etc/logodidact/feature.d
```

```
cd nextcloud
```

Erstellen Sie in diesem Ordner die Datei `appstore.yaml` mit folgendem Inhalt:

```
---  
appstore: locked
```

Pflegen Sie die Änderungen wie gewohnt ins git ein:

```
cd /etc/logodidact
```

```
git add .
```

```
git commit -m "Installation von APPs / Plugins in nextcloud deaktivieren".
```

Führen Sie danach gezielte **pruns** im Container **nextcloud-g1** durch, bis die Umstellung greift.

III.10.9. Update von Nextcloud über mehrere Versionen

Innerhalb einer Version lässt sich Nextcloud über ein **ldupdate** und das Konfigurations-Management mit Puppet problemlos aktualisieren. Gleiches gilt für ein Release-Wechsel auf die unmittelbar nächst höhere Version.



Achtung

Ein Update über mehr als eine Version wird von Nextcloud selbst nicht unterstützt und ist deshalb auch per **ldupdate** nicht möglich!

Wenn Sie beispielsweise auf einem LogoDIDACT-Server eine Nextcloud in der Version 18 betreiben und sehr lange keine Updates eingespielt haben, bricht das Update ab, wenn sie versuchen auf die Version 20 zu aktualisieren.

Das ist kein Fehler von LogoDIDACT, sondern eine Einschränkung in Nextcloud!

Wenn man im Container **nextcloud-g1** das Skript zur Aktualisierung ausführt, sieht man an der Ausgabe, dass ein solches Upgrade über 2 Versionen hinweg nicht unterstützt wird.

```
root@nextcloud-g1:/usr/sbin/ld-nextcloud-upgrade
```

```
Nextcloud or one of the apps require upgrade - only a limited number
of commands are available
You may use your browser or the occ upgrade command to do the upgrade
...
Exception: Updates between multiple major versions and downgrades
are unsupported.
Update failed
Maintenance mode is kept active
Resetting log level
```

Lösen lässt sich die Situation, indem zunächst das Update auf die nächst höhere Version der Nextcloud eingespielt wird, also im obigen Beispiel die Version 19. Welche Pakete installiert sind, lässt sich über den folgenden Befehl prüfen:

```
dpkg -l ld-*
```

In `/var/log/dpkg.log` ist zu sehen, von welcher Version auf welche neuere Version die Pakete aktualisiert wurden. Über den folgenden Befehl sieht man alle verfügbaren Paketversionen, die aus den Repositories heruntergeladen werden können:

```
apt-cache madison [paketname]
```

Im Falle von Nextcloud, sieht das dann in etwa so aus:

Konfiguration der Nextcloud für OnlyOffice anstelle Collabora

```
root@nextcloud-g1: /var/log
musterstadt-gym / lxc@ldhost / 17:02 / 1.3.22-12 / ssh@172.28.28.2
root@nextcloud-g1:/var/log # apt-cache madison ld-nextcloud
ld-nextcloud | 20.0.7 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
ld-nextcloud | 20.0.5 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
ld-nextcloud | 19.0.4-1 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
ld-nextcloud | 19.0.4 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
ld-nextcloud | 19.0.3+1 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
ld-nextcloud | 18.0.3-4 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
ld-nextcloud | 18.0.3-2 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
ld-nextcloud | 18.0.3-1 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
ld-nextcloud | 18.0.2-8 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
ld-nextcloud | 18.0.2-7 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
ld-nextcloud | 18.0.2-6 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
ld-nextcloud | 17.0.0-1 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
ld-nextcloud | 16.0.4-1 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
ld-nextcloud | 16.0.1-1 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
ld-nextcloud | 15.0.7-1 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
ld-nextcloud | 15.0.5-1 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
ld-nextcloud | 15.0.4-1 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
ld-nextcloud | 15.0.2-1 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
ld-nextcloud | 15.0.1-1 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
ld-nextcloud | 15.0.0-1 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
ld-nextcloud | 14.0.4-1 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
ld-nextcloud | 14.0.3-1 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
ld-nextcloud | 13.0.1-5 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
ld-nextcloud | 13.0.1-2 | http://packages.logodidact.com/lid=rjap-t5bm-zmgb/xenial-logodidact | xenial/main | amd64 | Packages
```

Um die Pakete der neuesten Version 19 einzuspielen, lautet der Befehl wie folgt:

```
apt install ld-nextcloud=19.0.4-1
```

Danach lässt sich die Aktualisierung per **lupdate** auf die nächst höhere Version 20 durchführen.

III.10.10. Konfiguration der Nextcloud für OnlyOffice anstelle Collabora

Per Standard wird für das gemeinsame Bearbeiten von Dokumenten in LogoDIDACT die OpenSource-Software Collabora des gleichnamigen Herstellers verwendet, der auch die Entwicklung der Software LibreOffice vorantreibt.

Die Dokumentenmanagement-Software Collabora ist damit auf die Verwendung des Office-Paketes LibreOffice und der dort genutzten Dokumente bzw. Formate optimiert. Dies ist sicherlich einer der wesentlichen Unterscheidungsmerkmale zu OnlyOffice, welches auf die Verwendung der Microsoft Office Dokumentformate optimiert ist.



Achtung

Voraussetzung für die Verwendung von OnlyOffice ist, dass Sie dieses Modul selbst in der Cloud hosten oder auf eine gehostete kostenpflichtige Lösung zugreifen.

Auf den folgenden Seiten wird beschrieben, wie **nextcloud** so konfiguriert wird, dass es als Dokumentenmanagement ein extern gehostetes **OnlyOffice** verwendet und nicht das lokal laufende **Collabora**.

Wechseln Sie dazu in den Puppeteer und dort in der Verzeichnis zur individuellen Konfiguration von Diensten:

```
lxc-ssh -n puppeteer
```

```
cd /etc/logodidact/hiera/custom.d
```


Editieren Sie in diesem Ordner die Datei `nextcloud-g1.yaml`, welche per Standard auf Collabora konfiguriert für unser Gymnasium Musterstadt in etwa folgendem Inhalt hat:

```
---
ld_nextcloud::config::app:
  richdocuments.wopi_url:
    value: 'https://collabora.musterstadt-gym.logoip.de'
  user_ldap.ldap_quota_def:
    value: '1GB'

ld_nextcloud::config::system:
  trusted_domains:
    - nextcloud.musterstadt-gym.logoip.de
```

Passen Sie die Konfiguration wie folgt an und ersetzen Sie dabei SCHULKUERZEL durch den individuellen festgelegten Namen.



Achtung

Setzen Sie sich mit dem Dienstleister in Verbindung, der OnlyOffice hostet, um die beiden anderen Parameter für den Betrieb in Erfahrung zu bringen und in der `nextcloud-g1.yaml` eintragen zu können.

Sie benötigen:

- die Adresse für den ONLYOFFICE-SERVER
- das SECRET, bzw. Kennwort, um eine abgesicherte Verbindung herzustellen

Bitte beachten Sie dabei unbedingt das Format von YAML-Dateien, in dem Einrückungen durch Leerzeichen eine maßgebliche Rolle spielen.

Um Fehler durch falsche Einrückungen oder Copy und Paste-Probleme zu vermeiden, sollten Sie die Vorlage-Datei über folgenden Befehl herunterladen und als Basis für ihre `nextcloud-g1.yaml` verwenden:

wget <https://files.sbe.de/logoDIDACT/nextcloud-g1.template>>

```
---
ld_nextcloud::app:
  richdocuments:
    ensure: absent
  onlyoffice:
    ensure: present

ld_nextcloud::config::app:
  richdocuments.wopi_url:
    ensure: absent
  app: richdocuments
  key: wopi_url
  user_ldap.ldap_quota_def:
    value: '1GB'
  onlyoffice.DocumentServerUrl:
```

```
    app: onlyoffice
    key: DocumentServerUrl
    value: 'https://ONLYOFFICE-SERVER.de'
onlyoffice.jwt_secret:
  app: onlyoffice
  key: jwt_secret
  value: 'SECRET'
onlyoffice.customizationToolbarNoTabs:
  app: onlyoffice
  key: customizationToolbarNoTabs
  value: 'false'
onlyoffice.sameTab:
  app: onlyoffice
  key: sameTab
  value: 'true'
onlyoffice.defFormats:
  app: onlyoffice
  key: defFormats
  value: '{"csv":"false","doc":"true","docm":"false","docx":"true",↵
"dotx":"false","epub":"false","html":"false","odp":"true","ods":"true",↵
"odt":"true","otp":"false","ots":"false","ott":"false","pdf":"false",↵
"potm":"false","potx":"false","ppsm":"false","ppsx":"false","ppt":"true",↵
"pptm":"false","pptx":"true","rtf":"true","txt":"false","xls":"true",↵
"xlsm":"false","xlsx":"true","xltm":"false","xltx":"false"}'
```

```
ld_nextcloud::config::system:
  trusted_domains:
    value:
      - "cloud.SCHULKUERZEL.logoip.de"
      - "nextcloud.SCHULKUERZEL.logoip.de"
      - "nextcloud-g1.SCHULKUERZEL.logoip.de"
  onlyoffice:
    jwt_header: "AuthorizationJWT"
    appstoreurl: "https://apps.nextcloud.com/api/v1"
```

Pflegen Sie die Änderungen wie gewohnt ins git ein:

```
cd /etc/logodidact
```

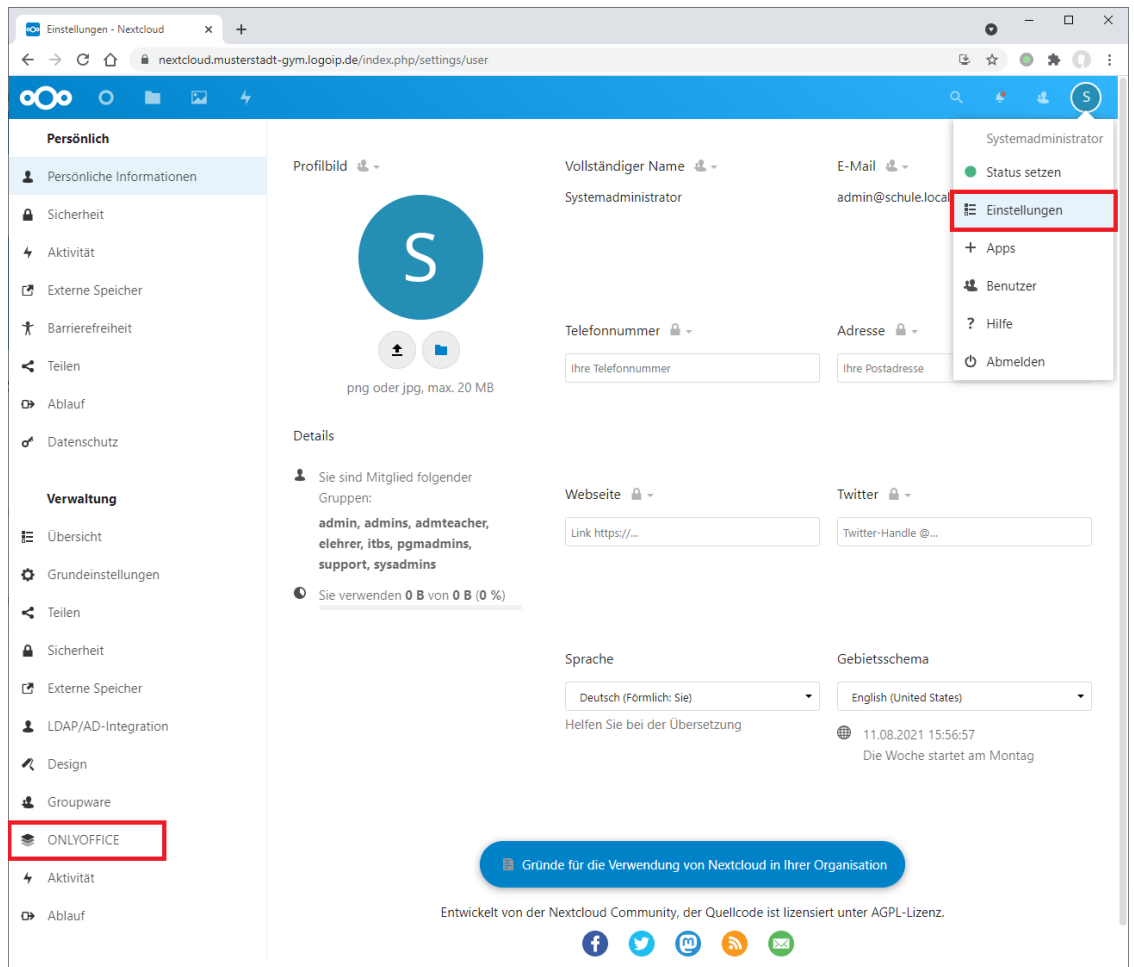
```
git add .
```

```
git commit -m "Konfiguration der Nextcloud für die Verwendung von  
OnlyOffice".
```

Führen Sie danach mindestens zwei gezielte **pruns** im Container **nextcloud-g1** durch, bis die Umstellung greift.

Melden Sie sich im nächsten Schritt über das Webinterface von Nextcloud mit den Zugangsdaten des Benutzers **admin** an. Wechseln Sie danach über das Benutzer-Symbol rechts oben auf den Menüeintrag **Einstellungen**. Sofern das Plugin über die zuvor erwähnten **pruns** installiert wurde, erscheint im Menü auf der linken Seite der Eintrag **ONLYOFFICE**.

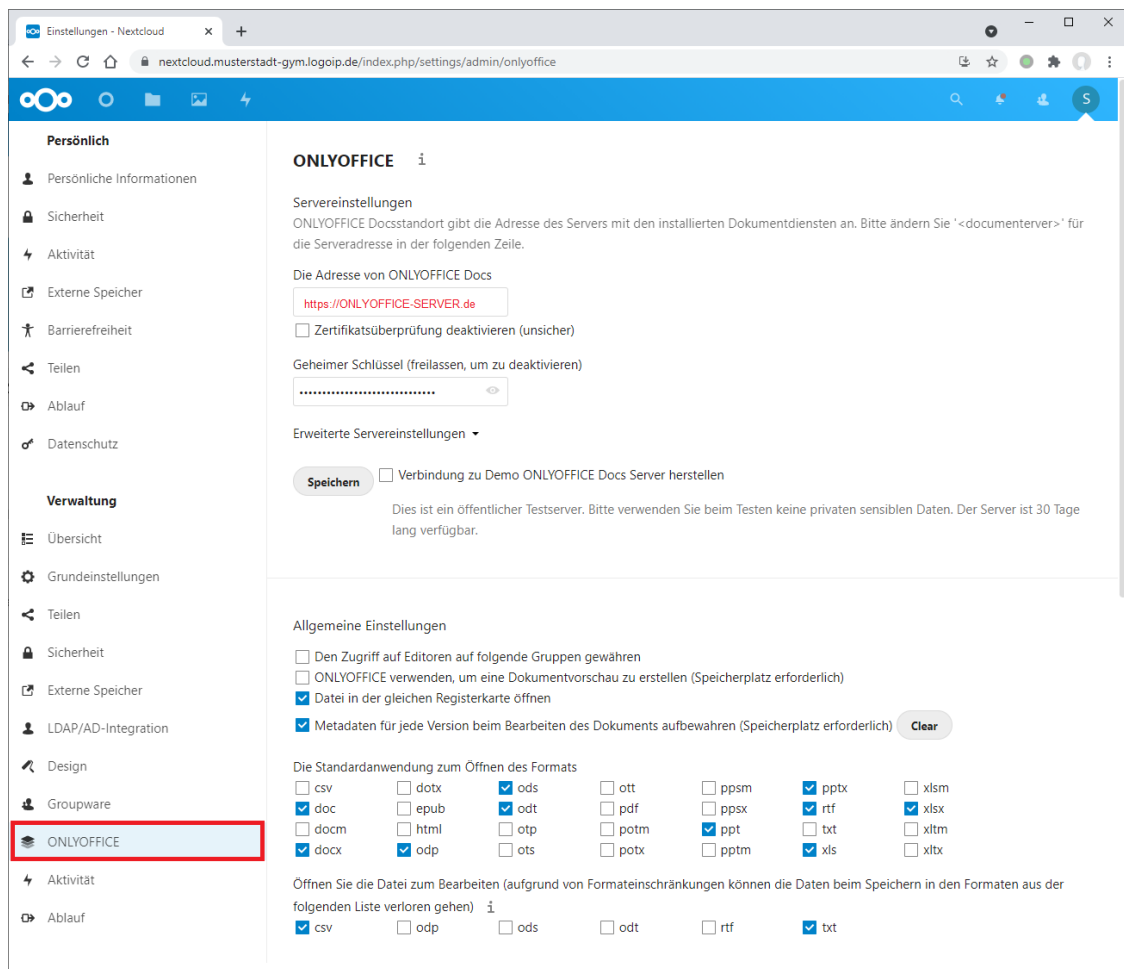
Konfiguration der Nextcloud für OnlyOffice anstelle Collabora



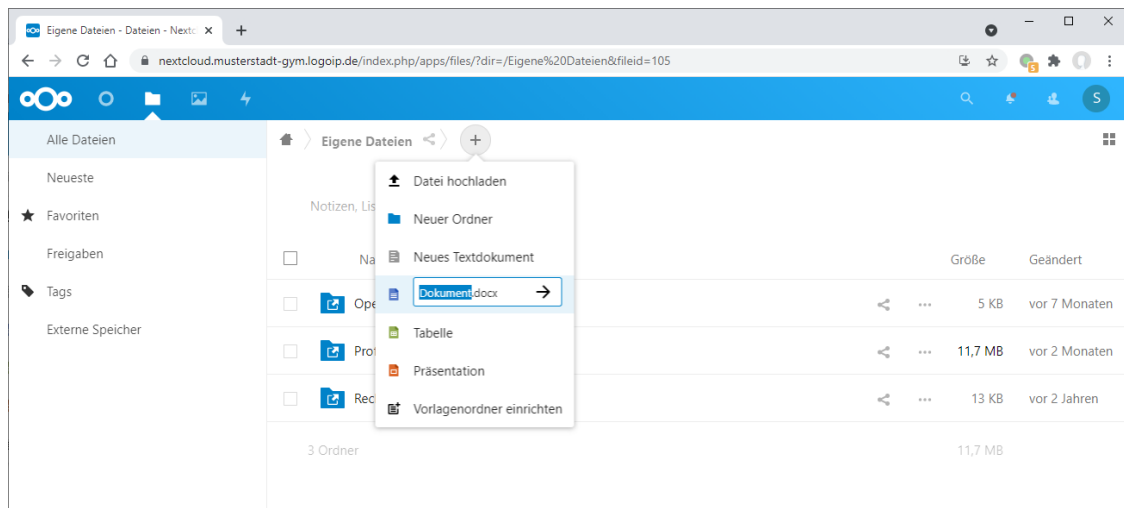
The screenshot shows the Nextcloud user settings interface. The left sidebar is divided into 'Persönlich' and 'Verwaltung'. Under 'Verwaltung', the 'ONLYOFFICE' option is highlighted with a red box. In the top right corner, the user menu is open, and the 'Einstellungen' option is also highlighted with a red box. The main content area displays user profile information, including a profile picture, full name (Systemadministrator), email (admin@schule.local), and various settings like language (Deutsch) and region (English).

Wenn Sie auf diesen Eintrag klicken, sehen Sie die in Puppet gemachten Einstellungen und können daraus ableiten, wie Sie die Formate und Standardanwendung entsprechend Ihren Vorstellungen anpassen können.

Konfiguration der Nextcloud für OnlyOffice anstelle Collabora



Im Anschluss können Sie über das Ordnersymbol in Ihren Eigenen Dateien ein Dokument im jeweiligen Format erstellen.



Kapitel III.11. Kopano

Bei Kopano handelt es sich um eine Groupware, die optimal in LogoDIDACT integriert ist.



Achtung

Die Lizenzierung von Kopano erfolgt über das Modell der User Subscription. Bitte wenden Sie sich bei Fragen an Ihren zuständigen LogoDIDACT-Partner.

III.11.1. Voraussetzungen

Um eine Mail-Kommunikation zu ermöglichen, müssen die folgenden Voraussetzungen gegeben sein:

- vorhandene Domäne bei einem Internetprovider (z.B. meineschule.de)
- für die Domäne muss es möglich sein, so genannte DNS MX-Records zu konfigurieren. Hierdurch wird festgelegt, an welchem Server E-Mails für die Domäne eingeliefert werden.
- ein externes Mail-Relay, das den Empfang und Versand der Mails gewährleistet und auch über einen Spam-Schutz verfügt (z.B. im Internet gehostetes Proxmox Mail Gateway)

Installation, Konfiguration und Betrieb dieser beiden Komponenten sind nicht Gegenstand dieser Dokumentation. Bitte wenden Sie sich an einen erfahrenen LogoDIDACT-Partner, der hierfür Lösungen bereitstellt.

III.11.2. Installation der Datenbank MariaDB 10.3

Eine weitere Voraussetzung aber eher konkreter Bestandteil von **Kopano** ist eine SQL-Datenbank in einem eigenen Container. Dieser Container **mariadb103** muss zwingend vor dem Container **kopano-g1** aktiviert und installiert werden.

Für eine aktuelle Neuinstallation mit **Kopano** ist es verbindlich, dass als Datenbank **mariadb103** zum Einsatz kommt. Falls Kopano bereits zum Einsatz kommt aber noch auf einer anderen Datenbank läuft, muss eine Migration erfolgen.

Sowohl für eine Neuinstallationen als auch eine Datenbankumstellung, muss zunächst der Container **mariadb103** aktiviert werden.

Wechseln Sie in den Puppeteer:

```
lxc-ssh -n puppeteer
```

Wechseln Sie in das Verzeichnis zur Konfiguration von Containern:

```
cd /etc/logodidact/hosts/ldhost
```

Öffnen Sie die Datei `guest.conf` mit einem Editor Ihrer Wahl, wie z.B. Nano:

```
nano guest.conf
```

Fügen Sie dort den Eintrag für den Datenbank-Container hinzu.

```
[Guest mariadb103]
```

Ensure running

Durch Eingabe der Tastenkombination <Strg>+<X> verlassen Sie den Editor Nano und geben „Y“ ein, damit die Änderung gespeichert wird. Wechseln Sie dann ins Stammverzeichnis der Konfiguration und übertragen Sie anschließend die Änderungen ins Versionierungssystem git:

```
cd /etc/logodidact
```

```
git add .
```

```
git commit -m "Aktivierung MariaDB 10.3 für Kopano"
```

Durch das Übertragen ins git-Repository wird auch automatisch `map_translate` aufgerufen, so dass die Konfigurationen in YAML übersetzt und von Puppet verarbeitet werden können.

Wie bereits beim Aufbau anderer Container mehrfach beschrieben, veranlasst ein `prun` im Host den Agent dazu, mit dem Aufbau des Containers `mariadb103` zu beginnen. Beobachten können Sie das Ganze wieder mit `pstat` im Puppeteer. Nach einer Weile wird sich dort der Container auftauchen. Sofern der Container grundlegend aufgebaut ist und läuft, kann man in einer neuen Sitzung per `lxc-attach -n mariadb103` dort hineinwechseln und sofern gerade kein `prun` läuft einen solchen neuen Durchlauf mit `prun` starten.

In der Regel sind mehrere dieser Durchläufe notwendig, bis der Container vollständig aufgebaut ist. Mit jedem `prun` im Container `mariadb103` nähert sich der Wert in der Spalte Successes einem Endwert, der nicht Null sein muss.

Führen Sie zum Abschluss nochmals gezielt einen `prun` im Container `ca-g1` durch, so dass die Zertifikate für den Container `mariadb103` erstellt werden. Ein letzter `prun` im Container `mariadb103` holt sich diese und installiert sie.

III.11.3. Prüfung der Verzeichnisstruktur

Im Rahmen der Installation und Konfiguration von `Kopano` sind Anpassungen notwendig, die per Puppet vorgenommen werden.



Achtung

Prüfen Sie im Container `puppeteer` über das nachfolgende Skript, ob die Verzeichnisstruktur zur Ablage von benutzerdefinierten YAML-Dateien korrekt ist.

Konkret muss der Ordner `custom.d` ein so genannter Symlink sein.

Das folgende Skript können Sie komplett in eine Shell kopieren und mit der Eingabetaste bestätigen:

```
if [ -h "/var/lib/ld-puppet/hiera.d/custom.d" ]; then
  echo "custom.d Ordner ist Symlink, alles in Ordnung."
else
  echo "Fehlerhafte Umgebung, bitte custom.d Ordner manuell korrigieren."
  # rmdir /var/lib/ld-puppet/hiera.d/custom.d
  # ln -s /etc/logodidact/hiera/custom.d /var/lib/ld-puppet/hiera.d/custom.d
fi
```

Falls bei diesem Kommando ein Fehler ausgegeben wird, muss zur Korrektur ein Symlink angelegt werden, so wie in den auskommentierten Zeilen des Skriptes beschrieben.

Sofern der Ordner ein Symlink ist, lässt sich über `ls -l` prüfen, wohin der symbolische Link für den Ordner `custom.d` zeigt:

```
root@puppeteer: /var/lib/ld-puppet/hiera.d
musterstadt-gym / lxc@idhost / 17:31 / 1.4.1-1 / ssh@172.28.28.2
root@puppeteer:/var/lib/ld-puppet/hiera.d # ls -l custom.d
lrwxrwxrwx 1 root root 30 May  5 2018 custom.d -> /etc/logodidact/hiera/custom.d
```

III.11.4. Festlegung von MariaDB 10.3 als Datenbank

Sowohl für eine Neuinstallation als auch eine Umstellung von MySQL auf die neue Datenbank, muss im System festgelegt werden, dass Maria DB verwendet wird.

Erstellen Sie dazu im Container **Puppeteer** im Pfad `/etc/logodidact/hiera/custom.d` die Datei `kopano-g1.yaml` mit folgendem Inhalt und dem Verweis auf die MariaDB als Datenspeicher:

```
---
ld_kopano::db_server: mariadb103
```

III.11.5. Datenbank-Migration auf MariaDB 10.3

Bei einer Neuinstallation von **Kopano** überspringen Sie diesen Abschnitt!

Wenn Sie **Kopano** schon länger einsetzen, sollte eine Migration der Datenbank von **mysql56** auf **mariadb103** erfolgen.

III.11.5.1. Voraussetzungen

Wie in den vorherigen Abschnitten erwähnt, gibt es einige Voraussetzungen, die sowohl für eine Kopano-Neuinstallation als auch eine Umstellung der Datenbank gelten:

- Aktualisierung des Servers auf Puppet-Rezeptstand 1.5.0
- Aktivierung und kompletter Aufbau des Containers **mariadb103**
- Prüfung der Verzeichnisstruktur (Symlink)
- Festlegung von **mariadb103** als Datenspeicher

Nachdem diese grundlegenden Voraussetzungen geschaffen wurden, muss vor einer Migration der Datenbank zusätzlich geprüft werden, wie groß diese ist und ob genügend freier Speicherplatz auf dem Server vorhanden ist.

III.11.5.2. Größe der Kopano-Datenbank und freien Speicherplatz prüfen

Je größer die Datenbank, desto länger dauert der Migrationsprozess. Bei großen Datenbanken muss ein Wartungs-Zeitfenster mit dem Kunden zur Durchführung vereinbart werden, in dem die Arbeiten erledigt werden können und Kopano temporär nicht zur Verfügung steht. Der freie Speicherplatz am Server sollte mindestens 3x so hoch liegen wie die Datenbankgröße von Kopano. Als Richtwert kann man mit einer Wartezeit von ca. 10 Minuten pro GB für die Migration der Datenbank rechnen.

Zum Abfragen der beiden Größen können folgende Kommandos im Container **kopano-g1** verwendet werden:

```
# Kopano SQL-Datenbanken
du -sch /var/lib/mysql/kopano*

# Freier Speicherplatz des Servers
df -h
```



Achtung

Sollte nicht genug freier Speicherplatz am Server zur Verfügung stehen, muss die Migration abgebrochen werden!

III.11.5.3. Kopano-Dienste anhalten

Bevor die Datenbank übernommen wird, müssen alle Kopano-Dienste sowie Puppet temporär gestoppt werden. Führen Sie dazu die folgenden Befehle nacheinander im Container **kopano-g1** durch:

```
prun
```

```
pdis
```

```
for svc in $(systemctl list-units --type=service --plain --all --no-pager --no-legend kopano* | awk '{ print $1 }'); do systemctl stop $svc done
```

```
systemctl is-enabled getmail.timer >/tmp/getmail-timer.status 2>&1
if grep -sqi enabled /tmp/getmail-timer.status; then systemctl disable --now getmail.timer fi
```

III.11.5.4. Datenbank erstellen lassen

Um automatisch eine neue Datenbank erstellen zu lassen, wechseln Sie in den Container **mariadb103** und geben den folgenden Befehl ein:

```
prun
```

III.11.5.5. Datenbank-Migration starten

Wechseln Sie im nächsten Schritt in den **ldhost** und führen Sie dort einen **prun** durch, um ggf. DNS-Einträge zu aktualisieren.

```
prun
```

Danach starten Sie die Migration über das Skript **mariadb-migrate** und die entsprechenden Parameter:

```
# Usage: mariadb-migrate [options]
# -c, --[no-]cleanup          Delete database dump after import (default: no)
# -d, --database=DATABASE    Database to be migrated
# -s, --source=CONTAINER     Source container from which the database is to be mi
# -t, --target=CONTAINER     Target container into which the database is to be mi
# -y, --assume-yes           Assume "yes" as answer to all prompts and run non-in
```



```
mariadb-migrate -c -d kopano -s mysql56 -t mariadb103 -y
```

```
mariadb-migrate -c -d kopano_state -s mysql56 -t mariadb103 -y
```

Wie oben bereits erwähnt, kann die Datenbankmigration entsprechend viel Zeit benötigen.

III.11.5.6. Kopano-Dienste wieder starten

Bei Erfolg der Datenbankübertragung können die Dienste im Container **kopano-g1** wieder gestartet werden.

```
pena
```

```
for svc in $(systemctl list-units --type=service --plain --all --no-pager --no-legend kopano* | awk '{ print $1 }'); do systemctl start $svc done
```

```
if grep -sqi enabled /tmp/getmail-timer.status; then systemctl disable --now getmail.timer fi
```

III.11.5.7. Alte Datenbanken im Container mysql56 löschen

Die übertragenen Datenbanken von Kopano können bei Erfolg am ursprünglichen Speicherort gelöscht werden. Dieser Schritt sollte erst nach einige Tage später durchgeführt werden, nachdem Kopano getestet wurde und sauber funktioniert!

```
mysql -h localhost -u root -e "DROP DATABASE kopano;"
mysql -h localhost -u root -e "DROP DATABASE kopano_state;"
```

```
# Zur Kontrolle: Auflistung der übrigen SQL-Datenbanken
```

```
mysql -h localhost -u root -e "SHOW DATABASES;"
```

```
# +-----+
# | Database          |
# +-----+
# | information_schema |
# | mysql              |
# | performance_schema |
# +-----+
```

```
# Wenn hier keine weiteren Datenbanken als die oberen 3 abgebildeten Einträge sind, kann der Datenbank-Container mysql56 komplett als LXC gelöscht werden
```

III.11.6. Installation Container Kopano

Voraussetzung für die Neuinstallation von **Kopano** ist der zuvor vollständig aufgebaute Container **mariadb103**, sowie die Datei **kopano-g1.yaml** mit dem entsprechenden Eintrag zur Verwendung der Datenbank.

Der Container **kopano-g1** selbst wird wieder auf die gleiche Weise aktiviert und konfiguriert, wie das bereits bei den Bausteinen zuvor gezeigt wurde.

Wechseln Sie in den Puppeteer:

```
lxc-ssh -n puppeteer
```

Wechseln Sie in das Verzeichnis zur Konfiguration von Containern:

```
cd /etc/logodidact/hosts
```

Öffnen Sie die Datei `guest.conf` mit einem Editor Ihrer Wahl, wie z.B. Nano:

```
nano guest.conf
```

Fügen Sie dort den Eintrag für Kopano hinzu.

```
[Guest kopano-g1]
Ensure running
```

Speichern Sie die Datei ab und übertragen Sie anschließend die Änderungen ins Versionierungssystem git:

```
cd /etc/logodidact
```

```
git add .
```

```
git commit -m "Aktivierung Groupware Kopano"
```

Wie auch zuvor beim Datenbank-Container beschrieben, veranlasst ein `prun` im Host den Agent dazu, mit dem Aufbau des Containers `kopano-g1` zu beginnen. Beobachten lässt sich das Ganze wieder mit `pstat` im Puppeteer. Nachdem der Container grundlegend aufgebaut ist, lässt sich per `lxc-attach -n kopano-g1` dort hineinwechseln und der Aufbau über `prun`s gezielt forcieren.

III.11.7. Kopano im Rev-Proxy freischalten

Wechseln Sie in den Puppeteer:

```
lxc-ssh -n puppeteer
```

Wechseln Sie in das Verzeichnis zur Konfiguration des Reverse-Proxy.



Achtung

Anstelle die Konfiguration in `.conf`-Dateien vorzunehmen, die dann über das Einchecken ins git-Repository in eine `.yaml`-Datei übersetzt wird, sollten Sie künftig alle Anpassungen direkt in der entsprechenden `.yaml`-Datei vornehmen.

Wechseln Sie also in das Verzeichnis, in dem spezifische Anpassungen direkt in der `rev-proxy.yaml` vorgenommen werden:

```
cd /var/lib/ld-puppet/hiera.d/custom.d
```

Öffnen Sie die Datei `rev-proxy.yaml` und ergänzen Sie diese mit einem Eintrag für Kopano:

```
---
ld_rproxy::hosts:
  "ldaps.SCHULKUERZEL.logoip.de":
    type: stream
```

```

template: ldap
ensure: present
"kopano.musterstadt-gym.logoip.de":
  proxy_url: https://kopano.schule.local
  template: kopano
  ensure: present
  listen_as_default: false

```

Das SCHULKUERZEL entspricht dabei dem individuell festgelegten Namen, in unserem obigen Beispiel "musterstadt-gym". Damit diese Änderung Damit die Änderung im Reverse-Proxy sofort wirksam wird, genügt ein Wechsel in den Container und ein Aufruf von **prun**.

III.11.8. Zertifikat für Kopano aktivieren

Bevor Sie das Zertifikat versuchen zu erstellen, prüfen Sie kurz die Verfügbarkeit der Zertifizierungsstelle. Gehen Sie dazu mit einem Webbrowser auf die Internetseite <https://letsencrypt.status.io/> und prüfen Sie, ob die Dienste dort verfügbar sind oder es eventuell Probleme gibt.



Achtung

Ab Puppet-Release 1.4.1-x steht für das Beantragen und Erneuern von Let's Encrypt Zertifikaten das modernere Tool **acme.sh** zur Verfügung.

Bitte beachten Sie, dass **acme.sh** nicht automatisch aktiviert wird, sondern Sie dies einmalig manuell umstellen und danach alle Zertifikate neu beantragen müssen.

Infos dazu finden Sie in Abschnitt III.3.6.3.1, „Umstellung auf das Tool acme.sh“

III.11.8.1. Zertifikat mit acme.sh beantragen

Wechseln Sie in den Container Puppeteer und geben dort den Befehl **sle** (sudo let's encrypt environment) ein, um in die Umgebung zur Verwaltung der Zertifikate über **acme.sh** zu gelangen:

```
sle
```

Beantragen Sie dort das Zertifikat über folgenden Befehl:

```
issue kopano.schulkuerzel.logoip.de
```

Hierbei steht **schulkuerzel** für den bereits mehrfach verwendeten individuellen Namen (z.B. musterstadt-gym). Bei **acme.sh** erhält man eine sehr ausführliche Rückmeldung mit vielen Informationen.

Einen Überblick der darüber verwalteten Zertifikate erhält man per:

```
acme.sh --list
```

Wenn das Zertifikat erstellt und heruntergeladen wurde, landet es über Puppet irgendwann im Container **rev-proxy** im Ordner `/etc/nginx/ssl`. Das Ganze lässt sich ggf. wieder über einen **prun** im **puppeteer** und danach im **rev-proxy** beschleunigen.

Teil IV. Installation der Arbeitsstationen

Inhaltsverzeichnis

IV.1. Arbeitsstationen	IV – 5
IV.1.1. Vorbereiten und Testen der Arbeitsstationen	IV – 5
IV.1.1.1. Ändern der Bootreihenfolge auf Netzwerkbetrieb	IV – 5
IV.1.1.2. Umstellen der Netzwerkkarte auf Netzwerkbetrieb	IV – 6
IV.1.2. Die Rechneraufnahme mit LD Deploy	IV – 7
IV.1.3. Die Phasen in LD Deploy	IV – 7
IV.1.4. Musterarbeitsstation mit Windows 10	IV – 8
IV.1.4.1. Windows 10 Image Download	IV – 8
IV.1.4.2. Windows 10 Image Synchronisation	IV – 10
IV.1.4.3. Hardwareerkennung und Systemanpassungen	IV – 11
IV.1.4.4. Fehlersuche und Behebung	IV – 16
IV.1.4.5. Windows 10 Installation anpassen	IV – 17
IV.1.4.6. Windows 10 Updates installieren	IV – 20
IV.1.4.7. Windows 10 Image erstellen	IV – 20
IV.1.5. Treiber-Aktualisierung ohne Imageerstellung	IV – 24
IV.1.5.1. Treiber aktualisieren	IV – 25
IV.1.5.2. Treiber hochladen	IV – 25
IV.1.5.3. Treiber verteilen	IV – 27
IV.1.6. Tools für die Systemanpassung von Windows 10	IV – 27
IV.1.7. Systemanpassung in LD Deploy mit AutoConf	IV – 28
IV.1.7.1. Rollen, Playbooks und Phasen	IV – 28
IV.1.7.2. Installation von Tools zur Automatisierung per AutoConf	IV – 29
IV.1.7.3. Anpassung von Windows 10 mit LD Deploy	IV – 29
IV.1.7.4. Systemanpassungen für Windows 10	IV – 32
IV.1.7.5. Anpassungen mit AutoConf anwenden und testen	IV – 33
IV.1.7.6. Drucker	IV – 35
IV.1.7.7. SMART-Board Kalibrierung und Lizenzierung	IV – 46
IV.1.7.8. Promethean Board Konfiguration und Kalibrierung	IV – 53
IV.1.8. Funktionsupgrade von Windows 10	IV – 57
IV.1.8.1. Image-Konfiguration und Partition für das Funktionsupgrade	IV – 58
IV.1.8.2. Ansible-Konfiguration für das Funktionsupgrade	IV – 61
IV.1.8.3. Konfigurationen einem Rechner zuweisen	IV – 63
IV.1.8.4. Image neu einspielen und Anpassungen vornehmen	IV – 64
IV.1.8.5. Funktionsupgrade durchführen	IV – 64
IV.1.8.6. In Audit-Mode wechseln und Image erstellen	IV – 65
IV.1.9. Installation Office 2019	IV – 67
IV.1.9.1. XML-Datei erstellen	IV – 67
IV.1.9.2. Setup mit Optionen ausführen	IV – 68
IV.1.10. Linux am Client	IV – 68
IV.1.10.1. Konfiguration um Linux erweitern	IV – 69
IV.1.10.2. Linux Master-Installation durchführen	IV – 73
IV.1.10.3. Linux Image importieren und zuweisen	IV – 77
IV.1.10.4. Linux-Image am Client aufspielen	IV – 78
IV.2. LogoDIDACT-Agent und Console	IV – 79
IV.2.1. Installation unter Windows	IV – 80

Kapitel IV.1. Arbeitsstationen

Ein wesentlicher Bestandteil von LogoDIDACT ist schon immer das Konzept der selbstheilenden Arbeitsstationen. Mit der offiziellen Freigabe von LogoDIDACT 2.0 zum 01.01.2016 wurde auch der komplett neu entwickelte Schutzmechanismus **ldprotect** freigegeben.

Auf Basis einer Virtualisierungsschicht sorgt **ldprotect** dafür, dass die Rechner gegen jegliche Manipulation geschützt sind und selbst das harte Ausschalten von Windows 7 oder Windows 10 dem Dateisystem nichts mehr anhaben kann. Ein weiterer riesiger Vorteil besteht darin, dass die Heilung keinerlei Zeit benötigt und die Rechner damit sehr viel schneller starten.

Für die Verteilung von Software steht nun mit **LD Deploy** eine weitere Neuentwicklung bereit, welche das in die Jahre gekommene Rembo/mySHN® endgültig ablöst.

Im Folgenden wird erklärt, wie man Computer als selbstheilende Arbeitsstationen in LogoDIDACT integriert. Ergänzend dazu besteht natürlich auch die Möglichkeit, Computer und Notebooks ohne Selbstheilung zu betreiben. Der normale Betrieb von Arbeitsstationen in LogoDIDACT ist allerdings der Modus mit Selbstheilung.

IV.1.1. Vorbereiten und Testen der Arbeitsstationen

IV.1.1.1. Ändern der Bootreihenfolge auf Netzwerkbetrieb

Starten Sie den Rechner und halten Sie den Bootvorgang mit der **Pause** Taste an. Am unteren Bildschirmrand finden Sie meistens die Informationen, wie Sie in das BIOS-Setup des Rechners gelangen. Setzen Sie den pausierten Bootvorgang mit der **Return** bzw. **Enter** Taste fort und drücken Sie mehrmals hintereinander die entsprechende Taste, z.B. **F2**, **F10** oder **Esc**. Das BIOS-Setup wird geladen. Ändern Sie die Bootreihenfolge ab und setzen Sie die Netzwerkkarte an die erste Position („Netzwerkboot“).



Achtung

Bei Onboard-Hardware müssen Sie ggf. zuerst Netzwerkkarte und/oder Boot-PROM im BIOS-Setup aktivieren, bevor Sie auf „Netzwerkboot“ umstellen können.

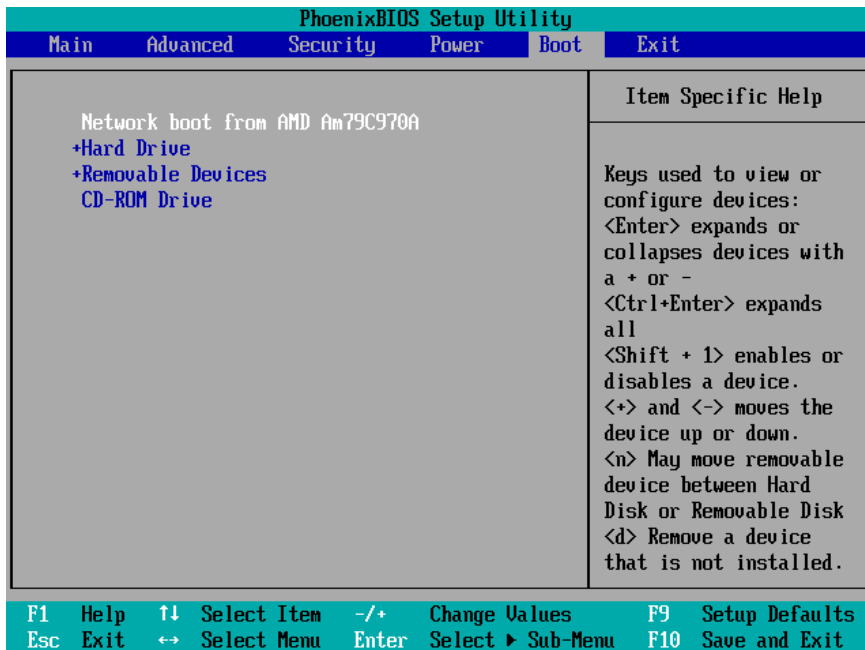


Abbildung IV.1.1. Ändern der Bootreihenfolge



Achtung

Die Einstellungen sind herstellerabhängig und können unterschiedlich lauten oder sich an verschiedenen Stellen im BIOS-Setup befinden.

Speichern Sie die Änderungen ab und verlassen Sie das BIOS-Setup. Der Rechner wird neu gestartet.

IV.1.1.2. Umstellen der Netzwerkkarte auf Netzwerkbetrieb

Drücken Sie während des Bootvorgangs die entsprechende Tastenkombination, um in das Setup der Netzwerkkarte zu gelangen. Mit den bereits bekannten Tasten **Pause** und **Enter** können Sie den Bootvorgang kontrollieren.



Tipp

- **Strg+Alt+B** für 3COM
- **Strg+S** für Intel
- **Shift+F10** für Realtek

Setzen Sie das **Boot Protocol** auf **PXE (Preboot eXecution Environment)** und den Wert für **Boot Order** auf **Network Boot**. Speichern Sie die Änderungen ab und verlassen Sie das Netzwerkkarten-Setup. Der Bootvorgang wird fortgesetzt.

Wenn der Rechner von PXE bootet und seine IP-Informationen vom DHCP-Server erhalten hat, wird die **LD Deploy** Client Software in den Hauptspeicher des Rechners geladen.

Sofern ein Rechner noch nicht im System bekannt ist, startet er in die so genannte Rechneraufnahme.

IV.1.2. Die Rechneraufnahme mit LD Deploy

Starten Sie einen Rechner über den so genannten PXE Netzwerkboot. Es spielt dabei keine Rolle, ob der Rechner über den BIOS-Modus startet oder im UEFI-Mode. Beide Varianten werden von **LD Deploy** unterstützt und zur Laufzeit wird automatisch die passende Clientunterstützung verwendet.

In dieser ersten Phase zeigen sich bereits die großen Vorteile von **LD Deploy** zu seinem Vorgänger. Was die Unterstützung verschiedenster Client-Hardware anbelangt, gibt es weder Einschränkungen hinsichtlich der USB-Geräte wie Maus und Tastatur, noch irgendwelche grundlegenden Probleme bei der Geschwindigkeit im Netzwerk oder auf der lokalen Festplatte. Selbstverständlich wird aber aus einer alten, langsamen SATA-Festplatte keine SSD und aus einem Pentium 4 kein Core i5.

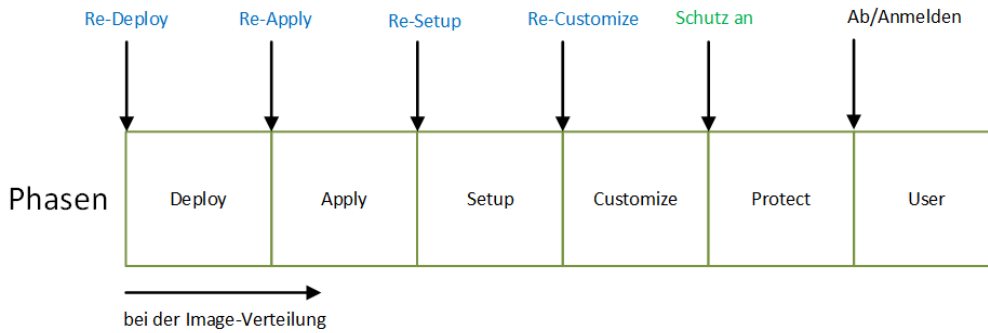
Geben Sie einen Raumnamen ein oder wählen Sie einen Raum aus, sofern Sie diesen zuvor über dasControlCenter erstellt haben. Der Rechnername orientiert sich automatisch am Raumnamen.

Vergeben Sie eine IP-Adresse entsprechend Ihrer Netzwerkkonfiguration und klicken Sie auf **Übernehmen**. Wenn das Gerät über eine WLAN-Schnittstelle verfügt, wird auch diese angezeigt und kann mit importiert werden.

IV.1.3. Die Phasen in LD Deploy

In **LD Deploy** gibt es mehrere Phasen, die ein Client der Reihe nach durchläuft. Dies ist in folgender Grafik anschaulich dargestellt. In den verschiedenen Phasen werden unterschiedliche Aufgaben durchgeführt, die im Normalfall aus Anwendersicht nicht speziell von Interesse sind. Auf technischer Ebene verbirgt sich hinter jeder Phase eine virtuelle Umgebung in einer VHDx-Container-Datei.

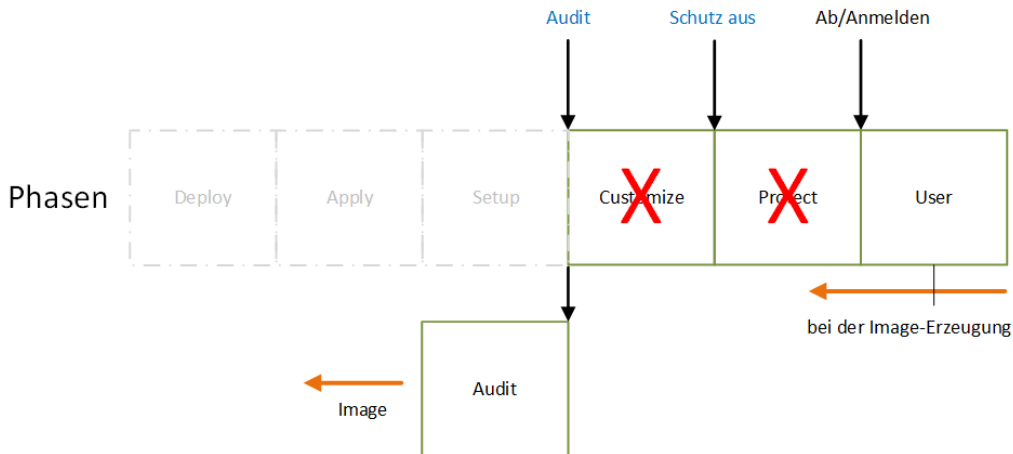
Wenn es ein neues Image am Server gibt und ein Client startet, lädt dieser das Image vom Server herunter (Phase Deploy) und packt es dann auf der Systempartition C:\ aus (Phase Apply).



In der Phase **Setup** findet die Treibererkennung und Installation statt und in der Phase **Customize** erfolgen kundenspezifische Anpassungen, wie z.B. welche Drucker sichtbar sind oder ob eine Grafikkarte einen Monitor und Beamer gleichzeitig im Clone-Mode ansteuert.

In der Phase **Protect** wird die Schutzfunktion aktiviert, die den Rechner vor jeglicher Manipulation durch Benutzer oder Viren und Trojaner schützt. Der Schutz basiert darauf, dass sämtliche Änderungen, die vom System normalerweise auf C:\ geschrieben werden, in der Container-Datei "Protect" landen. Diese wird beim Neustart einfach verworfen, so dass ein Rechner ohne Zeitverzug in sekundenschnelle wieder im funktionsfähigen Zustand ist.

Beim Erstellen eines Images gibt es gewissermaßen einen Durchlauf in umgekehrter Richtung der Phasen. Ausgehend von einem geschützten Rechner in der Phase **User** hat der Administrator als berechtigter Benutzer die Möglichkeit den Schutz auszuschalten oder sofort in den so genannten **Audit** Modus zu wechseln. Die Phase **Customize** wird dabei nicht durchlaufen, sondern einfach verworfen, damit keine rechner-spezifischen Anpassungen im Image landen. Die installierte Umgebung in der **Audit** Phase entspricht dem Stand, der am Ende der Setup-Phase vorliegt.



Dieses Wissen um die einzelnen Phasen in **LD Deploy** ist vor allem für Administratoren wichtig und das Verständnis dafür, welche Anpassungen in welcher Phase vorgenommen werden und warum das so notwendig ist.

IV.1.4. Musterarbeitsstation mit Windows 10

IV.1.4.1. Windows 10 Image Download

Unmittelbar nach einer erfolgreichen Rechneraufnahme beginnt der Downloadprozess und das Windows 10 Image wird auf den Rechner geladen. In der Phase **Initialisieren** lädt der Client

zunächst alle Konfigurationsdaten vom Server. Im Schritt **Partitionierung sicherstellen** erfolgt die Erkennung der Speichergeräte und die Partitionierung und Formatierung der lokalen Festplatte.



Danach erfolgt der eigentliche Download.



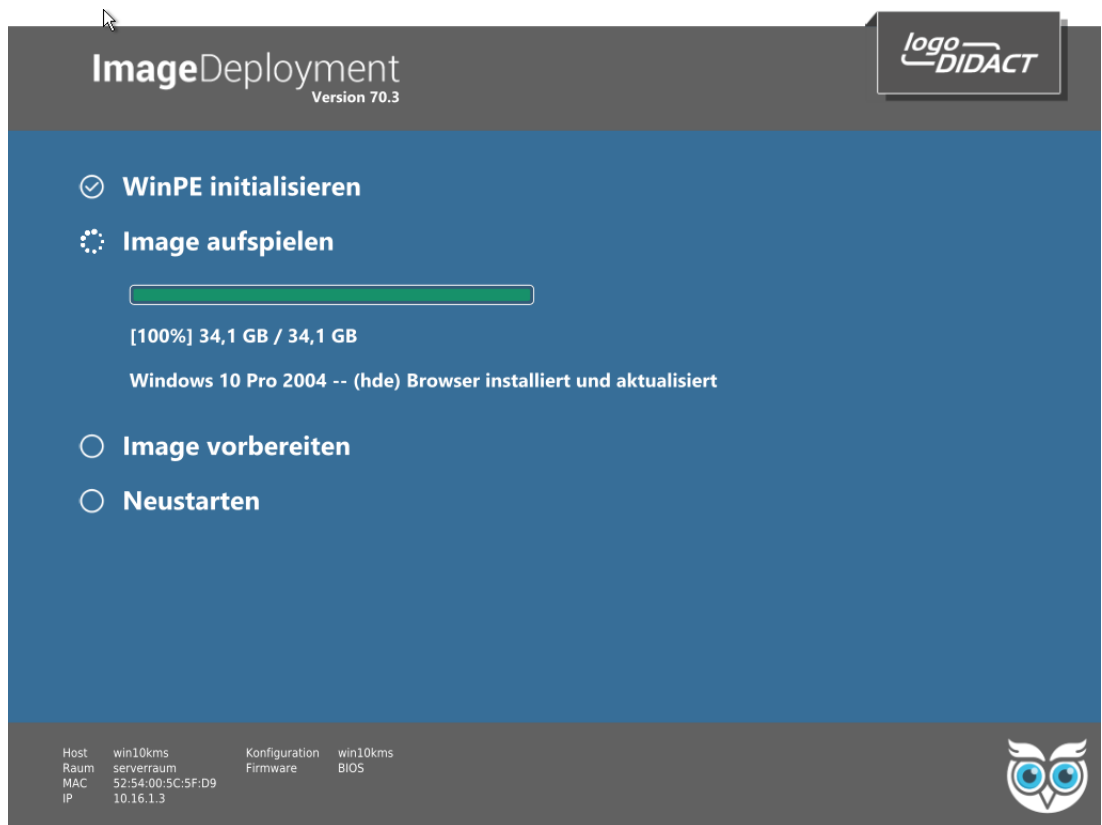
Abhängig von der Geschwindigkeit des Rechners und der Umgebung mit Server und Netzwerk dauert der Download des Basisimages von Windows 10 Build 2004 mit einer Größe von etwa 4.1 GB zwischen 5 und 10 Minuten, bei alten Rechnern aber gegebenenfalls auch länger.

Sobald das Image heruntergeladen wurde, erfolgt eine Überprüfung der Pakete, was an **Verifying Data** zu erkennen ist.

Je nach Größe des Images, der Geschwindigkeit des Netzwerkes und Qualität der Verkabelung, müssen Pakete nachgeladen und überprüft werden. Sobald das Image vom Server in den "Cachebereich" der Master-Arbeitsstation geladen wurde, startet er neu und beginnt mit der Phase der Synchronisation.

IV.1.4.2. Windows 10 Image Synchronisation

Die Synchronisation bzw. das Aufspielen des Images auf die C-Partition wird in **LD Deploy** auch als **Applying** bezeichnet und dauert für ein Windows 10 Basisimage ebenfalls zwischen 5 und 10 Minuten, bei alten Rechnern aber gegebenenfalls auch länger.

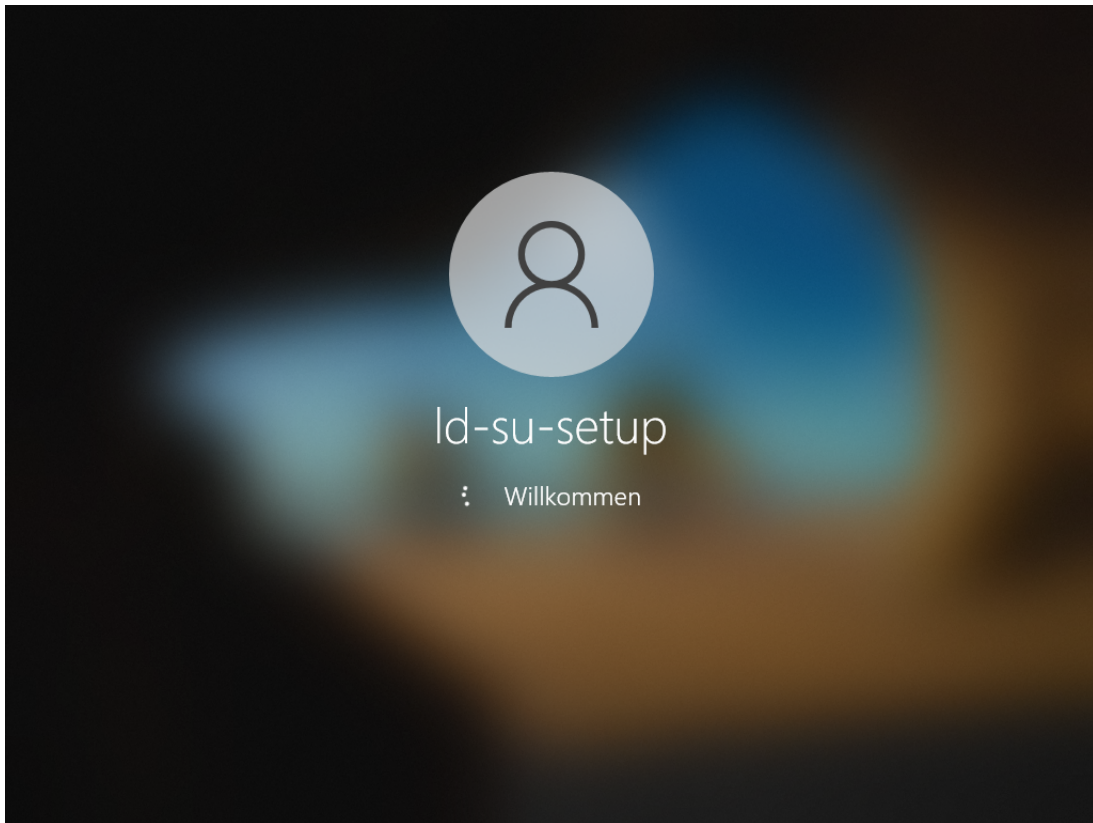


Maßgeblich für die Dauer dieses Vorgangs ist die Festplattengeschwindigkeit im jeweiligen Rechner. Für den Betrieb von Windows 10 ist die Verwendung von schnellen SSD dringend empfohlen. Sobald das Image kopiert und Anpassungen durchgeführt wurden, führt der Rechner einen weiteren Neustart durch.

IV.1.4.3. Hardwareerkennung und Systemanpassungen

Ein wesentlicher Unterschied zwischen Rembo/mySHN® und **LD Deploy** besteht vor allem in der dritten Phase der Verteilung eines Windows 10 Images. In dieser Phase erfolgen jetzt verschiedene individuelle Anpassungen. Zunächst erfolgt die Phase der grundlegenden Hardwareerkennung von Windows 10 mit Neustart.

Danach erfolgt eine automatische Anmeldung des lokalen Benutzers **ld-su-setup**.



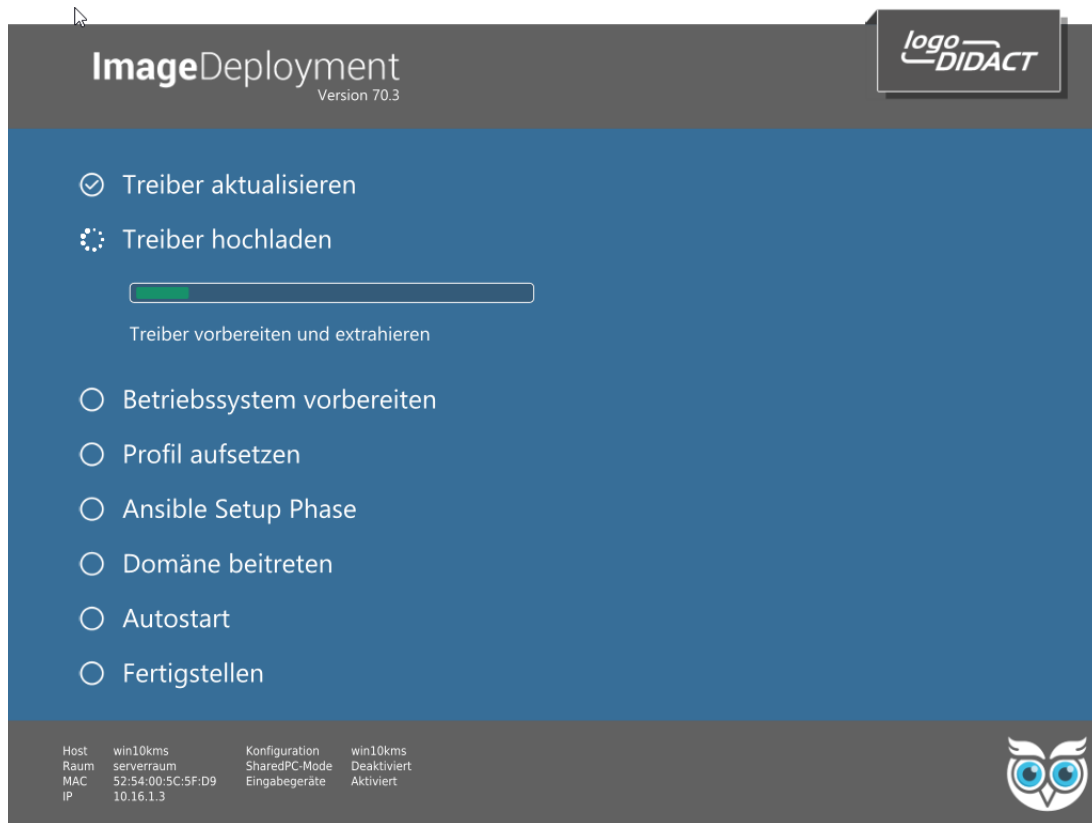
Nach dem Login ist es extrem wichtig, dass das LD Deploy System in seinem Ablauf der Automatisierung nicht gestört wird. Deshalb wird in dieser Phase die Maus und Tastatur gesperrt.

In der Phase der Hardwareerkennung erfolgt die Installation spezifischer Treiber per Windows Plug & Play. Aufgrund der topaktuellen Treiberdatenbank von Windows 10 Build 2004 wird ein sehr großer Teil der Treiber automatisch erkannt, so dass der gesamte Prozess in den meisten Fällen ohne Nutzereingriff abläuft.

Die Phase **Treiber aktualisieren** zeigt dabei diejenigen Treiber, die online aus dem Internet aktualisiert werden.

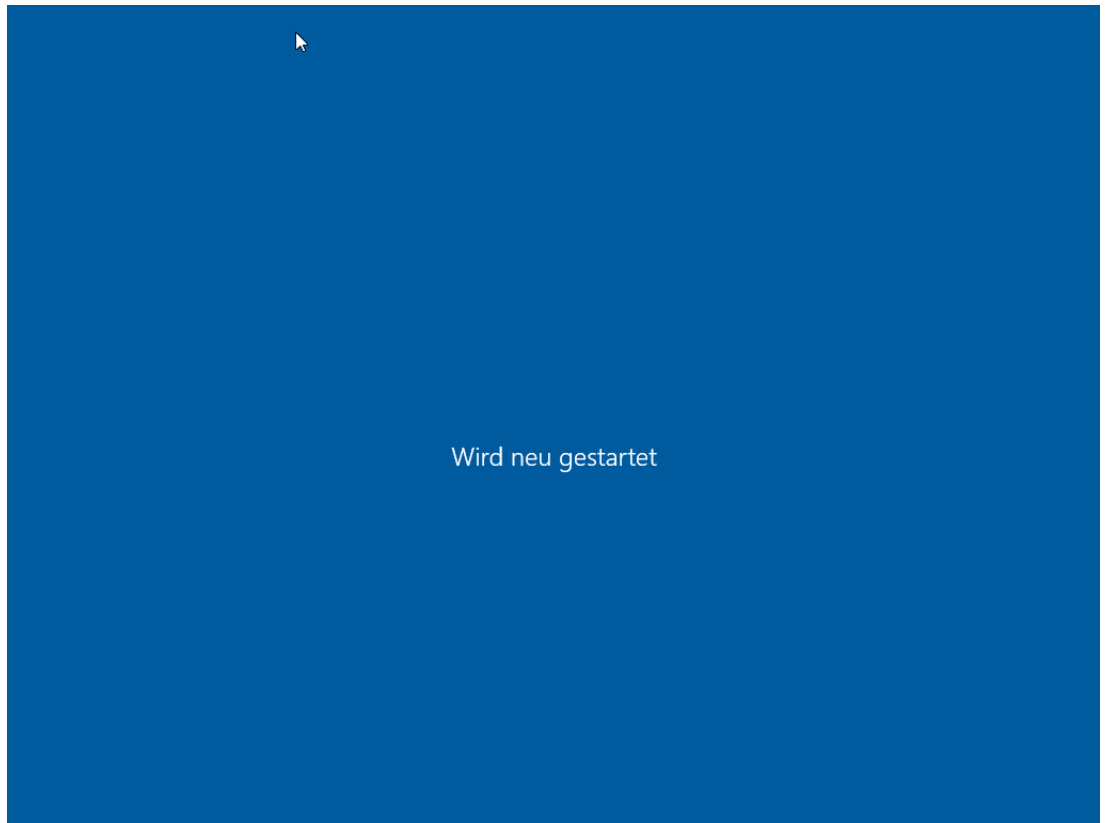


Die per Windows Update aus dem Internet heruntergeladenen Treiber werden anschließend sofort als Treiber-Pakete in den Container **nexus** zum Caching hochgeladen, so dass andere Arbeitsstationen sich diesen Treiber nicht ebenfalls aus dem Internet laden.

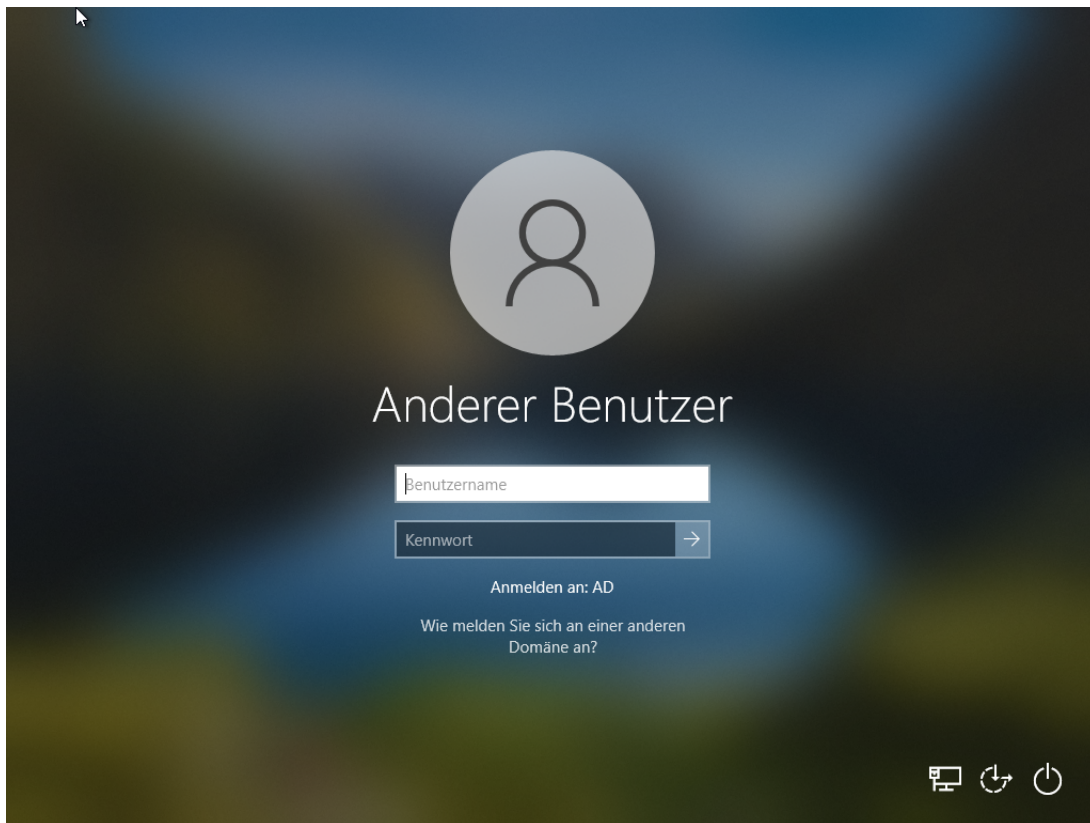


Auf neuen PCs mit SSD geht der gesamte Ablauf sehr schnell, auf alten Rechnern kann dieser Vorgang auch 20 Minuten und länger dauern. Ob ein älterer Rechner mit SATA-Platte tatsächlich noch etwas macht, sieht man gegebenenfalls am wilden Blinken der Platten-LEDs und hört das auch.

Sobald alle Komponenten erkannt wurden erfolgt ein weiterer Neustart.



Sofern Netzwerktreiber einen Zugriff auf den Server ermöglichen, erfolgt ein dynamischer Beitritt zur Domäne mit den unter Abschnitt III.5.9.4, „Den Domänenbeitritt konfigurieren“ eingetragenen Benutzerdaten.



Melden Sie sich mit dem Domänen-Benutzer **admin** und dessen Kennwort an der Domäne an.



Achtung

Wenn im obigen Dialog nicht **Anmelden an : AD** steht, liegt das in der Regel an einer falschen Konfiguration der Zugangsdaten oder an einer fehlenden Verknüpfung der Konfiguration.

IV.1.4.4. Fehlersuche und Behebung

In den verschiedenen Phasen Download, Synchronisation, Hardwareerkennung und Systemanpassung kann es zu verschiedenen Fehlern kommen, die sich jedoch gezielt untersuchen und beheben lassen.

Sowohl beim Verteilen eines Images, als auch beim Erstellen durchläuft ein Client drei verschiedene Phasen. Im Normalfall merkt man in den ersten beiden Phasen nicht einmal, dass sich der LD Deploy-Client in einer vollkommen unterschiedlichen Betriebssystemumgebung befindet und solange keine Fehler auftreten, spielt das auch keine Rolle. Im Fehlerfall ist es aber wichtig, die Umgebungen und Phasen zu kennen.

IV.1.4.4.1. LD Deploy Umgebung linpe

In der ersten Phase befindet sich der LD Deploy-Client in einer Betriebssystemumgebung mit linpe (=linux preboot environment). In diesem Modus werden Aktionen durchgeführt, die in einer Linux-Umgebung deutlich besser umgesetzt werden können, da eine optimale Treiberunterstützung auf Kernelebene vorhanden ist. Eingesetzt wird derzeit (29.05.2019) Fedora 30 mit dem Linux-Kernel 5.0.9 vom 29.04.2019.

Hierzu gehört das Erkennen und Konfigurieren der Speichergeräte, sowie das anschließende Partitionieren und Formatieren der Festplatte(n).

Auch der Download eines Images vom Server über das Netzwerk findet in der linPE-Umgebung von LD Deploy statt. Gleiches gilt für den Upload eines Images vom Client auf den Server.

Aktionen und gegebenenfalls auch Fehler, die auf dieser Ebene entstehen, werden am jeweiligen Client im Verzeichnis `C:\logoDIDACT\logs\linPE` protokolliert.

In dieser Umgebung, kann man über die Tastenkombination **strg+alt+F1** und **strg+alt+F3** auf eine andere Console wechseln. Die graphische **LD Deploy** Oberfläche selbst läuft in F2, so dass man über **strg+alt+F2** wieder dorthin zurückkehren kann.

Im fehlerfreien Betrieb ist das Wechseln in eine andere Console etwas schwierig, weil der Client entsprechend ausgelastet ist, was bei einem Fehler natürlich nicht der Fall ist. Gegebenenfalls hilft die Tastenkombination **str+alt+F1**.

Screenshots können in der linpe-Phase über die Funktionstaste **F12** erstellt werden und landen in `C:\logoDIDACT\ScreenShots`.

IV.1.4.4.2. LD Deploy Umgebung winpe

In WinPE liegen Infos zu den entsprechenden Funktionen, die mit LD Deploy in dieser Phase durchgeführt werden. Dazu gehört z.B. das Anlegen von VHDs, das Kopieren von wim-Dateien in eine VHD und der automatische Domänenbeitritt.

Aktionen und gegebenenfalls auch Fehler, die auf dieser Ebene entstehen, werden am jeweiligen Client im Verzeichnis `C:\logoDIDACT\logs\winPE` protokolliert.

Die entsprechenden Befehle für den Modus mit WinPE (= Windows Preboot Environment) lauten **alt+tab** und **Shift+F10**.

IV.1.4.4.3. LD Deploy Umgebung Windows 10

Sowohl bei der Erstellung eines Images als auch nach dem Verteilen, finden zahlreiche Anpassungen unter Windows 10 statt.

Aktionen und gegebenenfalls auch Fehler, die auf dieser Ebene entstehen, werden am jeweiligen Client im Verzeichnis `C:\logoDIDACT\logs\OS` protokolliert.

Dieses Verzeichnis hat für die Suche und Beseitigung von Fehlern die größte Bedeutung, was einfach daran liegt, dass sich durch Updates in Windows 10 die meisten Veränderungen ergeben können, welche die Automatismen von **LD Deploy**

IV.1.4.5. Windows 10 Installation anpassen

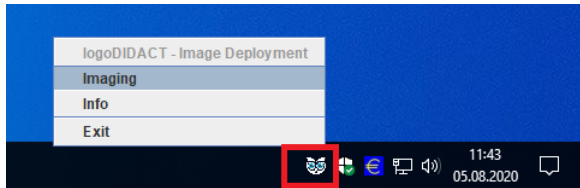
In **LD Deploy** gibt es eine grundlegende Änderung in der Art und Weise, wie ein Image erstellt wird. Der normale und auch empfohlene Weg geht dabei über Sysprep. Es gibt jedoch auch weiterhin einen Clone-Mode, der eine Installation auf ähnliche Weise als Image speichert, wie das unter Rembo/mySHN® der Fall war.

Grundlegend anders ist auch die Stelle von der aus man die Erstellung eines Images anstößt. Fast alles wird entweder über das ControlCenter per Web-Browser oder unter Windows über das ControlPanel gesteuert.

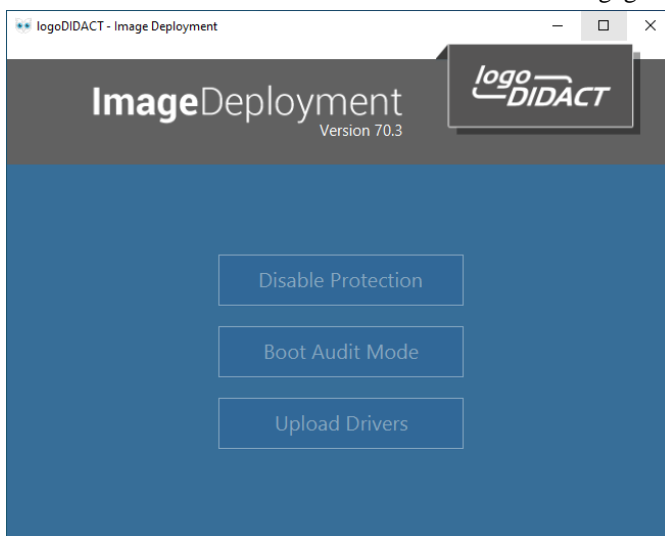
IV.1.4.5.1. Das ControlPanel in Windows

Ähnlich wie bei den bekannten Bausteinen LogoDIDACT-Agent und LogoDIDACT-Console gibt es auch bei **LD Deploy** sowohl auf Systemebene als auch auf Benutzerebene verschiedene Komponenten, über welche die Verteilung von Images und auch einzelner Pakete gesteuert wird.

Über das so genannte ControlPanel steuern Sie die wesentlichen Funktionen Imageerstellung und Aktivierung bzw. Deaktivierung des Schutzes (Selbstheilung). Das ControlPanel wird über das Taskleisten-Symbol von **LD Deploy** durch Klick über den Eintrag **Imaging** aus dem Auswahlmü gestartet.

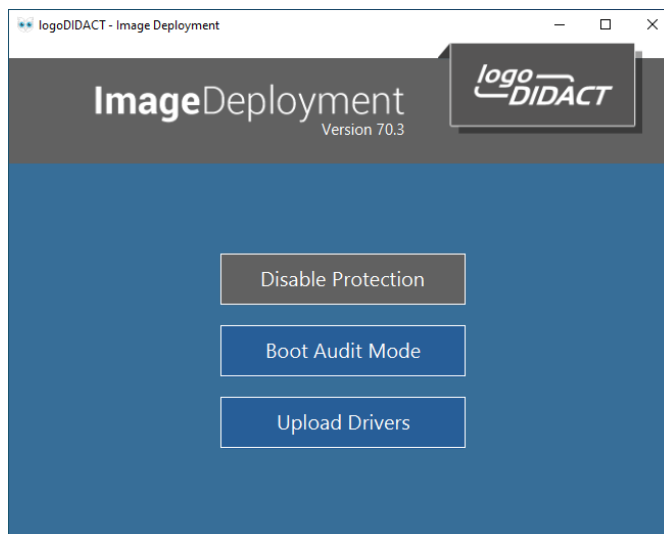


Trotz administrativer Rechte kann es vorkommen, dass die Schaltflächen im Controlpanel ausgegraut sind. Dafür gibt es verschiedene Gründe. Zwischen den Client- und Serverkomponenten gibt es eine Vertrauensstellung, die aus verschiedenen Gründen gestört oder nicht mehr vorhanden sein kann. Dies kann passieren, wenn die physische Netzwerkverbindung verloren geht aber auch, wenn das Computerkonto am Server gelöscht wurde oder das Computerkennwort zwischen Client und Server nicht mehr stimmt. In diesen Fällen sind alle Felder ausgegraut.

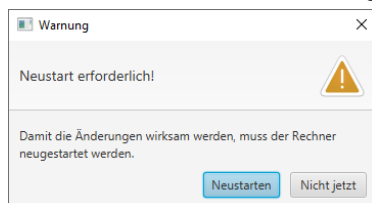


Schließen Sie in diesem Fall das Fenster und beenden Sie das Startprogramm mit Rechtsklick auf das Symbol auf der Taskleiste über **Exit**. Starten Sie das Panel manuell durch Doppelklick auf das VB-Script `ld-launch-panel` im Verzeichnis `C:\logoDIDACT\Deploy\Agent\shared`.

Starten Sie das ControlPanel erneut über das Auswahlmü durch Klick auf das Taskleisten-Symbol von **LD Deploy**. Sofern der Schutz aktiviert ist (Standard), ergibt sich das folgende Bild und die Möglichkeit diesen Schutz über die Schaltfläche **Disable Protection** zu deaktivieren.



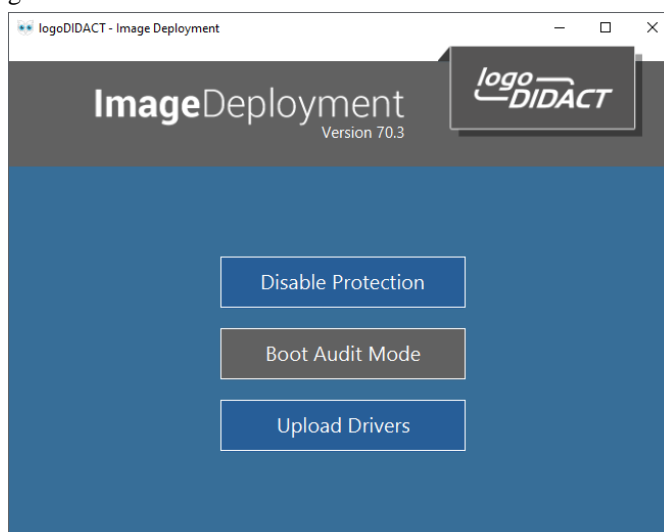
Der Rechner muss daraufhin neu gestartet werden.



IV.1.4.5.2. In den Audit Modus wechseln

Für die Installation von Software und die Definition eines Vorlageprofils, wechseln Sie in den **Audit Mode**. Das ist bis zur Version 42 des **LD Deploy**-Clients nur möglich, wenn der Schutz zuvor deaktiviert wurde bzw. deaktiviert ist. Ab Version 43 kann man direkt in den **Audit Mode** wechseln und der Schutz wird dabei automatisch deaktiviert.

Klicken Sie auf die Schaltfläche **Boot Audit Mode**. Der Rechner wird daraufhin automatisch neu gestartet.



Der **Audit Mode** hat einige sehr spezielle Eigenschaften, die zu beachten sind:



Achtung

1. Solange sich der Rechner im **Audit Mode** befindet, erfolgt bei jedem Start in Windows 10 eine automatische Anmeldung mit dem Konto des lokalen Benutzers **Administrator**. Das ist für die Verwendung von sysprep erforderlich und hat ansonsten keine Einschränkungen.
2. Am lokalen Benutzers **Administrator** darf nichts verändert werden. Dieser Benutzer wird von Microsoft sysprep verwendet und vor der Imageerstellung aktiviert und später wieder deaktiviert. Deshalb Finger weg von diesem Konto!
3. Wenn sich der Rechner im **Audit Mode** befindet und in den Sperrbildschirm wechselt, muss er einfach neu gestartet werden, so dass eine erneute automatische Anmeldung mit dem lokalen Benutzer **Administrator** erfolgt.
4. Wenn Sie für die Installation von Software Zugriff auf Netzlaufwerke benötigen oder vielleicht sogar Software auf das Netzlaufwerk P: installieren müssen, stellen Sie die Verbindung einfach über das Tool **GUILogon** her.
5. Um vom **Audit Mode** in den normalen Betrieb zu wechseln, gibt es nur zwei Möglichkeiten. Entweder erstellt man eine Image, das im Anschluss auch zurückgespielt wird oder man setzt den Rechner ohne Anpassungen per ReDeploy zurück.

IV.1.4.6. Windows 10 Updates installieren

Bevor Sie ein Image erstellen, achten Sie unbedingt darauf vorher alle anstehenden Windows Updates zu installieren. Dabei ist es in der Regel notwendig, den Rechner mehrfach neu zu starten und die Suche nach Windows Updates zu wiederholen.

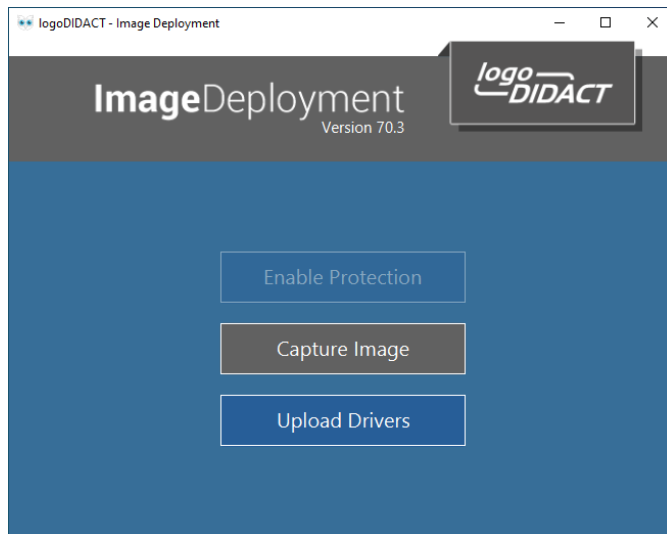


Achtung

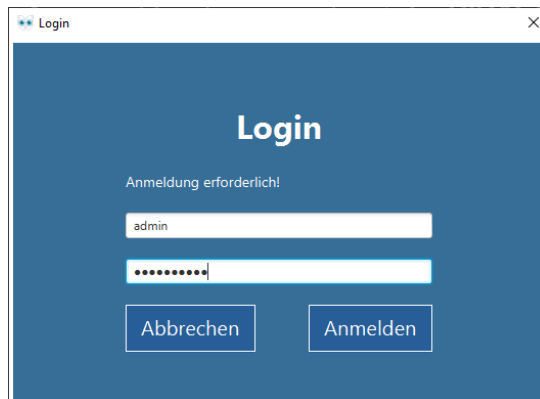
Wenn während der Erstellung eines Images noch im Hintergrund Windows Updates geladen oder installiert werden, führt das zwangsweise dazu, dass das Image kaputt ist!

IV.1.4.7. Windows 10 Image erstellen

Wenn man sich im Audit Mode befindet und alle Anpassungen an seiner Installation vorgenommen hat, startet man das ControlPanel und wählt die Schaltfläche **Capture Image** um ein Image zu erstellen.



Obwohl man den AuditMode nur über administrative Rechte erreicht, wird die Erstellung eines Images sicherheitshalber nochmals über eine Kennwortabfrage für den Benutzer **admin** abgesichert. Geben Sie diese Daten ein und betätigen Sie mit **Anmelden**.



Vergeben Sie anschließend einen kurzen Kommentar, aus dem hervorgeht, was Sie an der Installation verändert haben. Sofern sich mehrere Personen die Administration teilen oder Installationen am Image auch von Fachfirmen vorgenommen werden, ist es empfehlenswert ein Kürzel mit anzugeben, um zu wissen, wer ein Image erstellt hat. Über das untere Eingabefeld können Sie weitere und ausführliche Angaben z.B. zu einzelnen Anwendungspaketen machen und die Anpassungen detailliert beschreiben.

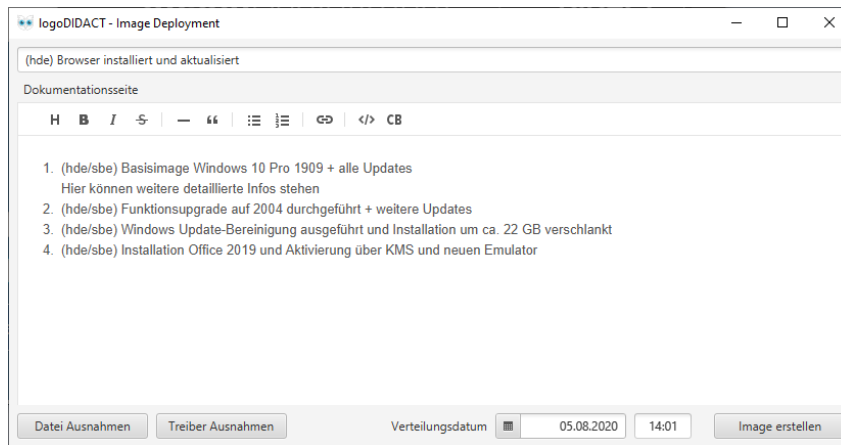


Achtung

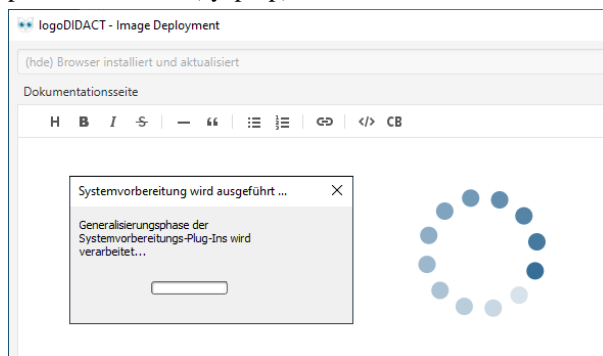
Die Optionen **Datei Ausnahmen** und **Treiber Ausnahmen** sind ausschließlich für Experten und wie Softwareentwickler gedacht, um in Sonderkonstellationen und hochkomplexen Umgebungen spezielle Anpassungen vornehmen zu können. Bitte sehen Sie davon ab, dort irgendwelche Anpassungen vorzunehmen.

Über die Option **Verteilungsdatum** können Sie grundsätzlich den Zeitpunkt der Imageverteilung verschieben. Aber auch dafür besteht in der Regel keine Notwendigkeit, weil auch der Prozess der Imageerstellung selbst niemals in die Phase des laufenden Unterrichtsbetrieb gelegt werden sollte.

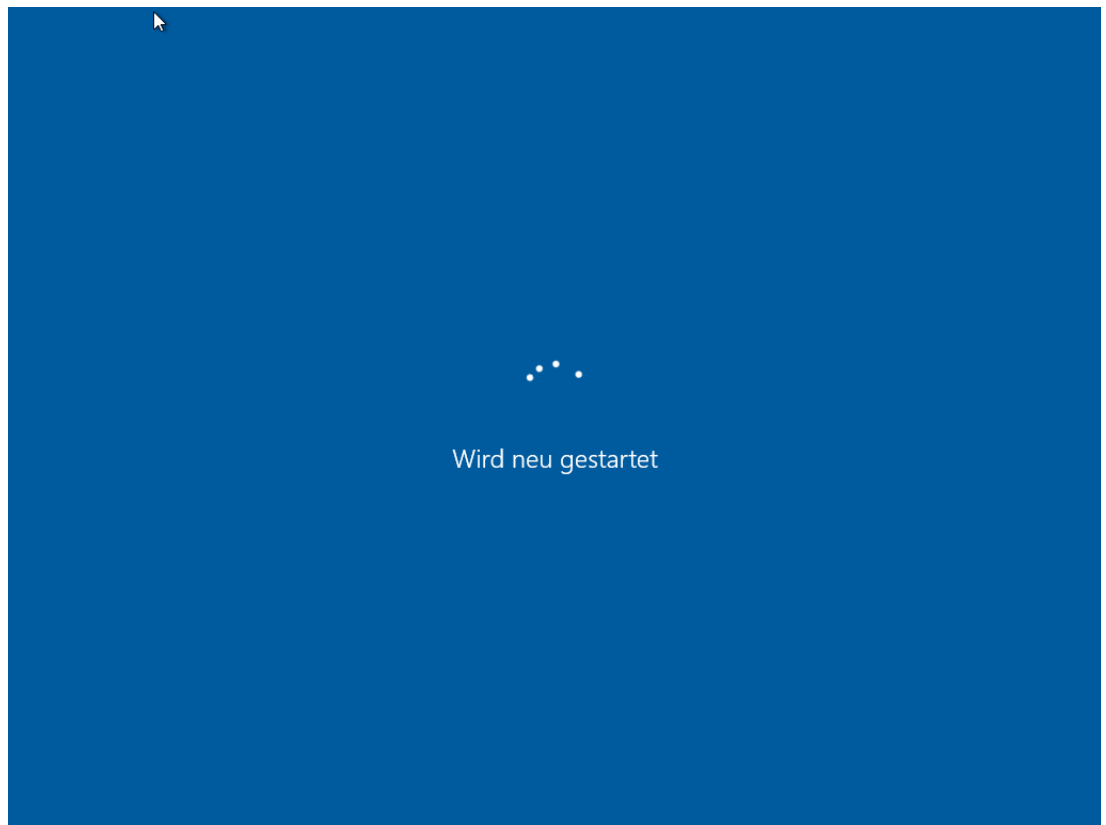
Klicken Sie auf die Schaltfläche **Image erstellen**.



Nach wenigen Augenblicken startet der Vorgang, der zunächst auch die so genannte Generalisierungsphase durchläuft (sysprep).



Der Rechner sollte im Anschluss neu starten, was nicht immer funktioniert. Starten Sie den Rechner in diesem Fall neu.



Beim Neustart beginnt die Erstellung des Images in 2 Phasen. In der ersten Phase wird das Image lokal gebaut in einer *.wim-Datei.



Danach wird diese Datei per Torrent auf den Server kopiert.

IV.1.5. Treiber-Aktualisierung ohne Imageerstellung

Wie bekannt, ist LD Deploy kein reines Imaging-System, sondern vereint die Vorteile von Imaging und paketbasierter Softwareverteilung. Die paketbasierte Verteilung reduziert sich dabei nicht nur auf Anwendersoftware, sondern wird in LD Deploy automatisch auch für die differentielle Verteilung von Treiberpaketen genutzt.



Achtung

Beim Vorgang der Imageerstellung werden per Standard sämtliche Änderungen an der Installation als Image auf den Server hochgeladen, d.h. neben Anpassungen und Softwareupdates selbstverständlich auch aktualisierte oder neu installierte Treiber.

Im Normalfall braucht man diese Funktion also nicht und Sie können diese Kapitel überspringen.

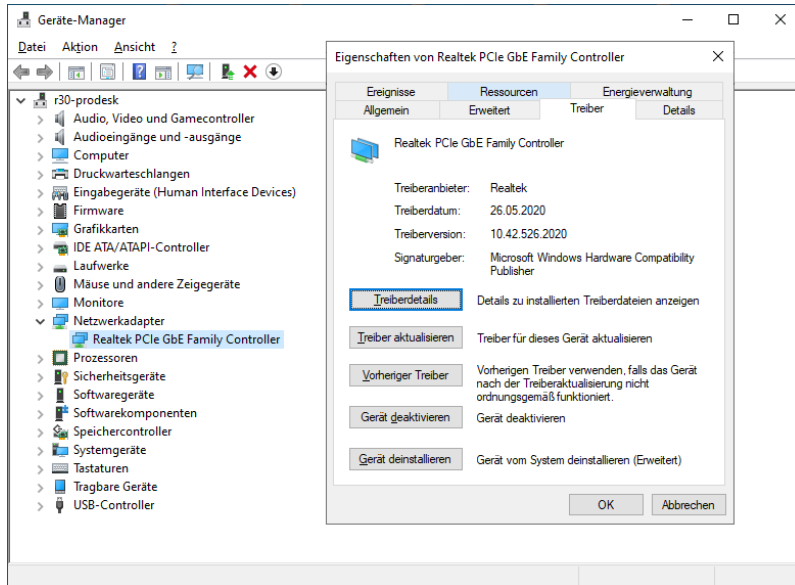
In speziellen Fällen ist das gezielte und separate Hochladen eines Treibers ohne Imageerstellung aber hilfreich und nützlich. Dies lässt sich an einem konkreten Beispiel am leichtesten erklären.

In Beispiel-Szenario stellt man fest, dass man im gerade erstellten Image vergessen hat, einen wichtigen Treiber für die Netzwerkkarte zu aktualisieren. Dieses Szenario ergibt sich real in Windows 10 immer wieder für mitgelieferte Treiber gerade von weit verbreiteten Chipsätzen für Netzwerkkarten von Realtek und Intel. Die per Standard in Windows 10 mitgelieferten Treiber bringen dann oftmals massive Durchsatzprobleme mit sich oder Funktionseinschränkungen beim Wake-on-lan (WOL) oder andere Probleme.

Anstelle nun ein weiteres neues Image zu erstellen nur mit dieser kleinen Treiberänderung, lädt man den Treiber separiert als Differenz auf den Server.

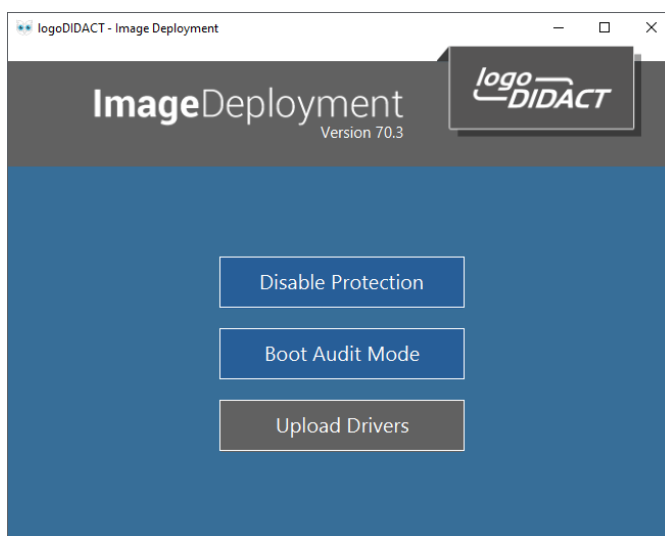
IV.1.5.1. Treiber aktualisieren

Um den Treiber separat als Paket hochzuladen spielt es keine Rolle, ob sich der Rechner im Audit-Mode befindet oder der Schutz aktiviert ist oder nicht. Zumindest gilt das für Treiber, die keinen Neustart des Rechners erfordern. In diesem Fall müssen Sie natürlich in den Audit-Mode wechseln. Das Vorgehen ist aber sonst denkbar einfach. Sie melden sich mit den administrativen Rechten in Windows 10 an, laden den richtigen Treiber von der Seite des Herstellers und installieren diesen.



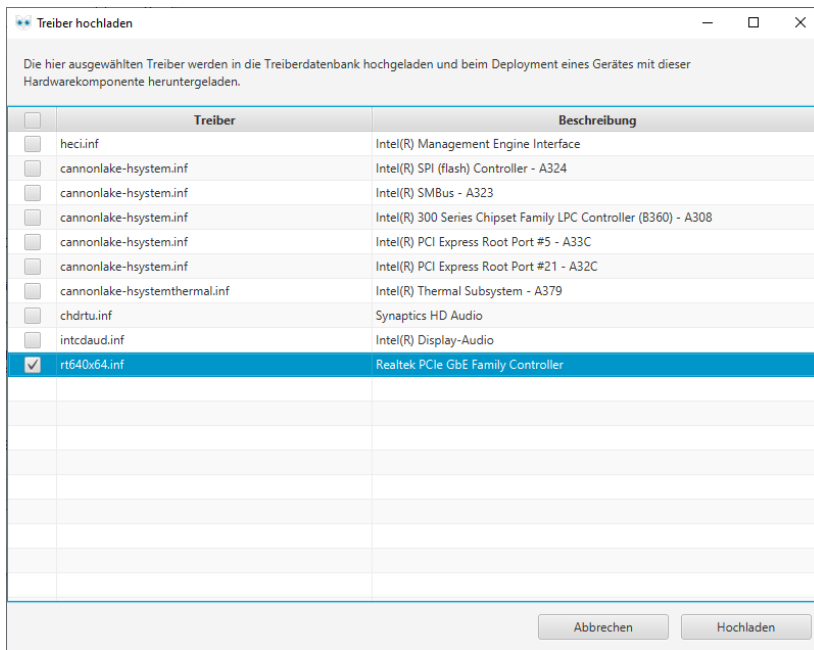
IV.1.5.2. Treiber hochladen

Öffnen Sie anschließend das Control Panel und wählen Sie dort **Upload Drivers**.

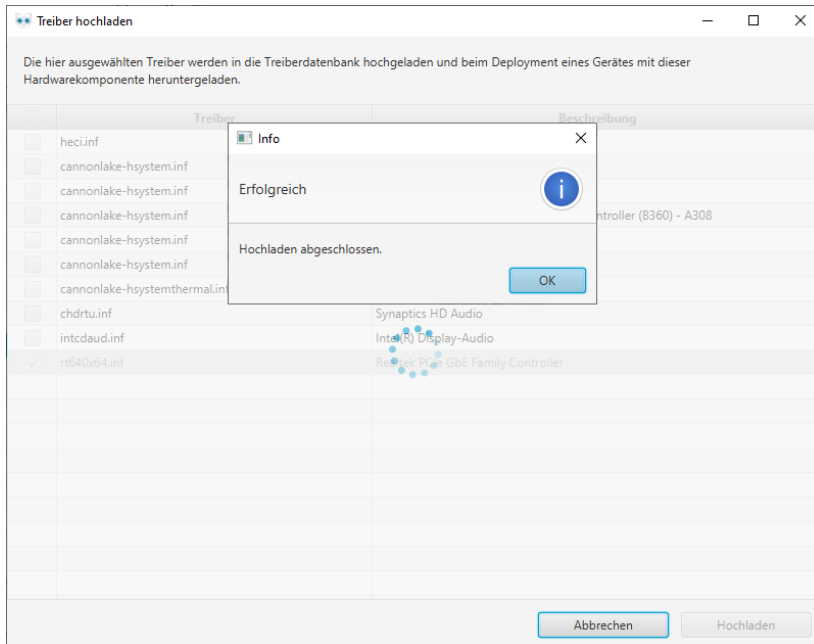


Wählen Sie im folgenden Dialog die Komponenten, deren Treiber Sie aktualisiert haben, setzen dort das entsprechenden Häkchen und bestätigen mit **Hochladen**.

Treiber hochladen



Der Treiber wird nun extrahiert und alle notwendigen Dateien als ZIP-Archiv und damit als Paket auf den **nexus** geladen, der in diesem Fall als Caching-Server für Treiber fungiert. Sofern nicht explizit deaktiviert, wird genau dieser Vorgang bei jeder Erstellung eines Images für alle separierbaren Treiber durchgeführt.



Die Treiberpakete können am **nexus** eingesehen werden und sind entsprechend an den HardwareIDs der Geräte strukturiert abgespeichert.


The screenshot shows the Sonatype Nexus Repository Manager interface. The main content area displays a list of driver files under the path 'win-driver-group'. A file named '19041' is highlighted with a red box. To the left, a red text overlay reads: 'Windows interne Build-Nummer für Windows 10 Version 2004'. Below this, a 'Windows-Spezifikationen' window is open, showing the following details:

Windows-Spezifikationen	
Edition	Windows 10 Pro
Version	2004
Installiert am	23.07.2020
Betriebssystembuild	19041.388
Leistung	Windows Feature Experience Pack 120.2202.130.0

On the right side, a 'Eigenschaften von Realtek PCIe GbE Family Controller' window is open, showing the 'Hardware-IDs' property with the following values:

```

PCIVEN_10EC&DEV_8168&SUBSYS_83F3103C&REV_15
PCIVEN_10EC&DEV_8168&SUBSYS_83F3103C
PCIVEN_10EC&DEV_8168&CC_020000
PCIVEN_10EC&DEV_8168&CC_0200
    
```



Tipp

Das Treiber-Caching im **nexus** hat vor allem den Vorteil, dass Treiber nicht unnötigerweise mehrfach von baugleichen Geräten aus dem Internet heruntergeladen werden.

IV.1.5.3. Treiber verteilen

Die differentielle Verteilung von Treibern erfolgt automatisch über LD Deploy in der linpe-Phase. Entsprechend den lokal im Rechner erkannten HardwareIDs wird die Datenbank im **nexus** nach Einträgen abgefragt und passende Treiber heruntergeladen. Diese Treiber werden dann unmittelbar nach dem zurückspielen in der Phase Apply eingespielt.

IV.1.6. Tools für die Systemanpassung von Windows 10

Bezüglich des Einsatzes von Windows 10 im Schulumfeld sollten Sie sich im Hinblick auf das Thema Datenschutz und Datenverarbeitung die Orientierungshilfe zur datenarmen Konfiguration von Windows 10 vom Arbeitskreis Informationssicherheit der deutschen Forschungseinrichtungen (AKIF) anschauen: https://www.it-sicherheit.mpg.de/Orientierungshilfe_Windows10.pdf.

Es gibt viele kostenfreie Werkzeuge, wie z.B. ShutUp10 oder das VMware OS Optimization Tool, welche ein erfahrener Fachinformatiker oder Systemingenieur ebenfalls nutzen kann, um Windows 10 zu "zähmen". Ebenso nützlich sind Tools wie USB DLM und andere kostenfreie Werkzeuge.



Achtung

Der Umgang mit den verschiedenen Tools wird hier nicht erklärt und ist auch **nicht** Gegenstand des Supports. Bitte wenden Sie sich bei Unklarheiten oder Problemen an den Support des jeweiligen Herstellers bzw. bei Open Source Projekten an die Community und die einschlägigen Wikis.

IV.1.7. Systemanpassung in LD Deploy mit AutoConf

Mit **AutoConf** steht ein weiteres Werkzeug zur Verfügung, das zur Automatisierung von Prozessen dient und innerhalb von LogoDIDACT dazu beiträgt, die Administration zu erleichtern, Zeit zu sparen und Kosten zu senken. Im Gegensatz zu **puppet** auf der Serverseite, arbeitet **AutoConf** auf den Arbeitsstationen und damit überwiegend auf Windows 10 Clients.

IV.1.7.1. Rollen, Playbooks und Phasen

In **AutoConf** wird auf Clientseite überwiegend Powershell genutzt. Über so genannte Rollen werden spezifische Systemanpassungen definiert und in einem Playbook am Client abgearbeitet. Es besteht jedoch keine Notwendigkeit sich mit der Erstellung solcher Anpassungen zu beschäftigen, da diese in LogoDIDACT für viele Aufgaben bereitgestellt werden.



Achtung

Es ist nicht zwingend notwendig im Detail darüber Bescheid zu wissen, welche Rolle in welcher oder welchen Phasen durchgeführt werden. Je nach Phase, kann in einer Rolle etwas deaktiviert oder auch wieder aktiviert werden. Es können Daten gelöscht, hinzugefügt oder eingesammelt werden.

Wichtig ist zu wissen, dass die Ausführung dieser Rollen und die damit verbundenen Anpassungen dafür sorgen, dass Windows 10 sowohl dem Endanwender als auch dem betreuenden LogoDIDACT Partner möglichst wenige Probleme bereitet.

Hier eine unvollständige Liste der derzeit verfügbaren Anpassungen bzw. Rollen und der Phasen, in der sie angewandt werden.

Name der Anpassung (Rolle)	Anwendung in den Phasen	Was wird gemacht
LogoDIDACT Komponenten in der Windows Firewall freigeben	CUSTOM	Firewall Ports geöffnet
Windows Updates deaktivieren	CUSTOM und AUDIT	Windows-Update Dienst wird in der CUSTOM-Phase deaktiviert und in der AUDIT-Phase aktiviert.
Windows Defender deaktivieren	CUSTOM	Virenschutz des Windows Defender wird deaktiviert
Microsoft Office Click2Run Updates deaktivieren	CUSTOM und AUDIT	Verhindert, dass über die Installation von Office 2019 weitere Updates über andere Kanäle geladen werden.

Name der Anpassung (Rolle)	Anwendung in den Phasen	Was wird gemacht
Anzeigeeinstellungen	USER	Bildschirmauflösung und Modus (clone, erweitert, nur Computer, nur Beamer) werden gesetzt
SMART Notebook	CUSTOM, USER und COLLECT	Sichert individuelle SMART Notebook Einstellungen auf dem Server und stellt diese gezielt wieder her.

IV.1.7.2. Installation von Tools zur Automatisierung per AutoConf

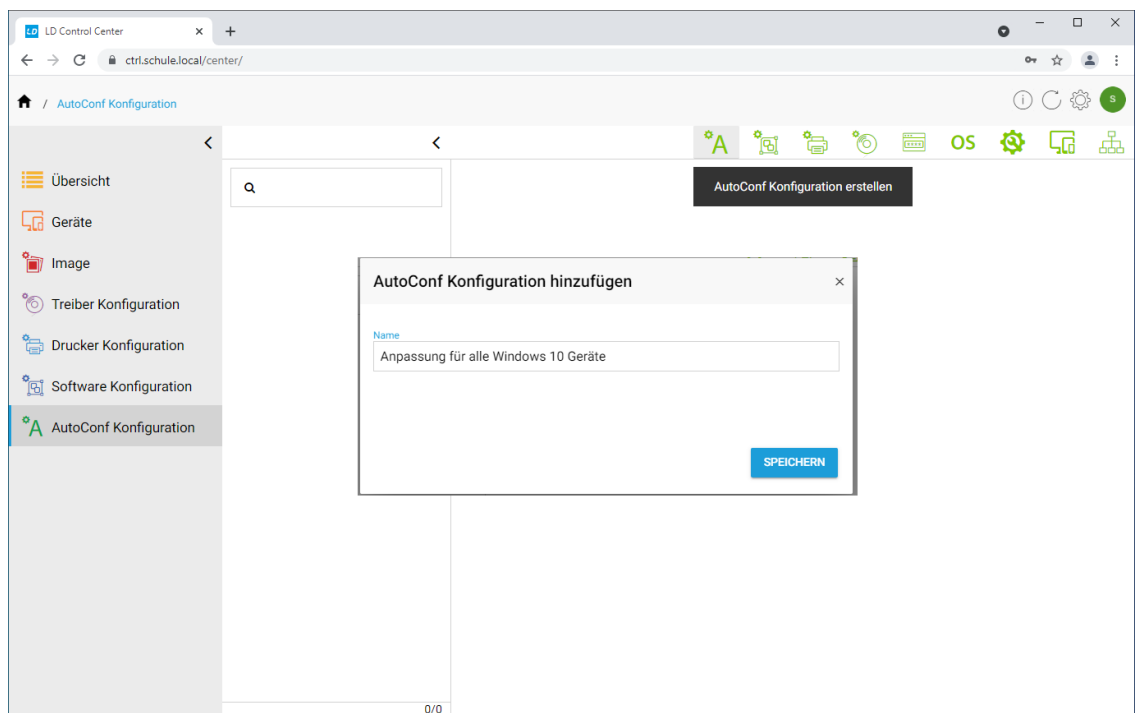
Zum Abarbeiten der AutoConf-Playbooks an den Clients werden verschiedene Tools wie PowerShell, Sysinternals, und Visual C-Pakete benötigt. Diese werden über den Container **nexus-g1** und einem darauf laufenden Squid als Cacher bereitgestellt.

IV.1.7.3. Anpassung von Windows 10 mit LD Deploy

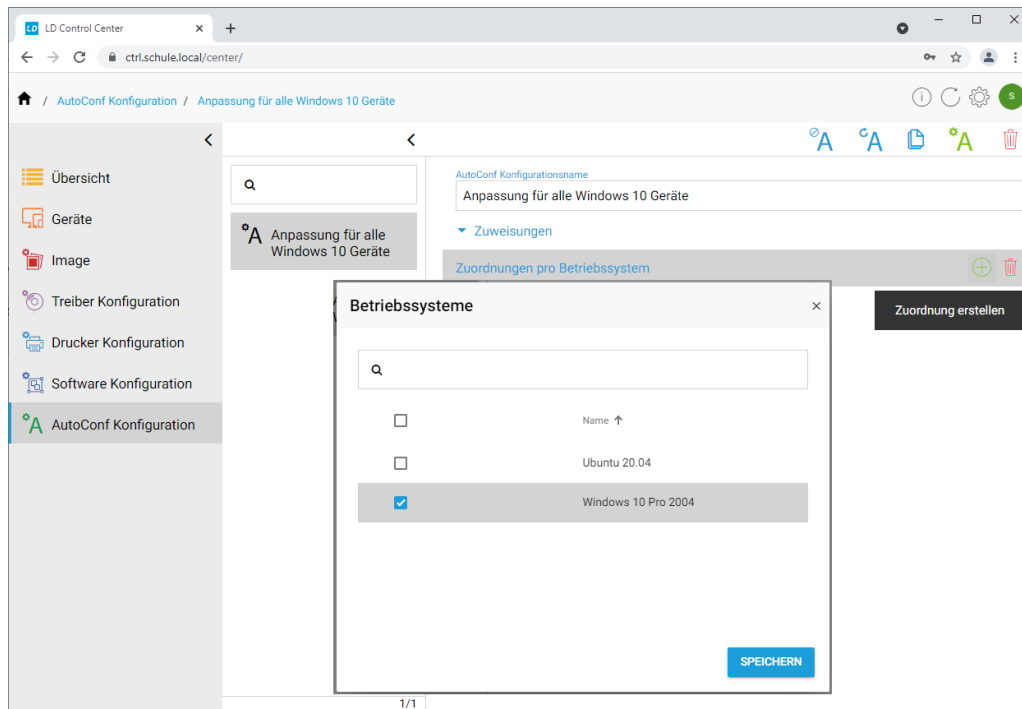
Für grundlegende Anpassungen, gibt es in **LD Deploy** vorgefertigte Rollen, die Sie in einem ersten Schritt zu einem Satz an Anpassungen für Windows 10 zusammenfassen müssen!

Öffnen Sie das ControlCenter und wählen Sie aus dem Menü auf der linken Seite den Eintrag **Auto-Conf Konfiguration** und aus der Menüleiste im oberen rechten Bereich das grüne Symbol zur Erstellung einer neuen AutoConf Konfiguration. Geben Sie der Konfiguration einen aussagekräftigen Namen und bestätigen Sie mit **SPEICHERN**.

Das es um eine allgemeine grundlegende Konfiguration für alle Windows 10 Stationen geht, ist die Bezeichnung "Anpassung für alle Windows 10 Geräte" wie im Beispiel passend.



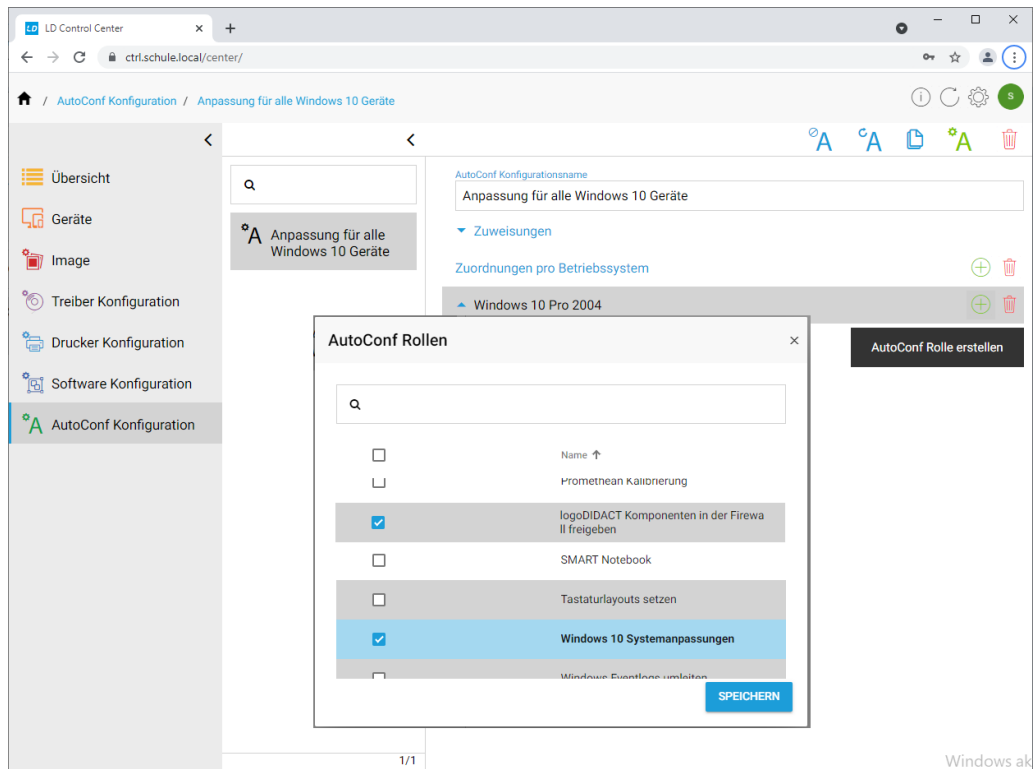
Im nächsten Schritt legen Sie die Verbindung zum passenden Betriebssystem fest. Bestätigen Sie mit **SPEICHERN**.



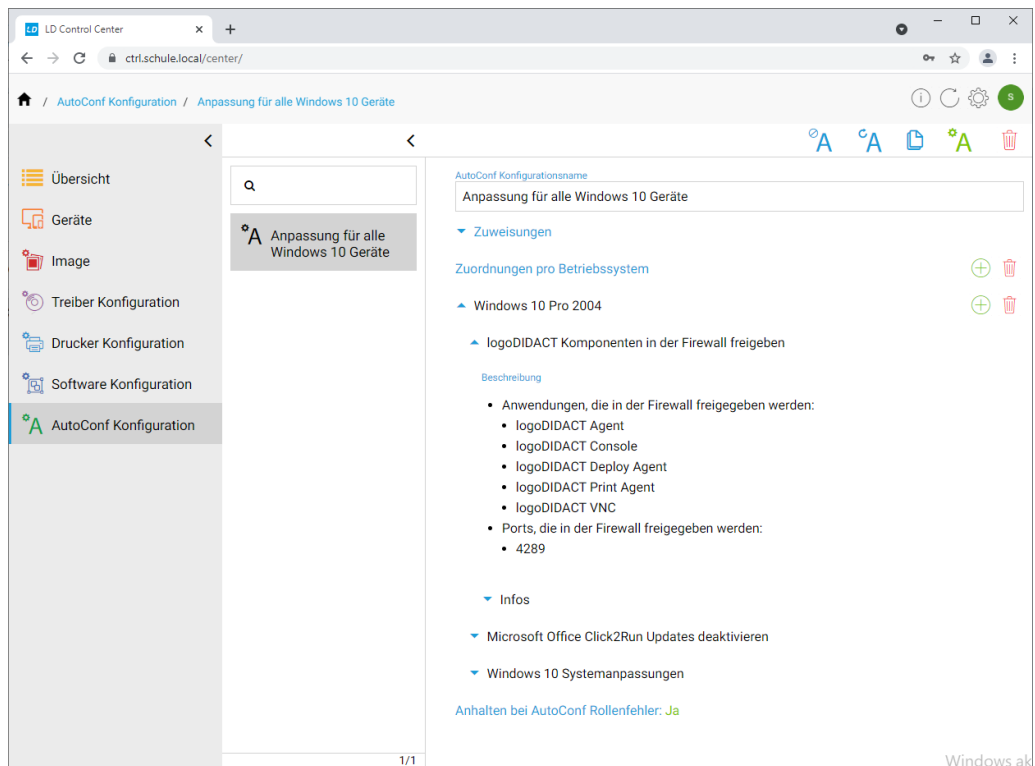
Wählen Sie nun die Anpassungen aus, die am Client abgearbeitet werden sollen. Markieren Sie dazu die gewünschte Rolle, indem Sie das zugehörige Häkchen vor der Beschreibung setzen. Scrollen Sie dabei über die Schieberegler nach unten und aktivieren Sie die folgenden 4 Anpassungen:

- LogoDIDACT Komponenten in der Windows Firewall freigeben
- Microsoft Office Click2Run Updates deaktivieren
- Windows 10 Systemanpassungen

Übernehmen Sie das Ganze mit **SPEICHERN**.

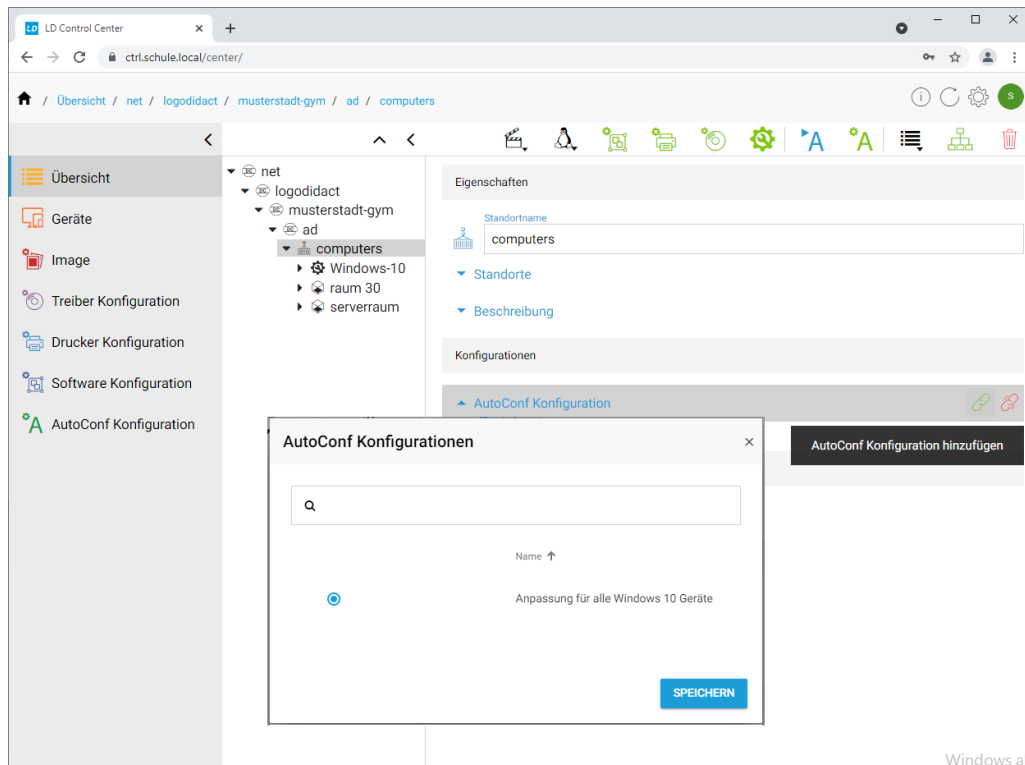


Über die kleinen blauen Pfeilsymbole vor der jeweiligen Rolle, können Sie erweiterte Informationen zu den Aktionen einblenden, die darüber auf den Arbeitsstationen durchgeführt werden. Über die Rolle **LogoDIDACT Komponenten in der Firewall freigeben** wird beispielsweise dafür gesorgt, dass am Windows 10 Client die notwendigen Ports in der Windows-Firewall geöffnet werden, damit die Bildschirmübertragung funktioniert und ebenso ein Großteil der vielen weiteren didaktischen Funktionen.



Im letzten Schritt legen Sie fest, welches Gerät den gerade erstellten Satz an Anpassungen erhalten soll. Da es in diesem Fall, um eine Anpassung für alle Windows 10 Geräte geht, ist die Zuordnung auf der Organisationsebene **computers** sinnvoll.

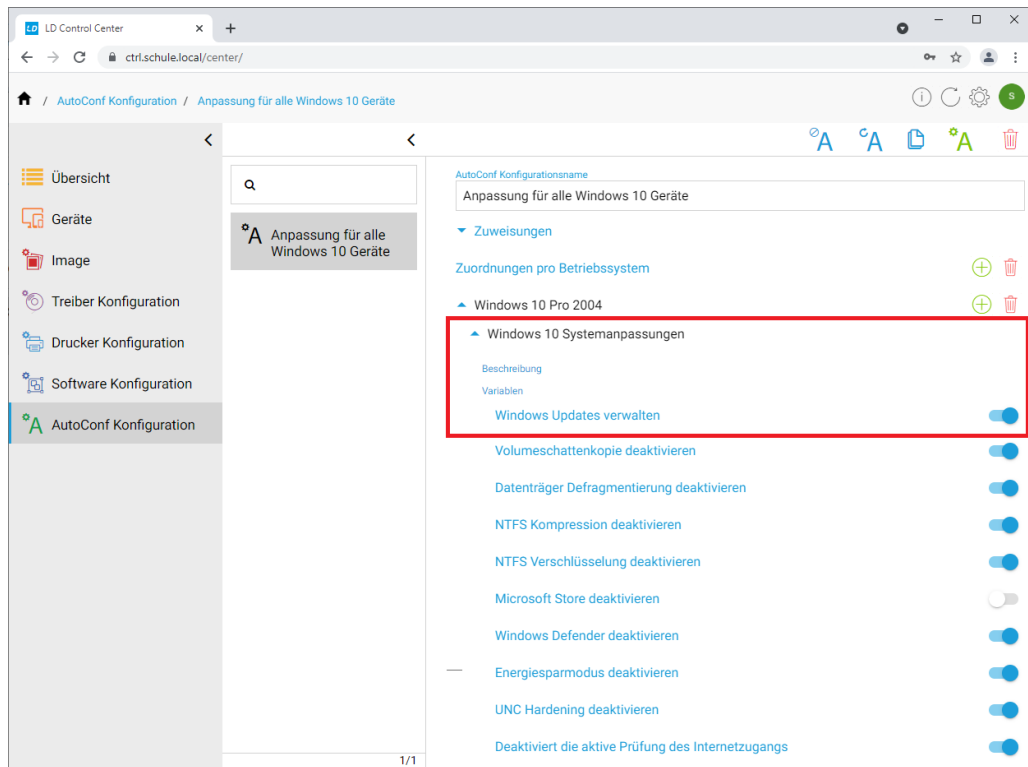
Wählen Sie in der linken Menüstruktur den Eintrag **Übersicht** und aus dem Baum im mittleren Menübereich die Organisationseinheit **computers**. Im rechten Menüfenster wählen Sie **AutoConf Konfiguration**. Über das grüne Verknüpfungssymbol verbinden Sie die zuvor erstellte Konfiguration und übernehmen mit **SPEICHERN**.



IV.1.7.4. Systemanpassungen für Windows 10

Die Rolle **Windows 10 Systemanpassungen** ist mit Abstand die wichtigste Rolle, wenn es darum geht, Windows 10 im Netzwerk in den Griff zu bekommen. Die Rolle und die darin getroffenen Einstellungen sind vor allem im Hinblick auf das Updateverhalten von Windows 10 entscheidend.

Aktivieren Sie den Schieberegler **Windows Updates verwalten**, um dafür zu sorgen, dass die Rechner im Netzwerk während des Betriebs bzw. Unterrichts nicht anfangen Windows-Updates herunterzuladen und das Internet lahmzulegen. Die Rolle sorgt umgekehrt bei Wechsel in den Audit-Modus dafür, dass Windows Updates explizit wieder möglich sind.

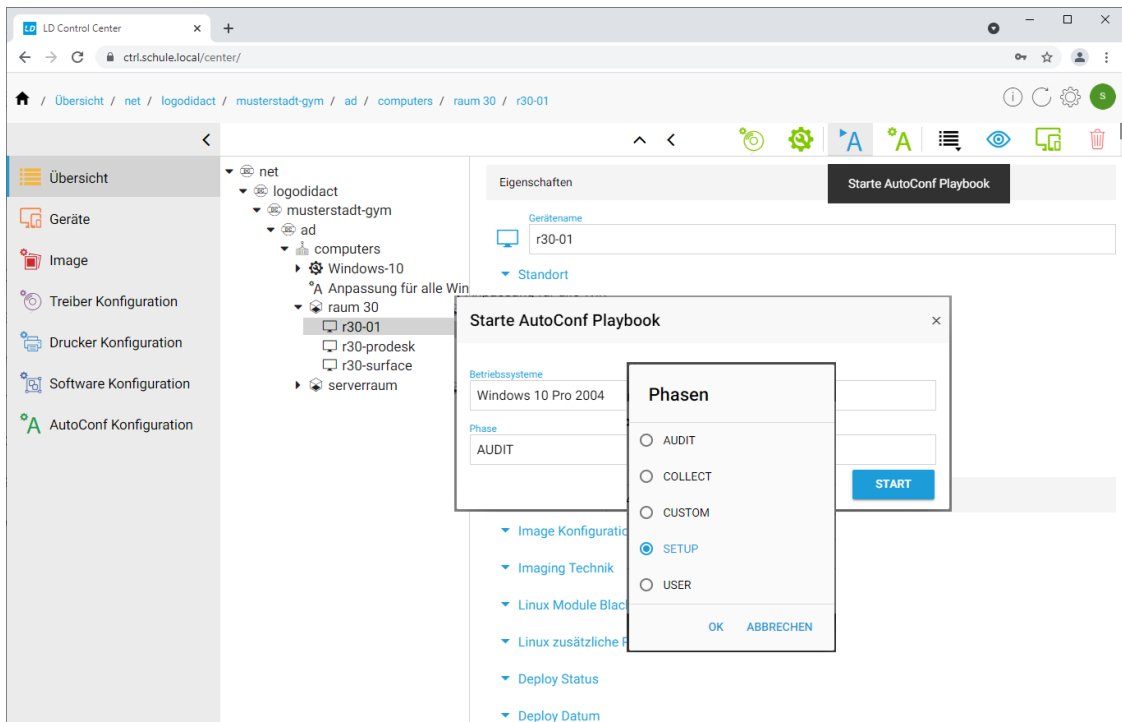


In der Rolle **Windows 10 Systemanpassungen** gibt es viele weitere Schieberegler über welche sinnvolle Anpassungen aktiviert werden können. Wenden Sie sich an Ihren zertifizierten LogoDI-DACT-Partner, der Sie bei der richtigen Konfiguration unterstützt.

IV.1.7.5. Anpassungen mit AutoConf anwenden und testen

Im Gegensatz zum alten Rembo/mySHN®, bei dem Systemanpassungen nur beim Neustart eine entsprechende Auswirkung hatten, arbeitet **LD Deploy** die Anpassungen mittels **AutoConf** dynamisch ab, wie das beispielsweise auch bei Gruppenrichtlinien der Fall ist. Die Anpassungen werden dabei in verschiedenen Phasen abgearbeitet.

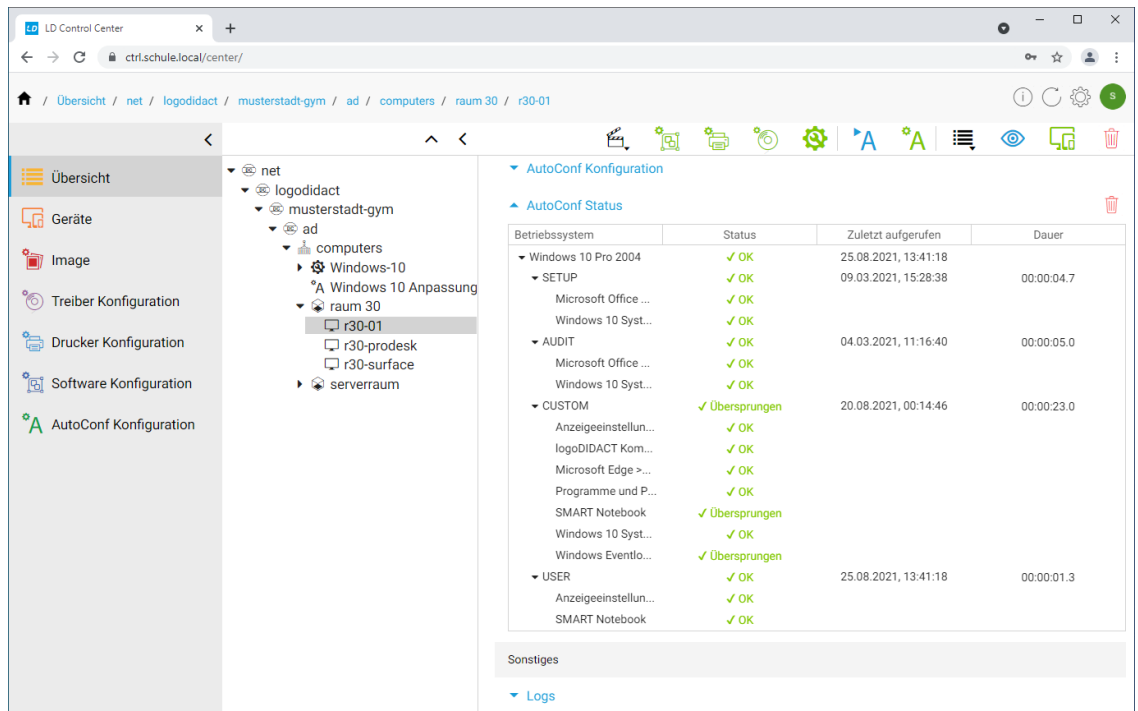
Um ein Playbook zu testen, wählen Sie in der linken Menüstruktur den Eintrag **Übersicht** aus und aus dem Baum im mittleren Fenster ein Gerät, an dem Sie die Anpassungen anwenden und testen wollen. Über das blaue AutoConf-Aktionssymbol öffnen Sie den Dialog zur Ausführung eines Playbooks.



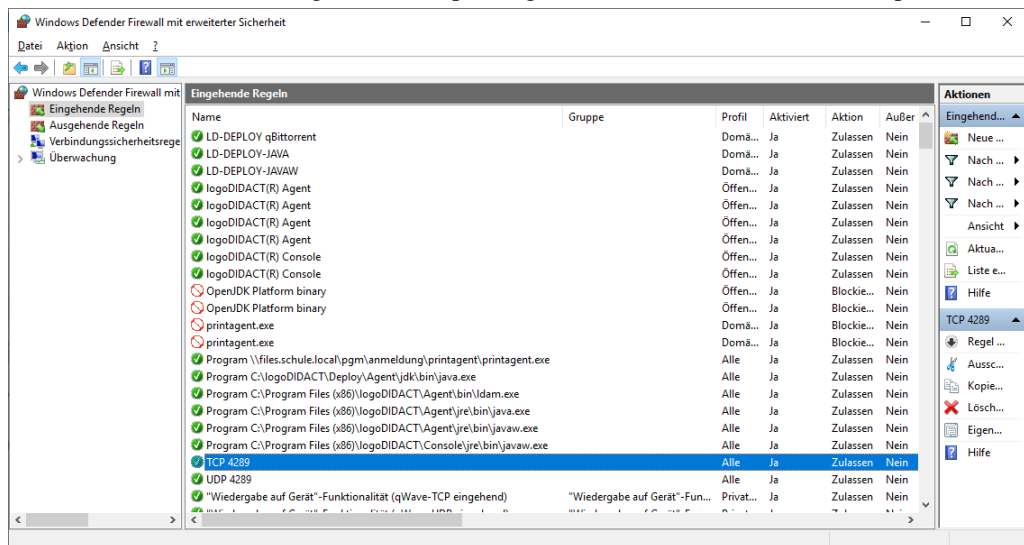
Klicken Sie in das Textfeld im Abschnitt **Phase**, wählen die passende Phase aus und übernehmen mit **OK**.

Klicken Sie nun auf **START** um die Abarbeitung am ausgewählten Client zu starten. Das Abarbeiten eines Playbooks kann sehr schnell gehen, aber auch mehrere Minuten Zeit in Anspruch nehmen. Das hängt davon ab, was in der jeweiligen Rolle definiert wird und ob dafür gegebenenfalls noch Zusatzsoftware installiert werden muss, um eine Aktion überhaupt ausführen zu können.

Um Informationen über den Status der Abarbeitung an einem Client zu bekommen, markieren Sie diesen im mittleren Menübaum und erweitern den Eintrag **AutoConf** im rechten Fenster. Sie können dabei nicht nur die vier verschiedenen Phasen **SETUP**, **AUDIT**, **CUSTOM** und **USER** erkennen, sondern auch, wann diese zuletzt durchlaufen wurden und ob die Abarbeitung erfolgreich war oder nicht.



Wenn Sie sich als Administrator an dem Client anmelden, an dem Sie das Playbook gerade angewandt haben, können Sie die durchgeführten Anpassungen an der Windows Firewall überprüfen.



IV.1.7.6. Drucker

Auch die Verwaltung von Druckern geschieht in **LD Deploy** im Hintergrund mittels **AutoConf**, jedoch mit einem eigenen Menüeintrag. Die Verwaltung und Konfiguration eines Druckers unterscheidet sich dabei vom Konzept her nicht vollkommen von der Art, wie das im alten System gemacht wurde:

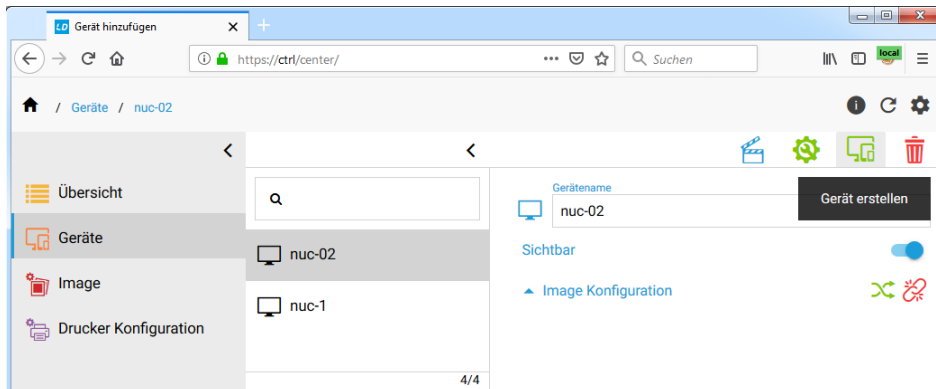
1. Aufnahme des Druckers als Gerät
2. Festlegung von logischem Druckernamen ("r30 - HP LaserJet 2100DN")
3. Festlegung des Standarddruckers

4. Zuordnung zu Räumen und Rechnern
5. Installation des Drucker am Client mit Imageerstellung

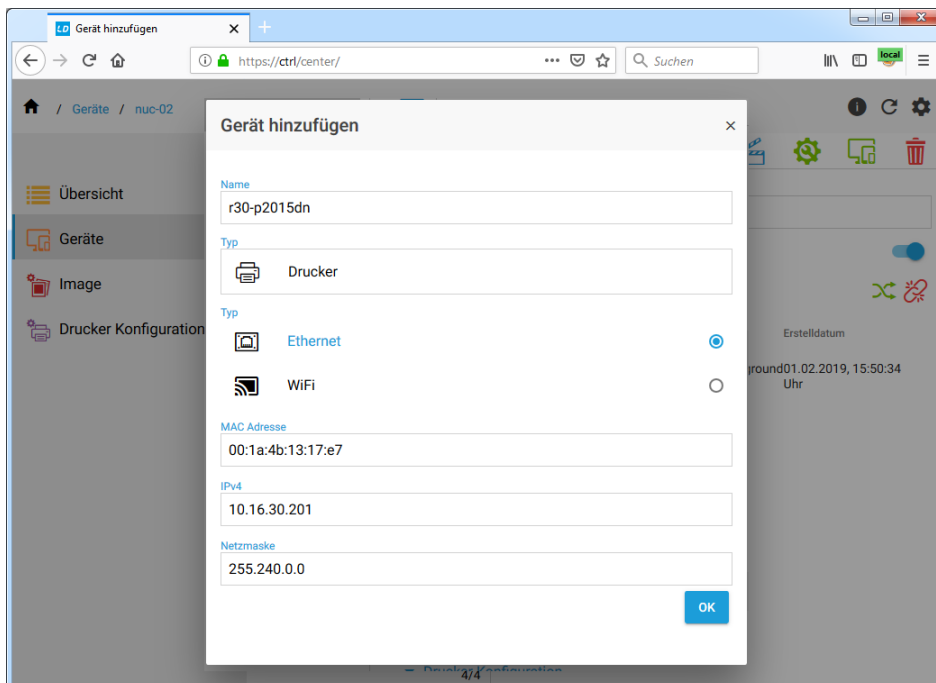
Die technische Umsetzung ist jedoch deutlich anders und in der Regel einfacher und flexibler.

IV.1.7.6.1. Aufnahme des Druckers im ControlCenter

Öffnen Sie das ControlCenter und melden Sie sich mit dem Benutzer **admin** und dessen Kennwort an. Wählen Sie im Hauptmenü auf der linken Seite den Eintrag **Geräte** und aus dem Symbolmenü am rechten oberen Bereich grüne Gerätesymbol, um ein neues Betriebssystem anzulegen.



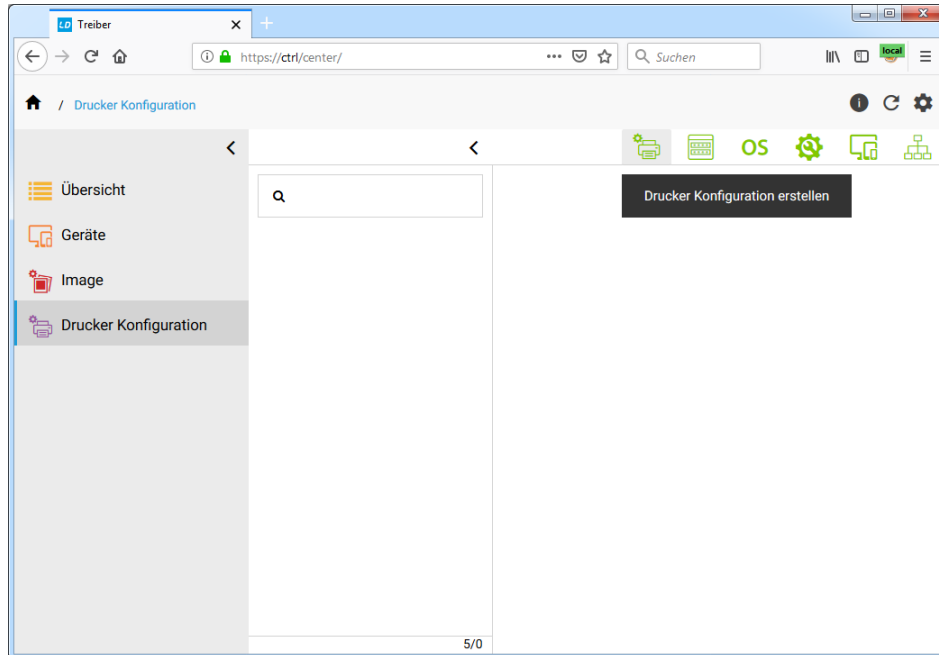
Geben Sie dann die Daten des Druckers ein. Bitte beachten Sie, dass Sie beim Namen entsprechend der Konvention für Geräte keine Leerzeichen oder Sonderzeichen verwenden dürfen und grundsätzlich Kleinbuchstaben verwenden müssen. Übernehmen Sie die Daten mit **OK**.



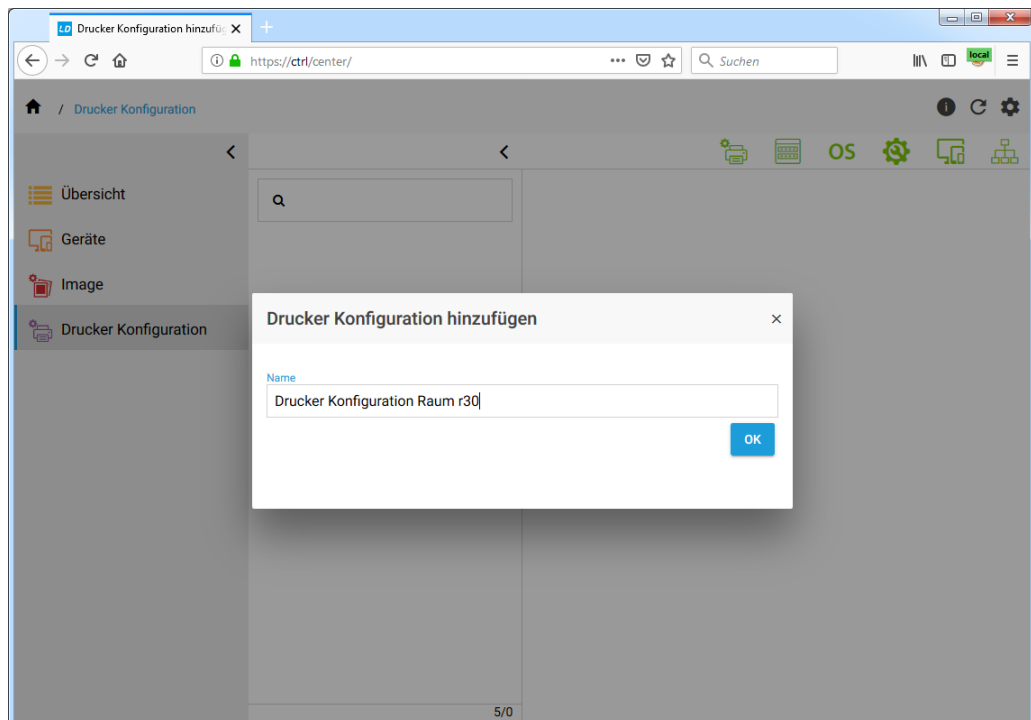
Bei Aufnahme eines Gerätes im ControlCenter wird im Hintergrund automatisch ein Import durchgeführt, so dass die neue IP-Adresse als Reservierung im DHCP-Server des **logosrv** gespeichert wird.

IV.1.7.6.2. Erstellen einer Druckerkonfiguration

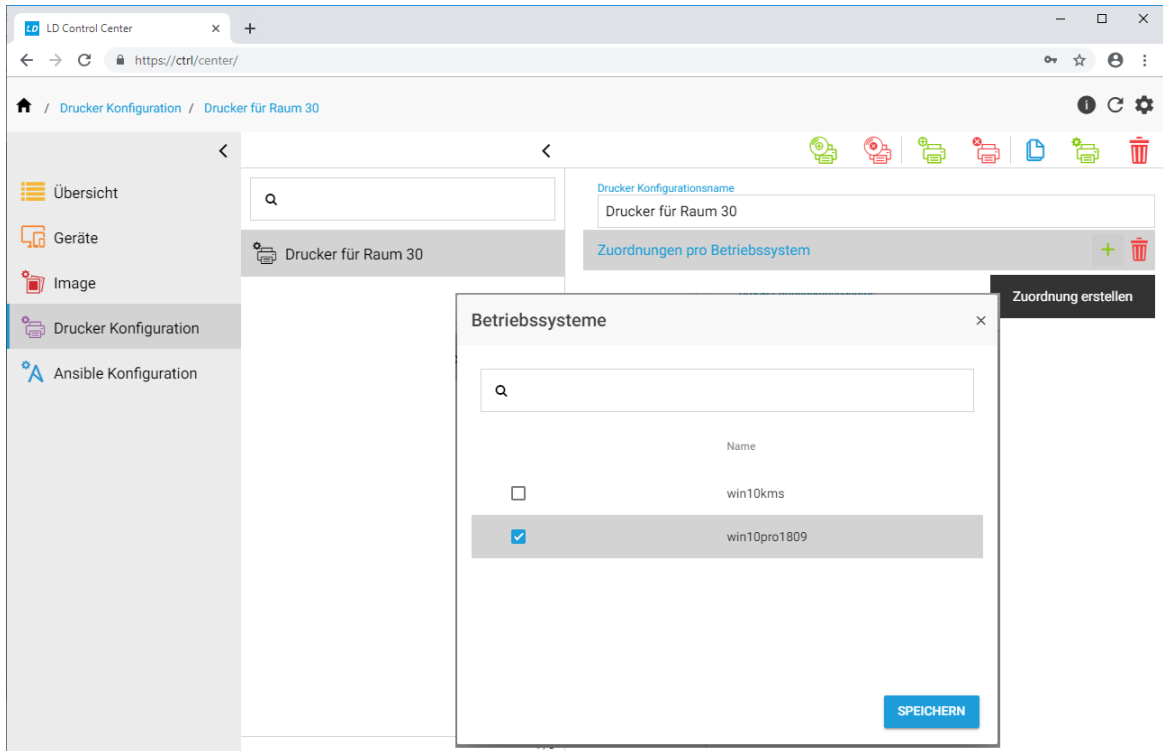
Typischerweise erstellt man Druckerkonfigurationen auf Raumbene und hat dort einen oder mehrere Drucker, wobei üblicherweise ein bestimmter Drucker automatisch als Standarddrucker definiert sein soll. Genau diese Dinge werden im ControlCenter über das Menü **Drucker Konfiguration** gesteuert. Wählen Sie im Hauptmenü auf der linken Seite diesen Eintrag aus und aus dem Symbolmenü am rechten oberen Bereich das grüne Druckersymbol.



Vergeben Sie einen aussagekräftigen Namen für die Konfiguration, die sich im Normalfall an Räumen oder einzelnen Rechnern orientiert.

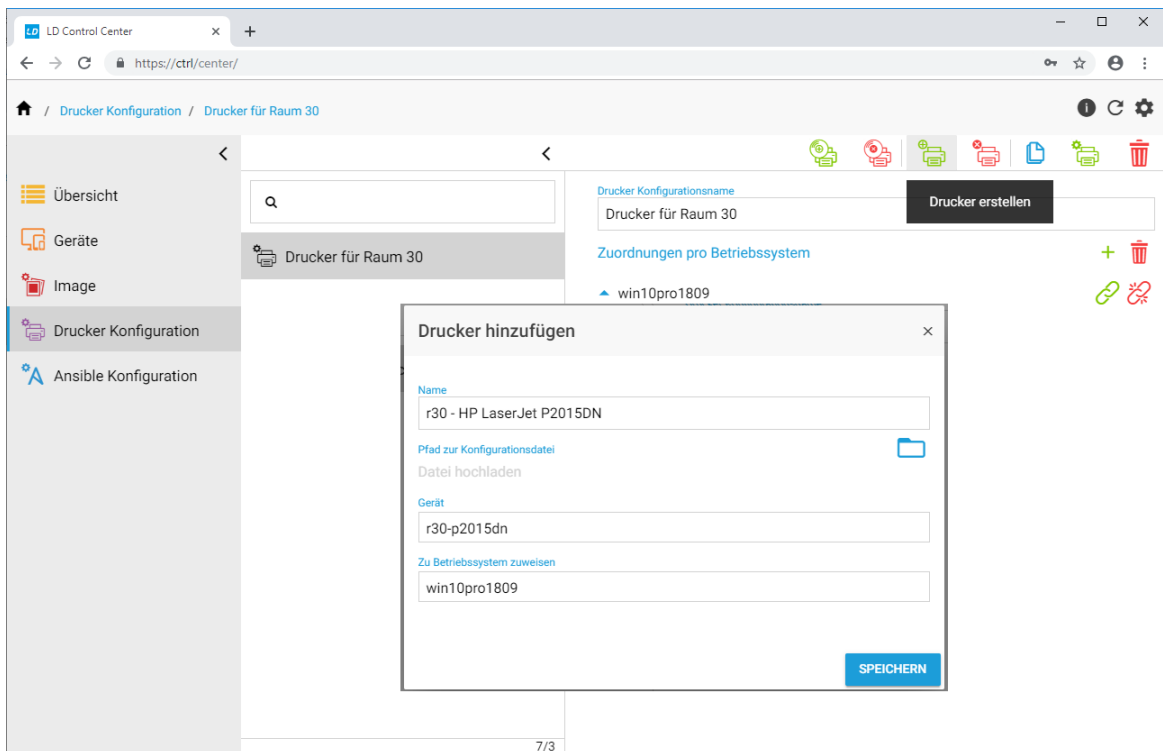


Ordnen Sie der Druckerkonfiguration anschliessend ein Betriebssystem zu.




IV.1.7.6.3. Erstellen eines logischen Druckerobjekts

Im Gegensatz zum physischen Drucker, der bei der Geräteaufnahme mit IP und MAC-Adresse erstellt wurde, wird beim Erstellen eines Druckers das gemacht, was man in Windows am Client sieht, also konkret der Name des Druckers.



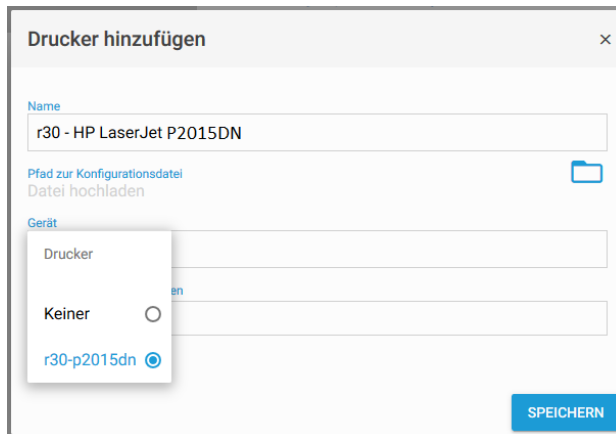
Der Name des Druckers muss bei der späteren Installation unter Windows 10 exakt so benannt werden, wie Sie ihn hier im Feld **Name** eingegeben haben.



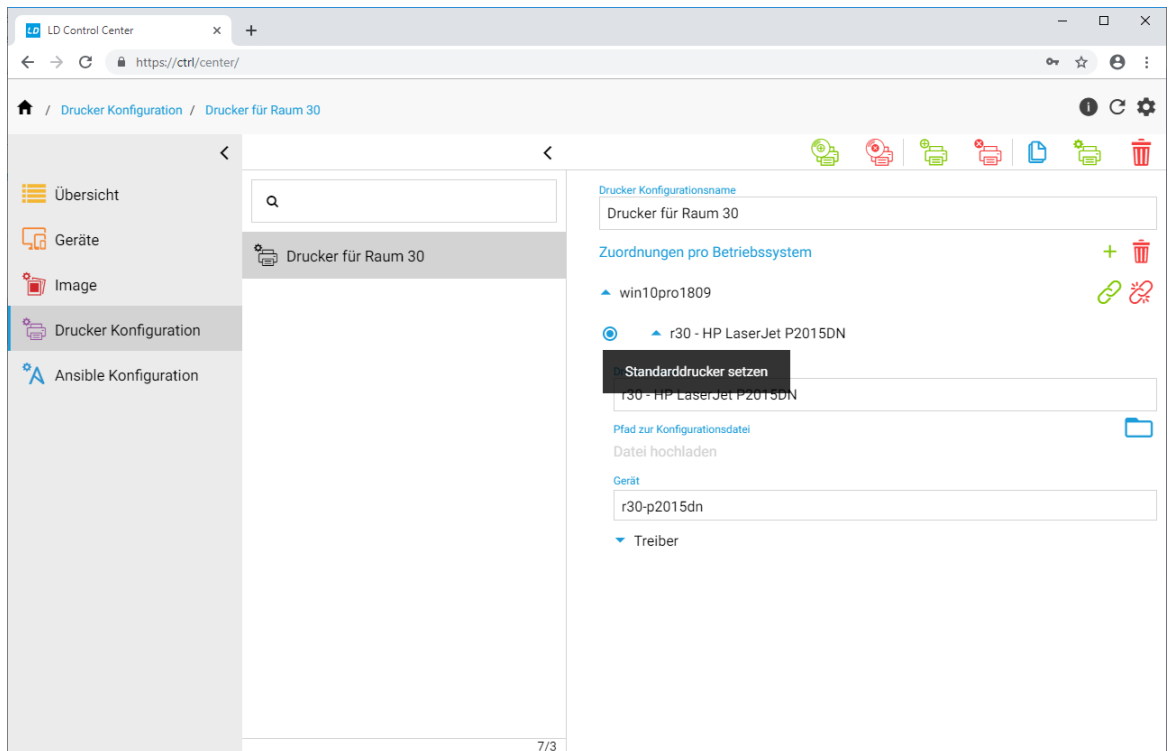
Tipp

Um Fehler zu vermeiden ist es am besten, wenn Sie den Namen des Druckers am Windows-Client aus dem ControlCenter kopieren und beim Druckernamen einfügen.

Nachdem Sie den Namen kopiert haben, klicken Sie in das Feld **Gerät** und wählen Sie das Gerät aus, mit dem Sie den Druckernamen verbinden wollen und übernehmen Sie mit **SPEICHERN**.

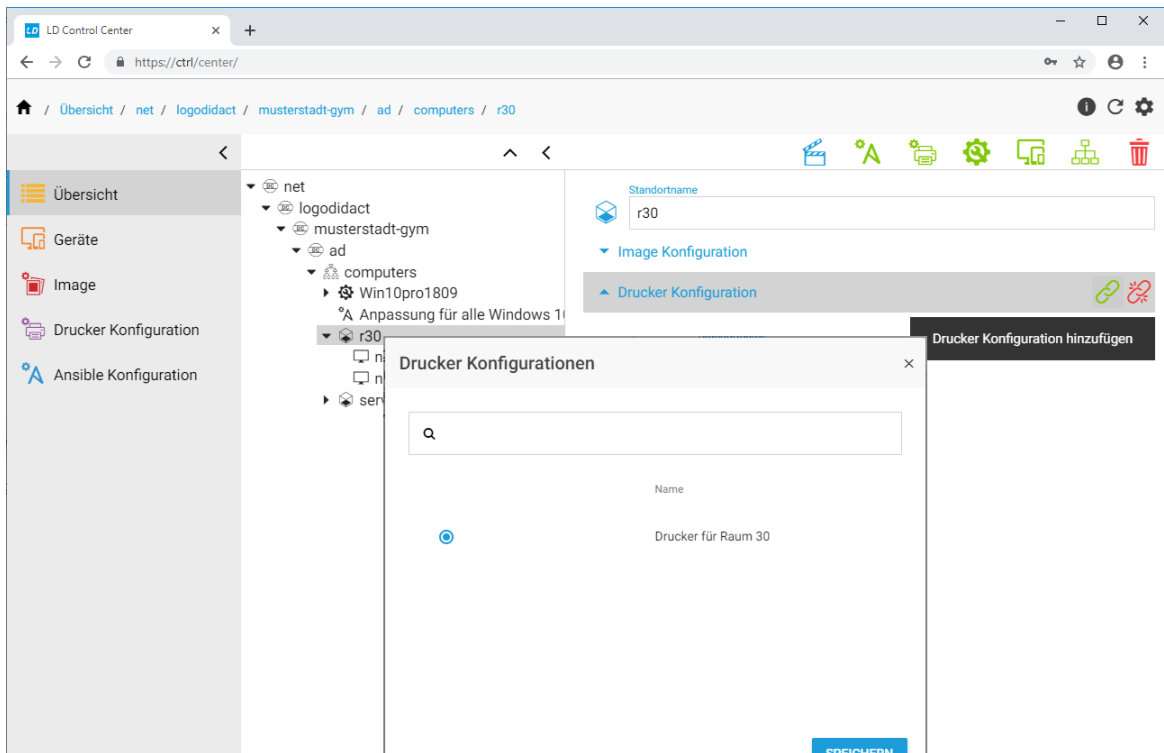


Im letzten Schritt legen Sie den Standarddrucker fest.



IV.1.7.6.4. Zuordnung der Druckerkonfiguration zum Raum

Wie bereits oben erwähnt, werden Drucker in der Regel auf Raumebene definiert, weshalb dies hier beispielhaft so gezeigt wird. Dazu wählt man wieder im linken Menü den Eintrag **Übersicht** und navigiert im mittleren Fenster in der Baumstruktur zum entsprechenden Raum (hier r30). Im rechten Fenster des ControlCenters wählt man den Eintrag **Drucker Konfiguration** und klickt auf das grüne Verknüpfungs-Symbol. Im Dialog wählt man dann die zuvor erstellte Konfiguration aus und übernimmt diese mit **SPEICHERN**.



In großen Umgebungen mit entsprechend vielen Drucker-Konfigurationen kann man diese über das Suchfeld einschränken. Auch deshalb ist es sinnvoll, in den Raumkonfigurationen immer den Raumnamen mit anzugeben, so dass man entsprechend gezielt danach suchen kann.

IV.1.7.6.5. WS-Discovery auf Druckern deaktivieren

Bevor Sie mit der Installation der Netzwerk-Druckers in Windows 10 beginnen, sollten Sie an jedem Netzwerkdrucker die Funktion **WS-Discovery** deaktivieren.

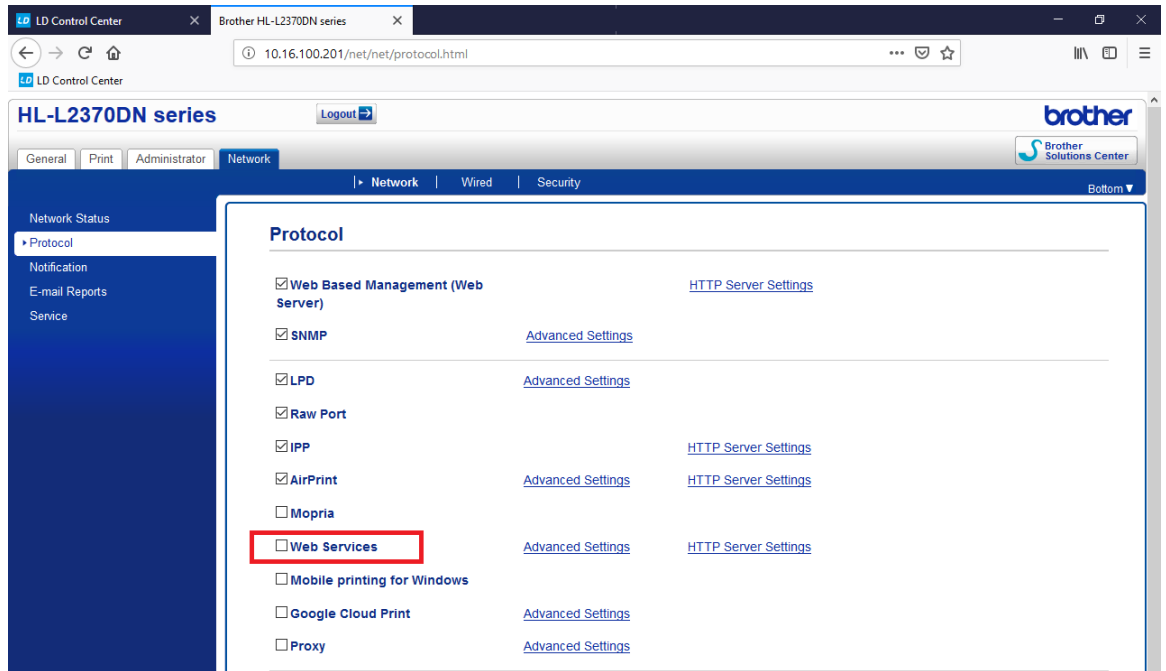


Achtung

Vollkommen unabhängig von LogoDIDACT oder **LD Deploy** verursacht die Funktion der dynamischen Druckererkennung per **WS-Discovery** in Windows 10 nur Probleme und Ärger. Ältere Drucker beherrschen dieses Protokoll zum Glück nicht, so dass es damit in der Regel auch keine Probleme gibt.

Ohne dass man es bemerkt, stellt Windows 10 einen bereits per TCP/IP konfigurierten Drucker auf WSD um, was zu absurden Szenarien führt, vor allem bei einer typischen Umgebung mit alten und neuen Druckern.

Je nach Druckermodell wird das Protokoll etwas unterschiedlich bezeichnet, taucht aber in jedem Fall im Bereich der Netzwerkeinstellungen unter den Protokollen auf. Deaktivieren Sie diese Funktion, indem Sie das entsprechende Häkchen entfernen und die Änderung speichern bzw. übernehmen.



IV.1.7.6.6. Installation des Druckers an einer Arbeitsstation

Gehen Sie an eine Windows 10 Arbeitsstation. Melden Sie sich mit dem administrativen Benutzer **admin** an der Domäne an. Wechseln Sie in den Installations-Modus (Audit-Modus), wie in Abschnitt IV.1.4.5.2, „In den Audit Modus wechseln“ beschrieben.

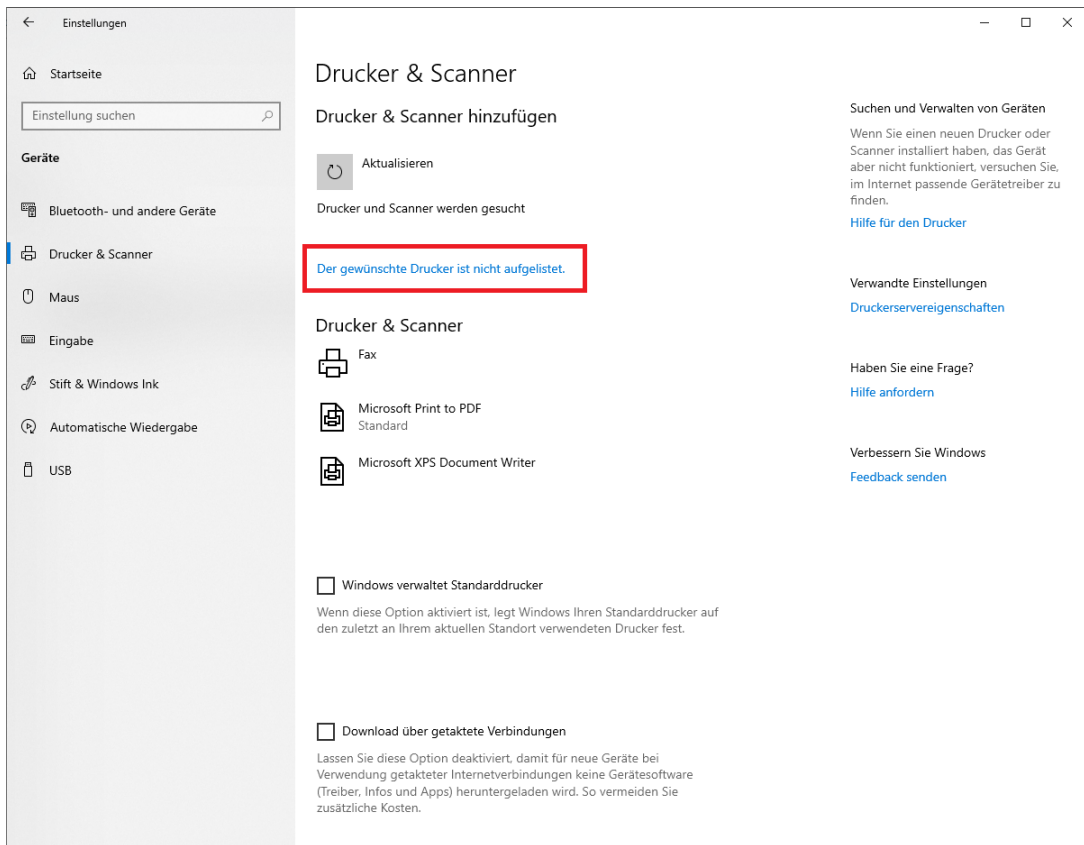


Achtung

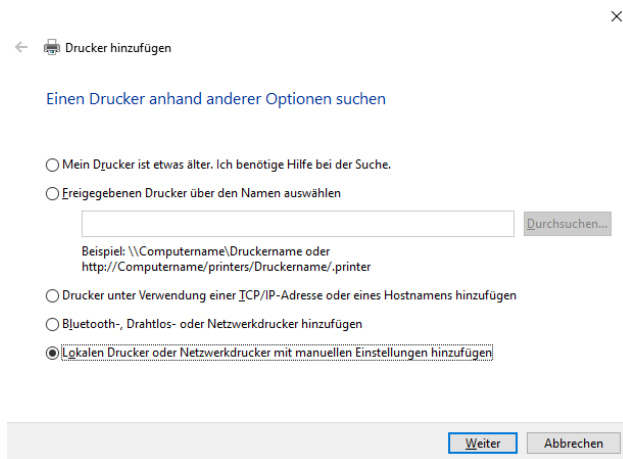
Bitte beachten Sie, dass Sie in der neuesten Version von **LD Deploy** direkt in den **Audit Mode** wechseln können und der Rechner danach zwei Mal automatisch neu startet!

Bitte warten Sie den zweiten Neustart ab und melden Sie sich **nicht** an!

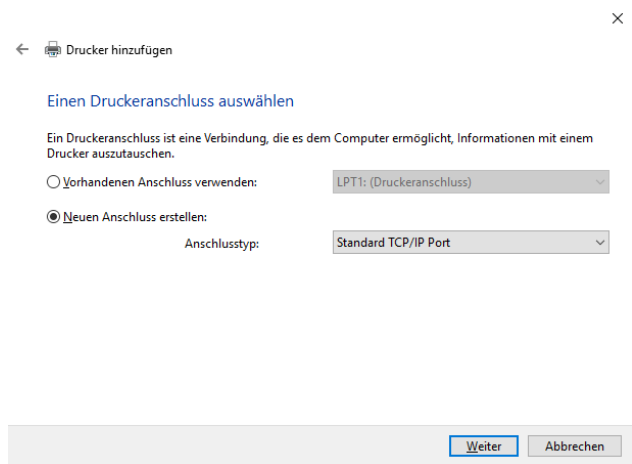
Fügen Sie einen neuen Drucker über die Systemeinstellungen von Windows 10 hinzu. Falls Sie WS-Discovery noch nicht deaktiviert habe, holen Sie das unbedingt vor der Installation des Druckers nach.



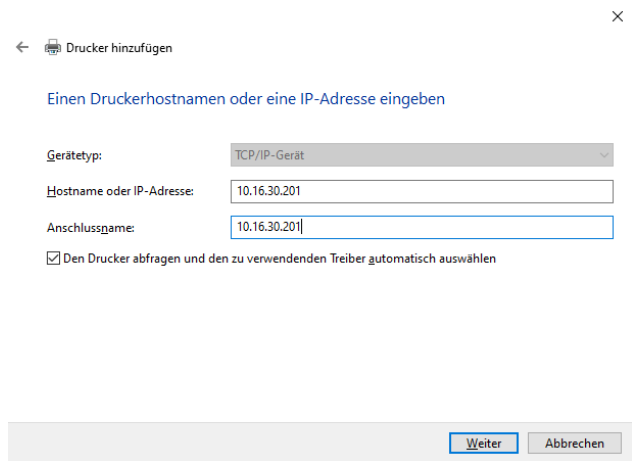
Wählen Sie **Lokalen Drucker oder Netzwerkdrucker mit manuellen Einstellungen hinzufügen** und klicken Sie auf **Weiter**.



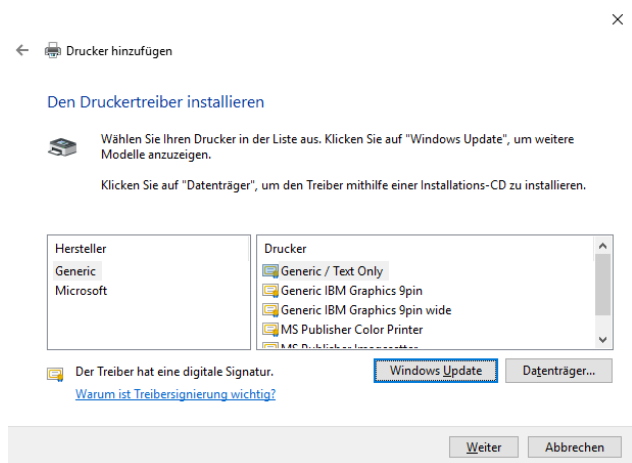
Erstellen Sie einen neuen Anschluss vom Typ **Standard TCP/IP Port** und klicken Sie auf **Weiter**.



Tragen Sie die IP-Adresse des Druckers ein und klicken Sie auf **Weiter**.



Wählen Sie den Druckertreiber aus, den Sie auf der Supportseite des Druckerherstellers zuvor heruntergeladen haben und klicken Sie auf **Weiter**. Warten Sie ab, bis der Druckertreiber installiert wurde.



Geben Sie nun dem Drucker exakt den Namen, den Sie im ControlCenter zuvor festgelegt haben. Um Fehler zu vermeiden, ist es am einfachsten, wenn Sie ins ControlCenter wechseln und die Bezeichnung dort über die Zwischenablage kopieren und im Druckerdialog einfügen. Bestätigen Sie mit **Weiter**.

← Drucker hinzufügen ×

Geben Sie einen Druckernamen ein

Druckername:

Dieser Drucker wird mit dem HP Universal Printing PCL 6 (v6.7.0)-Treiber installiert.

Wählen Sie **Drucker nicht freigeben** und klicken Sie auf **Weiter**.

← Drucker hinzufügen ×

Druckerfreigabe

Wenn dieser Drucker freigegeben werden soll, müssen Sie einen Freigabennamen angeben. Sie können den vorgeschlagenen Namen verwenden oder einen neuen eingeben. Der Freigabename wird anderen Netzwerkbenutzern angezeigt.

Drucker nicht freigeben

Drucker freigeben, damit andere Benutzer im Netzwerk ihn finden und verwenden können

Freigabename:

Standort:

Kommentar:

Ob Sie im folgenden Dialog den Drucker als Standarddrucker festlegen oder nicht, spielt keine Rolle, weil dies so oder so, über die Konfiguration im ControlCenter festgelegt ist und über **AutoConf** am Windows 10 Client angepasst wird. In jedem Fall sollten Sie jedoch eine Testseite drucken, um zu prüfen, ob der richtige Treiber installiert wurde und Sie die richtigen Exckdaten eingetragen haben. Klicken Sie zum Abschluss auf **Fertig stellen**.

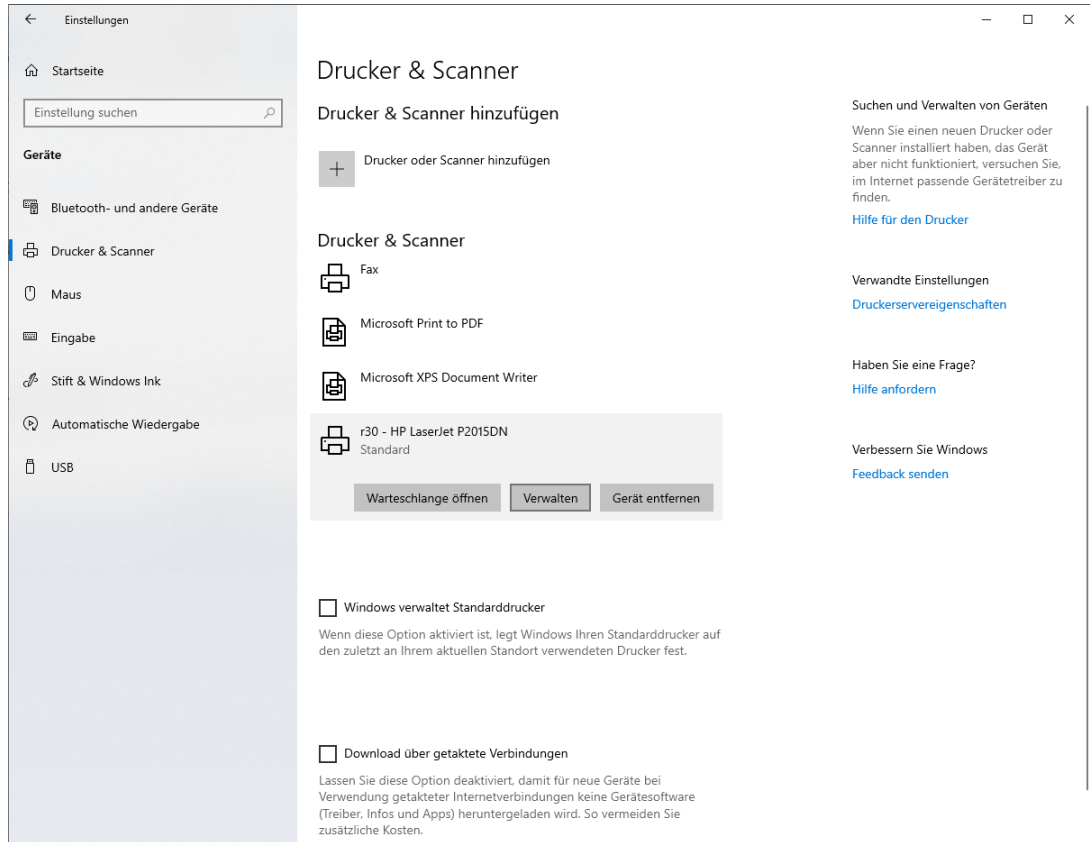
← Drucker hinzufügen ×

r30 - HP LaserJet P2015DN wurde erfolgreich hinzugefügt.

Als Standarddrucker festlegen

Drucken Sie eine Testseite, um zu überprüfen, ob der Drucker funktionsfähig ist, oder um Informationen zur Problembehandlung für den Drucker anzuzeigen.

Der Drucker ist nun im Image installiert und die Konfiguration im ControlCenter erfolgt, so dass Sie von diesem Zustand ein Image erstellen können.



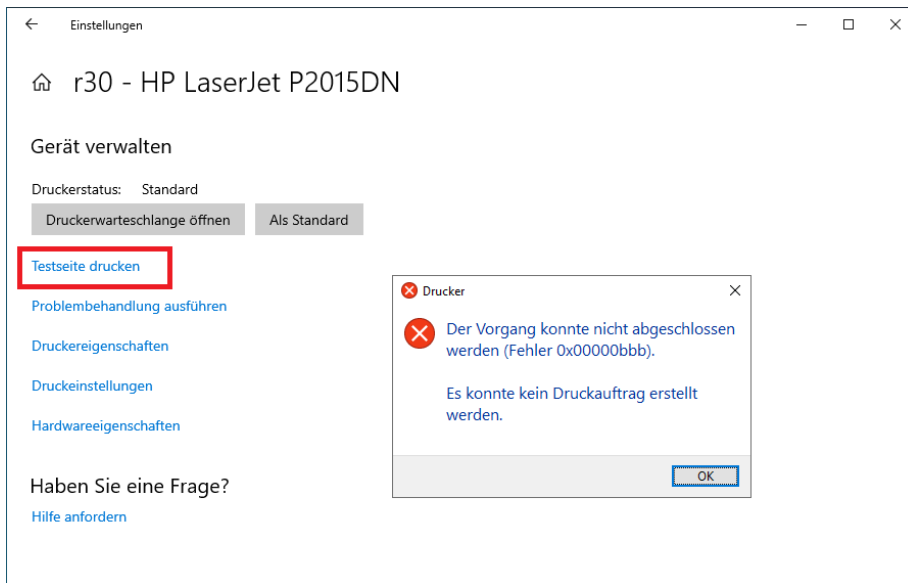
Achtung

Prüfen Sie die Druckerkonfiguration unmittelbar vor der Erstellung eines Images nochmals dahingehend, dass die Ports auf TCP/IP stehen. Sofern Windows 10 eine Umstellung per WS-Discovery auf eine WSD Druckerkonfiguration durchgeführt hat, ändern Sie diese wieder auf TCP/IP und löschen Sie die WSD Konfiguration!

Bitte beachten Sie, dass es in Windows 10 Version 1903 beim Ausdruck einer Testseite einen Bug gibt, der im nächsten Abschnitt erläutert wird.

IV.1.7.6.7. Fehler bei Testseite drucken in Windows 10 Version 1903

In der aktuellsten Windows 10 Version 1903 gibt es einen Fehler beim Versuch eine Testseite zu drucken, unmittelbar nachdem man den Drucker bzw. Druckertreiber am Client installiert hat. Diesen Fehler gibt es in Windows 10 Version 1809 mit dem gleichen Treiber und Drucker reproduzierbar nicht. Die genaue Ursache ist derzeit (10/2019) unbekannt.



Achtung

Sie können diesen Fehler ignorieren und wie gewohnt ein Image erstellen und verteilen. Der Fehler tritt nach dem Deployment nicht mehr auf!

IV.1.7.7. SMART-Board Kalibrierung und Lizenzierung

Da man in der Regel pro Raum ein Whiteboard hat, könnte man annehmen, dass man eine Konfiguration ebenfalls auf Raumebene erstellt oder sogar individuell pro Rechner, da ja die Kalibrierung individuell zwischen Rechner und Board erfolgt.

Das ist aber keinesfalls so!



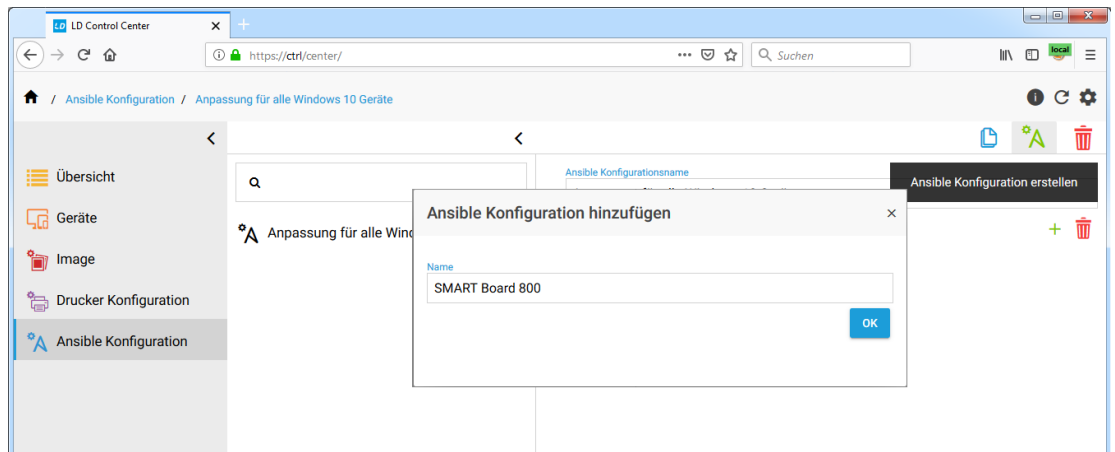
Achtung

Die Definition einer Ansible-Konfiguration für SMART-Boards ist vielmehr davon abhängig, ob man verschiedene SMART-Boards mit unterschiedlichen Auflösungen betreibt. Sofern es baugleiche SMART-Boards an der Schule gibt, die alle mit der gleichen Auflösung betrieben werden, kann man dafür eine einzige Konfiguration für alle Boards erstellen.

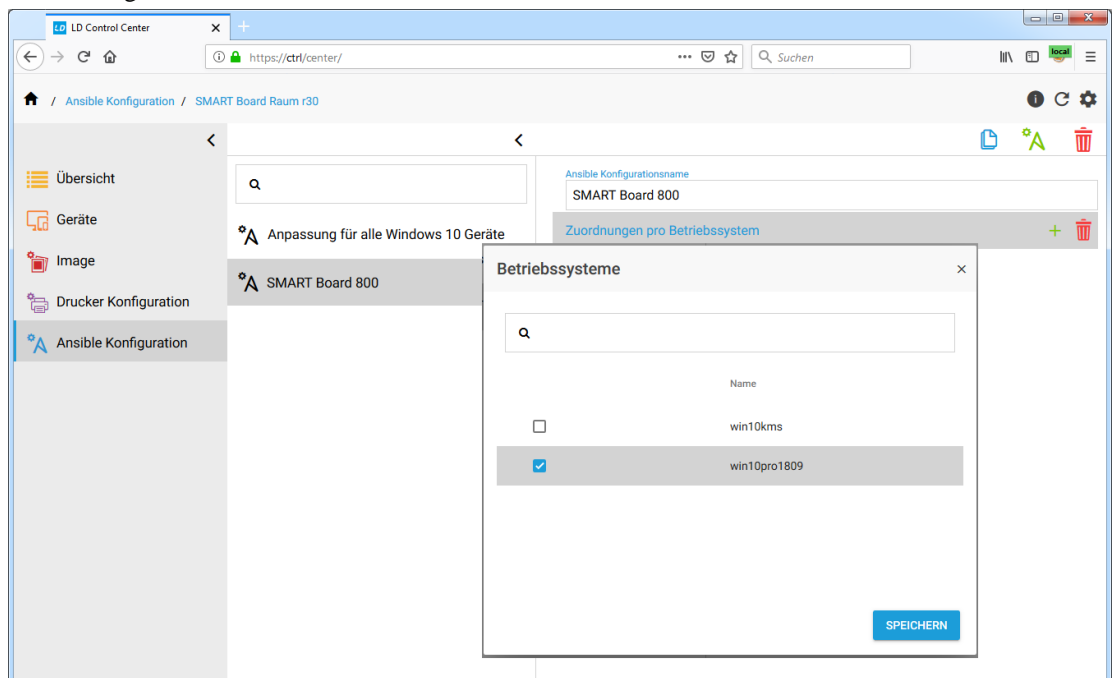
IV.1.7.7.1. Erstellen einer SMART-Board Konfiguration

Erstellen Sie zunächst eine neue Ansible-Konfiguration. Öffnen Sie das ControlCenter und wählen Sie aus dem Menü auf der linken Seite den Eintrag **Ansible Konfiguration** und aus der Menüleiste im oberen rechten Bereich das grüne Symbol zur Erstellung einer neuen Ansible Konfiguration. Geben Sie der Konfiguration einen aussagekräftigen Namen und bestätigen Sie mit **OK**.

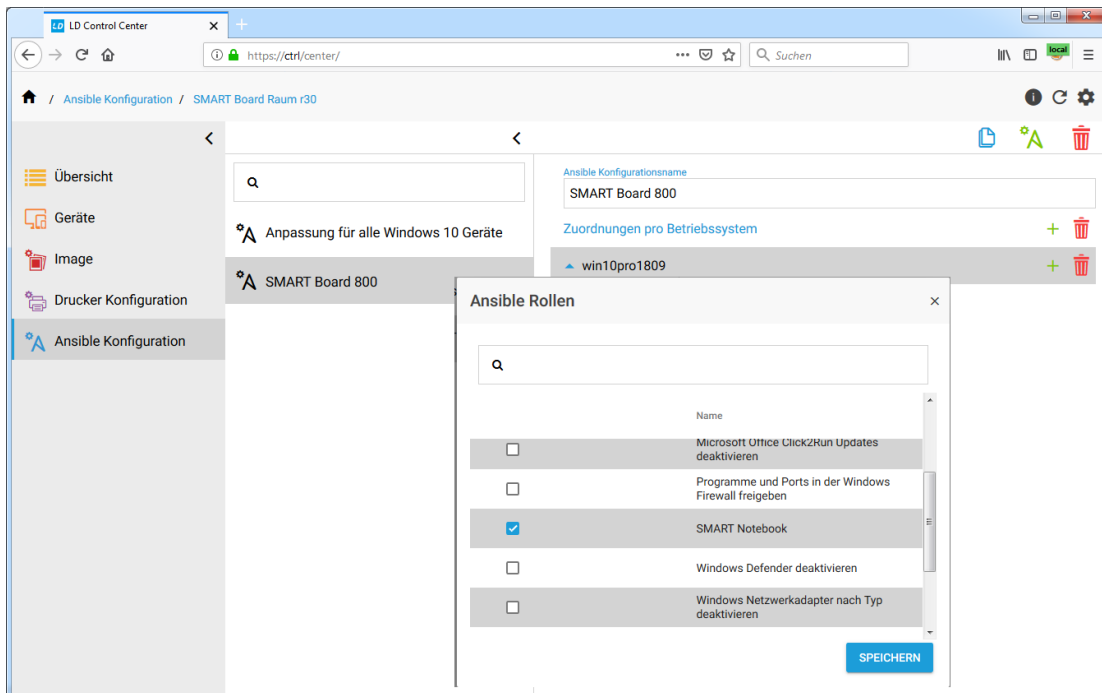
Eine Bezeichnung wie "SMART Board 800" wie im Beispiel ist z.B. dann passend, wenn Sie mehrere dieser Modelle in unterschiedlichen Räumen im Einsatz haben.



Markieren Sie im mittleren Menübereich die gerade erstellte Konfiguration und legen Sie die Verbindung zum passenden Betriebssystem fest. Klicken Sie dazu im rechten Fensterbereich auf **Zuordnung pro Betriebssystem**. Markieren Sie im darauf erscheinenden Dialog das System (hier win10pro1809) und bestätigen Sie mit **SPEICHERN**.

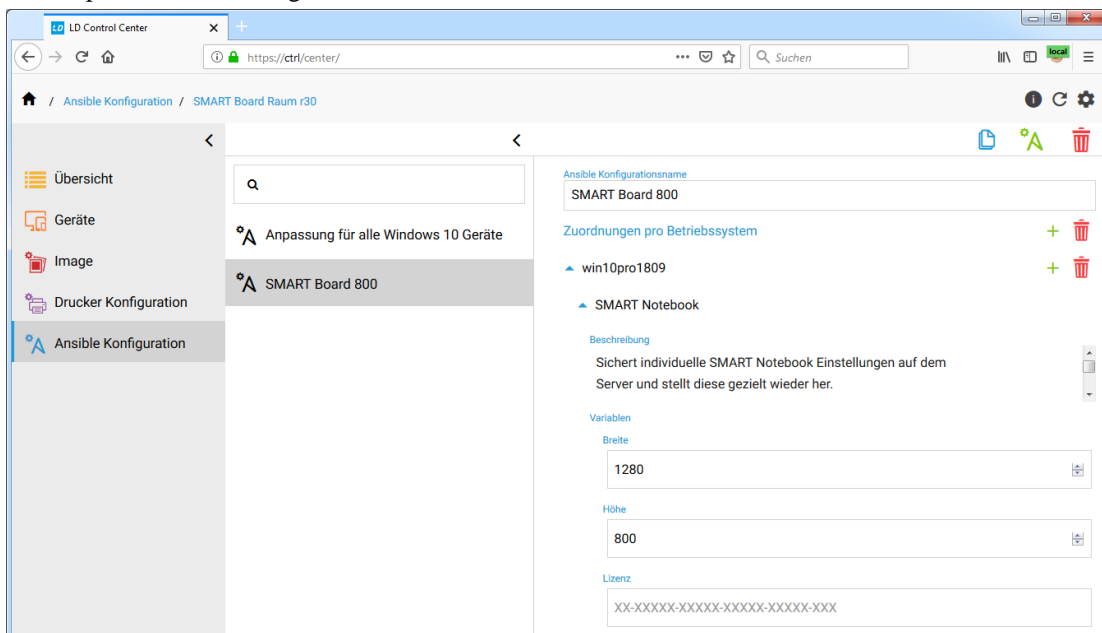


Fügen Sie im letzten Schritt die Rolle **SMART Notebook** hinzu und übernehmen Sie mit **SPEICHERN**.



IV.1.7.7.2. Board-Parameter festlegen und Lizenz eintragen

Markieren Sie im rechten Menübereich die gerade zugewiesene Rolle **SMART Notebook** und tragen Sie die passende Auflösung für das Whiteboard ein, sowie die Lizenz für die Software.

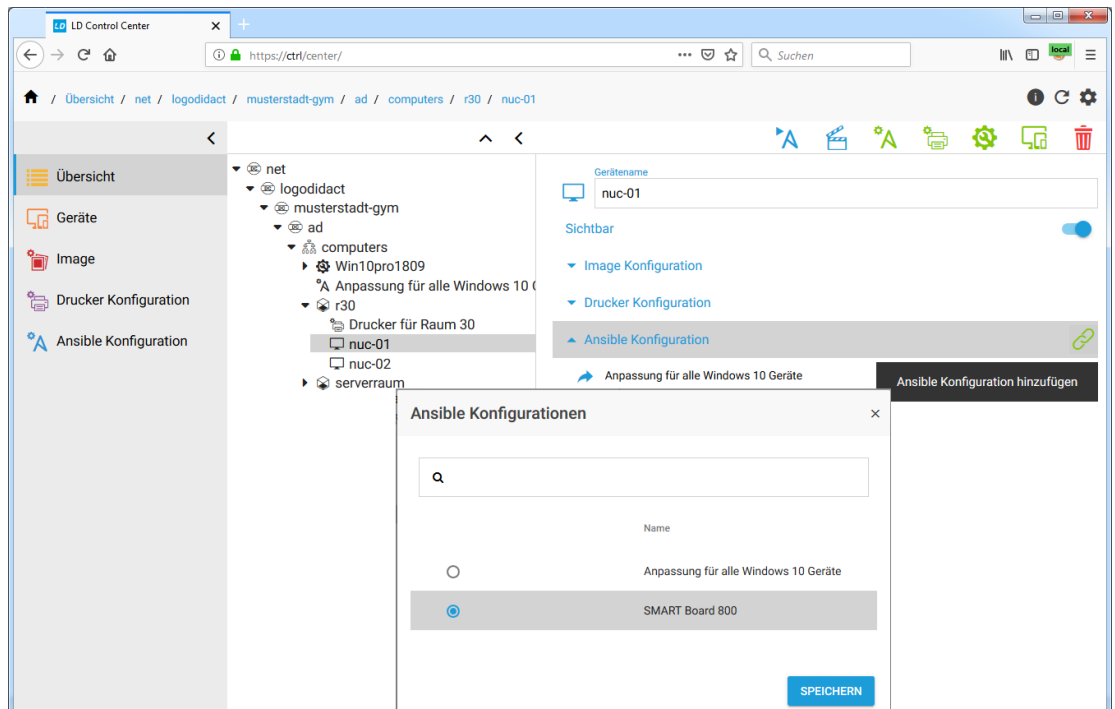


IV.1.7.7.3. SMART-Board Konfiguration einem Rechner zuweisen

Ordnen Sie nun diese Konfiguration denjenigen Rechnern individuell zu, die ein SMART-Board dieses Typs ansteuern. Im folgenden Beispiel, ist das der Rechner mit der Bezeichnung nuc-01.

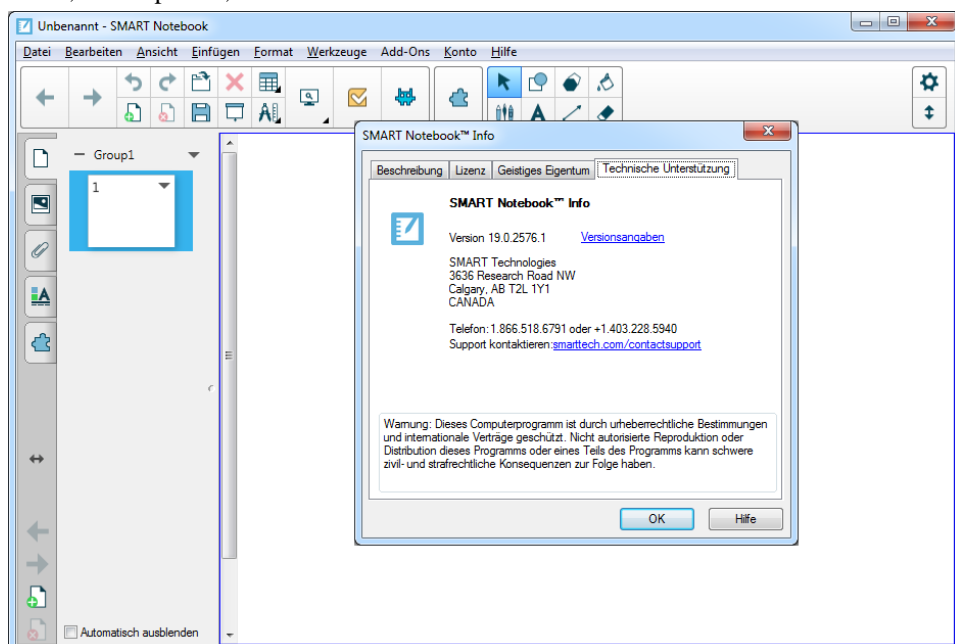
Dazu wählt man wieder im linken Menü den Eintrag **Übersicht** und navigiert im mittleren Fenster in der Baumstruktur zum entsprechenden Rechner (hier nuc-01). Im rechten Fenster des ControlCenters

wählt man den Eintrag **Ansible Konfiguration** und klickt auf das grüne Verknüpfungs-Symbol am rechten Rand. Im Dialog wählt man dann die zuvor erstellte Konfiguration aus und übernimmt diese mit **SPEICHERN**.



IV.1.7.7.4. Installation der SMART-Board Software

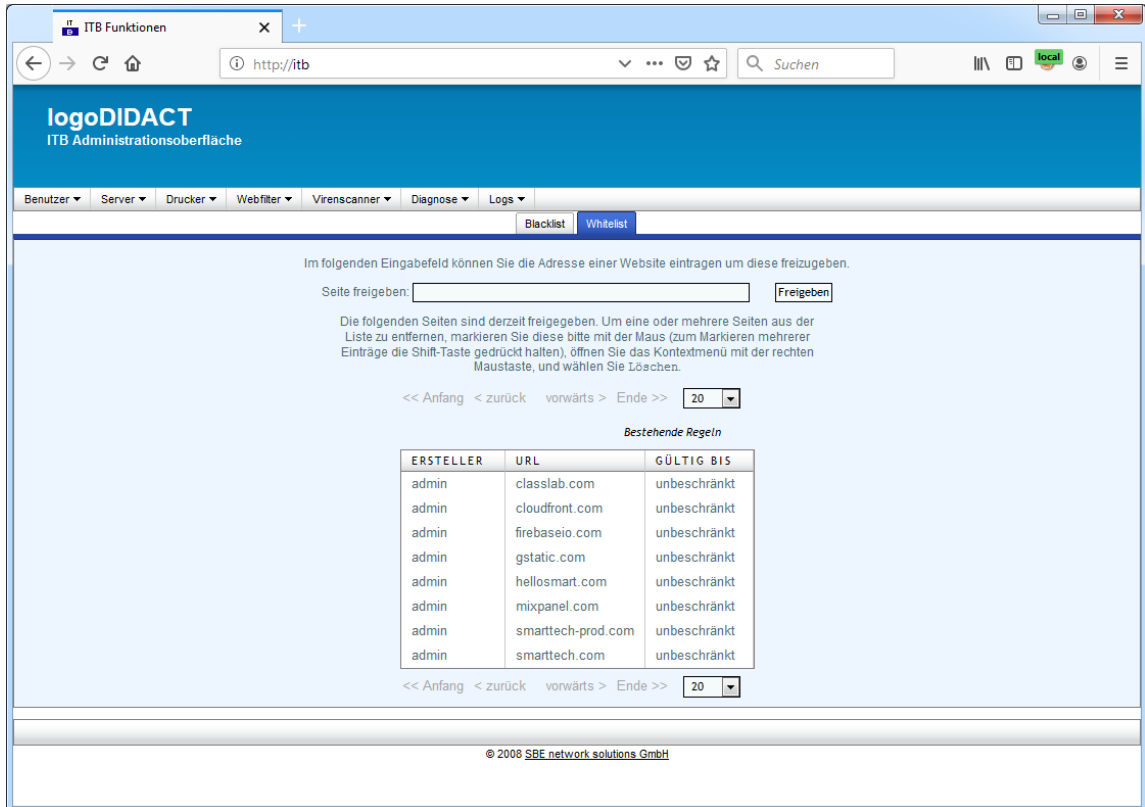
Im nächsten Schritt geht man an den Rechner, an dem das SMART-Board angeschlossen ist, meldet sich als Administrator an, wechselt in den **Audit-Mode** und installiert die SMART-Notebook-Software entsprechend den Anweisungen des Herstellers. Starten Sie jedoch die Software nach der Installation, um zu prüfen, dass diese korrekt installiert ist.



Sie brauchen bei der Installation weder die Lizenz einzugeben, noch ihr erstes Board zu kalibrieren!
Erstellen Sie dann ein Image.

IV.1.7.7.5. Webfilter für Lizenzierung anpassen

Damit die SMART-Software korrekt lizenziert und aktiviert werden kann, ist es erforderlich einige Seiten im Webfilter auf die Whitelist zu setzen. Gehen Sie dazu in das ITB-Interface und melden Sie sich mit dem Benutzer **Admin** an.



Laut Anwenderhandbuch von SMART, sollen die folgenden URLs zur Whitelist hinzugefügt werden:

smarttech.com

smarttech-prod.com

hellosmart.com

classlab.com

gstatic.com (wird von Google zum Laden von reCAPTCHA verwendet)

google.com

firebaseio.com

cloudfront.com

mixpanel.com

Wenden Sie sich bei Problemen an den Hersteller oder Lieferanten!

IV.1.7.7.6. Image aufspielen und Lizenzierung prüfen

Nach dem Auspielen des Images werden in der Phase der Ansible-Automatisierung die im Control-Center hinterlegte Lizenz auf den jeweiligen Rechner übertragen. Das passiert für die Rolle **SMART Notebook** in der Phase **CUSTOM**, wie man anhand der so genannten **Tags** im Abschnitt **Informationen** sieht.

▲ SMART Notebook

Beschreibung
Sichert individuelle SMART Notebook Einstellungen auf dem Server und stellt diese gezielt wieder her.

Variablen

Breite
1280

Höhe
800

Lizenz
[REDACTED]

▲ Informationen

Name
SMART Notebook

Tags
COLLECT, CUSTOM, USER

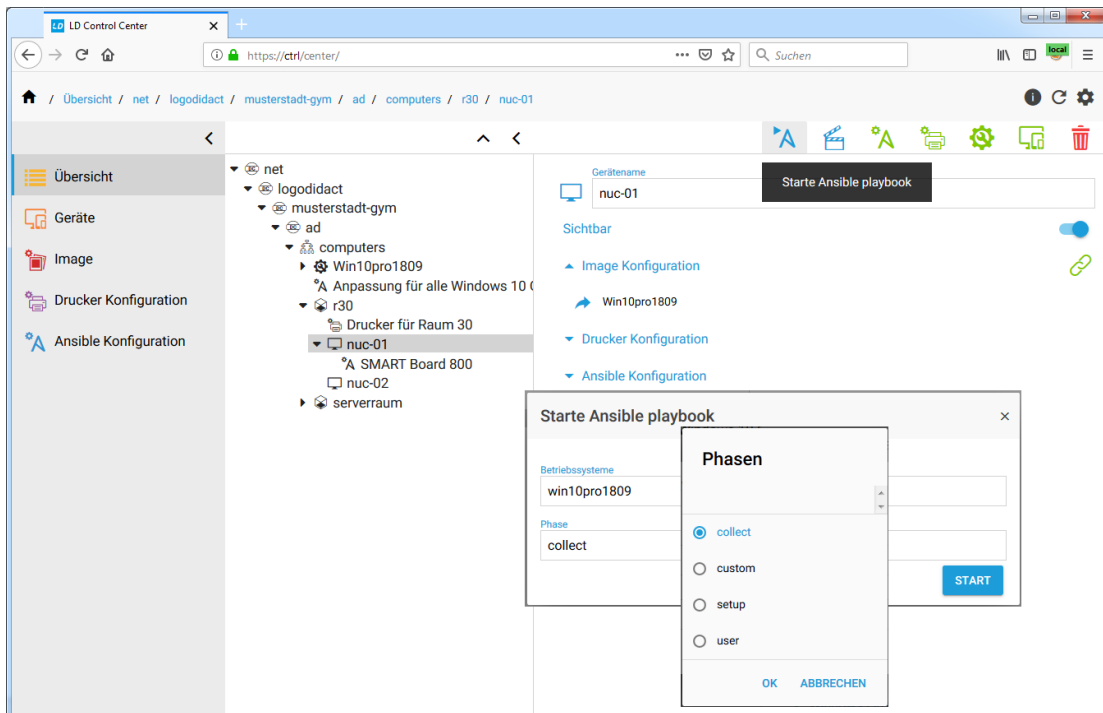
Ob die Lizenz richtig eingespielt wurde, lässt sich direkt am Rechner in der SMART-Software prüfen.

IV.1.7.7.7. Kalibrierung durchführen und sichern

Der letzte Schritt besteht darin, einmalig an jeden Rechner mit SMART-Board und zugewiesener Ansible-Rolle zu gehen und die folgenden Schritte durchzuführen.

1. Sie starten die Software und kalibrieren die Kombination aus Board, Beamer und Rechner
2. Sie öffnen das ControlCenter und melden sich als admin an
3. Sie wählen in der Baumstruktur den Rechner aus, an dem Sie sich befinden und sichern die Kalibrierung über COLLECT

Um die Informationen über die Kalibrierung der SMART-Notebook-Software zu sichern, wählt man den Rechner aus und im Menü am oberen rechten Rand das blaue Ansible-Aktionssymbol. Wählen Sie die Phase COLLECT zum Einsammeln der Daten und bestätigen Sie mit **OK**. Klicken Sie dann auf **START**, wodurch das entsprechende Playbook am Client ausgeführt wird.

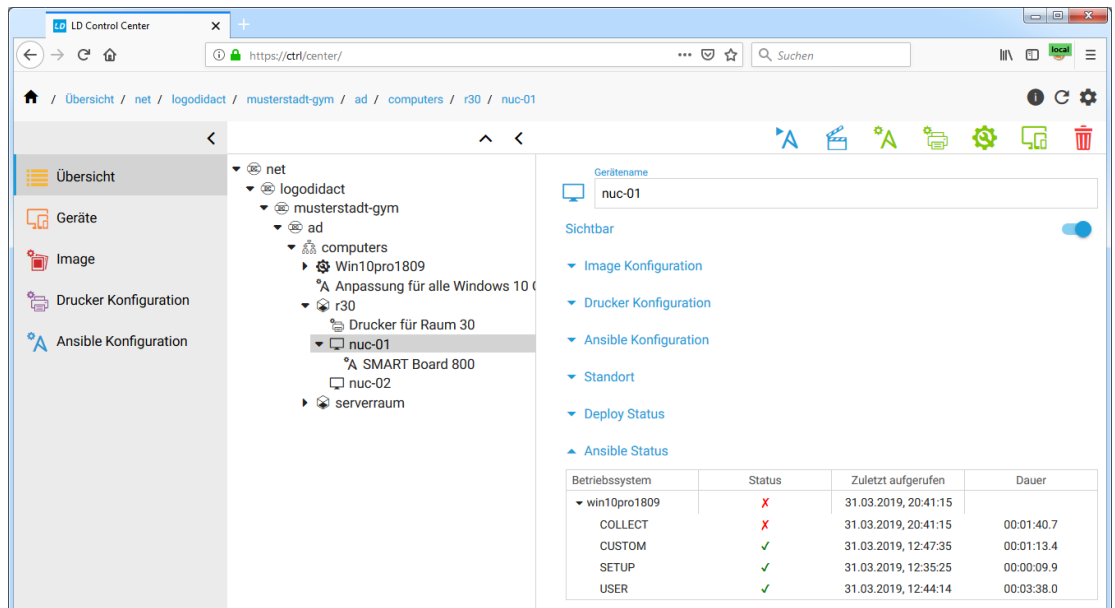


Achtung

Die Informationen über Kalibrierung, sowie individuelle Einstellungen der Stiftauswahl und Ähnliches werden individuell pro Rechner gespeichert und später auch wieder zurückgespielt!

IV.1.7.7.8. Prüfen des Playbooks

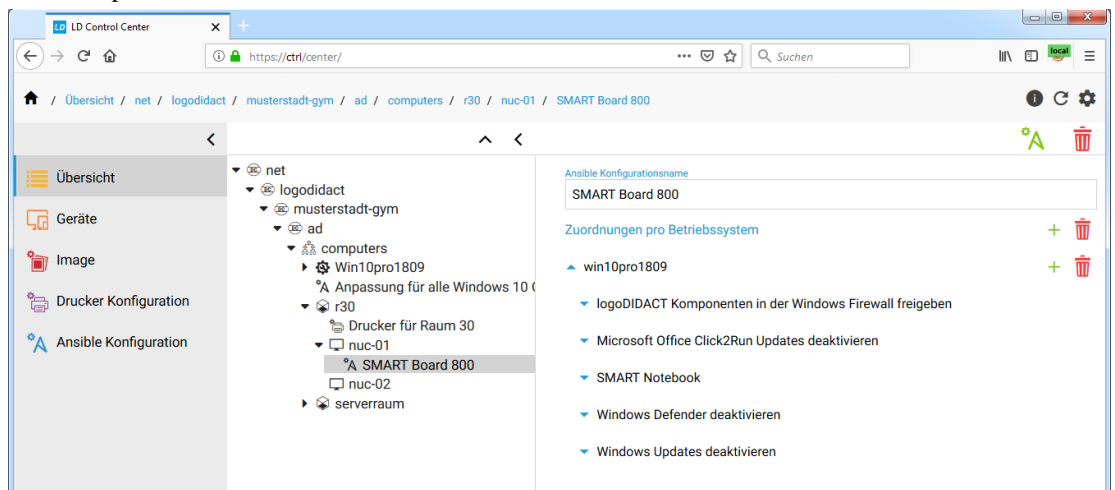
Ob das Playbook richtig ausgeführt wurde, lässt sich im rechten Menübereich über den Eintrag **Ansible Status** feststellen. Sollte die SMART-Software noch nicht auf dem Rechner installiert sein, erhält man natürlich einen Fehler.



IV.1.7.7.9. SMART-Board Konfiguration ergänzen

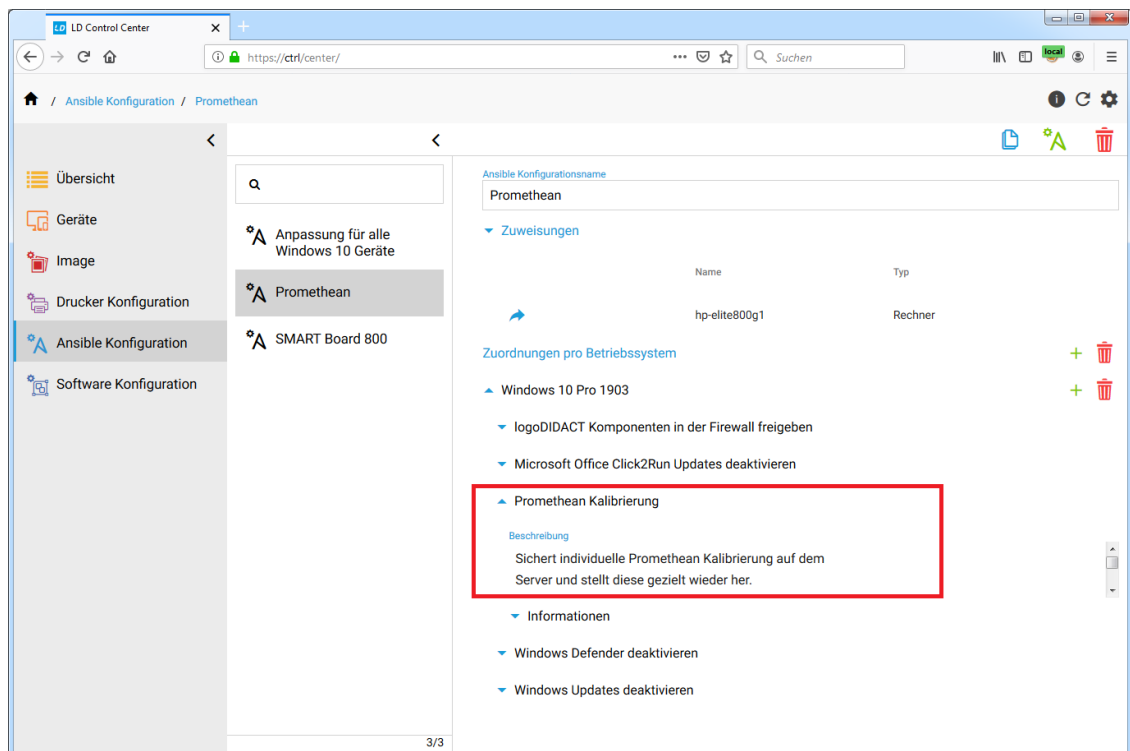
Möglicherweise ist Ihnen bei der Zuweisung der SMART-Board-Konfiguration zu einem Rechner aufgefallen, dass diese Auswahl exklusiv ist und man einem Rechner nur eine einzige Konfiguration zuweisen kann. Dafür gibt es sowohl technische als auch konzeptionelle Gründe.

Erweitern Sie deshalb die SMART-Board-Konfiguration, um die Anpassungen für Windows 10, wie in den Kapiteln zuvor beschrieben.



IV.1.7.8. Promethean Board Konfiguration und Kalibrierung

Das Anlegen einer Ansible-Konfiguration für Promethean-Boards erfolgt analog zu der für SMART-Boards., d.h. Sie erstellen eine Ansible-Konfiguration mit passendem Namen, und fügen neben den allgemeinen Anpassungen (Rollen) zusätzlich die Rolle **Promethean Kalibrierung** hinzu.



Weisen Sie diese Ansible-Konfiguration dann einer Gruppe an Rechnern oder auch gezielt einzelnen Rechnern zu, an denen ein Promethean-Board angeschlossen ist. Welchen Geräten eine Ansible-Konfiguration zugewiesen ist, sehen Sie unter dem Eintrag **Zuweisungen** und können darüber gezielt zu einzelnen Rechnern navigieren.

IV.1.7.8.1. Installation der Promethean Software

Im nächsten Schritt geht man an den Rechner, an dem das Promethean-Board angeschlossen ist, meldet sich als Administrator an, wechselt in den **Audit-Mode** und installiert die Software entsprechend den Anweisungen des Herstellers. Starten Sie jedoch die Software nach der Installation, um zu prüfen, dass diese korrekt installiert ist.



Achtung

In Windows 10 Version 1903 führt die offizielle Version der Promethean-Software etwa 30 Sekunden nach der Kalibrierung zu einem Windows Bluescreen.

Diese Problem tritt unter Windows 10 Version 1809 nicht auf!

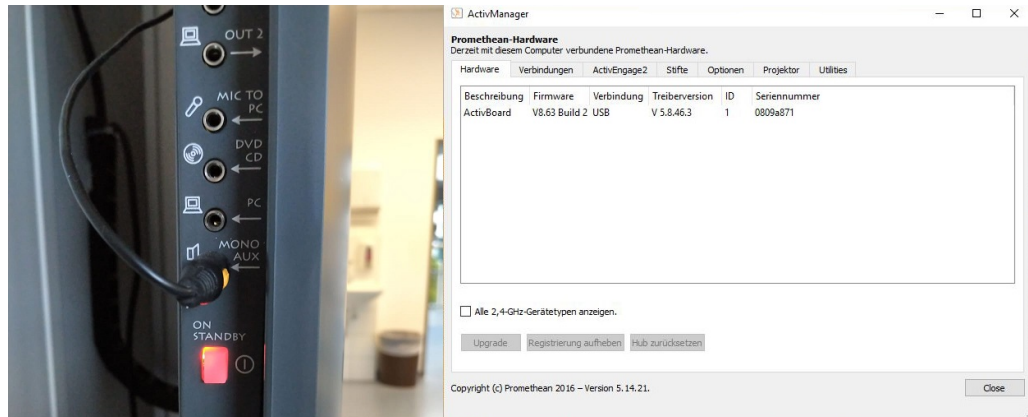
Verwenden Sie für 1903 die Beta-Version des ActiveDrivers von Promethean:

<https://promethean.app.box.com/s/vm0gqur9do6o24c0nlyfkgkie111p6j>

Bei Fragen und Problemen, wenden Sie sich bitte an den Hersteller bzw. schauen in die Support-Foren: <https://community.prometheanworld.com/forums/topic/1st-generation-2nd-generation-ab100-ab300-ab500-activboards-bsod-with-windows-10-update-1903-beta-activdriver/>

IV.1.7.8.2. Treiber-Installation und Board-Erkennung

Eine weitere Besonderheit bei den Promethean Boards besteht darin, dass die Erkennung des Boards nur funktioniert, wenn sich das Board im **STANDBY** befindet.



Ob dies bei allen Boards auftritt oder eine Besonderheit bestimmter Modelle ist, ist derzeit (15.10.19) unklar.



Achtung

Entgegen der Erwartung, wird das Board vom ActiveDriver nur erkannt, wenn es auf **STANDBY** steht, d.h. die Lampe **ROT** leuchtet.

Das ist sowohl bei einer manuellen Treiberinstallation so, als auch bei Vorgang der Softwareverteilung mit **LD DepLoy**, weil dort in der **SETUP**-Phase ebenfalls Treiber erkannt und installiert werden.

Wenn das Board während der Softwareverteilung auf **ON** steht und **GRÜN** leuchtet, bleibt der Rechner an dieser Stelle hängen. Der Bildschirm wird schwarz und der Rechner kann nur noch "hart" ausgeschaltet werden, führt dann aber den Prozess fort.

Nachem Sie die Software an Ihrem ersten "Master" installiert haben, erstellen Sie ein Image und verteilen dieses an die entsprechenden Geräte mit Promethean-Board.

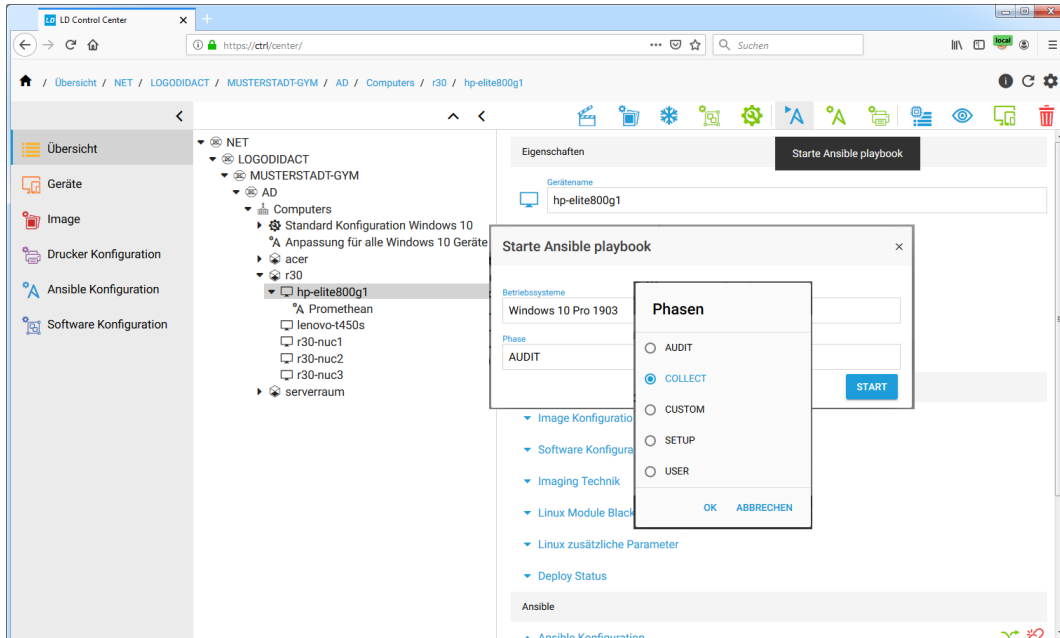
IV.1.7.8.3. Durchführung und Sicherung der Kalibrierung

Die Kalibrierung startet automatisch, wenn Sie mit dem Stift das erste Mal am Board arbeiten und das System erkennt, dass es noch nicht kalibriert wurde. Bitte führen Sie die Kalibrierung entsprechend der Dokumentation des Herstellers durch und wenden Sie sich bei Fragen oder Unklarheiten an den Lieferanten oder Hersteller des Boards.

Die folgenden Schritte sind einmalig an jedem Rechner mit Promethean-Board und zugewiesener Ansible-Rolle durchzuführen

1. Starten Sie die Software und kalibrieren die Kombination aus Board, Beamer und Rechner
2. Öffnen Sie das ControlCenter und melden sich als admin an
3. Wählen in der Baumstruktur den Rechner aus, an dem Sie sich befinden und sichern die Kalibrierung über COLLECT

Um die Informationen über die Kalibrierung der Promethean-Software zu sichern, wählt man den Rechner aus und im Menü am oberen rechten Rand das blaue Ansible-Aktionssymbol. Wählen Sie die Phase COLLECT zum Einsammeln der Daten und bestätigen Sie mit **OK**. Klicken Sie dann auf **START**, wodurch das entsprechende Playbook am Client ausgeführt wird.



Auf Serverseite lässt sich dann im Ansible-Status prüfen, ob die Daten erfolgreich eingesammelt wurden.

IV.1.7.8.4. Rückspielen der Kalibrierung

Für die Sicherung der Kalibrierung spielt es keine Rolle, in welchem Modus diese durchgeführt wird.

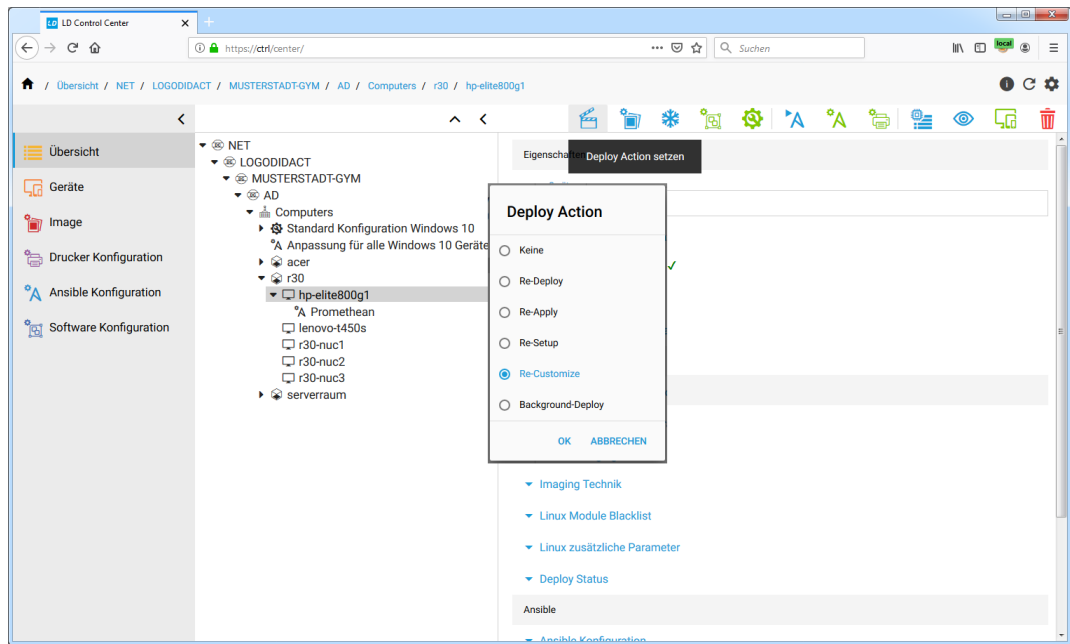
In der Praxis führt man die Kalibrierung in der Regel aber im geschützten Modus (=Selbsteinde Arbeitsstation) durch, unmittelbar nachdem man die Promethean-Software installiert und an alle Rechner verteilt hat. Würde man nun aber den Rechner neu starten, würde die Kalibrierung nicht zurückgespielt werden.



Achtung

Wichtig ist deshalb, dass Sie nach der Kalibrierung aller Boards, die Kalibrierungsinfos über den Befehl **Re-Customize** für alle Boards bzw. Rechner aktiv zurückspielen.

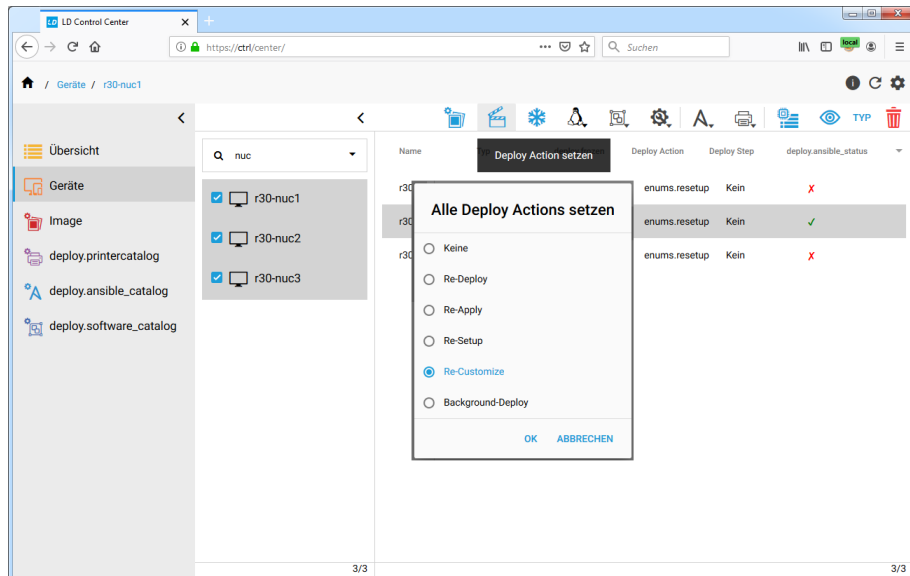
Das Zurückspielen der Kalibrierung erfolgt einzeln pro Gerät oder auch pro Gruppe über das Control-Center und den Menüeintrag **Deploy Action setzen**.



Diese Anweisung sorgt dafür, dass die Anpassungen ins System eingespielt werden und danach der Schutz aktiviert wird.

Wenn Sie für die Rechner zur Steuerung der Whiteboards eine passende Namenskonvention wie z.B. "pm" (für Prometheus) oder "sb" (für SMART-Board) verwenden, können Sie über das Menü **Geräte** und der Suche diese Geräte auflisten.

Markieren Sie das erste Gerät im Suchergebnis, halten Sie die **SHIFT**-Taste gedrückt und markieren Sie das letzte Gerät aus der Liste. Über die Häkchen können Sie dann alle Geräte für die Aktion auswählen und darüber z.B. den **Re-Customize** anstoßen.



IV.1.8. Funktionsupgrade von Windows 10

Bekanntermaßen hat Microsoft mit der Einführung von Windows 10 seine Upgrade-Zyklen angepasst und ergänzt den Namen für die jeweilige Version um Jahr und Monat des Erscheinens. Die tatsächli-

che Freigabe und Verfügbarkeit einer neuen Version erfolgt meist etwas später. Inzwischen gibt es Windows 10 seit 5 Jahren mit den folgenden 10 Versionenständen:

- Build 1507 (RTM, Release To Manufacturing)
- Build 1511 (November Update)
- Build 1607 (Anniversary Update)
- Build 1703 (Creators Update)
- Build 1709 (Fall Creators Update)
- Build 1803 (April 2018 Update)
- Build 1809 (October 2018 Update)
- Build 1903 (May 2019 Update)
- Build 1909 (November 2019 Update)
- Build 2004 (April 2020 Update)

Von LD Deploy werden grundsätzlich alle oben aufgeführten Windows-Versionen unterstützt. Beim so genannten Funktions-Upgrade ist dabei zu beachten, dass Microsoft dies nicht innerhalb einer VHD unterstützt.



Achtung

Die Installation von Windows 10 erfolgt mit LD Deploy per Standard in eine virtuelle Partition. Microsoft selbst unterstützt bzw. erlaubt aber kein Upgrade auf eine höhere Versionsnummer innerhalb einer VHD.

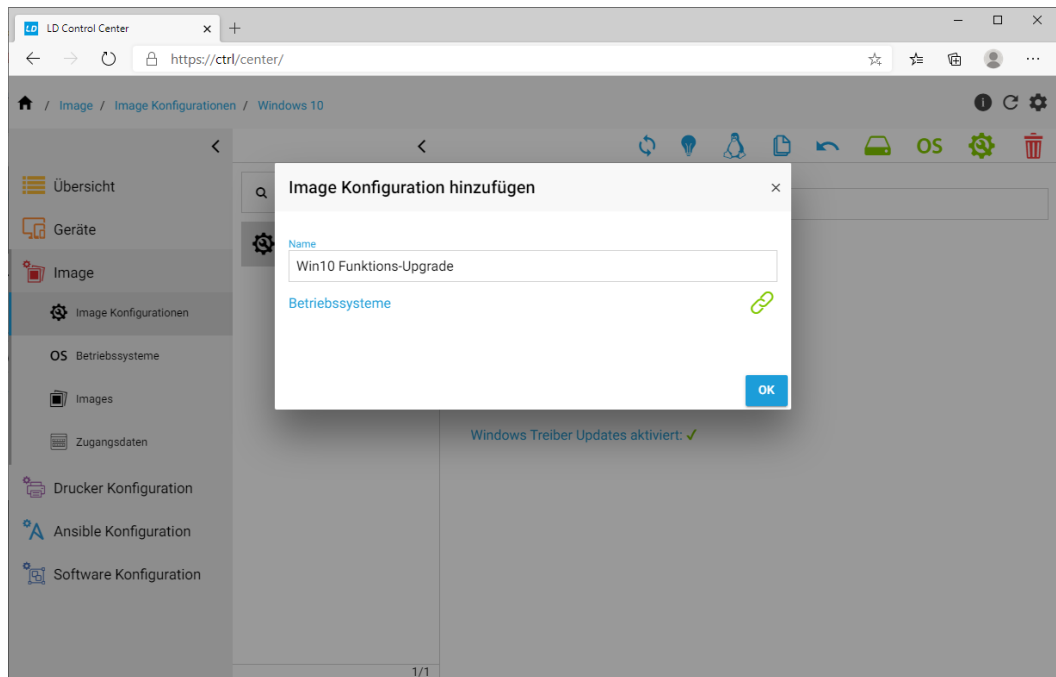
Bis auf die Aktualisierung von 1903 auf 1909 erfordern deshalb bisher alle oben aufgeführten Upgrades ein angepasstes Vorgehen. Um ein Funktions-Upgrade durchzuführen, muss ein bestehendes Image an einem Client einmalig in eine physische Partition gespielt werden. Danach sind zwingend einige Anpassungen notwendig, bevor das Upgrade durchgeführt und wieder per Imaging verteilt werden kann.

Eine weitere Besonderheit besteht darin, dass das Upgrade nicht im Audit-Mode durchgeführt werden darf, weil auch dies von Microsoft nicht unterstützt wird und in einer entsprechenden Fehlermeldung mündet.

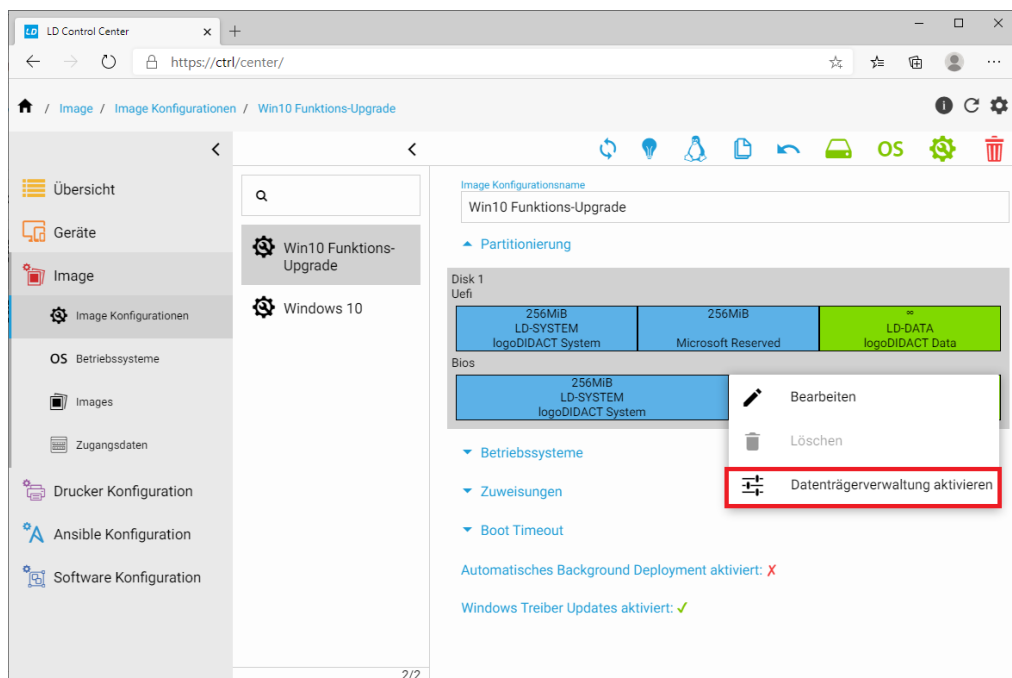
Das Vorgehen ist in den folgenden Abschnitten beschrieben.

IV.1.8.1. Image-Konfiguration und Partition für das Funktionsupgrade

Erstellen Sie zunächst eine neue Konfiguration und geben dieser einen aussagekräftigen Namen, wie z.B. "Win10 Funktions-Upgrade".

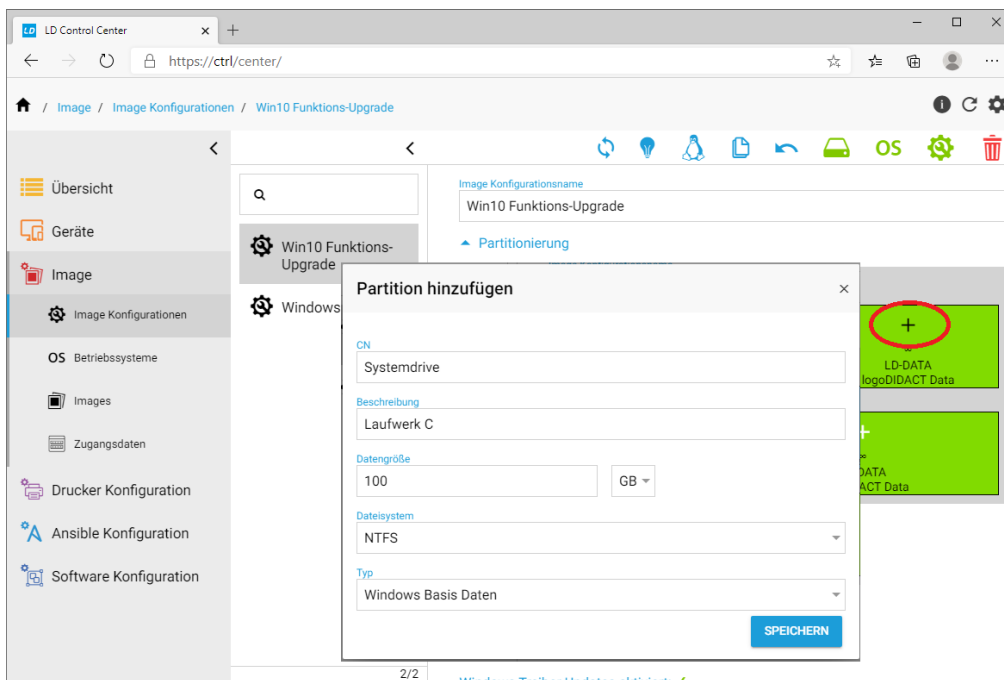


Aktivieren Sie dann im Abschnitt **Partitionierung** die Datenträgerverwaltung, indem Sie den Mauscursor über die grüne Fläche **LD-DATA** platzieren und dann die linke Maustaste drücken und gedrückt halten, bis das Kontextmenü erscheint.

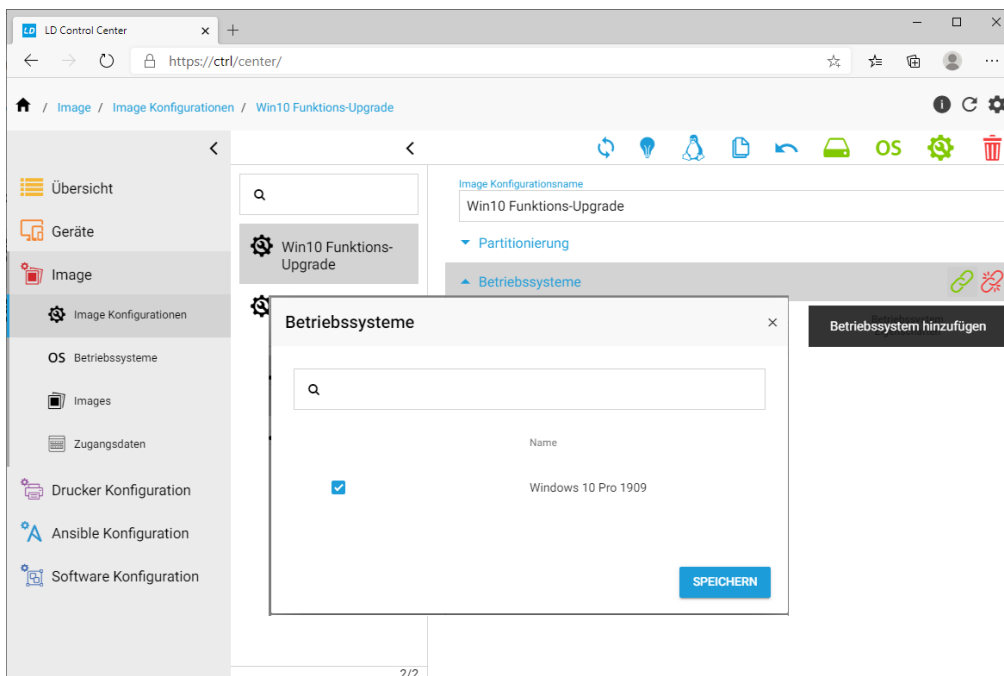


Durch **Datenträgerverwaltung aktivieren** ändert sich die Anzeige der einzelnen Partitionen. Wählen Sie das "+" Symbol bei **LD-DATA** und erstellen Sie eine hinreichend große Partition, in die ihr bisheriges System Platz findet und zudem ausreichend Platz für das Windows 10 Upgrade vorhanden ist. Angaben zum notwendigen freien Speicherplatz für das jeweilige Upgrade finden Sie beim Hersteller Microsoft.

Setzen Sie den Wert **Dateisystem** auf **NTFS** und **Typ** auf **Windows Basis Daten** und übernehmen Sie mit **SPEICHERN**.

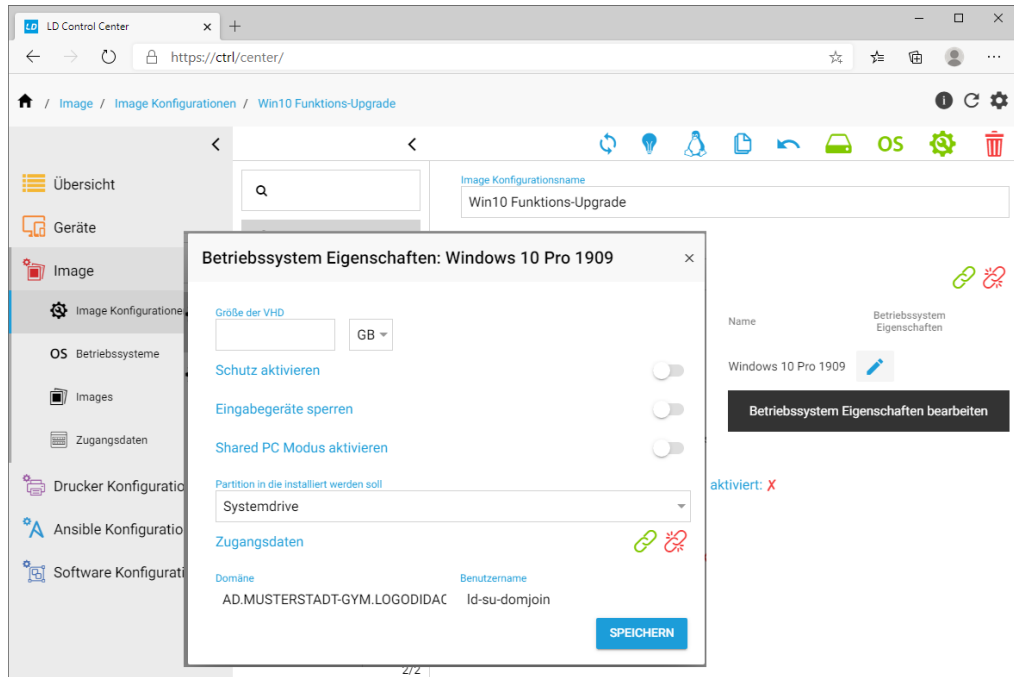


Verknüpfen Sie das die Konfiguration mit dem gewünschten Betriebssystem.



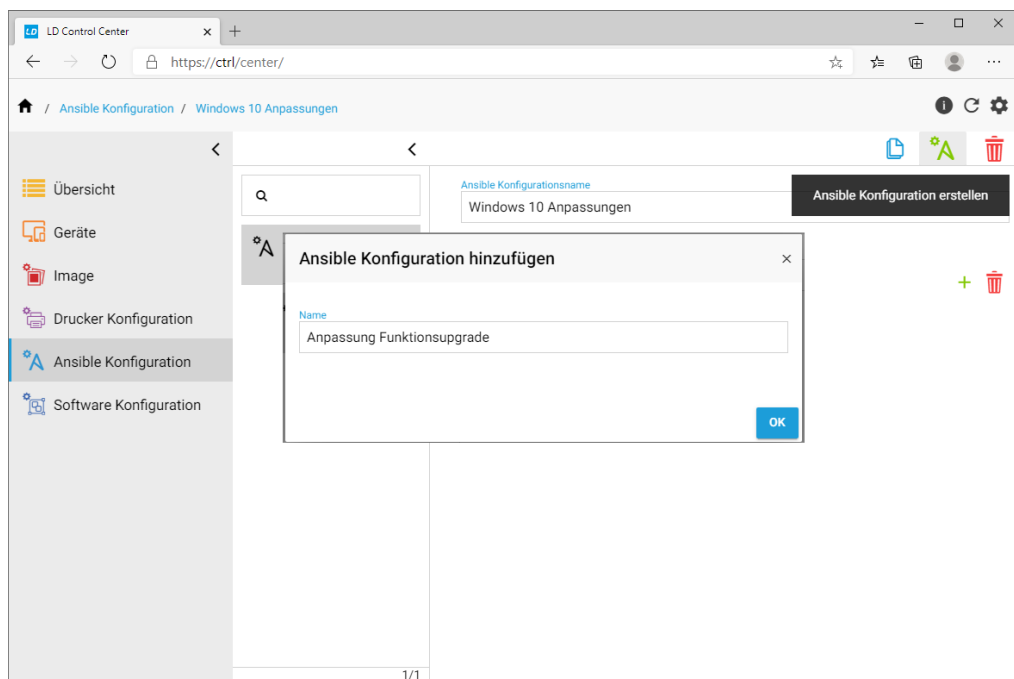
Im letzten Schritt müssen die Eigenschaften für das Betriebssystem in dieser speziellen Konfiguration angepasst werden. Entscheidend sind hierbei, dass die Schieberegler für **Schutz aktivieren**, **Eingabegeräte sperren** und **Shared PC Modus aktivieren** alle deaktiviert werden und das Image in die physische Partition installiert wird (im Beispiel Systemdrive). Zwingend erforderlich bleibt auch

der Domänenbeitritt, der über das Verknüpfungssystemsymbol der grünen Büroklammer konfiguriert wird. Übernehmen Sie mit **SPEICHERN**.

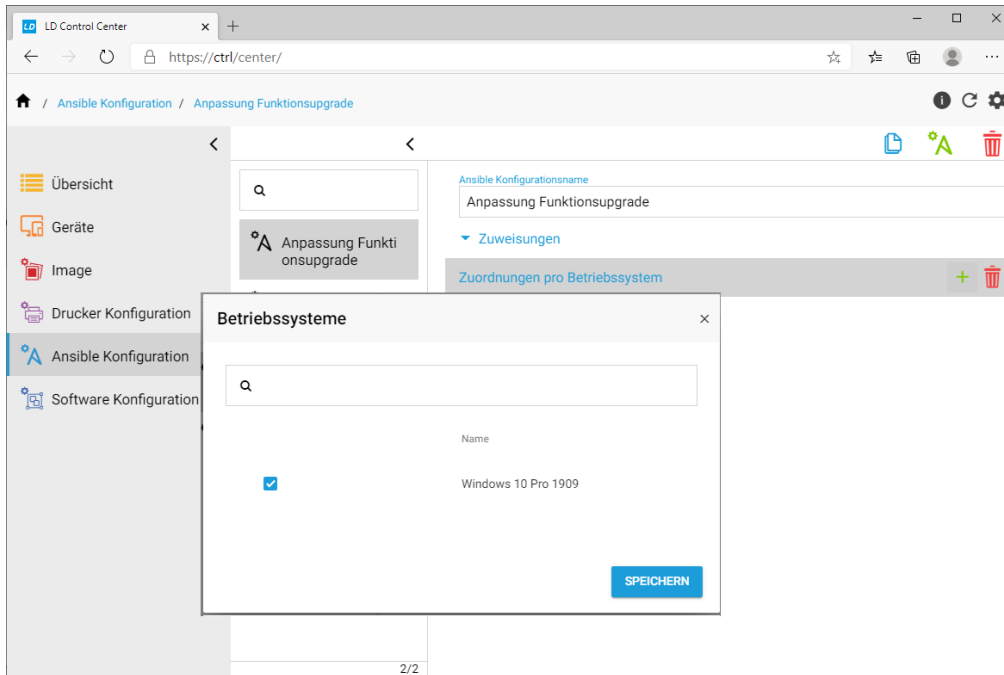


IV.1.8.2. Ansible-Konfiguration für das Funktionsupgrade

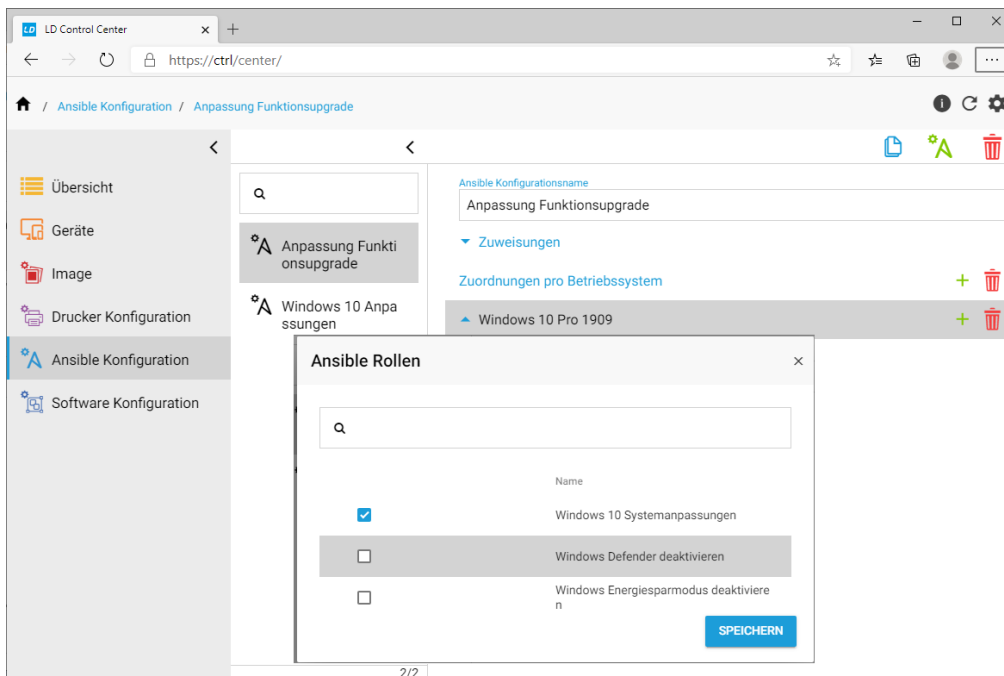
Zwingend notwendig für das Funktionsupgrade ist eine separate Ansible-Konfiguration. Legen Sie diese mit einem aussagekräftigen Namen, wie z.B. **Anpassung Funktionsupgrade** über das Control-Center an.



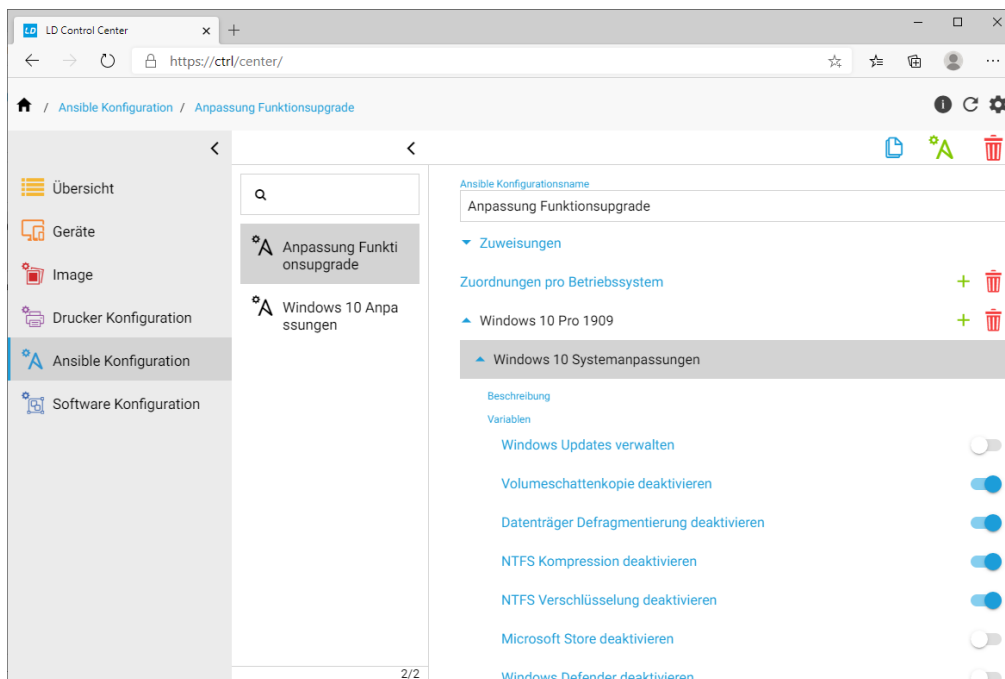
Verknüpfen Sie anschließend die Ansible Konfiguration mit einem Betriebssystem.



Legen Sie dann fest, welche Rollen bzw. Anpassungen in dieser Ansible-Anpassungen für das gewählte Betriebssystem durchgeführt werden sollen. Für das Funktionsupgrade entscheidend ist hierbei die Auswahl der Rolle **Windows 10 Systemanpassungen**. Setzen Sie dort das entsprechende Häkchen und übernehmen mit **SPEICHERN**.

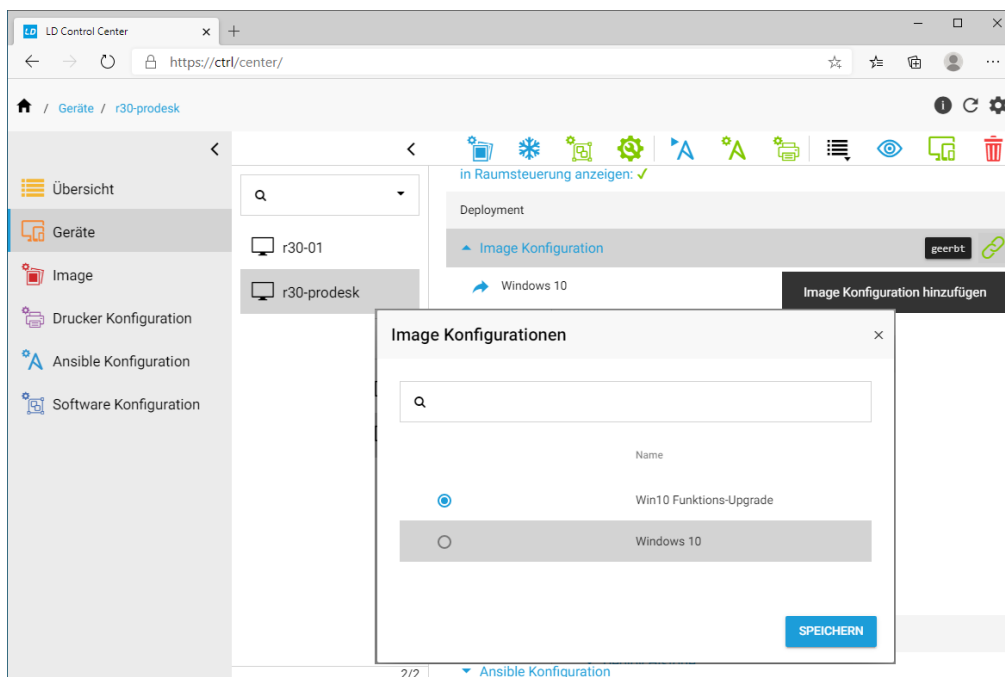


Verändern Sie dann die Schieberegler innerhalb der Rolle wie unten dargestellt. Zwingend erforderlich ist es, dass der Schieberegler **Windows Updates verwalten** deaktiviert bleibt, so dass das Funktionsupgrade durchgeführt werden kann.

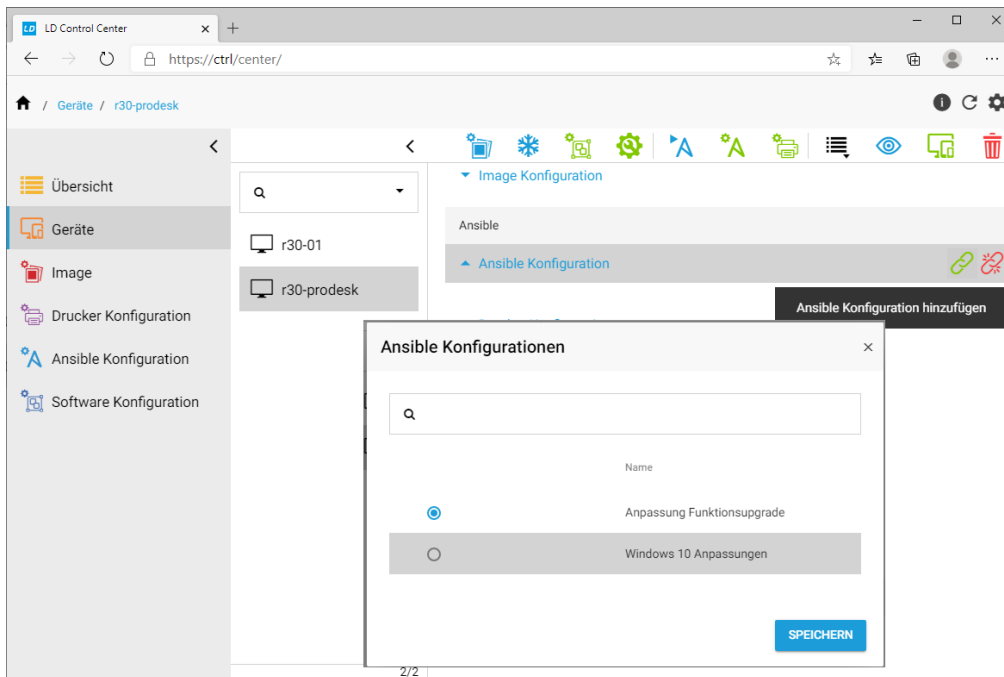


IV.1.8.3. Konfigurationen einem Rechner zuweisen

Der letzte Schritt der serverseitigen Vorbereitung besteht darin, einem Rechner die oben erstellten Konfigurationen für die Partitionierung und Ansible-Anpassung zuzuweisen. Dies erfolgt über das Menü **Geräte** und die Auswahl eines einzelnen Rechners für die Umstellung. Ändern Sie eine eventuell vorhandene geerbte Image-Konfiguration entsprechend ab und verknüpfen Sie diese mit der erstellten Konfiguration **Win10 Funktions-Upgrade**.



Analog dazu ändern Sie die Ansible-Konfiguration im gleichlautenden Abschnitt und weisen die zuvor erstellte Konfiguration **Anpassung Funktionsupgrade** zu.



IV.1.8.4. Image neu einspielen und Anpassungen vornehmen

Nach den oben gemachte Vorbereitungen kann Ihre bestehende Installation nun am Client in eine physische Partition eingespielt werden. Setzen Sie dazu den ausgewählten Client über das ControlCenter auf **Re-Deploy**.

Warten Sie ab, bis alle Phasen des Deployment-Vorgangs abgearbeitet wurden und der Rechner fertig ist und melden Sie sich mit dem administrativen Konto an der Domäne an.



Achtung

Vielfach findet nach dem Upgrade von Windows 10 automatisiert ein Rollback statt. Dies hat in der Regel mit Problemen bei der Übernahme von Benutzerprofilen zu tun.

Deshalb müssen "umgebogene" Pfade für die Ordner Downloads, Dokumente, Bilder usw. vor dem Funktionsupgrade auf C: zurückgelegt werden.

Ebenfalls sind etwaige Verknüpfungen auf dem Desktop zu entfernen, die auf Netzlaufwerke verweisen, wie z.B. H:\ auf **Eigene Dateien**.

IV.1.8.5. Funktionsupgrade durchführen

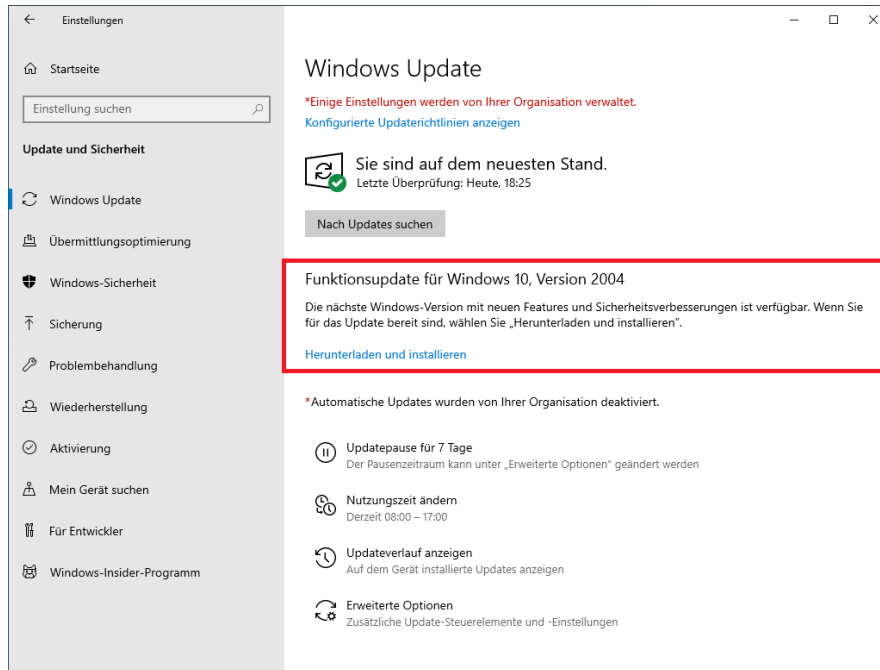
Sie können das Funktionsupgrade entweder als Domänen-Admin oder als lokaler Benutzer "Station" anstoßen. Bitte beachten Sie, dass es aus vollkommen verschiedenen und nicht näher nachvollziehbaren Gründen dazu kommen kann, dass das Upgrade scheitert und ein so genanntes Roll-Back stattfindet.



Achtung

Wechseln Sie **auf keinen Fall** in den Audit-Mode!

Das Funktionsupgrade kann entweder per Windows-Update Funktion installiert werden (siehe Abbildung) oder per ISO-Installationsmedium eines neueren Builds.



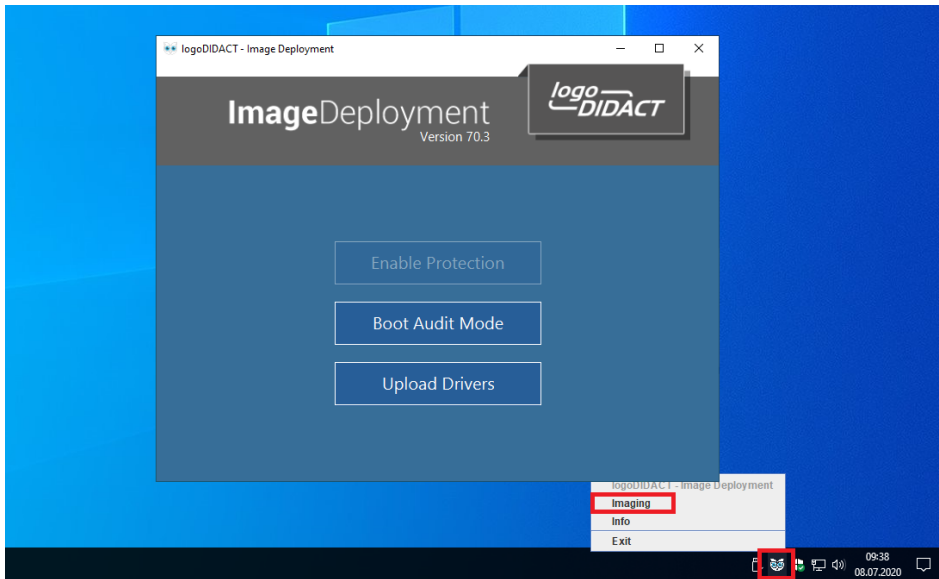
Nach dem Download warten Sie ab, bis das Windows Funktionsupdate durchgeführt wurde und der Vorgang abgeschlossen ist. Der PC wird mehrfach neu gestartet. Sobald der PC wieder in der Windows-Anmeldemaske steht, melden Sie sich mit dem Benutzer **admin** an der Domäne an.

Über **winver** können Sie prüfen, ob die Aktualisierung funktioniert hat.

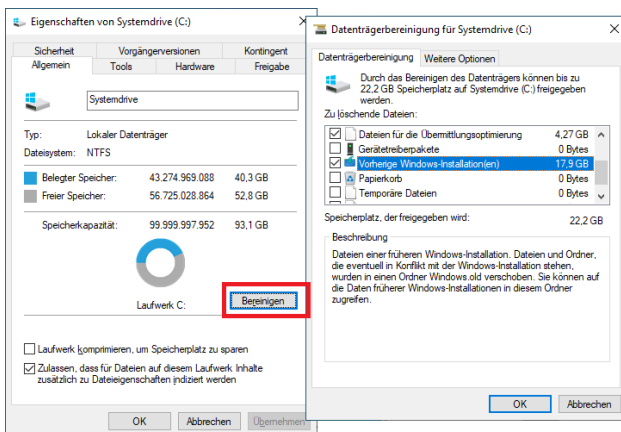


IV.1.8.6. In Audit-Mode wechseln und Image erstellen

Wechseln Sie in den Audit Mode und nehmen Sie ggf. weitere Änderungen vor, die Sie vor dem Funktionsupgrade rückgängig machen mussten.



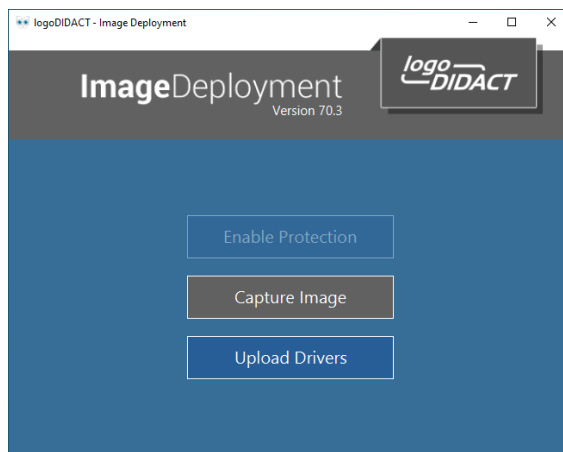
Extrem wichtig ist es, nach einem Funktionsupgrade die **Windows-Update Bereinigung** auszuführen, um nicht die komplette vorherige Installation per Imaging weiter mitzuschleppen. Je nach Versionsstand, können dies 20 GB und mehr werden, die sonst unnötig im Image und auf allen Clients landen.



Achtung

Die Bereinigung benötigt in der Regel einen Neustart!

Erstellen Sie danach wie gewohnt ein Image und verteilen dieses an alle übrigen Clients aus der Imagegruppe. Entfernen Sie auch die für das Funktionsupgrade erstellte Image- und Ansible-Konfiguration.



IV.1.9. Installation Office 2019

Für gewöhnlich ist bei der Installation des Microsoft Office-Paketes bis zur Version 2016 nichts besonders zu beachten. Dies ändert sich mit der Version 2019. Um Office 2019 in der volumenlizenzierten Version bereitzustellen, müssen Sie das Office-Bereitstellungstool (Office Deployment Tool, ODT) verwenden. Darüber erhalten Sie im wesentlichen verschiedene XML-Dateien, um Office 365, Office 2019 oder auch andere Microsoft-Produkte wie beispielsweise Visio 2019 zu installieren.

Detaillierte Informationen finden Sie auf den Seiten von Microsoft, wie z.B. hier:

<https://docs.microsoft.com/de-de/deployoffice/office2019/deploy>

IV.1.9.1. XML-Datei erstellen

Über den folgenden Link erreicht man das Office-Anpassungstool und kann darüber kundenspezifische XML-Dateien generieren:

<https://config.office.com/deploymentsettings>

Eine vorgefertigte XML-Datei für Office 2019 steht hier zum Download zur Verfügung und beinhaltet keinen kundenspezifischen Lizenzkey (PIDKEY), sondern lediglich eine produktspezifische ID für Office 2019:

<https://files.sbe.de/ld-deploy/Office2019.xml>

```
<Configuration ID="377c5387-e00b-4a9a-ac3d-e23391893b50">
  <Info Description="" />
  <Add OfficeClientEdition="64" Channel="PerpetualVL2019">
    <Product ID="ProPlus2019Volume" PIDKEY="NMMKJ-6RK4F-KMJVX-8D9MJ-6MWKP">
      <Language ID="MatchOS" />
      <ExcludeApp ID="Groove" />
      <ExcludeApp ID="OneDrive" />
      <ExcludeApp ID="Lync" />
    </Product>
  </Add>
  <Property Name="SharedComputerLicensing" Value="0" />
  <Property Name="PinIconsToTaskbar" Value="TRUE" />
  <Property Name="SCLCacheOverride" Value="0" />
  <Property Name="AUTOACTIVATE" Value="0" />
  <Property Name="FORCEAPPSHUTDOWN" Value="FALSE" />
```

```

<Property Name="DeviceBasedLicensing" Value="0" />
<Updates Enabled="TRUE" />
<AppSettings>
  <Setup Name="Company" Value="SCHULE" />
  <User Key="software\microsoft\office\16.0\excel\options" Name="defaultformat" />
  <User Key="software\microsoft\office\16.0\powerpoint\options" Name="defaultformat" />
  <User Key="software\microsoft\office\16.0\word\options" Name="defaultformat" />
</AppSettings>
<Display Level="Full" AcceptEULA="TRUE" />
</Configuration>

```

IV.1.9.2. Setup mit Optionen ausführen

Für die Installation muss in jedem Fall das ODT (Office Deployment Tool) verwendet werden. Entpacken Sie die Datei in ein Verzeichnis C:\ODT. Kopieren Sie die heruntergeladene Datei `Office2019.xml` ebenfalls in dieses Verzeichnis.

Über den folgenden Befehl laden Sie die Office 2019-Installationsdateien im Umfang von etwa 2 GB aus dem Netz herunter:

```
Setup.exe /download Office2019.xml
```

Beim Download werden entsprechende Unterverzeichnisse erstellt und die Daten dort abgelegt. Diese Daten können, ähnlich wie bei einer ISO-Datei auch auf anderem Wege verteilt und damit Offline genutzt werden.

Die eigentliche Installation von Office 2019 erfolgt über folgenden Befehl:

```
Setup.exe /configure Office2019.xml
```

IV.1.10. Linux am Client

Das modular aufgebaute freie Betriebssystem Linux wird weltweit von einer großen Entwicklergemeinschaft an Freiwilligen, Non-Profit-Organisationen aber auch vielen kommerziellen Firmen weitentwickelt. Linux hat vor allem eine hohe Bedeutung im Server-Umfeld und im mobilen Bereich (z.B. Routern, Mobiltelefone, Embedded Systems).

In dieser Hinsicht ist Linux fester Bestandteil im Berufsleben der meisten IT-Experten und in Forschung und Lehre eine feste Größe. Linux sollte nicht nur Gegenstand der Ausbildung im Hochschulbereich sein, sondern unbedingt auch an weiterführenden Schulen und erst Recht an berufsbildenden Schulen gelehrt werden.



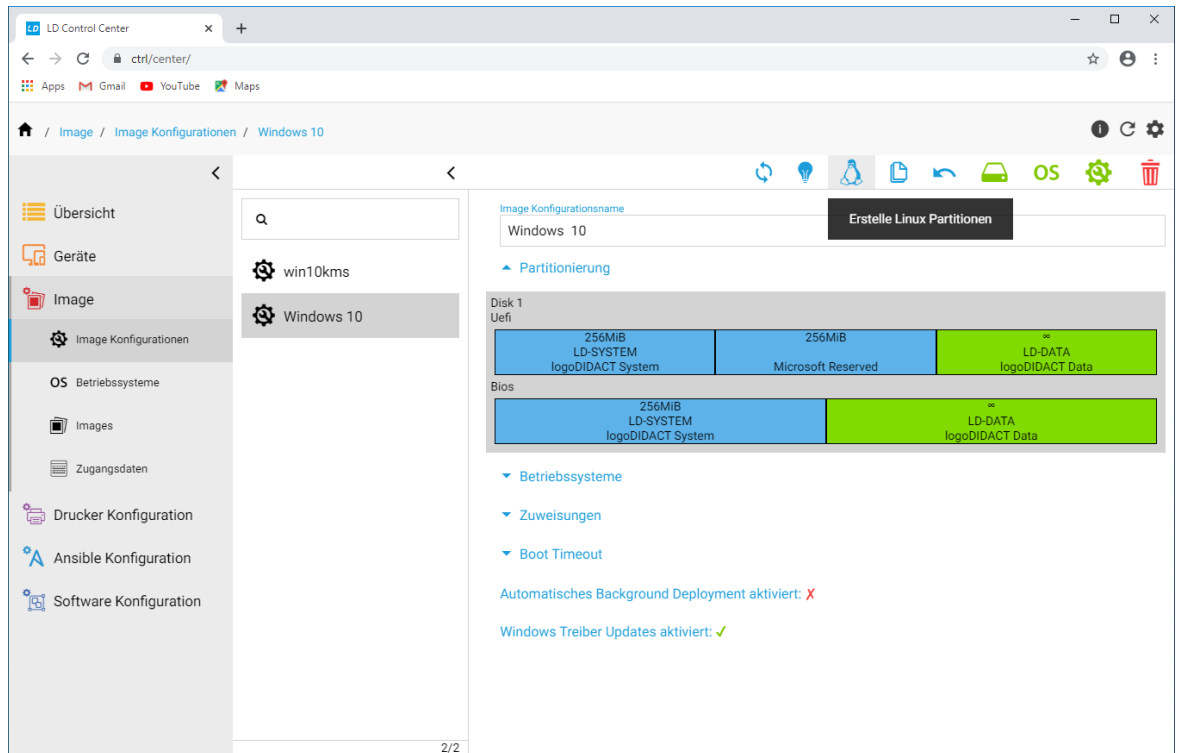
Achtung

In diesem Abschnitt wird beschrieben, wie Sie in LD Deploy eine Konfiguration für Linux-Clients erstellen und welche Voraussetzungen bei Ihrer eigenen Linux-Installation mit der entsprechend ausgewählten Distribution zu beachten sind. Diese Voraussetzungen sind notwendig aber nicht hinreichend für die grundlegende Funktionsfähigkeit.

SBE stellt kein Image für einen vorgefertigten Linux-Client bereit und leistet in diesem Bereich auch keinerlei Grundlagen-Support für Linux. Das entsprechende Know-how für Ihre gewünschte Linux-Distribution müssen Sie selbst bereitstellen oder von externer Stelle einkaufen.

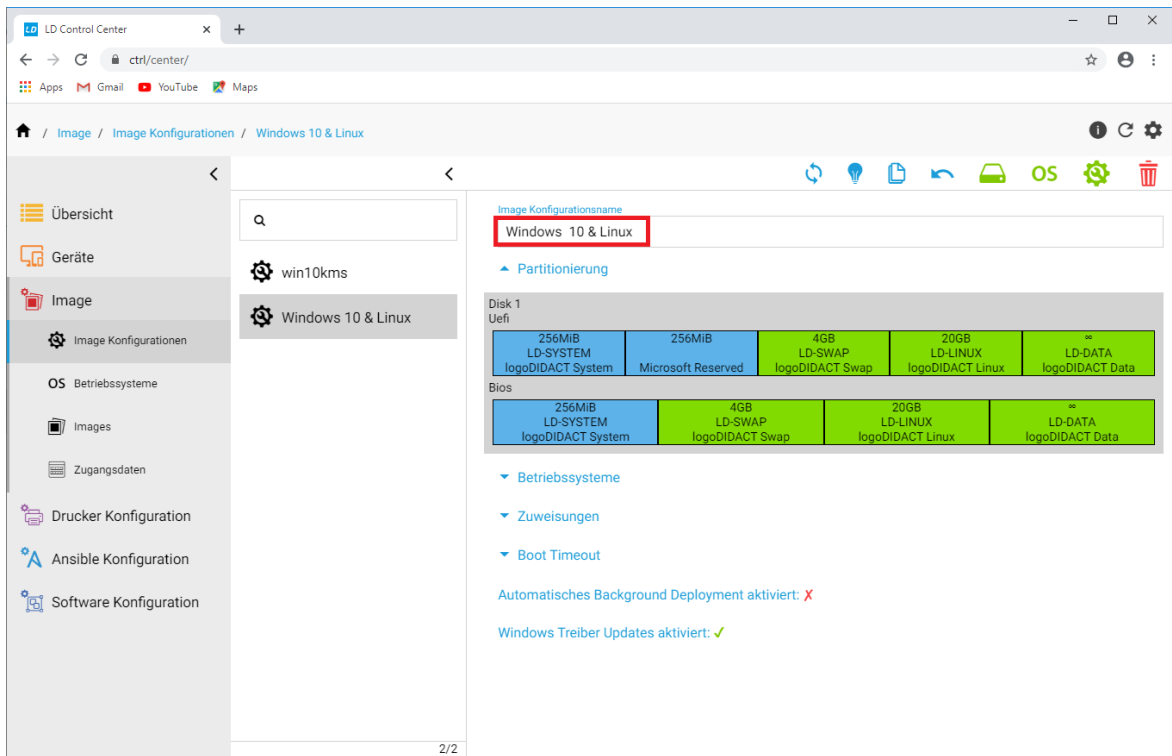
IV.1.10.1. Konfiguration um Linux erweitern

Grundlage für den Einsatz am Client ist die Definition eines zweiten Systems, das in der Regel parallel zu Windows 10 zum Einsatz kommt. Für den Parallelbetrieb sind spezielle Anpassungen notwendig, die über die Datenträgerverwaltung abgebildet werden. Wählen Sie zunächst die bestehende Image-Konfiguration aus und erweitern Sie den Abschnitt **Partitionierung**. Klicken Sie anschließend auf den Pinguin als Symbol für Linux.

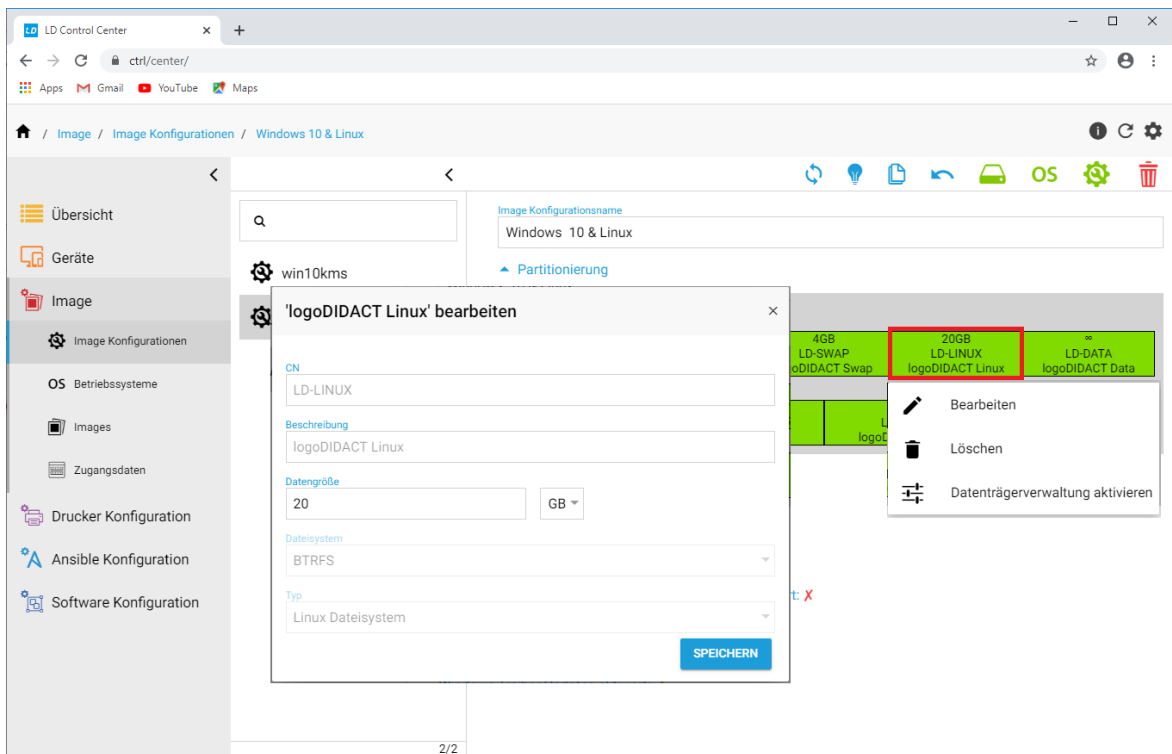


Dadurch werden nun neben **LD-DATA** die zwei für Linux typischen Partitionen angelegt. Eine für das System und ergänzend dazu die so genannte Swap-Partition, die "Auslagerungsdatei" von Linux.

Ändern Sie an dieser Stelle gleich auch den Namen der Imagekonfiguration, so dass der Parallelbetrieb der zwei Systeme sichtbar ist.



Sofern Sie die Partitionsgröße anpassen wollen, fahren Sie mit der Maus auf die grüne Fläche der jeweiligen Partition, klicken mit der linken Maustaste darauf und halten diese gedrückt, bis ein Dialogfenster erscheint. Wählen Sie dort den Eintrag **Bearbeiten**. Im darauf erscheinenden Dialog lässt sich die Größe entsprechend anpassen.

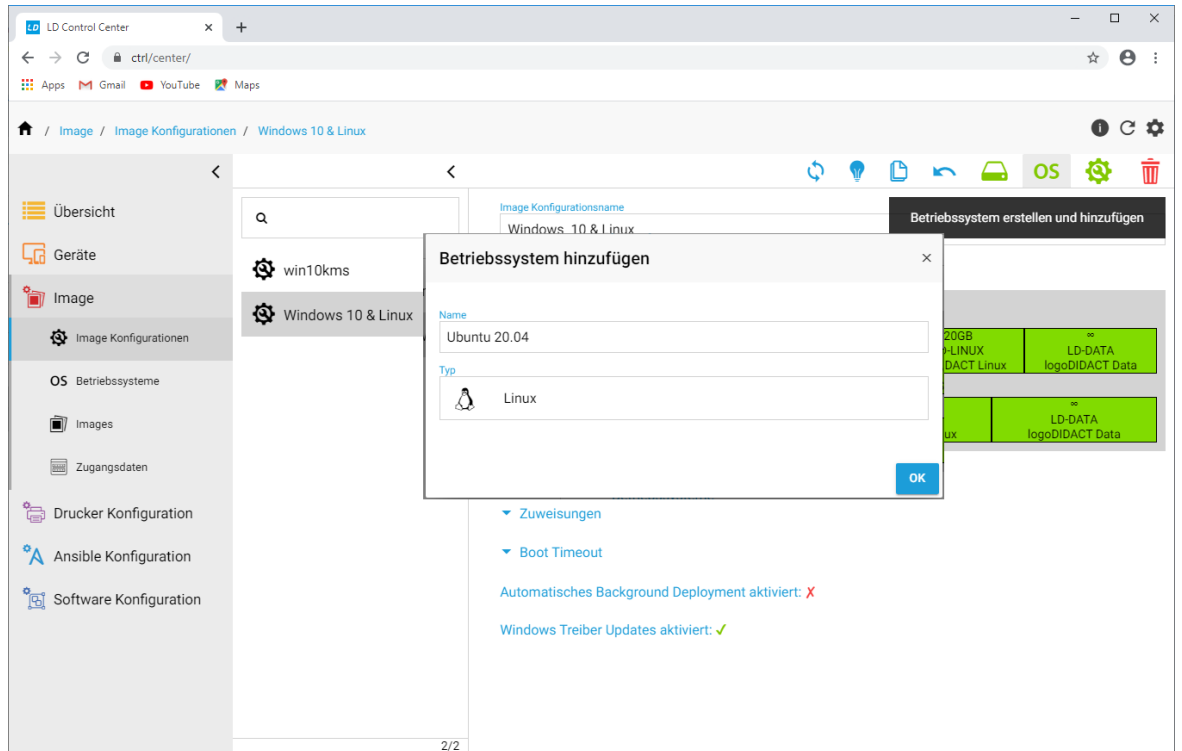




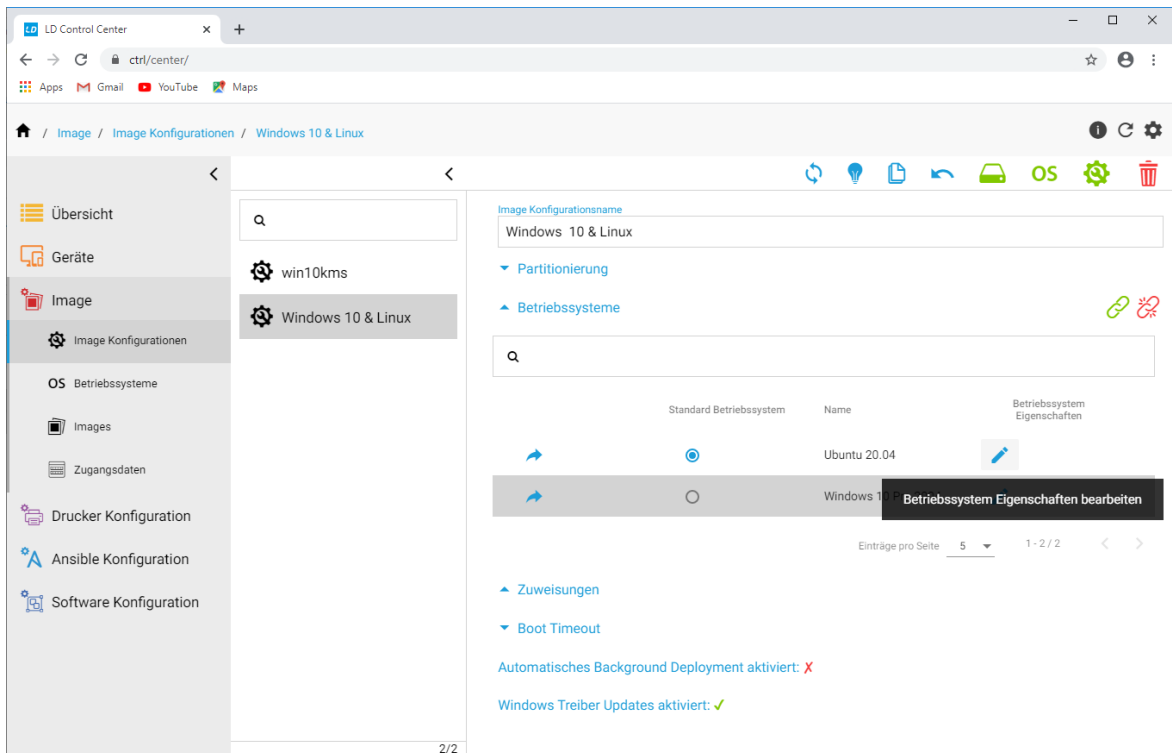
Achtung

Falls das Auswahlmü nicht erscheint, kann das an einem zu kleinen Browserfenster liegen. Maximieren Sie in diesem Fall das Fenster des Browsers.

Nachdem Sie den Namen der Konfiguration sinnvoll angepasst haben, fügen Sie ein neues Betriebssystem hinzu. Wählen Sie dazu aus dem obern Menübereich das grüne Symbol **OS**, geben dem System einen passenden Namen und wählen als **Typ** Linux aus. Bestätigen Sie mit **OK**.



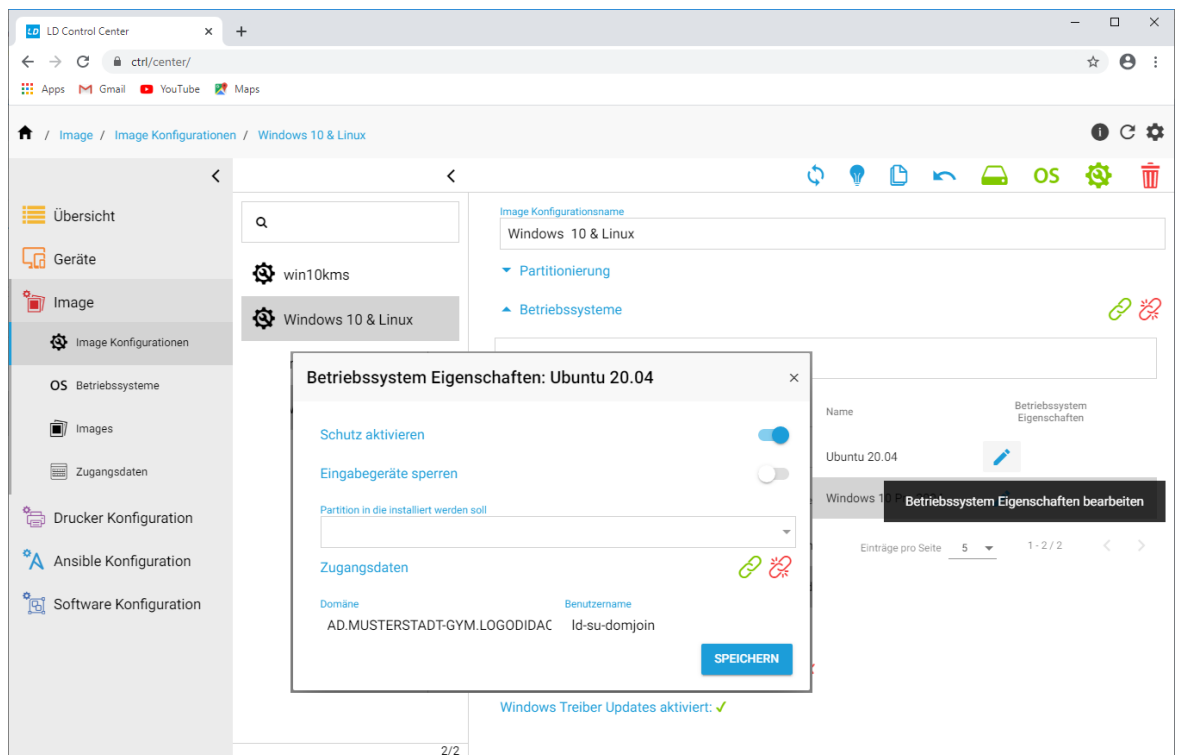
Im Abschnitt **Betriebssysteme** erscheint nun neben dem bereits konfigurierten Windows 10 das neu angelegte Linux-Betriebssystem auf.



Legen Sie im nächsten Schritt die Details für das Linux-System fest. Wählen Sie dazu rechts unten das blaue Editiersymbol. Konfigurieren Sie den Domänenbeitritt analog zu Windows und setzen Sie die Schieberegler entsprechend Ihren Vorstellungen der Nutzung des Systems.

Auch für Linux-Systeme ist die Schutzfunktion vorhanden, wenngleich technisch über **BTRFS** vollkommen anders implementiert, als für Windows 10 mit xVHD. Lassen Sie also den Schieberegler **Schutz aktivieren** aktiviert, wenn die Benutzer gefahrlos mit Linux spielen sollen. Deaktivieren Sie **Eingabegeräte sperren**, weil das Setup in Linux sehr viel schneller abläuft, als in Windows und damit keine Gefahr besteht, dass sich Personen während der kurzzeitigen Anpassung am System anmelden.

Beachten Sie, dass der Eintrag **Partition in die installiert werden soll** leer bleibt, da automatisch die von LD Deploy angelegten Partitionen verwendet werden..



Übernehmen Sie die Anpassungen für das neue Betriebssystem mit **SPEICHERN**.

IV.1.10.2. Linux Master-Installation durchführen

Ähnlich wie bei Windows stellt SBE selbst kein fertiges Betriebssystem zur Verfügung. Sie müssen dieses selbst neu aufbauen, was entsprechendes tiefgehendes Know-how im Linux-Bereich voraussetzt.



Achtung

Bitte beachten Sie, dass SBE für die Installation von Linux keinerlei Support leistet und Sie selbst das entsprechende Know-how bereitstellen oder von externer Stelle einkaufen müssen.

Die hier gemachten Angaben sollen lediglich dabei helfen, die notwendigen Voraussetzungen bei Ihrer eigenen Linux-Installation mit der entsprechend ausgewählten Distribution zu beachten.

Diese Voraussetzungen sind notwendig aber nicht hinreichend für die grundlegende Funktionsfähigkeit.

Das Vorgehen wird auf Basis der Distribution Ubuntu 20.04 gezeigt und dabei lediglich stichpunktartig aufgeführt, was zu beachten ist und welche Voraussetzungen zu erfüllen sind.

Grundsätzlich gliedert sich die Installation in drei Abschnitte:

1. Download und Grundinstallation Ihrer gewünschten Distribution
2. Spezifische Anpassung für LD Deploy

3. Erstellen eines tar.gz Archivs

IV.1.10.2.1. Download und Installation Ubuntu 20.04 LTS

Laden Sie die ISO-Datei für Ihre Linux-Distribution von einer entsprechende Quelle aus dem Internet (<https://releases.ubuntu.com/20.04/>) und übertragen Sie diese mittels eines Tools wie z.B. balenaEtcher (<https://www.balena.io/etcher/>) auf einen bootbaren Stick.

Führen Sie die Installation entsprechend den Hinweisen im Internet durch.



Tipp

Führen Sie die Installation so durch, dass Ihr Linux zunächst das einzige System auf der Festplatte bzw. SSD ist. Lassen Sie bestehende Partitionen durch den Installer löschen.

Nach der Basis-Installation müssen einige Anpassungen vorgenommen und damit Anforderungen erfüllt werden, damit Ihr Linux-Client in der Umgebung mit LD Deploy bzw. LogoDIDACT grundlegend funktioniert.

IV.1.10.2.2. Voraussetzungen

Die folgenden Anforderungen sind nur in Stichpunkten aufgeführt und für den Linux-Fachmann selbsterklärend.

"Abhängigkeit" bedeutet im Prinzip, dass das jeweilige Paket per **apt-get install PAKET-NAME** installiert werden muss aber dies keine Garantie dafür ist, dass jede Version dieses Paketes funktioniert. Zuvor muss man per **sudo -i** in den Kontext des Benutzers **root** wechseln.

1. Agent herunterladen

Struktur für Agent anlegen

```
cd /var/lib/
```

```
mkdir -p /logoDIDACT/Deploy/Agent
```

Archiv und Prüfsumme vom Deploy-Container herunterladen und Prüfsumme vergleichen

```
wget http://deploy/agent/ld-deploy-agent.tar.gz
```

```
wget http://deploy/agent/ld-deploy-agent.tar.gz.md5
```

In Verzeichnis wechseln und Archiv entpacken:

```
cd /logoDIDACT/Deploy/Agent
```

```
tar xfvz /var/lib/logoDIDACT/Deploy/Agent ld-deploy-agent.tar.gz
```

2. Agent als Service installieren (Voraussetzung systemd)

Ins Verzeichnis von systemd wechseln und die Datei für den Dienst anlegen bzw. herunterladen:

```
cd /etc/systemd/system
```

```
wget https://files.sbe.de/ld-deploy/ld-deploy-agent.service
```

Der Inhalt der Datei sieht wie folgt aus, wobei die rot markierten Zeilenumbrüche # nicht vorhanden sind und auch nicht vorhanden sein dürfen!

```
[Unit]
Description=logoDIDACT Deploy Agent

[Service]
Type=simple
WorkingDirectory=/var/lib/logoDIDACT/Deploy/Agent
ExecStart=/var/lib/logoDIDACT/Deploy/Agent/jdk/bin/java -D
java.rmi.server.hostname=127.0.0.1 -Dlog4j.configurationFile=
/var/lib/logoDIDACT/Deploy/Agent/etc/log4j2-linux.xml
-jar /var/lib/logoDIDACT/Deploy/Agent/lib/ld-deploy-agent.jar

[Install]
WantedBy=multi-user.target
```

Systemctl Konfiguration neu laden, Dienst aktivieren und starten:

```
systemctl daemon-reload
```

```
systemctl enable ld-deploy-agent.service
```

```
systemctl start ld-deploy-agent.service
```

3. Für den Systemstart muss **initramfs** auch **btrfs** enthalten

Das Dateisystem **btrfs** ist normalerweise Bestandteil des Kernels, sollte aber geprüft werden:

```
lsinitramfs -l /boot/initrd.img | grep btrfs
```

4. Symlinks erstellen lassen

Damit LD Deploy unabhängig von einer Distribution funktioniert, erwartet es zur Konfiguration des Grub-Bootloaders symbolische Links auf **/boot**-Ebene.

Da es nach jedem Kernelupdate einen neuen Satz von **vmlinuz*** und **initrd*** Dateien in **/boot** gibt, empfiehlt es sich diese Symlinks automatisch per Skript erstellen zu lassen.

Wechseln Sie ins Verzeichnis **/etc/kernel.postinst.d** und laden Sie das entsprechende Skript herunter und ausführbar machen:

```
wget https://files.sbe.de/ld-deploy/update-symlinks
```

```
chmod +x update-symlinks
```

Der Inhalt sollte wie folgt aussehen:

```
#!/bin/bash

set -ex

echo "Linking kernel for ld-deploy..."

KERNEL_VERSION="$1"
```

```

KERNEL_IMAGE="$2"

# links in /boot
cd /boot
ln -sf vmlinuz-${KERNEL_VERSION} vmlinuz
ln -sf initrd.img-${KERNEL_VERSION} initrd.img
cd -

```

Zumindest bei Ubuntu ist es so, dass beim Aufruf dieses Skripts die notwendigen KERNEL-Infos als Variable \$1 und \$2 an das Skript übergeben werden. Das ist bei anderen Distributionen möglicherweise nicht der Fall und muss entsprechend anders gelöst werden.

5. Deployment Progress

Display-Manager mit Service-Unit (getestet mit Gnome Display Manager)

```
/etc/systemd/system/display-manager.service
```

6. Ansible

sshd muss aktiviert und der SSH Port 22 in der Firewall freigegeben sein. Im Falle von Ubuntu 20.04 kann der Port über die vereinfachte Verwaltungsschnittstelle UFW (Uncomplicated Firewall) aktiviert werden.

```
$ sudo ufw allow 22
```

7. Notwendige Pakete und Abhängigkeiten

Für LD Control-Agent **ruby** und **x11vnc**

Für LD Deploy-Agent **libappindicator1**

Für Domänen-Beitritt **sssd**, **realmd**, **sssd-dbus** und **pam_mount?** (libpam-mount?)

8. LD-Deploy-Panel

TrayIcons und Startup Applications müssen aktiviert sein. Alternativ ist das Alias **ld-deploy** über `/etc/profile.d` einbindbar.

9. SSL-Zertifikate

Das System muss der ca-chain vertrauen. Automatisiert für Fedora und Ubuntu.

10. Optional

ld-su-setup für den jeweiligen Display-Manager vom Login-Screen ausschließen.

11. Skel

Die Datei `/etc/pam.d/common-session` um Folgendes erweitern:

```
session required pam_mkhomedir.so skel=/etc/skel/umask=0022
```

IV.1.10.2.3. Archiv bauen und auf Server kopieren

Der dritte Schritt besteht darin, ein Archiv als `.tar.gz` zu erstellen, das dann in der LD-Deploy Umgebung am Server eingebunden werden kann. Dazu wechselt man ins `root`-Verzeichnis und erstellt

ein Archiv als `.tar.gz`. Dabei sollten bzw. müssen bestimmte Verzeichnisse (`dev`, `proc`, `run`, `sys`, `tmp` usw.) exkludiert werden:

```
cd /
```

```
tar cfvz ubuntu2004.tar.gz /
```

Kopieren Sie das Archiv anschließend direkt in den Deploy-Container auf dem Server:

```
rsync -av ubuntu2004.tar.gz root@deploy.schule.local:/var/lib/
deploy/qBittorrent
```

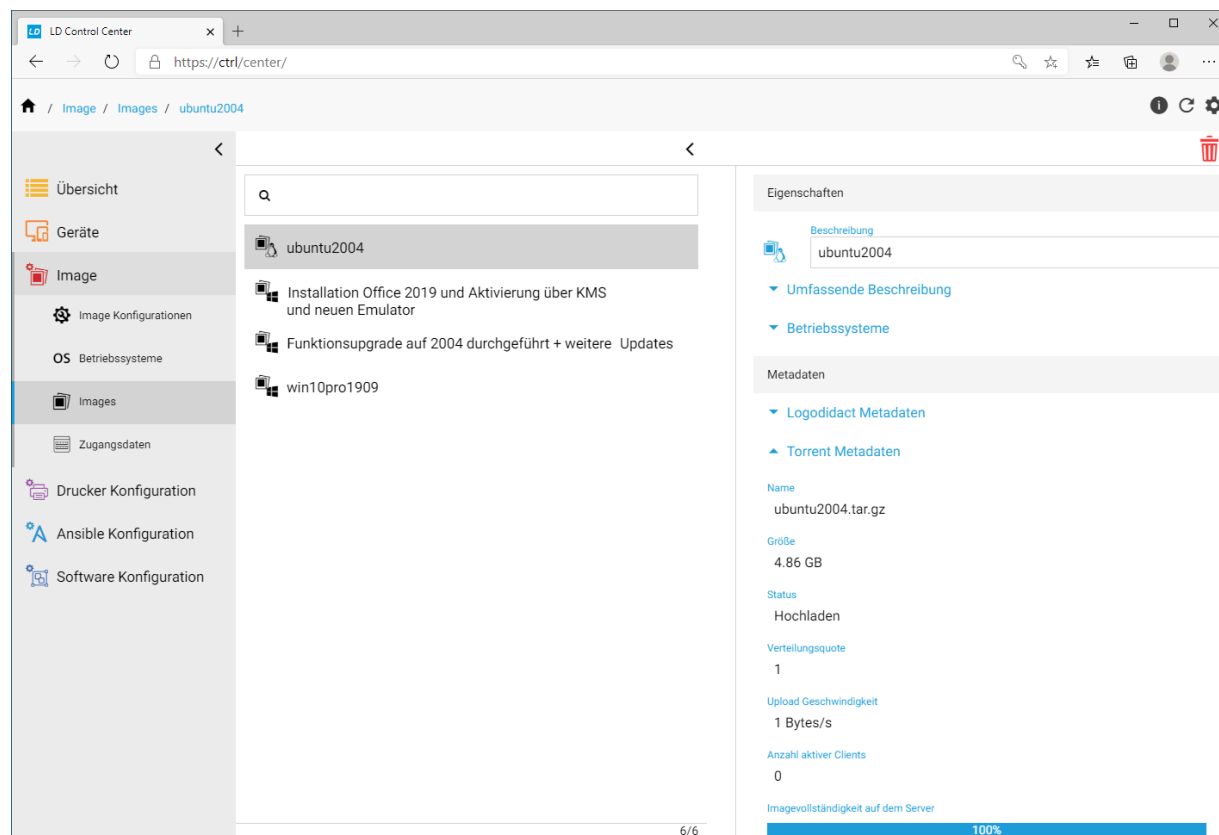
IV.1.10.3. Linux Image importieren und zuweisen

Wechseln Sie dann auf Serverseite in den Container `deploy-g1` und dort in das oben angegebenen Ziel-Verzeichnis. Importieren Sie das Image, wie auch in Abschnitt III.5.7.2, „Image importieren“ beschrieben:

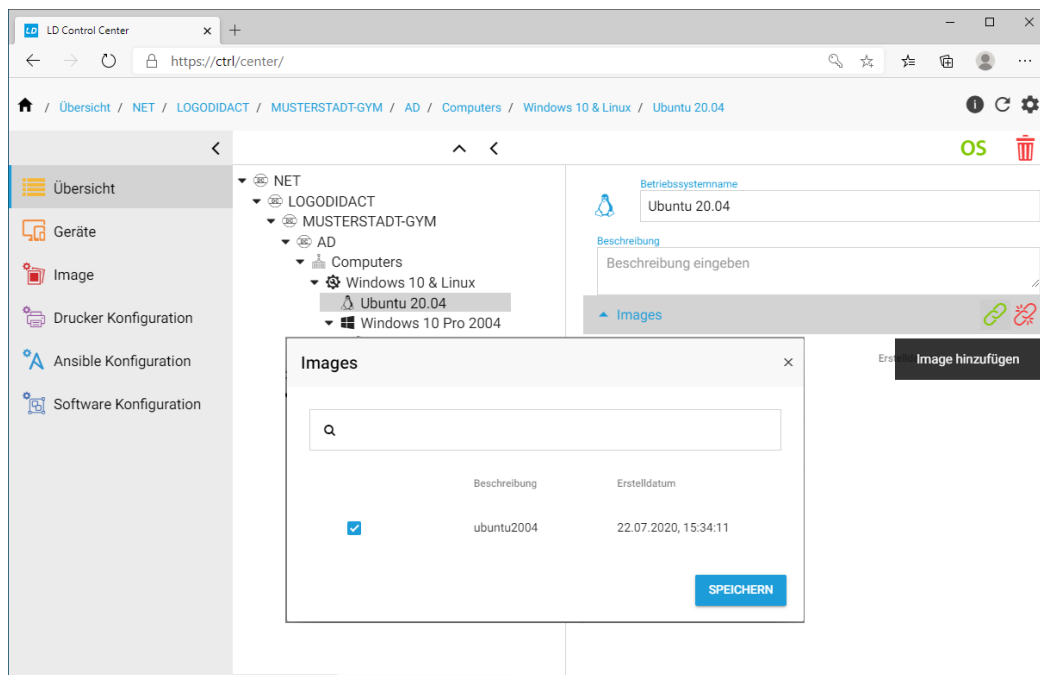
```
chown deploy:deploy ubuntu2004.tar.gz
```

```
ld-control-client image add --description ubuntu2004 --file
ubuntu2004.tar.gz
```

Der Fortschritt des Imports kann im Control Center geprüft werden.



Die Zuweisung des Betriebssystems erfolgt auf Ebene der Konfiguration im Abschnitt **Images**.



IV.1.10.4. Linux-Image am Client aufspielen

Durch die Konfiguration des Parallelbetriebs werden nun an Clients mit dieser Konfiguration beim ersten Start folgende Schritte durchgeführt:

1. Die Platte (SSD) wird neu partitioniert
2. Beide Betriebssysteme werden per Torrent parallel heruntergeladen
3. Das erste Betriebssysteme (hier Windows 10) wird auf die Platte geschrieben und das komplette Setup durchgeführt
4. Das zweite Betriebssysteme (hier Ubuntu 20.04) wird auf die Platte geschrieben und das komplette Setup durchgeführt

Kapitel IV.2. LogoDIDACT-Agent und Console

Der LogoDIDACT-Agent ist die Komponente in LogoDIDACT, die eine Interaktion zwischen dem Server und den Arbeitsstationen oder auch direkt zwischen den Arbeitsstationen ermöglicht. Der LogoDIDACT-Agent steht in Verbindung mit dem Server und übernimmt dabei viele verschiedene Aufgaben, angefangen von der Bildschirmübertragung bis hin zur Ausgabe von Statusmeldungen an der Arbeitsstation oder den Aktionen zum Sperren oder Freigeben von lokal angeschlossenen Geräten wie Maus, Bildschirm, Tastatur und USB-Sticks.

Weitere Systemkomponenten wie z.B. der Idcmaster sorgen dafür dass der LogoDIDACT-Agent automatisch aktualisiert wird, sofern es auf Serverseite eine aktuellere Version gibt. Die Versionierung des LogoDIDACT-Agent ist am Client leicht ersichtlich und orientiert sich am Datum der Freigabe, d.h. die Version 10.4.15 des LogoDIDACT-Agent wurde am 14.05.2010 freigegeben.

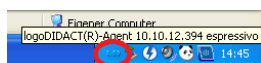


Abbildung IV.2.1. Version des LogoDIDACT-Agent am Client anzeigen

Während der LogoDIDACT-Agent gewissermaßen im Hintergrund seine Arbeit verrichtet ist die LogoDIDACT-Console derjenige Teil von LogoDIDACT mit dem der Anwender (Lehrer) arbeitet. Die LogoDIDACT-Console stellt dabei die Steuerzentrale dar sowohl für Arbeitsstationen als auch Benutzer.

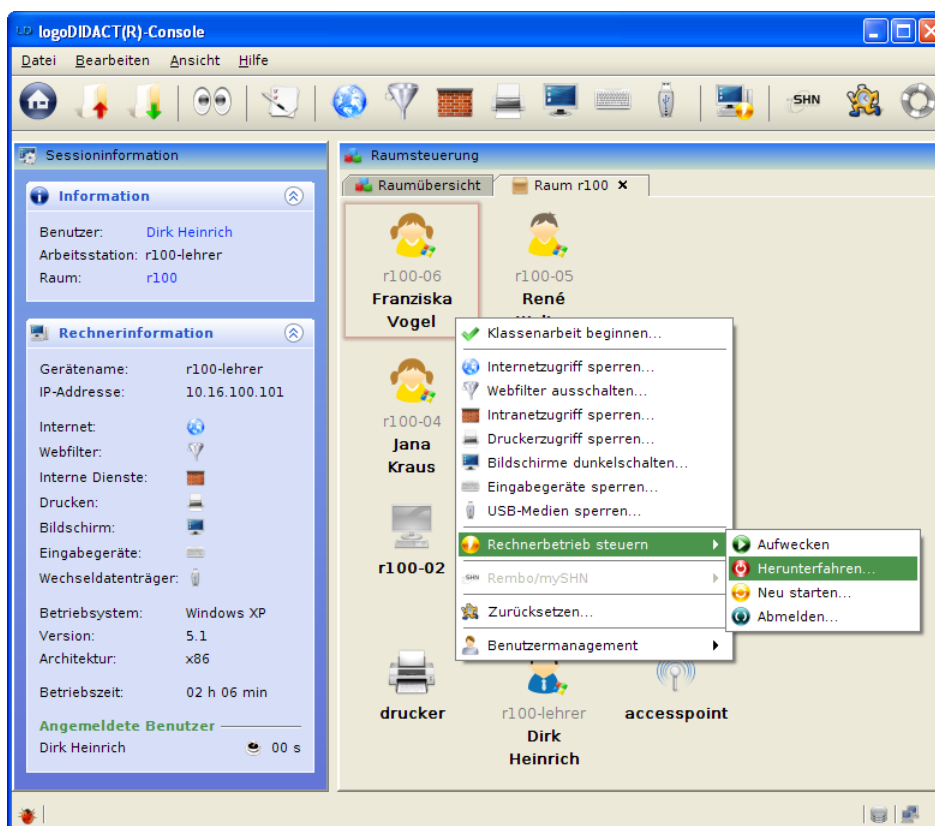


Abbildung IV.2.2. Die LogoDIDACT-Console als Steuerzentrale

IV.2.1. Installation unter Windows

In diesem Kapitel wollen wir auf die Installation bzw. Integration der Clients unter LogoDIDACT eingehen.



Wichtig

Führen Sie die nachfolgenden Installationsanweisungen mit dem vordefinierten Domänen-Benutzer `pgmadmin` (siehe ????) aus.

Beide Anwendungen wurden hauptsächlich in der Programmiersprache Java entwickelt, sodass diese als Voraussetzung für die Ausführung dient und vor der Installation dieser Programme auf dem Zielsystem vorhanden sein muss. Ab der Version 10.4.15 liegt im Installationsverzeichnis auch die notwendige Java-Version, die automatisch verwendet wird.



Tipp

Führen Sie vor der Installation ein Update Ihres LogoDIDACT-Servers aus (siehe Abschnitt II.1.3.4, „LogoDIDACT Update“). Dadurch werden auch die mitgelieferten Installer für LogoDIDACT-Agent und Console aktualisiert.

Beginnen Sie jetzt mit der Installation von LogoDIDACT-Agent und LogoDIDACT-Console. Verwenden Sie dazu die mitgelieferten Installer, die Sie im Verzeichnis `P:\Install\logoDIDACT Agent` bzw. `P:\Install\logoDIDACT Console` finden.

Nach der Installation der beiden Komponenten, müssen Sie den Computer in der Regel neu starten. Selbstverständlich müssen Sie diesen Neustart zunächst ohne Heilung durchführen. Fahren Sie danach den Rechner herunter und erstellen Sie ein Image.

Teil V. Administration und Betrieb

Für wen dieser Teil gedacht ist

Dieser Teil der Dokumentation ist vor allem für diejenigen Lehrer an Schulen gedacht, die für ihre Kollegen und Kolleginnen als Ansprechpartner in Sachen EDV tätig sind. In der Dokumentation wird diese Position öfters neutral als ITB (IT Betreuer) bezeichnet. Je nach Region sind die Bezeichnungen sehr verschieden und reichen von Multimediaberater bis hin zu Medienbeauftragter oder einfach nur EDV-Betreuer. Die Tätigkeiten, die ein ITB durchführen können soll bzw. muss sind etwas anspruchsvoller, als das, was ein "normaler" Lehrer vom Gesamtsystem wissen muss. Die Aufgaben sind aber gleichzeitig nicht so, dass der ITB irgendwelche tiefgehenden Systemkenntnisse benötigt.

Die typischen Aufgaben, die man als IT-Betreuer durchführen kann und soll:

- - Anlegen und Versetzen von Benutzern zum Schuljahreswechsel oder auch während des Schuljahres
 - - Installation und Verteilung von Software mit
 - - Ansprechpartner sein für alles, was es an kleineren Problemen mit Druckern, Computern, Software und sonstigen Dingen im Netzwerk gibt
 - - Ansprechpartner nach Außen sein für den externen Dienstleister (Systemhaus)
 - - Auswerten von Systeminformationen/Statistiken
 - - Überwachung des Servers und der Dienste
-

Kapitel V.1. Anleitung LogoDIDACT-Console

V.1.1. Benutzerverwaltung

Die Benutzerverwaltung der LogoDIDACT-Console lässt sich über das Menü „Ansicht“ und der Tastenkombination **Alt+U** aufrufen.

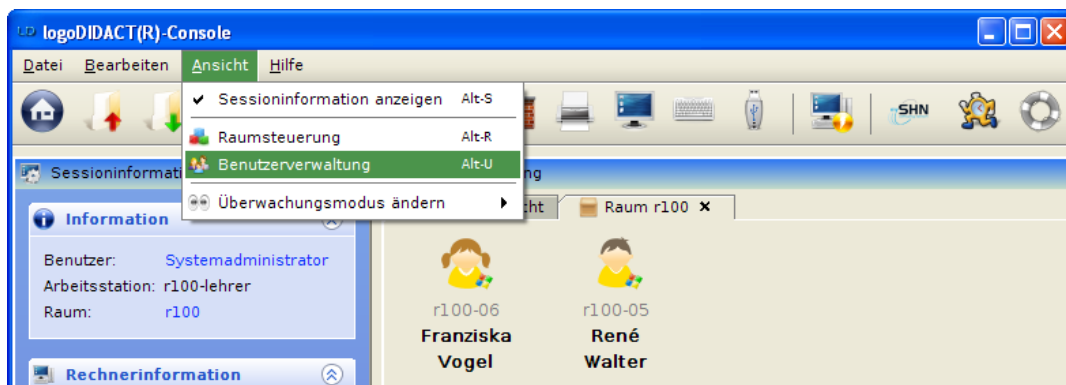


Abbildung V.1.1. Benutzerverwaltung aufrufen (über Menü „Ansicht“)



Achtung

Grundsätzlich sollten Benutzer in LogoDIDACT immer über Listen angelegt und gepflegt werden und nicht einzeln.

Nur über den Listenimport spart man viel Zeit und Aufwand und nur darüber ist ein automatisches Versetzen beim Schuljahreswechsel möglich.

Nur der Listenimport bietet die Möglichkeit viele Aufgaben zu automatisieren und Hunderte oder gar Tausende Benutzer leicht zu verwalten.

Schüler die manuell angelegt werden, können im Nachhinein nicht mehr über den Listenimport versetzt werden.

Auch Lehrer sollten über den Listenimport angelegt werden. Das Hinzufügen eines einzelnen Lehrers kann praktikabel direkt in der Importliste erfolgen.

Wenn man zum ersten Mal Benutzer anlegt, d.h. dies im Zusammenhang mit der Installation von LogoDIDACT macht, dann erklärt der nächste Abschnitt das Vorgehen.

Wenn das System bereits läuft und Benutzer aus dem letzten Jahr angelegt waren, dann geht es nun um das Versetzen, Neuanlegen oder auch Nachpflegen der Benutzer. Dies wird in Abschnitt V.1.1.2, „Versetzen, Löschen und Anlegen beim Schuljahreswechsel“ behandelt.

V.1.1.1. Anlegen neuer Benutzer über Listen



Tipp

In der Registerkarte „Importieren“ → „Bearbeiten“ gibt es bereits mehrere vordefinierte Benutzerlisten für Kurse, Schüler und Lehrer, die genutzt werden können.

Über den Eintrag „Benutzerliste anlegen“ in der Symbolleiste und im Kontextmenü können jedoch auch eigene Benutzerlisten erstellt werden.



Abbildung V.1.2. Benutzerliste anlegen (über Symbolleiste)

Bei den erwähnten Benutzerlisten handelt es sich um einfache Textdateien mit strukturierten Daten.

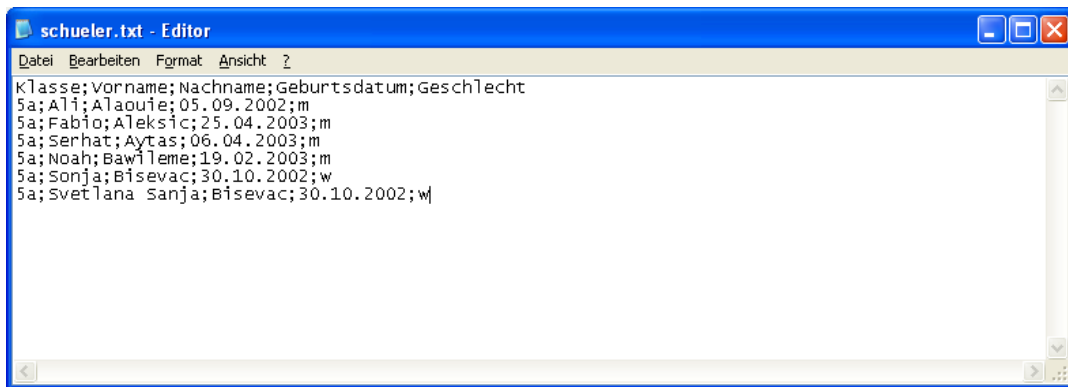


Abbildung V.1.3. Aufbau einer Benutzerliste („schueler.txt“)

Jede Zeile entspricht dabei einem Datensatz, der durch Trennzeichen wie Semikolon, Komma oder Ähnliches in beliebige Datenfelder (Spalten) unterteilt wird.



Tip

Benutzerlisten für Schüler, Lehrer oder sonstige Benutzer lassen sich auch aus den meisten Schulverwaltungsprogrammen als TXT oder CSV (Comma Separated Values) Datei exportieren und in die LogoDIDACT-Console laden.



Anmerkung

Eine Schritt für Schritt Anleitung zum Anlegen eines Export-Filters und Durchführen des Daten-Exports unter SchILD-NRW und SCHULKARTEI (BaWü) befindet sich im Anhang B. Schulverwaltungsprogramme.

Im Dialog zum Erstellen neuer Benutzerlisten wird zunächst in der Registerkarte „Inhalt“ die gespeicherte Textdatei mit den Daten der Schüler oder Lehrer über den Button „Laden...“ in die Benutzeroberfläche geöffnet.

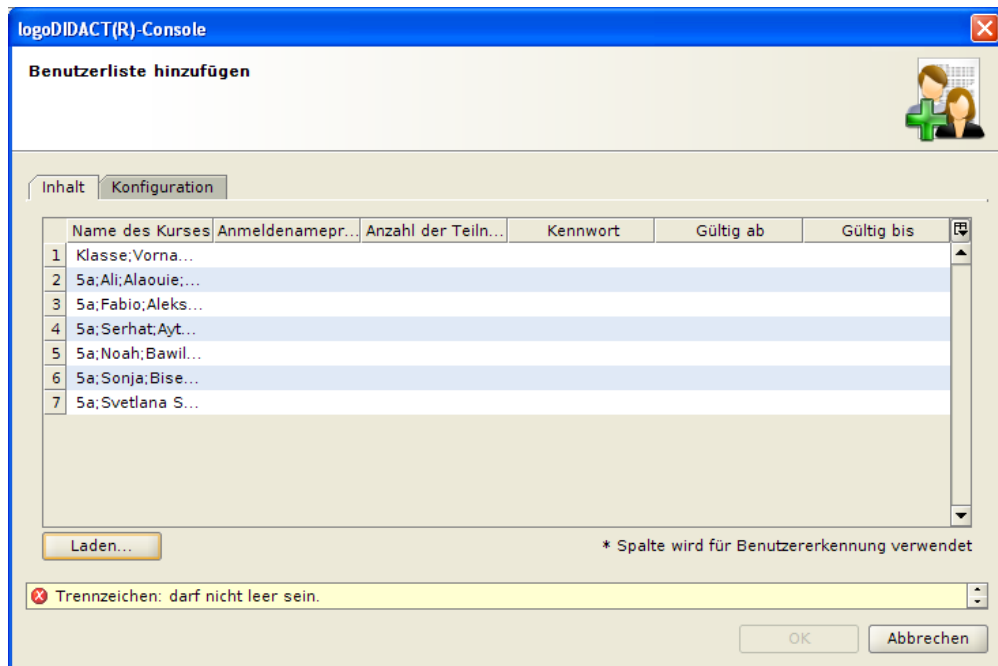


Abbildung V.1.4. Benutzerliste anlegen („Inhalt“)

Über die Registerkarte „Konfiguration“ werden anschließend Eigenschaften und Einstellungen für die Benutzerliste festgelegt.

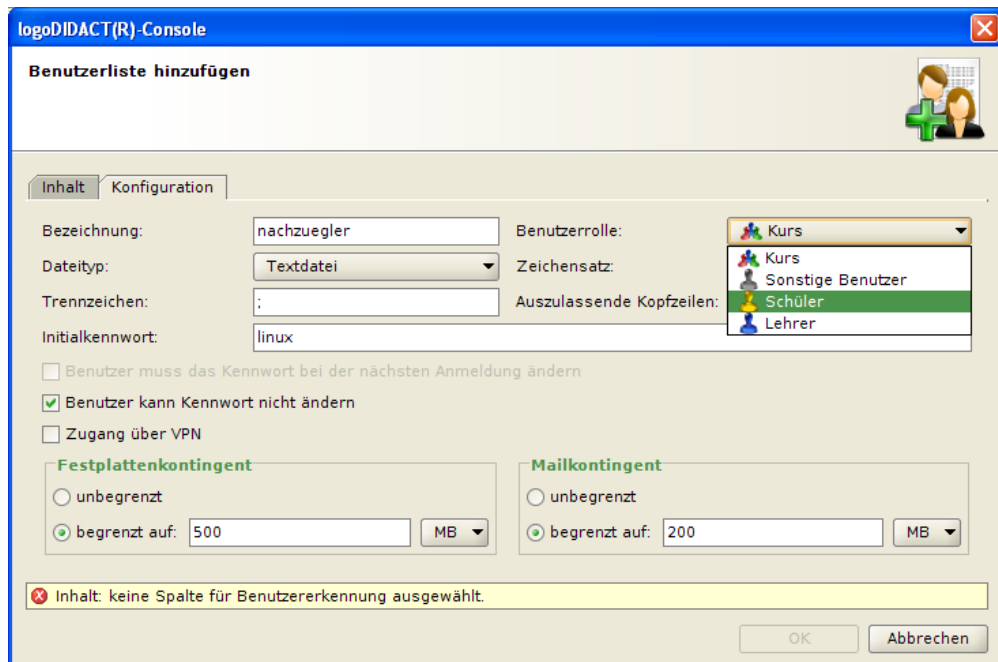


Abbildung V.1.5. Benutzerliste anlegen („Konfiguration“)

Nachdem alle Angaben gemacht wurden, werden die einzelnen Datenfelder der Benutzerliste in der Registerkarte „Inhalt“ als Spalten erkannt.

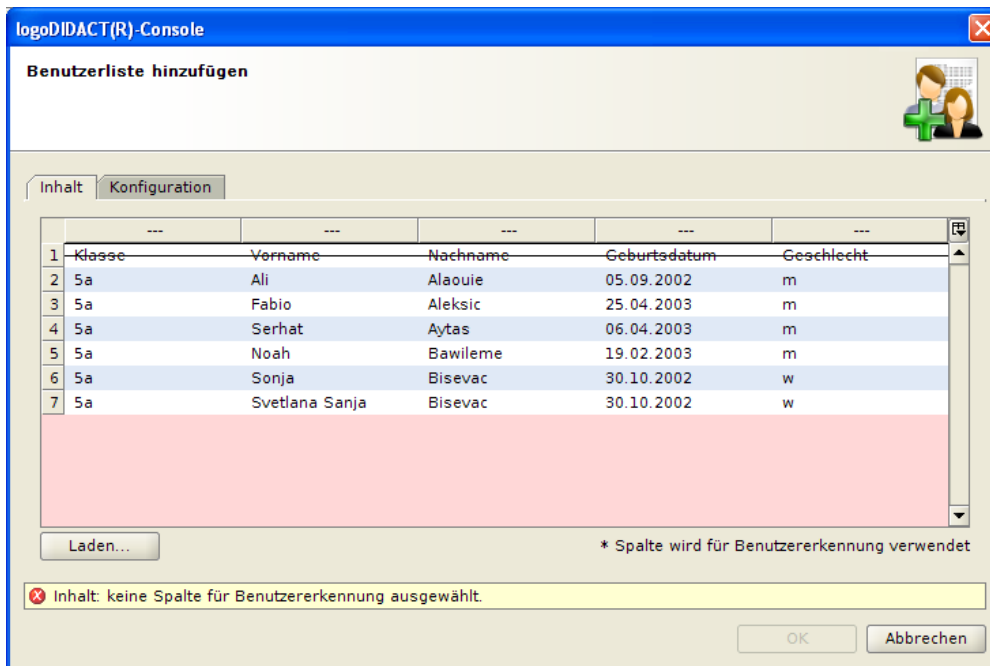


Abbildung V.1.6. Benutzerliste anlegen („Inhalt“)



Tipp

Über Rechtsklick lässt sich ein Kontextmenü öffnen und nachträglich Benutzer in die Liste hinzufügen oder entfernen. Mit Doppelklick können die Inhalte der Datenfelder bearbeitet werden. Beachten Sie jedoch, dass diese Änderungen NUR auf dem LogoDIDACT Server gespeichert werden und NICHT in der Schulverwaltung, d.h. beim nächsten Laden und Speichern einer Benutzerliste werden diese Anpassungen nicht berücksichtigt und dementsprechend überschrieben.

Die Spalten müssen noch den Feldern der Benutzerdatenbank zugeordnet werden. Ein Klick auf den leeren Spaltenkopf öffnet den dazugehörigen Dialog.



Achtung

Für die Benutzererkennung sollten möglichst eindeutige Datenfelder gewählt werden. Bei den Schülern sind das Nachname, Vorname und Geburtsdatum und bei den Lehrern das Kürzel.

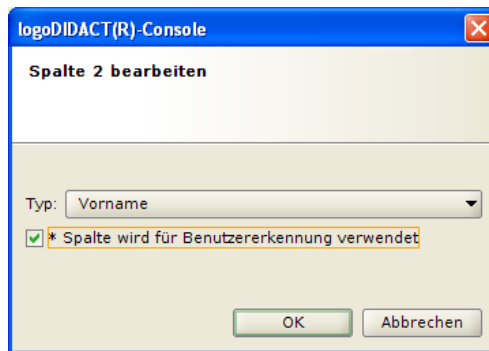


Abbildung V.1.7. Spaltentyp bearbeiten

Nachdem alle Spalten der Benutzerliste richtig zugewiesen wurden, kann der Dialog über den Button „OK“ geschlossen werden. Die neue Benutzerliste wird jetzt im System erstellt.

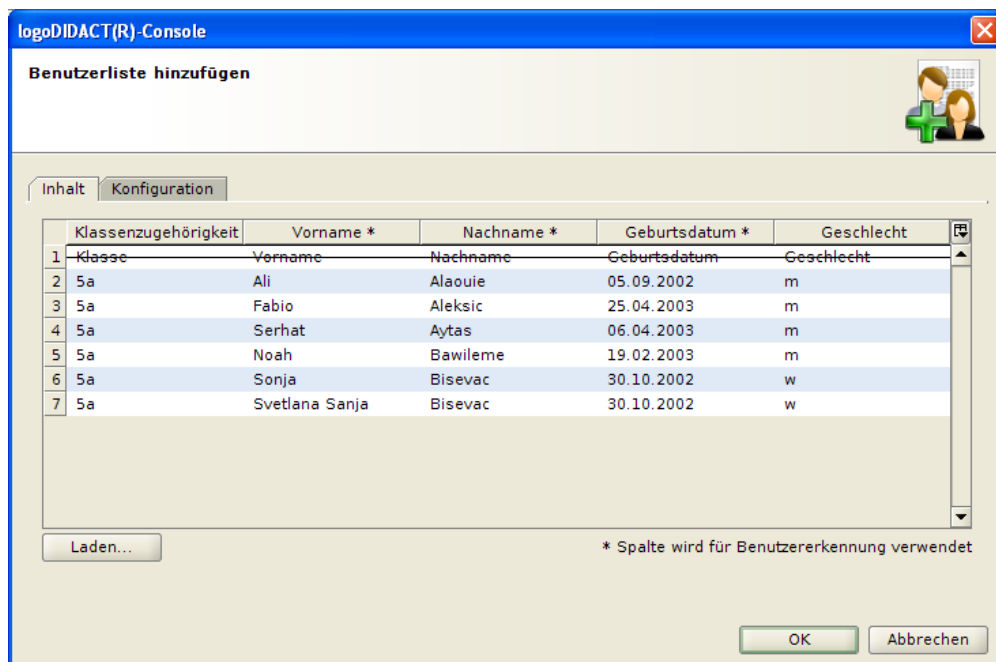


Abbildung V.1.8. Benutzerliste anlegen („Inhalt“)

In der Registerkarte „Importieren“ → „Ausführen“ müssen die Benutzerlisten anschließend noch auf Fehler überprüft und ins System importiert werden.

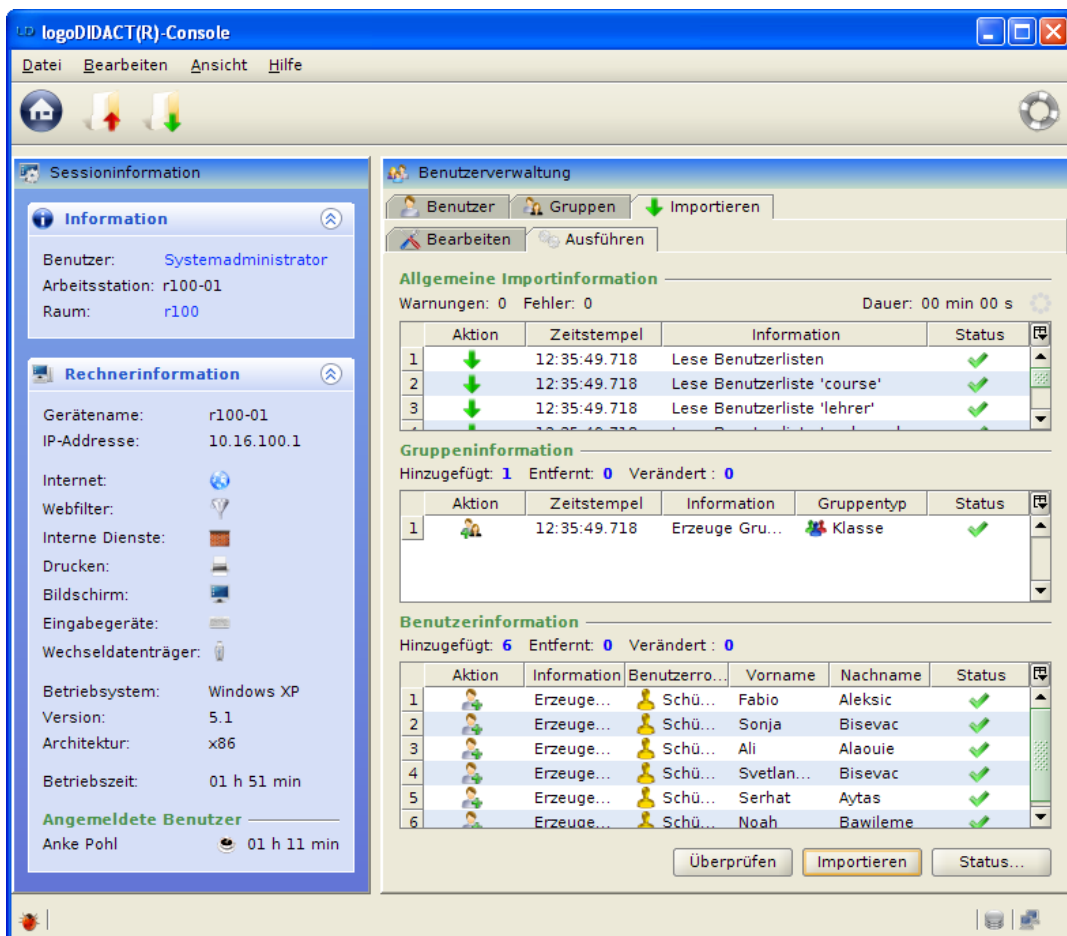


Abbildung V.1.9. Benutzerlisten überprüfen und importieren



Tipp

Exportieren Sie im neuen Schuljahr aktuelle Schüler- und Lehrer Textdateien aus Ihrem Schulverwaltungsprogramm und laden Sie diese jeweils einzeln über die LogoDIDACT-Console in die entsprechenden (bereits konfigurierten) Benutzerlisten aus dem Vorjahr. Der Inhalt der Benutzerlisten wird dadurch aktualisiert. Sofern Sie keine neuen Spalten exportiert haben, können Sie die Benutzerlisten einfach übernehmen und importieren. Die Schüler werden anschließend automatisch entsprechend den (neuen) Informationen ins nächste Schuljahr versetzt oder nicht.

V.1.1.2. Versetzen, Löschen und Anlegen beim Schuljahreswechsel

Der Ablauf beim Versetzen ist ähnlich zu dem beim ersten Listenimport, bzw. beim ersten Anlegen der Benutzer unmittelbar nach der Inbetriebnahme.

Es gibt in LogoDIDACT keine spezielle Schaltfläche mit der Funktion "Versetzen", der die Schüler der Klasse 3a in die Klasse 4a versetzen würde. Das Versetzen erfolgt vielmehr im Zusammenhang mit dem Import einer neuen Schülerliste, die man aus der Schulverwaltungssoftware exportiert.

Das Sekretariat einer Schule verwaltet in der Regel die Schüler der Schule mit einer entsprechenden EDV-Software und das Versetzen oder Nichtversetzen wird dort vor Beginn oder zu Anfang des neuen

Schuljahres durchgeführt. Ebenso werden dort neue Schüler angelegt oder die Schulabgänger gelöscht oder ausgepflegt. Die dort exportierte Schülerliste beschreibt somit die derzeitige Benutzer-Situation, aus der sich über den Import einer einzigen Liste alle Aktionen ableiten lassen:

- Schüler wird versetzt
(ist in der neuen Liste z.B. in der Klasse 4a und war vorher in 3a)
- Schüler überspringt eine Klassenstufe
(ist in der neuen Liste z.B. in der Klasse 5c und war vorher in 3a)
- Schüler wird nicht versetzt
(ist in der neuen Liste z.B. in der Klasse 4a und war vorher auch in 4a)
- Schüler ist Schulabgänger
(ist nicht mehr in der neuen Liste. Es wird erkannt, dass der Schüler über den Listenimport angelegt wurde und jetzt gelöscht werden soll)
- Schüler ist neu
(ist bisher nicht im System und wird deshalb neu angelegt)

V.1.1.2.1. Schritt 1: Starten der Benutzerverwaltung als Administrator

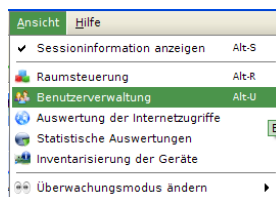


Abbildung V.1.10. Benutzerverwaltung starten

V.1.1.2.2. Schritt 2: Registerkarte Import und Auswahl der Schülerliste



Abbildung V.1.11. Aktuelle Schülerimportliste anzeigen

V.1.1.2.3. Schritt 3: Prüfen der derzeitigen (alten) Schülerliste

Die angezeigte Liste spiegelt den derzeitigen Zustand der Benutzer wider, bzw. zeigt die zuletzt importierte Benutzerliste an.

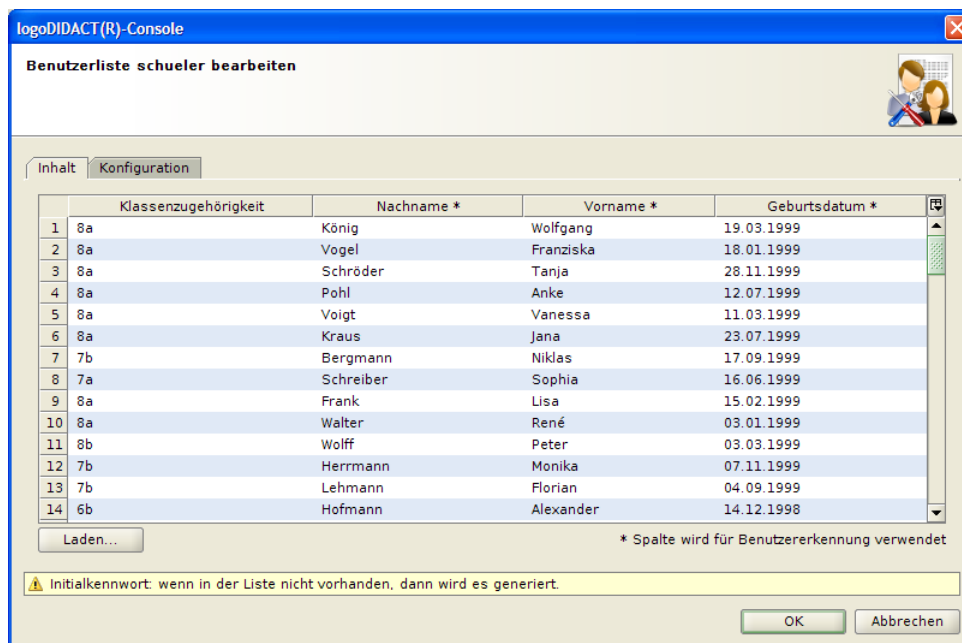



Abbildung V.1.12. Schülerliste prüfen

 **Tipp**

Bevor Sie sich die aktuelle (neue) Schülerliste aus der Schulverwaltung besorgen, werfen Sie einen Blick auf die Reihenfolge der Felder (Spalten), wie diese beim letzten Import ausgesehen hat.

Ideal ist es natürlich, wenn Sie auch jetzt wieder die Daten in exakt dieser Reihenfolge der Felder aus der Schulverwaltung bekommen.

V.1.1.2.4. Schritt 4: Laden der neuen Schülerliste

Laden Sie die Schülerliste, die Sie von der Schulverwaltung entsprechend als Text- oder csv-Datei bekommen haben.

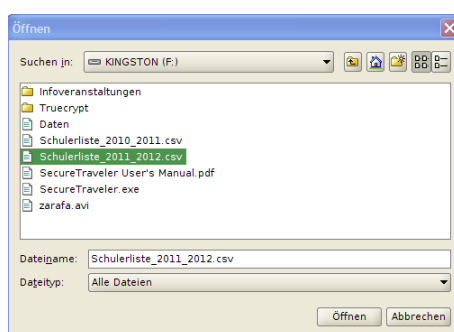


Abbildung V.1.13. Neue Schülerliste laden

V.1.1.2.5. Schritt 5: Neue Schülerliste prüfen

Sofern die eingelesene Liste die Benutzerdaten exakt in der Reihenfolge beinhaltet, wie das beim ersten Anlegen der Fall war, beschränkt sich das Prüfen eher auf die Änderung der Klassenbezeich-

nung einiger bestehender Schüler oder darauf, dass Abgänger nicht mehr in der Liste auftauchen und es auch neue Schüler gibt, die einem unbekannt erscheinen.

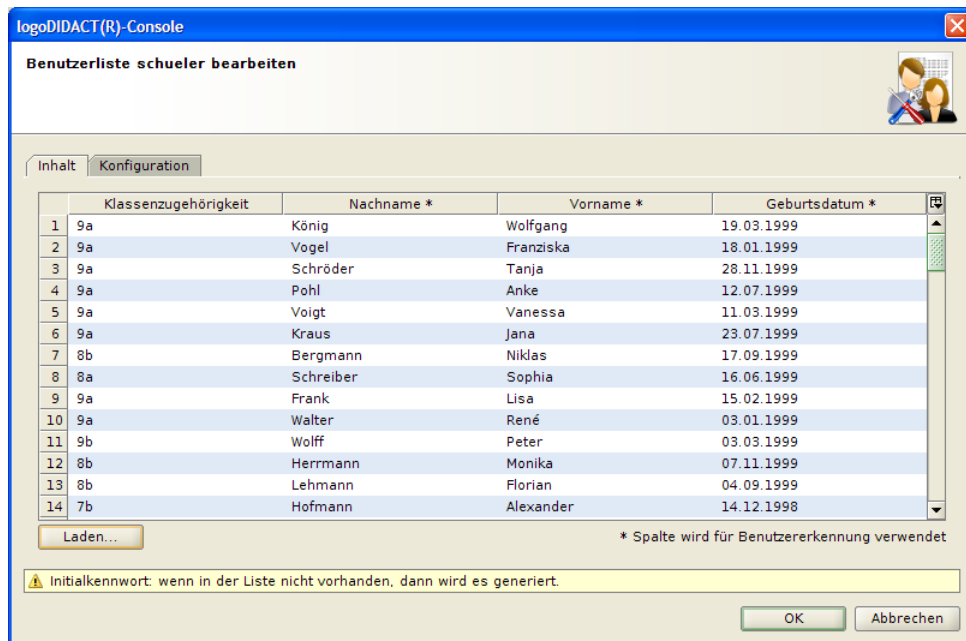


Abbildung V.1.14. Neue Schülerliste prüfen

Wenn sich die Reihenfolge der Daten in der Exportdatei geändert hat, gibt es zwei Möglichkeiten. Die erste besteht darin, die Daten nochmals aus der Schulverwaltung zu exportieren und dafür zu sorgen, dass die Reihenfolge entsprechend dem letzten Importvorgang angepasst wird.

Die Standardreihenfolge bei Schülern ist dabei **Klasse ; Nachname ; Vorname ; Geburtsdatum** wobei für das Erkennen eines Benutzers per Standard die Felder Nachname, Vorname und Geburtsdatum ausgewählt sind und auch ausgewählt sein sollten.

Die zweite Möglichkeit besteht im Anpassen der Importfelder. Dies ist exemplarisch in der folgenden Abbildung dargestellt, wobei dort eine Schülerliste geladen wurde, bei der die Daten der Spalten Vorname und Nachname vertauscht wurden. Um das anzupassen kann man direkt auf die Spaltenbezeichnung klicken und dort dann das Importfeld entsprechend den Daten in der Spalte anpassen.

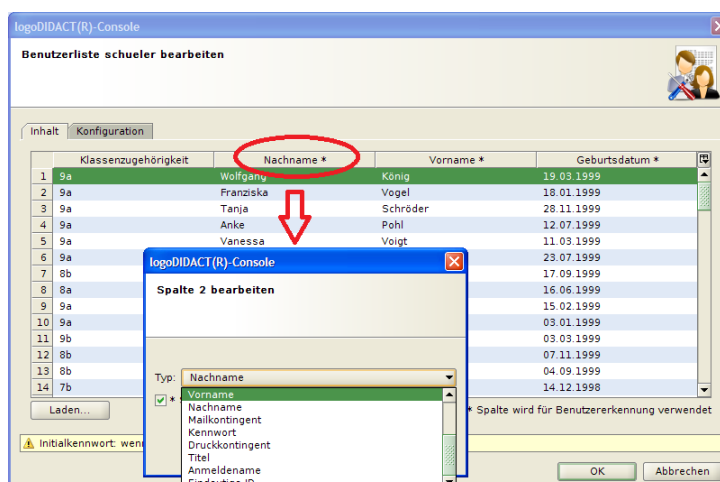


Abbildung V.1.15. Zuordnung zu Importfeld einer Spalte und den Daten prüfen und gegebenenfalls anpassen.

V.1.1.3. Anlegen einzelner Benutzer



Achtung

Das Anlegen einzelner Nutzer sollte nur in speziellen Ausnahmefällen gemacht werden, wenn es über eine Liste nicht geht.

Weder Lehrer noch Schüler sollten so angelegt werden!

Lehrer und Schüler können zu jeder Zeit auch einzeln über den Listenimport angelegt werden, indem man dort direkt in der jeweiligen Liste den Benutzer anlegt und dann den Import durchführt.

Ein Beispiel aus der Praxis, welches das einzelne Anlegen eines Benutzers rechtfertigt, sind Konten für den Hausmeister oder die Sekretärin, die im System nicht in der Gruppe der Lehrer geführt werden sollten, aber trotzdem einen Zugang benötigen. Auch Konten für Austauschschüler kann man durchaus auch manuell einpflegen, sofern sich eine separate Liste nicht lohnt und es bei diesen Benutzern nur darum geht, z.B. einen Zugang zum Internet zu ermöglichen.

Über den Eintrag „Benutzer anlegen“ in der Symbolleiste und im Kontextmenü wird der Dialog zum Erstellen neuer Benutzer aufgerufen.

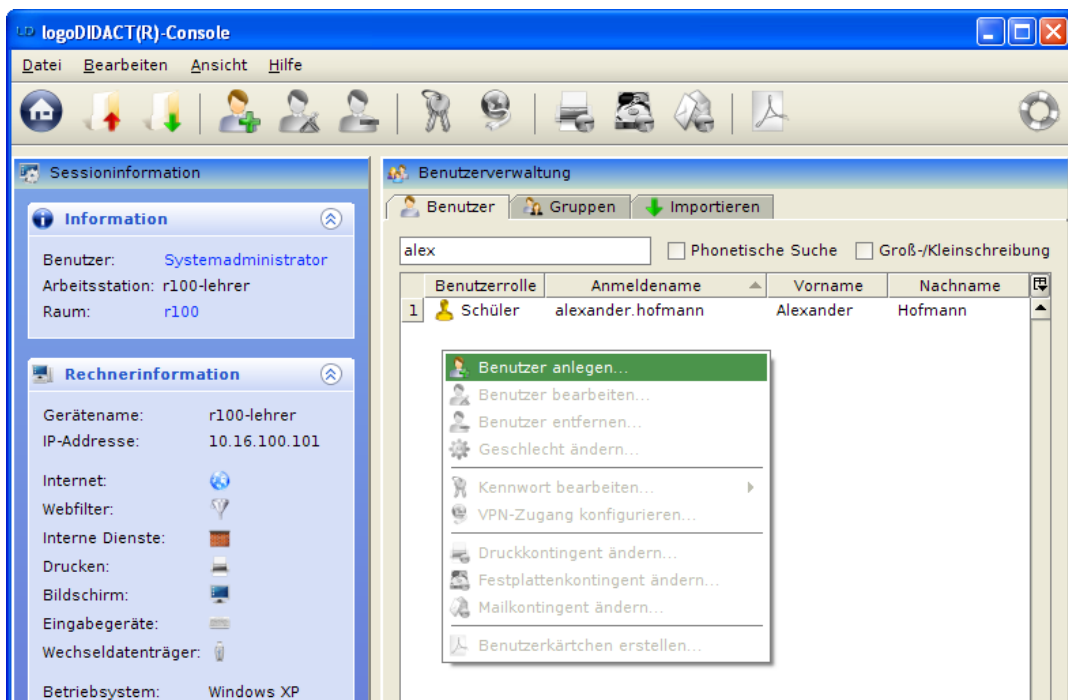


Abbildung V.1.16. Benutzer anlegen (über Kontextmenü)



Achtung

Im oberen Teil der Beschreibung findet sich ein Hinweis, dass Schüler und Lehrer zu importieren sind. Über den verlinkten Text gelangt der Anwender an die richtige Stelle in der LogoDIDACT-Console.

Die rot gekennzeichneten Textfelder und Registerkarten gehören zu den Pflichtangaben und müssen dementsprechend richtig ausgefüllt werden.

LogoDIDACT(R)-Console

Benutzer hinzufügen

Schüler oder Lehrer sollen über die [Import-Funktion](#) angelegt werden, da manuell hinzugefügten Benutzer beim Import-Vorgang nicht berücksichtigt werden.

Allgemeine Information
 Anmeldeinformation
 Kontingente

Nachname: Müller Vorname: Hendrik

Geburtsdatum: 13.10.1975 Geschlecht: ♂ männlich

Kommentar:

Benutzerrolle:

- Schüler
- Sonstige Benutzer
- Administrativer Benutzer
- Lehrer

Benutzerrolle: darf nicht leer sein.

OK Abbrechen

Abbildung V.1.17. Benutzer anlegen („Allgemeine Information“)

LogoDIDACT(R)-Console

Benutzer hinzufügen

Schüler oder Lehrer sollen über die [Import-Funktion](#) angelegt werden, da manuell hinzugefügten Benutzer beim Import-Vorgang nicht berücksichtigt werden.

Allgemeine Information
 Anmeldeinformation
 Kontingente

Anmeldeiname: mue

Kennwort: ●●●●●●

Kennwort wiederholen: ●●●●●●

Benutzer muss das Kennwort bei der nächsten Anmeldung ändern
 Benutzer kann Kennwort nicht ändern
 Kennwort läuft nie ab
 Konto ist deaktiviert
 Konto ist gesperrt
 Zugang über VPN

Klassen: keine Auswahl getroffen.

OK Abbrechen

Abbildung V.1.18. Benutzer anlegen („Anmeldeinformation“)

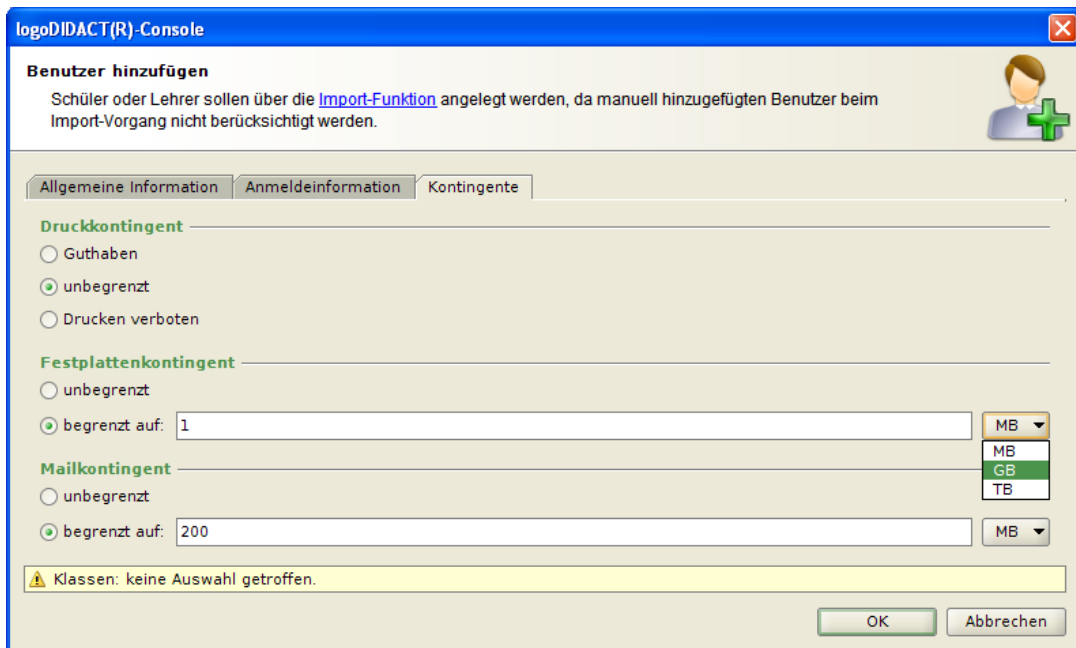


Abbildung V.1.19. Benutzer anlegen („Kontingente“)

Nachdem alle Benutzerangaben gemacht wurden, kann der Dialog über den Button „OK“ geschlossen werden. Der neue Benutzer wird jetzt im System erstellt.

Über das Suchfeld der Benutzerverwaltung kann anschließend geprüft werden, ob der neu angelegte Benutzer im System existiert und alle Angaben richtig sind.

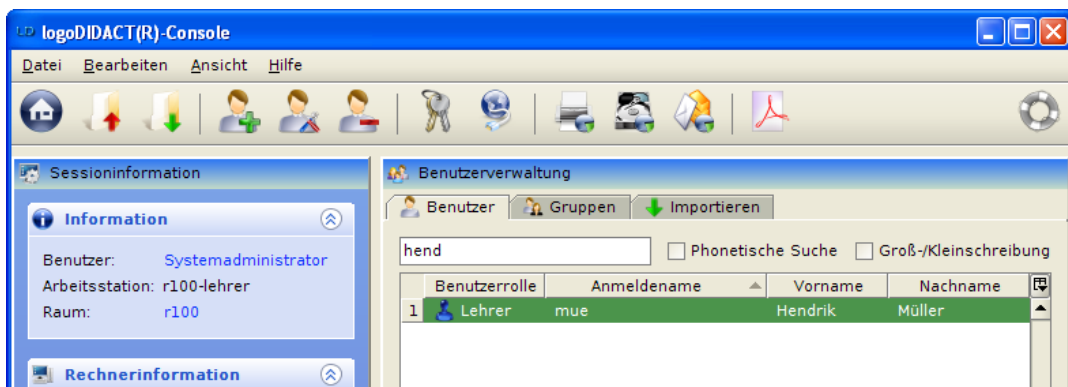


Abbildung V.1.20. Suchfeld der Benutzerverwaltung

Über das kleine Rechteck am oberen Ende des rechten Scrollbalkens der Tabelle lassen sich weitere Spalten mit benutzerbezogenen Informationen einblenden.

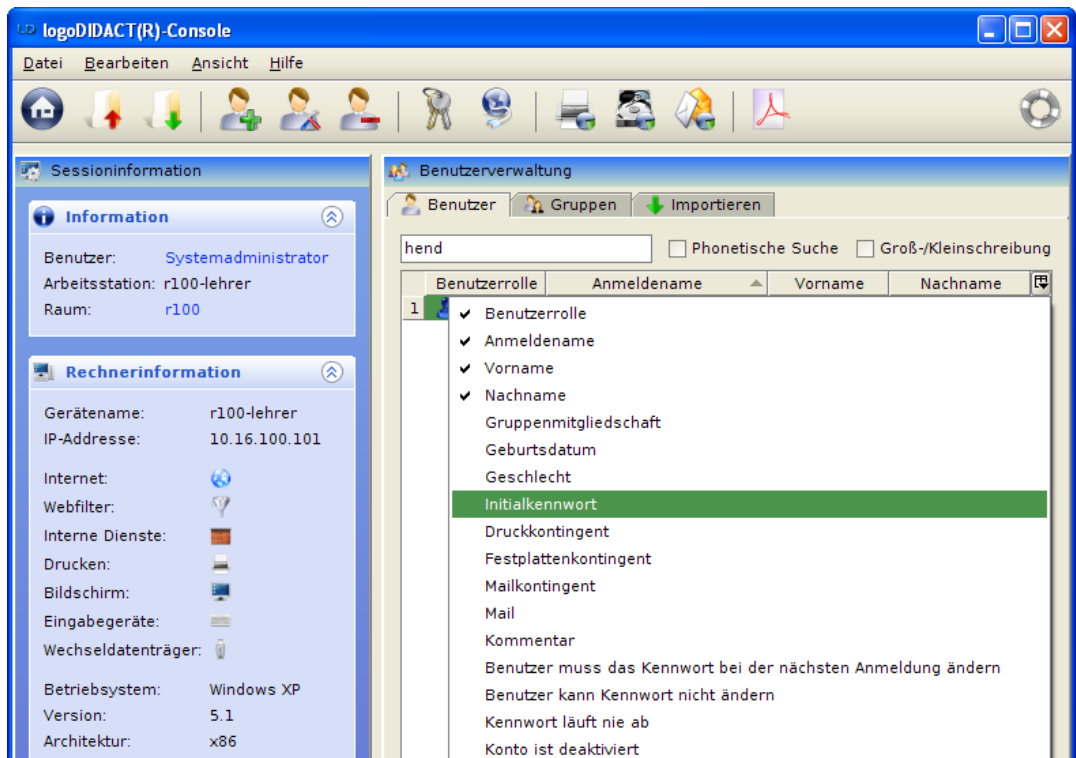


Abbildung V.1.21. Spaltenkonfiguration der Benutzerverwaltung

Sind nachträglich noch Änderungen oder Anpassungen an den Benutzerdaten vorzunehmen, können die zahlreichen Funktionen der Benutzerverwaltung herangezogen werden.

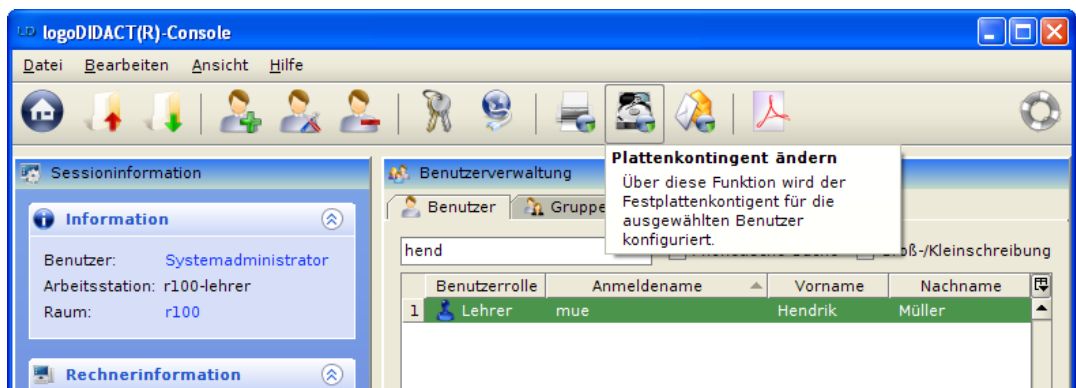


Abbildung V.1.22. Plattenkontingent ändern (über Symbolleiste)

Die verschiedenen Aktionen lassen sich auch auf mehrere Benutzer gleichzeitig ausführen, ohne die Benutzer einzeln zum Bearbeiten öffnen zu müssen.

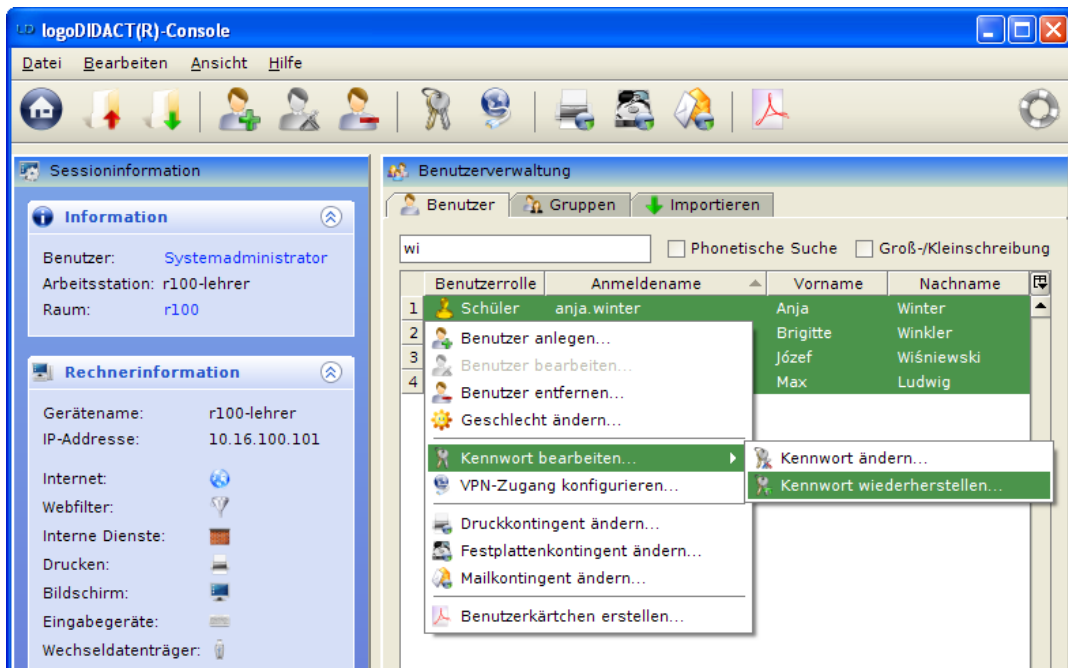


Abbildung V.1.23. Kennwort wiederherstellen (über Kontextmenü)

Das Erstellen neuer Benutzergruppen folgt dem gleichen Prinzip. Über die Registerkarte „Gruppen“ lassen sich die Benutzer zu Rollen und Projektgruppen zusammenfassen.

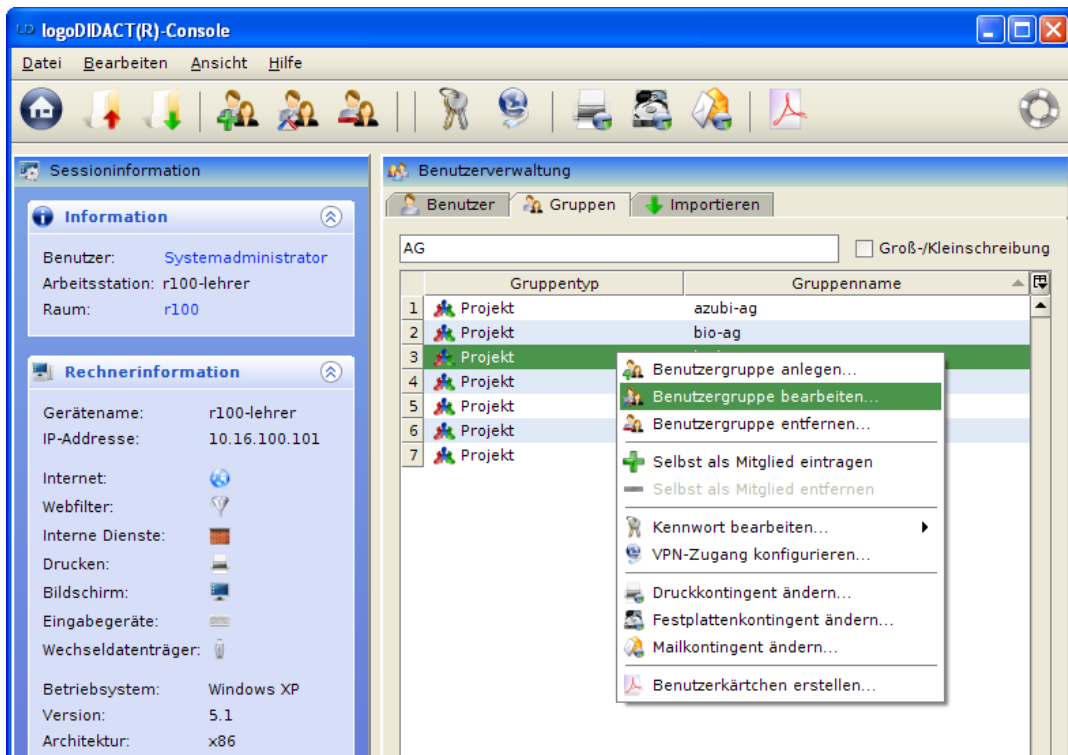


Abbildung V.1.24. Benutzergruppe bearbeiten (über Kontextmenü)

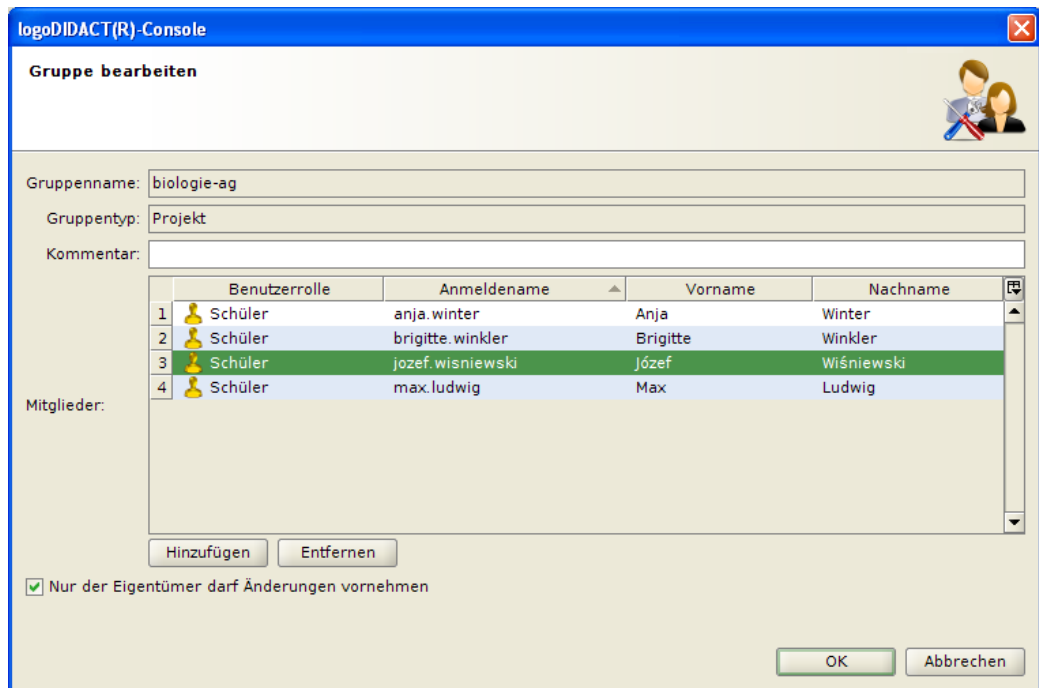


Abbildung V.1.25. Benutzergruppe bearbeiten („Mitglieder“)

V.1.1.4. Verwalten mehrerer Schularten

In der Praxis kann es durchaus vorkommen, dass mehrere Schularten wie Gymnasium, Realschule und Hauptschule gemeinsam über einen LogoDIDACT-Server betreut werden. In diesem Fall müssen die verschiedenen Benutzerlisten für Schüler und Lehrer, als auch die einzelnen Klassenzugehörigkeiten der Schüler/-innen durch ein entsprechendes Präfix oder Kürzel gekennzeichnet werden.

Mögliche Kennzeichnung der bekanntesten Schularten

- Gymnasium gym-, Realschule rs-, Hauptschule hs-
- Benutzerlisten gym-schueler bzw. gym-lehrer
- Klassenzugehörigkeiten gym-05a ... gym-13

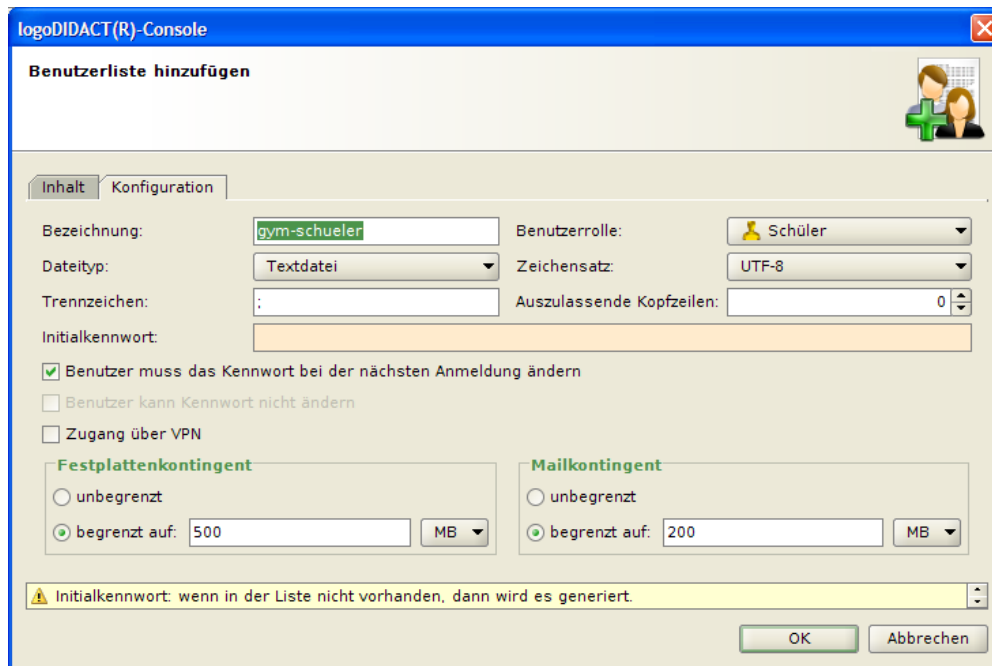


Abbildung V.1.26. Benutzerliste gym-schueler („Konfiguration“)

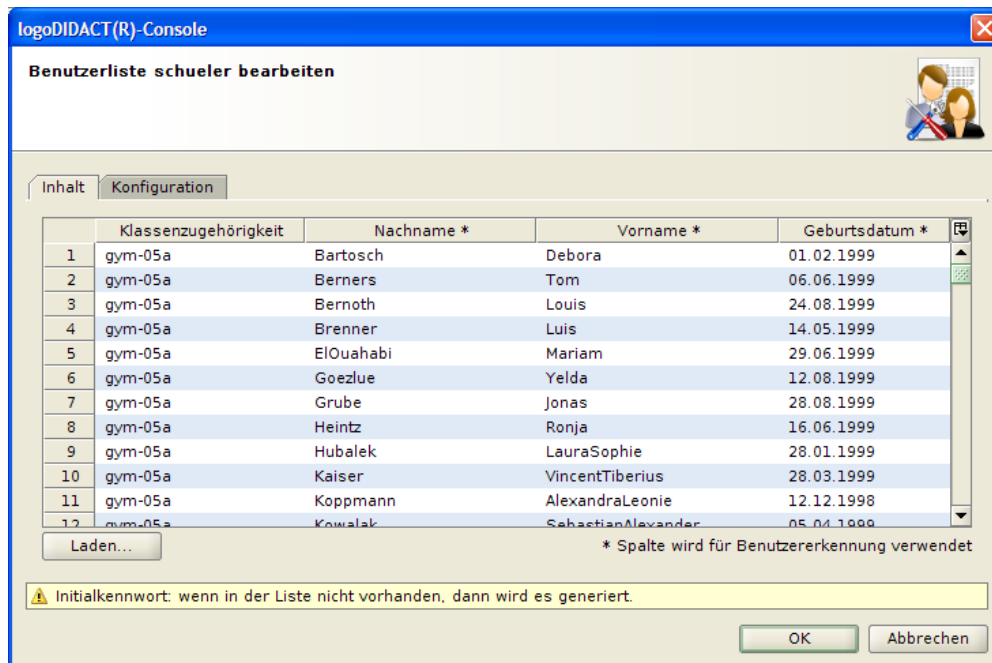


Abbildung V.1.27. Benutzerliste gym-schueler („Inhalt“)

V.1.1.5. VPN-Keys erzeugen und VPN-Zugang freischalten

Der VPN-Zugang kann direkt am Server über eine Shell für einzelne Benutzer oder auch eine Gruppe von Benutzern aktiviert werden. Wesentlich einfacher ist es jedoch als Administrator des Netzwerks über die grafische Oberfläche der LogoDIDACT-Console.

Starten Sie die Benutzerverwaltung und wählen Sie einen einzelnen speziellen Benutzer aus, um nur für diesen Benutzer den OpenVPN-Zugang freizuschalten.

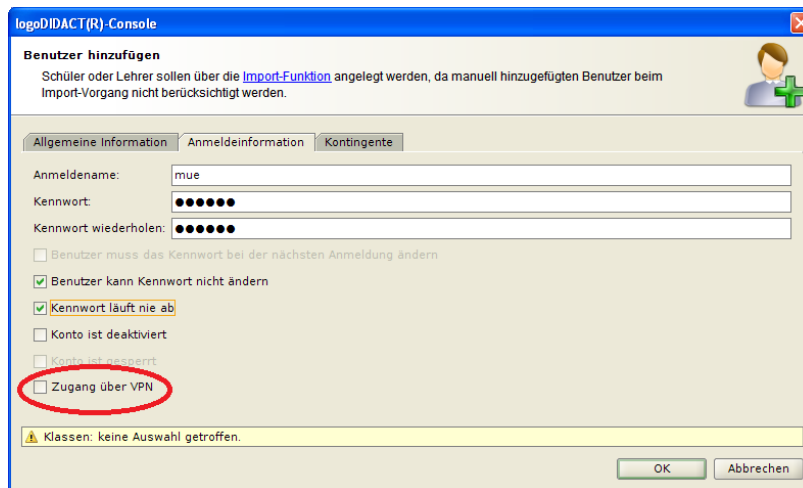


Abbildung V.1.28. OpenVPN Keys erzeugen und Zugang freischalten über die LogoDIDACT-Console

Um den Zugang für mehrere Personen (z.B. einige oder alle Lehrer) freizuschalten, starten Sie ebenfalls die Benutzerverwaltung. Wählen Sie dort aber die gewünschten Benutzer über ein Sortierkriterium (z.B. den Begriff "Lehrer" aus, so wie unten abgebildet. Über die Registerkarte Gruppen können Sie den Zugang z.B. für die gesamte Gruppe Lehrer am einfachsten freischalten. In der Praxis ist es jedoch oftmals so, dass Sie aufgrund der Bandbreitenproblematik nur denjenigen Kollegen einen Zugang per OpenVPN gewähren, die sich über die technischen Gegebenheiten im Klaren sind.

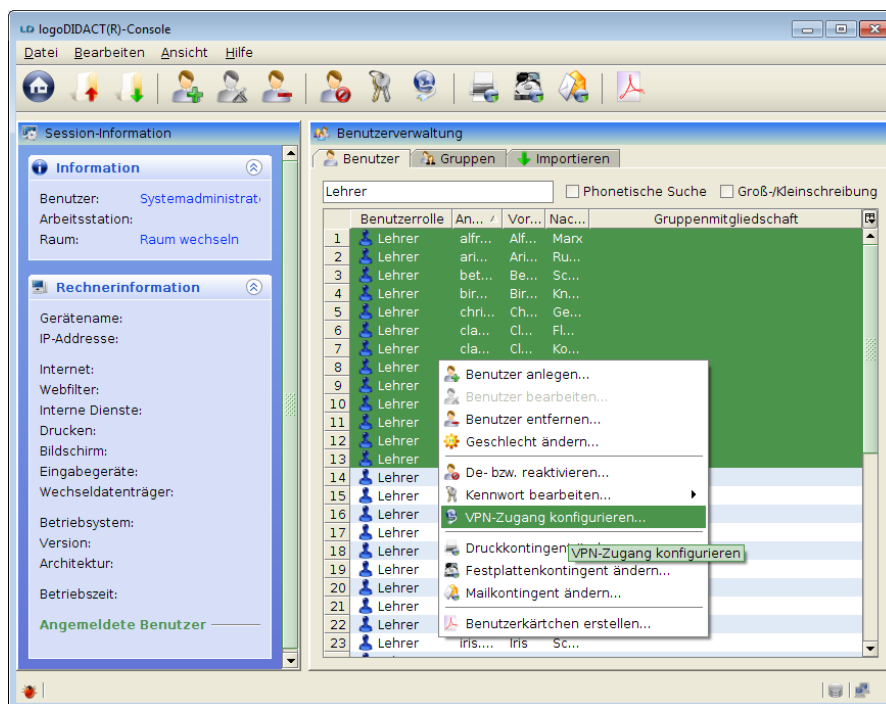


Abbildung V.1.29. OpenVPN Keys über die LogoDIDACT-Console für mehrere Benutzer erzeugen und Zugang freischalten

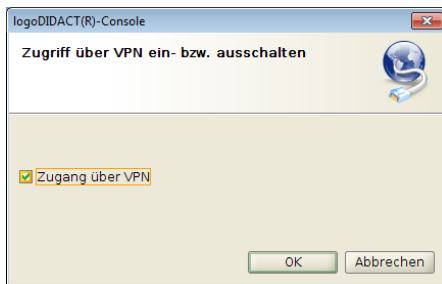


Abbildung V.1.30. OpenVPN Zugang aktivieren oder deaktivieren

V.1.2. Raumsteuerung

Die Raumsteuerung der LogoDIDACT-Console lässt sich über das „Häuschen“ in der Symbolleiste, das Menü „Ansicht“ und der Tastenkombination **Alt+R** aufrufen.

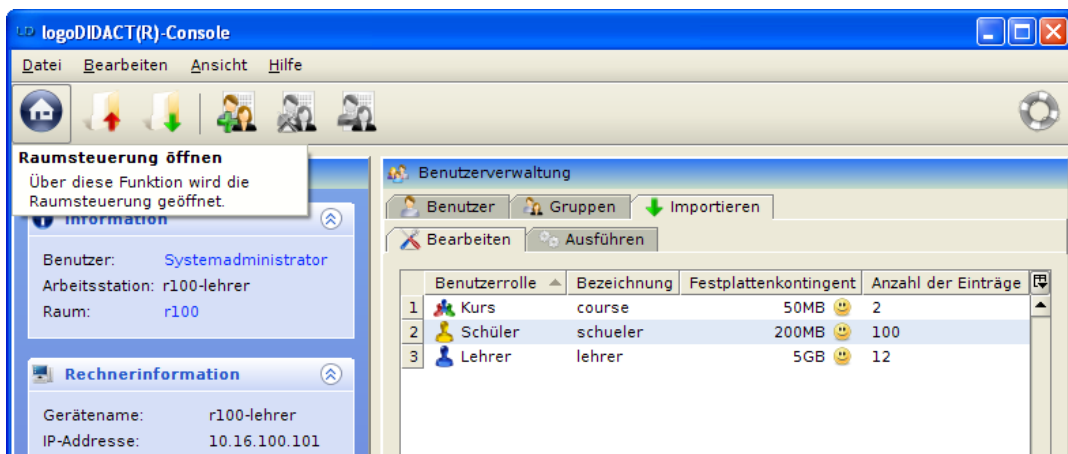


Abbildung V.1.31. Raumsteuerung öffnen (über Symbolleiste)

V.1.2.1. Rembo/mySHN® Funktionen

Über den Eintrag „Rembo/mySHN“ in der Symbolleiste und im Kontextmenü können verschiedene Rembo/mySHN® Aktionen wie „Rechner formatieren“, „Speichertest ausführen“ oder Ähnliches aufgerufen werden.

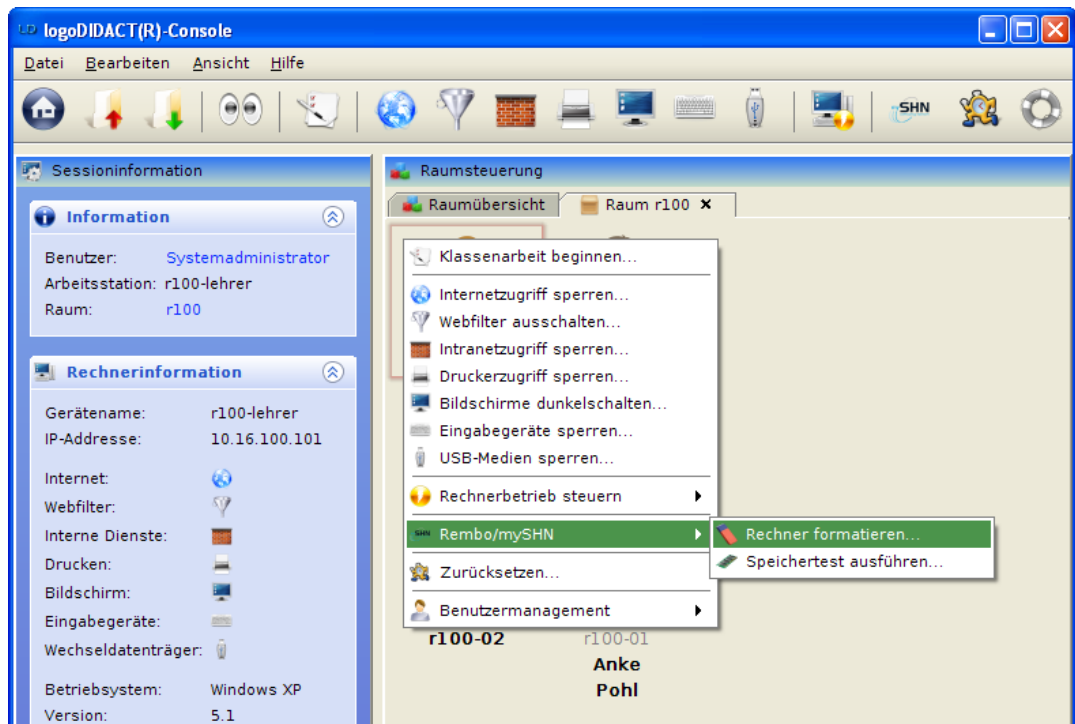


Abbildung V.1.32. Rembo/mySHN Funktionen (über Kontextmenü)

Die einzelnen Funktionen lassen sich jedoch auch weiterhin über die Rembo/mySHN® Oberfläche beim Startvorgang des Rechners auswählen.

V.1.3. Surfverhalten

V.1.3.1. Auswertung der Internetzugriffe

Über den Eintrag „Auswertung der Internetzugriffe“ im Menü „Ansicht“ wird dem Anwender eine personenbezogene Auswertung aller Seitenaufrufe bereitgestellt.



Achtung

Die Internetauswertung kann nur von Benutzern durchgeführt werden, die auch Mitglied in der Gruppe „Datenschutz“ oder „Schulleitung“ sind. Aus datenschutzrechtlichen Gründen, ist die Verwaltung von Benutzern für diese beiden Gruppen nicht über die LogoDIDACT-Console möglich. Dies ist nur direkt am Server als Benutzer root machbar und wird in Abschnitt III.4.11.2.1, „Lehrer zur Gruppe Datenschutz hinzufügen“ erläutert.

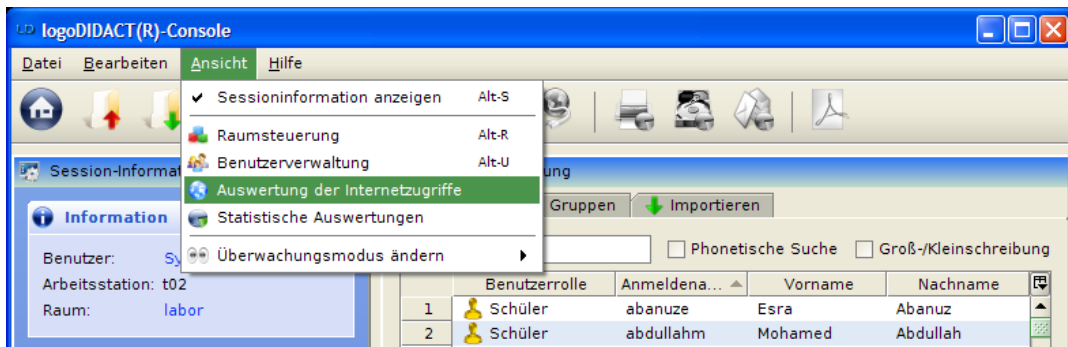


Abbildung V.1.33. Auswertung der Internetzugriffe (über Menü „Ansicht“)

Zugriffsmöglichkeiten

Zugriff nur auf Schüler Logs (NUR für „Datenschutz“ mit erneuter Kennworteingabe zugänglich)

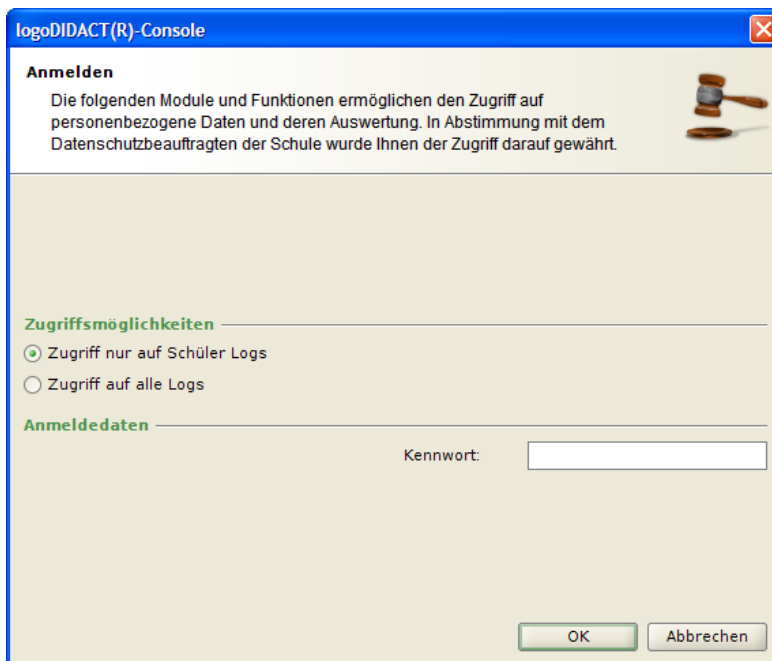


Abbildung V.1.34. Zugriff nur auf Schüler Logs

Zugriff auf alle Logs (erfordert 2. Person aus „Datenschutz“ bzw. „Schulleitung“, „Vier-Augen-Prinzip“)

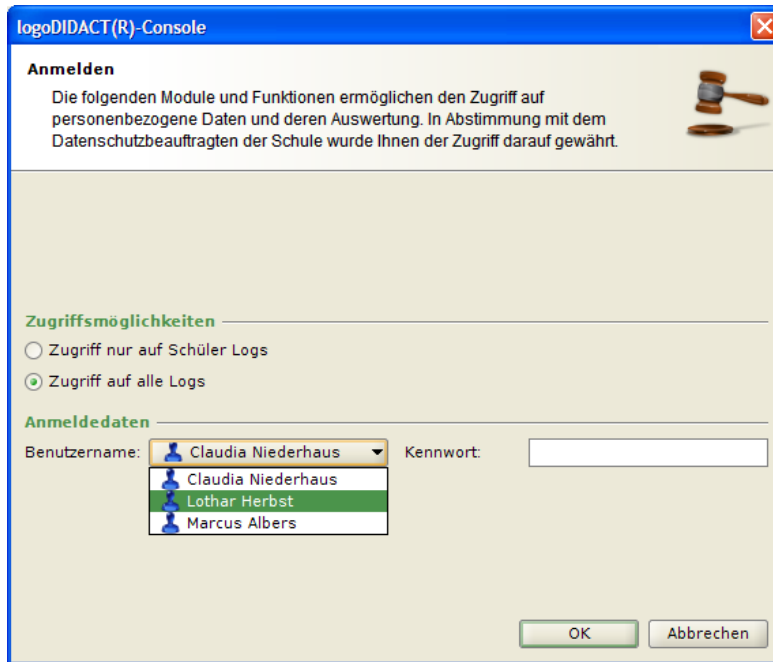


Abbildung V.1.35. Zugriff auf alle Logs

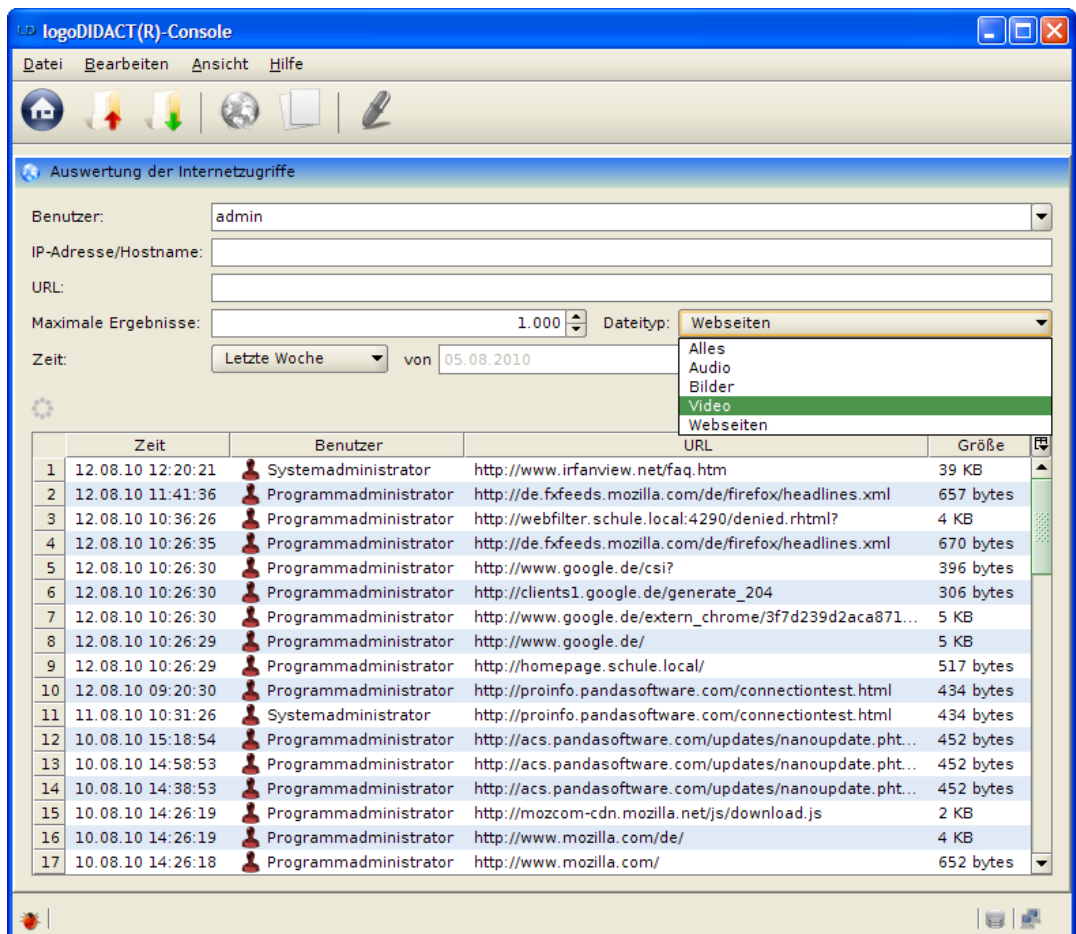


Abbildung V.1.36. Auswertung der Internetzugriffe

V.1.3.2. Statistische Auswertungen

Über den Eintrag „Statistische Auswertungen“ im Menü „Ansicht“ lassen sich alle Seitenaufrufe der Benutzer nach bestimmten Kriterien aufzeigen.



Achtung

Die Funktionalität ist jedoch allein dem Systembenutzer „admin“ vorbehalten.

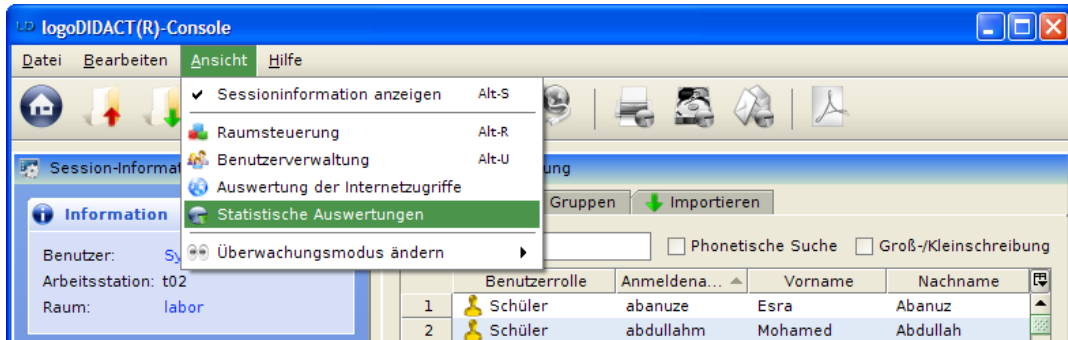


Abbildung V.1.37. Statistische Auswertungen (über Menü „Ansicht“)

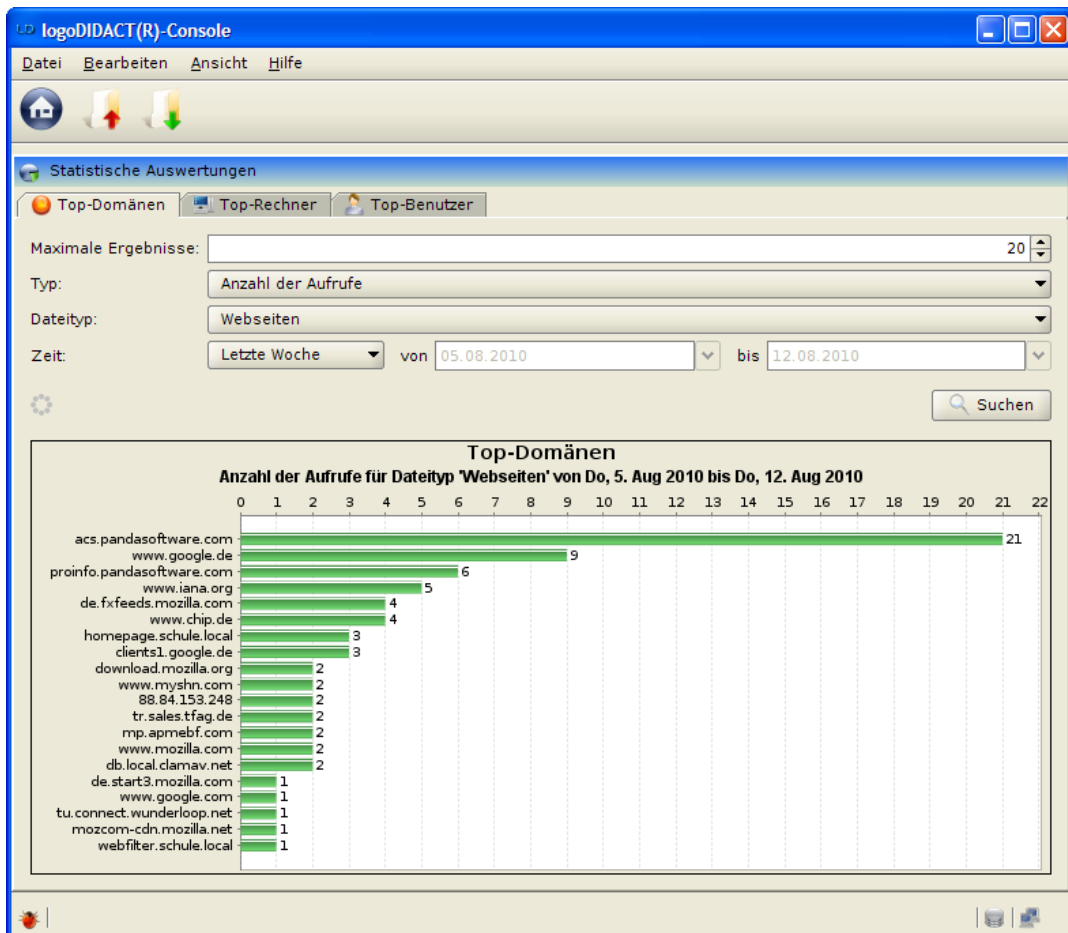


Abbildung V.1.38. Statistische Auswertungen

V.1.4. Service- und Support Modul

Das Thema Service- und Support aus Lehrersicht wird in Abschnitt VI.2.5, „Service- und Support für Lehrer“ ausführlich beschrieben. Dort wird auch der Assistent zur Neuaufnahme von Störungen detailliert erklärt und auch das Hauptmenü des Moduls, in dem die offenen und auch geschlossenen Störungen eines Gerätes hinterlegt sind.

Um das Service- und Supportmodul richtig zu nutzen, muss aus administrativer Sicht mindestens ein Lehrer der Gruppe "Support" zugeordnet werden. Damit ist eine interne Abarbeitung von Störungen möglich. Der zweite Schritt ist, dass sich die Mitglieder der Gruppe Support mit dem Ablauf der Störungsbearbeitung auseinandersetzen und den Umgang dann den Kollegen und Kolleginnen erklären.

V.1.4.1. Lehrer der Gruppe Support zuordnen

Das Service- und Support-Modul wird über ein IdUpdate automatisch installiert und vorkonfiguriert. Die Gruppe "Support" wird angelegt und der Benutzer admin wird der Gruppe zugeordnet. Der Gruppe sollten zunächst mindestens ein bis zwei Lehrer zugeordnet werden, die sich um die EDV der Schule kümmern. Je nach Größe der Schule können das natürlich auch mehr Kollegen und Kolleginnen sein.

Gehen Sie dazu über **Module** → **Benutzerverwaltung** → **Gruppen** und geben Sie im Suchfeld "Support" ein. Durch Doppelklick auf den Eintrag öffnet sich der Dialog "Gruppe bearbeiten" über den sich dann Lehrer hinzufügen lassen.

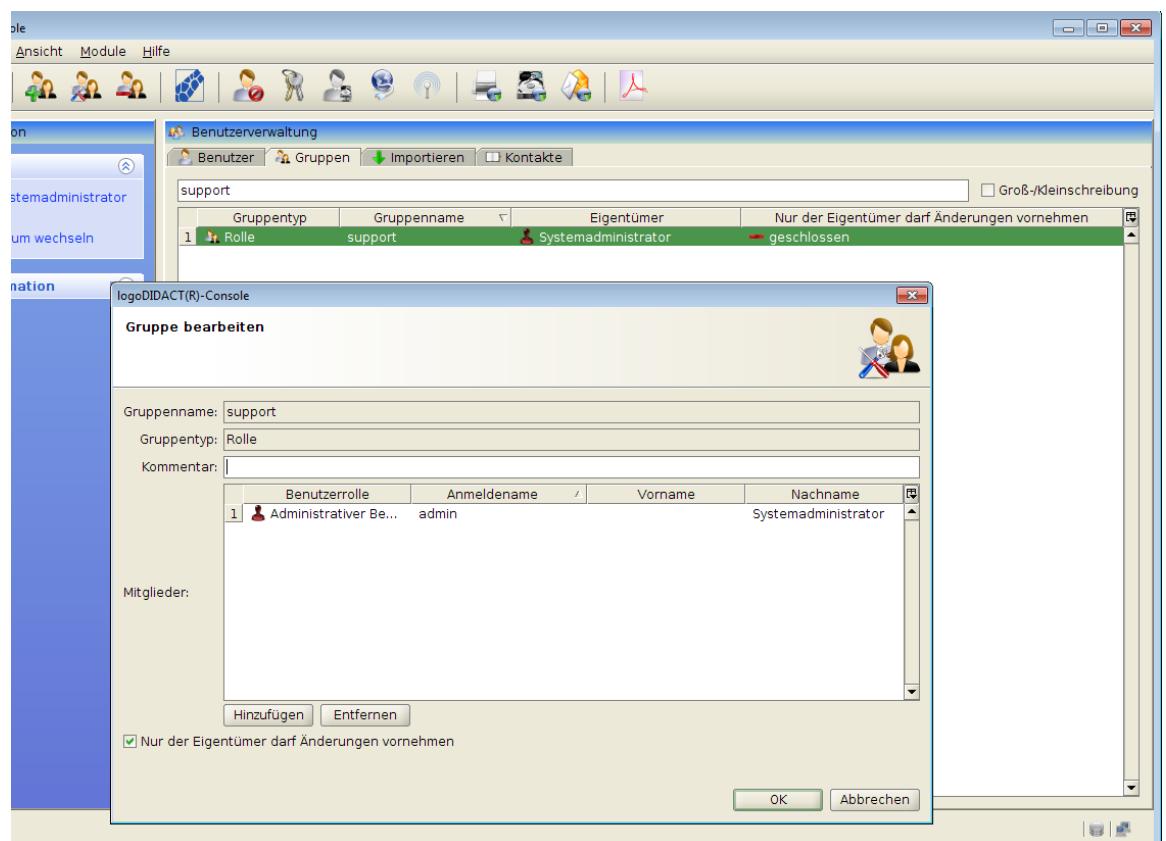


Abbildung V.1.39. Lehrer der Gruppe Support zuordnen

Die Gruppe Support ist eine so genannte geschlossene Gruppe, d.h. es können dort keine Lehrer dieser Gruppe beitreten, sondern nur der Administrator selbst kann dort Mitglieder hinzufügen.



Tipp

Wenn ein "normaler" Lehrer ein Problem weiterleitet, dann erscheinen dort bei der Auswahl nur Mitglieder der Gruppe Support.

V.1.4.2. Kontakte für externen Support anlegen

Lehrer die nicht Mitglied der Gruppe Support sind, können Störungen nur intern weiterleiten. Damit ist eine vernünftige Strukturierung vorgegeben, die in der EDV üblicherweise mit so genannten Support-Levels bezeichnet wird. Mitglieder der Gruppe Support hingegen können eine Störung z.B. per EMail auch nach außen an einen externen Kontakt weiterleiten.

Legen Sie dazu über **Module** → **Benutzerverwaltung** → **Kontakte** externe Personen und Ansprechpartner von Firmen und/oder dem Schulträger an.

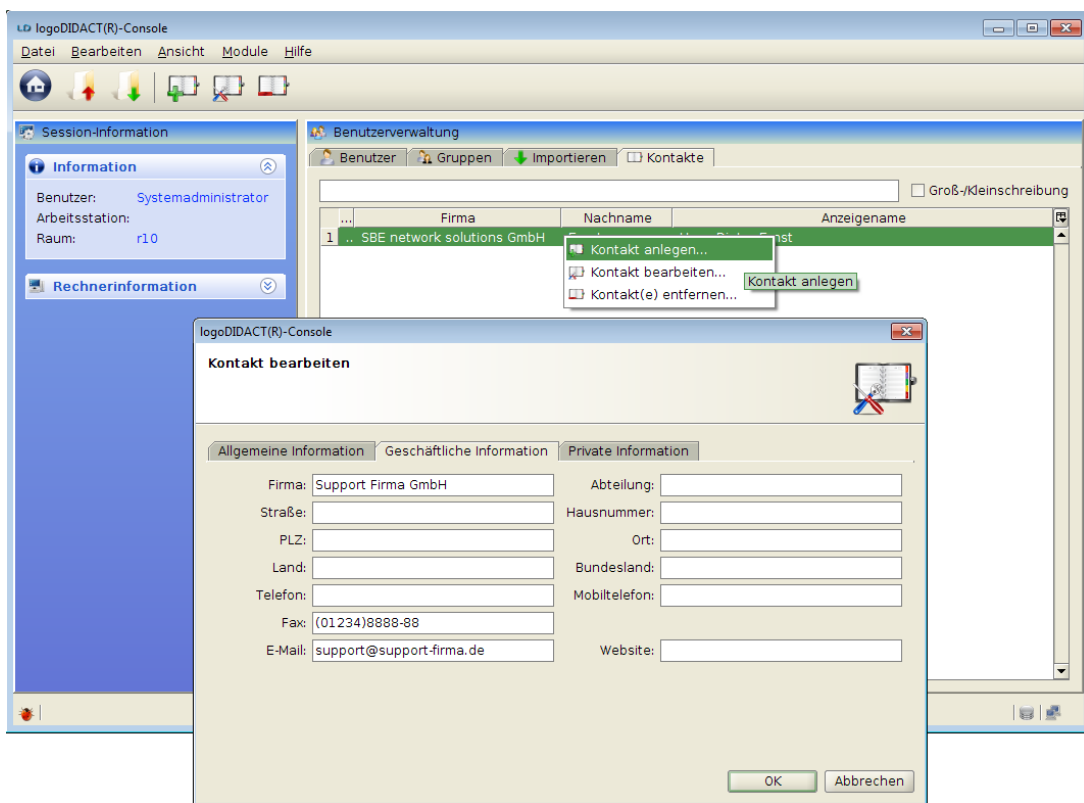


Abbildung V.1.40. Einen neuen externen Kontakt anlegen



Achtung

Als Mitglied der Gruppe Support kann man eine Störung sowohl an andere Mitglieder dieser Gruppe weiterleiten als auch an die externen Kontakte und Ansprechpartner.

In der Registerkarte "Allgemeine Informationen" können Sie neben den personenbezogenen Daten auch ein Bild hinterlegen. Dieses darf bis zu 150 Pixel hoch sein um komplett in die Anzeige zu passen.

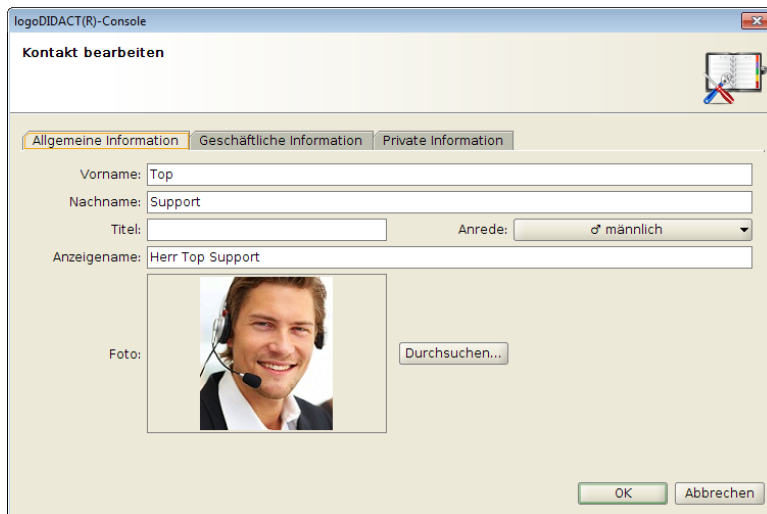


Abbildung V.1.41. Personenbezogene Daten mit Bild hinterlegen

V.1.4.3. Das Hauptfenster im Modul Service und Support

Das Haupt- bzw. Übersichtsfenster über alle bestehenden oder vergangenen Störungen erreicht man über **Module** → **Service und Support für Geräte**. Damit hat man als Administrator eine zentrale Übersicht über sämtliche Probleme und Störungen im gesamten Netzwerk. Wie in LogoDIDACT gewohnt, lassen sich über die Suchmaske einzelne Geräte, Räume oder auch andere Angaben filtern und die Liste an Störungen über jede Spalte beliebig sortieren.

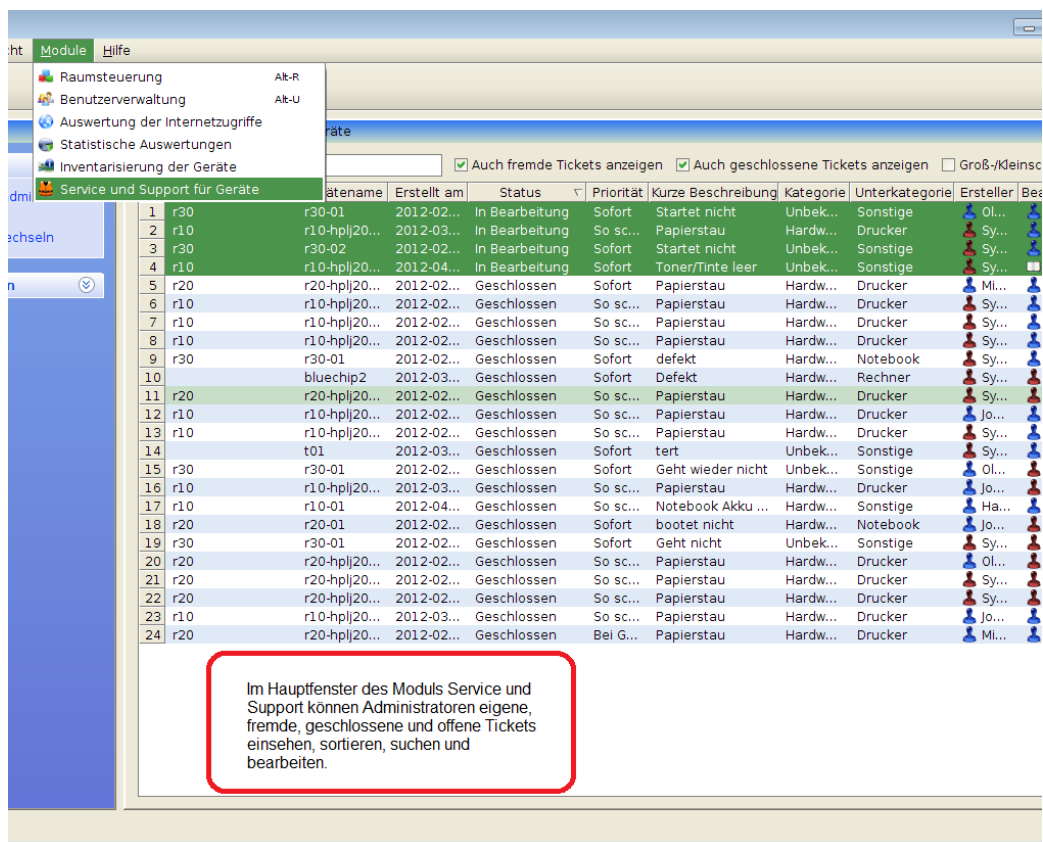


Abbildung V.1.42. Das Hauptfenster mit der Übersicht über alle Störungen

Einzelne Störungen lassen sich durch Doppelklick auf die entsprechende Zeile öffnen und bearbeiten.

V.1.4.4. Störungen bearbeiten, weiterleiten und abschließen

Für jedes Gerät werden in LogoDIDACT sämtliche aufgetretenen Störungen und die damit zusammenhängenden Vorgänge und Aktionen protokolliert. Das Fenster zum Bearbeiten von Störungen eines speziellen Gerätes lässt sich auf zwei Wegen erreichen. Entweder zentral über **Module** → **Service und Support für Geräte** und Doppelklick auf einen Eintrag für das Gerät oder über die symbolische Ansicht in der Raumdarstellung.

Letzteres ist vor allem der sehr viel schnellere Weg, wenn man sich bereits in der symbolischen Raumansicht befindet und eine Störung durch das entsprechende Baustellen-Symbol deutlich erkennt.

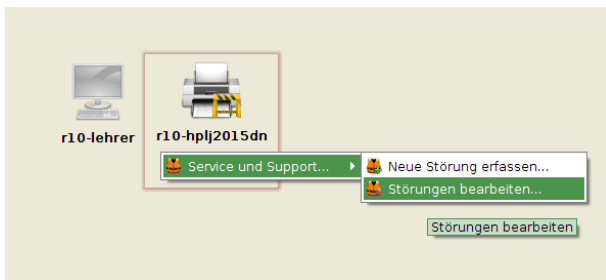


Abbildung V.1.43. Öffnen des Dialogs zum Bearbeiten von Störungen über die symbolische Ansicht

Beide Wege führen jedoch zum gleichen Ziel - dem gerätebezogenen Dialog zur Bearbeitung von Störungen.

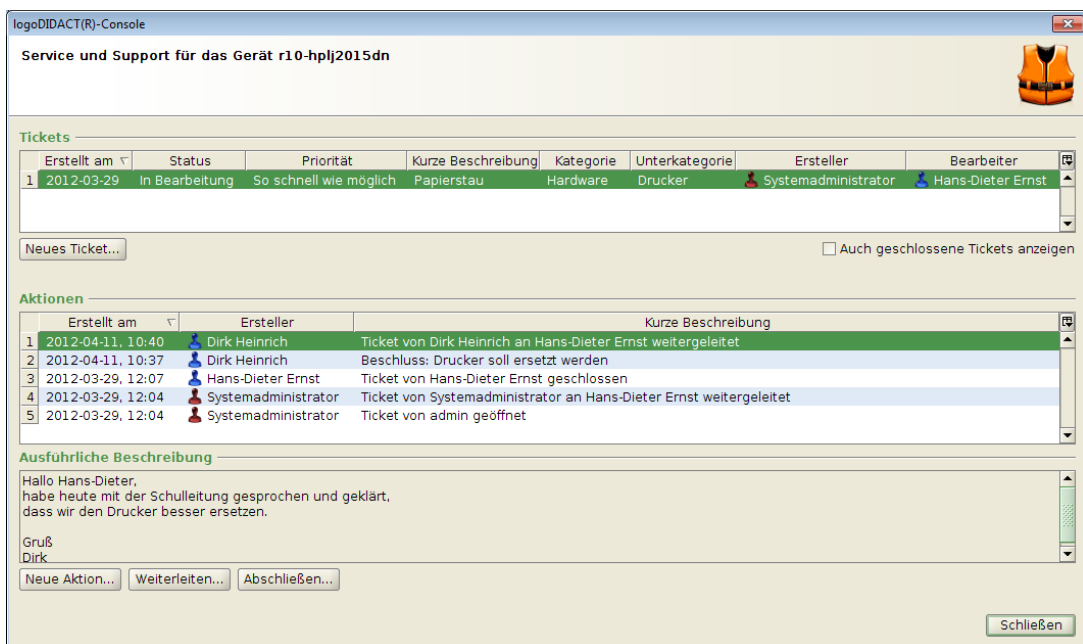


Abbildung V.1.44. Störungen bearbeiten, weiterleiten und abschließen



Achtung

Obwohl das Bearbeiten von Störungen primär durch Mitglieder der Gruppe Support geleistet werden wird, ist es sinnvoll dies grundsätzlich auch den anderen Kolleginnen und Kollegen zu erlauben.

Deshalb ist der Umgang in Abschnitt VI.2.5.7, „Störungen bearbeiten“ dokumentiert.

Kapitel V.2. Anleitung ITB Funktionen

Über die IT Betreuer (kurz: ITB) Funktionen haben Netzwerkbetreuer die Möglichkeit verschiedene administrative Tätigkeiten am Server durchzuführen.



Abbildung V.2.1. Benutzeroberfläche der ITB Funktionen

Über den Eintrag „ITB Panel“ in der Lesezeichen-Symbolleiste des Mozilla Firefox und der Internet-Adresse `http://itb` können die ITB Funktionen im Webbrowser aufgerufen werden.



Abbildung V.2.2. Lesezeichen-Symbolleiste des Mozilla Firefox



Achtung

Die ITB Funktionen sind vor Zugriff Dritter geschützt und verlangen Benutzernamen und Passwörter. Mit den vordefinierten Systembenutzern „admin“ und „itb“ können sich Netzwerkbetreuer als Benutzer authentifizieren und für weitere Zugriffe autorisieren.

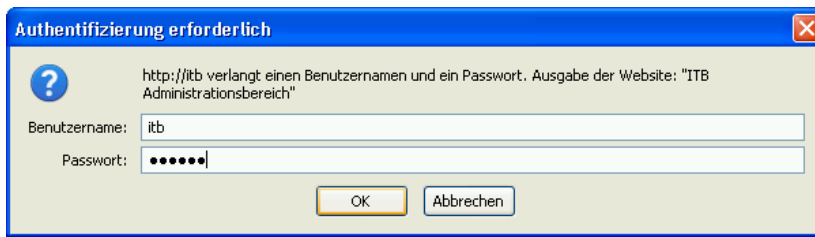


Abbildung V.2.3. Anmeldedialog der ITB Funktionen

V.2.1. Server

V.2.1.1. Dienste

Über den Eintrag „Dienste neustarten“ lassen sich verschiedene Dienste wie „Samba“, „CUPS“, „Rembo“ und Ähnliches am Server zur Fehlerbehebung neustarten.

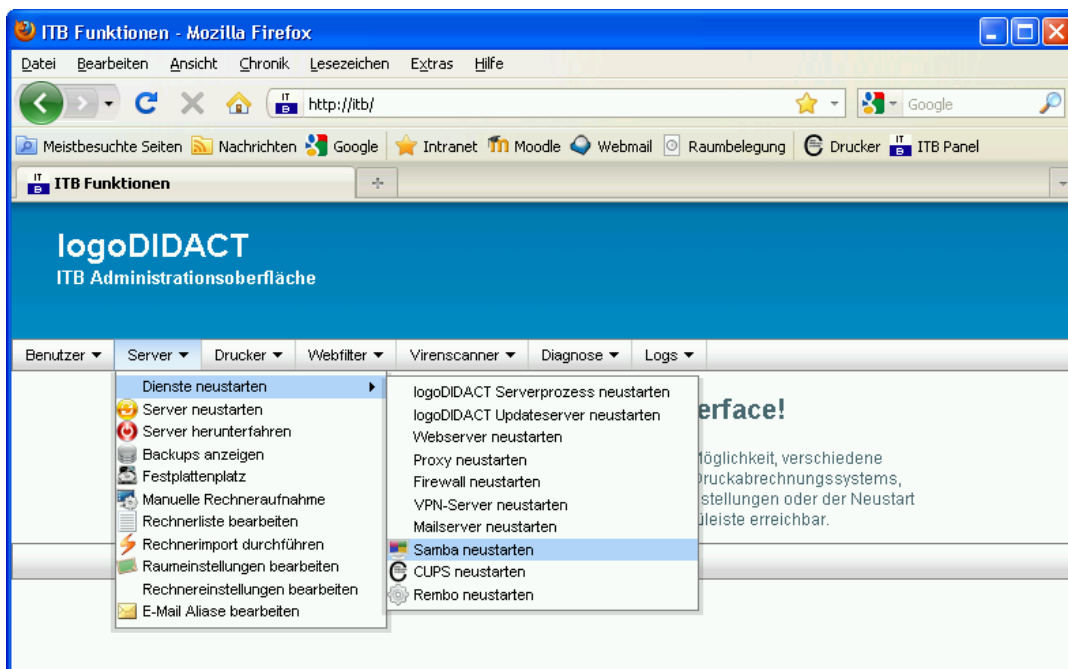


Abbildung V.2.4. Samba neustarten (über ITB Funktionen)

V.2.1.2. Geräteaufnahme

Über den Eintrag „Manuelle Geräteaufnahme“ können bisher unbekannte Rechner einzeln in das System aufgenommen werden.



Abbildung V.2.5. Manuelle Geräteaufnahme (über ITB Funktionen)



Achtung

Im oberen Bereich der Beschreibung findet sich ein Hinweis, dass lediglich Rechner aufgenommen werden können, deren Rechnername, IP- und MAC-Adresse im System noch nicht verwendet werden.

Benutzer ▾ Server ▾ Drucker ▾ Webfilter ▾ Virens Scanner ▾ Diagnose ▾ Logs ▾

Manuelle Rechneraufnahme

Um einen bisher unbekanntem Rechner in das System aufzunehmen, geben Sie bitte dessen Daten in der folgenden Maske ein.

Bitte beachten Sie, dass nur Rechner aufgenommen werden können, deren Rechnername, IP Adresse und MAC Adresse im System bisher noch nicht verwendet werden. Um die Daten von bestehenden Rechnern zu ändern oder diese aus dem System zu entfernen, nehmen Sie bitte die entsprechenden Änderungen direkt in der Rechnerliste vor.

Rechnername:	<input type="text" value="r100-lehrer"/>
Raum:	<input type="text" value="r100"/>
IP-Adresse:	<input type="text" value="10.16.100.101"/>
MAC-Adresse:	<input type="text" value="00:25:b3:17:ef:fc"/>
Typ:	<input type="text" value="Desktop Computer"/>
Imagegruppe:	<input type="text" value="schulnetz"/>

© 2008 SBE network solutions GmbH

Abbildung V.2.6. Manuelle Rechneraufnahme („Konfiguration“)



Tipp

Über die Geräteliste („wimport_data“) lassen sich die Rechnerdaten jederzeit ändern oder aus dem System entfernen.

V.2.1.3. Geräteliste

Über den Eintrag „Geräteliste bearbeiten“ kann die „wimport_data“ am Server bearbeitet und ein Geräteimport durchgeführt werden.



Abbildung V.2.7. Geräteliste bearbeiten (über ITB Funktionen)

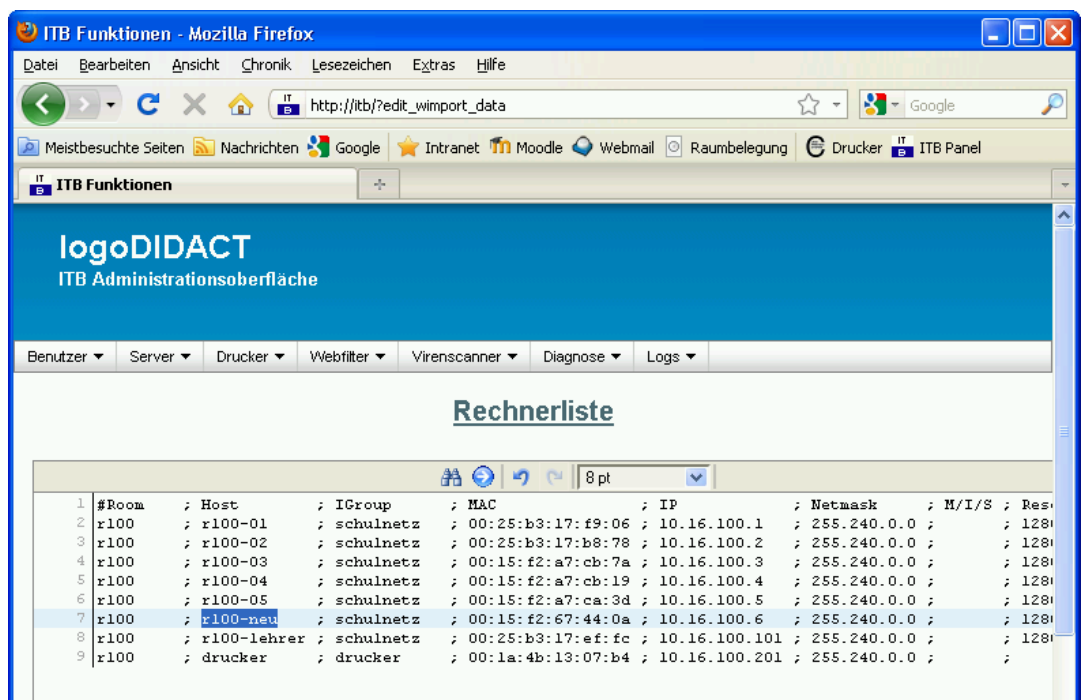


Abbildung V.2.8. Geräteliste bearbeiten („Konfiguration“)

V.2.1.3.1. Zusätzliche MAC/IP Adressen

Die Spalte M/I/S der Geträdeliste ist für zusätzliche MAC/IP Adressen (optional Subnet) vorgesehen, z.B. für die WLAN Karten bei Notebooks.

Beispiel für M/I/S:

00:3f:1c:59:1b:24/10.16.100.101

Beispiel für nb-01:

```
r100;nb-01;win7;00:0d:9d:44:f8:8e;10.16.100.1;255.240.0.0; \
00:3f:1c:59:1b:24/10.16.100.101;1600x1080x32,60Hz;;1;notebook;unicast
```

V.2.1.3.2. Bildschirmauflösung

Wenn ein Image auf identischer Rechner-Hardware mit einer identischen Grafikkarte betrieben wird, dann sind die Einstellungen für die Bildschirmauflösung im Treiber für die Grafikkarte festgelegt. Betreibt man diese identischen Rechner aber an verschiedenen Monitoren, dann benötigt man eine Anpassung an den jeweiligen Monitor. Über den Eintrag Auflösung in der Geräteliste ist es z.B. also möglich, manche PCs mit einem 17" Monitor mit einer Auflösung von 1024x768 zu betreiben und andere PCs mit einem 19" Monitor mit einer Auflösung von 1280x1024 ohne dass man dafür das Image trennen müsste. Die Syntax für das Feld lautet Pixelbreite x Pixelhöhe x Farbtiefe x Bildwiederholfrequenz Bsp.: 1024x768x32x60 Bitte beachten Sie, dass keine Leerzeichen verwendet werden dürfen und die verschiedenen Parameter durch ein "x" getrennt werden.



Tipp

Damit die Bildschirmauflösung auch in Windows 7 richtig gesetzt wird, muss der Parameter *AgentSetResolution* in der Datei `global.conf` am LogoDIDACT-Server gesetzt werden.

Durch diese Option übernimmt dann der Dienst myAgent in Windows aktiv das Setzen der richtigen Bildschirmauflösung.

19 Zoll, Auflösung: 1280x1024

22 Zoll Wide, Auflösung: 1680x1050



```
#Room ; Host ; IGroup ; MAC ; IP ; Netmask ; M/I/S ; Resolution
r210 ; r210-01 ; win7 ; d0:27:88:0b:37:37 ; 10.16.210.1 ; 255.240.0.0 ; ; 1280x1024x32,60Hz
r210 ; r210-02 ; win7 ; d0:27:88:0b:37:c0 ; 10.16.210.2 ; 255.240.0.0 ; ; 1280x1024x32,60Hz
r210 ; r210-lehrer ; win7 ; d0:27:88:0b:36:fd ; 10.16.210.101 ; 255.240.0.0 ; ; 1680x1050x32,60Hz
```

Anpassung über Geräteliste (ITB-Interface)
und logoDIDACT Agent über Parameter *AgentSetResolution* (in `global.conf`)

Abbildung V.2.9. Anpassung der Bildschirmauflösung über myAgent und Eintrag im ITB-Interface

Die Anpassung in der Datei `global.conf` kann auch über Bedingungen ausgeführt werden, so dass z.B. nur Clients mit Windows 7 diese spezielle Anpassung über den Dienst myAgent erhalten. Im folgenden Beispiel ist dies so realisiert.

Weiterhin kann myAgent über den Parameter `AgentDisplayMode` auch dafür sorgen, dass unter Windows die Grafikeinstellungen für die Anzeige auf einem zweiten Bildschirm oder Beamer manipuliert werden.

```
@if SYSTEM == "win7"
  AgentSetResolution
  @if HOST: *beamer*
    AgentDisplayMode clone
  @endif
@endif
```

Über `AgentDisplayMode clone` wird der Bildschirm dupliziert, bzw. geclont. Das geschieht dadurch, dass der Dienst myAgent das Microsoft-Programm `C:\Windows\System32\DisplaySwitch.exe` aufruft und den Parameter übergibt, den auch das Tool selbst verwendet.

Für den Betrieb mit Beamern ist in der Regel der clone-Modus empfehlenswert, was im obigen Beispiel für alle Rechner aktiviert wird, die das Wort "beamer" im Rechnernamen haben. Heisst der Lehrer-PC also z.B. "r210-lehrer-beamer" wird an diesem Rechner durch den Dienst myAgent automatisch der Bildschirm auf den zweiten Bildschirm bzw. den Beamer geclont. Über den Parameter `extend` würde der Desktop auf einen zweiten Bildschirm erweitert werden.

V.2.1.4. Raumeinstellungen

Über den Eintrag „Raumeinstellungen bearbeiten“ lassen sich Raumstandards für die bestehenden Räume aus der Geräteliste festlegen.

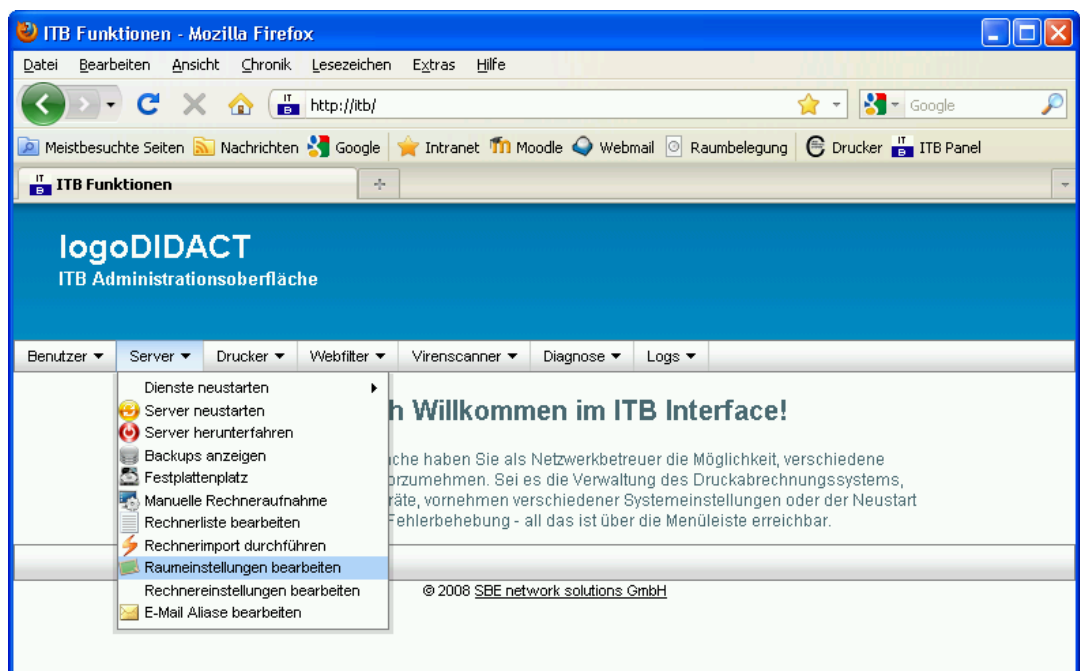


Abbildung V.2.10. Raumeinstellungen bearbeiten (über ITB Funktionen)



Tipp

Die Funktionen der Raumsteuerung können entweder über das Symbol + für den Raum freigegeben bzw. über ein Minuszeichen gesperrt werden.

Um den Webfilter per Standard in einem Raum wie z.B. dem Lehrerzimmer auszuschalten, trägt man dort in der Spalte Webfilter das Symbol - für den Raum ein.

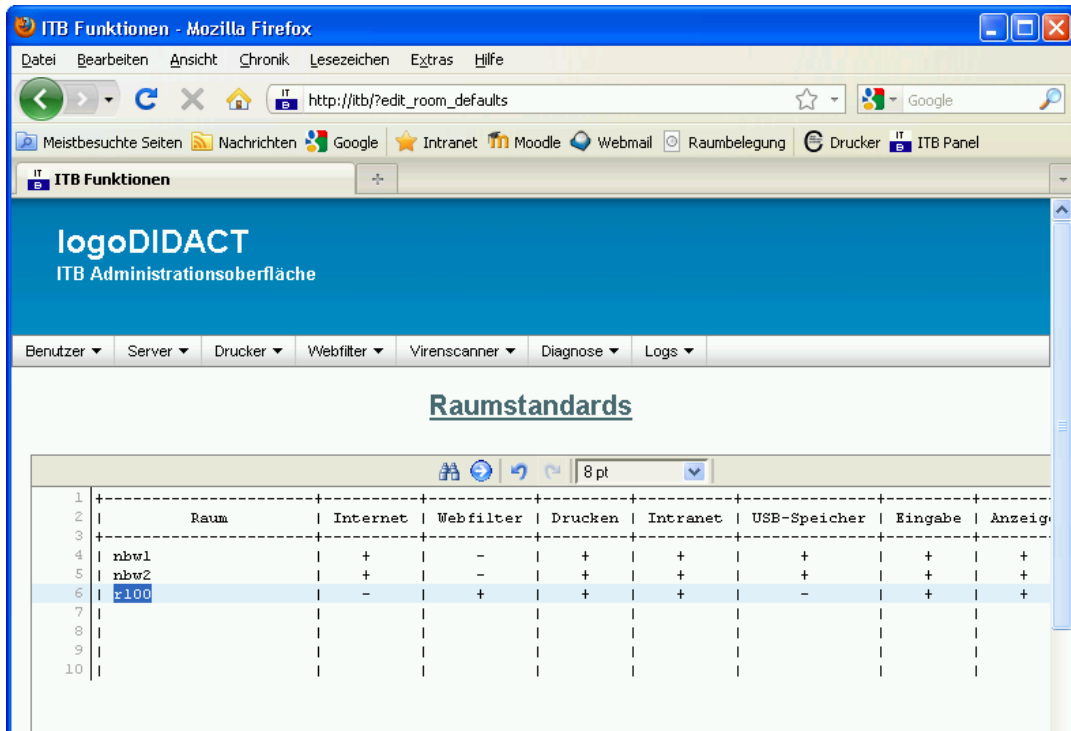


Abbildung V.2.11. Raumeinstellungen bearbeiten („Konfiguration“)

V.2.1.5. Rechnereinstellungen

Über den Punkt „Rechnereinstellungen bearbeiten“ können analog zu den Raumeinstellungen auch Rechnerstandards definiert werden.

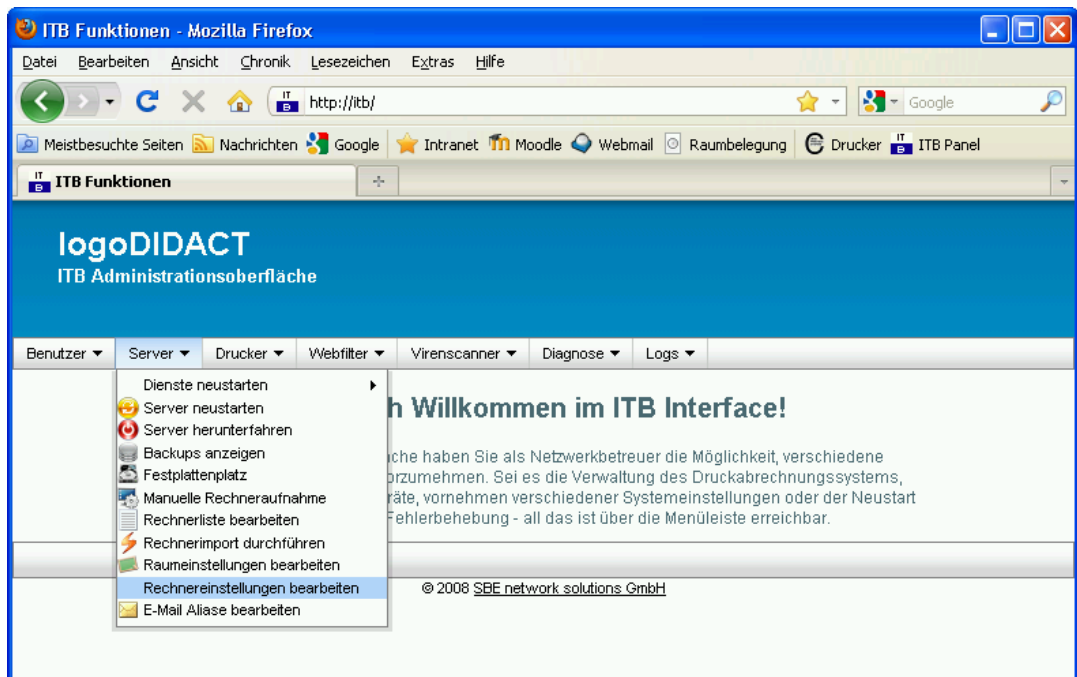


Abbildung V.2.12. Rechnereinstellungen bearbeiten (über ITB Funktionen)

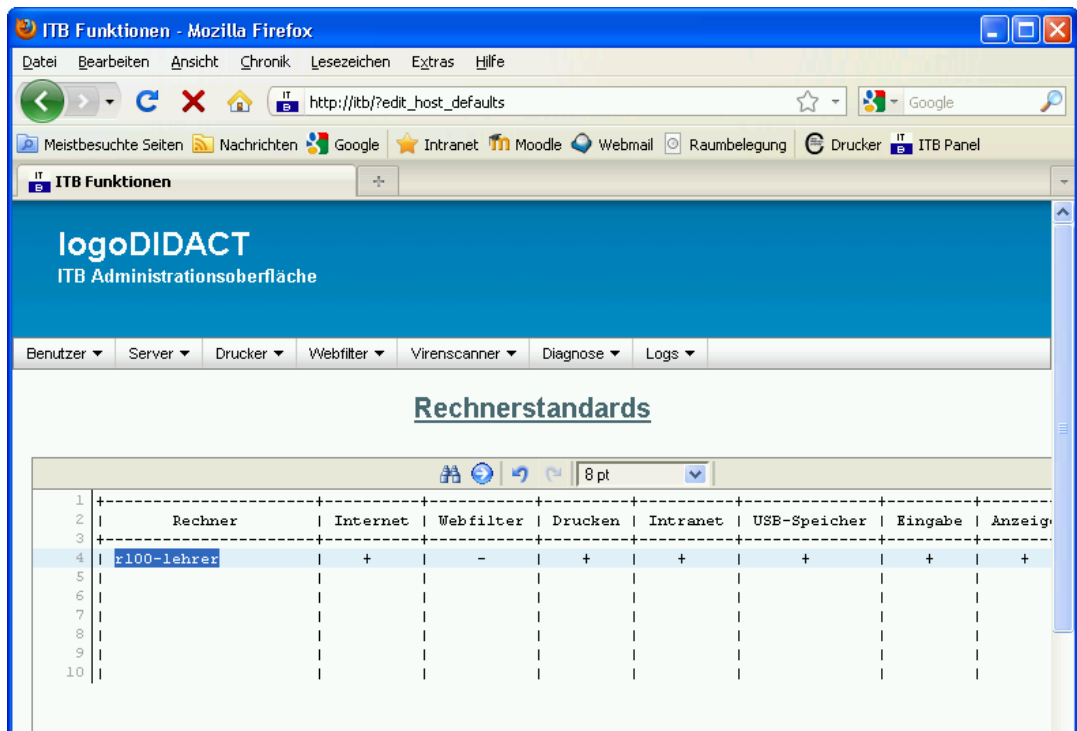


Abbildung V.2.13. Rechnereinstellungen bearbeiten („Konfiguration“)

V.2.1.6. Rechner zeitgesteuert herunterfahren

Über das ITB-Interface lassen sich die Computersysteme im Netzwerk zeitgesteuert herunterfahren. Es ist dabei möglich, mehrere Ausschaltzeiten zu definieren. Damit können Rechner, die nach dem ersten Herunterfahren nochmals eingeschaltet und benutzt wurden, auch ein zweites oder drittes Signal

erhalten. Dabei werden auch so genannte Wildcards unterstützt, so dass es sehr sinnvoll ist, mit einem Eintrag wie z.B.

| * | 20:00 | + | 30 | |

allen Rechnern um 20:00 Uhr das Signal zum Herunterfahren zu geben. Die Zeiten sollten entsprechend so an die Umgebung angepasst werden, dass die Geräte möglichst früh abgeschaltet werden und somit nicht unnötige Energie verbrauchen.

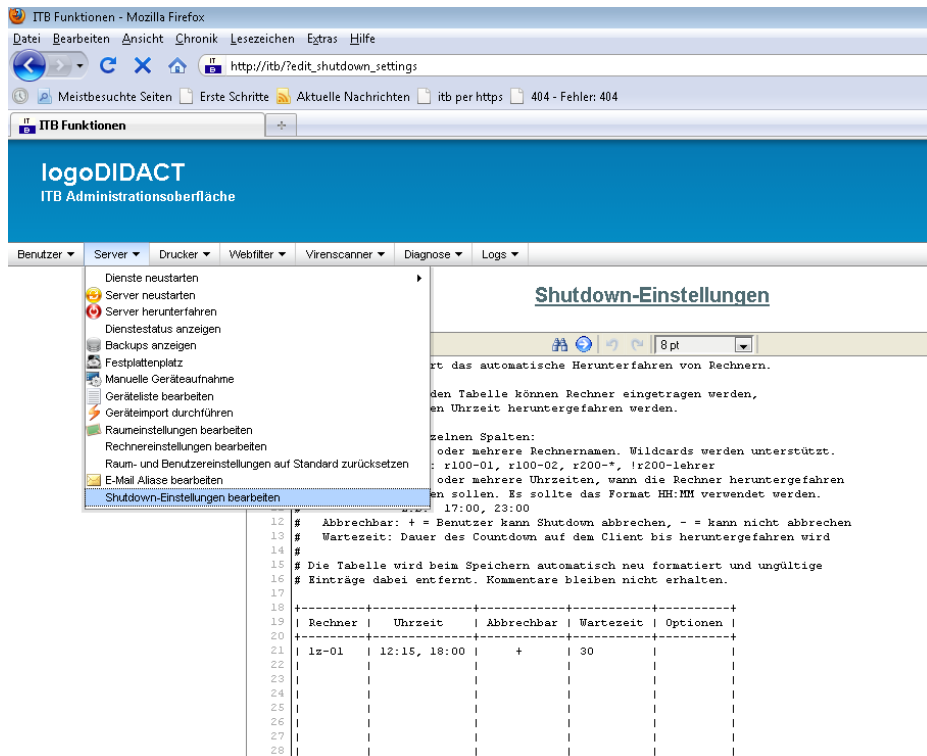


Abbildung V.2.14. Rechner über das ITB-Interface zeitgesteuert herunterfahren

Die Beschreibung zur Nutzung der Zeitsteuerung finden Sie im ITB-Interface selbst. Die Berechtigung für das Abbrechen der Aktion (Symbol "+") kann prinzipiell immer gesetzt sein. Die Wartezeit entspricht auf den Arbeitsstationen dem Countdown in Sekunden, die der Anwender dort sieht, bis seine Station abgeschaltet wird, sofern er die Aktion nicht abbricht. Die Wartezeit sollte entsprechend dem Benutzerverhalten am Rechner angepasst werden. Eine Wartezeit von 30 Sekunden ist in einem EDV-Raum, der zu 99% nach einer bestimmten Uhrzeit nicht mehr genutzt wird, sicherlich unproblematisch, während der Wert für einen Computer im Lehrerzimmer besser auf 300 Sekunden und damit 5 Minuten steht.



Achtung

Die Voraussetzung dafür, dass die Computer herunterfahren, ist ein installierter LogoDIDACT-Agent, der diesen Befehl über den gleichen Mechanismus entgegennimmt, wie das bei der Steuerung über die LogoDIDACT-Console im Livebetrieb geschieht.

V.2.1.7. Rechner zeitgesteuert aufwecken (Wake-On-LAN)

Über das ITB-Interface lassen sich die Computersysteme im Netzwerk zeitgesteuert aufwecken. Es ist dabei möglich, mehrere Aufweckzeiten zu definieren und auch Wochentage anzugeben, so dass die Computer z.B. nur von Montag bis Freitag und nicht auch am Wochenende aufgeweckt werden.

Vor allem bei älteren Rechnersystemen, die z.B. beim Starten durchaus 5 Minuten und länger benötigen bis man diese richtig verwenden kann, ist es extrem hilfreich, wenn man solche Geräte per Wake-On-LAN gezielt 5 Minuten vor Unterrichtsbeginn einschaltet.

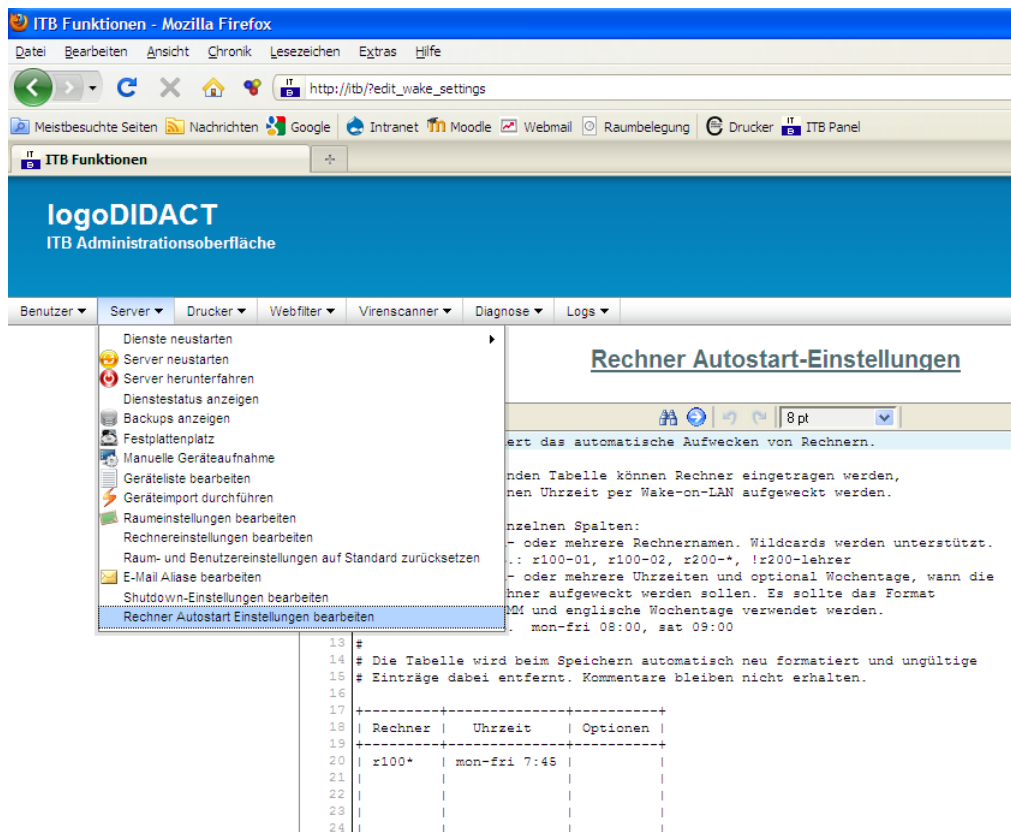



Abbildung V.2.15. Rechner über das ITB-Interface zeitgesteuert aufwecken



Achtung

Die Voraussetzung dafür, dass die Rechner tatsächlich aufwachen, müssen selbstverständlich gegeben sein und können von LogoDIDACT nicht beeinflusst werden. Die Systeme müssen sowohl vom BIOS her WOL unterstützen und entsprechend richtig konfiguriert sein, als auch durchgehend mit dem Stromnetz verbunden sein (keine Schüsselschalter und/oder nächtliche Stromabschaltung). Weiterhin funktioniert WOL in aller Regel nur, wenn die Computer sauber Heruntergefahren wurden, so dass sich die Netzwerkkarten in einem definierten Zustand befinden.

In der folgenden Tabelle finden Sie einige Beispiele für Zeit und Wochentagsangaben, um die Rechner im Netzwerk gezielt zu bestimmten Zeiten aufzuwecken.

Tabelle V.2.1. Beispiele für Zeit- und Wochentagsangaben zur Steuerung der Aufweckzeiten

Eintrag	Bedeutung
08:00	Jeden Tag 8 Uhr
08:00 09:00	Jeden Tag 8 Uhr und 9 Uhr
mon-fri 08:00	Montag bis Freitag 8 Uhr
mon-fri 08:00 09:00	Montag bis Freitag 8 Uhr und 9 Uhr
mon wed 17:00	Montags und Mittwochs 17 Uhr
!sun 07:00	Jeden Tag um 7 Uhr ausser Sonntags
mon-sun !tue 07:00	Jeden Tag um 7 Uhr ausser Dienstags
mon 05:00, tuesday 07:00	Montags um 5 Uhr und Dienstags um 7 Uhr

V.2.2. Drucker

V.2.2.1. Druckerzuordnungsliste

Über den Eintrag „Druckerzuordnungsliste bearbeiten“ lassen sich die installierten Drucker für die bestehenden Räume und Rechner aus der Geräteliste anzeigen.

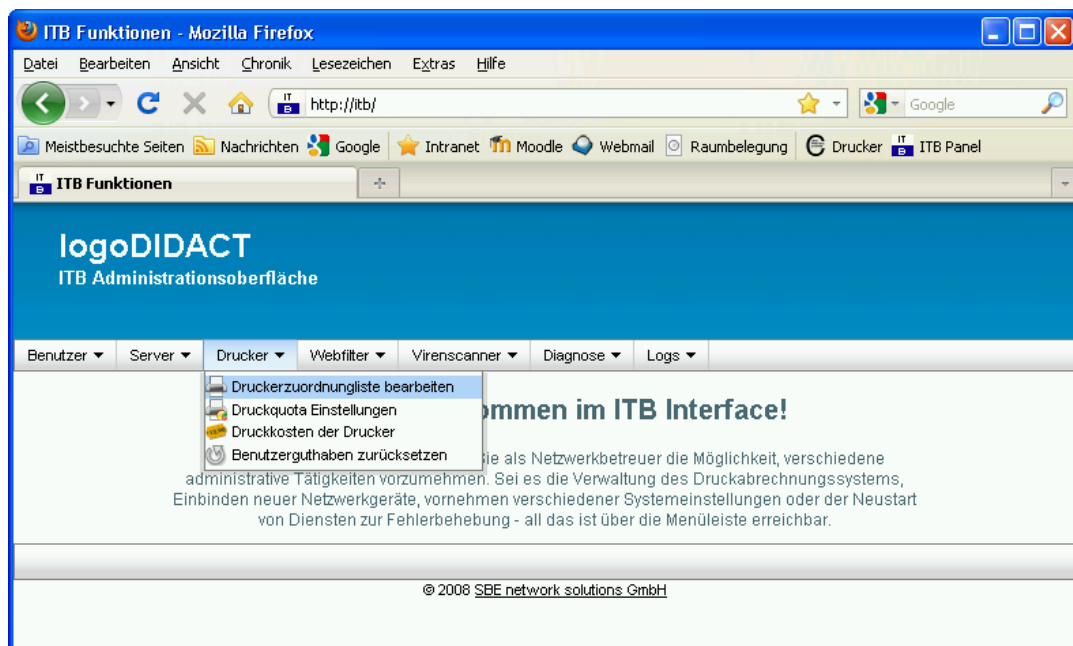


Abbildung V.2.16. Druckerzuordnungsliste bearbeiten (über ITB Funktionen)

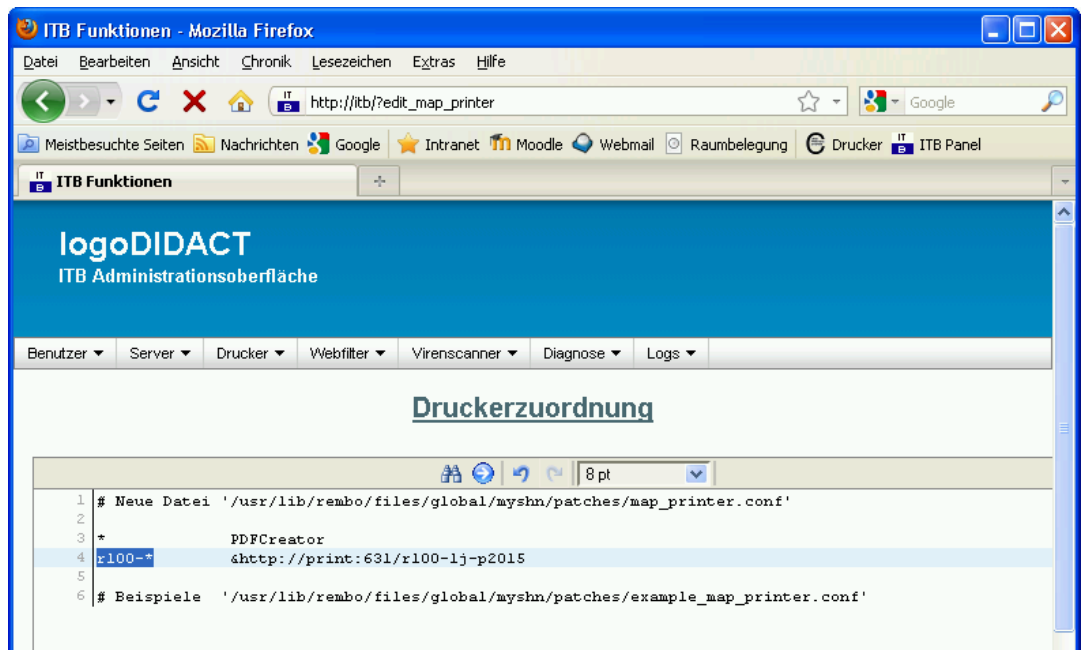


Abbildung V.2.17. Druckerzuordnungsliste bearbeiten („Konfiguration“)

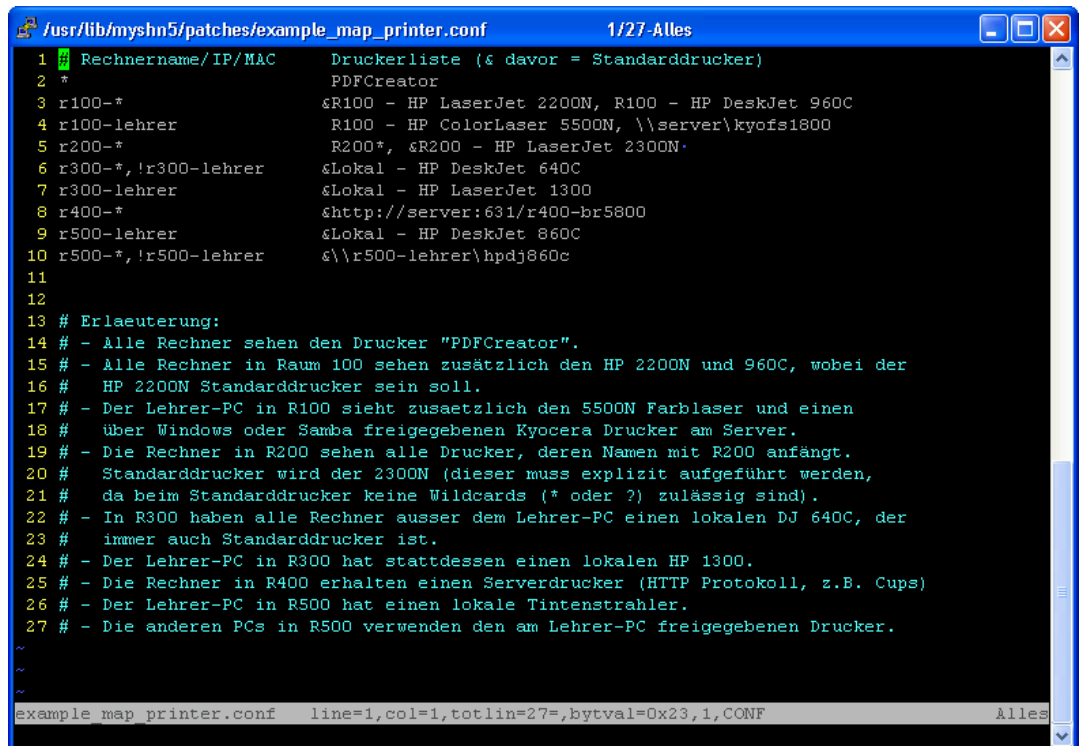


Abbildung V.2.18. Druckerzuordnungsliste („example_map_printer.conf“)

V.2.2.2. Druckquota

Über den Eintrag „Druckquota Einstellungen“ können Standardeinstellungen für die Druckquotierung konfiguriert werden.

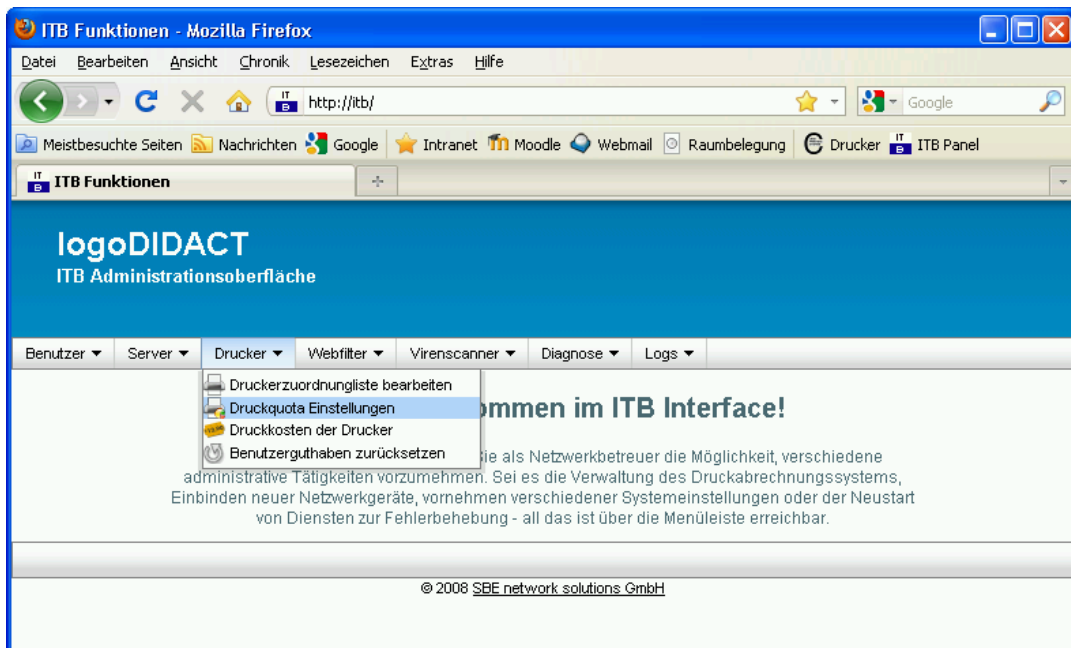



Abbildung V.2.19. Druckquota Einstellungen (über ITB Funktionen)



Tipp

Im oberen Bereich der einzelnen Kategorien finden sich in der Beschreibung wichtige Hinweise zur Bedeutung und Handhabung der jeweiligen Guthaben.

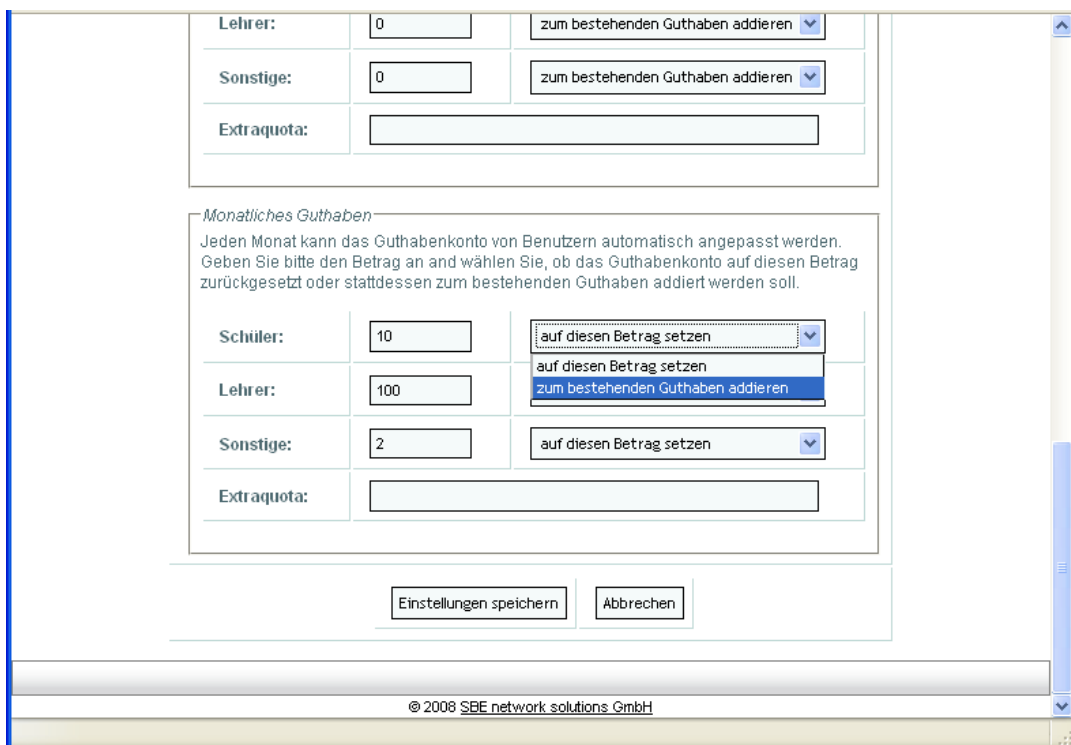


Abbildung V.2.20. Druckquota Einstellungen („Konfiguration“)

V.2.2.3. Druckkosten

Über den Eintrag „Druckkosten der Drucker“ lassen sich die am Server installierten Drucker mit Kosten (Preis pro Seite / Auftrag) belegen, um die Ausdrücke einzuschränken.

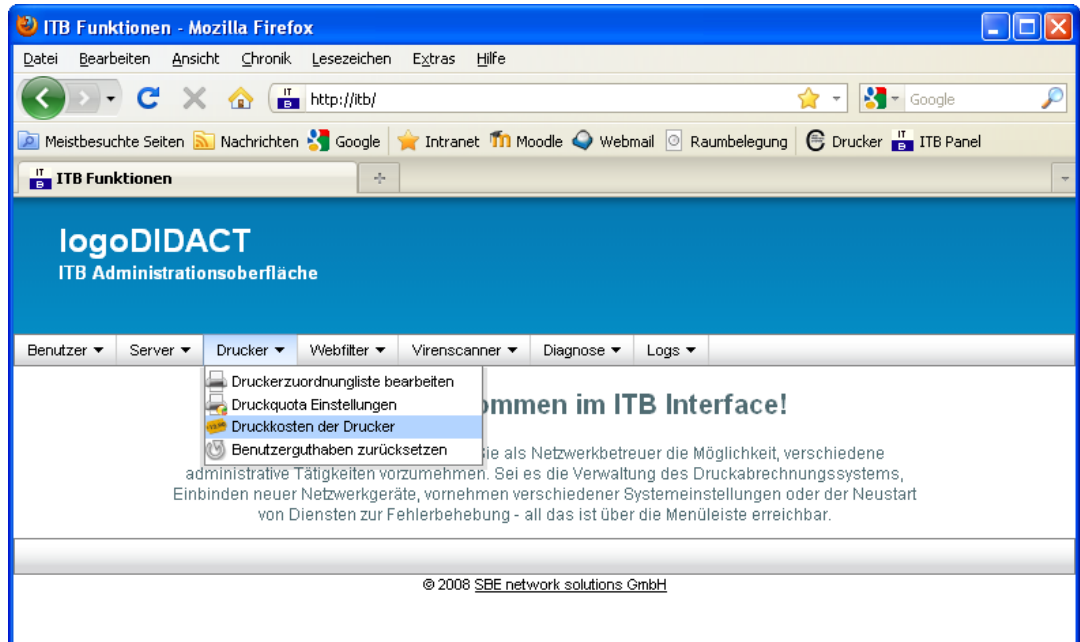


Abbildung V.2.21. Druckkosten der Drucker (über ITB Funktionen)

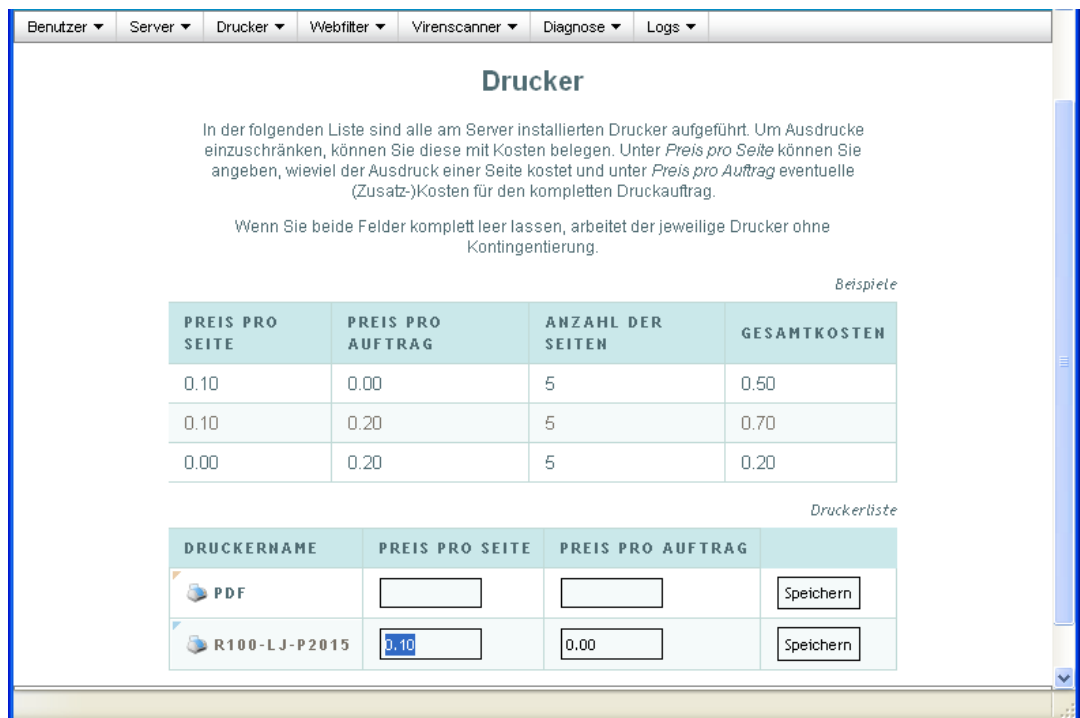


Abbildung V.2.22. Druckkosten der Drucker („Konfiguration“)



Achtung

Wenn die Eingabefelder Preis pro Seite / Auftrag leer gelassen werden, arbeiten die jeweiligen Drucker ohne Quotierung.

V.2.2.4. Druckauswertung

Über den Eintrag „Druckstatistiken anzeigen“ kann man sich verschiedene Auswertungen zu den über cups/pykota installierten Druckern anzeigen lassen.

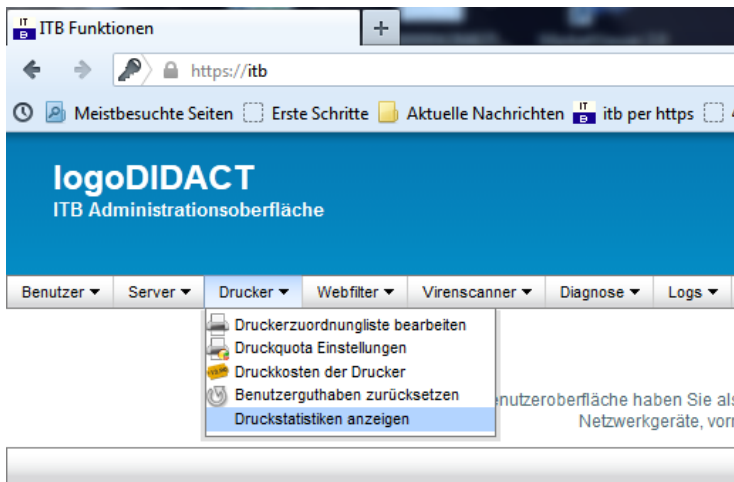


Abbildung V.2.23. Druckstatistiken anzeigen (über ITB-Interface)

Es gibt hierbei sowohl personenbezogene Auswertungen als auch gerätebezogene Statistiken. Der Abschnitt "PrinterAccounting" gibt die absolute Anzahl an Seiten aus, die ein Benutzer gedruckt hat und ist bei überdurchschnittlichem Tonerverbrauch sicherlich die erste Stelle, nach der man schauen sollte.

Username	PrinterAccounting		
	Requests	Pages	Pages/Request
sil	12	12	1
oc	9	9	1
sc	9	9	1
su	6	6	1
sc	5	5	1
rc	5	5	1
ar	5	5	1
sl	3	3	1
hk	3	3	1
kg	2	2	1
bn	2	2	1
rs	1	1	1
lg	1	1	1
uz	1	1	1
bt	1	1	1

Abbildung V.2.24. Absolute Anzahl an Ausdrucken pro Benutzer

Die erste und oberste Auswertung "Queue-User zeigt die Anzahl Ausdrücke gerätebezogen, d.h. sortiert nach Drucker und dann Benutzer.

Druckstatistiken

Queue	Queue Heuristic %Requests	%Pages	Pages
r108-hplj3015	86.15	86.15	56
r108-hpclj3600	13.85	13.85	9

Queue	Queue-User	Pages
	r108-hpclj3600	
-	si ber	4
-	su	2
-	bm	2
-	bt	1
	r108-hplj3015	
-	o rt	9
-	th	9
-	s er	8
-	sc	5
-	ro er	5
-	anke. er	5
-	su	4
-	sl	3
-	hb	3
-	kg	2
-	rs	1
-	lg	1
-	tz	1

Abbildung V.2.25. Anzahl Ausdrücke sortiert nach Drucker und Benutzer

Der letzte Abschnitt enthält gerätebezogene Statistikdaten, die eine zeitliche Übersicht geben, d.h. an welchem Tag wurde wie viel gedruckt und zu welcher Uhrzeit.

Hour	Hour Usage Requests
07	0
08	6
09	14
10	6
11	6
12	19
13	7
14	1
15	1
16	1
17	4
18	0
19	0
20	0
21	0
22	0

Date	Daily Usage %Requests	Pages
25/07/12	28	28
26/07/12	4	4
27/07/12	9	9
30/07/12	3	3
31/07/12	1	1
02/08/12	11	11
03/08/12	9	9

Abbildung V.2.26. Zeitangaben zum Druckverhalten pro Tag und nach Uhrzeit

V.2.3. Webfilter

V.2.3.1. Kategorien

Über den Eintrag „Webfilter Kategorien“ können die verschiedenen Webfilter Kategorien am Server konfiguriert werden.

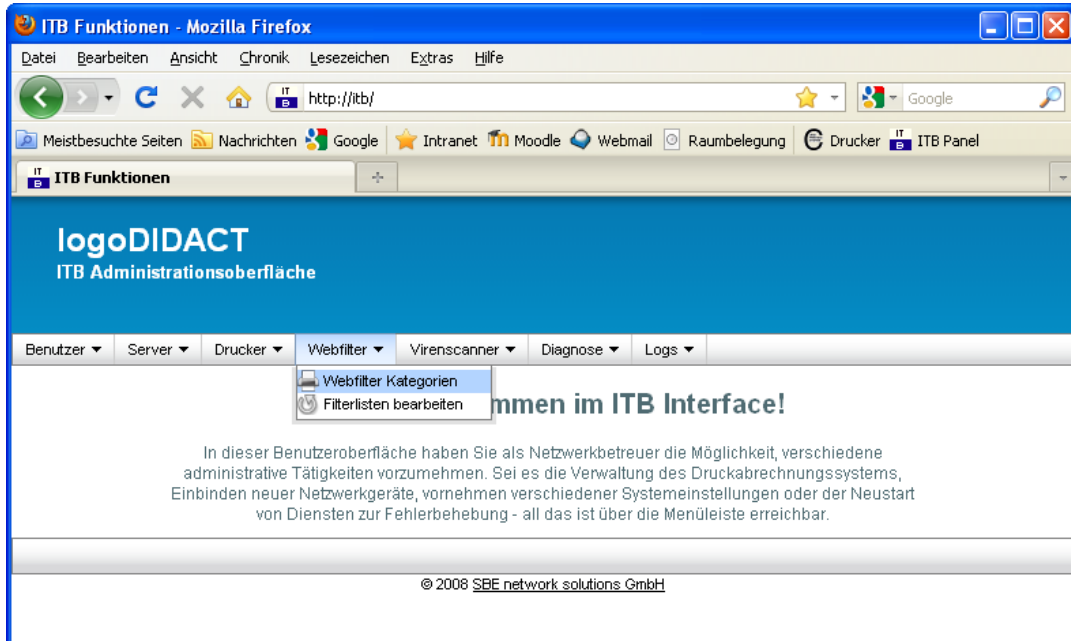


Abbildung V.2.27. Webfilter Kategorien (über ITB Funktionen)

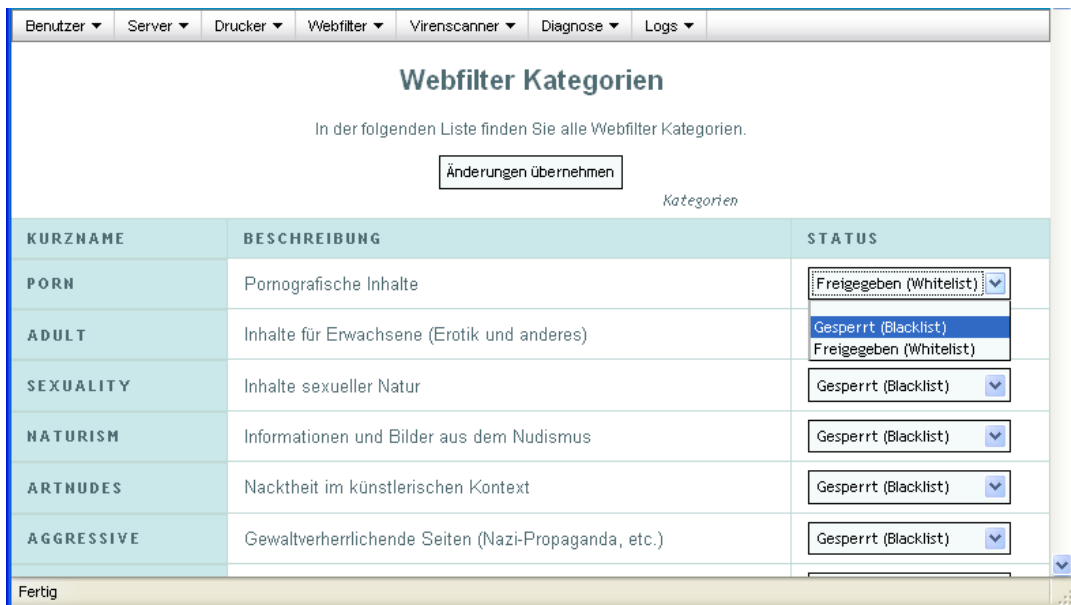


Abbildung V.2.28. Webfilter Kategorien („Konfiguration“)

Die vordefinierten Filterkategorien und dahinterstehenden jeweiligen Listen werden kontinuierlich über die Serverseite aktualisiert. Eine direkte Erweiterung dieser Listen um eigene Einträge ist nicht möglich. Individuelle Anpassungen erfolgen über eigene Black- und Whitelists im nächsten Abschnitt.

V.2.3.2. Filterlisten

Über den Eintrag „Filterlisten bearbeiten“ lassen sich die bestehenden Black- und Whitelisten des Webfilters durch eigene Einträge ergänzen.

Die eigene Blacklist ergänzt dabei die vorhandenen aktivierten Filterlisten. Die eigene Whitelist hat eine höhere Priorität als alle Blacklisteinträge, d.h. wenn Sie www.sex.de auf die Whitelist setzen, ist Seite frei, gleichgültig davon, ob diese Seite auf einer vorhandenen Standardfilterliste steht oder auf ihrer eigenen Blacklist.

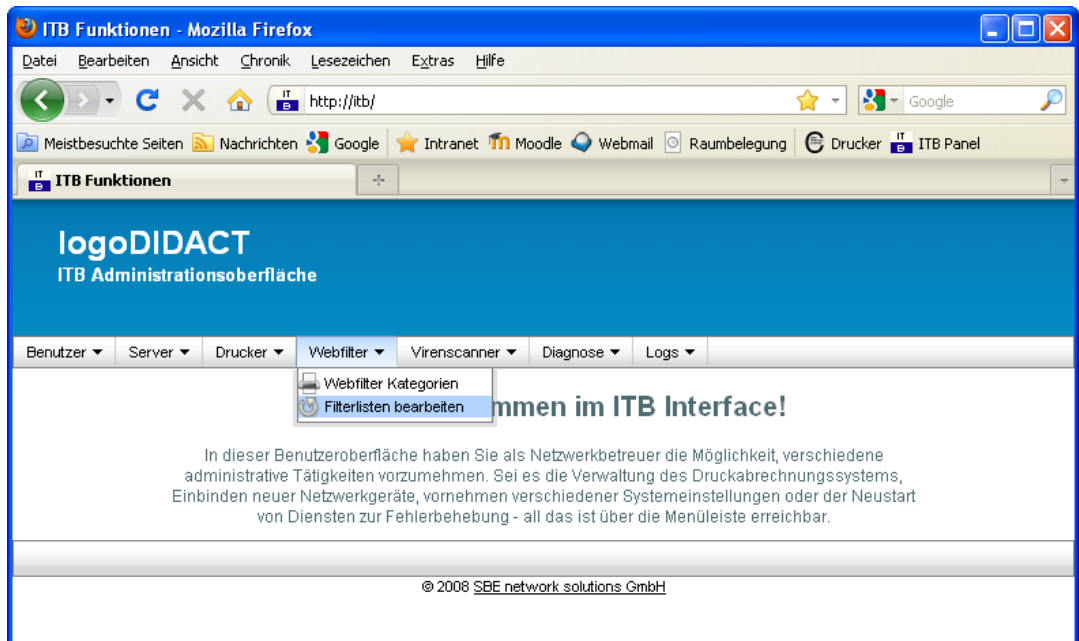


Abbildung V.2.29. Filterlisten bearbeiten (über ITB Funktionen)

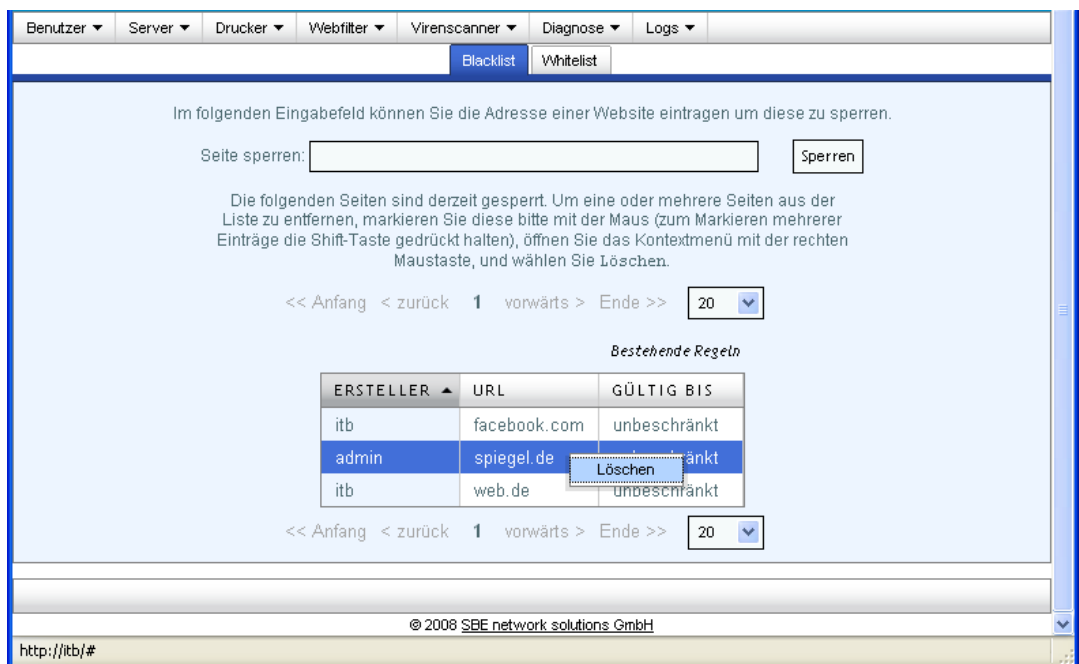


Abbildung V.2.30. Filterlisten bearbeiten („Konfiguration“)

V.2.4. Rembo/mySHN® Statistik und Images

Vor allem für die Fehlersuche im Bereich des Imaging mit Rembo/mySHN® ist es wichtig zu wissen, ob und wann ein Rechner zuletzt Online gestartet und synchronisiert wurde. Obwohl diese Information auch direkt am Client beim Start erkennbar ist, achten viele Endbenutzer nicht genau auf das Symbol "Offline", so dass im Supportfall die Aussagen oftmals nicht zuverlässig sind und man besser die Log-Dateien am Server prüft.

Diese Auswertung auf Dateiebene innerhalb von rechner-spezifischen Log-Dateien ist zum einen nicht ganz einfach und zum anderen braucht man dazu root-Zugang am Server.

Um die Auswertung auch dem admin bzw. itb zu ermöglichen und auch für den root deutlich zu vereinfachen, gibt es im ITB-Interface im Menü Server den Eintrag "mySHN Gerätestarts anzeigen".

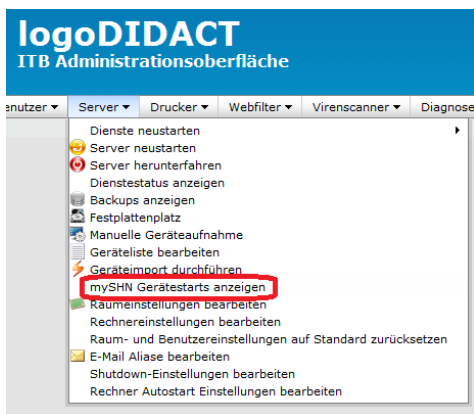


Abbildung V.2.31. Gerätestarts in Rembo/mySHN® anzeigen

Die Auswertung gibt primär den letzten synchronisierten Start eines Geräts an. Darüber hinaus erkennt man in der Spalte Images aber auch, ob es ein rechner-spezifisches Image gibt. Rechner-spezifische Images werden häufig eher versehentlich denn bewusst erstellt. Der "Fehler" wird dann oftmals erst beim nächsten Installieren und Verteilen von Software bemerkt, wenn ein oder mehrere Stationen die Software über das Gruppenimage nicht erhalten.

mySHN Gerätestarts			
Rechnername	Zeit seit letztem Start	Letzter Start	Images
netbook-10	4 Minuten	2012-08-07 15:00:09	
r108-04	4 Tage	2012-08-03 12:39:36	
r108-01	4 Tage	2012-08-03 12:04:41	
r108-03	8 Tage	2012-07-29 16:42:49	
r108-02	11 Tage	2012-07-27 10:58:35	
r221-04	13 Tage	2012-07-25 09:08:23	
fac-nb-05	13 Tage	2012-07-25 09:01:41	
r221-05	13 Tage	2012-07-25 08:52:50	
r221-13	13 Tage	2012-07-25 08:48:44	
r221-16	13 Tage	2012-07-25 08:47:28	
r221-14	13 Tage	2012-07-25 08:46:41	
r221-09	13 Tage	2012-07-25 08:46:35	
r221-08	13 Tage	2012-07-25 08:46:27	
r221-15	13 Tage	2012-07-25 08:46:27	
r221-02	13 Tage	2012-07-25 08:46:09	
r221-07	13 Tage	2012-07-25 08:45:58	
r221-10	13 Tage	2012-07-25 08:45:57	
r221-11	13 Tage	2012-07-25 08:45:55	
r221-06	13 Tage	2012-07-25 08:45:54	
r221-03	13 Tage	2012-07-25 08:45:48	
r221-lehrer	13 Tage	2012-07-25 08:05:42	
r329-lehrer	13 Tage	2012-07-25 07:39:48	
r108-05	13 Tage	2012-07-25 07:31:54	
fac-nb-06	14 Tage	2012-07-24 09:53:07	
r329-05	14 Tage	2012-07-24 08:07:57	
r329-10	14 Tage	2012-07-24 08:07:29	
r329-14	14 Tage	2012-07-24 08:06:04	
r329-09	14 Tage	2012-07-24 08:04:58	
r329-15	14 Tage	2012-07-24 08:04:43	
r329-08	14 Tage	2012-07-24 08:04:39	
r329-07	14 Tage	2012-07-24 08:04:33	
r329-06	14 Tage	2012-07-24 08:04:26	
r329-12	14 Tage	2012-07-24 08:04:08	

Abbildung V.2.32. Anzeige der letzten Synchronisation und rechner-spezifischer Images

Teil VI. Anwender

Inhaltsverzeichnis

VI.1. Übersicht	VI – 5
VI.1.1. Selbstteilende Arbeitsstationen	VI – 5
VI.1.2. Benutzer, Rechte und Rollen	VI – 5
VI.1.3. Verzeichnisstruktur in LogoDIDACT	VI – 5
VI.1.3.1. Netzlaufwerke H-, T- und P:	VI – 5
VI.1.3.2. Verzeichnisstruktur und Ordneransicht der Schüler	VI – 6
VI.1.3.3. Verzeichnisstruktur und Ordneransicht der Lehrer	VI – 7
VI.1.3.4. Reduzierte Ansicht für Lehrer durch Eintrag in Klassen	VI – 7
VI.2. Anleitung LogoDIDACT-Console	VI – 11
VI.2.1. Schnelleinstieg	VI – 11
VI.2.1.1. Internet an/aus	VI – 11
VI.2.1.2. Bildschirme sperren	VI – 14
VI.2.2. Benutzeroberfläche	VI – 16
VI.2.3. Raumsteuerung	VI – 18
VI.2.3.1. Austeilen und Einsammeln von Dateien	VI – 20
VI.2.3.2. Bildschirmübertragung	VI – 23
VI.2.3.3. Klassenarbeitsmodus	VI – 25
VI.2.3.4. Didaktische Funktionen	VI – 33
VI.2.4. Benutzerverwaltung	VI – 34
VI.2.4.1. Die Möglichkeiten als Lehrer	VI – 35
VI.2.4.2. Erstellen der Benutzerkärtchen	VI – 35
VI.2.4.3. Bearbeiten der Kennwörter	VI – 38
VI.2.4.4. Kennwortrichtlinien in der LogoDIDACT-Console ändern	VI – 39
VI.2.4.5. Eigenes Kennwort ändern	VI – 39
VI.2.5. Service- und Support für Lehrer	VI – 40
VI.2.5.1. Problemstellung	VI – 40
VI.2.5.2. Die Lösung in der Übersicht	VI – 41
VI.2.5.3. Vorteile	VI – 41
VI.2.5.4. Anzeige von Störungen	VI – 41
VI.2.5.5. Das Hauptfenster im Ticketsystem	VI – 42
VI.2.5.6. Neue Störung per Assistent erfassen	VI – 43
VI.2.5.7. Störungen bearbeiten	VI – 47
VI.2.5.8. Störungen weiterleiten	VI – 47
VI.2.5.9. Störungen abschliessen	VI – 49
VI.3. Arbeiten von Zuhause aus	VI – 51
VI.3.1. Remote-Einwahl Vorbereitungen	VI – 51
VI.3.2. Installation auf Windows-Clients	VI – 51
VI.3.3. VPN-Einwahl	VI – 52
VI.3.3.1. VPN-Einwahl per graphischer Oberfläche mit OpenVPN GUI	VI – 52
VI.3.4. Die LogoDIDACT-Console über OpenVPN	VI – 54
VI.3.4.1. Start der LogoDIDACT-Console per VPN	VI – 54
VI.3.5. Zugriff auf Web-Dienste per OpenVPN	VI – 56
VI.3.6. Zugriff auf Dateien per VPN	VI – 56
VI.3.6.1. Verbindung von Netzlaufwerken mit GUILogon	VI – 56
VI.4. Microsoft 365	VI – 59
VI.4.1. LogoDIDACT-Ankopplung an Office 365	VI – 59
VI.4.1.1. Automatisierung mit LD Azure Connect	VI – 59
VI.4.1.2. Vorteile	VI – 59
VI.4.1.3. Was macht der Connector LD Azure Connect	VI – 60
VI.4.2. Anmelden an Office 365	VI – 60
VI.4.2.1. Keine Anmeldung bei zu einfachem und kurzem Kennwort	VI – 62
VI.4.2.2. Kennwort- Sicherheit und Komplexität	VI – 63

VI.4.2.3. Der LogoDIDACT-Server ist die Zentrale für Benutzer-Identitäten	VI – 64
VI.4.2.4. Empfohlene Kennwort-Komplexität	VI – 65
VI.4.2.5. Das SSP Portal zum Ändern des Kennwortes	VI – 66
VI.4.3. Der richtige Umgang mit Teams	VI – 68
VI.4.3.1. Besprechungs-Richtlinien	VI – 68
VI.5. Nextcloud	VI – 71
VI.5.1. Nextcloud in LogoDIDACT	VI – 71
VI.5.1.1. Zugriff auf Nextcloud	VI – 71
VI.5.1.2. Anmeldung und Voraussetzung	VI – 72
VI.5.1.3. Teilen von Dokumenten	VI – 72
VI.5.1.4. Arbeiten mit Nextcloud und Collabora	VI – 76
VI.6. Webdienste	VI – 77
VI.6.1. Content Management System	VI – 77
VI.6.1.1. Erste Schritte	VI – 77
VI.6.1.2. Ihre Vorteile	VI – 83
VI.6.2. Raumbuchungssystem	VI – 83
VI.6.2.1. Räume anlegen	VI – 84
VI.6.2.2. Zeitreservierungen erstellen	VI – 86
VI.6.3. Webmailer	VI – 89
VI.6.3.1. Die Roundcube Oberfläche	VI – 90
VI.6.3.2. E-Mail Nachricht verfassen	VI – 91
VI.6.4. Interne Webseiten	VI – 92
VI.6.4.1. Zugriff auf Webseiten über private_html und public_html	VI – 92
VI.6.5. Zugriff per Browser auf Dateien	VI – 92

Kapitel VI.1. Übersicht

VI.1.1. Selbstheilende Arbeitsstationen

Ein wesentlicher Bestandteil von LogoDIDACT ist das Prinzip der selbstheilenden Arbeitsstationen mit Rembo/mySHN®. Selbstheilend bedeutet dabei, dass bei jedem Neustart die Arbeitsstationen innerhalb von wenigen Sekunden wieder auf einen definierten funktionsfähigen Zustand gebracht werden. Je nach Betriebssystem kann dieser Vorgang z.B. bei Windows 7 auch sehr viel länger dauern, wenn die Benutzer die Computersysteme nicht sauber herunterfahren. Als Lehrer haben Sie aber mit der LogoDIDACT-Console sehr viel Kontrolle sowohl über die Schüler als auch die Arbeitsstationen und können diese gezielt steuern.

Der Mechanismus der "Selbstheilung" sorgt aber in jedem Fall dafür, dass die Arbeitsstationen zuverlässig und mit minimalem Aufwand betrieben werden können und sich alle Computer auch vollkommen identisch verhalten.



Achtung

Selbstheilende Arbeitsstation bedeutet auch, dass keine Dokumente auf C: abgespeichert werden dürfen, weil diese beim Neustart automatisch und unwiederbringlich entfernt werden. Dateien müssen auf eines der Serverlaufwerke H: oder T: gespeichert werden (siehe Abschnitt VI.1.3, „Verzeichnisstruktur in LogoDIDACT“).

VI.1.2. Benutzer, Rechte und Rollen

In LogoDIDACT erhält jeder Benutzer einen eigenen individuellen Nutzerzugang, mit dem er sich am System anmelden muss, um auf die Dienste (Dateiablage, Drucken, Internet, Mail usw.) des Servers zugreifen zu können. Mehr oder weniger anonyme Anmeldungen in der Form schueler01, schueler02 oder lehrer01 sind zwar prinzipiell möglich, sollten aber unbedingt vermieden werden. Mit LogoDIDACT ist es sehr einfach, auch Hunderte Benutzer leicht zu verwalten und neue Benutzer über Listen anzulegen. Zu Beginn erhält jeder Benutzer vom Administrator ein Benutzerkärtchen mit seinen Anmeldeinformationen. Ob Sie als Benutzer ihr Passwort ändern können, dürfen oder sogar bei der ersten Anmeldung ändern müssen, kann Ihr Administrator individuell pro Klasse bzw. Gruppe oder auch einzelnen Benutzer festlegen.

VI.1.3. Verzeichnisstruktur in LogoDIDACT

VI.1.3.1. Netzlaufwerke H:, T: und P:

Wie weiter oben bereits erwähnt, dürfen Dokumente wegen der Funktion der selbstheilenden Arbeitsstation nicht lokal auf dem Laufwerk C: abgelegt werden. In LogoDIDACT verfügt jeder Benutzer automatisch auch über einen eigenen Speicherbereich auf dem Server. Dieser Bereich wird bei der Anmeldung automatisch mit dem Laufwerksbuchstaben H: verbunden. Umgangssprachlich wird H: in aller Regel als Homelaufwerk oder Heimatlaufwerk bezeichnet, so dass man sich diese Zuordnung auch etwas einfacher merken kann. Weder Lehrer noch Schüler können aber auf diesem Laufwerk beliebig viele Daten ablegen. In der Regel gibt es dafür eine Beschränkung (Quotierung). Sobald der Speicherplatz eines Benutzers in seinem Homelaufwerk nicht mehr ausreicht, erhält er eine entsprechende Rückmeldung auf der Arbeitsstation.

Sinn und Zweck des Laufwerks mit dem Buchstaben T: ist ebenfalls leicht zu merken, denn darüber ist das Tauschen von Dokumenten möglich.

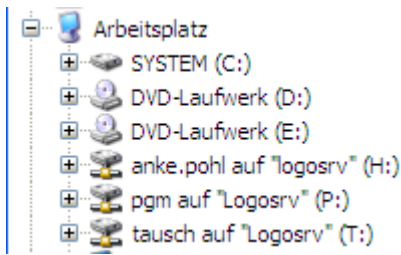


Abbildung VI.1.1. Lokale Laufwerke und Netzlaufwerke

Innerhalb von T: gibt es verschiedene Ordner für Klassen, Projekte, Lehrer und Übergreifend. Je nachdem ob man Lehrer, Schüler oder Administrator ist oder auch in bestimmten Projekten Mitglied ist, hat man hier verschiedene Sichtweisen und Zugriffsmöglichkeiten.

Tabelle VI.1.1. Laufwerksbuchstaben und Freigaben

Laufwerk	Freigabe	Pfad am Server	Beschreibung
H:	homes	/home/users/Benutzername	Persönliches Arbeitsverzeichnis mit Vollzugriff auf eigene Dateien.
T:	tausch	/home/tausch	Tauschverzeichnis mit Unterordnern für Klassen, Kurse, Projekte, Lehrer und Schulweit.
P:	pgm	/home/samba/progs	Verzeichnis bzw. Laufwerk für serverbasiert installierte Programme.

VI.1.3.2. Verzeichnisstruktur und Ordneransicht der Schüler

Als Schüler hat man in seinem Homelaufwerk H: einen Unterordner **Einsammeln** und **Profi-
le**. Der Ordner **OpenVPN** ist nur vorhanden, wenn der Administrator des Netzwerkes den Zugang per VPN freigegeben hat. Ein Unterordner **Ausgeteilt** wird ebenfalls erst dynamisch erstellt, wenn ein Lehrer ein Dokument an Schüler verteilt.

Im Tauschlaufwerk T: sieht man als Schüler nur den Tauschordner seiner Klasse und den Ordner "Schulweiter Tausch". Wenn man auch Mitglied einer Projektgruppe ist, dann sieht man dort auch sämtliche Tauschordner der jeweiligen Gruppe (z.B. Internet AG).

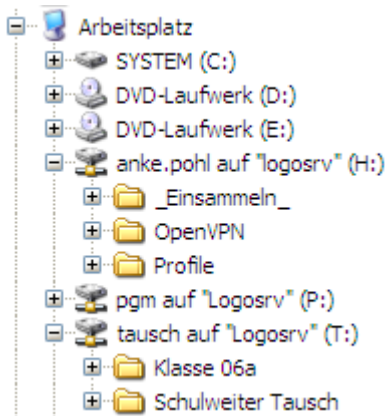


Abbildung VI.1.2. Verzeichnisstruktur und Ordneransicht als Schüler

VI.1.3.3. Verzeichnisstruktur und Ordneransicht der Lehrer

Sowohl Lehrer als auch Schüler sehen die Laufwerke H:, T: und P:. Innerhalb dieser Laufwerke befinden sich jedoch je nach Rolle bzw. Gruppe verschiedene Unterordner. Als Lehrer hat man im Tauschlaufwerk über den Unterordner **Klassen** Zugriff auf alle Klassentauschlaufwerke. Ist man in Projektgruppen Mitglied, dann sieht man auch die Tauschlaufwerke dieser Gruppen. Weiterhin sieht man einen Ordner **Lehrertausch** auf den nur alle Lehrer Zugriff haben.

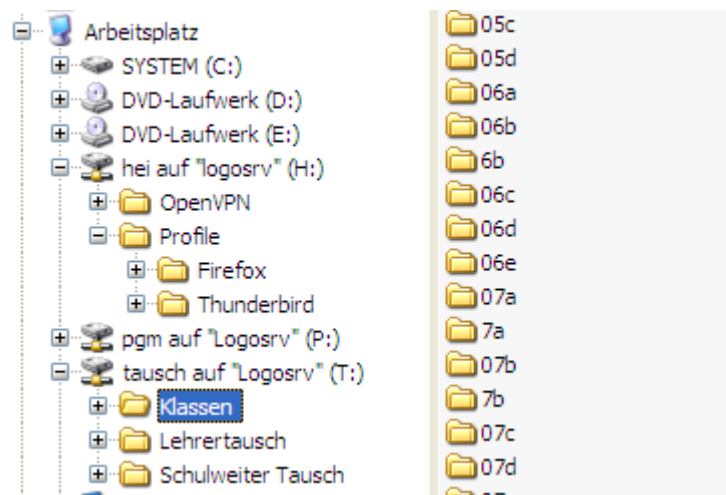


Abbildung VI.1.3. Verzeichnisstruktur und Ordneransicht als Lehrer

VI.1.3.4. Reduzierte Ansicht für Lehrer durch Eintrag in Klassen

Per Standard ist ein Lehrer keiner speziellen Klasse zugeordnet und sieht deshalb alle Tauschordner aller Klassen. Auch in der Benutzerverwaltung sieht er alle Schüler der gesamten Schule. Es besteht die Möglichkeit, dass man diese Ansichten für Kollegen, die nur selten die EDV für den Unterricht nutzen, etwas vereinfacht. Damit reduziert man die Ansicht auf eine oder mehrere Klassen sowohl in der Benutzerverwaltung als auch auf Dateisebene.



Achtung

Jeder Lehrer kann diese Aufgabe selbst übernehmen und sich seiner Klasse oder seinen Klassen zuordnen. Beim Schuljahreswechsel muss diese Zuordnung manuell korrigiert werden, d.h. ein Lehrer, der für die Klasse 8a eingetragen war, wird durch das Versetzen der Schüler in die 9a nicht automatisch der 9a zugeordnet.

VI.1.3.4.1. Lehrer einer Klasse zuordnen

Um sich als Lehrer in eine Klasse einzutragen, startet man die LogoDIDACT-Console und wählt aus dem Menü **Ansicht** den Eintrag **Benutzerverwaltung**. Ohne Zuordnung zu einer speziellen Klasse sieht man alle Schüler sämtlicher Klassen.

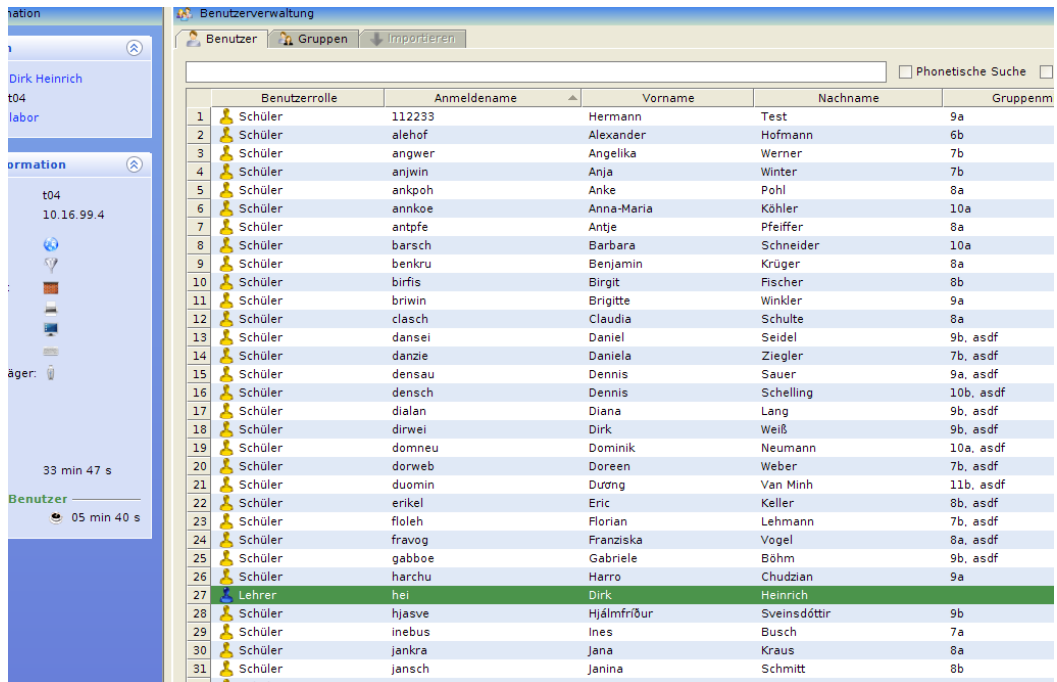


Abbildung VI.1.4. Als Lehrer ohne Klassenzuordnung sieht man alle Schüler

Wechseln Sie zunächst zur Registerkarte **Gruppen**. Markieren Sie dort die Klasse und wählen Sie mit der rechten Maustaste aus dem erscheinenden Kontextmenü den Eintrag **Selbst als Mitglied eintragen**.

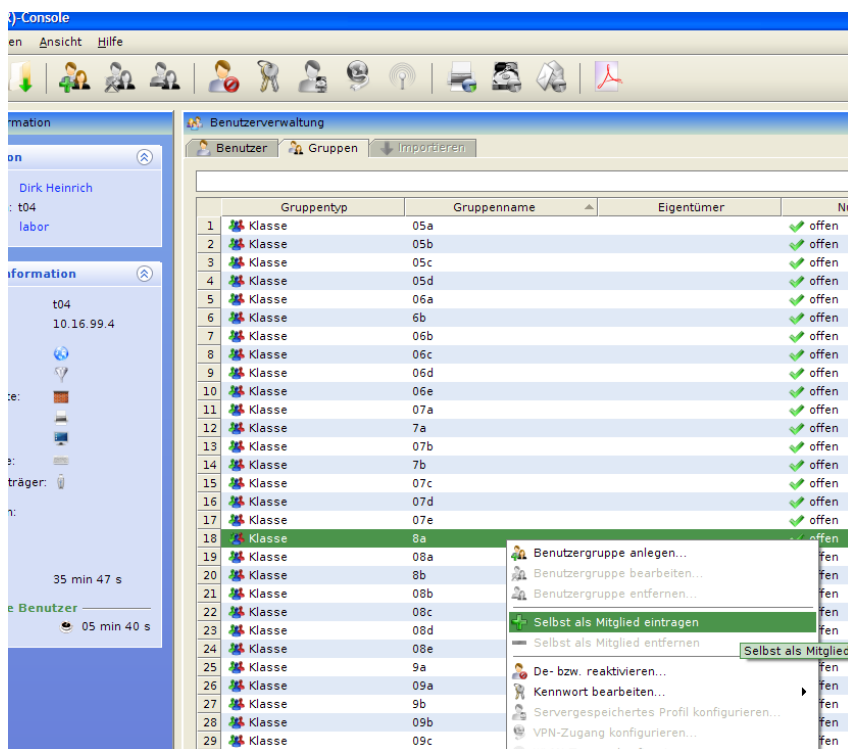


Abbildung VI.1.5. Sich selbst als Lehrer einer Klasse zuordnen

VI.1.3.4.2. Reduzierte Ansicht nach Klassenzuordnung

Nach der Zuordnung eines Lehrers zu einer Klasse sieht man in der Registerkarte **Benutzer** bei sich selbst die entsprechende Klasse in der Spalte **Gruppenmitgliedschaft**. Weiterhin sehen Sie nur noch die Schüler Ihrer zugeordneten Klasse. Selbstverständlich können Sie sich auf diese Art und Weise auch mehreren Klassen zuordnen, so dass Sie beispielsweise nur alle Schüler der Klassenstufe 8 sehen.

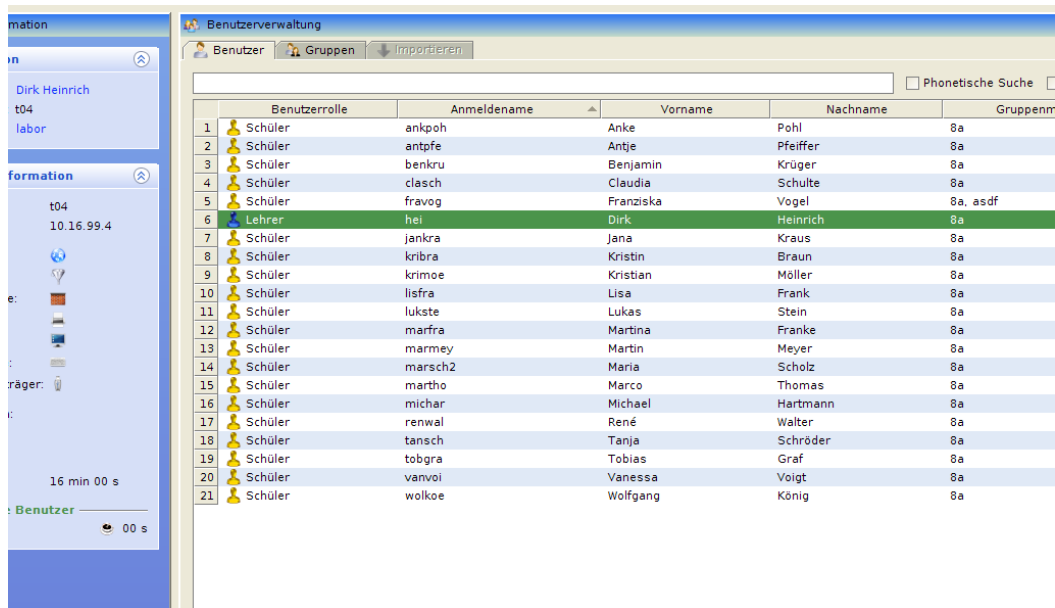


Abbildung VI.1.6. Reduzierte Benutzeransicht nach Zuordnung zu einer Klasse

Diese reduzierte und damit einfachere Ansicht ergibt sich auch im Dateisystem und Sie sehen im Tauschbereich nur noch die Klassen, für die Sie sich eingetragen haben.



Abbildung VI.1.7. Reduzierte Ordneransicht nach Zuordnung zu einer Klasse

Auch beim Austeilen von Dokumenten über die LogoDIDACT-Console wird die reduzierte und vereinfachte Ansicht deutlich.

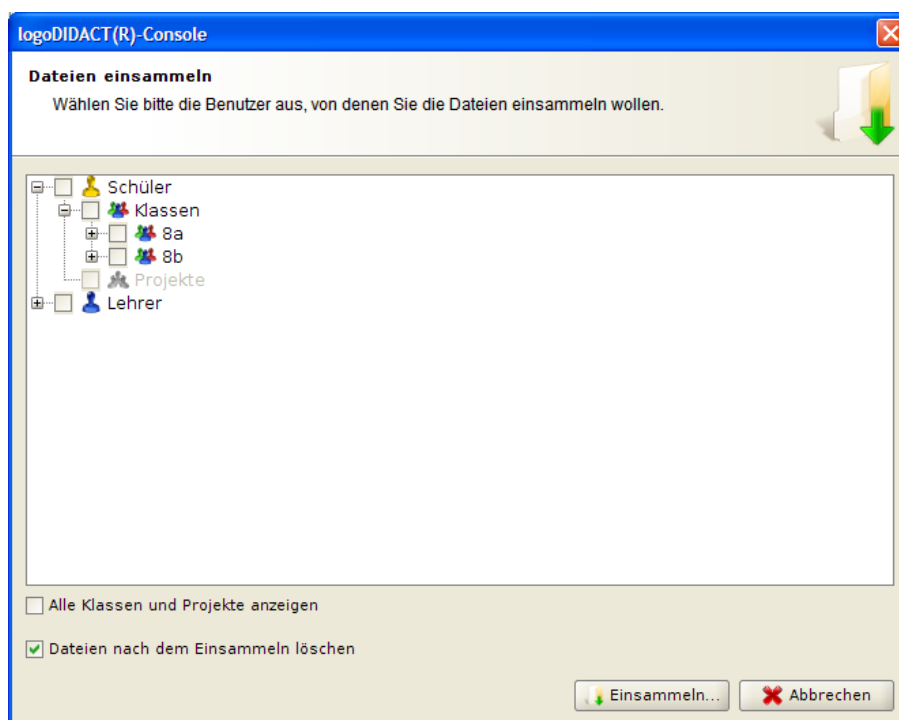
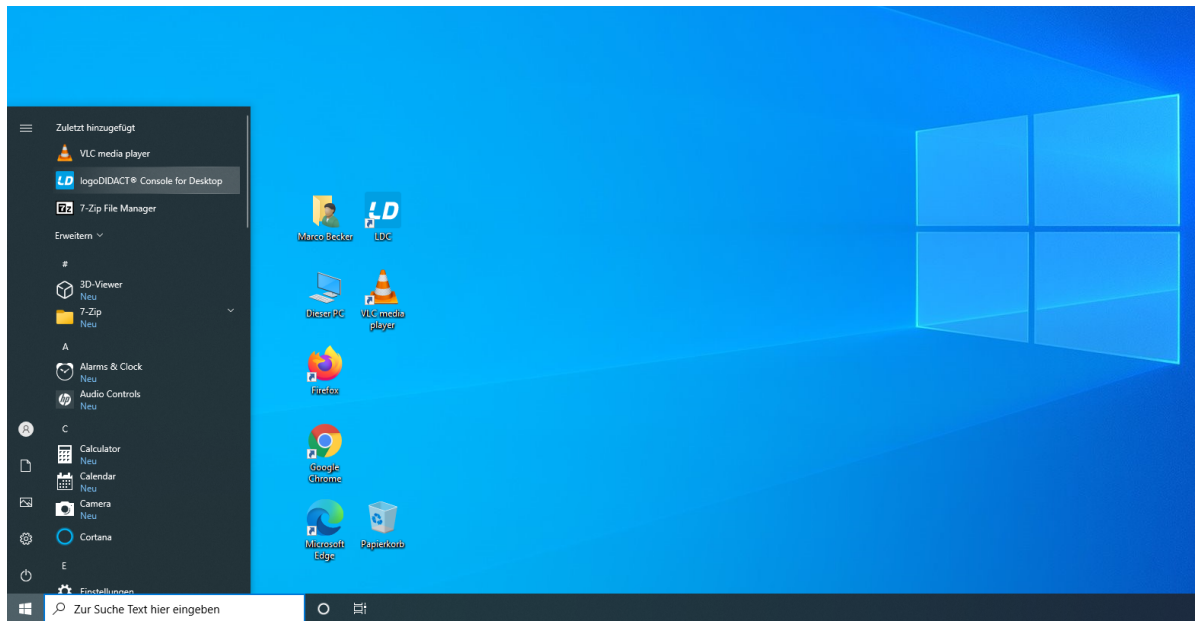


Abbildung VI.1.8. Reduzierte Ansicht beim Austeilen und Einsammeln

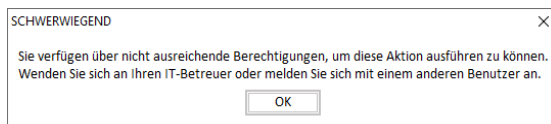
Kapitel VI.2. Anleitung LogoDIDACT-Console

VI.2.1. Schnelleinstieg

Die grafische Oberfläche LogoDIDACT-Console lässt sich unter Windows zum einen über das Startmenü, zum anderen über die Verknüpfung „LDC“ auf dem Desktop aufrufen.



Das Arbeiten mit der LogoDIDACT-Console ist Lehrern und Systemadministratoren vorbehalten. Alle anderen Benutzerkonten, die nicht über ausreichende Berechtigungen verfügen, erhalten beim Versuch, das Programm zu starten, eine Fehlermeldung.



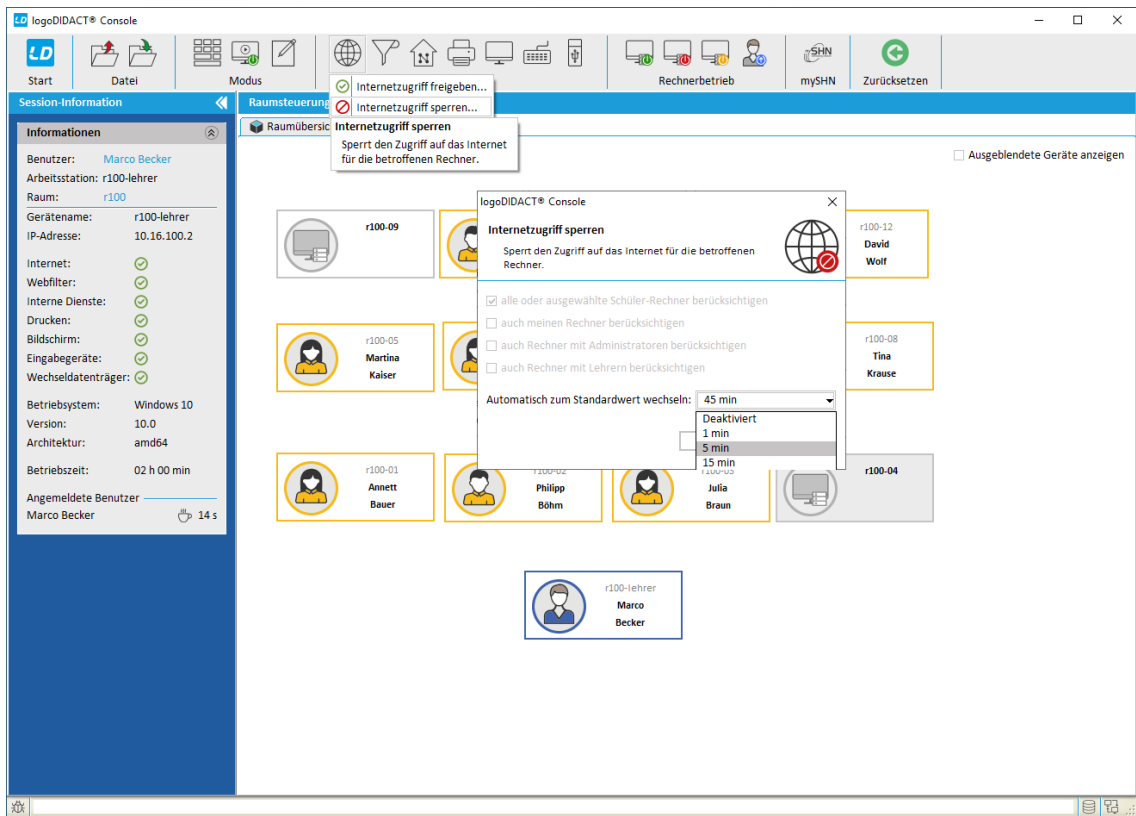
Achtung

Benutzer die sich an Windows mit dem Konto eines Lehrers oder Administrators anmelden, werden beim Programmstart der LogoDIDACT-Console automatisch erkannt und gegenüber dem System authentifiziert.

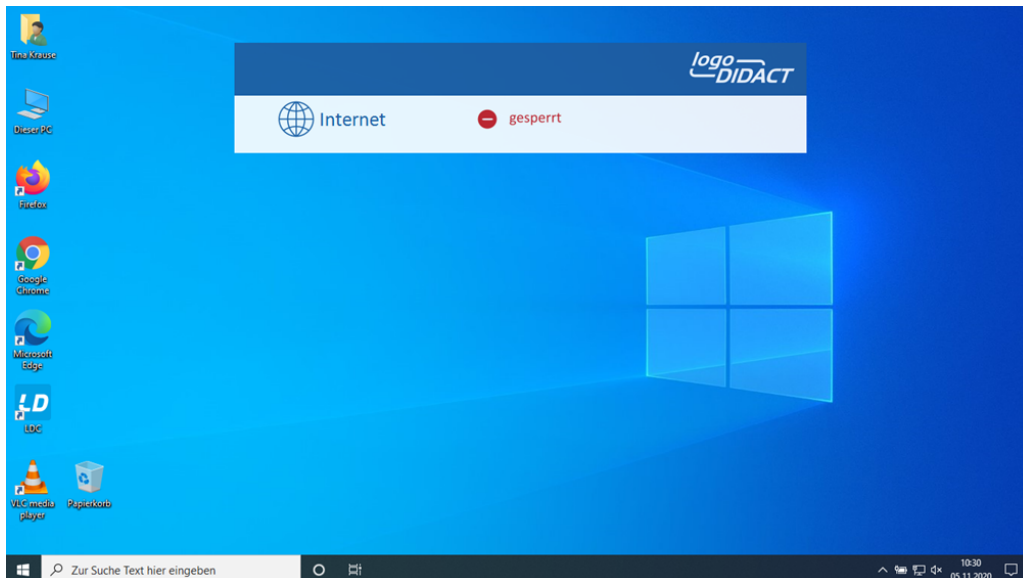
Nach dem Start landen Sie automatisch im Modul der Raumsteuerung. In dieser Oberfläche stehen Ihnen vielfältige Funktionen zur Gestaltung des digitalen Unterrichts zur Verfügung.

VI.2.1.1. Internet an/aus

Durch Klick auf das Internet-Symbol in der Menüleiste und den Eintrag **Internet sperren...** kann der Zugriff auf das Internet für den Raum gesperrt werden. Sie können im nachfolgenden Dialog dabei festlegen, wie lange das Internet gesperrt werden soll, bis es automatisch wieder freigegeben wird.



Alle Schüler*innen bekommen auf den Rechnern eine entsprechende Rückmeldung, dass der Internetzugang gesperrt wurde. Die Meldung wird dabei dynamisch eingeblendet, bleibt einige Sekunden stehen und verschwindet dann wieder.

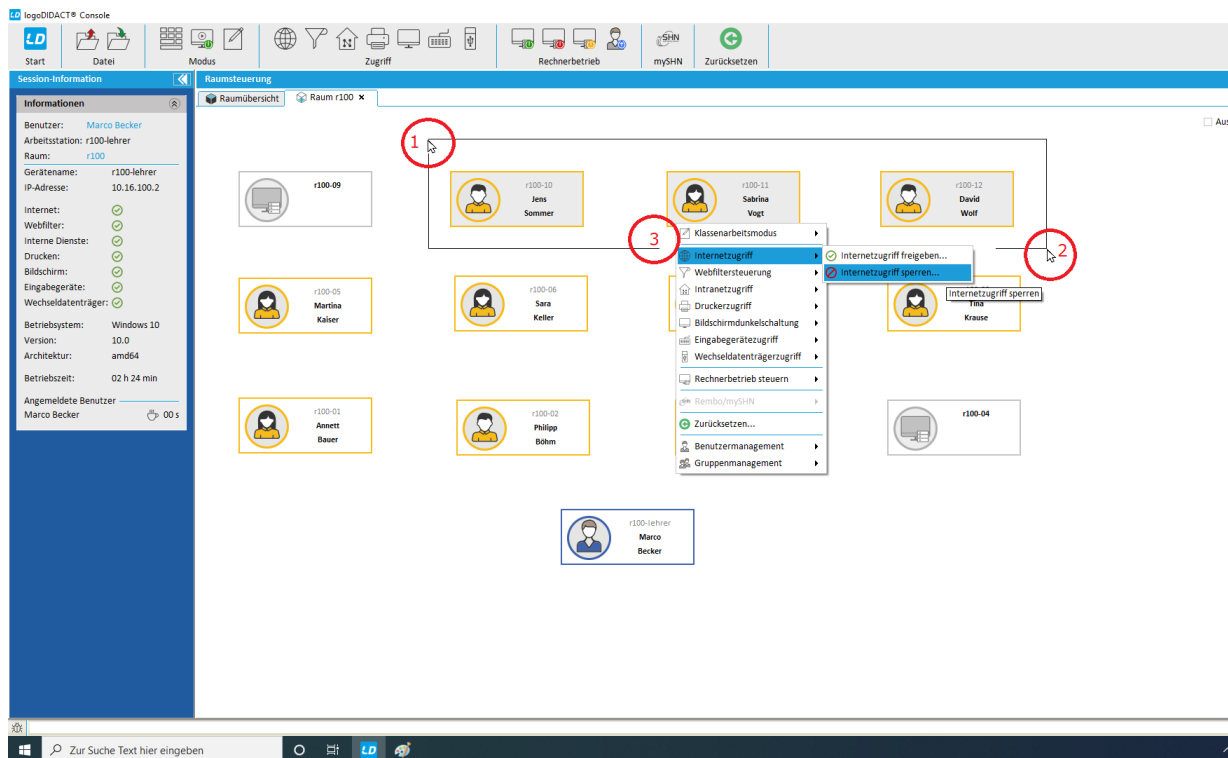




Tipp

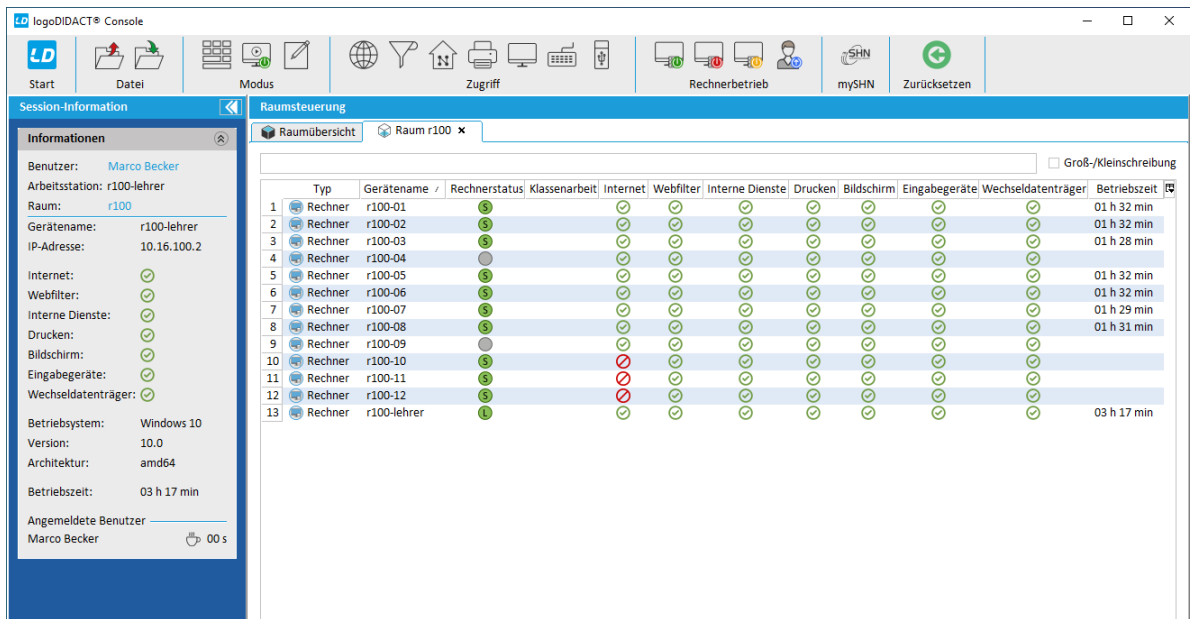
Bei ausgewählten Rechnern werden die Aktionen der Raumsteuerung lediglich auf die markierten Geräte und nicht auf den Raum ausgeführt.

Eine Auswahl mehrerer Benutzer erfolgt dabei über die Maus, indem Sie den Mauszeiger an eine Position platzieren, die linke Maustaste gedrückt halten und durch Bewegung der Maus eine Rechteck aufspannen und darüber mehrere Elemente markieren. Über die rechte Maustaste wählt man dann aus dem Kontextmenü den Eintrag **Internet sperren...**



Alle Aktionen lassen sich über das Kontextmenü selbstverständlich auch gezielt auf einen einzelnen Benutzer anwenden.

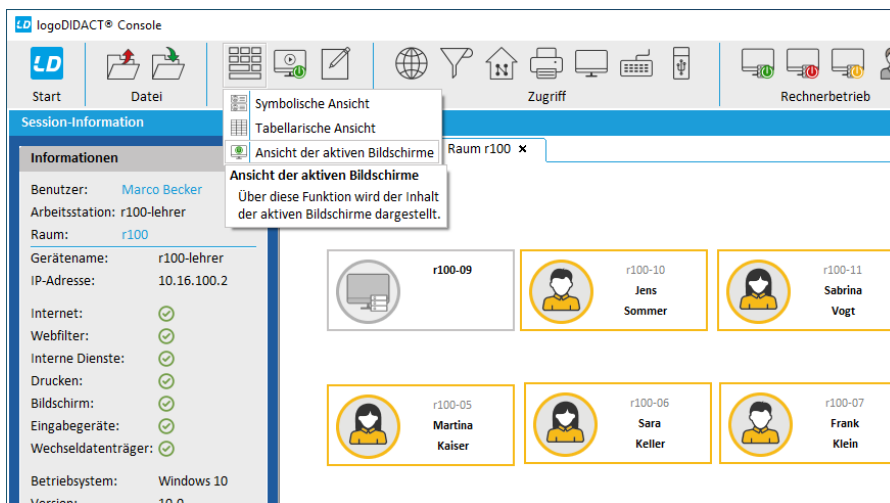
Da es neben dem Sperren des Internets viele weitere Aktionen gibt, die Sie gezielt für einzelne Schüler*innen oder Gruppen anwenden können, ist die Tabellarische Ansicht oftmals sehr hilfreich. Sie wechseln zwischen der symbolischen oder tabellarischen Darstellung über die Menüleiste und dem Symbol für Ansichten.



In der tabellarischen Ansicht lässt sich einfach erkennen, bei welchen Arbeitsstationen genau der Zugriff auf das Internet gesperrt ist.

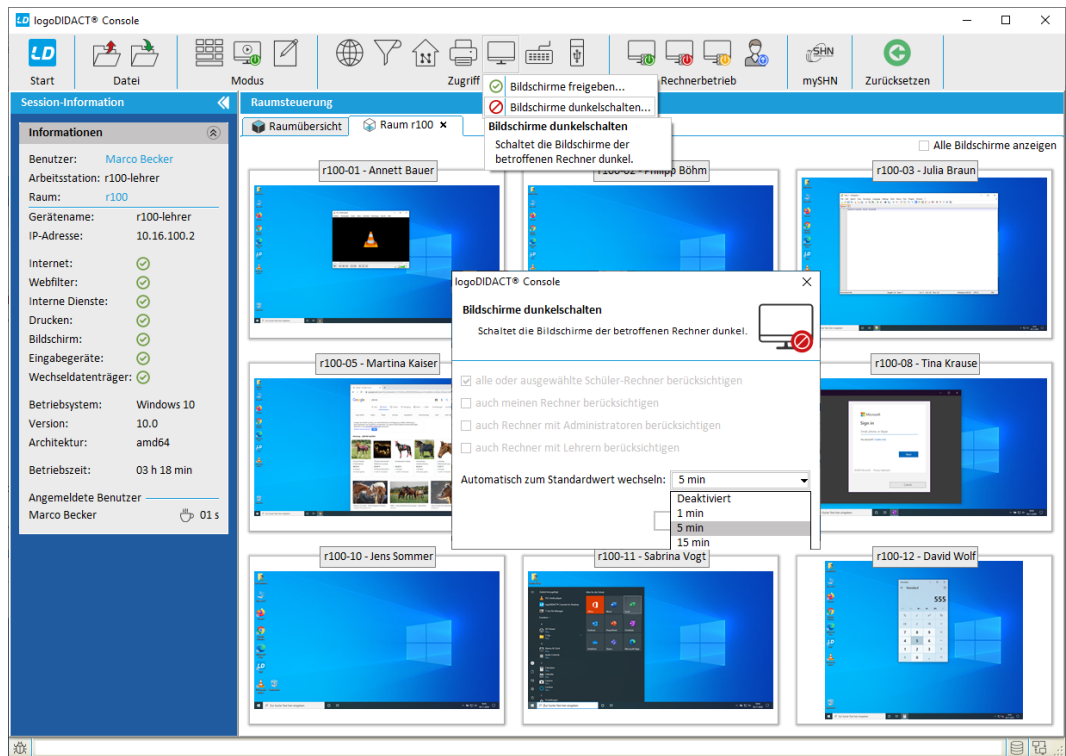
VI.2.1.2. Bildschirme sperren

Genau so hilfreich und nützlich wie das Sperren des Internetzugangs, ist das Sperren der Bildschirme, um die Aufmerksamkeit der Schüler*innen zu erreichen. Um den Effekt der Bildschirmsperre sichtbar machen zu können, wechseln Sie zunächst über das Ansichten-Symbol in der Menüleiste zur **Ansicht der aktiven Bildschirme**.

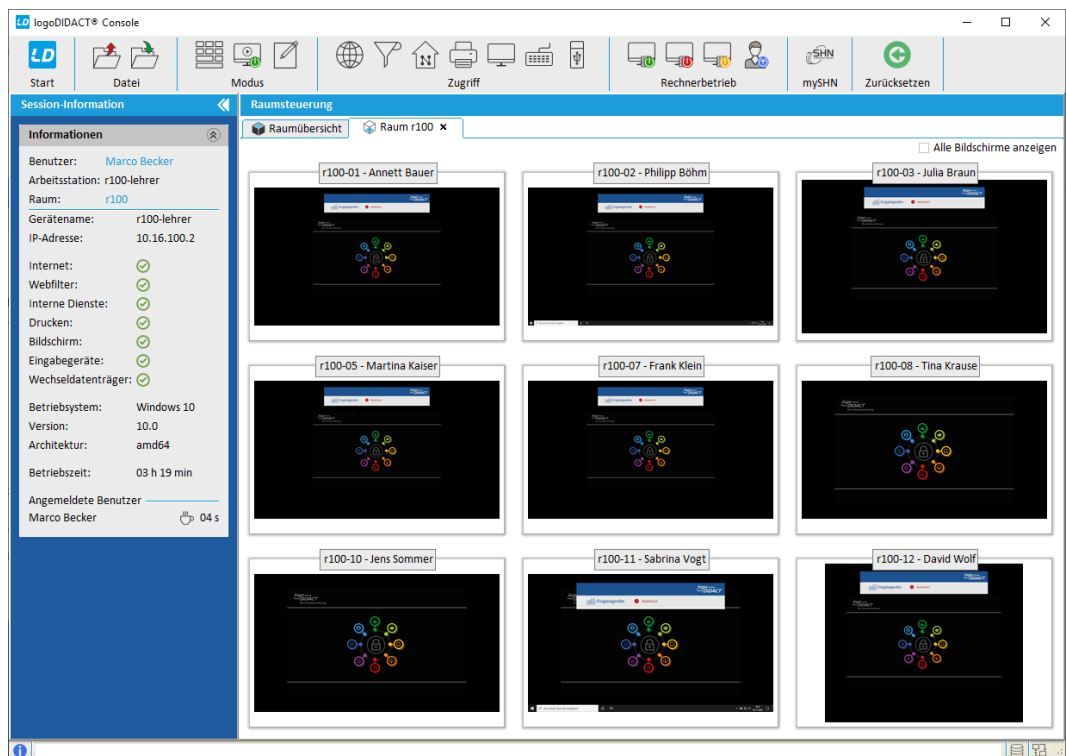


Sie sehen dann eine Miniaturansicht aller Bildschirme der Schülerinnen und Schüler. Klicken Sie anschließend in der Menüleiste auf das Monitor-Symbol und wählen dort den Eintrag **Bildschirme dunkelschalten**. Im darauf erscheinenden Dialog können Sie wieder eine Zeit angeben, die lange diese Aktion gültig und danach wieder aufgehoben werden soll.

Bildschirme sperren



Nach Bestätigung über **OK** werden alle bzw. alle ausgewählten Bildschirme gesperrt. Auch hier ist es wieder so, dass eine Meldung mit Informationen erscheint. Neben der Bildschirmsperre, die offensichtlich ist, erhalten die Schüler*innen die Rückmeldung, dass Maus und Tastatur gesperrt werden.



Unabhängig von einer eventuell gewählten Zeitdauer der Sperre, können Sie die Sperre zu jeder Zeit über den Eintrag **Bildschirme freigeben** auf dem Menü wieder aufheben.

VI.2.2. Benutzeroberfläche

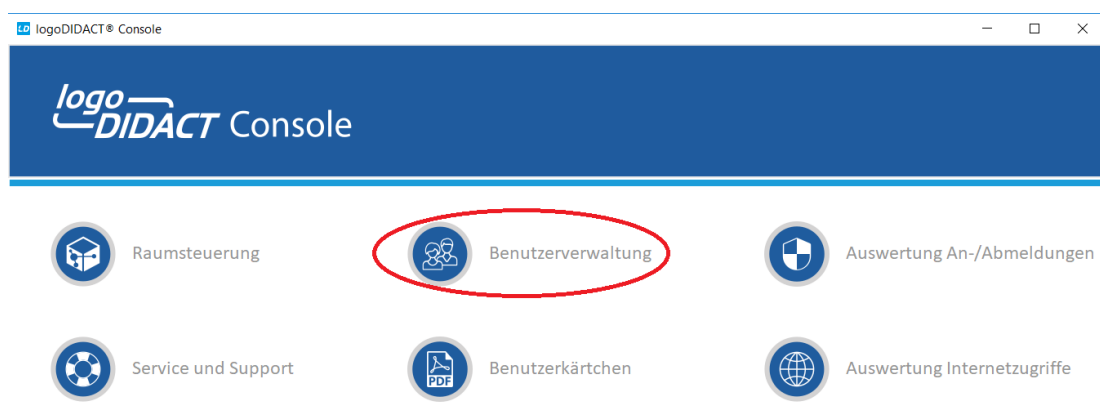
Der Aufbau der LogoDIDACT-Console ist übersichtlich gehalten und gewährleistet den schnellen Zugriff auf die unterschiedlichsten Funktionen. Sofern man in Windows mit einem Lehrer-Konto angemeldet ist, landet man beim Start der Anwendung über das Menü oder die Desktop-Icon direkt in der pädagogischen Oberfläche und ist dort ebenfalls angemeldet.

Das System erkennt automatisch an welchem Rechner man angemeldet ist und in welchem Raum man sich befindet. Im mittleren Fensterbereich der **Raumsteuerung** werden alle im Raum befindlichen Geräte angezeigt. Nicht eingeschaltete PCs sind dabei grau dargestellt, eingeschaltete Geräte blau. Sobald sich ein Benutzer anmeldet, ändert sich das Symbol und aus dem Gerät wird ein Benutzer.

Auf der linken Seite im Fensterbereich der **Session-Informationen** erhält man Informationen zu sich selbst und dem Rechner, an dem man angemeldet ist. Neben eher technische Informationen wie z.B. der IP-Adresse, werden vor allem die Stati zu den zahlreichen Funktionen angezeigt, die man über die LogoDIDACT Console steuern kann.

Im Bereich der **Raumsteuerung** gibt es neben der Registerkarte für den eigenen Raum in dem man sich befindet auch den Eintrag **Raumübersicht**. Wechselt man auf diese Anzeige, hat man einen Überblick über alle Räume und Geräte an der Schule, sowie dem Status der Rechner. Jeder Rechner wird dabei über einen kleinen Kreis symbolisiert. Dieser Kreis ist grau ausgefüllt, wenn das Gerät ausgeschaltet ist und grün, wenn es eingeschaltet ist. Sofern ein Benutzer an dem Gerät angemeldet ist, wird im grünen Kreis zusätzlich ein Buchstabe eingeblendet, der die Rolle des Benutzers anzeigt. Die Bedeutung der Buchstaben wird im unteren Bereich im Fenster **Raumübersicht** erklärt.

Über das LogoDIDACT-Symbol im linken oberen Menübereich gelangt man aus allen Modulen heraus immer zum zentralen Hauptmenü, um von dort zu den jeweiligen Modulen zu gelangen. Abhängig von der Rolle, die man im System hat, hat man damit verbundene Rechte und kann spezielle Module nutzen oder auch nicht. Durch die Rollenverteilung werden insbesondere auch datenschutzrechtliche Vorgaben sauber und rechtssicher abgebildet.



Über den Eintrag **Benutzerverwaltung** gelangen Sie zum gleichnamigen Modul.

Die Symbolleiste unterhalb des Menüs bietet, zusätzlich zum Kontextmenü über die rechte Maustaste, ebenfalls schnellen Zugriff auf wichtige Funktionen. Die Symbole stehen von links nach rechts für die Funktionen der Raumsteuerung bzw. Benutzerverwaltung.

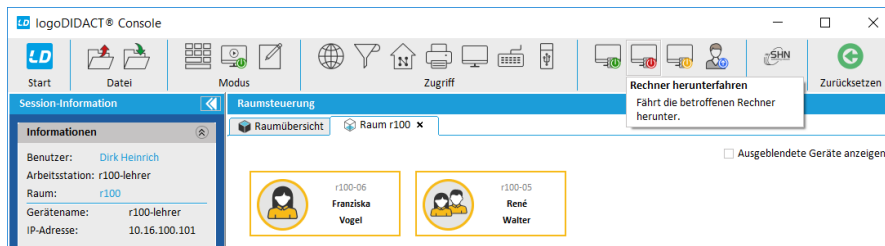


Abbildung VI.2.1. Rechnerbetrieb steuern (über Symbolleiste)

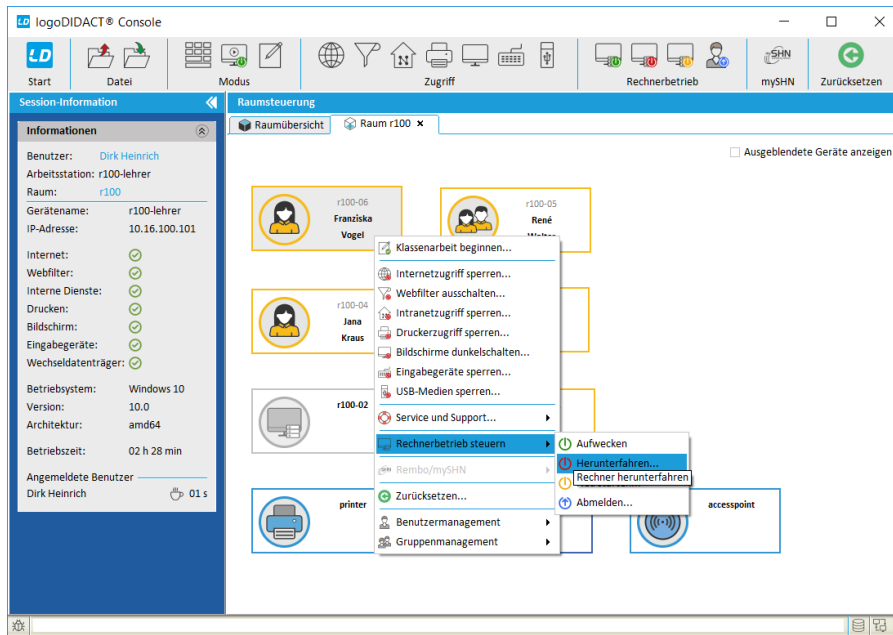


Abbildung VI.2.2. Rechnerbetrieb steuern (über Kontextmenü)

Im zentralen Teil der Benutzeroberfläche befindet sich auf der linken Seite ein Bereich mit „Session-information“. Auf der rechten Seite wird bei Auswahl über das Menü „Ansicht“ die Raumsteuerung bzw. Benutzerverwaltung angezeigt.

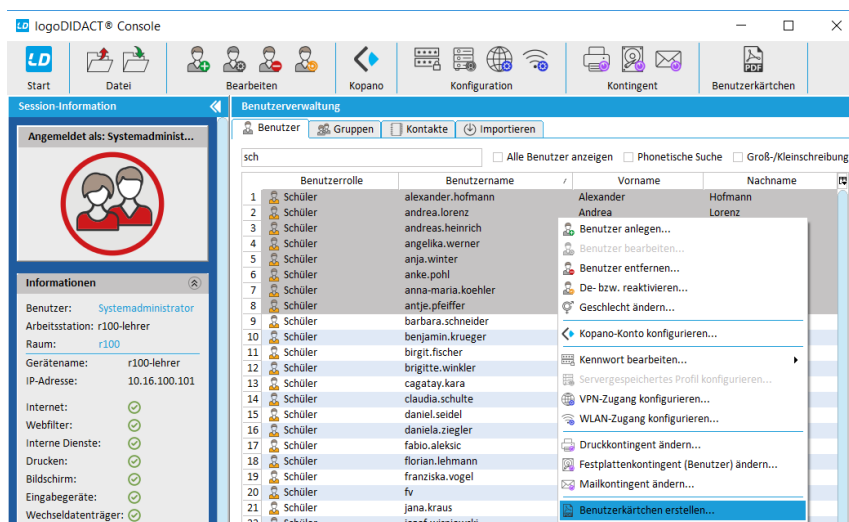


Abbildung VI.2.3. Benutzerverwaltung der LogoDIDACT-Console

Einige Funktionen, die nicht über die Symbolleiste zur Verfügung stehen, können auch über das Kontextmenü heraus angesteuert werden. Über die rechte Maustaste lässt sich für die meisten Objekte ein Kontextmenü mit entsprechenden Menüeinträgen öffnen.

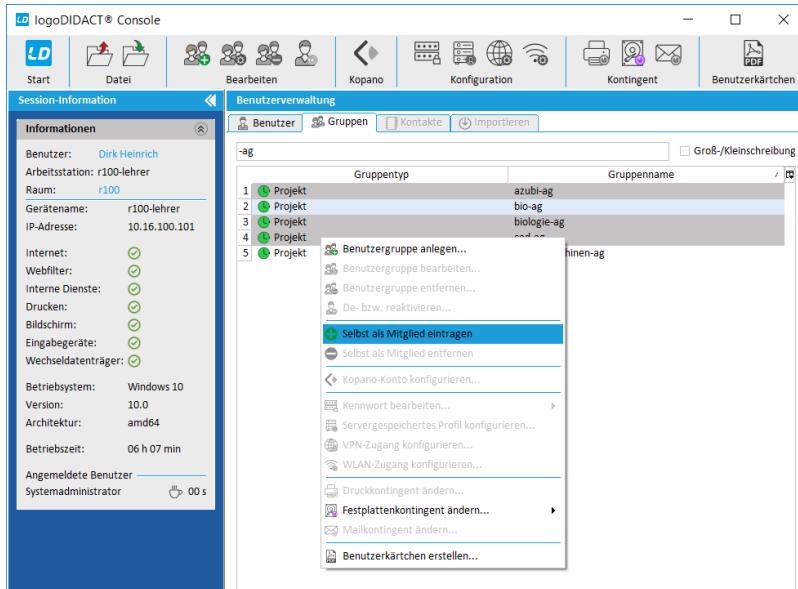


Abbildung VI.2.4. Mitglied einer Benutzergruppe werden (über Kontextmenü)

Die Statusleiste am unteren Rand zeigt unter Umständen bestimmte Statusinformationen wie „Lese Benutzer ein...“ oder Ähnliches an.

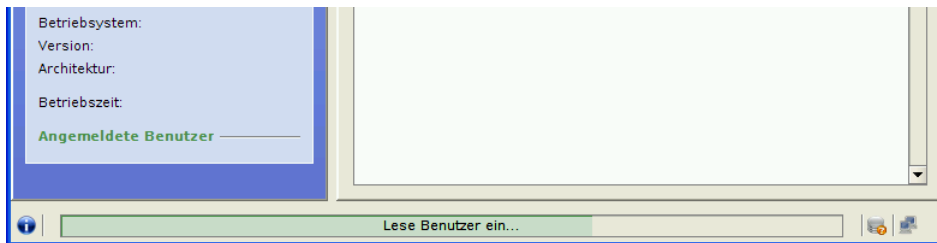


Abbildung VI.2.5. Statusinformationen der LogoDIDACT-Console

VI.2.3. Raumsteuerung

Beim Starten der LogoDIDACT-Console wird standardmäßig die Ansicht der Raumsteuerung aufgerufen und der aktuelle Raum, in dem sich der Anwender befindet, in einer neuen Registerkarte angezeigt.

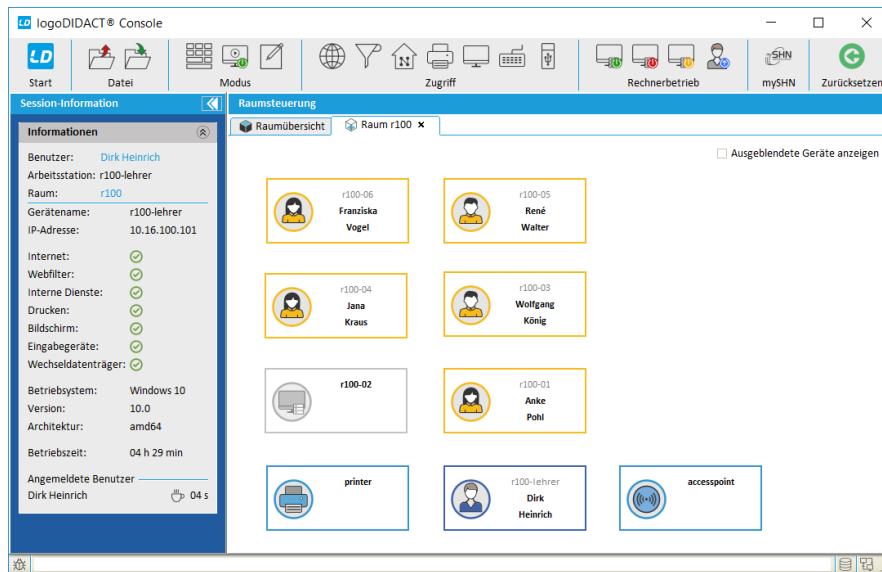



Abbildung VI.2.6. Raumsteuerung der LogoDIDACT-Console



Tipp

Per Rechtsklick lässt sich ein Kontextmenü öffnen und die Anordnung der Symbole im Raum verändern („Layout ändern/speichern“). Über die Tasten +/- kann die Rechnerdarstellung individuell skaliert werden. Diese Funktionen sind jedoch allein den Systemadministratoren vorbehalten.

Über die Registerkarte „Raumübersicht“ kann der Raum jederzeit über Doppelklick auf einen der Einträge in der Tabelle gewechselt werden.

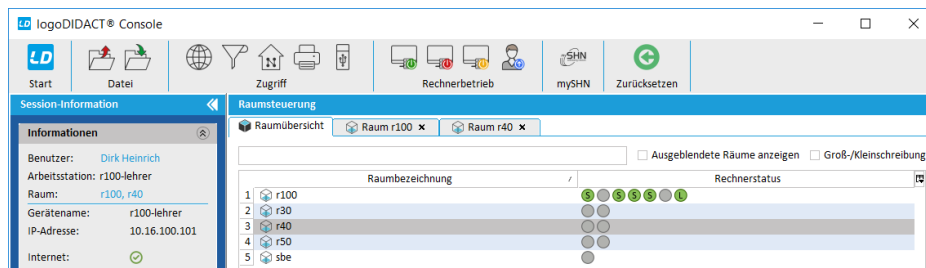
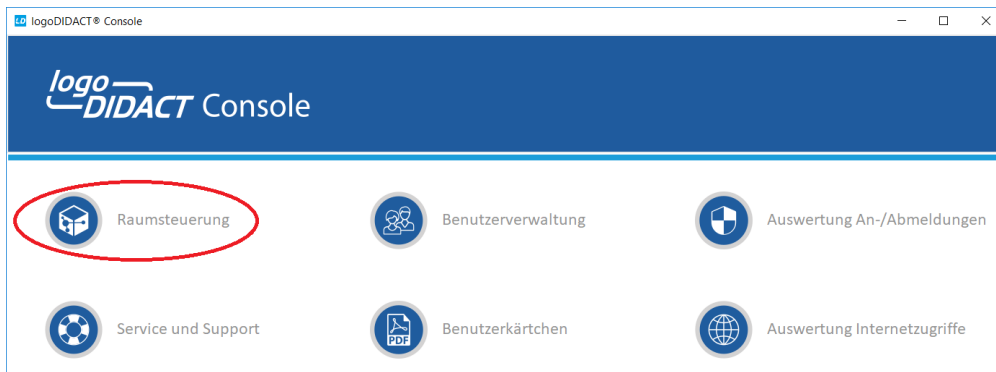


Abbildung VI.2.7. Raumübersicht der LogoDIDACT-Console

Die Raumsteuerung der LogoDIDACT-Console lässt sich immer über den Eintrag Start links oben in der Symbolleiste erreichen.



VI.2.3.1. Austeilen und Einsammeln von Dateien

Über den Eintrag „Dateiexplorer anzeigen“ in der Symbolleiste und im Menü „Datei“ wird ein Dateiexplorer, ähnlich dem Windows-Explorer, zum Auswählen der auszuteilenden Dateien bereitgestellt.

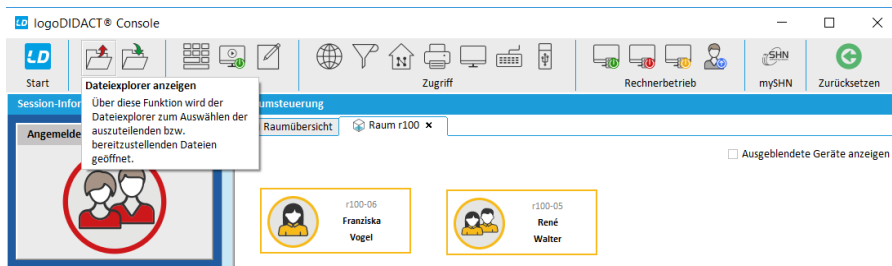


Abbildung VI.2.8. Dateiexplorer anzeigen (über Menü „Datei“)

Der Dateiexplorer ermöglicht das Navigieren und Auswählen der auszuteilenden Dateien und Verzeichnisstrukturen direkt aus der LogoDIDACT-Console heraus.

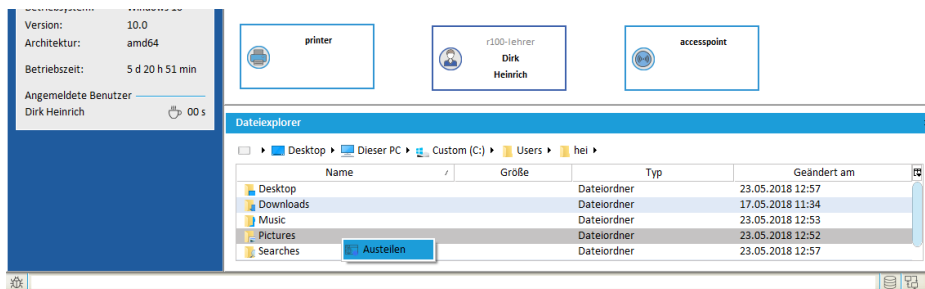


Abbildung VI.2.9. Dateiexplorer der LogoDIDACT-Console

Die auszuteilenden Dateien lassen sich per Drag-and-Drop in den Raum bzw. auf die ausgewählten Benutzer ziehen oder über das Kontextmenü der rechten Maustaste austeilen.

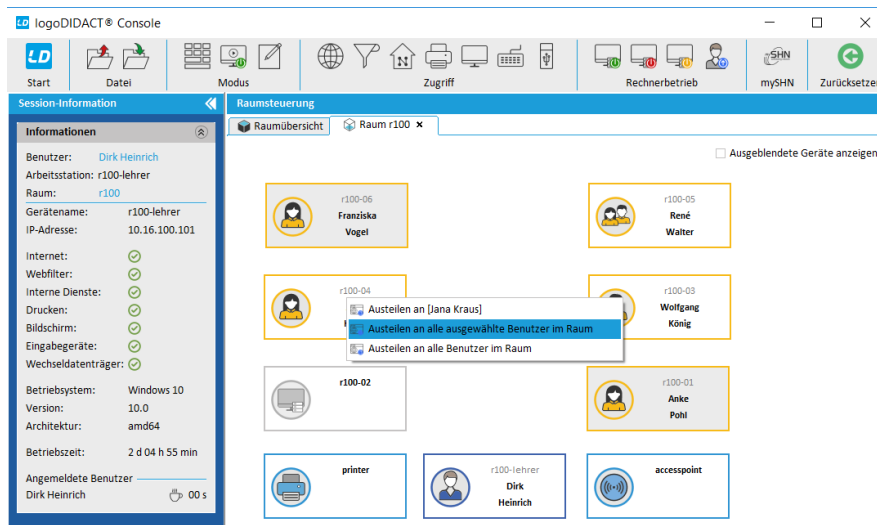


Abbildung VI.2.10. Dateien austeilen (per Drag-and-Drop)

Über den Eintrag „Austeilen/Bereitstellen...“ im Kontextmenü wird ein zusätzlicher Dialog geöffnet, über den sich alle Benutzer im System ansprechen lassen (dazu die Option „Alle Klassen und Projekte anzeigen“ im unteren Teil des Dialogs aktivieren).

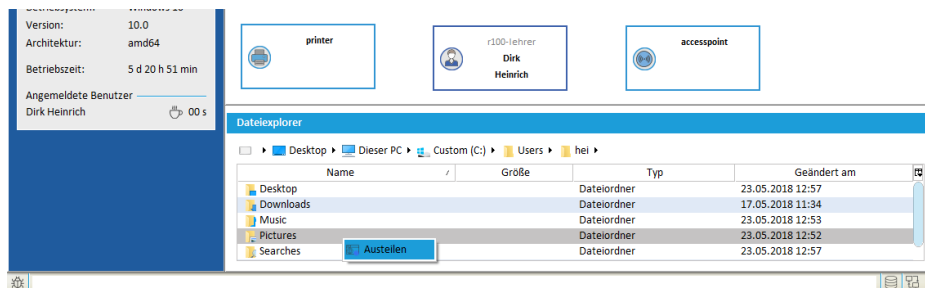


Abbildung VI.2.11. Dateien austeilen (über Kontextmenü)

Tipp

Lehrer und Systemadministratoren, die Mitglieder in Benutzergruppen sind, können aus deren Mitgliedern wählen, ohne die Option „Alle Klassen und Projekte anzeigen“ vorher zu aktivieren.

Die ausgeteilten Dateien finden sich anschließend in den Eigenen Dateien der ausgewählten Benutzer im Verzeichnis `H:_Ausgeteilt_` wieder.

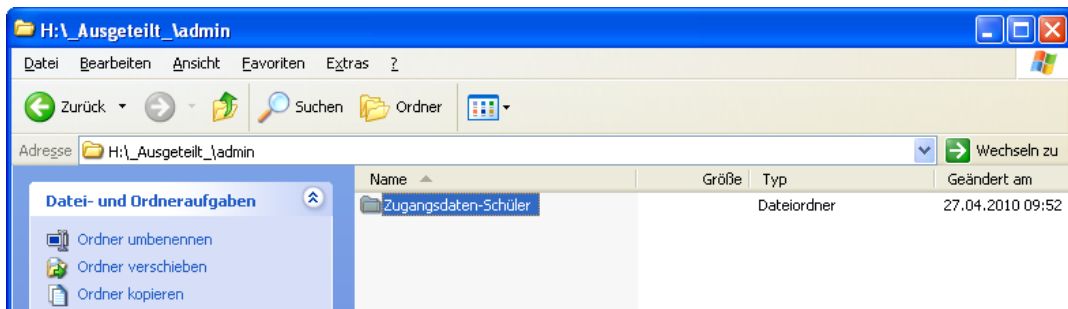


Abbildung VI.2.12. Ausgeteilte Dateien in den Eigenen Dateien

Für das Einsammeln von Dateien gelten vergleichbare Schritte. Alle Benutzer haben in den Eigenen Dateien ein Verzeichnis H:_Einsammeln_, in dem einzusammelnde Dateien abzulegen sind.

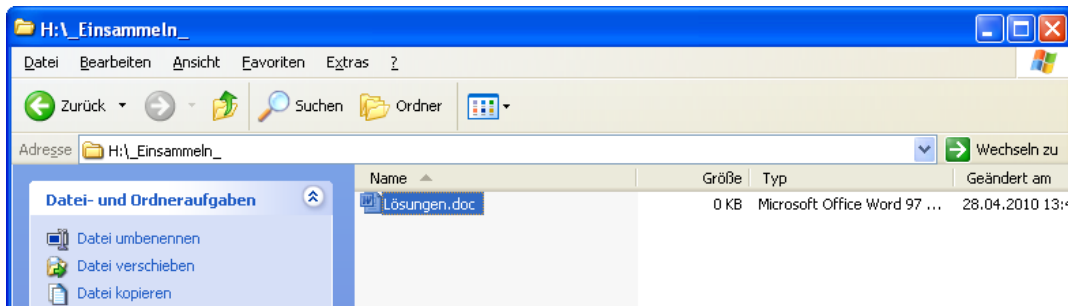


Abbildung VI.2.13. Einzusammelnde Dateien in den Eigenen Dateien

Über den Eintrag „Einsammeln von Dateien“ in der Symbolleiste und im Menü „Datei“ wird der dazugehörige Dialog aufgerufen.

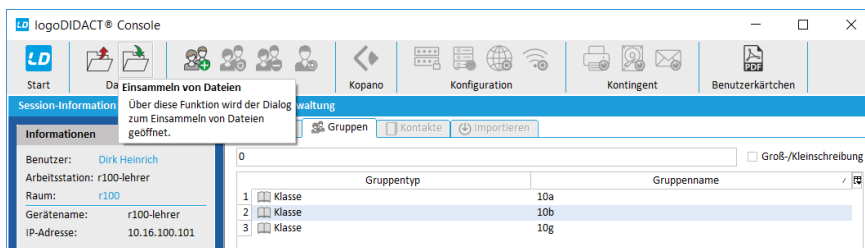


Abbildung VI.2.14. Einsammeln von Dateien (über Symbolleiste)

Der Aufbau ähnelt dem Dialog zum Austeilen von Dateien. Einzig die Option „Dateien nach dem Einsammeln löschen“ am unteren Rand ist zu beachten.

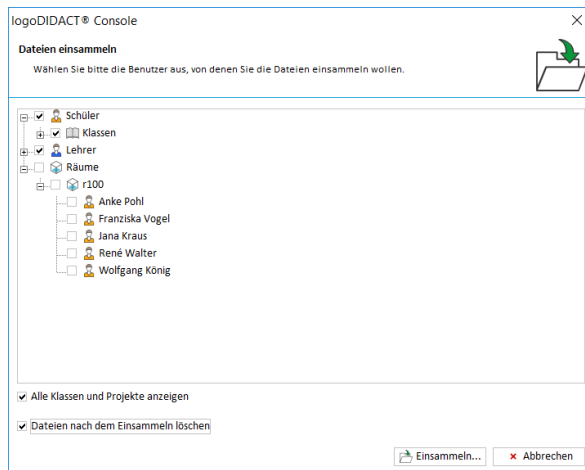


Abbildung VI.2.15. Dialog zum Einsammeln von Dateien

Die eingesammelten Dateien der ausgewählten Benutzer findet der Anwender anschließend bei sich in den Eigenen Dateien im Verzeichnis H:_Eingesammelt_ wieder.

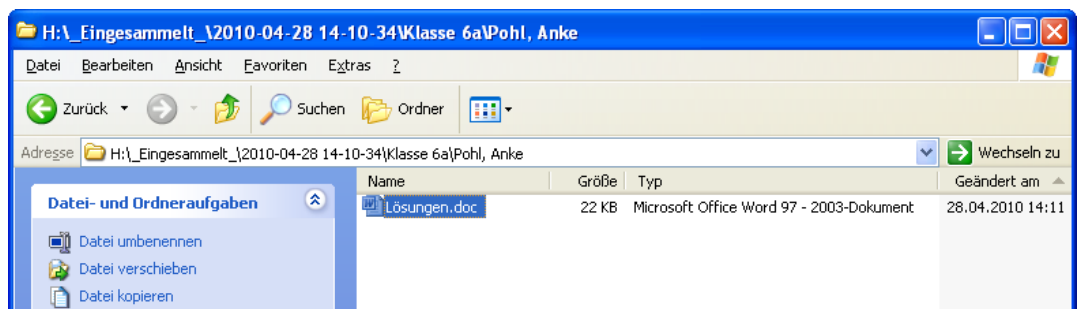


Abbildung VI.2.16. Eingesammelte Dateien in den Eigenen Dateien

VI.2.3.2. Bildschirmübertragung



Achtung

Lehrer und Systemadministratoren sind von der Bildschirmübertragung ausgenommen und können über die LogoDIDACT-Console nicht eingesehen werden.

Über den Eintrag „Überwachungsmodus ändern“ → „Ansicht der Bildschirme“ in der Symbolleiste, Kontextmenü und im Menü „Ansicht“ wird eine Übersicht der Bildschirminhalte für den aktuellen Raum bereitgestellt.

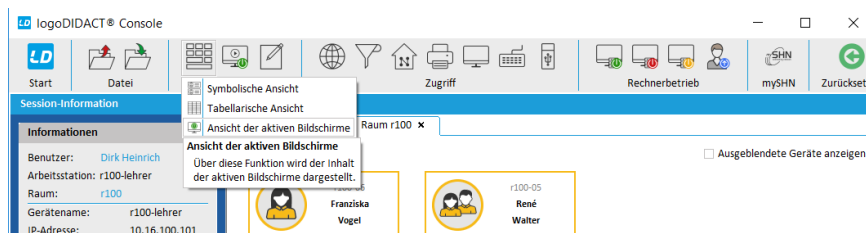


Abbildung VI.2.17. Ansicht der Bildschirme (über Symbolleiste)

Über den Eintrag „Überwachungsmodus ändern“ → „Symbolische Ansicht“ kann jederzeit wieder in die „gewohnte“ Ansicht der Raumsteuerung gewechselt werden.

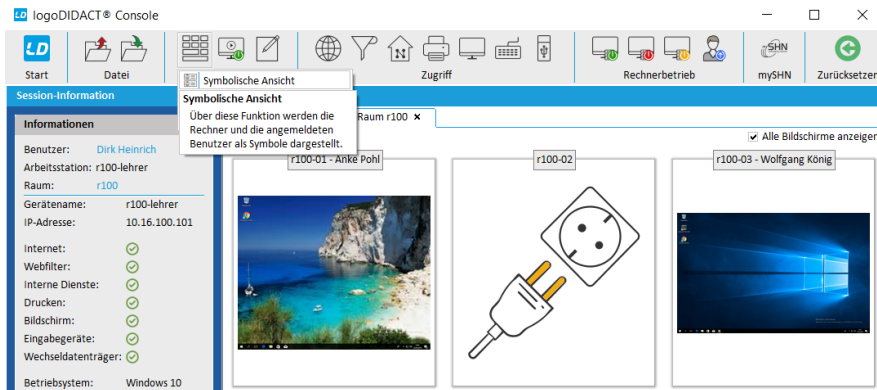


Abbildung VI.2.18. Symbolische Ansicht (über Symbolleiste)

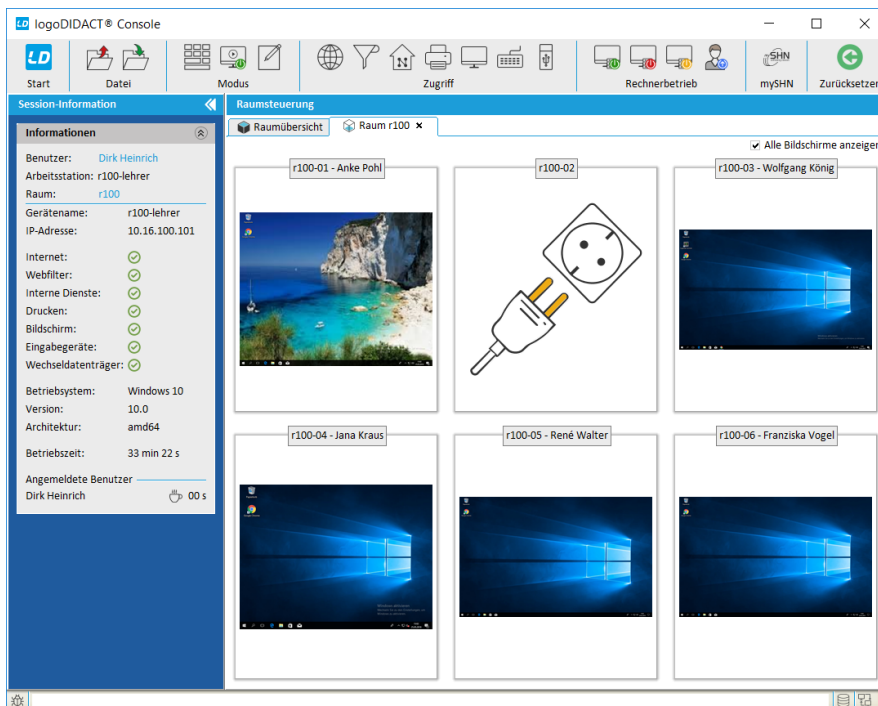


Abbildung VI.2.19. Bildschirmübertragung der LogoDIDACT-Console

Die Vorschau-Ansicht der Bildübertragung kann für einen ausgewählten Rechner über das Symbol für Maximieren auf die Höhe und Breite der Raumsteuerung vergrößert werden.

Über das „Augenpaar“ wird die reine Bildschirmübertragung in einem neuen Fenster geöffnet. Die Bildschirm Inhalte mehrerer Rechner lassen sich auf diese Weise im Vollbildmodus betrachten.

Das Symbol mit dem „Steuerknüppel“ startet die Bildschirmübertragung mit voller Rechnerkontrolle und ermöglicht das Fernsteuern der ausgewählten Rechner.

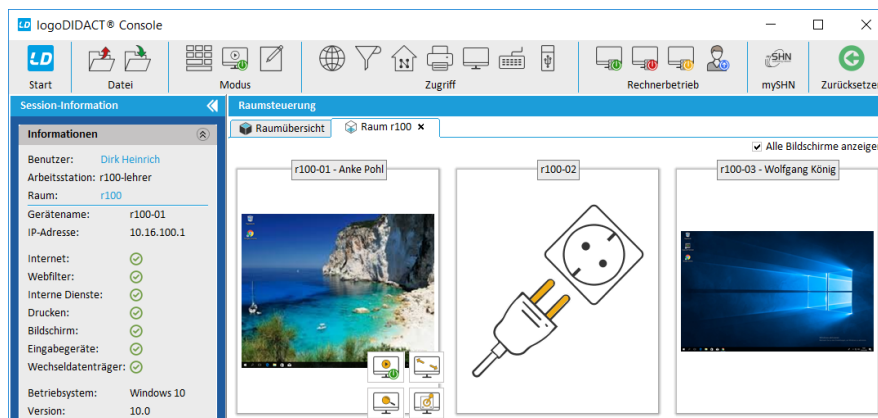


Abbildung VI.2.20. Steuerelemente der Bildschirmübertragung

VI.2.3.3. Klassenarbeitsmodus

VI.2.3.3.1. Klassenarbeit starten und beenden

Über den Eintrag „Klassenarbeitsmodus“ in der Symbolleiste und im Kontextmenü kann für den aktuellen Raum bzw. ausgewählte Rechner eine Klassenarbeit gestartet werden.



Achtung

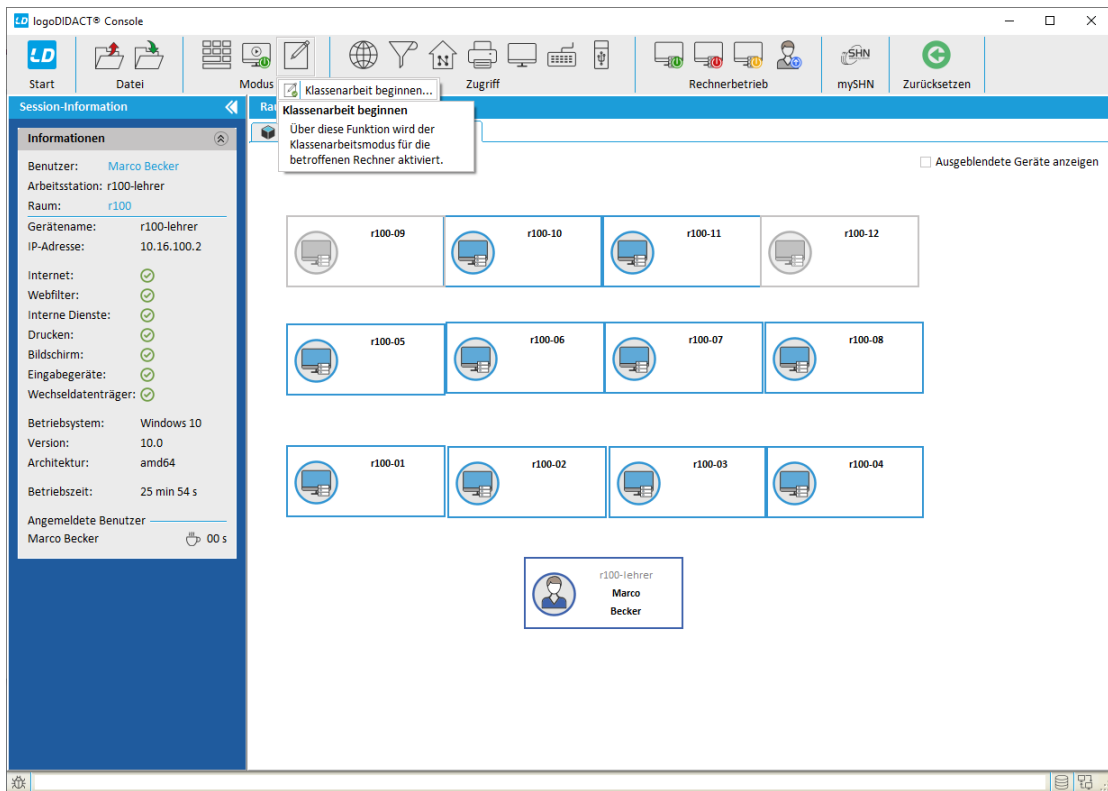
Bitte beachten Sie folgende Punkte:

- Die Schüler sollten sich erst an den Rechnern anmelden, nachdem Sie den Klassenarbeitsmodus gestartet haben.
- Für die Klassenarbeit melden sich die Schüler*innen mit ihren gewohnten Zugangsdaten an.

Warum dies problemlos möglich ist, selbst wenn Schüler ihre Kennwörter vorab untereinander austauschen sollten, steht in Abschnitt VI.2.3.3.4. „Sicherheit im Klassenarbeitsmodus“)

- Schüler, die sich an den ausgewählten Arbeitsstationen anmelden, nehmen dann automatisch an der Klassenarbeit teil.
- Die Farbe der Symbole ändert sich im Klassenarbeitsmodus von gelb auf grün.

Um als Lehrer*in eine Klassenarbeit im gesamten Raum zu starten, klicken Sie in der Menüleiste auf das Symbol für Klassenarbeiten und dann auf den Eintrag dort den **Klassenarbeit beginnen**.



Im darauf folgenden Dialog müssen Sie lediglich einen Namen für die Klassenarbeit im Feld **Bezeichnung** eingeben.

Tipp

Über den Eintrag **Suchen...** können Sie eine zuvor angelegte Klassenarbeit auswählen und starten. Infos zur Vorbereitung einer Klassenarbeit, finden Sie in Abschnitt VI.2.3.3.3, „Eine Klassenarbeit vorbereiten“)

Wenn keine umfangreichen Vorbereitungen notwendig sind, können Sie die Klassenarbeit auch direkt starten.

Je nach Art der Klassenarbeit können bestimmte technische Funktionen deaktiviert oder zugelassen werden. Es ist sicherlich selbsterklärend, dass das Tauschen von Dokumenten während einer Klassenarbeit grundsätzlich nicht gewünscht wird, zumindest nicht aus Sicht der Lehrer*innen. Für eine Klassenarbeit, die aber die Recherche im Internet mit einschließt, muss das Häkchen bei **Zugriff auf Internet sperren** logischerweise entfernt werden.

logoDIDACT® Console

Klassenarbeit

Alle Schüler, die sich an den betroffenen Arbeitsstationen anmelden, nehmen automatisch an dieser Klassenarbeit teil.

Bezeichnung: Mathearbeit-6a - 2020-06-15 Suchen...

Räume: r100 Ändern...

Geräte: r100-02 Ändern...

Automatisch beenden: Deaktiviert

Initialer Status der Rech: Deaktiviert

Zugriff auf Internet 45 min

Zugriff auf interne Webdienste sperren

Zugriff auf Tauschlaufwerke sperren

Zugriff auf Drucker sperren

Zugriff auf USB-Laufwerke sperren

Aktionen vor dem Beginn

Keine

Rechner neustarten

⚠ Rechner werden ohne Nachfrage sofort neu gestartet.

OK Abbrechen

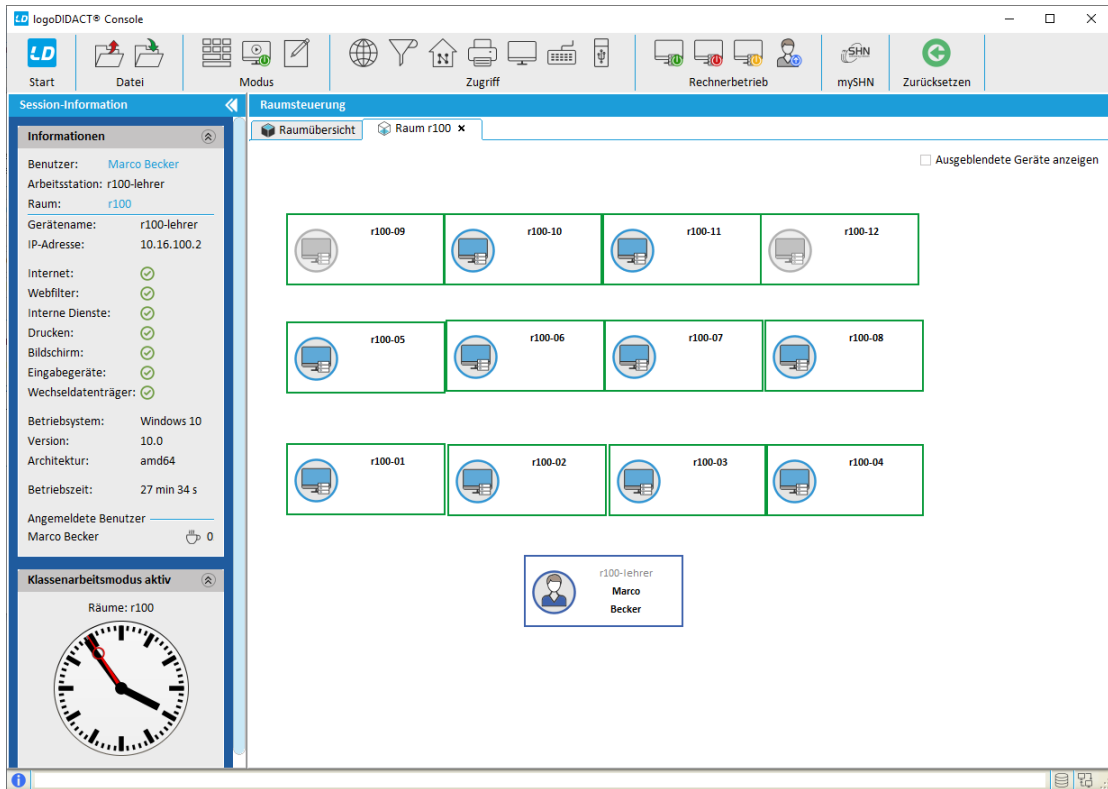


Achtung

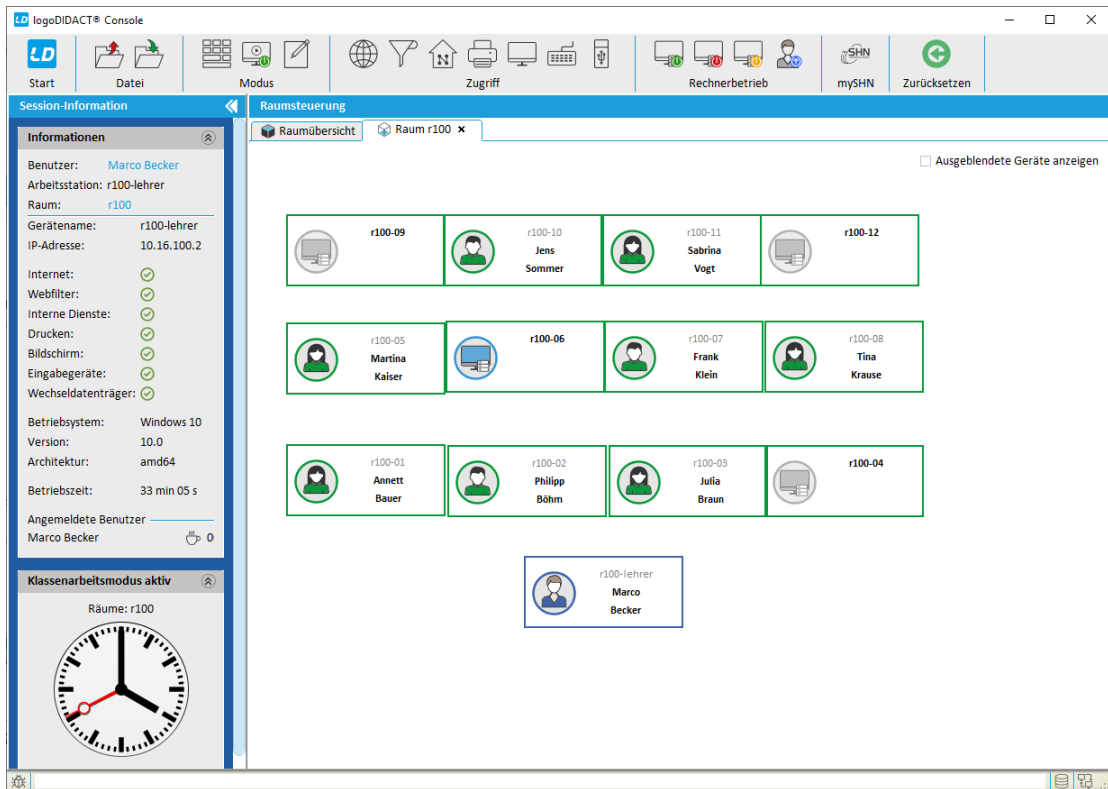
Verwenden Sie die Funktion **Automatisch beenden** mit äußerster Vorsicht, denn die Arbeit wird in diesem Fall auf technischem Wege beendet.

Dabei wird dann nicht der Zustand einer Arbeit eingesammelt, der von einem Schüler gerade noch live bearbeitet wird oder vor 30 Sekunden eingetippt wurde, sondern derjenige, der zuletzt auf Dateiebene im Dokument abgespeichert wurde.


Nach dem Start einer Klassenarbeit, werden die Rechner in den Klassenarbeitsmodus versetzt. Dies ist an den Rechner- und auch Benutzersymbolen durch Änderung der Symbolfarbe von gelb auf grün erkennbar. Ebenfalls wird im Klassenarbeitsmodus auf der linken Seite der LogoDIDACT-Console deutlich erkennbar eine Uhr eingeblendet.



Nachdem der Klassenarbeitsmodus gestartet wurde, können sich die Schüler*innen mit ihren gewohnten Benutzerdaten anmelden.



Über das Symbol für Klassenarbeiten in der Menüleiste und den Eintrag **Klassenarbeit beenden** lässt sich eine Klassenarbeit zu jeder Zeit beenden.

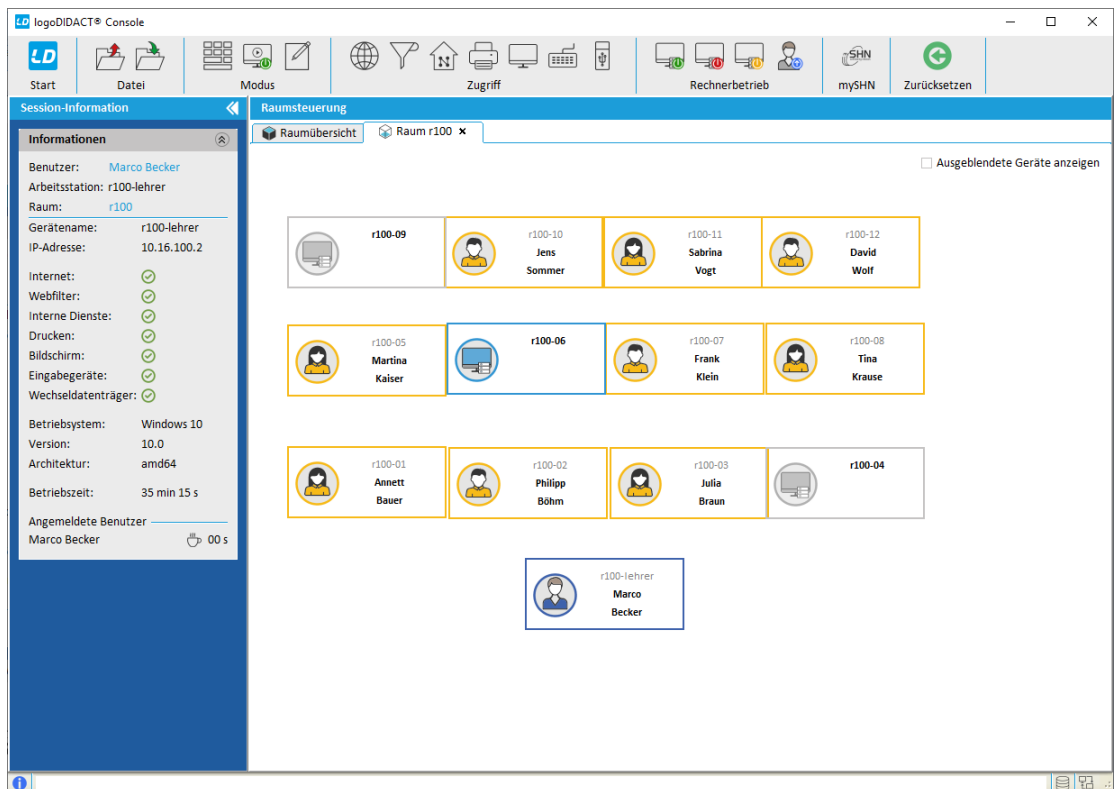


Achtung

Bitte fordern Sie die Schüler*innen vor dem Beenden der Klassenarbeit dazu auf, die Dokumente zu speichern und die für die Klassenarbeit verwendeten Programme zu schließen.

Weisen Sie die Schüler*innen drauf hin, dass nur der im Dokument zuletzt abgespeicherte Zustand für die Bewertung der Arbeit maßgeblich ist!

Nachdem der Klassenarbeitsmodus beendet wurde, wechselt die Farbe der Symbole wieder auf gelb und die Uhr in der LogoDIDACT Console verschwindet.



VI.2.3.3.2. Ergebnisse der Klassenarbeit "einsammeln"

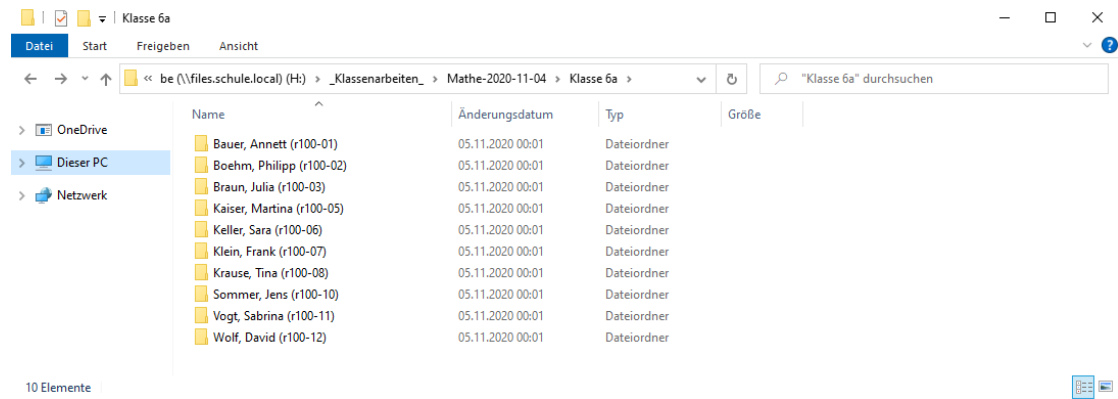
Im Gegensatz zur Funktion Austeilen und Einsammeln von Dokumenten, wo Dateien auf Serverseite tatsächlich zwischen Ordnern hin- und herkopiert werden, funktioniert der Klassenarbeitsmodus komplett anders.

Der entscheidende Unterschied besteht darin, dass im Klassenarbeitsmodus das Einsammeln der Arbeiten entfällt!

Die Homeverzeichnisse der teilnehmenden Schüler finden die Lehrer*innen während und nach der Klassenarbeit bei sich im eigenen Homelaufwerk. In Anlehnung an den festgelegten Namen der Klassenarbeit wird dort eine Ordnerstruktur erstellt, die automatisch um den Namen der Klasse und der Schüler*innen, sowie den Rechnern an dem sie arbeiten ergänzt wird:

H:_Klassenarbeiten_\[Klassenarbeit]\[Klasse]\[Nachname, Vorname (Rechnername)]

Dies ist in folgender Abbildung beispielhaft dargestellt, wobei das Kürzel **be** für den Lehrer **Marco Becker** steht, in dessen Homeverzeichnis und H:\ sich die oben genannte Struktur abbildet:




VI.2.3.3.3. Eine Klassenarbeit vorbereiten

Im Abschnitt VI.2.3.3.1, „Klassenarbeit starten und beenden“) wird gezeigt, wie eine Klassenarbeit live ohne vorherige Vorbereitung angelegt wird und was es dabei im Hinblick auf die Anmeldung von Schülern zu beachten gilt.

Gezeigt wird in den vorherigen Abschnitten auch, dass beim Starten einer Klassenarbeit eine Dateistruktur erstellt wird und wie diese Dateistruktur aussieht.

Beim Vorbereiten einer Klassenarbeit geht es konkret darum, den Schülern Aufgaben oder Dokumente in Form von Dateien bereitzustellen und diese nicht erst live während der Klassenarbeit verteilen zu müssen.

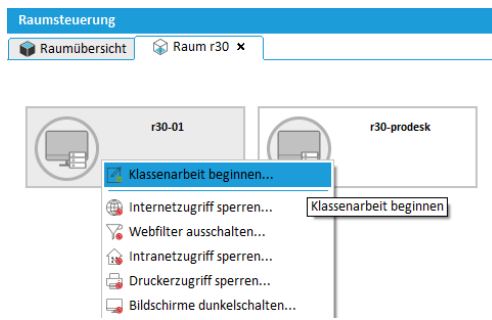
Ob das nun "die Klassenarbeit" als zu bearbeitende Word- oder Excel-Datei ist oder PDF-Dateien mit zusätzlichen Informationen ist unerheblich. Wichtig ist nur, dass diese Dokumente bereits vorher in den richtigen Ordner gelegt werden können.



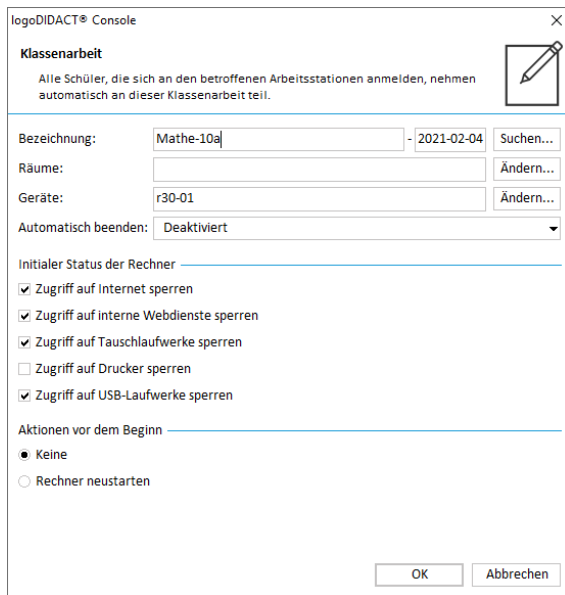
Achtung

Bei der Vorbereitung einer Klassenarbeit besteht der entscheidende Schritt darin, dass die Dateistruktur dafür aufgebaut wird. Das passiert dadurch, dass sie mindestens einen Rechner in den Klassenarbeitsmodus versetzen, den Namen der Klassenarbeit eingeben, die Klassenarbeit starten und unmittelbar danach sofort wieder beenden.

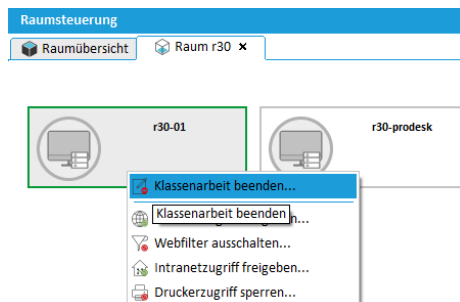
Zum Start dieser "virtuellen" Klassenarbeit wählen Sie am besten einen Rechner, der ausgeschaltet ist. Versetzen Sie nur diesen einen Rechner über das Kontextmenü in den Klassenarbeitsmodus durch die Auswahl des Menüeintrags **Klassenarbeit beginnen....**



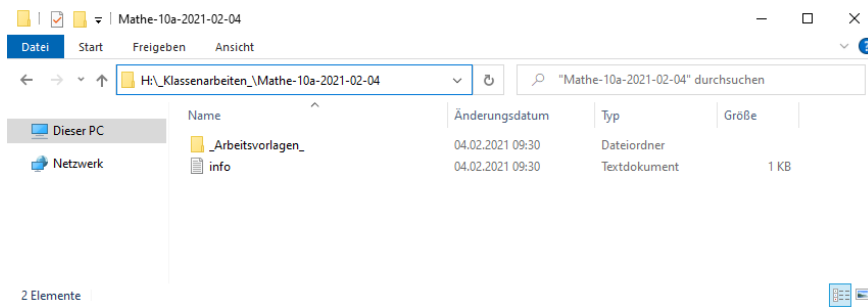
Vergeben Sie einen sinnvollen Namen und starten die Arbeit über die Schaltfläche **OK**.



Nachdem der Rechner sichtbar in den Klassenarbeitsmodus gewechselt ist, beenden Sie den Modus über das Kontextmenü sofort wieder.

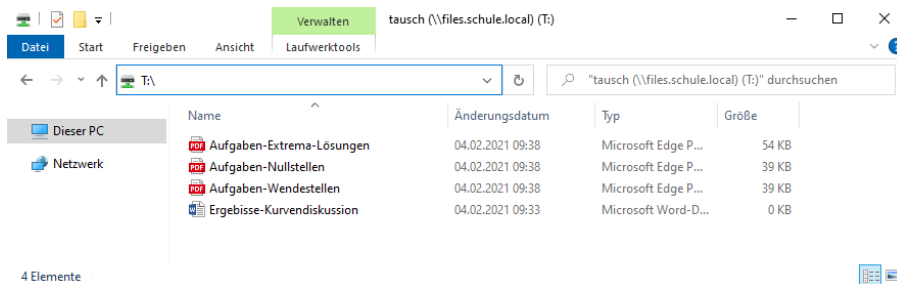


Danach finden Sie die entsprechende Datei-Struktur in Ihrem Home-Laufwerk.



Alle Dokumente die Sie für die Klassenarbeit vorbereitend ablegen wollen, kopieren Sie in den Ordner `H:_Klassenarbeiten_\[Klassenarbeit]_Arbeitsvorlagen_`. Im Beispiel sieht der Pfad für diese Dokumente wie folgt aus:

Dieses Verzeichnis `_Arbeitsvorlagen_` wird den an der Klassenarbeit teilnehmenden Schülern dann im Tauschlaufwerk `T:\` bereitgestellt:



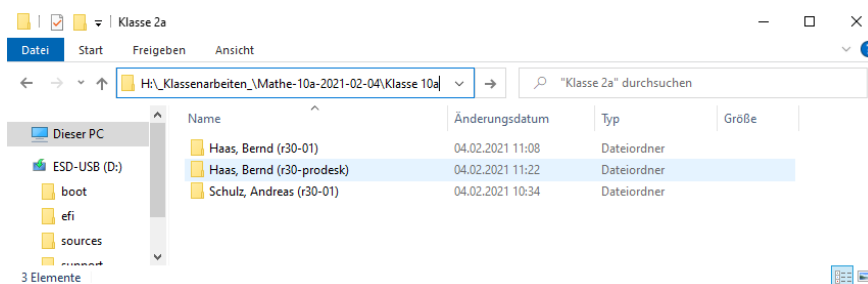
VI.2.3.3.4. Sicherheit im Klassenarbeitsmodus

Die Anmeldung der Schüler erfolgt auch im Klassenarbeitsmodus mit den bekannten individuellen Zugangsdaten, bestehend aus Anmeldenamen und Kennwort.

Sollten nun Schüler auf die Idee kommen, ihre Kennwörter im Vorfeld auszutauschen, um sich während der Klassenarbeit kurz unter anderem Namen anzumelden und Ergebnisse abzugleichen und "abzuschreiben", so ist dies technisch gar nicht möglich.

Wenn sich die Schüler an einem Rechner anmelden, der sich im Klassenarbeitsmodus befindet, wird dynamisch ein Ordner angelegt, der für den Schüler während der Klassenarbeit als Laufwerk `H:\` sichtbar ist.

In der Dateistruktur im Verzeichnis des Lehrers beinhaltet dieser Ordnername aber sowohl den Namen des Schülers, als auch den Namen des Rechners, an dem er sich während der Klassenarbeit angemeldet hat.



Wie aus der Grafik ersichtlich ist, lässt sich der Betrugsversuch sogar nachweisen und ebenso die daran beteiligten Personen. Viel wichtiger ist aber, dass Schüler A zu keinem Zeitpunkt auf die Dateien und Ergebnisse von Schüler B zugreifen, wenn er dessen Kennwort kennt und sich damit anmeldet.

VI.2.3.4. Didaktische Funktionen

In der Symbolleiste und im Kontextmenü finden sich weitere interessante Funktionen, die den Zugriff auf Internet, Webfilter, Intranet, Drucker, Eingabegeräte und Wechseldatenträger sowie Bildschirmdunkelschaltung und Rechnerbetrieb steuern.



Achtung

Lehrer, die sich an der LogoDIDACT-Console anmelden, werden sicher festgestellt haben, dass einige der Funktionen für den Anwender „ausgegraut“ erscheinen. Diese sind allein den Systemadministratoren vorbehalten.



Tipp

Mit dem Ausdruck „Interne Dienste“ sind die Einträge Intranet, Moodle, Webmail, Raumbelegung, Drucker und ITB Panel in der Lesezeichen-Symbolleiste des Mozilla Firefox gemeint.

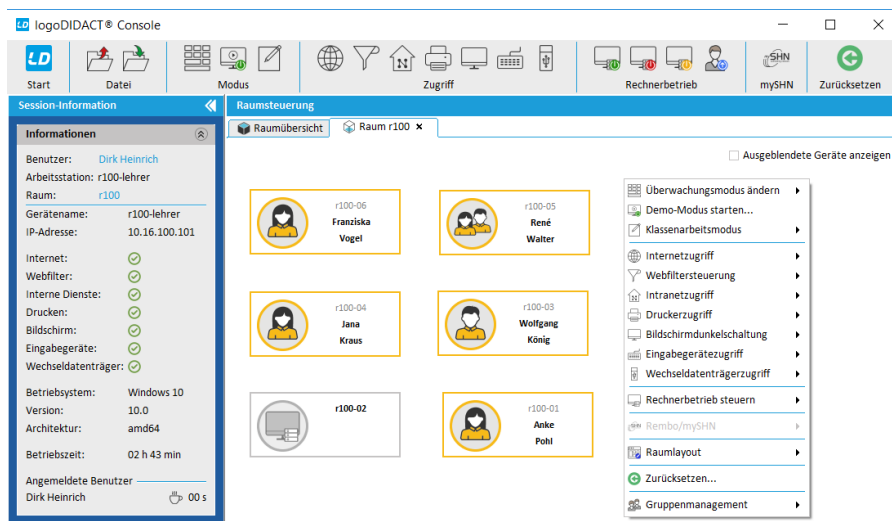


Abbildung VI.2.21. Didaktische Funktionen der LogoDIDACT-Console

Wenn sich Benutzer im Raum anmelden, können einige Funktionen der Benutzerverwaltung auch über den Eintrag „Benutzermanagement“ im Kontextmenü aufgerufen werden.

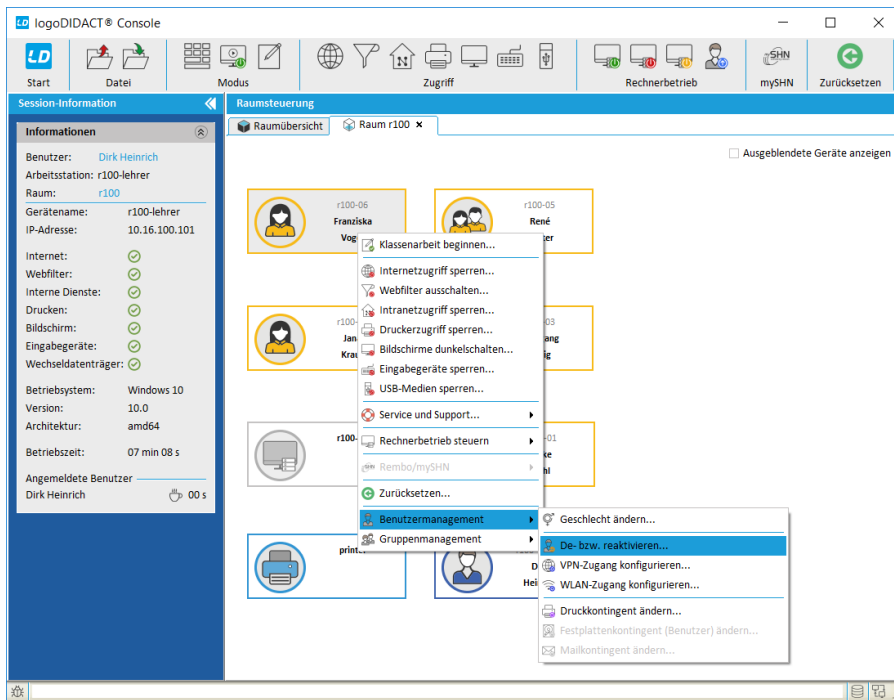


Abbildung VI.2.22. Funktionen der Benutzerverwaltung (über Kontextmenü)

Bevor die Funktionen ausgeführt werden, öffnet sich ein dazugehöriger Dialog, über den sich noch einige Einstellungen vornehmen lassen.

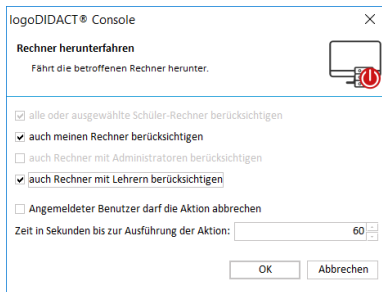


Abbildung VI.2.23. Rechner herunterfahren (Konfiguration)

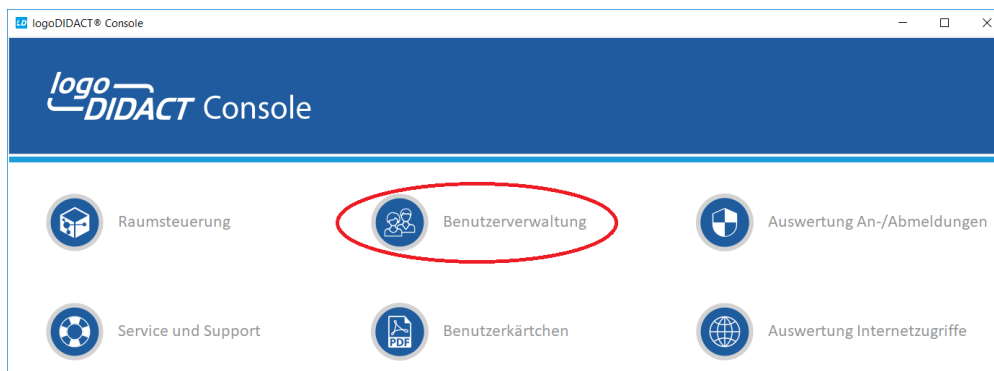


Achtung

Sind keine Benutzer bzw. Rechner ausgewählt, werden die einzelnen Funktionen der Raumsteuerung für den Raum ausgeführt.

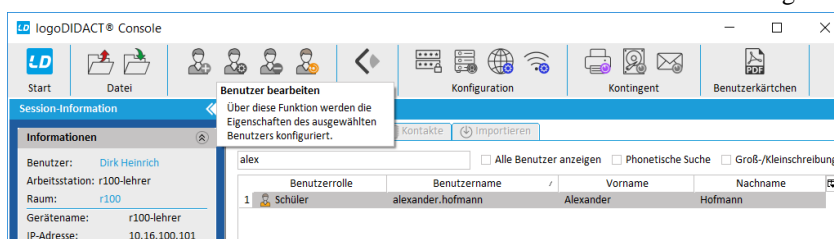
VI.2.4. Benutzerverwaltung

Die Benutzerverwaltung der LogoDIDACT-Console lässt sich über das Hauptmenü aufrufen.



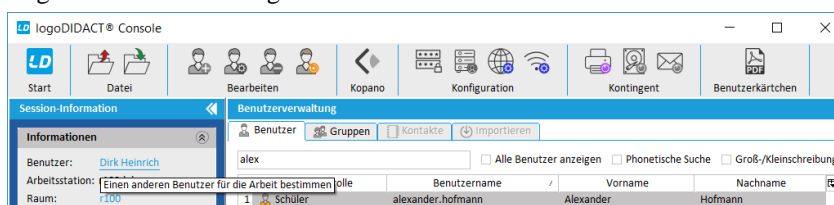
VI.2.4.1. Die Möglichkeiten als Lehrer

Wenn sich Lehrer an der LogoDIDACT-Console anmelden, werden diese feststellen, dass einige Funktionen für den Anwender „ausgegraut“ erscheinen. Alles, was ein "normaler" Lehrer im Unterricht machen können muss, ist möglich. Mit "normaler" Lehrer sind alle gemeint, die das System aus Anwendersicht bedienen und sich nicht mit der Administration beschäftigen.

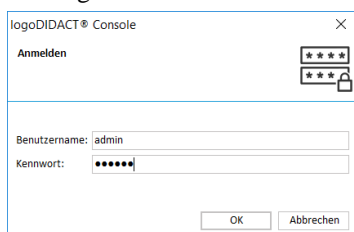


Dies hat seine Richtigkeit und ist kein Fehler vom Programm. Diese Funktionen sind allein den Systemadministratoren vorbehalten.

Im Bereich „Sessioninformation“ auf der linken Seite kann jedoch der angemeldete Benutzer in der LogoDIDACT-Console gewechselt werden.



Über den verlinkten Namen lässt sich ein Anmeldedialog aufrufen, über den sich andere Benutzer an der LogoDIDACT-Console anmelden können.



VI.2.4.2. Erstellen der Benutzerkärtchen

Das Erstellen von "Benutzerkärtchen" stellt eine sehr einfache und praktikable Möglichkeit zur Verfügung, neu angelegte Benutzer mit ihren Zugangsdaten zu versorgen.

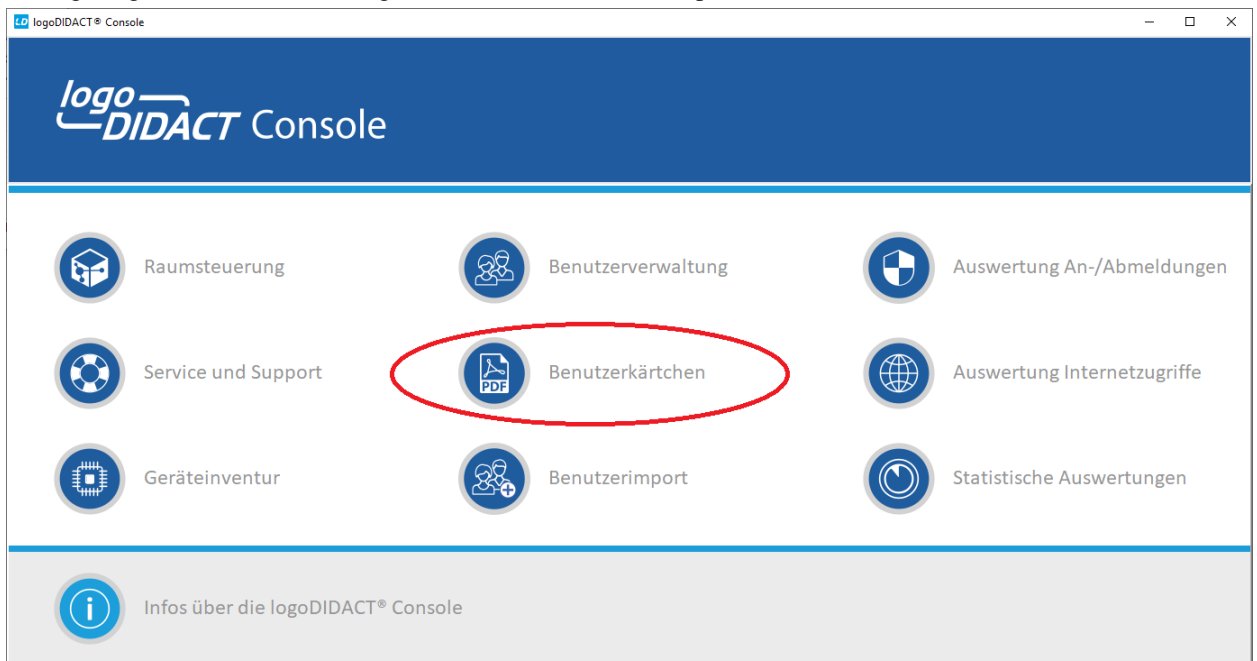
Es wird dabei eine Datei im benutzerfreundlichen PDF-Format (Portable Document Format) erstellt, auf der sich in der Standardausgabe auf jeder Seite jeweils 16 Kärtchen befinden, mit den wesentlichen Infos wie Vor- und Nachname, sowie Anmeldenamen und Initialkennwort eines Benutzers.

Die Seiten sind strukturiert nach Gruppen bzw. Klassen, so dass diese Listen nach dem Ausdruck an die Klassenlehrer*in übergeben werden kann.

VI.2.4.2.1. Erstellen einer Gesamtliste mit allen oder neuen Benutzern

Das Erstellen einer Gesamtliste über alle Klassen und Gruppen ist vor allem dann sinnvoll, wenn sehr viele oder auch alle Benutzer neu angelegt, wie es bei der Einführung von LogoDIDACT oder bei jedem Schuljahreswechsel der Fall ist.

Dann gelangen Sie über den Eintrag „Benutzerkärtchen“ im Hauptmenü am schnellsten zum Ziel.



Unmittelbar nachdem Sie den Eintrag **Benutzerkärtchen** gewählt haben, erscheint der Dialog, auf dem Sie festlegen können, ob weitere Daten auf den Kärtchen angezeigt werden sollen oder nicht. Es besteht in der Regel keine Notwendigkeit hier weitere Daten auszuwählen.

Eine für die Praxis wesentliche wichtigere Anpassung erfolgt über die Angabe des Datums, ab dem ein Benutzer angelegt wurde. Das ist insbesondere beim Schuljahreswechsel genau die Stelle, an der Sie nur die neu angelegten Schülerinnen und Schüler und gegebenenfalls neu angelegte Lehrer*innen in einer Liste ausdrucken und die neuen Benutzer mit ihren Zugangsdaten versorgen möchten.



Tipp

Sind keine Änderungen an den Standardeinstellungen für das Layout vorzunehmen, kann der Vorgang zur Erstellung der Benutzerkärtchen auch direkt über den Button „Fertigstellen“ gestartet werden.

Über die Schaltfläche **Weiter** des vorherigen Dialogs lassen sich detaillierte Anpassungen am Layout der Benutzerkärtchen vornehmen, wie z.B. die Anzahl an Kärtchen pro Zeile oder die Schriftart und ob die PDF für den Ausdruck im Hoch- oder Querformat erstellt wird.

Über die Schaltfläche **Weiter** gelangen Sie zur abschließenden Übersicht mit einer Zusammenfassung der getroffenen Anpassungen und dem per Standard aktivierten Häkchen **Datei nach dem Erstellen automatisch öffnen**.

Sofern dieses gesetzt bleibt und ein PDF-Reader installiert oder PDF-Viewer im Browser aktiviert ist, wird die gerade erstellte PDF-Datei mit den Benutzerkärtchen automatisch angezeigt. Über **Fertigstellen** wird aber zunächst die Datei mit den Benutzerkärtchen abgespeichert.



Achtung

Bitte beachten Sie, dass sich in dieser Liste personenbezogene Daten und Anmeldeinformationen befinden, die auf keinen Fall in falsche Hände gelangen sollten!

Speichern Sie diese Daten also an einem sicheren und nur Ihnen zugänglichen Ort ab!

Nach dem Ausdrucken und Verteilen der Benutzerzugangsdaten mit den initiellen Kennwörtern besteht in der Regel keine Notwendigkeit, die PDF-Datei aufzubewahren, so dass diese gelöscht werden kann.

Wie weiter oben beschrieben, ist der Aufbau der PDF-Datei strukturiert nach Gruppen und Klassen und beinhaltet auf der ersten Seite einige Infos sowie ein Inhaltsverzeichnis.

Der Aufbau einer Seite mit den Benutzerkärtchen sieht exemplarisch wie folgt aus:

Für das Verteilen von Benutzerkärtchen an die neuen Anwender hat sich folgendes Vorgehen in der Praxis bewährt und wird daher empfohlen

- der Administrator legt neue Benutzer an und erstellt die PDF-Datei mit allen neuen Konten
- der Administrator druckt die gesamte PDF-Datei aus und übergibt die Seiten mit den Benutzerkärtchen einer Klasse an den jeweiligen Klassenlehrer bzw. die Klassenlehrerin.
- der Klassenlehrer schneidet die Kärtchen aus und übergibt diese an seine Schüler*innen

VI.2.4.2.2. Erstellen von angepassten Benutzerlisten

Wenn eine Liste mit Benutzerkärtchen einzeln für eine ganz spezielle Gruppe von Benutzern erstellt werden soll oder andere Kriterien für die Auswahl benötigt werden, ist das über das Modul **Benutzerverwaltung** im Hauptmenü möglich.

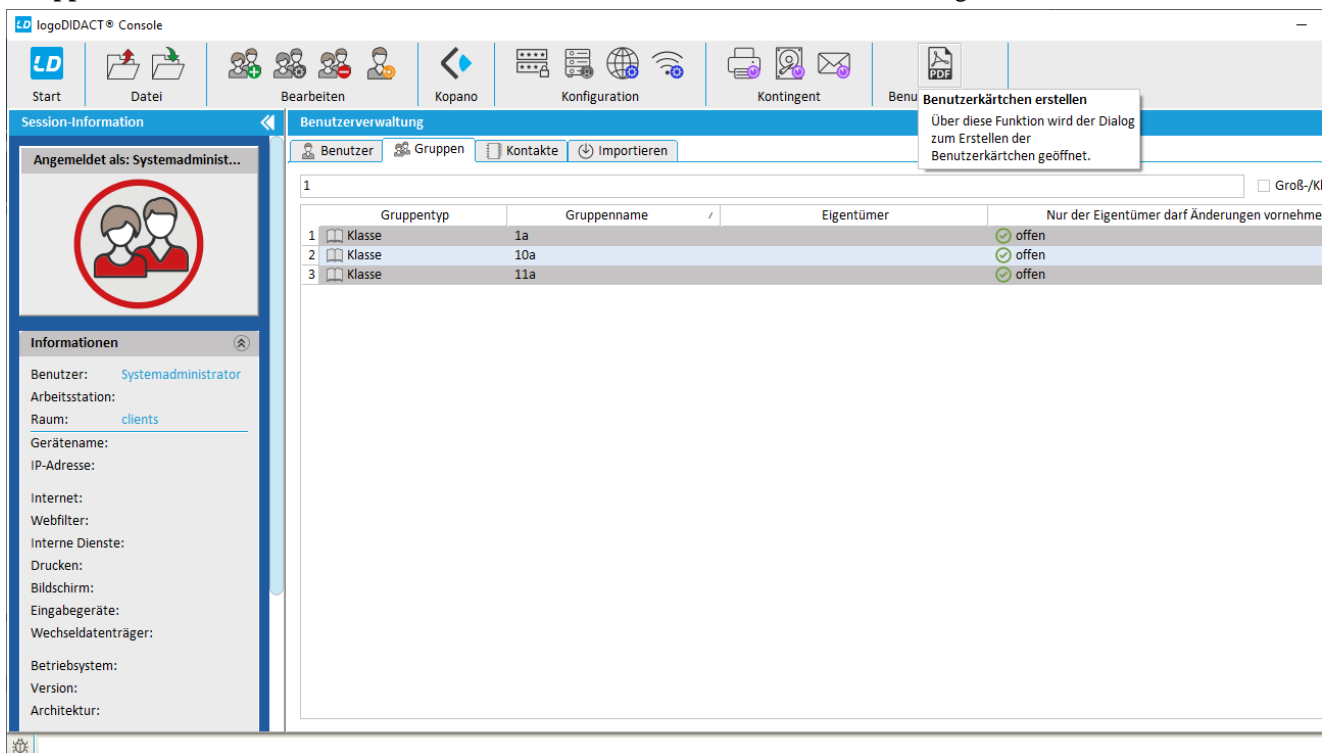
Über das Suchfeld und die Sortierung der Spalten haben Sie unzählige Möglichkeiten und Kriterien, nach denen Sie gezielt eine bestimmte Gruppe von Benutzerkonten anzeigen und auswählen können, um anschließend eine Liste mit Benutzerkärtchen exakt für diese Gruppe zu erstellen.

Möchten Sie beispielsweise eine Liste nur mit Schülern der Klasse 6a erstellen, schränken Sie die Anzeige dafür über das Suchfeld durch Eingabe der entsprechenden Klasse ein. Danach können Sie die Liste durch Auswahl der Schaltfläche **Benutzerkärtchen** im Menüband erstellen. Alternativ können Sie die Benutzer mit der Maus auswählen oder über die Tastenkombination **Strg+a** markieren und danach über die rechte Maustaste aus dem Kontextmenü den Eintrag **Benutzerkärtchen erstellen...** wählen.

Weitere Kriterien lassen sich über Konfiguration der Anzeige von Spalten im rechten oberen Bereich einblenden. So können Sie beispielsweise das **Erstelldatum** als Spalte anzeigen und danach sortieren lassen, um dann die Benutzerkärtchen und Listen nur für neu erstellte Schülerinnen und Schüler auszudrucken.

Ähnlich können Sie vorgehen, wenn neue Kolleginnen und Kollegen an die Schule kommen. Nachdem Sie diese über den Listenimport angelegt haben, schränken Sie die Benutzeranzeige im Suchfeld einfach auf die Gruppe **Lehrer** ein und sortieren nach der Spalte **Erstelldatum**. Markieren Sie dann gezielt nur die neu erstellten Konten und wählen Sie wieder über die rechte Maustaste aus dem Kontextmenü den Eintrag **Benutzerkärtchen erstellen...**

Wollen Sie entsprechende Benutzerlisten für mehrere Klassen erstellen, wechseln Sie zum Reiter **Gruppen** und schränken die Auswahl über das Suchfeld ein oder markieren die Klassen gezielt aus.



VI.2.4.3. Bearbeiten der Kennwörter

Über den Eintrag „Kennwort bearbeiten“ in der Symbolleiste und im Kontextmenü werden Aktionen zum Bearbeiten der Kennwörter für die ausgewählten Benutzer angeboten.

Über die Funktion „Kennwort wiederherstellen“ kann das aktuelle Kennwort durch den initiellen Wert ersetzt werden.

Abhängig davon, ob man zu der Gruppe Lehrer gehört oder zu einer administrativen Gruppe, lassen sich nur bestimmte Kennwörter bearbeiten. Als "normaler" Lehrer hat man beispielsweise nur das Recht sein eigenes Kennwort zu ändern und man sieht in der Benutzerverwaltung auch nur einen einzigen Lehrer und zwar sich selbst. Im Standardfall kann jedoch jeder Lehrer das Kennwort aller Schüler ändern, weil dies der Anforderung im Unterricht entspricht. Vergisst ein Schüler sein Kennwort, so muss jeder Lehrer das Kennwort z.B. auf den ursprünglichen Wert setzen können, ohne erst den Administrator zu informieren.

VI.2.4.4. Kennwortrichtlinien in der LogoDIDACT-Console ändern

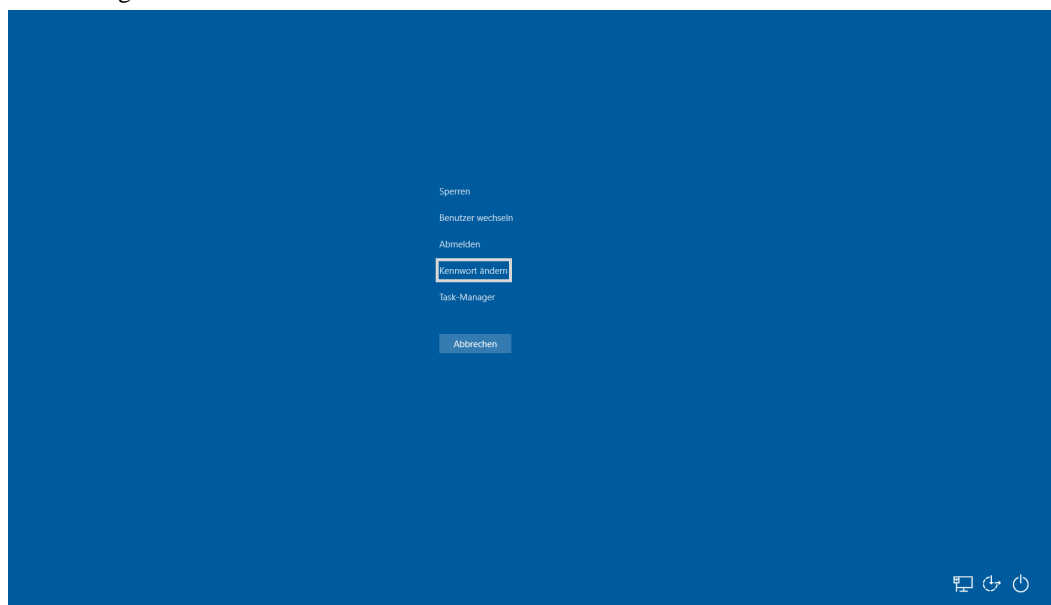
In der Standardeinstellung von LogoDIDACT können auch Lehrer die Kennwortrichtlinien von einzelnen Schüler oder auch ganzen Klassen ändern. Über die Kennwortrichtlinie kann man festlegen ob ein Benutzer sein Kennwort ändern darf oder nicht. Ebenso kann man erzwingen, dass das Kennwort bei der nächsten Anmeldung geändert werden muss.

Bitte überlegen Sie sich in diesem Zusammenhang genau, was für Ihre Schule oder die jeweilige Klassenstufe sinnvoll und passend ist. Die von LogoDIDACT generierten zufälligen Kennwörter sind oftmals deutlich besser, als das, was die Nutzer an Kennwörtern definieren, wenn sie beim ersten Login zur Änderung ihres Kennwortes aufgefordert werden.

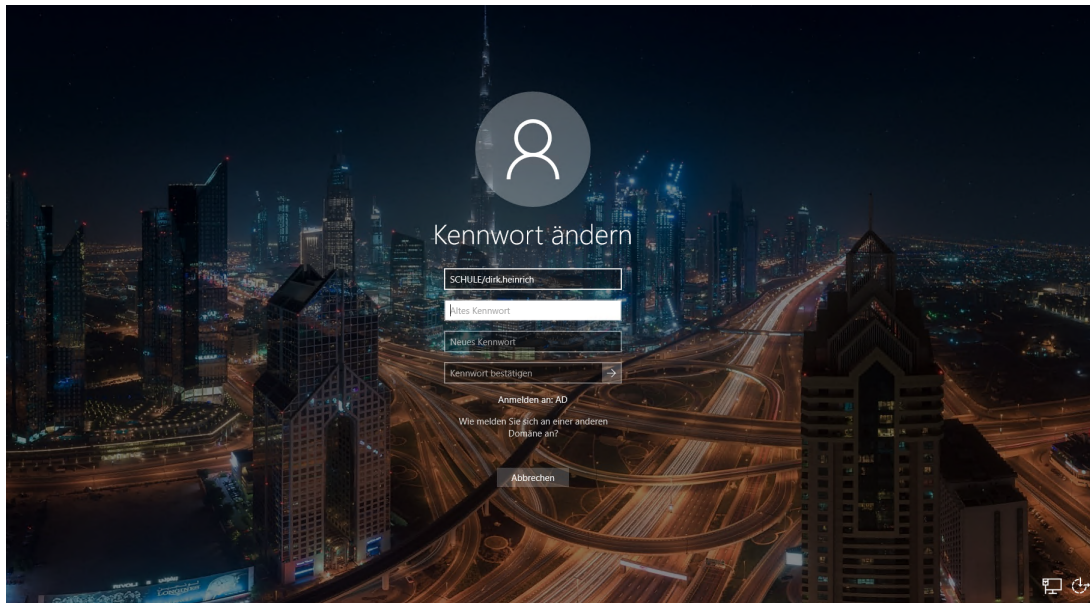
In vielen Fällen kann es daher sinnvoll sein, die obige Einstellung zu wählen, welche die Nutzer sogar daran hindert, daa von LogoDIDACT erstellte gute Knnwort zu ändern.

VI.2.4.5. Eigenes Kennwort ändern

Ob ein Benutzer sein eigenes Kennwort ändern darf oder bei der ersten Anmeldung sogar ändern muss, legt der Administrator über Kennwortrichtlinien fest. Per Standard kann ein Lehrer sein Kennwort ändern. Das ist sowohl über die LogoDIDACT-Console möglich, als auch aus Windows heraus. Um das Kennwort zu ändern, müssen Sie sich zunächst mit dem bestehenden Kennwort an der Domäne anmelden. Anschliessend drücken Sie die Tastenkombination **Strg+Alt+Entf** und wählen dann den Eintrag Kennwort ändern.



Geben Sie das alte Kennwort an und legen Sie ein neues fest, das Sie ein weiteres Mal im Feld **Kennwort bestätigen** eintragen.



VI.2.5. Service- und Support für Lehrer

VI.2.5.1. Problemstellung

Zunächst gibt es das zeitliche und organisatorische Problem, bei dem sich ein oder zwei Kollegen oder Kolleginnen pro Schule so nebenbei um alles kümmern sollen, was es so an Fehlern und Wünschen gibt. Dass dies sowohl zeitlich als auch oftmals fachlich nicht funktionieren kann ist allen Beteiligten klar, wird aber aus Kostengründen so festgelegt.

Das nächste Problem besteht überwiegend in der Kommunikation, d.h. sowohl intern an der Schule werden Fehler nicht oder nicht zeitnah gemeldet, als auch extern zum Dienstleister oder Schulträger gibt es keine geregelten Abläufe. Störungen werden mündlich oder per Schmierzettel gemeldet, gehen verloren oder werden schlichtweg vergessen. Dadurch entstehen häufig Missverständnisse und daraus dann unnötiger Frust und Ärger der Kollegen und Kolleginnen über nicht funktionierende Geräte.

Das dritte große Problem besteht in der Qualifizierung der Störungsmeldung. Vereinfacht ausgedrückt geht es nur darum, die wesentlichen und vor allem richtigen Informationen an jemanden weiterzugeben und sofern möglich, in etwa zu formulieren, um was für ein Problem es sich handelt. Jeder, der schon einmal mit einer Meldung "der dritte PC in der zweitletzten Reihe im oberen EDV-Raum geht nicht" konfrontiert wurde, weiß wie schwierig die Bearbeitung solcher Fälle ist, vor allem wenn sich im Nachhinein herausstellt, dass es die falsche Reihe war, der falsche Raum oder der falsche Rechner.

VI.2.5.2. Die Lösung in der Übersicht

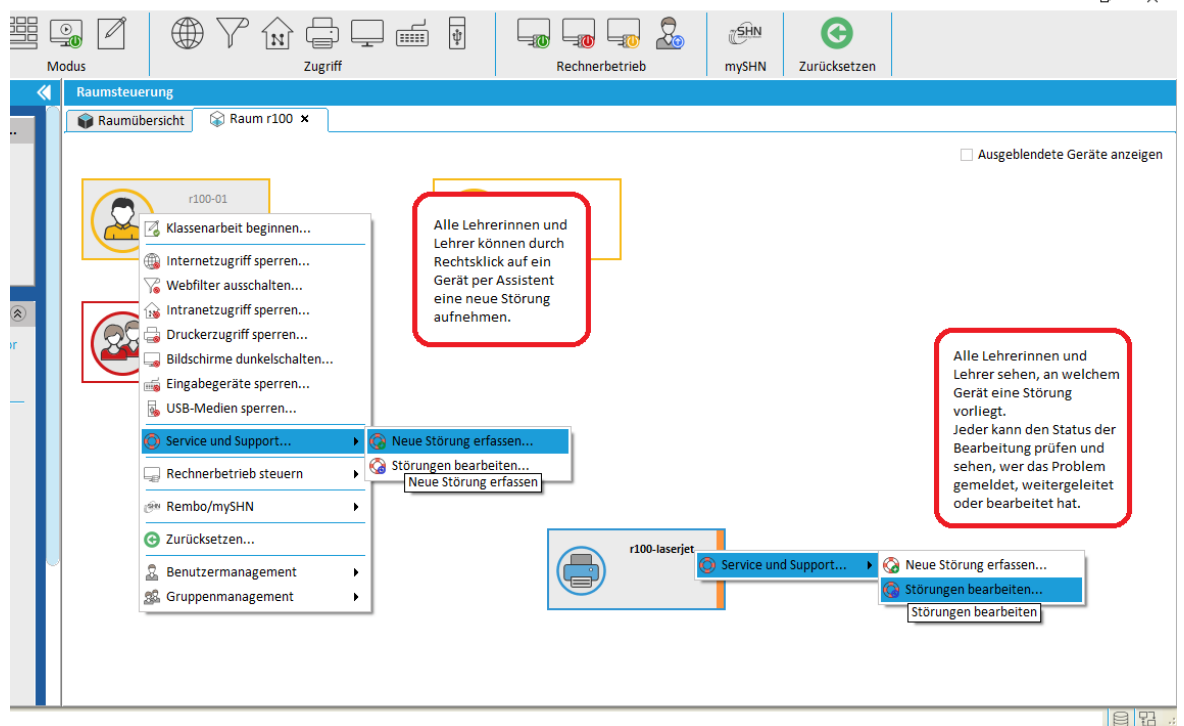


Abbildung VI.2.24. Anzeige und Erfassung von Störungen

VI.2.5.3. Vorteile

Das Service und Support-Modul in LogoDIDACT löst die typischen Probleme bei der Meldung, Bearbeitung und Behebung von EDV-Störungen sowohl schulintern als auch zwischen Schule und Dienstleister oder Schulträger.

- Einfache und schnelle Meldung.

Intuitive Bedienung ohne viel Eingabe, möglichst kurz und knapp und so, dass man als Laie eine Meldung absetzen kann.

- Zeitnahe Meldung und sichtbare Störung.

Über die LogoDIDACT-Console erfolgt die Eingabe einer Störung und durch entsprechende Warnsymbole die sofortige Anzeige, wo eine Störung vorliegt. Durch die einfache Bedienung entfallen vergessene Meldungen, es gibt weniger Missverständnisse und weniger Ärger.

- Qualifizierte Störungs-Meldung und Abarbeitung.

Für jedes Gerät gibt es bereits vordefinierte typische Störungsfälle. Angaben zur Bearbeitung der Störung werden automatisch erfasst und weitergeleitet (wer, was, wann, wo...).

VI.2.5.4. Anzeige von Störungen

Es ist selbsterklärend, dass man bei einer offensichtlich erkennbaren und bereits gemeldeten Störung an einem Gerät nicht noch eine weitere Störung meldet, ohne zu prüfen, was dort bereits gemeldet wurde.

Wichtig ist zunächst, dass am Baustellen-Symbol deutlich erkennbar ist, dass eine Störung an einem Gerät vorliegt. Ausführliche Informationen zu dem Problem erhält man durch Rechtsklick auf das Symbol und die Auswahl **Service und Support** → **Störungen bearbeiten**.

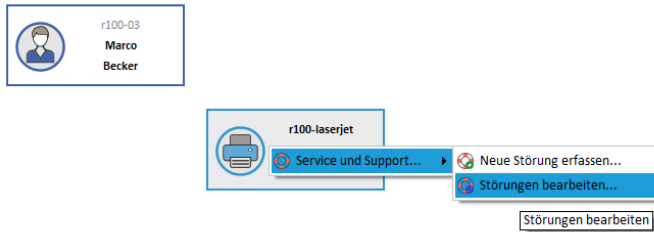


Abbildung VI.2.25. Anzeige vorhandener Störungen über Symbole

Dadurch öffnet sich das Hauptfenster für den Support des ausgewählten Gerätes.

VI.2.5.5. Das Hauptfenster im Ticketsystem

Der Begriff Ticketsystem wurde im Service und Support Modul bewusst so gewählt, weil damit künftig auch Wünsche oder Anforderungen abgebildet werden sollen.

Derzeit ist ein Ticket in LogoDIDACT zunächst einfach eine Art Akte, in der überwiegend Störungen und Probleme von Geräten festgehalten und protokolliert werden.

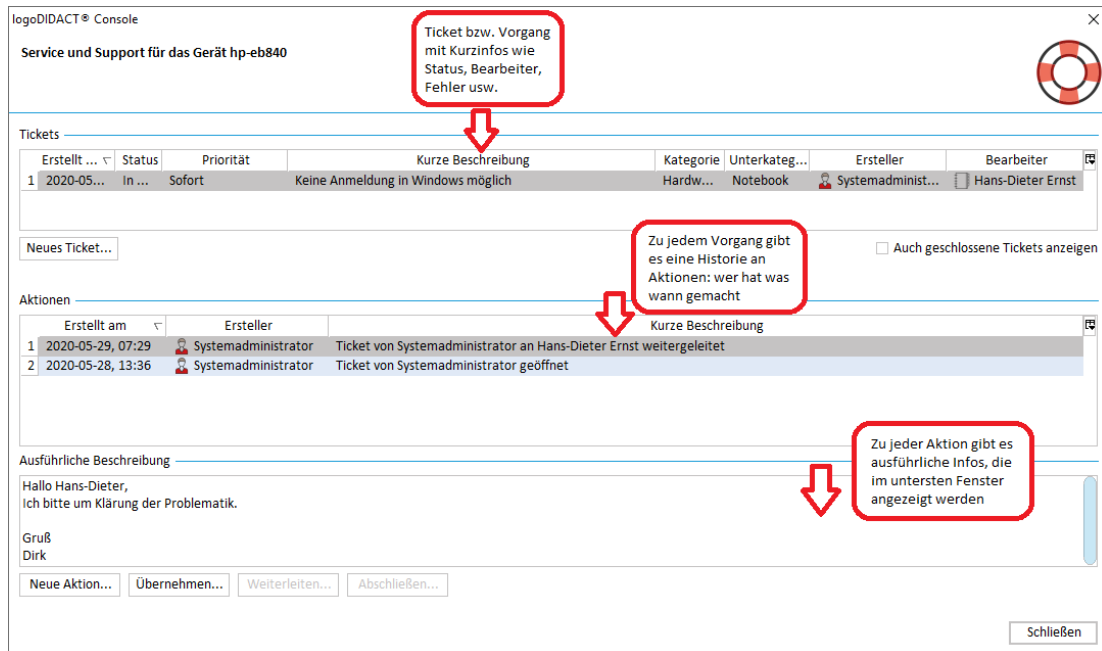


Abbildung VI.2.26. Anzeige der Störung mit Historie sämtlicher Aktionen am Beispiel eines Druckers.

Die eigentliche Bearbeitung von Störungen wird in aller Regel durch die Mitglieder der Gruppe Support erfolgen. In vielen Fällen kann es aber durchaus hilfreich sein, dass andere Kolleginnen und Kollegen dort Aktionen eintragen und damit zum Lösen eines Problems beitragen können. Der Umgang mit dem Dialog ist daher am Ende des Kapitels in Abschnitt VI.2.5.7, „Störungen bearbeiten“ beschrieben.



Tipp

Für die meisten Benutzer ist alleine die Information, dass es ein Problem mit einem Gerät gibt und sich jemand darum kümmert, extrem hilfreich.

Dass man darüber hinaus auch sehen kann, wer wann was gemacht hat und dass z.B. schon Termin mit einer externen Firma vereinbart wurde, um die Störung zu beheben, löst so gut wie alle bekannten Probleme in der Kommunikation und Organisation in diesem Bereich.

Das Aufnehmen und Weiterleiten neuer Störungen wird im nächsten Abschnitt behandelt.

VI.2.5.6. Neue Störung per Assistent erfassen

Die Meldung einer Störung erfolgt kinderleicht über die LogoDIDACT-Console. Jeder Lehrer kann Störungen melden, indem er in der symbolischen Ansicht das betroffene Gerät wählt und mit der rechten Maustaste aus dem Menü den Eintrag **Service und Support...** → **Neue Störung erfassen...** wählt. Es spielt dabei keine Rolle, ob das Gerät ein oder ausgeschaltet ist, funktioniert oder auch nicht.

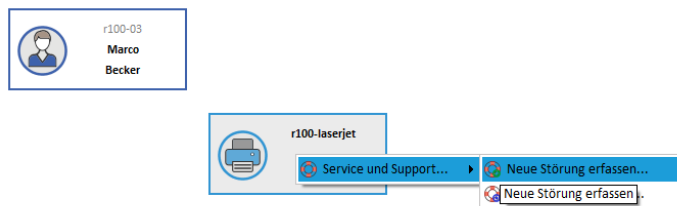


Abbildung VI.2.27. Störungsmeldung über Symbole

Das System weiß selbstverständlich welche Person gerade eine Störung melden möchte und auch an welchem Gerät, in welchem Raum und an welcher Schule. Alle diese Angaben müssen nicht manuell eingegeben werden.

Der Assistent führt selbsterklärend durch alle Schritte der Störungsmeldung.

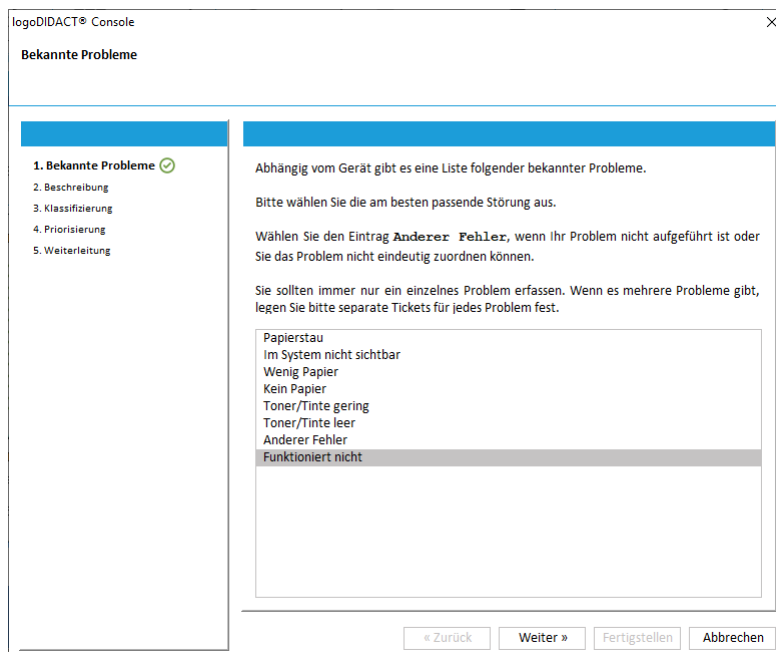


Abbildung VI.2.28. Auswahl möglicher bekannter Probleme und Störungen für das Gerät

Da über die Symbolik und die Hardwareinventarisierung bekannt ist, um was für ein Gerät es sich handelt, erfolgt eine vordefinierte Störungsangabe für das entsprechende Gerät.

Somit sind auch an dieser Stelle in aller Regel keine oder minimale manuelle Angaben notwendig. Die Störungen, die bei einem Drucker bekannt sind und auftreten können, stehen sofort zur Auswahl bereit. Eigene Angaben sind selbstverständlich auch möglich.

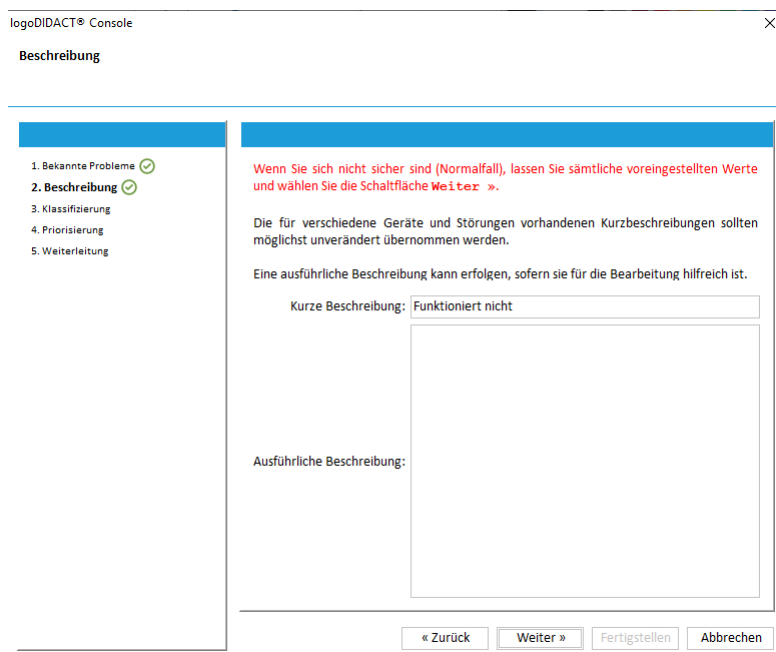


Abbildung VI.2.29. Optional kann man eine ausführliche Beschreibung geben.

Oftmals weiß man ja aber gar nicht, was genau nun an einem Gerät nicht geht, sondern nur, dass es nicht geht. In solchen Fällen sollten man besser keine zusätzlichen Angaben machen und einfach auf **Weiter** klicken.

logoDIDACT® Console

Klassifizierung

1. Bekannte Probleme ✓
2. Beschreibung ✓
3. **Klassifizierung** ✓
4. Priorisierung
5. Weiterleitung

Wenn Sie sich nicht sicher sind (Normalfall), lassen Sie sämtliche voreingestellten Werte und wählen Sie die Schaltfläche **Weiter** ».

Sofern eine Störung eindeutig als Hardware- oder Softwarefehler erkennbar ist, können Sie das über den Eintrag **Kategorie** festlegen.

Weitere Festlegungen sind über den Eintrag **Unterkategorie** möglich.

Kategorie:

Unterkategorie:

Ersteller:

Bearbeiter:

« Zurück Weiter » Fertigstellen Abbrechen

Abbildung VI.2.30. Optional kann man eine Kategorisierung des Fehlers vornehmen.

logoDIDACT® Console

Priorisierung

1. Bekannte Probleme ✓
2. Beschreibung ✓
3. Klassifizierung ✓
4. **Priorisierung** ✓
5. Weiterleitung

Wenn Sie sich nicht sicher sind (Normalfall), lassen Sie sämtliche voreingestellten Werte und wählen Sie die Schaltfläche **Weiter** ».

Die Angaben zu Priorität oder Termin können intern genutzt werden, um die Bearbeitung bestimmter Probleme zeitlich grob einzuplanen.

Priorität:

Termin:

Status:

« Zurück Weiter » Fertigstellen Abbrechen

Abbildung VI.2.31. Optional kann man eine Priorisierung vornehmen.

Im letzten Dialog muss auf jeden Fall eine Auswahl für die Weiterleitung des Problems an eine Person aus der Gruppe Support getroffen werden.

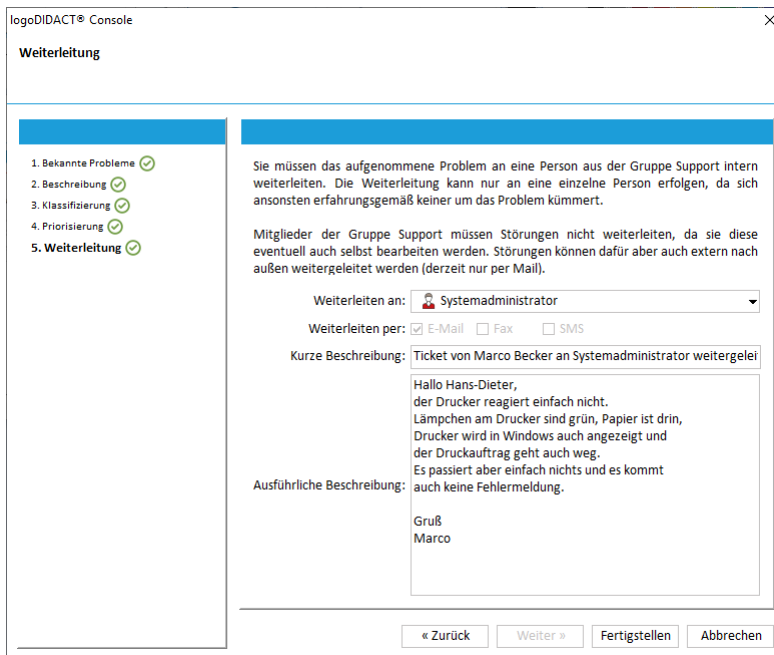


Abbildung VI.2.32. Weiterleitung der Störung an eine Person aus der Gruppe Support.

Wie auch im Dialog erwähnt, ist eine Weiterleitung bewusst nur an eine einzelnen Person möglich, weil Weiterleitungen an mehrere Personen in aller Regel dazu führen, dass sich niemand um das Problem kümmert.

Auch hier ist es möglich aber nicht zwingend erforderlich, zusätzliche Infos einzutragen, sofern sie hilfreich sind. Das Problem wird durch Auswahl von **Fertigstellen** weitergeleitet und der Dialog geschlossen.

Unmittelbar danach, wird die neu aufgenommene Störung an dem Gerät in der symbolischen Raumansicht durch das Baustellen-Symbol für alle erkennbar.

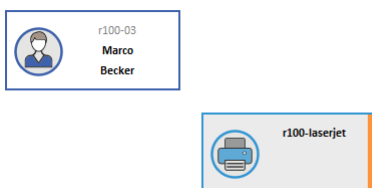


Abbildung VI.2.33. Gemeldete Störung wird in der symbolischen Ansicht für alle erkennbar.

VI.2.5.7. Störungen bearbeiten

logoDIDACT® Console

Service und Support für das Gerät r100-laserjet

Tickets

	Erstellt am	Status	Priorität	Kurze Beschreibung	Kategorie	Unterkategorie	Ersteller	Bearbeiter
1	2020-06-15	In Bearbeitung	So schnell wie m...	Papierstau	Hardware	Drucker	Marco Becker	Systemadmin...

Neues Ticket... Auch geschlossene Tickets anzeigen

Aktionen

	Erstellt am	Ersteller	Kurze Beschreibung
1	2020-06-15, 10:34	Marco Becker	Ticket von Marco Becker an Systemadministrator weitergeleitet
2	2020-06-15, 10:32	Marco Becker	Ticket von Marco Becker geöffnet

Ausführliche Beschreibung

Hallo Hans-Dieter,
der Drucker verursacht seit etwa 3-4 Tagen immer häufiger einen Papierstau.
Wir verwenden kein spezielles Papier und der Drucker ist erst einige Monate alt.

Gruß Marco

Neue Aktion... Übernehmen... Weiterleiten... Abschließen...

Schließen

Abbildung VI.2.34. Störung bearbeiten und neue Aktion eintragen

Über die Schaltfläche **Neue Aktion...** wird der Dialog zum Eintragen eines Vorgangs geöffnet.

logoDIDACT® Console

Neue Aktion hinzufügen

Kurze Beschreibung:

Ausführliche Beschreibung:

OK Abbrechen

Abbildung VI.2.35. Dialog Aktion bzw. Tätigkeit hinzufügen

Wie viele Aktionen man hier notiert oder wie ausführlich, hängt sowohl vom Problem als auch dem eigenen Wissen über die Lösung von Problemen ab. Grundsätzlich sollte man hier aber immer möglichst kurze und aussagekräftige Beschreibungen wählen.

VI.2.5.8. Störungen weiterleiten

Die vorherige eingetragene Aktion ist im Hauptfenster sichtbar und eine Weiterleitung an verschiedenen Personen möglich. Alle Lehrer können ein Ticket intern weiterleiten entweder an Mitglieder der Gruppe Support oder auch an denjenigen, der das Ticket erstellt hat (im Beispiel der Lehrer Dirk Heinrich).

Eine Weiterleitung zu einem externen Kontakt ist nur für Mitglieder der Gruppe Support möglich.

logoDIDACT® Console

Service und Support für das Gerät r100-laserjet

Tickets

Erstellt am	Status	Priorität	Kurze Beschreibung	Kategorie	Unterkategorie	Ersteller	Bearbeiter
1 2020-06-16	In Bearbeitung	Sofort	Papierstau	Unbekannt	Sonstige	Marco Becker	Systemadministrator

Neues Ticket... Auch geschlossene Tickets anzeigen

Aktionen

Erstellt am	Ersteller	Kurze Beschreibung
1 2020-06-16, 13:52	Systemadministrator	Papiereinzug vermutlich defekt
2 2020-06-16, 13:52	Marco Becker	Ticket von Marco Becker an Systemadministrator weitergeleitet
3 2020-06-16, 13:51	Marco Becker	Ticket von Marco Becker geöffnet

Ausführliche Beschreibung

Drucker geprüft
zieht immer mehrere Seiten Papier auf einmal ein

Neue Aktion... Übernehmen... Weiterleiten...

logoDIDACT® Console

Ticket weiterleiten

Weiterleiten an: Marco Becker

Weiterleiten per: Marco Becker

Kurze Beschreibung: Ticket von Systemadministrator an Marco Becker weitergeleitet

Ausführliche Beschreibung:

Ausführliche Beschreibung: den Grund fürs Weiterleiten des Tickets angeben!

OK Abbrechen

Abbildung VI.2.36. Eingetragene Aktion ist für alle sichtbar und eine Weiterleitung möglich

Im Folgenden ist dargestellt, wie die Meldung nach außen zu einem externen Kontakt per Mail weitergeleitet wird. Voraussetzung ist selbstverständlich eine korrekte Ankopplung des Mailservers nach außen.

logoDIDACT® Console

Ticket weiterleiten

Weiterleiten an: Systemadministrator

Weiterleiten per: E-Mail Fax SMS

Kurze Beschreibung: Ticket von Marco Becker an Systemadministrator weitergeleitet

Ausführliche Beschreibung:

mail@mans-oretz,
der Drucker hat vermutlich ein Problem mit dem Papiereinzug.
Wir haben ja 3 Jahre Vor-Ort-Service.
Bitte kümmern Sie sich darum.
(Daten werden im Ticket automatisch angehängt)

Gruß
Marco

OK Abbrechen

Abbildung VI.2.37. Weiterleitung extern nach außen z.B. zu Systemhaus oder Schulträger

Durch das Weiterleiten wechselt die Zuständigkeit.

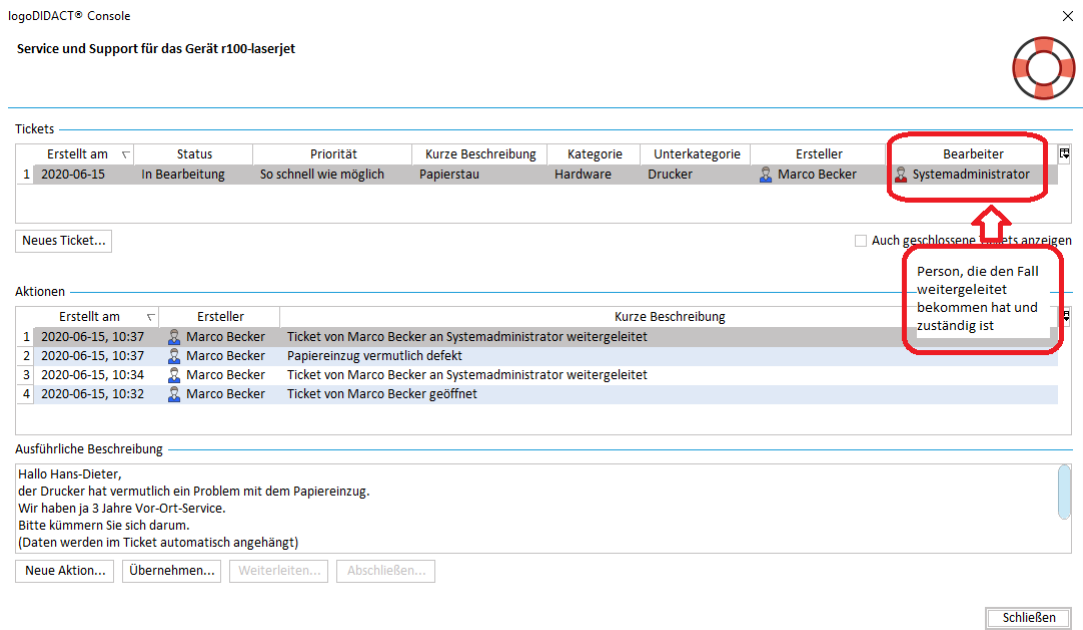


Abbildung VI.2.38. Durch Weiterleitung wechselt der Bearbeiter, der aktuell zuständig ist.

VI.2.5.9. Störungen abschliessen

Das Abschliessen einer Störung geschieht über die Schaltfläche **Abschließen...**, wobei ausgewählt werden kann, ob der Ersteller, der letzte Bearbeiter, niemand oder alle informiert werden sollen. In der Regel wird man alle Beteiligten informieren, wenn man eine Störung beseitigt hat.

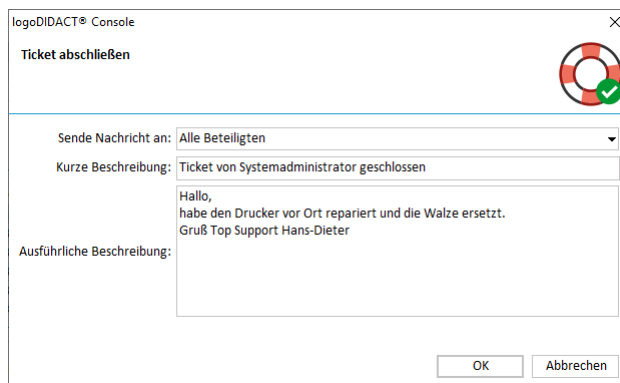


Abbildung VI.2.39. Das Abschliessen und Informieren einer Störung.

Unmittelbar nach dem Abschliessen "verschwindet" das Ticket und sämtliche Vorgänge und ausführliche Beschreibungen.

logoDIDACT® Console

Service und Support für das Gerät r100-laserjet

Tickets

Erstellt am	Status	Priorität	Kurze Beschreibung	Kategorie	Unterkategorie	Ersteller	Bearbeiter
-------------	--------	-----------	--------------------	-----------	----------------	-----------	------------

Neues Ticket... Auch geschlossene Tickets anzeigen

Aktionen

Erstellt am	Ersteller	Kurze Beschreibung
-------------	-----------	--------------------

Ausführliche Beschreibung

Neue Aktion... Übernehmen... Weiterleiten... Abschließen...

Schließen

Abbildung VI.2.40. Nach dem Abschliessen ist das Ticket und sämtliche Aktionen dazu nicht mehr sichtbar.

Durch Setzen des Häkchens "Auch geschlossene Tickets anzeigen" wird das letzte Ticket und auch alle zuvor eventuell vorhandenen Tickets angezeigt.

logoDIDACT® Console

Service und Support für das Gerät r100-laserjet

Tickets

Erstellt am	Status	Priorität	Kurze Beschreibung	Kategorie	Unterkategorie	Ersteller	Bearbeiter
1 2020-06-15	Geschlossen	So schnell wie möglich	Papierstau	Hardware	Drucker	Marco Becker	Systemadministrator
2 2020-06-15	Geschlossen	So schnell wie möglich	Papierstau	Hardware	Drucker	Marco Becker	Marco Becker
3 2020-06-15	Geschlossen	So schnell wie möglich	Papierstau	Hardware	Drucker	Systemadministr...	Marco Becker

Neues Ticket... Auch geschlossene Tickets anzeigen

Aktionen

Erstellt am	Ersteller	Kurze Beschreibung
1 2020-06-16, 11:13	Systemadmin...	Ticket von Systemadministrator geschlossen
2 2020-06-15, 13:45	Marco Becker	Ticket von Marco Becker an Systemadministrator weitergeleitet
3 2020-06-15, 13:45	Marco Becker	Beschluss: Drucker soll ersetzt werden
4 2020-06-15, 10:37	Marco Becker	Ticket von Marco Becker an Systemadministrator weitergeleitet
5 2020-06-15, 10:37	Marco Becker	Papiereinzug vermutlich defekt
6 2020-06-15, 10:34	Marco Becker	Ticket von Marco Becker an Systemadministrator weitergeleitet

Ausführliche Beschreibung

Hallo,
haben den Drucker vor Ort repariert und die Walze ersetzt.
Grüß Top Support Hans-Dieter

Neue Aktion... Übernehmen... Weiterleiten... Abschließen...

Schließen

Abbildung VI.2.41. Geschlossene Tickets anzeigen.

Kapitel VI.3. Arbeiten von Zuhause aus

LogoDIDACT bietet seit vielen Jahren die Möglichkeit, dass man sich von zu Hause aus über das Internet auf dem Schulserver einwählt und dort auf Dokumente und/oder Dienste zugreift. Die Verbindung von zu Hause auf den Schulserver kann dabei über die kostenfreie Software „OpenVPN“ und so genannte „VPN-Keys“ (Schlüssel) individuell für jeden Benutzer freigeschaltet werden. Der Administrator des Netzwerkes muss den Zugriff per OpenVPN für die Benutzer explizit aktivieren (siehe Abschnitt V.1.1.5, „VPN-Keys erzeugen und VPN-Zugang freischalten“). Aus technischen Gründen erfolgt die Freischaltung in der Regel gezielt für einzelne Lehrer oder Klassen.

Der Datendurchsatz und damit die Geschwindigkeit des Zugriffs von zu Hause aus wird dabei immer von der langsamsten Upload-Geschwindigkeit auf der jeweiligen Seite zum Internet hin bestimmt. Die folgende Skizze „Flaschenhals“ verdeutlicht die Problematik.

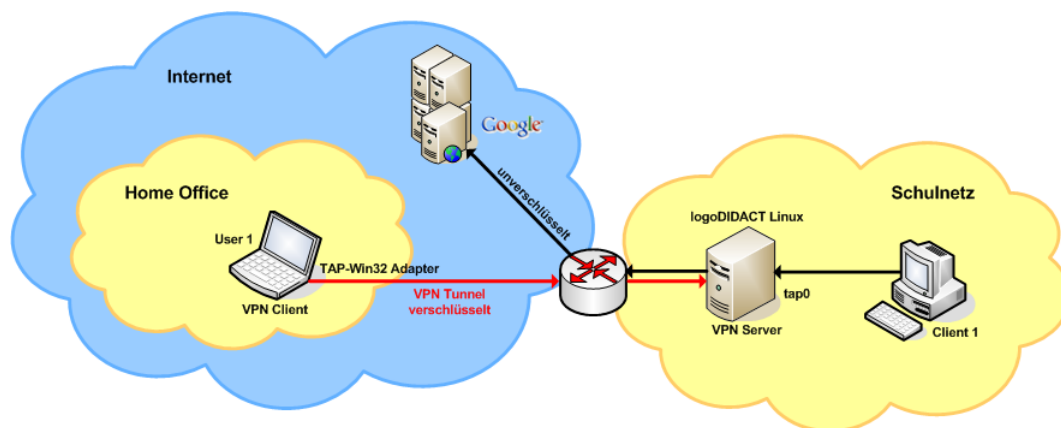


Abbildung VI.3.1. VPN-Tunnel

Wurde der OpenVPN-Zugang vom Administrator für einen Benutzer aktiviert, findet dieser die notwendigen Keys in seinem Homeverzeichnis im Ordner „OpenVPN“ auf dem Schulserver.

VI.3.1. Remote-Einwahl Vorbereitungen

Kopieren Sie den Inhalt des OpenVPN Ordners aus Ihrem Homeverzeichnis z.B. auf einen USB-Stick und nehmen Sie diese Dateien mit nach Hause. Dort kopieren Sie die Daten auf Ihren privaten Rechner.

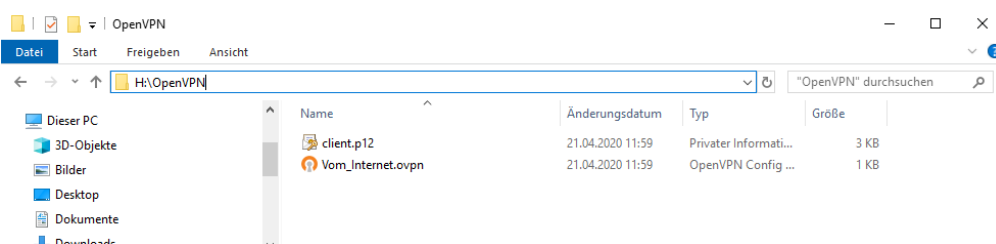


Abbildung VI.3.2. Homeverzeichnis

Kopieren Sie auch gleich den Ordner GUILogon vom Server im Verzeichnis P:\Programme auf Ihren USB-Stick. Wozu dieses Tool gut ist, wird im weiteren Verlauf erklärt.

VI.3.2. Installation auf Windows-Clients

Installieren Sie die OpenVPN Software. Sie erhalten diese kostenfrei im Internet unter <http://openvpn.net/>. Über das Menü **Community** finden sich unter Downloads die aktuellen Versionen für alle gängigen Betriebssysteme. Für Windows benötigen Sie die .exe Datei.

Am einfachsten ist es, wenn Sie die Installation entsprechend den Vorgaben nach `C:\Programme\OpenVPN` und mit allen vorgewählten Optionen durchführen. Dazu gehört vor allem auch die graphische Oberfläche OpenVPN GUI.

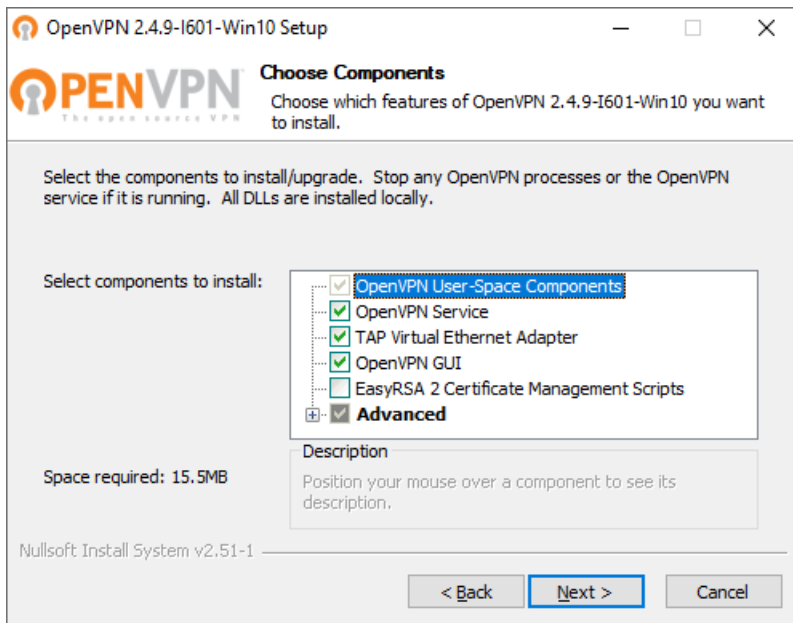


Abbildung VI.3.3. Installer für OpenVPN

Nach Abschluss der Installation finden Sie auf dem Desktop des Rechners ein Icon OpenVPN GUI.

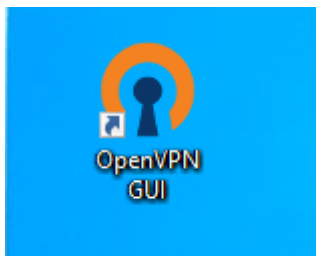


Abbildung VI.3.4. Desktop Icon für OpenVPN

Kopieren Sie nun die beiden Dateien `Vom_Internet.ovpn` und `client.p12` in den Installationspfad `C:\Programme\OpenVPN\config`. Damit ist die Installation und Konfiguration abgeschlossen.

VI.3.3. VPN-Einwahl

Für die Einwahl per VPN gibt es nun zwei Möglichkeiten, wobei die graphische Variante für die meisten Anwender zu empfehlen ist.

VI.3.3.1. VPN-Einwahl per graphischer Oberfläche mit OpenVPN GUI

Durch Doppelklick auf das Desktop Symbol **OpenVPN GUI** startet eine kleine Anwendung, die dann als Symbol unten rechts auf der Taskbar erscheint. Ein Rechtsklick auf das Icon öffnet das entsprechende Menü und über die Auswahl **Verbinden** wird die Verbindung aufgebaut.

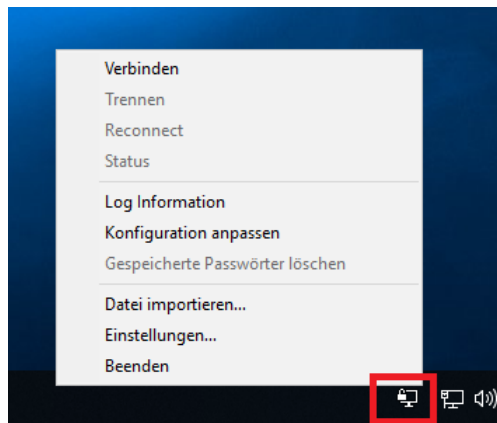


Abbildung VI.3.5. OpenVPN Icon mit Menü an der Taskbar

Während des Verbindungsaufbaus wird ein Dialogfenster angezeigt, das jedoch bei erfolgreichem Aufbau schnell wieder minimiert wird.

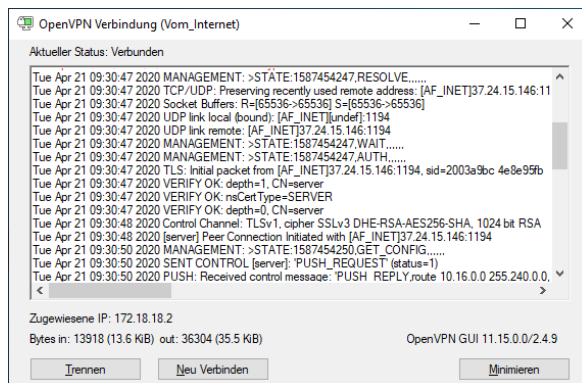


Abbildung VI.3.6. Aufbau der VPN-Verbindung mit Log-Daten

Das Icon auf der Menüleiste ändert bei erfolgreicher Verbindung seine Farbe auf grün und zeigt Informationen zu der Verbindung an, wie z.B. IP-Adresse, die Verbindungszeit- und Dauer.

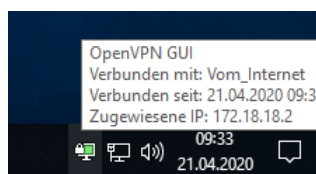


Abbildung VI.3.7. Erfolgreiche VPN-Verbindung mit weitem Infos



Achtung

Bitte beachten Sie, dass die VPN-Verbindung zwischen Ihrem privaten Gerät und dem Schulserver durch spezielle Einschränkungen oder Software auf Ihrem privaten Gerät verhindert werden kann.

In aller Regel, liegt es an fehlenden Berechtigungen. Führen Sie deshalb sowohl die Installation als auch die Einwahl mit OpenVPN mit dem lokalen Konto **Administrator** durch.

Weitere Einschränkungen können durch lokale Firewalls, Routersperren oder Einstellungen in den Windows 10 Berechtigungen (UAC) oder der Namensauflösung bestehen.

Auf individueller privater Endkundenebene kann dafür kein Support geleistet werden!

VI.3.4. Die LogoDIDACT-Console über OpenVPN

Die LogoDIDACT-Console kann von zu Hause aus über VPN bis auf eine Ausnahme genau so verwendet werden, wie lokal an der Schule. Einzig die Bildschirmübertragung ist aufgrund der zu geringen Bandbreite deaktiviert.

Um die LogoDIDACT-Console auf dem privaten Rechner auszuführen, benötigt man natürlich die Clientsoftware. Der Installer kann hier heruntergeladen werden:

https://files.sbe.de/logoDIDACT/LDC_Setup.exe

Doppelklicken Sie auf die Datei LDC_Setup.exe und folgen Sie den Anweisungen. Damit haben Sie nun alle drei Programme installiert und konfiguriert, um von zu Hause aus an Daten auf dem Server zu kommen und über die LogoDIDACT-Console Dateien auszuteilen oder mit entsprechenden Rechten auch die Benutzerverwaltung durchzuführen.



Abbildung VI.3.8. Die drei Tools für die Arbeit von zu Hause aus

VI.3.4.1. Start der LogoDIDACT-Console per VPN

Starten Sie die LogoDIDACT-Console wie gewohnt durch Doppelklick auf das entsprechende Symbol auf dem Arbeitsplatz.

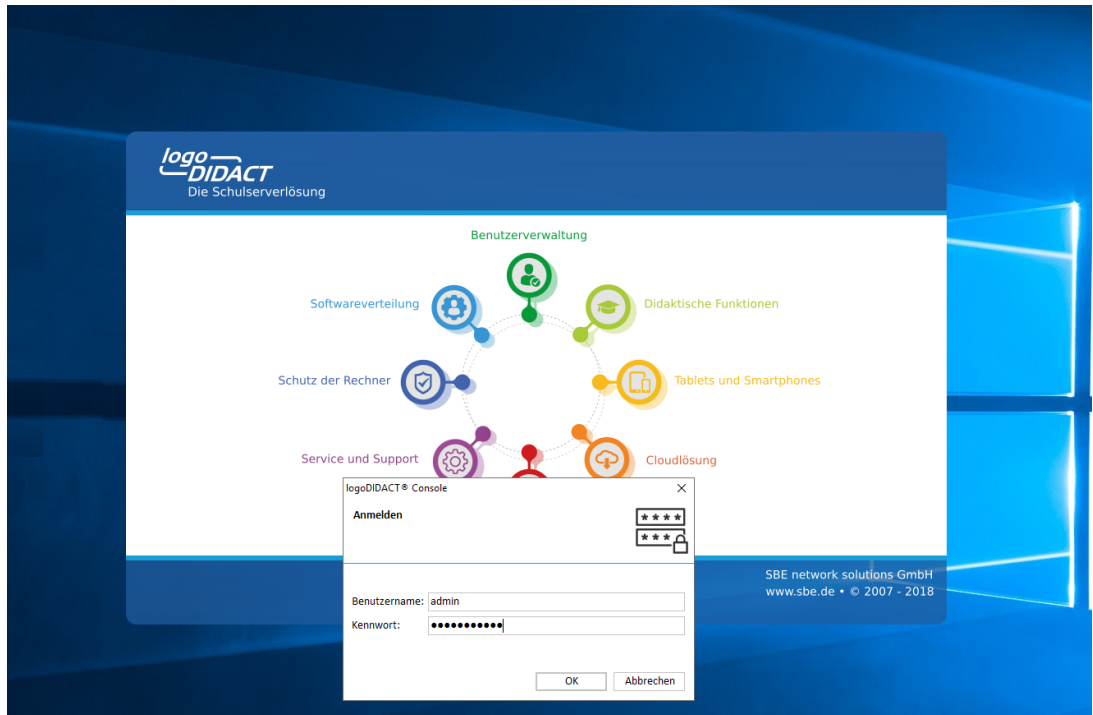


Abbildung VI.3.9. Der Start der LogoDIDACT-Console per VPN

Sollte das Anmeldefenster nicht sofort erscheinen, so liegt die Ursache eventuell darin, dass es an Ihrem privaten Rechner Probleme mit der Namensauflösung gibt. Um das zu vermeiden, können Sie der LogoDIDACT-Console beim Start auch die interne IP-Adresse des Servers mit übergeben (per Standard 10.16.1.1).

Ändern Sie dazu über die Eigenschaften des Desktop-Symbols den Wert **Ziel:** in

"C:\Program Files\logoDIDACT\Console\bin\ldc.exe --host 10.16.1.1"

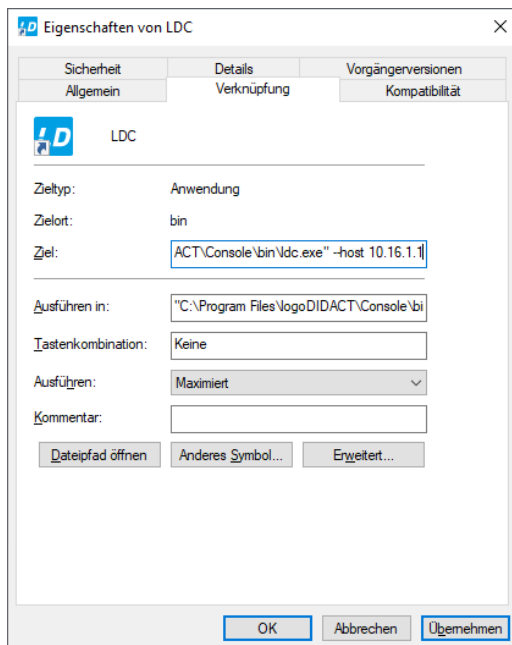


Abbildung VI.3.10. IP-Adresse des Servers an der Schule der LogoDIDACT-Console als Parameter übergeben

VI.3.5. Zugriff auf Web-Dienste per OpenVPN

Sofern die OpenVPN-Verbindung steht und die Namensauflösung korrekt funktioniert, besteht der erste und einfachste Nutzen dieser VPN-Verbindung darin, dass man von zu Hause aus auf die Web-Dienste des LogoDIDACT Servers zugreift.

Wenn die Namensauflösung im privaten System richtig funktioniert, dann erkennt man dies daran, dass im Browser alle Dienste per Name angesprochen werden können, die auch direkt vor Ort an der Schule erreichbar sind. Aus Endanwendersicht gehören dazu vor allem **moodle** (Lernplattform), **mrbs** (Raumbuchungssystem) und **webmail** (Roundcube Web-Mailer), **pydio** oder **nextcloud**. Aus Administrationsicht sind zusätzlich **cups** (Drucker), **itb** und das **Control Center** nutzbar.

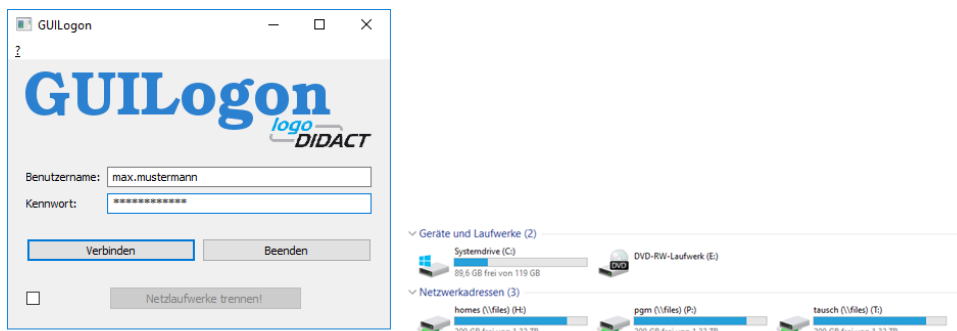
Abbildung VI.3.11. Raumbuchungssystem mrbs von zu Hause aus per OpenVPN aufrufen

VI.3.6. Zugriff auf Dateien per VPN

VI.3.6.1. Verbindung von Netzlaufwerken mit GUILogon


Speziell für private Geräte gibt es in LogoDIDACT das Tool GUILogon, über das man sich unter Windows sehr einfach mit dem LogoDIDACT-Server verbinden kann. Das Tool kann per Browser über den folgenden Link heruntergeladen werden: <https://files.sbe.de/logoDIDACT/GUILogon/GUILogon.exe>.

Es handelt sich um eine portable Anwendung ohne Setup, damit sie jederzeit schnell zur Verfügung steht. Das Programm kann durch Doppelklick auf die Anwendungsdatei direkt gestartet werden. Es müssen in die entsprechenden Felder gültige Zugangsdaten eingegeben werden, um die Verbindung zu den Freigaben am Server herzustellen. Verwenden Sie für Benutzername und Kennwort die Daten Ihres LogoDIDACT Benutzerkontos.



Nach Eingabe der Logindaten und Klick auf den Button „Verbinden“ werden standardmäßig die Laufwerke H: (Home), P: (Programme) und T: (Tausch) verbunden.

Abbildung VI.3.12. Laufwerksmapping für private Geräte mit GUILogon

 **Achtung**

Die Netzlaufwerke können selbstverständlich nur dann mit den entsprechenden Buchstaben H:, T: und P: verbunden werden, wenn diese an dem privaten Rechner nicht bereits benutzt werden. Sollte das der Fall sein, dann vergeben Sie bitte für Ihre lokalen Laufwerke andere Buchstaben.

Die Netzlaufwerke werden durch das Tool nur temporär in der jeweiligen Sitzung verbunden. Nach Neustart des Endgeräts sind sie wieder weg, GUILogon lässt sich zu einem späteren Zeitpunkt aber selbstverständlich wieder starten.

Kapitel VI.4. Microsoft 365

VI.4.1. LogoDIDACT-Ankopplung an Office 365

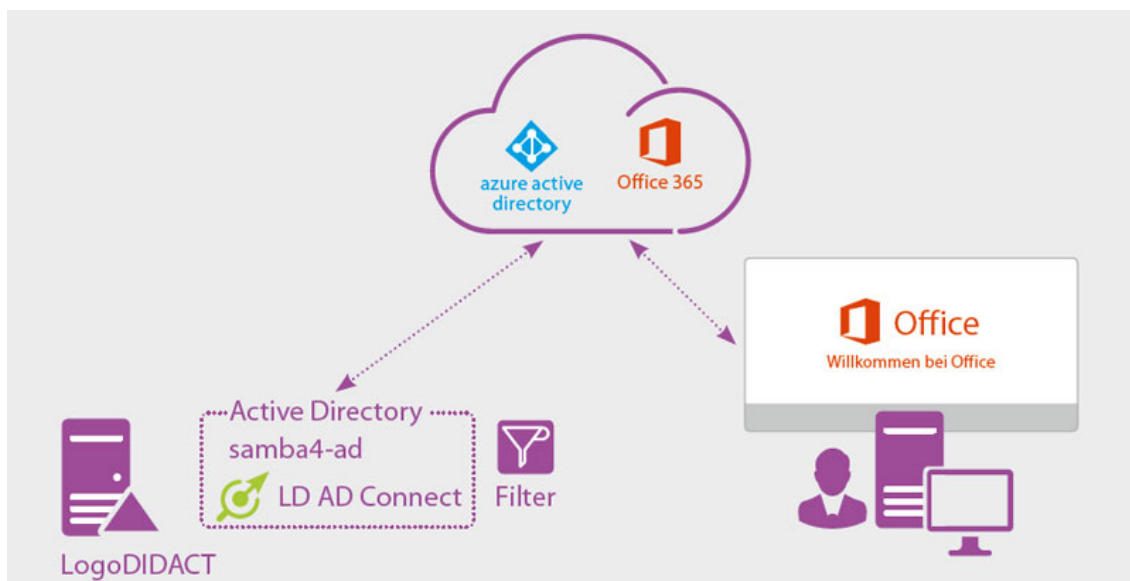
Microsoft hat den Namen für seine Cloudplattform im Laufe des Jahres 2020 von Office 365 abgeändert in Microsoft 365. Mit der Bezeichnung "Microsoft 365" kommt auch eher zum Ausdruck, dass die Cloud-Plattform mehr als nur Office ist und inzwischen das gesamte Microsoft Lösungsportfolio extrem umfangreiche Cloud-Plattform bestehend aus Hunderten Diensten und APPs.

VI.4.1.1. Automatisierung mit LD Azure Connect

Auch für Endanwender ist es wichtig zu wissen und zu verstehen, wie der LogoDIDACT-Server und die Microsoft-Cloud miteinander verbunden sind und welche Vorteile sich daraus ergeben.

Der Connector **LD Azure Connect** verbindet den LogoDIDACT-Schulserver mit der Microsoft 365-Infrastruktur und erledigt die gesamte Administration von Office 365 weitestgehend automatisiert.

Benutzer, Kennwörter, Gruppen, Lizenzen und Rechte werden vom LogoDIDACT-Server für die automatisierte Konfiguration von Azure-AD, Sharepoint, Exchange und Teams übernommen.



VI.4.1.2. Vorteile

Die manuelle Administration von Azure-AD, Sharepoint, Exchange, Teams und weiterer (komplexer) Serverprodukte ist alles andere als trivial und erfordert neben tiefgehendem Know-how vor allem auch Zeit. Entscheidende Vorteile von **LD Azure Connect** ergeben sich aus der automatisierten Konfiguration und Administration dieser Systeme in Office 365.

Sie sparen Kosten sowohl bei der Ersteinrichtung als auch im Betrieb, weil der Großteil durch **LD Azure Connect** automatisch erledigt wird und Sie weniger Experten-Know-how einkaufen müssen. Die Vermeidung von Fehlern auf technischer und logischer Ebene erspart ebenfalls unnötige Kosten und Ärger.

Mit LD Azure Connect haben Sie die Gewissheit, dass die grundlegende Konfiguration der Dienste richtig ist und Sie Office 365 schnell und sicher einführen können. Die Ankopplung über **LD Azure**

Connect spart Ihnen und Ihrem Kollegium nicht nur viel Zeit und Nerven, sondern ermöglicht die einfache und sofortige Nutzung für alle Schüler*innen.

VI.4.1.3. Was macht der Connector LD Azure Connect

LD Azure Connect synchronisiert nicht nur Benutzerkonten und Anmeldedaten vom LogoDIDACT-Server zur Microsoft-Cloud, sondern übernimmt dort einen Großteil der Konfiguration für viele Dienste.

Für Endanwender maßgeblich sind dabei:

- Benutzername und Kennwort
- Gruppen inkl. Klassen und Projekte
- Gruppenzugehörigkeit inkl. Berechtigungen
- Lizenzen
- Richtlinienpakete

VI.4.2. Anmelden an Office 365

Um mit Office 365 arbeiten zu können, muss man im Wesentlichen nur den Einstiegspunkt von Microsoft kennen, den Namen der Anmelde-Domäne und seine individuellen Anmeldedaten, wie man diese an der Schule nutzt.



Tipp

Für den Zugang zur Microsoft Cloud und Office 365 benötigt man folgende URL:

`portal.office.com`

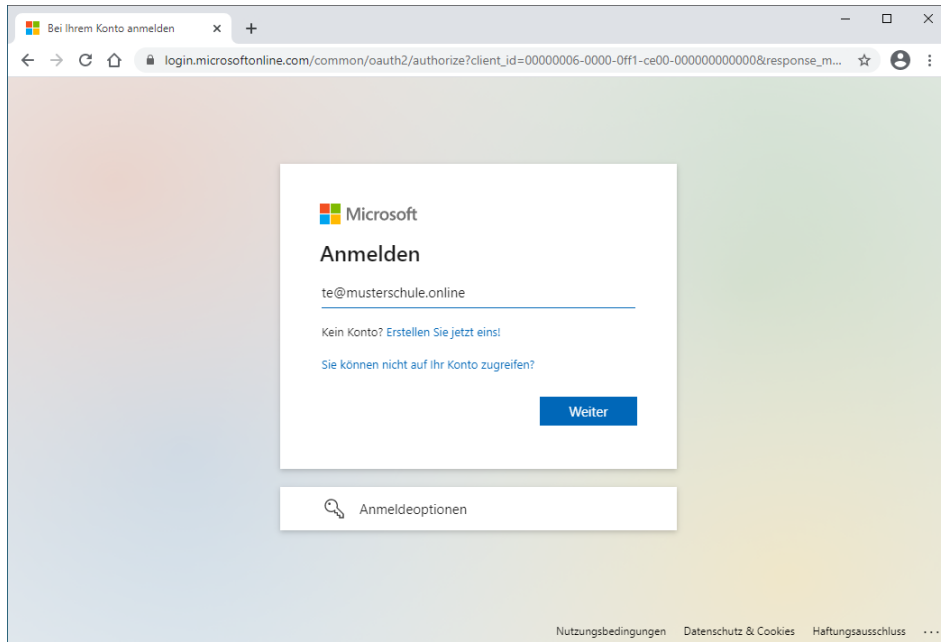
Melden Sie sich über das Webinterface mit Ihrem Lehrer- oder Schülerkonto nach folgendem Schema an:

anmeldename@domainname.online

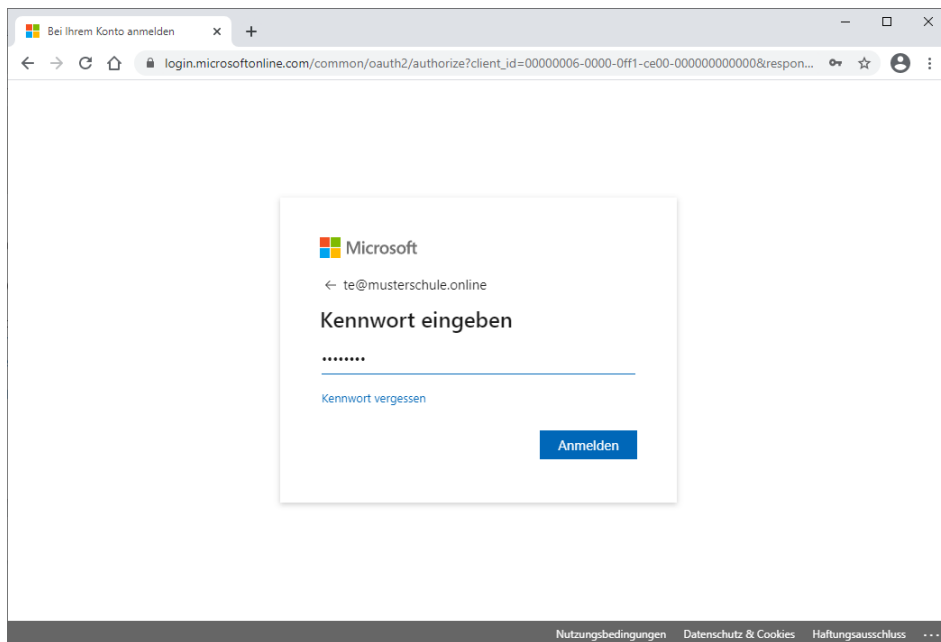
oder

anmeldename@domainname.schule

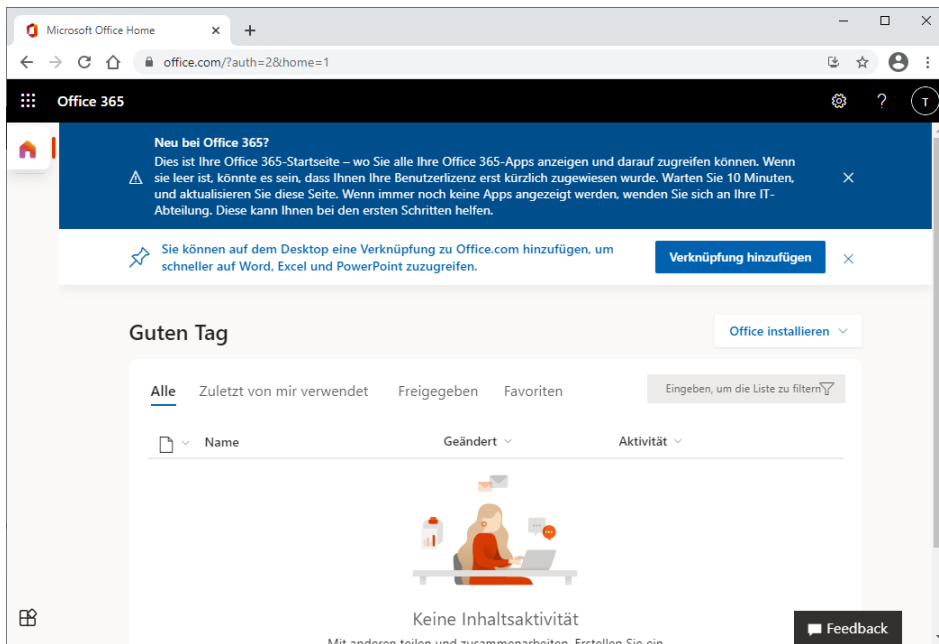
In unserem konkreten Beispiel der Musterschule Musterstadt meldet sich der Lehrer "Tom Engel" mit den gleichen Daten an, wie er diese vom lokalen LogoDIDACT-Netzwerk kennt, d.h. seinem Benutzernamen und dem Kennwort.



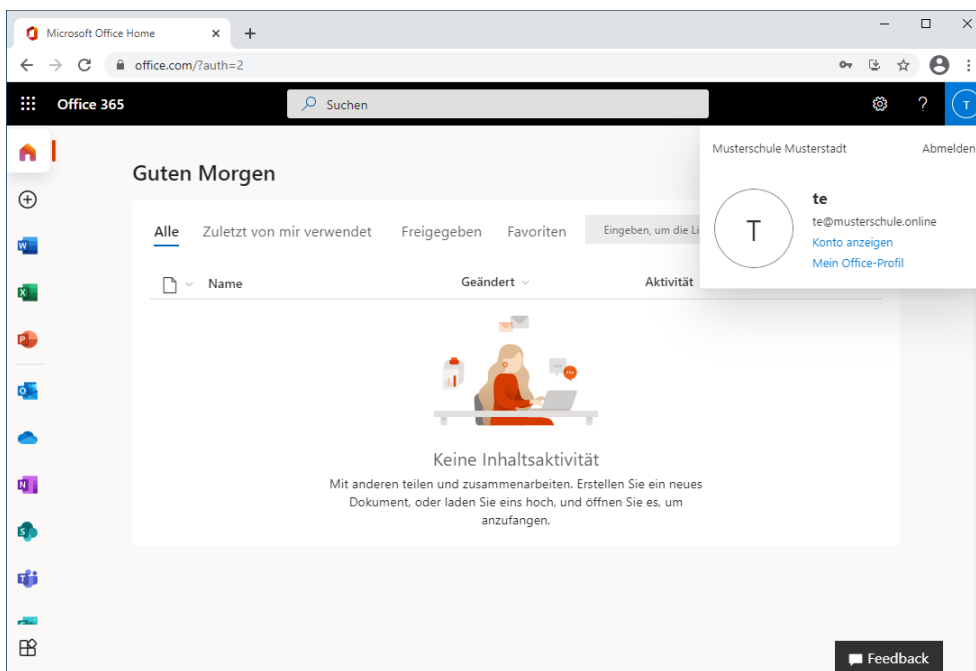
Sofern das Kennwort den Kennwortrichtlinien von Office 365 entspricht, erfolgt die Anmeldung. Wenn die zusätzliche Sicherheit nicht deaktiviert wurde, erhalten die Benutzer für eine Übergangszeit die Auswahl **Vorerst überspringen (in x Tagen ist dies erforderlich)**. Bitte wenden Sie sich in diesem Fall an den Administrator oder Dienstleister, der Ihre Microsoft 365 Umgebung verwaltet.



Nach erfolgreicher Anmeldung und Begrüßung kann es losgehen. Wenn das Konto über **LD Azure Connect** erst kürzlich angelegt wurde, erscheint eventuell eine Meldung, dass die APPs nicht angezeigt werden, weil die Lizenzen noch nicht zugewiesen wurden.

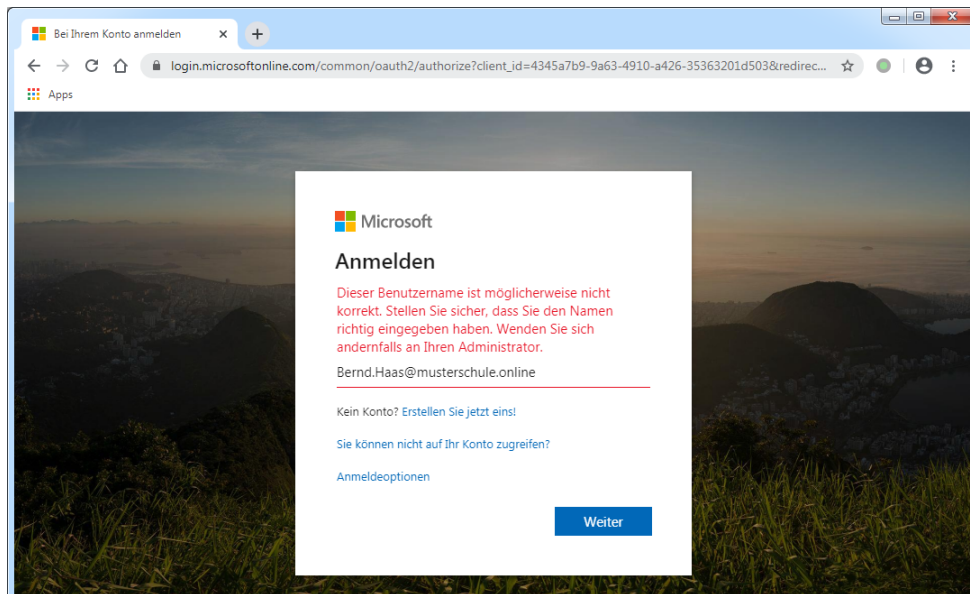


Sofern ihr Administrator im Control Center die richtigen Lizenzen zugewiesen hat und dieses vom LogoDIDACT-Server in die Microsoft-Cloud synchronisiert wurden, sehen Sie die APPs beim Login auf der linken Seite. Im rechten oberen Bereich können Sie sich abmelden oder Infos zu Ihrem Konto einsehen.



VI.4.2.1. Keine Anmeldung bei zu einfachem und kurzem Kennwort

Sofern ein Benutzer nicht in Azure-AD existiert, erhält man eine Fehlermeldung:



Der Grund für die Fehlermeldung liegt in der Regel darin, dass das bisherige Kennwort des Benutzers nicht den Anforderungen und Bedingungen der Microsoft-Cloud entspricht und deshalb dort erst gar nicht angelegt wurde.



Achtung

Ein Kennwort in Microsoft 365 muss:

1. eine Länge von mindestens **8 Zeichen** haben
2. einen **Großbuchstaben** enthalten
3. eine Zahl und ein **Sonderzeichen** enthalten

Eine weitere Besonderheit besteht darin, dass das Kennwort **nicht** den Anmeldenamen enthalten darf!

Dies ist insbesondere für Lehrerinnen und Lehrer wichtig zu beachten, weil deren Anmeldenamen in LogoDIDACT einem Kürzel entsprechen, das in der Regel an allen Schulen verwendet wird.

Der Lehrer "Tom Engel", dessen Kürzel und damit Anmeldeame **te** lautet, darf also in seinem Kennwort diese Buchstabenfolge nicht verwenden!

VI.4.2.2. Kennwort- Sicherheit und Komplexität

Wenn Sie mit Diensten wie Office 365, Teams oder Nextcloud arbeiten, die über das Internet von überall aus zu jeder Zeit erreichbar sind, müssen Sie sich zwingend mit dem Thema Kennwortsicherheit beschäftigen.

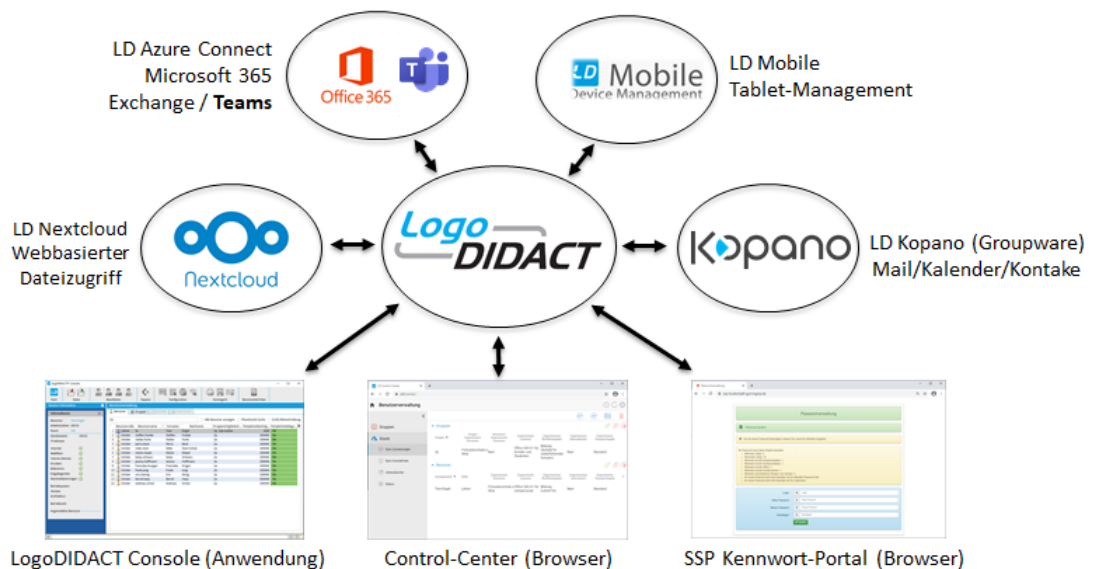
Setzen Sie sich schulintern mit dem Administrator oder Ihrem LogoDIDACT-Partner in Verbindung, um die Kennwortrichtlinien im lokalen LogoDIDACT Netz anzupassen und im ersten Schritt das Kollegium für dieses extrem wichtige Thema zu sensibilisieren!

Im Anschluss müssen Sie den Schülerinnen und Schülern dieses Thema und seine Bedeutung ebenfalls klarmachen.

VI.4.2.3. Der LogoDIDACT-Server ist die Zentrale für Benutzer-Identitäten

So wichtig wie das Verständnis zur Bedeutung von Kennwörtern für die Sicherheit der Daten und Identitäten von Schülern und Lehrern ist auch die Kenntnis, wie die Systeme miteinander zusammenhängen.

In der folgenden Grafik kommt gut zum Ausdruck, dass alle Systeme an LogoDIDACT angekoppelt sind.



Der LogoDIDACT-Server ist die Zentrale für das gesamte Benutzermanagement für alle Module.



Achtung

1. Alle Systeme sind an die Benutzerverwaltung von LogoDIDACT angekoppelt.
2. Benutzer, Kennwörter, Klassen, Gruppen, Projekte sind in allen Modulen verfügbar.
3. Mit LogoDIDACT erfolgt eine automatisierte Konfiguration aller Module.

Aus obiger Konstellation ergeben sich grundlegend wichtige Erkenntnisse:

1. Kennwortänderung per Browser nur über das SSP

Sie können das Kennwort **nicht** in Office 365 ändern, sondern ausschließlich über das SSP Kennwort-Portal (siehe unten). Jede Kennwortänderung direkt in Microsoft 365 wird über die Synchronisation von **LD Azure Connect** wieder rückgängig gemacht und auf den Wert gesetzt, der in der zentralen Benutzerverwaltung von LogoDIDACT vorhanden ist.

2. Verschiedene Systeme haben verschiedene Kennwortrichtlinien

Ein Kennwort in Microsoft 365 darf keine Umlaute (ä,ö,ü usw.) enthalten, weshalb das SSP bereits so konfiguriert ist, dass es diese Zeichen ebenfalls nicht annimmt, obwohl diese im lokalen LogoDIDACT-Netz zulässig wären.

Möglicherweise müssen die lokalen Kennwortrichtlinien im LogoDIDACT-Netzwerk beim Einsatz der Microsoft Cloud noch auf einen höheren Sicherheits-Standard angepasst werden.

3. Keine Kontoerstellung in der Microsoft-Cloud bei zu schlechtem Kennwort

Wenn sich ein Benutzer mit seinem bisherigen Kennwort im lokalen LogoDIDACT-Netz anmelden kann aber nicht in der Microsoft-Cloud, liegt die Ursache in 99% der Fälle in einem zu schlechten Kennwort. Bei zu schlechtem Kennwort wird das Benutzerkonto in der Microsoft-Cloud erst gar nicht angelegt.

4. Keine Kontoerstellung in der Microsoft-Cloud wegen nicht erlaubter Zeichen im Kennwort

Ein Konto wird auch dann nicht in Microsoft 365 angelegt, wenn es gut und hinreichend komplex ist aber unerlaubte Zeichen wie Umlaute oder den bereits oben erwähnten Benutzernamen (im Beispiel **te**) enthält.

VI.4.2.4. Empfohlene Kennwort-Komplexität

Für die Generierung sicherer und hinreichend komplexer Kennwörter gibt es in LogoDIDACT schon immer klare Empfehlungen.

Diese waren in der Vergangenheit ausgelegt auf die Sicherheit im LAN, d.h. im lokalen Schulnetz ohne Zugang von außen und ohne Ankopplung an externe Systeme.

Die Standardvorgabe für die Erzeugung eines Kennwortes lag bei einer Länge von 5 Zeichen, gebildet aus 2 Silben mit je 2 Kleinbuchstaben, gefolgt von einer Zahl, also z.B. **rubu4** oder **kose2**.

Für die Ankopplung an die Microsoft Cloud oder auch für den externen Zugriff auf webbasierte Dienste am LogoDIDACT-Server muss diese Richtlinie angepasst werden.

Auch hier gibt es eine klare Empfehlung, die darin besteht, an der aussprechbaren Varinate **phone-mic(5)** festzuhalten aber diese zu verdoppeln und durch ein Sonderzeichen zu trennen. Der erste Buchstabe ist nun ein Großbuchstabe, so dass bei einem solchen neu generierten Initial-Kennwort die Kriterien im Hinblick auf die Länge und Komplexität in jedem Fall erfüllt sind.

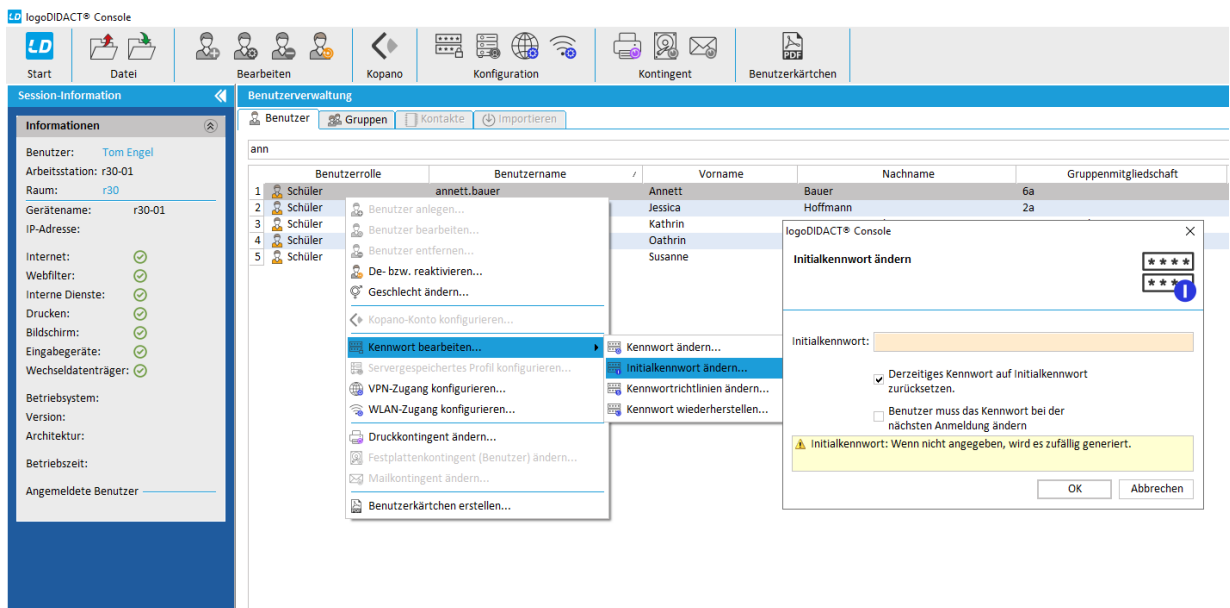
In der folgenden Grafik wird veranschaulicht, wie sich die Änderung der Passwort-Komplexität auf das Initialkennwort auswirkt.



Wenden Sie sich an Ihren Administrator bzw. LogoDIDACT-Partner, so dass dieser die Generierung von Initial-Kennwörtern im System entsprechend anpasst, wie dies in Abschnitt III.4.12.2.1, „Komplexität für generierte Kennwörter“ beschrieben ist.

Nach der Anpassung, können Sie über die LogoDIDACT-Console den Schülerinnen und Schülern ein neues hinreichend langes und komplexes Kennwort generieren, so dass der Zugang zu Microsoft 365 möglich ist.

Wählen Sie dazu im Modul der Benutzerverwaltung einen einzelnen Benutzer oder eine ganze Klasse aus und wählen Sie aus dem Kontextmenü den Eintrag **Kennwort bearbeiten...** und dort den Unterpunkt **Initialkennwort ändern...**



Wenn Sie die voreingestellten Häkchen gesetzt lassen und den Dialog mit **OK** bestätigen, passiert genau das, was gewünscht ist. Es wird ein neues zufälliges Kennwort nach dem neu festgelegten Schema generiert und dieses sowohl im Live-System als Kennwort gesetzt, als auch als Initial-Kennwort. Letzteres ist deshalb wichtig, weil die Schülerinnen und Schüler irgendwie an ihr Kennwort gelangen müssen und dies über den Ausdruck der Karteikärtchen erfolgt auf denen nur Initial-Kennwörter angezeigt werden können!

VI.4.2.5. Das SSP Portal zum Ändern des Kennwortes

Um das Kennwort den Richtlinien von Office 365 anzupassen, gibt es in LogoDIDACT das Portal zum Ändern des Kennworts. Das SSP-Portal (Self-Service-Passwort) ist von außen erreichbar über

<https://ssp.schulname.logoip.de>

Der dynamische DNS-Dienst [.logoip.de](https://www.logoip.de) steht allen LogoDIDACT Kunden mit aktiver Softwarepflege kostenfrei zur Verfügung und wird von vielen Schulen auch für andere Dienste wie z.B. Nextcloud, Kopano oder Moodle genutzt.

Wählen Sie sich auf dem Portal mit Ihrem Benutzernamen und dem bisherigen Kennwort ein. Dies ist im folgenden Beispiel für den Benutzer Bernd Haas exemplarisch dargestellt.

Passwortverwaltung

ssp.musterstadt-gym.logoip.de

Apps

Passwortverwaltung

Passwort ändern

Um ein neues Passwort festzulegen müssen Sie zuerst Ihr aktuelles eingeben.

Ihr Passwort muss diese Regeln beachten:

- Minimale Länge: 8
- Maximale Länge: 16
- Minimale Anzahl Kleinbuchstaben: 1
- Minimale Anzahl Großbuchstaben: 1
- Minimale Anzahl Ziffern: 1
- Minimale Anzahl Sonderzeichen: 1
- Minimum verschiedener Klassen von Zeichen: 2
- Ihr neues Passwort darf nicht dasselbe wie Ihr aktuelles Passwort sein
- Ihr neues Passwort darf nicht dasselbe wie Ihr Loginname

Login

Altes Passwort

Neues Passwort

Bestätigen

Vergeben Sie ein neues Kennwort mit mindestens 8 Zeichen Länge, mindestens einer Zahl, einem Großbuchstaben und einem Sonderzeichen.

Passwortverwaltung

ssp.leingarten-eps.logoip.de/#

Apps

Passwortverwaltung

Ihr Passwort wurde erfolgreich geändert



Achtung

Zunächst wird dadurch das Kennwort lokal auf dem LogoDIDACT-Server geändert.

Alle 5 Minuten wird die Synchronisation zu Office 365 geprüft und Konten in der Cloud angelegt, sofern die Kennwort-Richtlinien stimmen.

Es kann also etwa 10 Minuten dauern, bis Sie sich in Office 365 anmelden können.

VI.4.3. Der richtige Umgang mit Teams

Wir können in einem Handbuch für LogoDIDACT nicht im Detail den Umgang mit Fremdprodukten wie Microsoft Teams oder gar der gesamten Microsoft 365 Plattform erklären, geschweige denn, wie Sie damit Ihren digitalen Unterricht gestalten.

Was wir Ihnen aber sehr bewusst und gezielt in den folgenden Abschnitten erklären wollen, ist die Ankopplung über **LD Azure Connect** und wie er Sie vor Stress und Ärger bewahrt.

Das Ziel unseres Konnektors besteht darin, Sie vor Fehlern zu bewahren, Sie von unnötigen Arbeiten zu entlasten und Ihnen klare Empfehlungen mit auf den Weg zu geben, die Ihnen in der Praxis beim digitalen Unterricht helfen.

VI.4.3.1. Besprechungs-Richtlinien

Über so genannte Richtlinien-Pakete bestimmt Ihr Administrator des Netzwerkes, wer in einer Teams-Besprechung welche Rechte und damit auch Möglichkeiten hat:

- wer darf an einer Sitzung teilnehmen
- wer darf den Wartebereich umgehen
- wer darf präsentieren bzw. seinen Bildschirm teilen

Jeder Benutzer der eine Teams-Sitzung einstellt, hat grundsätzlich die Möglichkeit diese Standard-Einstellungen unmittelbar nach der Einplanung seiner Besprechung individuell anzupassen.

Ein Großteil des Kollegiums an Schulen hat jedoch zu wenig praktisches Know-how im Umgang mit IT und der grundlegenden Bedienung von Besprechungen in Microsoft Teams. Dies kann dann zu einem Missbrauch derart führen, dass z.B. fremde Personen anonym am Unterricht teilnehmen oder gar jugendgefährdende Inhalte und Dokumente verteilen.



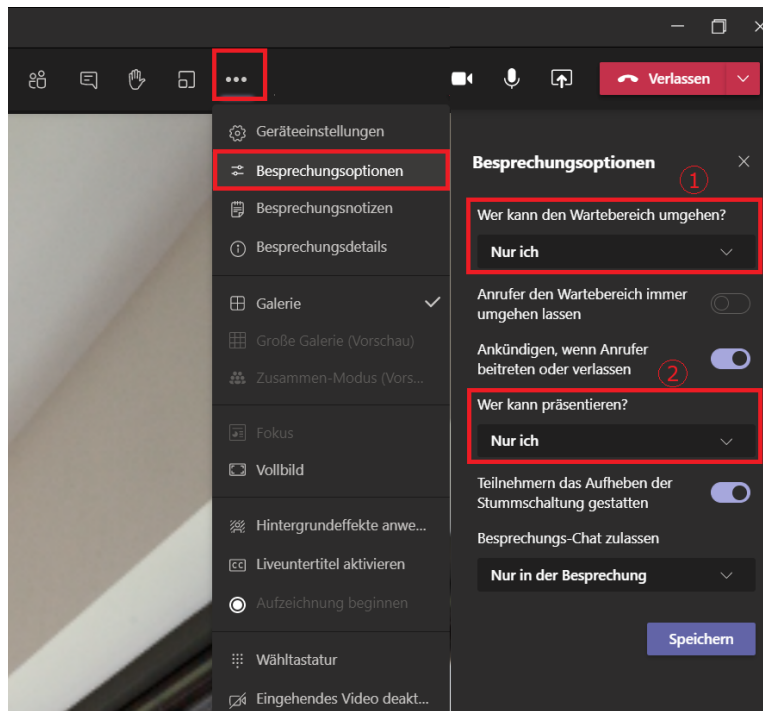
Achtung

Um die Schulen vor Missbrauch von Teams-Besprechungen zu schützen, überschreibt **LD Azure Connect** die folgenden beiden Einstellungen für Besprechungen, unabhängig vom gewählten Richtlinienpaket:

- nur der Besprechungs-Organisator kann den Wartebereich umgehen
- nur der Besprechungs-Organisator kann präsentieren

In der neuesten Version von **LD Azure Connect** besteht die Möglichkeit, alle diese Einstellungen individuell pro Schule anzupassen. Dies erfolgt auf Ebene von Puppet und wird in Abschnitt III.9.5, „Besprechungs-Richtlinien in Teams anpassen“ beschrieben.

Alle anderen Optionen werden so gesetzt, wie das über das zugewiesene Microsoft-Richtlinienpaket im ControlCenter eingestellt ist. In der Praxis führt dies nicht wirklich zu einer Einschränkung, da die Besprechungsoptionen selbstverständlich in der Sitzung angepasst werden können. Grundvoraussetzung dafür ist natürlich, dass sich die Schulen im Umgang mit Teams auseinandersetzen.



Einstellungen 1 und 2 werden von LD Azure Connect als Standard für jede Teams-Besprechung gesetzt und "überschreiben", den im Richtlinienpaket definierten Wert.

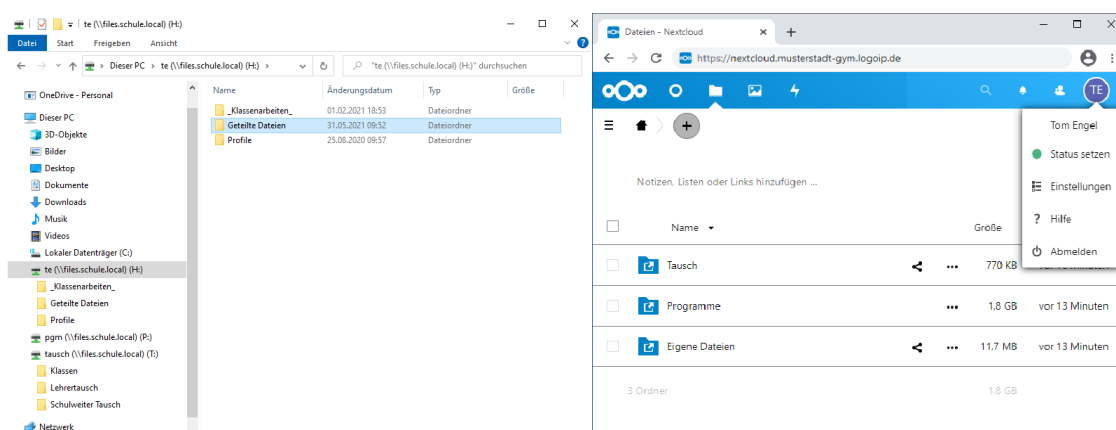
Alle anderen Optionen bleiben so gesetzt, wie das über das zugewiesene Microsoft-Richtlinienpaket im ControlCenter eingestellt ist.

Kapitel VI.5. Nextcloud

VI.5.1. Nextcloud in LogoDIDACT

In LogoDIDACT wird das Modul Nextcloud per Standard an das gleiche Speichersystem angekoppelt, das die Benutzer bereits im lokalen System nutzen und kennen. Dieser so genannte Objektspeicher nutzt also die intern an der Schule vorhandenen Freigaben (Samba Shares), so dass für die Anwender eine relativ einfache Zuordnung möglich ist. Alles was lokal im Laufwerk H:\ liegt, findet sich in Nextcloud unter **Eigene Dateien**.

Entsprechendes gilt für das Laufwerk T:\ mit der Freigabe **Tausch** und P:\ mit der Freigabe **Programme**. Dies ist in folgender Grafik exemplarisch für den Lehrer "Tom Engel" dargestellt, wobei auf der linken Seite die Ansicht an einem Computer innerhalb der Schule mit den Laufwerksbuchstaben zu sehen ist und auf der rechten Seite die Ansicht in Nextcloud per Webbrowser.



VI.5.1.1. Zugriff auf Nextcloud

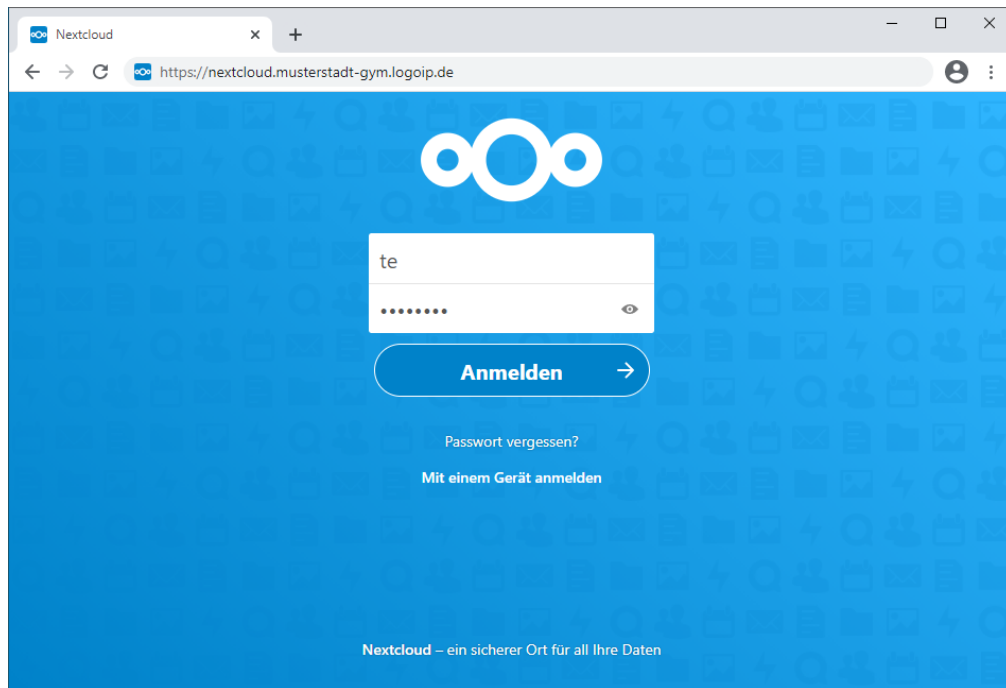
Der Zugriff auf Nextcloud erfolgt per Webbrowser entweder direkt an der Schule oder von jedem beliebigen Ort aus, sofern ein Internetzugang vorhanden ist.

Der Zugriff von außen erfolgt über:

<https://nextcloud.SCHULKUERZEL.logoip.de>

Im Beispiel der Musterschule lautet das Schulkürzel **musterstadt-gym**, so dass man die Nextcloud dieser Schule über die entsprechende Adresse erreicht:

<https://nextcloud.musterstadt-gym.logoip.de>



Im lokalen Netzwerk der Schule genügt die Kurzform:

`https://nextcloud/`

VI.5.1.2. Anmeldung und Voraussetzung

Die Anmeldung an der Nextcloud erfolgt mit exakt den gleichen Zugangsdaten, wie Sie diese von der Schule her kennen, d.h., dem Anmeldenamen und zugehörigem Kennwort. Für Lehrer*innen ist der Anmeldenamen in der Regel das Kürzel, für Schüler in der Standardeinstellung "vorname.nachname".



Achtung

Wenn Sie sich trotz korrekter Eingabe von Benutzernamen und Kennwort nicht anmelden können, liegt das in der Regel daran, dass Sie noch nicht Mitglied der Gruppe **ld-sg-nextcloud** sind.

Wenden Sie sich in diesem Fall an Ihren Administrator bzw. an diejenige Person, welche an der Schule für das Benutzermanagement zuständig ist. Weitere Infos finden Sie unter Abschnitt III.10.6, „Zugriff auf Nextcloud erlauben“.

VI.5.1.3. Teilen von Dokumenten

Für das Teilen von Dokumenten gibt es verschiedene Möglichkeiten, deren Nutzung aber entscheidend von Ihrer Umgebung und der aktivierten Dienste abhängt. Sie können Dokumente verständlicherweise nur per E-Mail teilen, wenn auf Ihrem Server diese Dienste von Ihrem Partner konfiguriert wurden.

VI.5.1.3.1. Keine Verwendung interner Links

Leider zeigt die Nextcloud-Oberfläche Menüs und Funktionen an, die in bestimmten Umgebungen nicht sinnvoll sind, weil sie gar nicht funktionieren können. Hierzu gehört z.B. die Möglichkeit Dateien oder auch Ordner per internem Link anderen Benutzern zuzusenden.



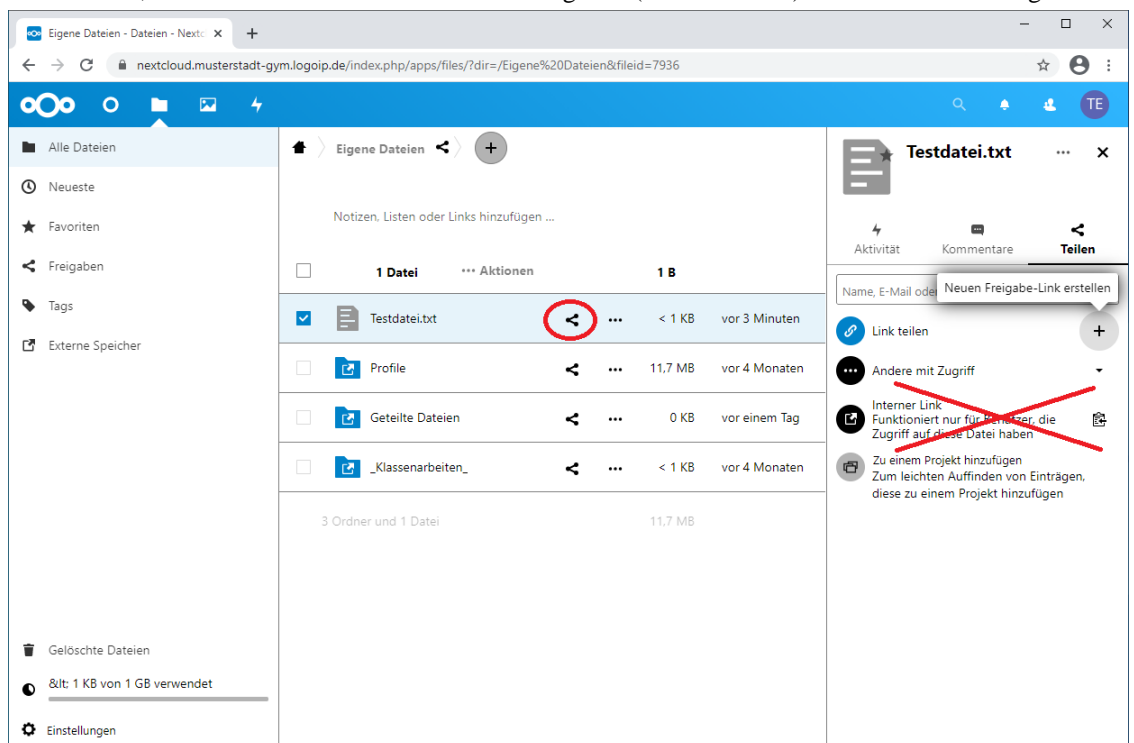
Achtung

Im Standardmodus der Nexcloud mit dem Zugriff auf Ordner- und Verzeichnisstrukturen können Benutzer keine Dokumente per internem Link verteilen!

Diese Funktionalität ist in diesem Betriebsmodus von Nextcloud weder sinnvoll noch technisch möglich!

Verwenden Sie deshalb nur "Link teilen" oder Freigaben für Benutzer oder Gruppen.

Leider lässt sich die Funktion "Interner Link" in der graphischen Oberfläche von Nextcloud nicht deaktivieren, obwohl sie im Betriebsmodus mit Freigaben (Samba Shares) vollkommen unsinnig ist.

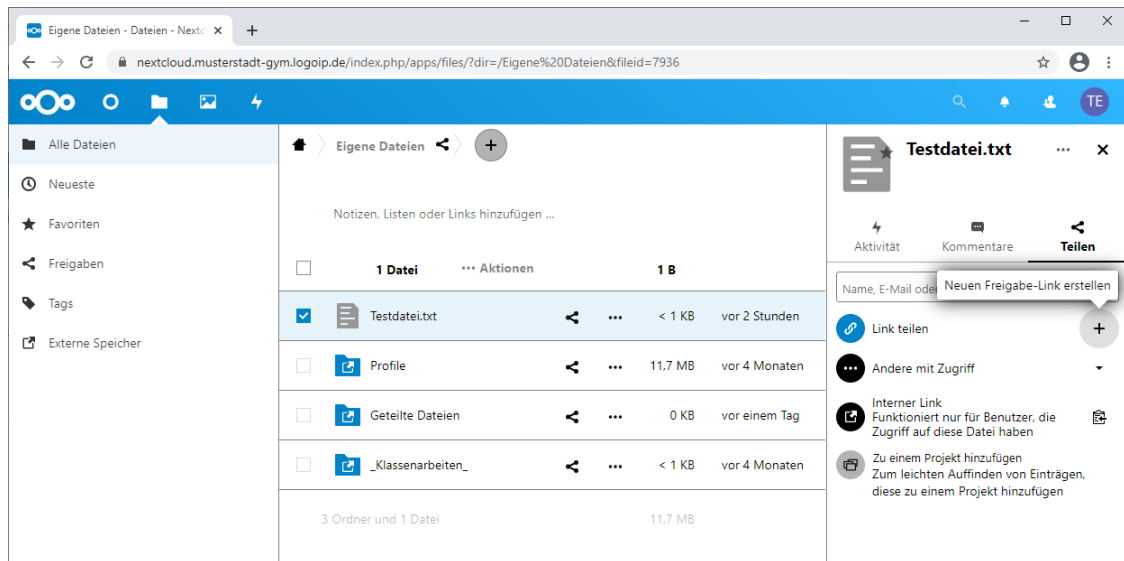


Auf technischer Ebene wird bei "Interner Link" eine URL erstellt, welche eine benutzergebundene FileID beinhaltet. Ein anderer Benutzer kann mit diesem Link nichts anfangen.

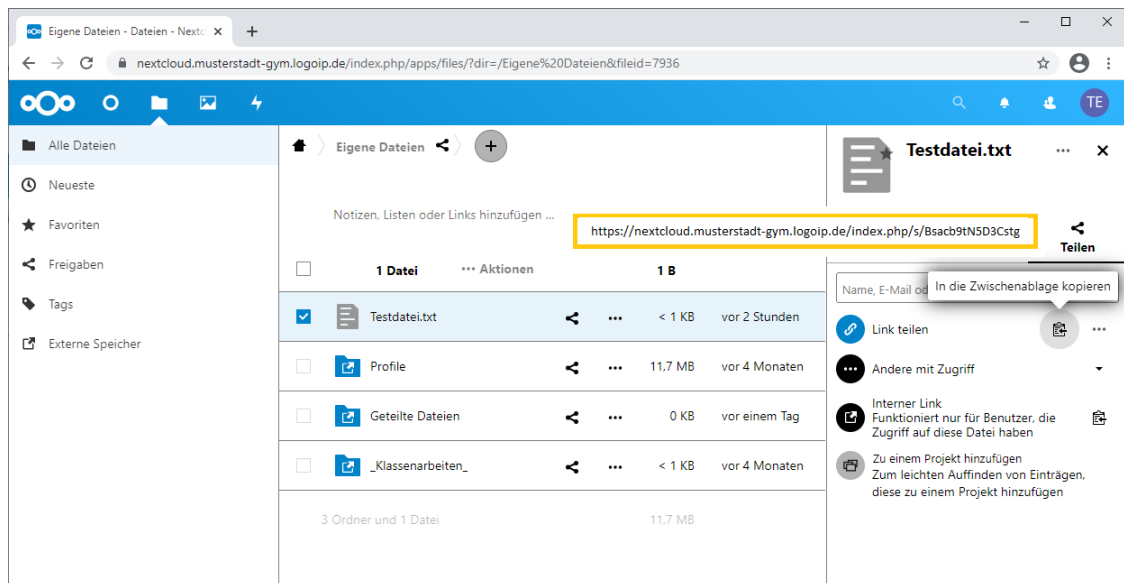
VI.5.1.3.2. Dokumente richtig teilen per Link

Es gibt zwei Möglichkeiten, wie in Nextcloud Dokumente richtig geteilt bzw. gemeinsam bearbeitet werden können.

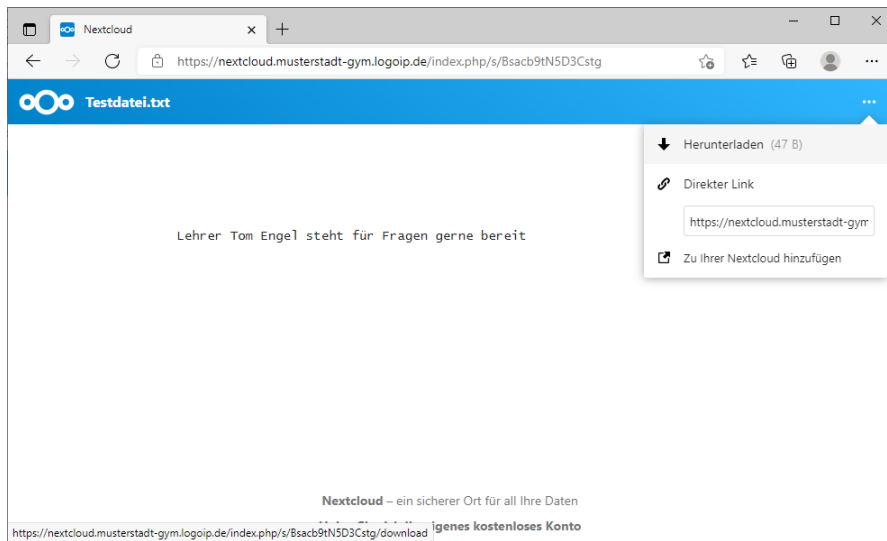
Bei "Link erstellen" hingegen wird eine URL erzeugt, welche die Anmeldeinformationen des Benutzers (User Credentials) in verschlüsselter Form beinhaltet, so dass man über diesen Link auf die Datei problemlos zugreifen kann.



Nachdem man im ersten Schritt über das "+" Symbol den Link auf die zuvor ausgewählte Datei erstellt hat, erscheint nach wenigen Sekunden die Möglichkeit den Link in die Zwischenablage zu kopieren.



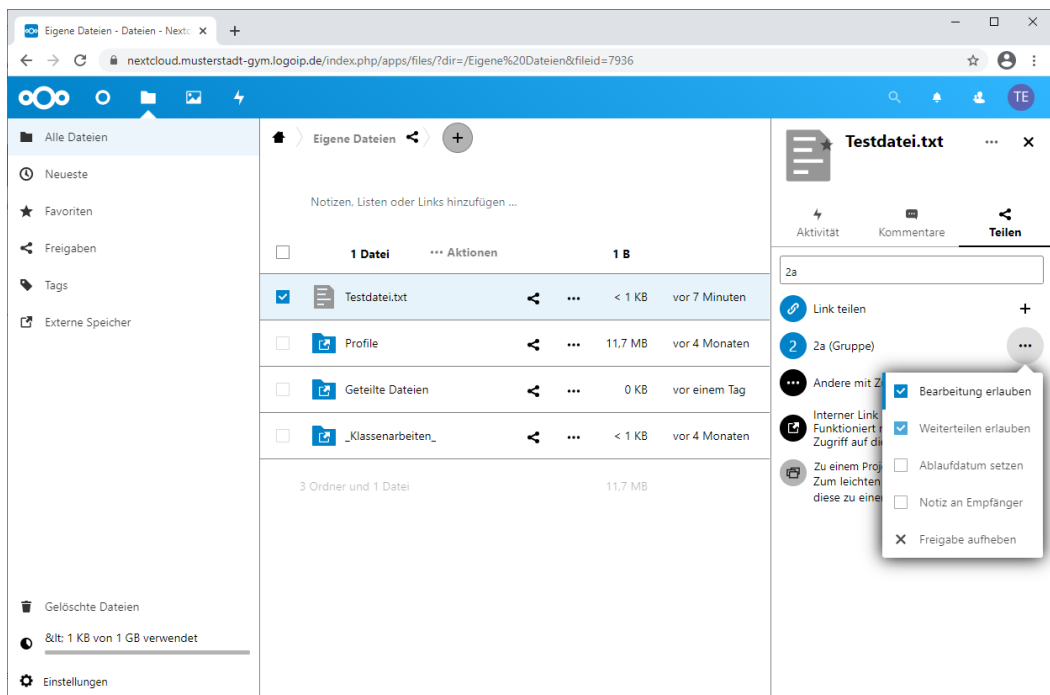
Vollkommen unabhängig davon, wem Sie diesen Link zusenden, kann diese Person in einem Web-Browser ohne Login auf die von Ihnen bereitgestellte Datei zugreifen und diese herunterladen.



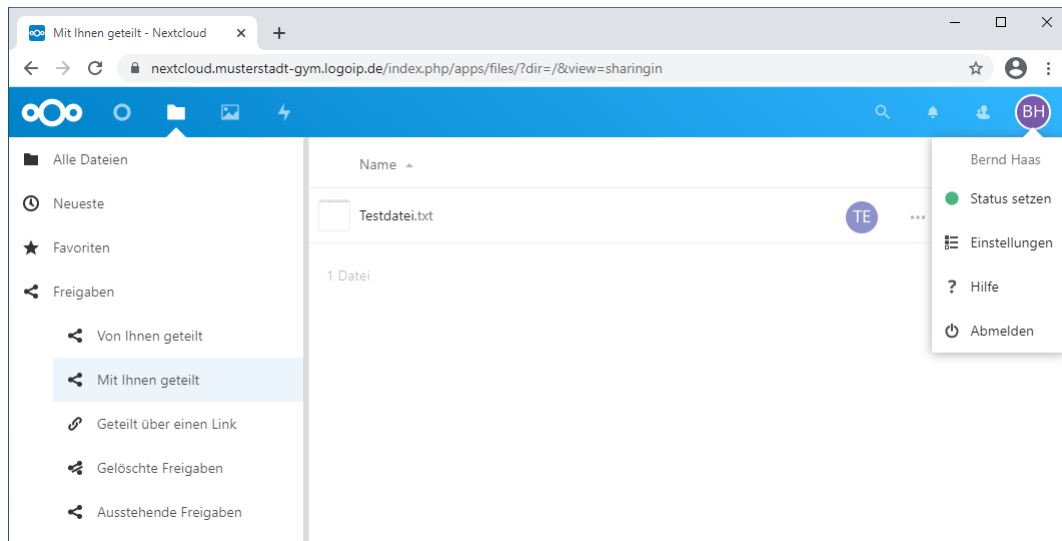
VI.5.1.3.3. Dokumente richtig teilen per Freigabe

Deutlich praktikabler und passender für das Bereitstellen z.B. von Hausaufgaben oder Arbeitsmaterialien ist die Verwendung von Freigaben für einzelne Benutzer oder Gruppen bzw. Klassen.

Um beispielsweise ein Dokument für eine Klasse bereitzustellen, wählt man dieses aus und geht auch dort wieder auf das Symbol zum Teilen. Im Suchfenster des Teilen-Dialogs gibt man dann z.B. die Klasse an, die das Dokument erhalten soll, in diesem Fall die Klasse 2a. Über das Symbol ... neben der Gruppe lässt sich einstellen, ob die Mitglieder das Dokument bearbeiten können sollen oder wie lange die Freigabe gelten soll. Ebenso lässt sich eine Notiz an die Empfänger senden.



Ein Schüler der Klasse 2a, in unserem Beispiel Bernd Haas, sieht das vom Lehrer Tom Engel freigegebene Dokument in seiner Nextcloud-Umgebung im Menü **Freigaben** unter **Mit Ihnen geteilt**.



VI.5.1.4. Arbeiten mit Nextcloud und Collabora

Die vorherigen Abschnitte beinhalten einige wesentliche Infos für die Verwendung von Nextcloud.



Tipp

Speziell zu Nextcloud und Collabora gibt es auch ein Schulungsvideo, das in nur 10 Minuten die wesentlichen Grundlagen im Umgang damit erklärt.

Dieses und viele weitere Videos finden Sie im Downloadbereich unter: <https://portal.sbe.de/support/schulungsvideos/>.

Kapitel VI.6. Webdienste

VI.6.1. Content Management System

Drupal ist ein Open Source bzw. quelloffenes Content Management System (CMS) und Framework mit dem sich Inhalte im Internet veröffentlichen und verwalten lassen. Im Vergleich zu anderen CMS wie z.B. Joomla! oder TYPO3 eignet es sich besonders für den Aufbau von Online Communities, die gemeinsam an Inhalten arbeiten und sich über Themen austauschen und informieren wollen. Drupal ist Freie Software und steht unter der GNU General Public License (GPL). Für weitere Informationen besuchen Sie bitte die Projektseite im Internet unter <http://drupal.org/>.



Abbildung VI.6.1. Projektseite drupal.org

VI.6.1.1. Erste Schritte

Drupal zeichnet sich durch ein hohes Maß an Anwenderfreundlichkeit aus und lässt sich so auch ohne Programmier- oder HTML-Kenntnisse bedienen.

VI.6.1.1.1. Inhalte erzeugen

Rufen Sie Ihre Drupal Installation über die Adresse `http://cms/` in Ihrem Browser auf und melden Sie sich z.B. als Systemadministrator an. Wenn Sie Firefox als Browser verwenden, können Sie auch einfach Intranet aus der Lesezeichen-Symbolleiste wählen.

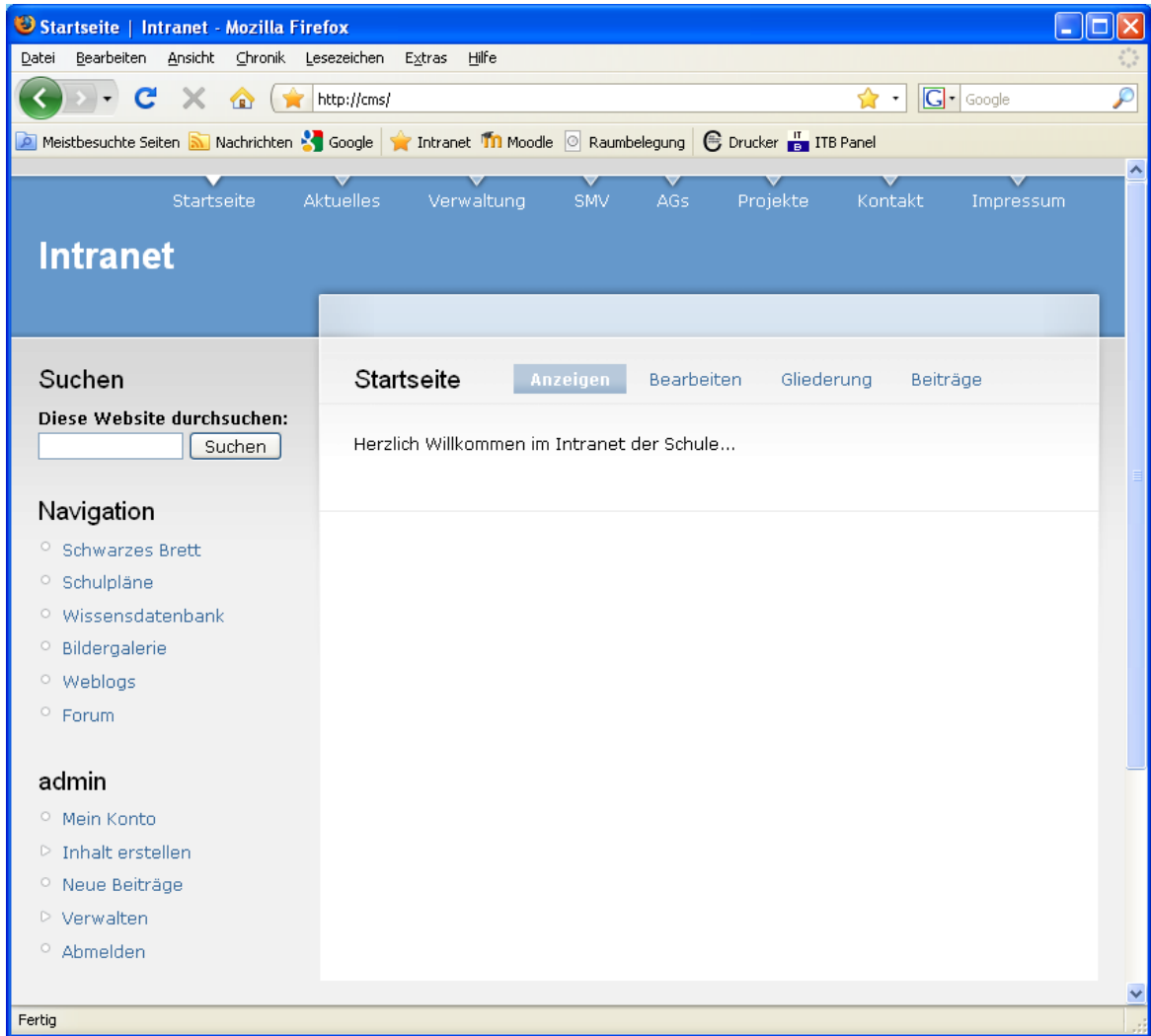


Abbildung VI.6.2. Startseite der Drupal Installation

Nachdem Sie sich erfolgreich angemeldet haben, navigieren Sie in Ihrem Benutzerblock zum Punkt **Inhalt erstellen** und wählen einen Inhaltstyp Ihrer Wahl z.B. Artikel. Sie erhalten ein Eingabeformular mit zahlreichen Auswahlmöglichkeiten, die aber allesamt selbsterklärend sind. Im Abschnitt **Menüeinstellungen** können Sie einen Menüpunkt erstellen und direkt mit dem Inhalt verknüpfen lassen.

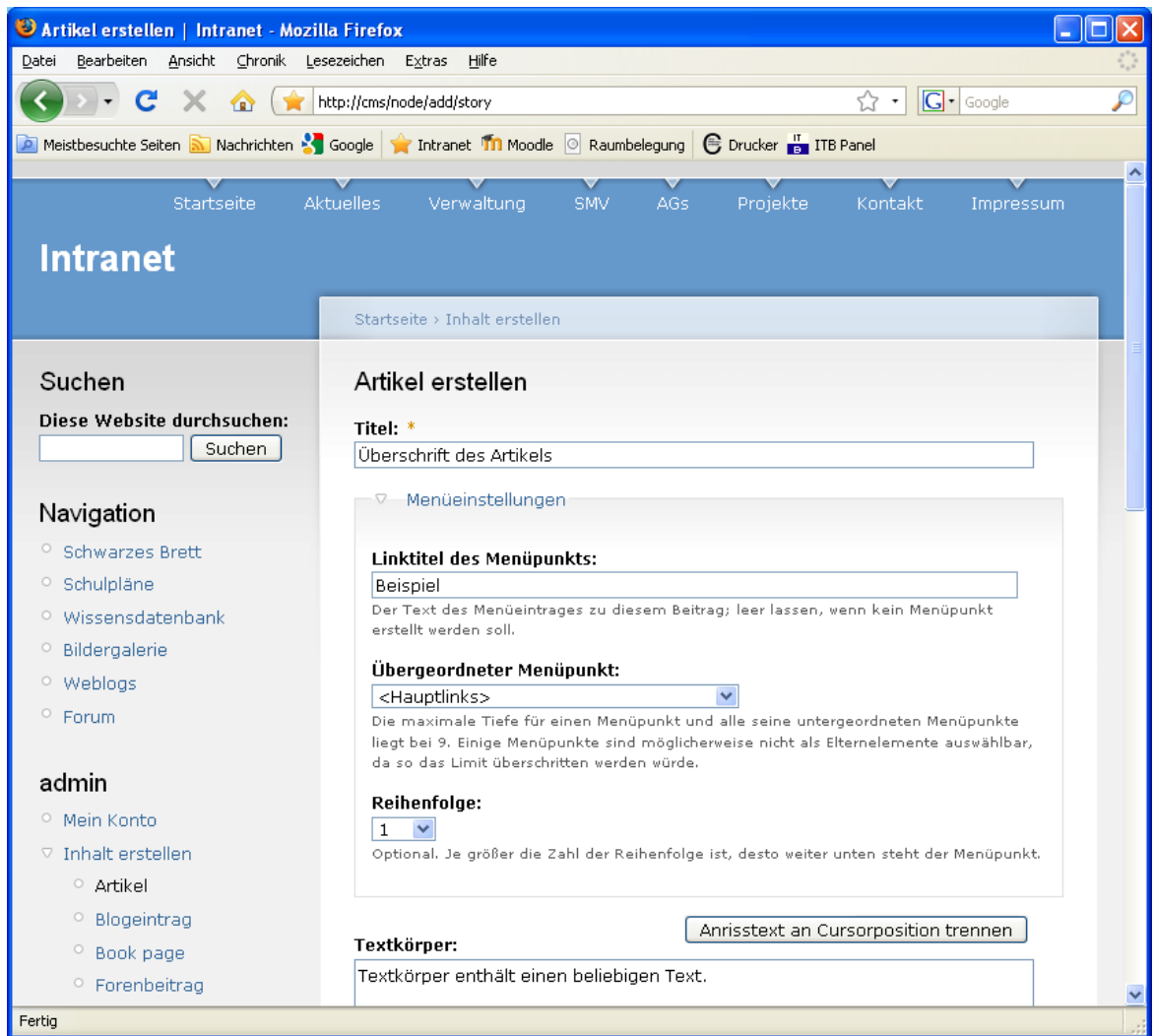



Abbildung VI.6.3. Menüeinstellungen für den Inhalt



Tipp

Sie können die Zuordnung zwischen Menüpunkt und Inhalt später jederzeit unter **Verwalten** → **Strukturierung** → **Menüs** ändern.

Geben Sie im Abschnitt **URL-Alias-Einstellungen** eine alternative URL an, mit der auf den Inhalt zugegriffen werden kann. Dieser Schritt ist optional, aber für suchmaschinenfreundliche URLs empfehlenswert.

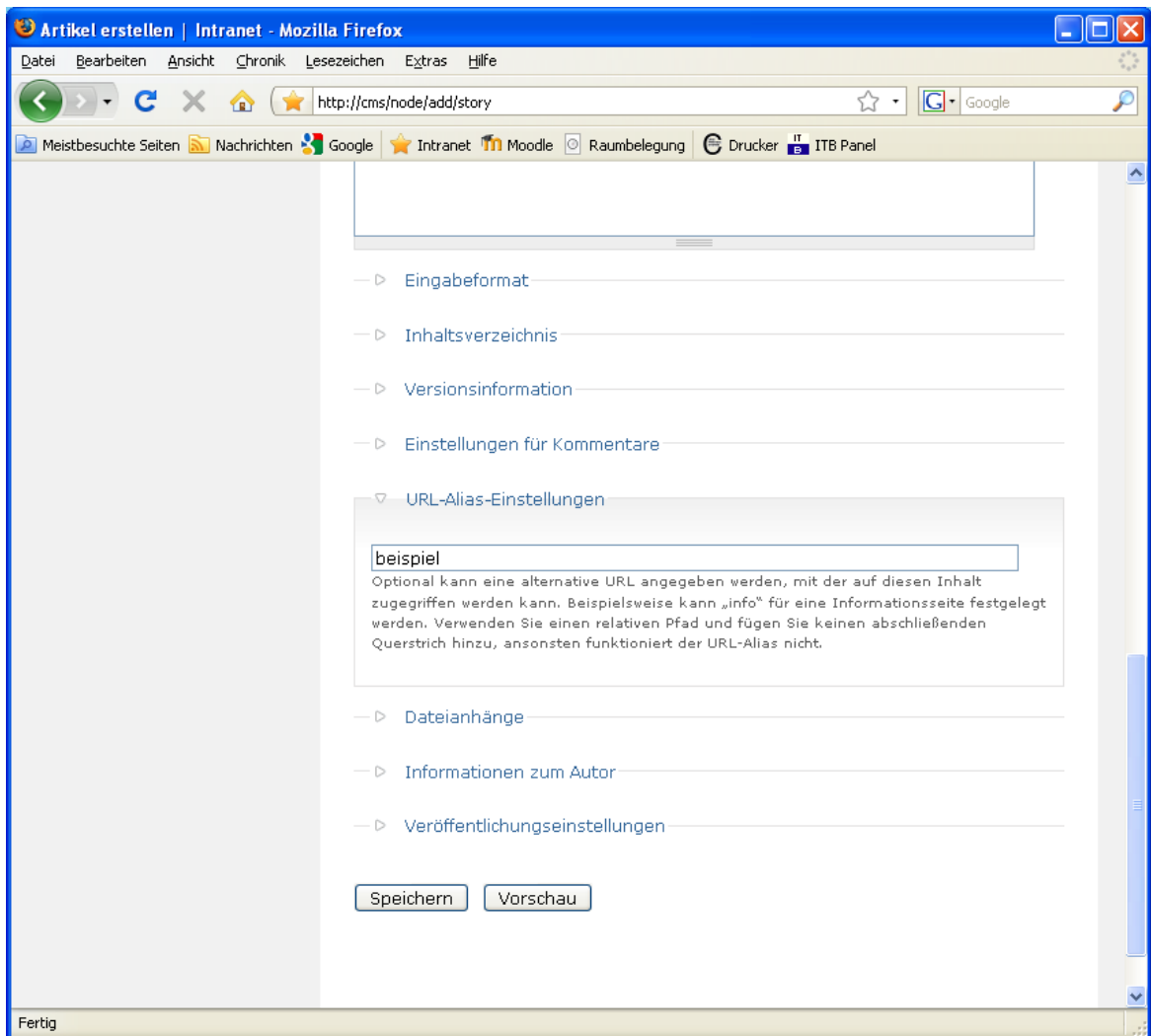


Abbildung VI.6.4. URL-Alias-Einstellungen für den Inhalt

Bevor Sie den Artikel durch Speichern veröffentlichen, sollten Sie sich den Inhalt über die Vorschau Funktion im Browser anzeigen lassen, um etwaige Flüchtigkeitsfehler wie ungeeignete Textformatierungen oder Rechtschreibfehler frühzeitig zu erkennen.

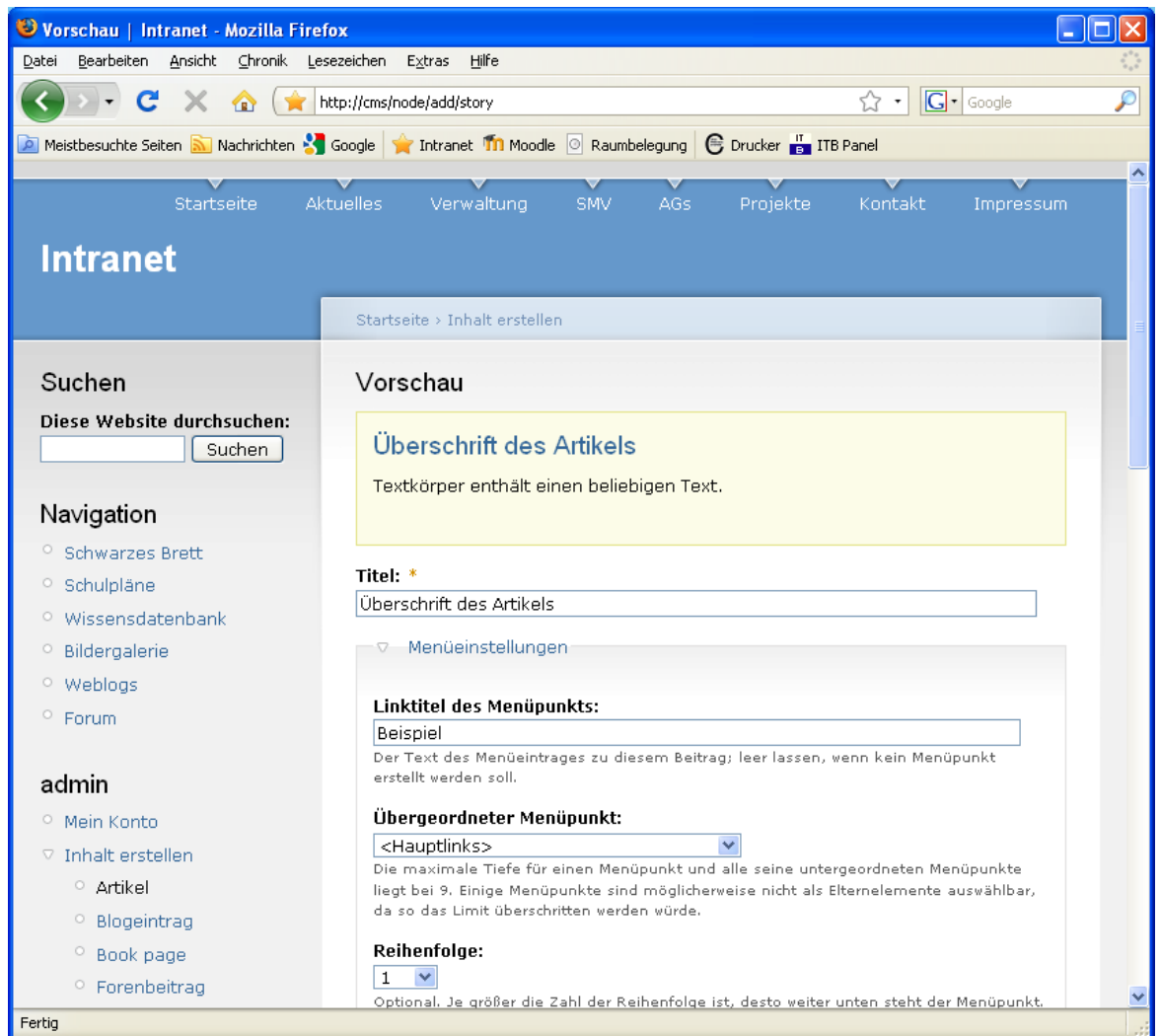


Abbildung VI.6.5. Vorschau des Inhalts

VI.6.1.1.2. Module einsetzen

Sie können Drupal mit Hilfe von Modulen in seiner Kernfunktionalität erweitern und so z.B. ohne großen Aufwand ein einfaches Forum nachrüsten. Module werden von der Drupal Entwicklergemeinde frei zur Verfügung gestellt und nachwirkend mit Bugfixes und Updates versorgt. In seiner Grundinstallation bietet Drupal bereits eine Vielzahl an zusätzlichen Modulen, die Sie lediglich zu aktivieren brauchen. Weitere Module können Sie kostenlos von der Projektseite im Internet unter <http://drupal.org/> herunterladen.

Navigieren Sie in Ihrem Benutzerblock zu **Verwalten** → **Strukturierung** → **Module**, um sich die mitgelieferten Module anzeigen zu lassen.

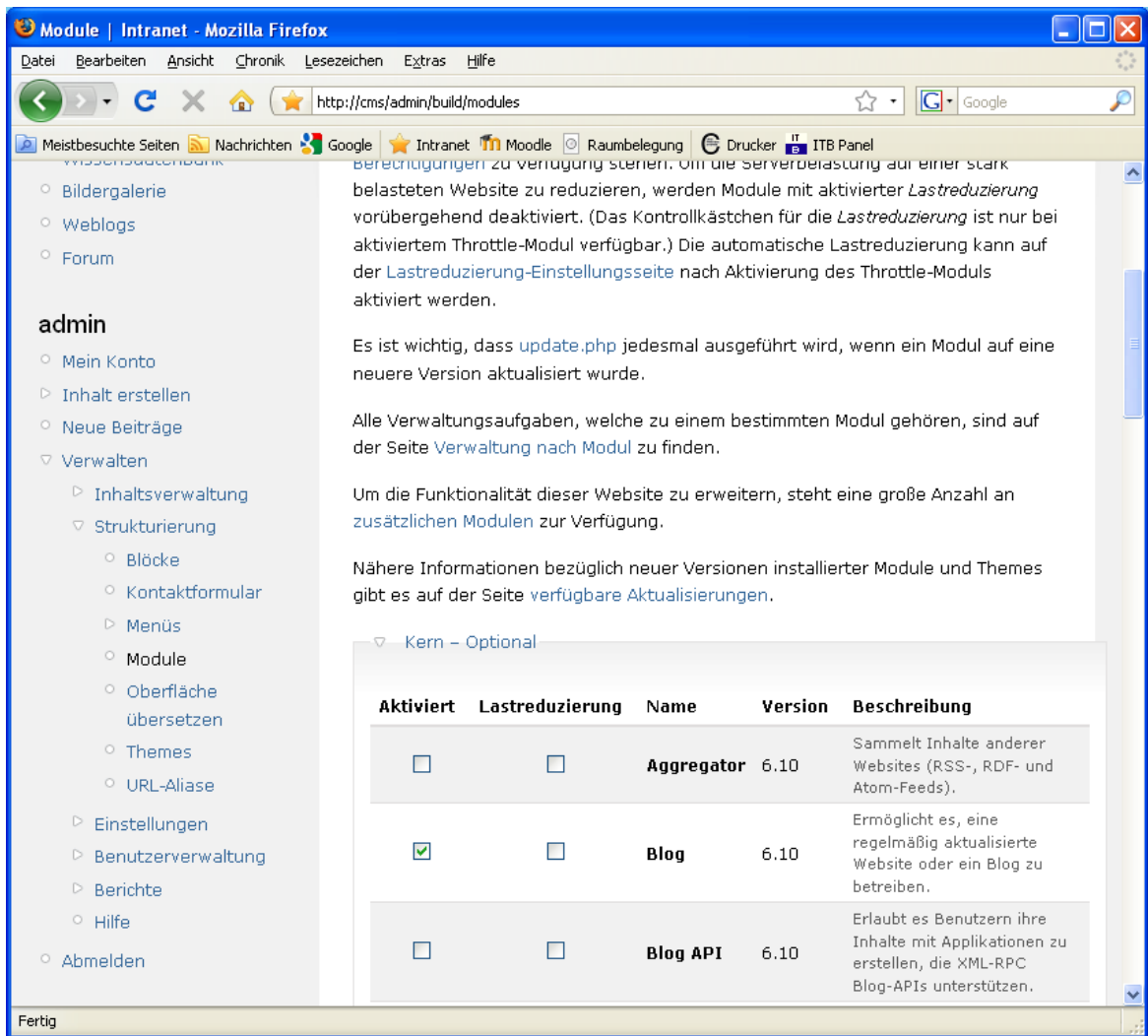



Abbildung VI.6.6. Übersicht der mitgelieferten Module

Für alle Module in dieser Ansicht liegen die Installationspakete bereits physikalisch im `modules` Verzeichnis Ihrer Drupal Installation bereit und brauchen nicht nachgereicht werden.



Tipp

Wenn Sie zusätzliche Module von der Projektseite unter <http://drupal.org/> herunterladen, entpacken und kopieren Sie die Module zunächst nach `sites/all/modules`, um diese später unter **Verwalten** → **Strukturierung** → **Module** auswählen und installieren zu können.

Setzen Sie für die Module, die Sie installieren wollen, ein Häkchen bei der Option **Aktiviert** und speichern Sie die Konfiguration.

Navigieren Sie in Ihrem Benutzerblock zu **Verwalten** → **Benutzerverwaltung** → **Berechtigungen**, um die Berechtigungen der einzelnen Benutzerrollen für die installierten Module zu überprüfen.

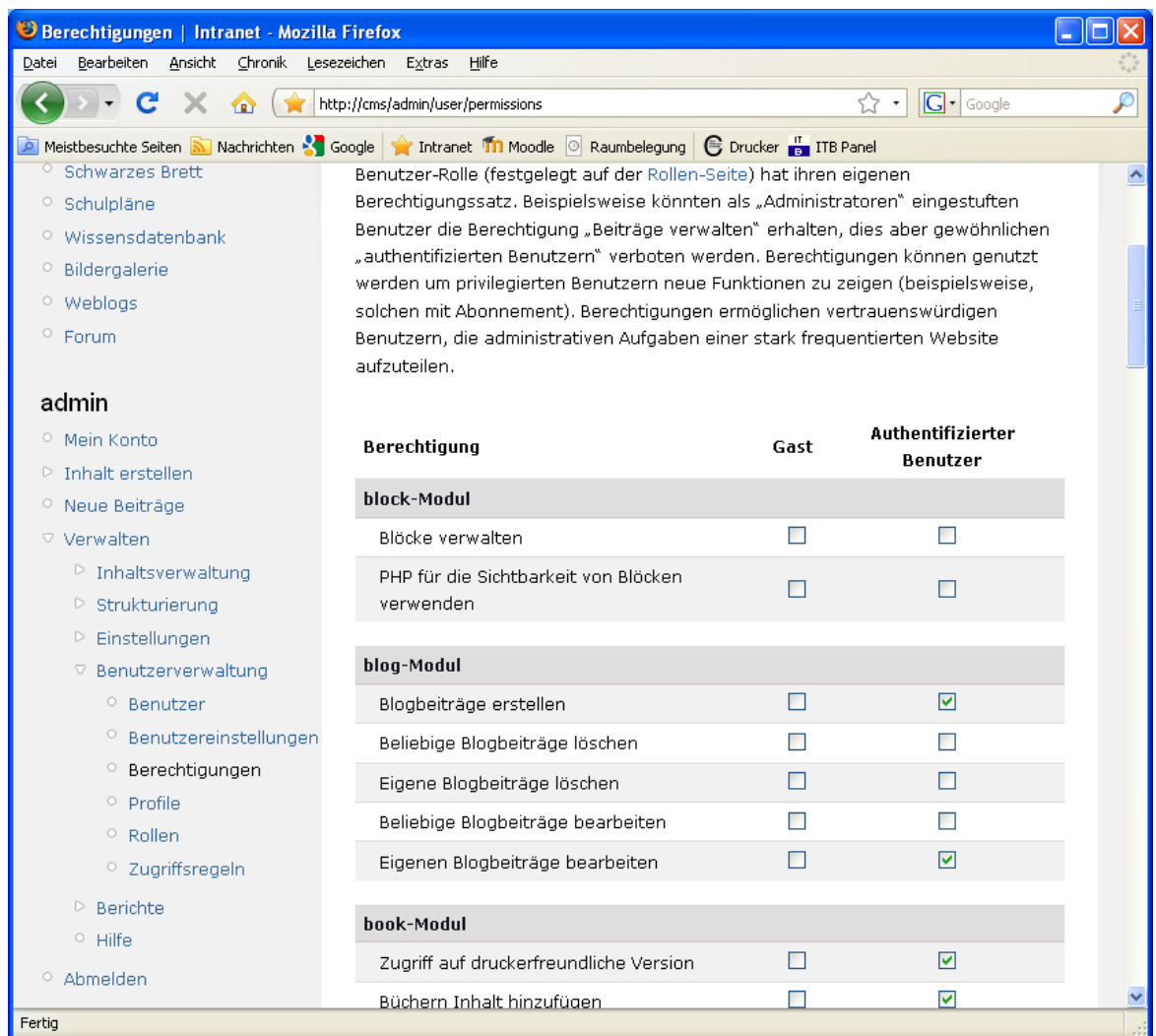


Abbildung VI.6.7. Berechtigungen der Benutzerrollen für die Module

Setzen Sie gegebenenfalls fehlende Berechtigungen für die Benutzerrollen durch ein Häkchen an entsprechender Stelle und speichern Sie die Berechtigungen.

VI.6.1.2. Ihre Vorteile

- einfache und flexible Kommunikation auf Basis von Weblogs und Foren (Informations- und Gedankenaustausch fördern)
- zentrale Dokumentenverwaltung als "Wissensdatenbank" (Informationen jederzeit und von überall aus über das Internet abrufen)
- Online Bereitstellung von Lehrer-, Raum-, Stunden- und Vertretungsplänen etc. (Zeit- und Kostenersparnis bei schul- und verwaltungsrelevanten Prozessen)

VI.6.2. Raumbuchungssystem

MRBS (Meeting Room Booking System) ist ein Open Source bzw. quelloffenes Raumbuchungssystem mit dem sich Zeitreservierungen für Räume oder Medien verwalten lassen. MRBS ist Freie Software und steht unter der GNU General Public License (GPL). Für weitere Informationen besuchen Sie bitte die Projektseite im Internet unter <http://mrbs.sourceforge.net/>.

VI.6.2.1. Räume anlegen

Rufen Sie Ihre MRBS Installation über die Adresse <http://mrbs/> in Ihrem Browser auf und melden Sie sich z.B. als Systemadministrator an. Wenn Sie Firefox als Browser verwenden, können Sie auch einfach Raumbelegung aus der Lesezeichen-Symbolleiste wählen.

Nachdem Sie sich erfolgreich angemeldet haben, navigieren Sie zum Punkt **Admin**.

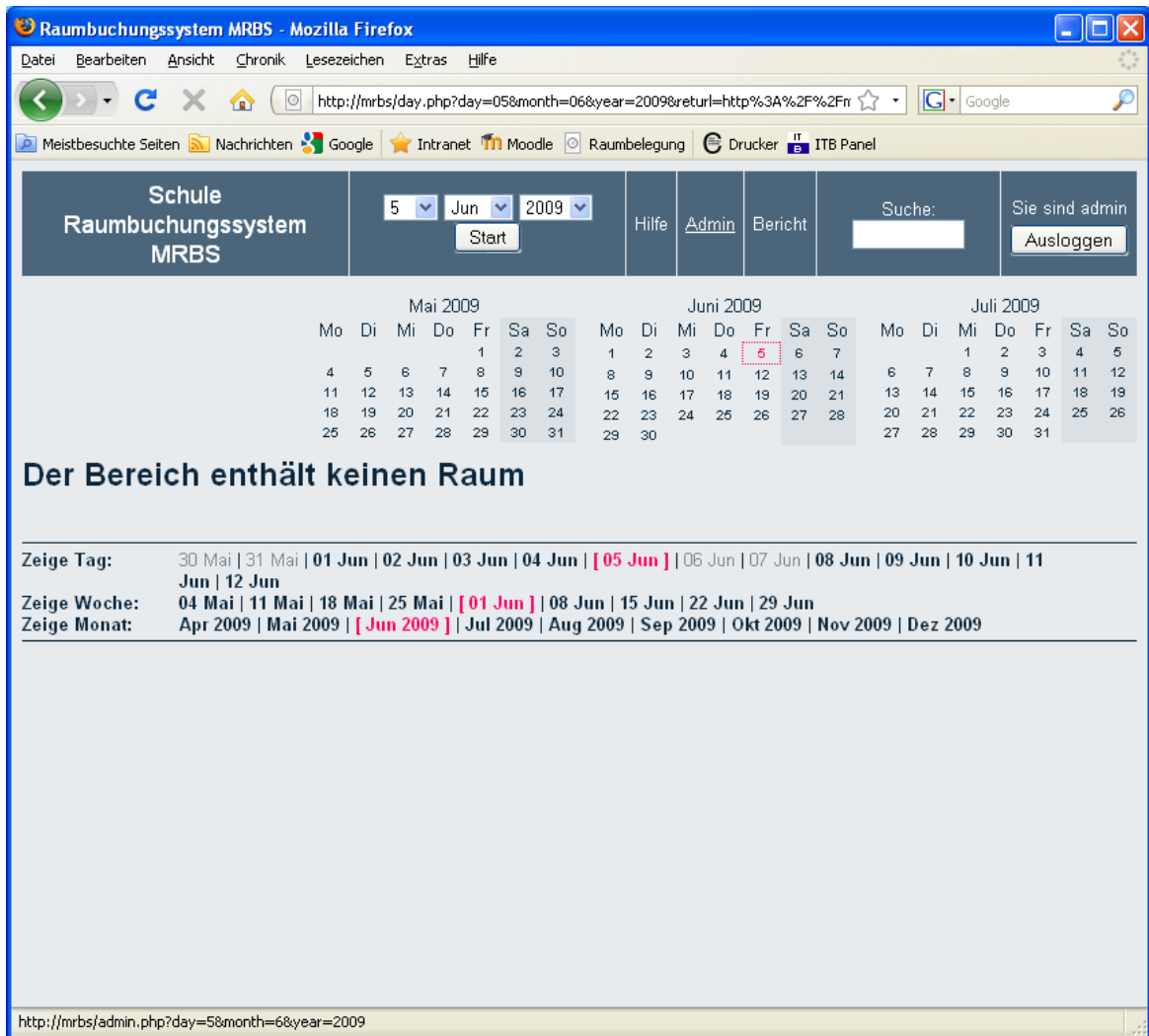


Abbildung VI.6.8. Startseite der MRBS Installation

Wählen Sie einen Bereich, für den neue Räume oder Medien angelegt werden sollen. Wenn keine Bereiche vorhanden sind, erstellen Sie einen oder mehrere neue Bereiche.

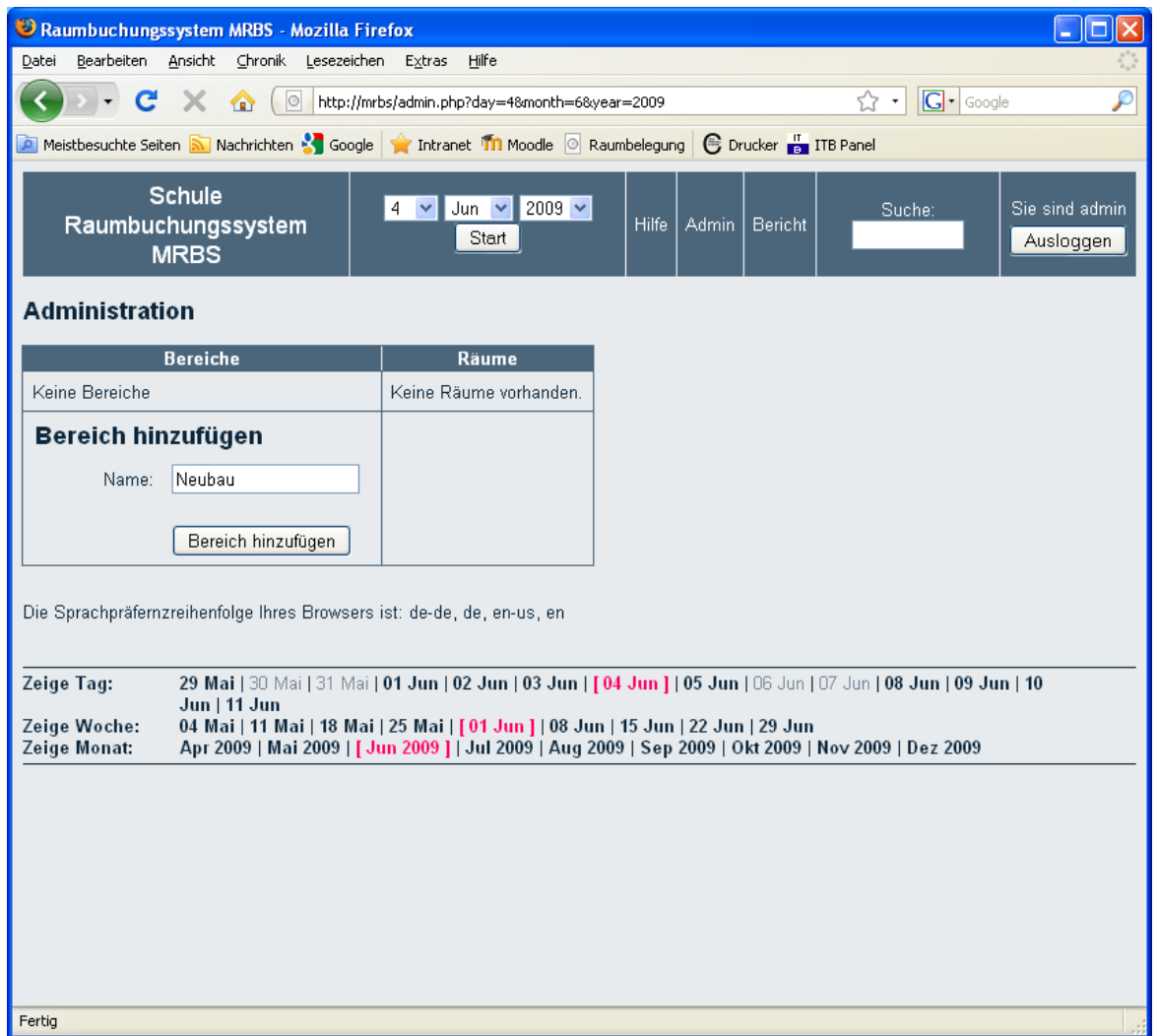


Abbildung VI.6.9. Bereich erstellen

Sie können dann für einen Bereich einen oder mehrere neue Räume oder Medien anlegen.

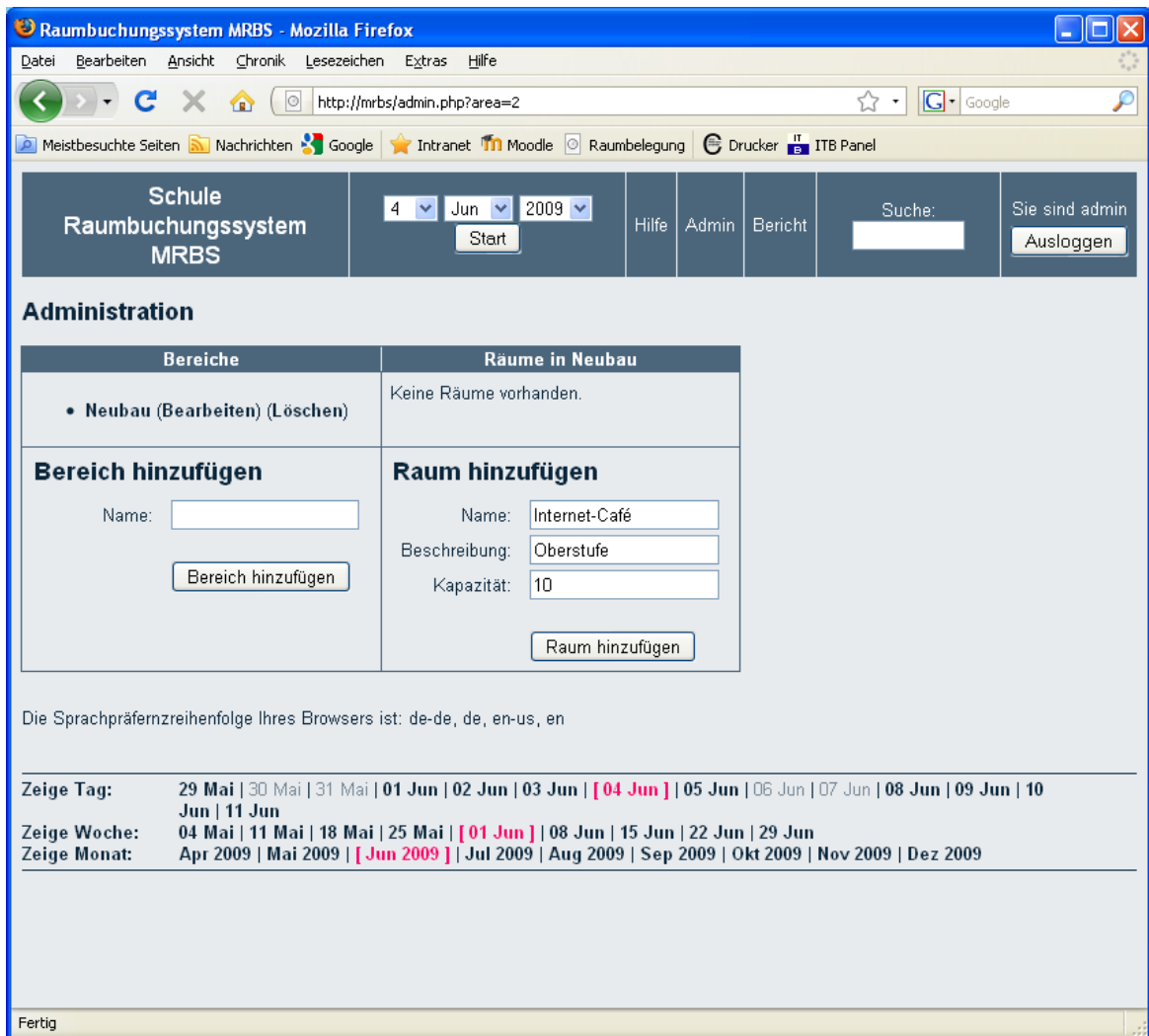


Abbildung VI.6.10. Raum anlegen

VI.6.2.2. Zeitreservierungen erstellen

Wählen Sie eine Kalenderansicht Tag / Woche / Monat und bestimmen Sie den Wochentag, an dem Sie einen oder mehrere Räume oder Medien für sich reservieren wollen.

Schule Raumbuchungssystem MRBS

4 Jun 2009

Hilfe Admin Bericht Suche: Sie sind admin Ausloggen

Mai 2009							Juni 2009							Juli 2009						
Mo	Di	Mi	Do	Fr	Sa	So	Mo	Di	Mi	Do	Fr	Sa	So	Mo	Di	Mi	Do	Fr	Sa	So
				1	2	3	1	2	3	4	5	6	7							
4	5	6	7	8	9	10	8	9	10	11	12	13	14	6	7	8	9	10	11	12
11	12	13	14	15	16	17	15	16	17	18	19	20	21	13	14	15	16	17	18	19
18	19	20	21	22	23	24	22	23	24	25	26	27	28	20	21	22	23	24	25	26
25	26	27	28	29	30	31	29	30						27	28	29	30	31		

Donnerstag 04 Juni 2009

<< gehe zum vorherigen Tag gehe zum heutigen Tag gehe zum nächsten Tag >>

Unterrichtsstunde:	Internet-Café(10)
1. Stunde	
2. Stunde	
3. Stunde	
4. Stunde	
5. Stunde	
6. Stunde	
7. Stunde	
8. Stunde	

<< gehe zum vorherigen Tag gehe zum heutigen Tag gehe zum nächsten Tag >>

außerplanmäßig **planmäßig**

Zeige Tag: 29 Mai | 30 Mai | 31 Mai | 01 Jun | 02 Jun | 03 Jun | **04 Jun** | 05 Jun | 06 Jun | 07 Jun | 08 Jun | 09 Jun | 10 Jun | 11 Jun

Zeige Woche: 04 Mai | 11 Mai | 18 Mai | 25 Mai | **01 Jun** | 08 Jun | 15 Jun | 22 Jun | 29 Jun

Zeige Monat: Apr 2009 | Mai 2009 | **Jun 2009** | Jul 2009 | Aug 2009 | Sep 2009 | Okt 2009 | Nov 2009 | Dez 2009

http://mrbs/edit_entry.php?area=2&room=1&period=0&year=2009&month=6&day=4

Abbildung VI.6.11. Wochentag für Zeitreservierung

Sie erhalten ein Eingabeformular mit zahlreichen Auswahlmöglichkeiten, die aber allesamt selbsterklärend sind.

Schule Raumbuchungssystem MRBS

4 Jun 2009 Start Hilfe Admin Bericht Suche: Sie sind admin Ausloggen

Eintrag hinzufügen

Kurzbeschreibung : Seminarkurs

Vollständige Beschreibung: Besprechung / Diskussion
7 Teilnehmer
(Anzahl der Teilnehmer etc)

Tag: 4 Jun 2009

Unterrichtsstunde: 1. Stunde

Dauer: 2 Unterrichtsstunden Ganztägig

Räume: Internet-Café Strg-Click um mehr als einen Raum auszuwählen

Art: planmäßig

Art der Wiederholung: Keine täglich wöchentlich monatlich jährlich monatlich, entsprechender Tag
 jede n-te Woche

Ende der Wiederholung: 4 Jun 2009

Fertig

Abbildung VI.6.12. Eingabeformular für Zeitreservierung

Nachdem Sie erfolgreich gespeichert haben, finden Sie einen neuen Eintrag mit der Zeitreservierung in der Kalenderansicht.

The screenshot shows the MRBS web interface. At the top, there's a navigation bar with 'Datei', 'Bearbeiten', 'Ansicht', 'Chronik', 'Lesezeichen', 'Extras', and 'Hilfe'. The address bar shows the URL: <http://mrbs/day.php?year=2009&month=6&day=4&area=2&room=1>. The main content area includes a header for 'Schule Raumbuchungssystem MRBS' with a 'Start' button and a search bar. Below this is a calendar view for June 2009, with the 4th of June highlighted. The current day is 'Donnerstag 04 Juni 2009'. A table below the calendar shows the lesson schedule for the day, with the first lesson 'Seminarkurs' in the 'Internet-Café(10)' room highlighted in green. Navigation links for previous, current, and next days are visible.

Abbildung VI.6.13. Zeitreservierung in der Kalenderansicht

VI.6.3. Webmailer

Roundcube ist ein Open Source bzw. quelloffener Webmailer, der die Verwaltung von E-Mails über einen Webbrowser ermöglicht. Roundcube ist Freie Software und steht unter der GNU General Public License (GPL). Für weitere Informationen besuchen Sie bitte die Projektseite im Internet unter <http://roundcube.net/>.



Anmerkung

Sie können das LogoDIDACT-Paket am Server über den Befehl **aptitude update && ldinstall ld-site-webmail** installieren.

Rufen Sie Ihre Webmail Installation über die Adresse <http://webmail/> in Ihrem Browser auf und authentifizieren Sie sich mit Benutzername und Passwort.

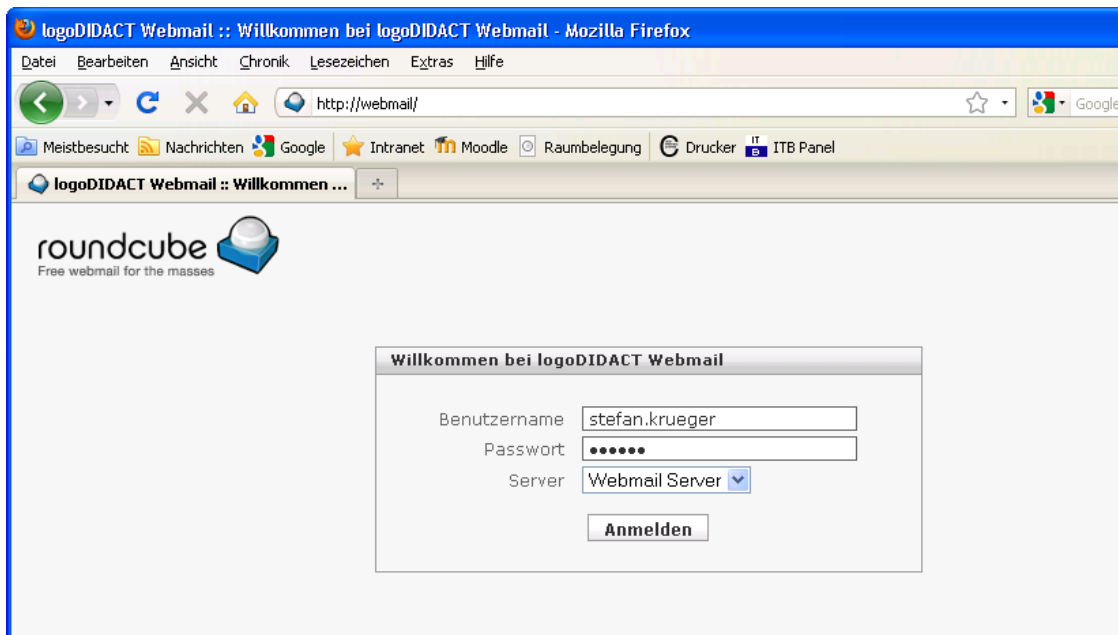


Abbildung VI.6.14. Anmeldung

VI.6.3.1. Die Roundcube Oberfläche

Die grafische Oberfläche von Roundcube sieht in der Grundeinstellung wie folgt aus:

- Im oberen Abschnitt finden Sie allgemeingültige Optionen wie E-Mail, Adressbuch, Einstellungen und Abmelden.
- Auf der linken Seite sehen Sie die verfügbaren Ordner Posteingang, Entwürfe, Gesendet, Spam und Gelöscht.
- Im mittleren Teil befinden sich die gewohnten Aktionen Auf neue Nachrichten überprüfen, Neue Nachricht schreiben, Antwort verfassen etc. eine Auflistung der E-Mail Nachrichten sowie eine Detailansicht der jeweils ausgewählten E-Mail.
- Im unteren Abschnitt finden Sie nützliche Aktionen, die den Umgang mit den E-Mail Nachrichten vereinfachen.

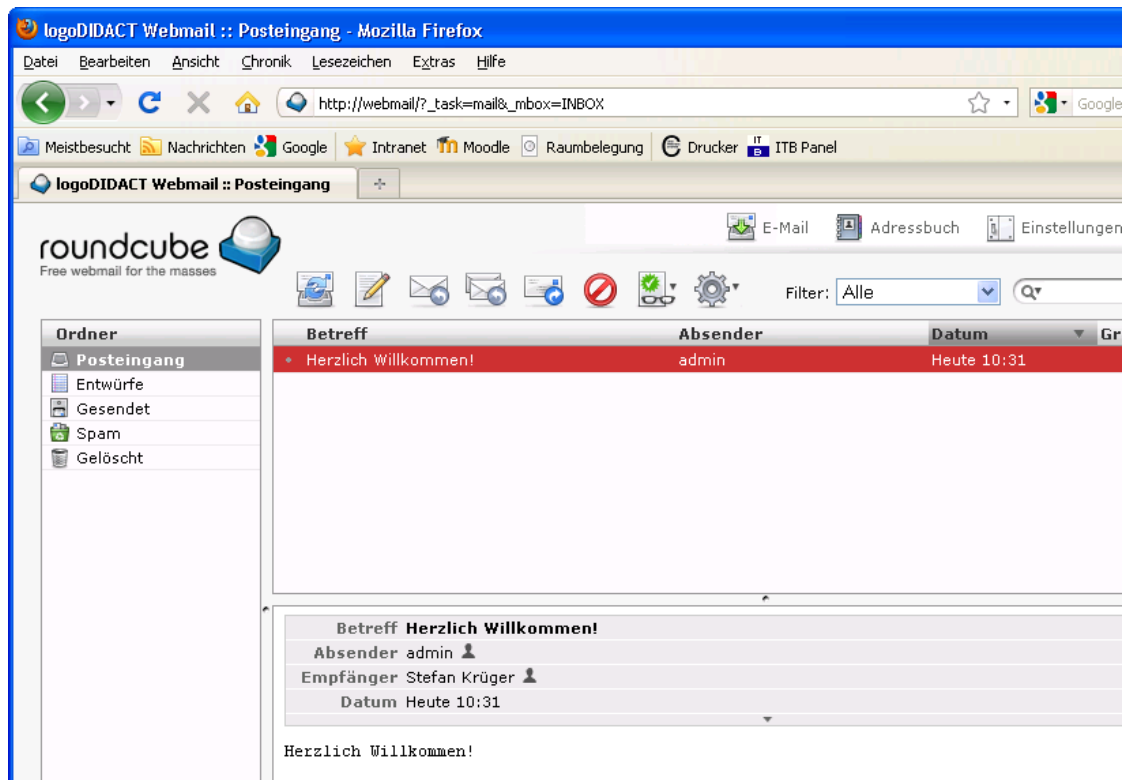


Abbildung VI.6.15. Posteingang

VI.6.3.2. E-Mail Nachricht verfassen

Um eine neue E-Mail zu schreiben, wählen Sie die Aktion **Neue Nachricht schreiben**. Sie erhalten ein Eingabeformular mit zahlreichen Auswahlmöglichkeiten.

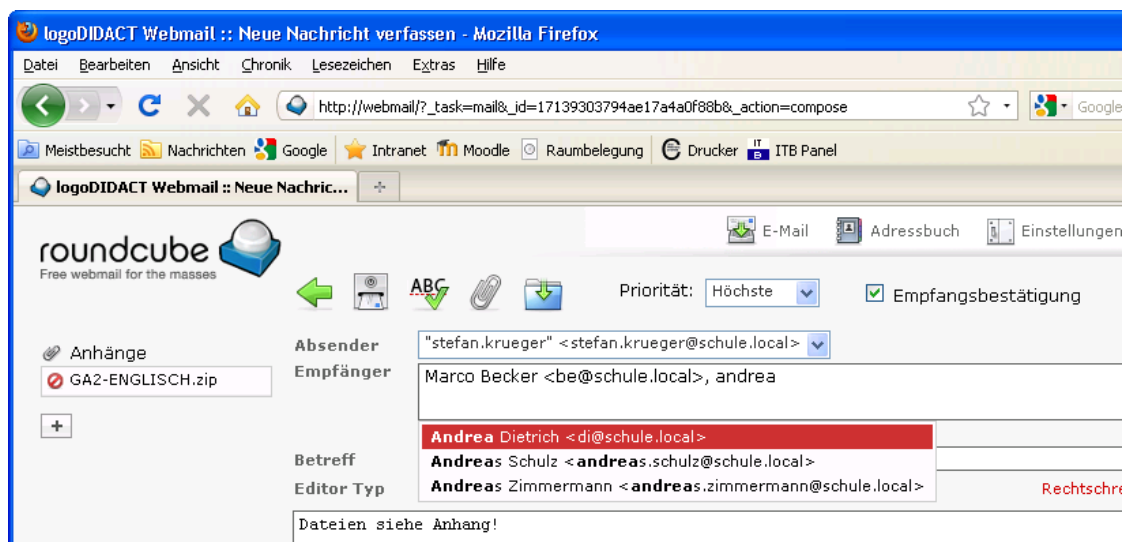


Abbildung VI.6.16. Neue Nachricht verfassen

Nachdem Sie die notwendigen Angaben gemacht haben, gehen Sie auf **Nachricht jetzt senden**. Sie erhalten eine Erfolgsmeldung und finden die E-Mail anschließend im Ordner **Gesendet**.

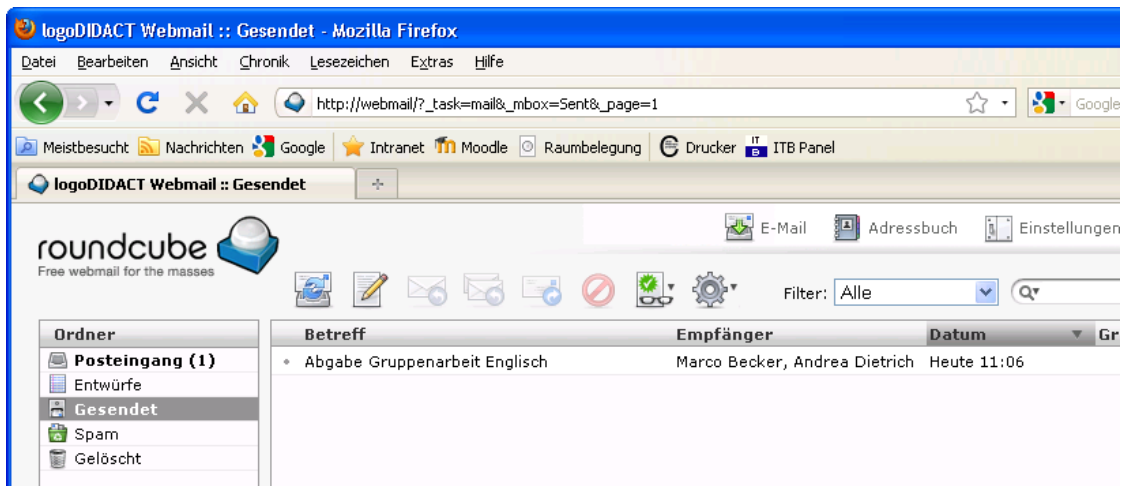


Abbildung VI.6.17. Ordner Gesendet

VI.6.4. Interne Webseiten

Es besteht die Möglichkeit, dass jeder Benutzer intern HTML-Seiten und PHP-Skripte in seinem Homeverzeichnis erstellt und diese sich auch testen und abrufen lassen. Dazu kann man im Homeverzeichnis H: den Ordner `private_html` erstellen oder auch `public_html`, je nachdem, ob man den Zugriff nur für sich oder auch für andere Nutzer erlauben möchte.



Achtung

Die `public_html` Funktionalität stellt in gewisser Weise ein Sicherheitsrisiko dar, weil Schüler darüber ebenfalls Dateien freigeben und php Skripte am Server ausführen lassen können, sofern man das nicht einschränkt.

Sofern das Erstellen bzw. Anzeigen der Seiten bei Ihnen nicht funktioniert, wurde es vom Administrator vermutlich wegen der Sicherheitsbedenken nicht aktiviert (siehe Abschnitt III.4.10, „Apache Webserver“).

VI.6.4.1. Zugriff auf Webseiten über `private_html` und `public_html`

Der Zugriff von einem Web-Browser aus erfolgt über folgenden Link (bitte beachten Sie die Tilde ~):
<http://server/~BENUTZERNAME/test.php>

VI.6.5. Zugriff per Browser auf Dateien

Um einen vom Betriebssystem möglichst unabhängigen Zugriff auf Dateien am Server zu gewährleisten, ist auf dem LogoDIDACT-Server der Online-Dateimanager PYDIO (put your data in orbit) installiert (ehemals AjaXplorer). Diese Open-Source-Software läuft im Kern nur auf dem Server, so dass der Zugriff prinzipiell von jedem Web-Browser aus möglich ist.

PYDIO ist ans LDAP des LogoDIDACT-Server angebunden, so dass die Anmeldung mit den bekannten Benutzerdaten durchgeführt werden kann. Der Zugriff erfolgt über `http://files:`

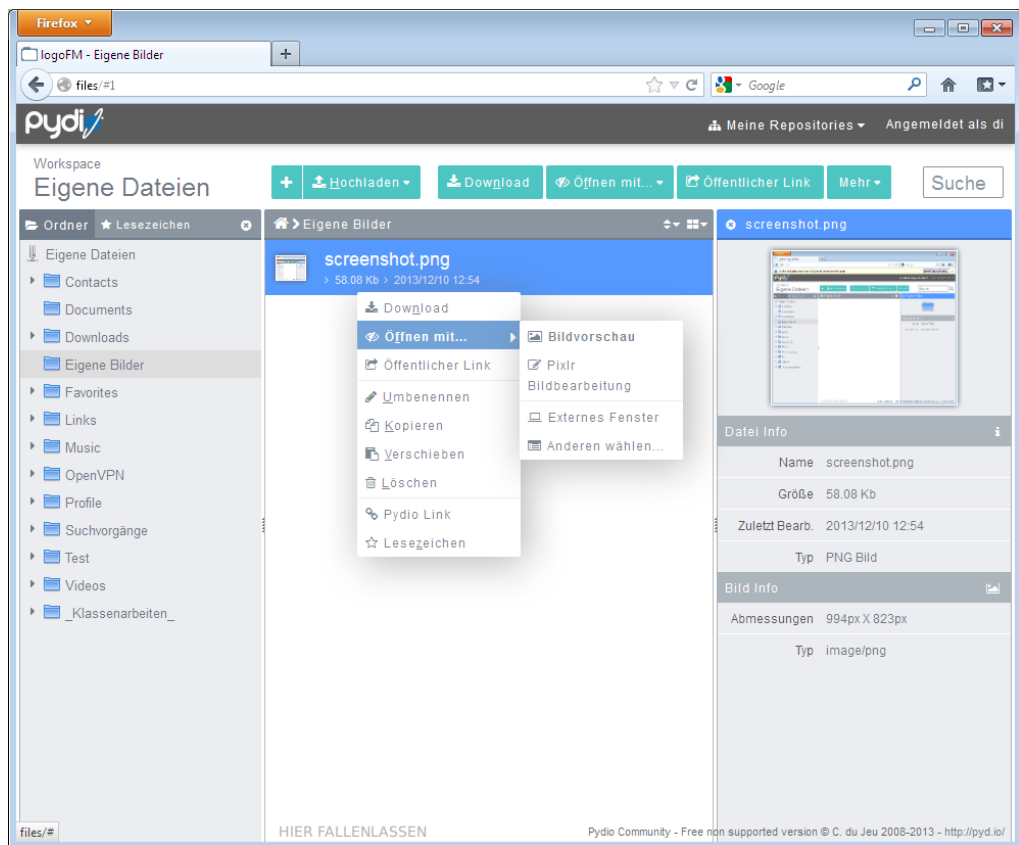


Abbildung VI.6.18. Aufruf über <http://files> und Zugriff auf Eigene Dateien im Laufwerk H:

Der Zugriff kann nun sowohl auf das eigene Home-Laufwerk erfolgen

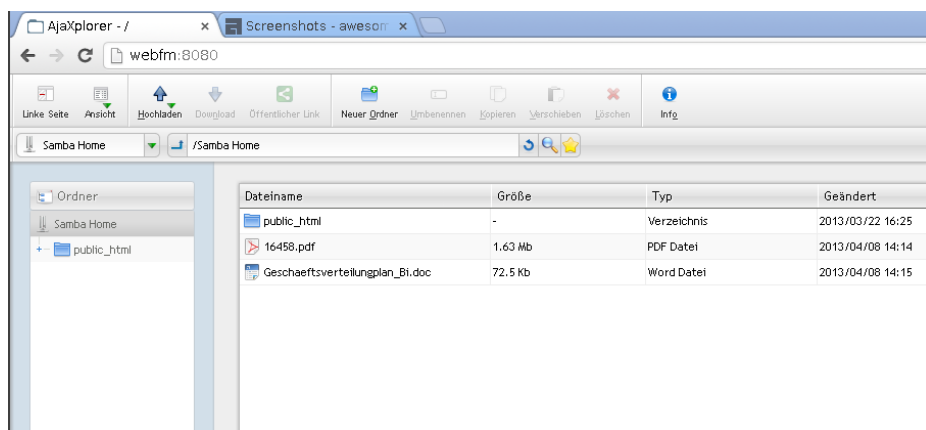


Abbildung VI.6.19. Zugriff auf Homelaufwerk über AjaXplorer

als auch auf Dateien im Tausch-Laufwerk.

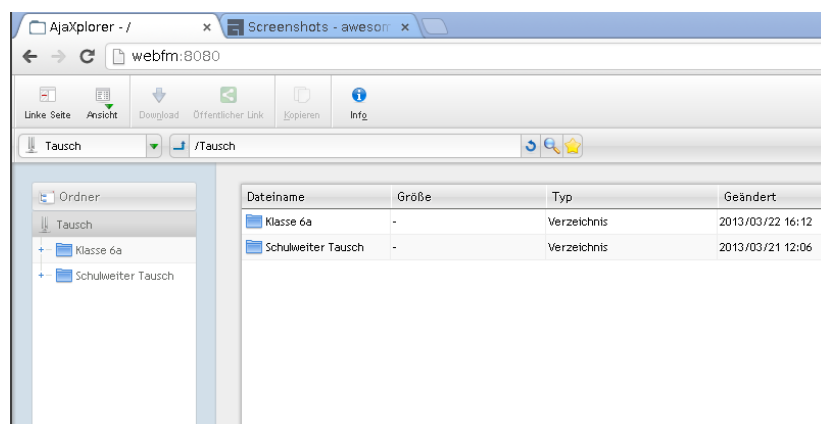


Abbildung VI.6.20. Zugriff auf Tauschlaufwerk über AjaXplorer

Stichwortverzeichnis

A

Abuse-Meldungen, III – 101
ACL, III – 107
ACME, III – 79
acme.sh, III – 79
AD, III – 70
AEP, III – 165
AgentDisplayMode, V – 37
AgentSetResolution, V – 36
AjaXplorer (Siehe PYDIO)
Aktivierung (Siehe Produktaktivierung)
Aktualisierung des Servers, III – 67
Apache Webserver, III – 115
Apple School, III – 223
ASM, III – 221
Aufbau des Netzwerks, II – 5
Auflösung des Bildschirms ändern, V – 36
Aufwecken (Siehe Wake-On-LAN)
AutoConf, IV – 27

B

Backup, III – 13
 Anzahl für Rotation, III – 16
 auf NAS, III – 22
 Backupfestplatte neu initialisieren, III – 16
 Benachrichtigung per Mail, III – 14
 Hot-Plug, III – 18
 Notfallwiederherstellung, III – 43
 Problem, III – 22
 Sicherung des Auslieferungszustandes, III – 20
 Zeitplan für Sicherungen, III – 14
Befehle und Skripte am Server, III – 114
Benutzer
 Identität, VI – 64
 Konvention der Anmeldenamen festlegen, III – 121
 Rollen, VI – 5
 Versetzen, Löschen und Anlegen beim Schuljahreswechsel, V – 8
Benutzer anlegen
 einzeln, V – 12
 über Listen, V – 3
Benutzerkärtchen erstellen, VI – 35
Benutzerprofil
 servergespeichert, III – 122
Benutzerverwaltung, VI – 34
Bildschirmauflösung über wimport_data, V – 36
Bildschirmübertragung, VI – 23
BitLocker, III – 130
Bonding, III – 54

C

CA, III – 84
Certification Authority, III – 84
Clients
 Netzwerkboot (PXE) aktivieren, IV – 5
Collabora, III – 298
Collabora>, III – 288
Container
 aufbauen, III – 68
 löschen, III – 70
 verwalten, III – 58
Cron-Jobs, III – 113

D

Dansguardian, III – 103
Dateien austeilen und einsammeln, VI – 20
 Größe anpassen, III – 113
Dateiressourcen
 Zugriff, VI – 92
Datenschutz
 Anzahl Backups begrenzen, III – 16
 Log-Dateien, III – 15
 Mitglieder der Gruppe, III – 120
Datensicherung (Siehe Backup)
Datenträgerverwaltung, III – 170
DDNS, III – 106
DEP, III – 221
 Händler-ID, III – 223
Device Enrollment Program, III – 221
DHCP
 dynamischer Bereich, III – 104
 Optionen, III – 104
Didaktische Funktionen, VI – 33
Disaster Recovery, III – 43
DMZ
 Netzwerk, III – 56
 Netzwerkbereich anpassen, III – 51
DMZ Host , III – 98
DNS
 dynamisches, III – 106
 Rechnereintrag per wimport_data, III – 105
 vhost, III – 116
 vhost anlegen, III – 117
DNS-Server, III – 105
Domänenname festlegen, III – 71
Domänenbeitritt
 automatisiert, III – 149
Druckauswertung, V – 46
Drucker Anpassungen
 Bestätigung des Druckauftrags am Client deaktivieren, III – 103
 Printagent Symbol am Client ausschalten, III – 104
Druckerzuordnungsliste bearbeiten, V – 42
Druckkosten der Drucker, V – 45

Druckquota Einstellungen, V – 43

Dynamische DNS Dienste

 DynDNS , III – 97

 logoIP , III – 96

E

E-Mail

 Port 25 sperren/freigen, III – 101

F

Fedora, IV – 16

Fernzugriff auf den Server , III – 95

 Besonderheiten , III – 99

 Dynamischer Rechnername , III – 96

 Freischaltung in der Serverfirewall , III – 99

 Portweiterleitung am Router , III – 98

Filterlisten bearbeiten, V – 49

Filterung

 Protokoll FTP, III – 100

 Protokoll SMTP, III – 101

 Protokolle, III – 100

Firewall

 Anpassungen, III – 95

 FTP-Ports öffnen/schließen, III – 100

 Ports und Protokolle, III – 100

 shorewall, III – 85

 SMTP-Ports öffnen, III – 101

FQDN, III – 149

FTP, III – 100

Funktions-Upgrade Windows 10 (Siehe Upgrade von Windows 10)

FWU, III – 165

FWU-Vertrag, III – 165

G

Gateway (Siehe Router)

Geräteaufnahme

 manuell, V – 32

Geräteliste

 bearbeiten, V – 34

getfacl, III – 108

git, III – 64

 commit, III – 65

 status, III – 64

Grafische Benutzeroberfläche, VI – 16

graylog, III – 161

Gruppe

 Datenschutz und Verwaltung, III – 120

guest.conf, III – 68

GUILogon, VI – 56

H

Händler-DEP-ID, III – 223

Homepage schulintern, III – 116

Hot-Plug-Backup, III – 18

HTTP-Server, III – 115

I

Image

 importieren, III – 140

Inplace-Upgrade Windows 10 (Siehe Upgrade von Windows 10)

Internetauswertung

 Löschfrist, III – 103

Internetzugriff sperren, VI – 11

Internetzugriffe auswerten, V – 21

inxi, III – 48

IP-Adresse

 extern anpassen, III – 49

 extern auf DHCP stellen, III – 50

 ldhost, III – 50

 logosrv, III – 53

IP-Schema, II – 5

iSCSC, III – 22

ITB

 Druckauswertung, V – 46

 Druckerzuordnungsliste bearbeiten, V – 42

 Druckkosten der Drucker, V – 45

 Druckquota Einstellungen, V – 43

 Filterlisten bearbeiten, V – 49

 Geräteliste bearbeiten, V – 34

 Manuelle Geräteaufnahme, V – 32

 Raumeinstellungen bearbeiten, V – 37

 Rechnereinstellungen bearbeiten, V – 38

 Serverdienste neustarten, V – 32

 Webfilter Kategorien, V – 48

K

Kabelkonzept, I – 9

Kennwort

 ändern, VI – 38

 eigenes ändern, VI – 39

 für alle Schüler neu generieren, III – 125

 Komplexität für generierte Kennwörter, III – 124

 sperren, III – 126

 von root ändern, II – 26

Kennworterfassungsbogen, A – 1

Kennwortrichtlinien in der LogoDIDACT-Console

 ändern, VI – 39

Klassenarbeitsmodus, VI – 25

KMS, III – 163

Konvention

 Anmeldenamen, III – 121

kopano, III – 303

KVM, III – 93

L

LACP, III – 54

-
- Laufwerk
 - Buchstaben, VI – 5
 - Netzlaufwerke H., T: und P:, VI – 5
 - zusätzliches share einrichten, III – 106
 - LD Azure Connnect
 - Sync-ID, III – 271
 - LD Deploy, III – 129
 - Selbstheilendes Prinzip, IV – 5
 - LD Mobile, III – 207
 - ld-sg-nextcloud, III – 291
 - ld-su-domjoin
 - auf Serverseite, III – 74
 - im Control Center, III – 149
 - LD-USB-BAK, III – 18
 - LDAP, I – 7
 - LDAPs, III – 84
 - ldprivacy, III – 120
 - ldupdate
 - LogoDIDACT 2.0, III – 67
 - Lehrer einer Klasse zuordnen, VI – 7
 - Let's Encrypt, III – 77
 - libvirt, III – 175
 - linpe, IV – 16
 - Lizenzverträge, III – 165
 - Log-Dateien, III – 126
 - in Backups, III – 15
 - LogoDIDACT-Agent
 - Installation unter Windows, IV – 80
 - LogoDIDACT-Agent und Console, IV – 79
 - LogoDIDACT-Console
 - Benutzerkärtchen erstellen, VI – 35
 - Benutzerverwaltung, VI – 34
 - Bildschirmübertragung, VI – 23
 - Dateien austeilen und einsammeln, VI – 20
 - Didaktische Funktionen, VI – 33
 - Grafische Benutzeroberfläche, VI – 16
 - Internetzugriff sperren, VI – 11
 - Internetzugriffe auswerten, V – 21
 - Kennwörter bearbeiten, VI – 38
 - Klassenarbeitsmodus, VI – 25
 - Raumsteuerung, VI – 18
 - Rembo/mySHN® Funktionen, V – 20
 - Schularten verwalten, V – 17
 - Statistische Auswertungen, V – 24
 - Zugriff auf Funktionen anpassen, III – 118
 - Zugriff für Benutzer anpassen, III – 119
 - Zugriff für Lehrer anpassen, III – 118
 - Zugriff für Schüler, III – 120
 - LogoDIDACT-Server
 - Serversoftware, I – 6
 - LogoDIDACT-Server Mindestanforderungen, I – 7
 - logoIP , III – 96
 - logrotate, III – 126
 - Löschfrist
 - Webfilter, III – 103
 - LXC
 - aufbauen, III – 68
 - löschen, III – 70
 - RAM-Bedarf, III – 58
- ## M
- MariaDB 10.3, III – 303
 - MDM, III – 207
 - Token, III – 225
 - Microsoft Produktaktivierung, III – 163
 - Grundlagen der Produktaktivierung, III – 164
 - mrbs (Siehe Webdienste)
 - myAgent, V – 36
- ## N
- Namenskonvention, III – 121
 - NAS
 - Backup einrichten, III – 40
 - NAT Loopback, III – 81
 - NetworkScope, III – 51
 - Netzwerkadapter
 - am Server konfigurieren, III – 48
 - Netzwerkbereich
 - intern ändern, III – 51
 - Netzwerkstruktur, II – 5
 - Nextcloud, III – 287
 - Zugriff Dateien in LogoDIDACT, VI – 71
 - nginx, III – 74
 - Notfallwiederherstellung, III – 43
- ## O
- Office 365
 - für Lehrer*innen, VI – 59
 - OnlyOffice, III – 298
 - OPEN License, III – 165
 - Open License, III – 166
 - Open Value Subscription, III – 165
 - Open vSwitch
 - Update, II – 25
 - Ordner und Dateistrukturen, VI – 5
- ## P
- Partition, III – 170
 - Anpassung für Funktionsupgrade, IV – 58
 - Passwortmanagemnt, III – 67
 - pdbedit, III – 126
 - pdis, III – 63
 - pena, III – 63
 - Phasen, IV – 28
 - Ports
 - am Router weiterleiten, III – 98
 - für Apple- und Google-Server freischalten, III – 214
 - in der Firwall freischalten, III – 99

Ports und Protokolle, III – 100
Portweiterleitung , III – 98
Portweiterleitung am Router
 DMZ Host , III – 98
 Portweiterleitung , III – 98
printagent, III – 104
Produktaktivierung, III – 163
Profil
 servergespeichertes Benutzerprofil, III – 122
Protokoll-Filterung, III – 100
 Firewall, III – 95
 FTP, III – 100
 SMTP, III – 101
Proxy-Server, III – 102
prun, III – 63
pstat, III – 62
public_html, VI – 92
Puppet
 Arbeitsweise, III – 62
Puppet Agent
 aktivieren, III – 63
 deaktivieren, III – 63
PXE
 Netzwerkboot, IV – 5
PYDIO, VI – 92

Q

qBittorrent, III – 142
qcow2, III – 175
QEMU Guest Agent, III – 94
qemu-img, III – 175

R

Radius-Server, III – 127
RAM-Bedarf Container, III – 58
range, III – 104
Raumeinstellungen bearbeiten, V – 37
Raumsteuerung, VI – 18
Rechneraufnahme, V – 32
 mit LD Deploy, IV – 7
Rechnereinstellungen bearbeiten, V – 38
Rechnerliste
 bearbeiten, V – 34
Rechte
 auf Verzeichnisse, VI – 5
 in der LogoDIDACT-Console als Lehrer, VI – 35
 in der LogoDIDACT-Console anpassen, III – 118
redis, III – 67
Reimaging-Recht, III – 164
Rembo/mySHN®
 Statistik des Olinestarts, V – 50
Rembo/mySHN® Funktionen, V – 20
Remote-Einwahl, VI – 51
rev-proxy, III – 74

Reverse-Proxy, III – 74
Rollen, VI – 5
 in Ansible, IV – 28
 vordefiniert für AutoConf, III – 158
root
 Kennwort ändern, II – 26
Router
 IP-Adresse ändern, III – 49
 IP-Adresse angeben, II – 18
 Portweiterleitung, III – 98

S

Samba 4
 Domänenname festlegen, III – 71
samba4-ad
 aktivieren, III – 70
SchILD-NRW, A – 1
Schularten verwalten, V – 17
SCHULKARTEI, A – 8
Schulverwaltungsprogramme, A – 1
 SchILD-NRW, A – 1
 SCHULKARTEI, A – 8
Secret
 Radius, III – 127
SecureBoot, III – 130
Selbsteilende Arbeitsstationen, VI – 5
Select, III – 165
Server
 Basisinstallation, II – 10
Server-Token, III – 225
Serverdienste neustarten, V – 32
Servergespeichertes Benutzerprofil, III – 122
Serverinstallation
 Ändern der Bootreihenfolge, II – 10
 Benutzeranmeldung am Server, II – 21
 Deployment beobachten, II – 23
 Deployment Logfile, II – 23
 deutsches Tastaturlayout laden, II – 21
 Domänenname, II – 15
 Externe IP-Adresse, II – 18
 Externe Subnetzmaske, II – 18
 externes Interface, II – 17
 interne Interface, II – 17
 IP des Routers / Gateways, II – 18
 Kennwort für administrative Benutzer, II – 16
 Kennwort für Benutzer root, II – 15
 LogoDIDACT Lizenzvereinbarung, II – 13
 Schulname, II – 15
 Start von CD/DVD, II – 11
 Überprüfen der Netzwerkeinstellungen, II – 21
Serverkonfiguration
 IP-Adresse extern, III – 49
 IP-Adresse intern, III – 50
 Netzwerkbereich ändern, III – 51

-
- Puppet Grundlagen, III – 61
 - Service- und Support Modul
 - für IT-Betreuer, V – 25
 - für Lehrer, VI – 40
 - Vorteile, VI – 41
 - shortname, II – 15
 - Sicherheit
 - IP-Adress-Vergabe für fremde Rechner sperren, III – 104
 - Tor- Verbindungen/Protokoll sperren, III – 102
 - sle, III – 80, III – 82
 - SMART-Board, IV – 46
 - SMTP für einzelne Clients, III – 101
 - Software Assurance, III – 167
 - Speicherplatzbedarf eines Containers, III – 58
 - spice, III – 176
 - Split-DNS, III – 81
 - Squid, III – 102
 - SSL-Zertifikate
 - eigene, gekaufte, III – 83
 - erstellen, III – 79
 - freie mit Let's Encrypt, III – 77
 - SSL/TLS, III – 84
 - Statistische Auswertungen, V – 24
 - Störungsmeldung
 - abschliessen, VI – 49
 - Aktionen eintragen, VI – 47
 - anzeigen, VI – 41
 - Neu anlegen per Assistent, VI – 43
 - weiterleiten, VI – 47
 - Support
 - externe Kontakte anlegen, V – 26
 - Hauptfenster aller Störungen, V – 27
 - Lehrer der Gruppe zuordnen, V – 25
 - Störungen bearbeiten, weiterleiten und abschließen, V – 28
 - SurflogMaxAge, III – 103
 - systemctl, III – 60
 - systemd, III – 48
 - Anpassung der Netzwerk-Schnittstellen, II – 8
- T**
- Tablet-Management, III – 207
 - Tastaturlayout
 - auf deutsch stellen, II – 21
 - Tauschlaufwerke
 - Klassen-Tauschlaufwerke deaktivieren, III – 112
 - Lehrer-Tausch Zugriffsrechte ändern, III – 110
 - Vollzugriff auf Klassentausch , III – 111
 - Vollzugriff auf Schulweiter Tausch , III – 110
 - zyklisch löschen, III – 112
 - Teams
 - Besprechungs-Richtlinien, VI – 68
 - Besprechungs-Richtlinie anpassen, III – 280
 - Ticketsystem, VI – 42
 - Token, III – 225
 - Tor- Verbindungen/Protokoll sperren, III – 102
 - Torrent, III – 142
 - Metainfo generieren, III – 140
 - Tracker, III – 142
 - Trunk, III – 54
- U**
- Ubuntu
 - Upgrade auf 16.04, II – 6
 - Unifi, III – 195
 - Upgrade Windows 10 (Siehe Upgrade von Windows 10)
 - upgrade-retained-package, II – 25
 - Upload Drivers, IV – 24
 - USB
 - Hot-Plug-Backup, III – 18
 - USV, I – 9, III – 9
 - usv
 - APC Smart-UPS SMX750i, III – 9
- V**
- Versionsverwaltung
 - git, III – 64
 - Verwaltung
 - Mitglieder der Gruppe, III – 120
 - Verzeichnisstruktur, VI – 5
 - aus Lehrersicht, VI – 7
 - aus Schülersicht, VI – 6
 - Lehrer in Klassen eintragen, VI – 7
 - VHDx, IV – 7
 - virsh
 - Befehle, III – 176
 - Virt-Viewer, III – 176
 - Virtio-Treiber, III – 94
 - Virtualisierung
 - Am Client per VHDx, IV – 7
 - KVM am Server, III – 93
 - LogoDIDACT und LXCs, I – 4
 - VLANs, III – 56
 - Volumenlizenzverträge, III – 165
 - Vorratsdatenspeicherung
 - Dauer der Internetprotokollierung festlegen, III – 103
 - VPN
 - Installation auf Windows-Clients, VI – 51
 - Keys erzeugen, V – 18
 - OpenVPN, VI – 51
 - Remote-Einwahl, VI – 51
 - Verwendung der LogoDIDACT-Console, VI – 54
 - Zugang freischalten, V – 18
 - Zugriff auf Dateien, VI – 56
 - Zugriff auf Web-Dienste, VI – 56

W

Wake-On-LAN (WOL)

- per LogoDIDACT-Console, VI – 18
- zeitgesteuert, V – 41

Webdienste

- Content Management System, VI – 77
- Freischaltung für Zugriff von Außen, III – 74
- Raumbuchungssystem, VI – 83
- Webmailer, VI – 89

Webfilter

- für Gruppe deaktivieren, V – 38
- Schwellwert ändern, III – 103

Webfilter Anpassungen, III – 103

Webfilter Kategorien, V – 48

Webseiten

- intern erstellen, VI – 92

Webserver, III – 115

wim-Datei importieren, III – 140

wimport_data

- im ITB-Interface, V – 34

Windows 10

- Inplace-Upgrade, IV – 57
- Produktaktivierung, III – 163

Windows 7

- Produktaktivierung, III – 163

WLAN, III – 195

Wortfilter

- Schwellwert ändern, III – 103

WS-Discovery, IV – 40

WSD - Web Services on Devices, IV – 40

Z

Zeitsteuerung

- Rechner aufwecken per WOL, V – 41
- Rechner herunterfahren, V – 39
- über cron-jobs, III – 113

Zertifikate, III – 77 (Siehe SSL-Zertifikate)

Zugriffsberechtigungen

- auf Ordner und Dateien, III – 106
- auf Schüler Homelaufwerke, III – 109
- lesender Zugriff auf Schüler Homelaufwerke, III – 109
- prüfen, III – 108
- Vollzugriff auf Schüler Homelaufwerke, III – 109

Zusätzliche MAC/IP Adressen über wimport_data, V – 35

Anhang A. Kennworterfassungsbogen

_____ .logoip.de

LogoDIDACT Linux Server

Lokaler Serverbenutzer

root (root ist Administrator des Servers.)	
--	--

Clientbenutzer (Domäne)

admin (Domänenadministrator wird für mySHN und alle vorhandenen Webdienste verwendet.)	
itb (IT-Betreuer wird für den Zugriff auf das ITB-Interface unter http://itb/ verwendet.)	
pgmadmin (Programmadministrator wird für die Installation von Anwendungen auf den Clients verwendet.)	

Clientbenutzer (lokal)

Administrator	
Station	

Sonstiges

Anhang B. Schulverwaltungsprogramme

B.1. SchILD-NRW für Nordrhein-Westfalen

B.1.1. Anlegen eines Export-Filters

Über **Datenaustausch** → **Export in Text-Dateien** → **Exportieren** können Sie den Dialog zum Daten-Export aufrufen.

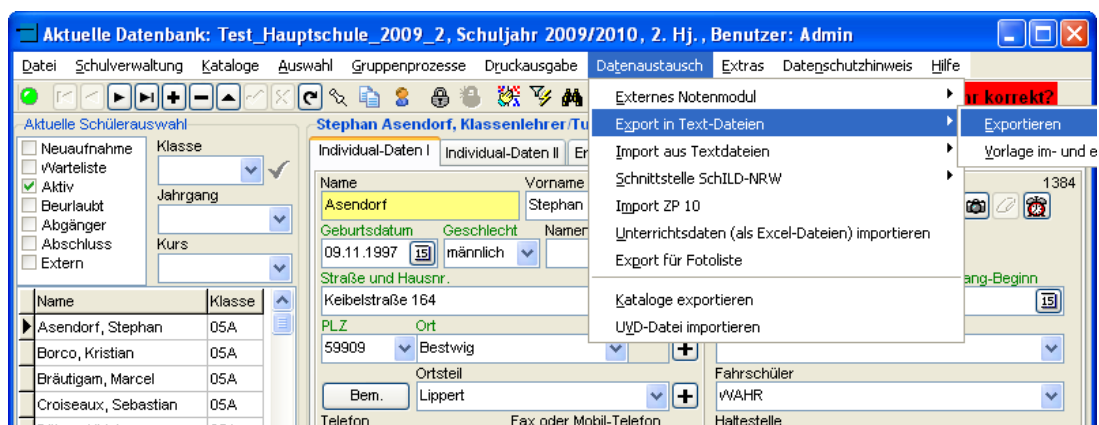


Abbildung B.1. Dateimenu zum Datenaustausch („Export in Text-Dateien“)

Wählen Sie zunächst oben links den Wert **Schüler** aus dem Drop-Down-Menü „Datenart“ und

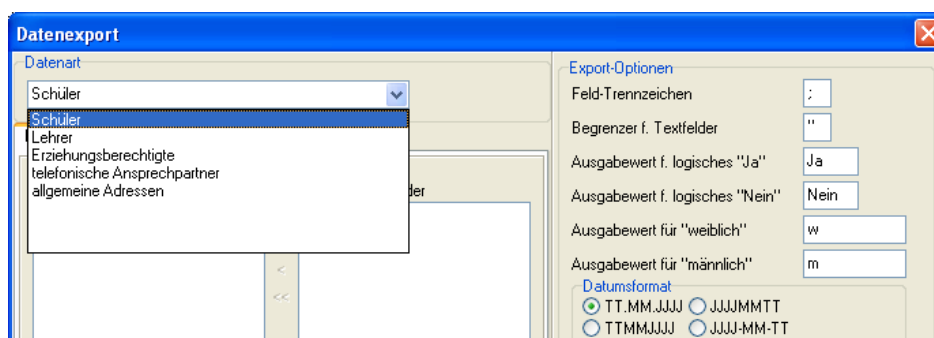


Abbildung B.2. Festlegen der „Datenart“ Schüler

löschen Sie rechts unter „Export-Optionen“ den vorgegebenen Wert " im Eingabefeld „**Begrenzer für Textfelder**“.

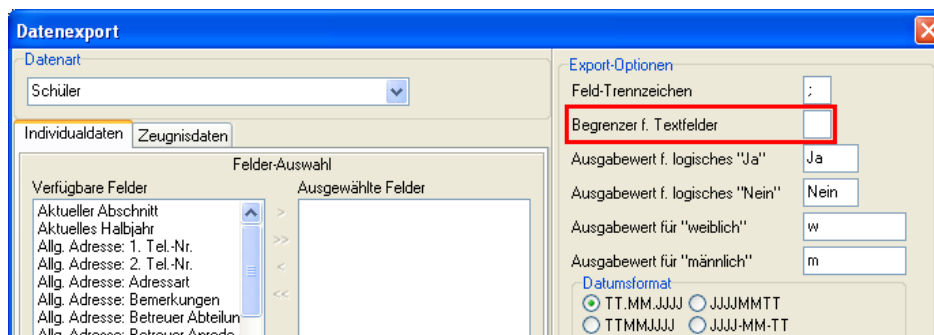


Abbildung B.3. Löschen der Eingabe unter „Begrenzer für Textfelder“

Wählen Sie anschließend in der Registerkarte „**Individualdaten**“ die zu exportierenden Benutzerdaten.



Tipp

Per Doppelklick oder alternativ auch über die Schaltfläche > lassen sich die einzelnen Felder gezielt für den Daten-Export bestimmen.

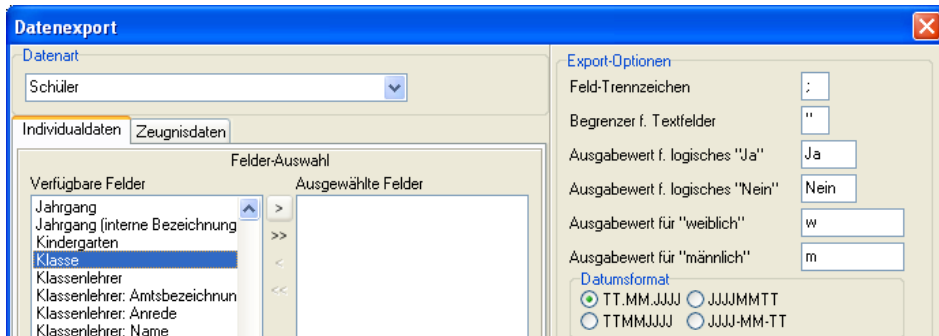


Abbildung B.4. Registerkarte mit „Individualdaten“ der Schüler

Für die Benutzerliste der Schüler benötigen Sie mindestens die nachfolgenden Felder:

1. Klasse
2. Nachname
3. Vorname
4. Geburtsdatum
5. Geschlecht

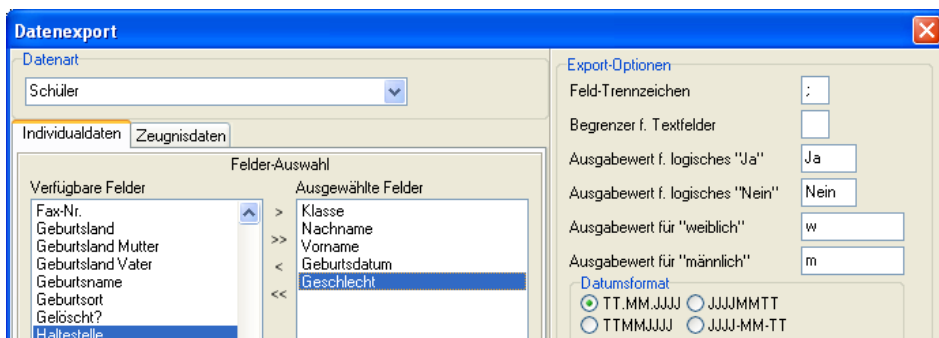


Abbildung B.5. Festlegen der Benutzerdaten der Schüler

Wenn Sie damit fertig sind, können Sie die Einstellungen unten rechts „**Als Vorlage speichern**“.

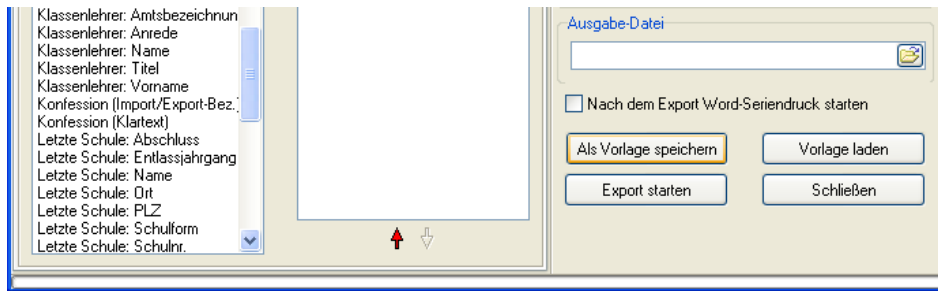


Abbildung B.6. Speichern der Vorlage für den Daten-Export

Speichern Sie die Vorlage mit einem passenden Namen, z.B. **LD Schüler**. Klicken Sie dazu in das mit * gekennzeichnete Textfeld und geben Sie den Wert ein. **Übernehmen** Sie anschließend die fertige Vorlage für den Text-Export.

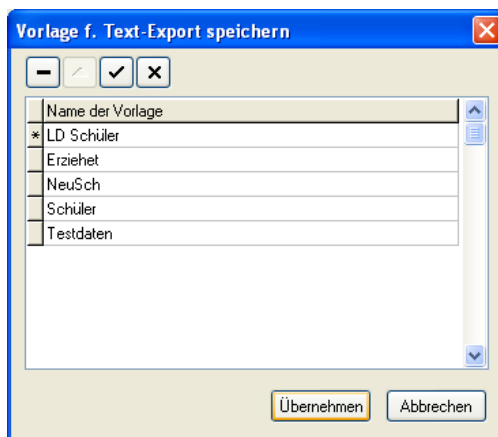


Abbildung B.7. Speichern der Vorlage als „LD Schüler“

Für die Benutzerliste der Lehrer können Sie analog zur Schülerliste vorgehen. Wählen Sie zunächst oben links wieder die „**Datenart**“ aus dem Drop-Down-Menü. In diesem Fall den richtigen Wert **Lehrer**.

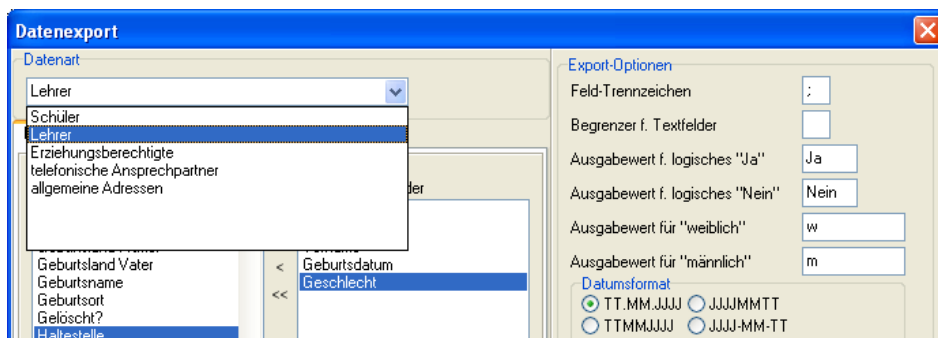


Abbildung B.8. Festlegen der „Datenart“ **Lehrer**

Für die Benutzerliste der Lehrer benötigen Sie mindestens die nachfolgenden Felder:

1. Nachname
2. Vorname

3. Kürzel

4. Geschlecht

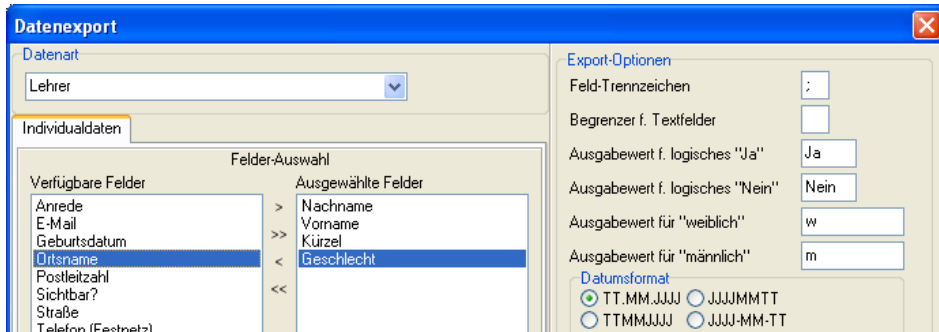


Abbildung B.9. Festlegen der Benutzerdaten der Lehrer

Speichern Sie die Vorlage mit einem passenden Namen, z.B. **LD Lehrer**.

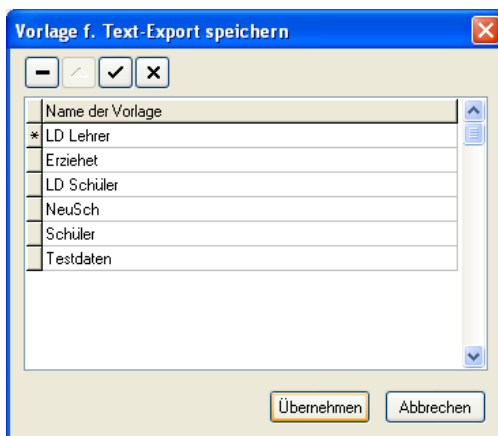


Abbildung B.10. Speichern der Vorlage als „LD Lehrer“

B.1.2. Durchführen des Daten-Exports



Achtung

Berücksichtigen Sie die „**Aktuelle Schülersauswahl**“ in SchILD-NRW, bevor Sie einen Daten-Export durchführen.

Über **Datenaustausch** → **Export in Text-Dateien** → **Exportieren** können Sie den Dialog zum Daten-Export aufrufen.

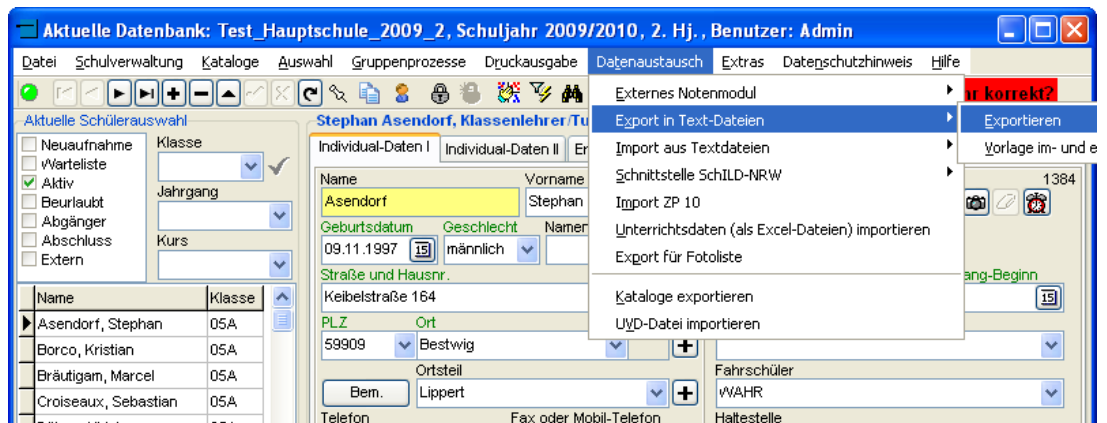


Abbildung B.11. Dateimenu zum Datenaustausch („Export in Text-Dateien“)

Gehen Sie zunächst auf „Vorlage laden“ und

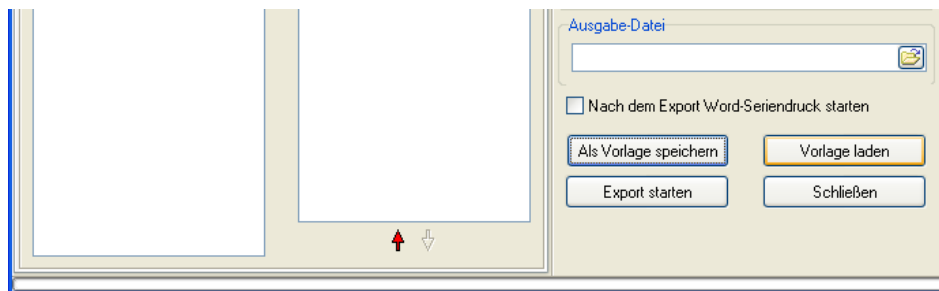


Abbildung B.12. Öffnen einer Vorlage für den Daten-Export

wählen Sie die Vorlage **LD Schüler** o.ä. Klicken Sie anschließend auf „Übernehmen“.



Abbildung B.13. Auswählen der Vorlage „LD Schüler“

Klicken Sie nun unten rechts unter „Ausgabe-Datei“ auf die Schaltfläche mit dem Ordnersymbol für Dateiname und Speicherort der Export-Datei.

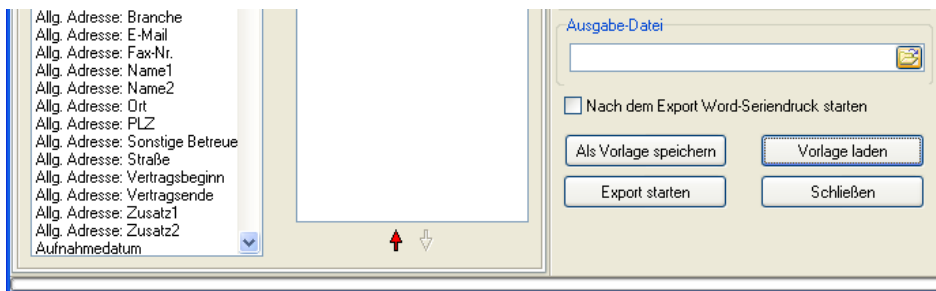


Abbildung B.14. Festlegen der Ausgabe-Datei („Dateiname und Speicherort“)

Wählen Sie einen passenden Dateinamen, z.B. **schueler**. Der Wert für den Dateityp „Text-Datei“ ist im Drop-Down-Menü bereits vorausgewählt.



Tipp

Über das obere Drop-Down-Menü „Suchen in:“ können Sie auf lokale Festplatten, sowie Netzlaufwerke und etwaige Wechseldatenträger (sofern angebunden) zugreifen.

Wenn Sie damit fertig sind, können Sie über „Öffnen“ die Werte für Dateiname und Speicherort für den anschließenden Daten-Export übernehmen.

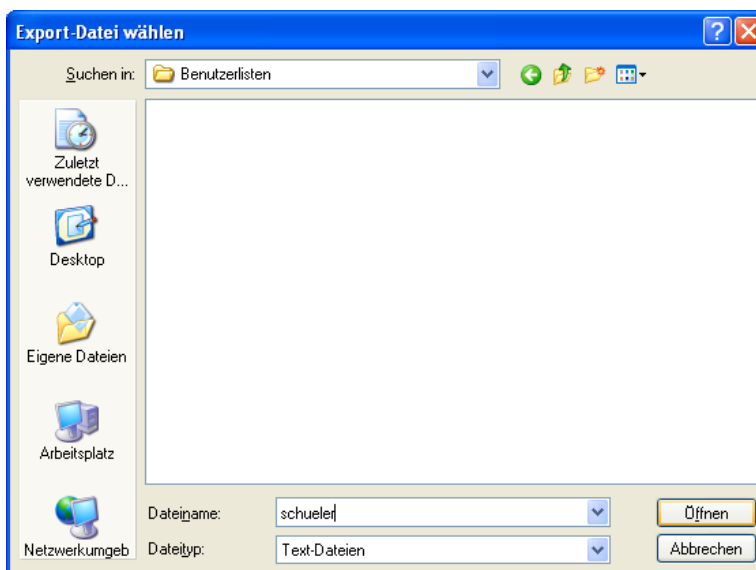


Abbildung B.15. Speichern der Export-Datei **schueler**

Klicken Sie auf „Export starten“, um die Schülerliste als Text-Datei aus SchILD-NRW zu exportieren.

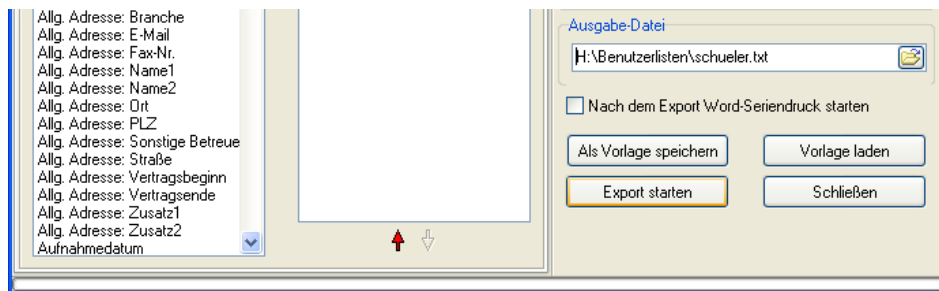


Abbildung B.16. Exportieren der Schülerliste als Text-Datei

Für die Lehrerliste wählen Sie dementsprechend die Vorlage **LD Lehrer** o.ä. und

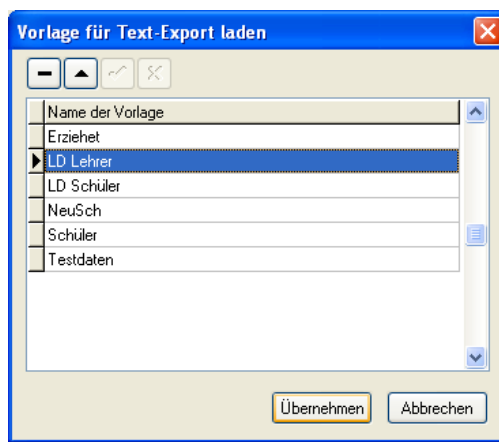


Abbildung B.17. Auswählen der Vorlage „LD Lehrer“

als Dateinamen, z.B. **Lehrer**.

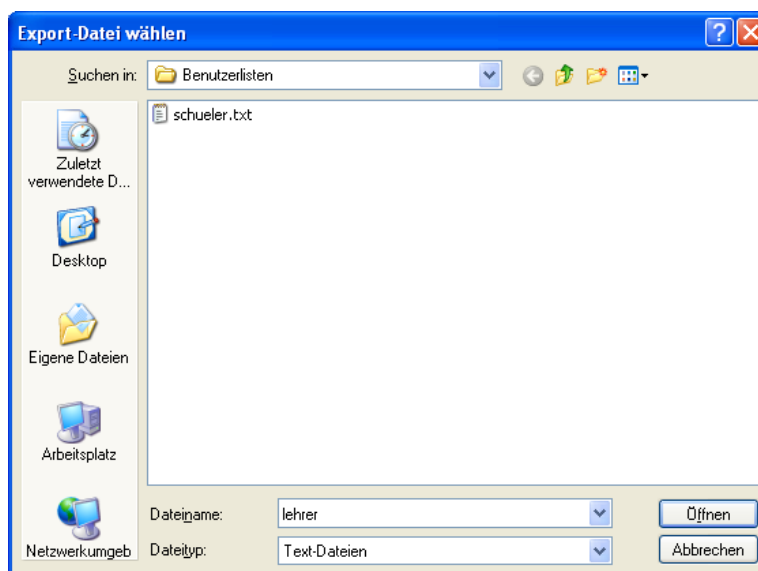


Abbildung B.18. Speichern der Export-Datei **Lehrer**

Überprüfen Sie anschließend die aus SchILD-NRW exportierte Schüler- und Lehrerliste auf ihre Richtigkeit.

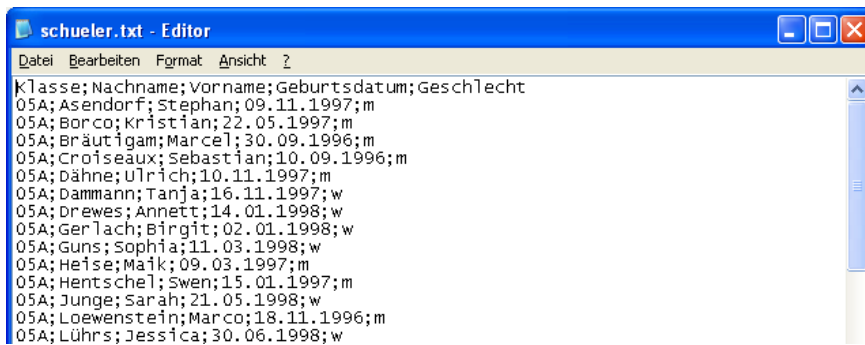


Abbildung B.19. Überprüfen der Text-Datei schueler.txt

B.2. SCHULKARTEI für Baden-Württemberg

B.2.1. Anlegen eines Export-Filters

Die Software SCHULKARTEI 8 integriert bereits einen passenden Export-Filter für LogoDIDACT Linux.

B.2.2. Durchführen des Daten-Exports

Über **Weiteres** → **Daten exportieren** → **logoDIDACT Linux** können Sie die Schüler- und Lehrerliste direkt für LogoDIDACT Linux exportieren.

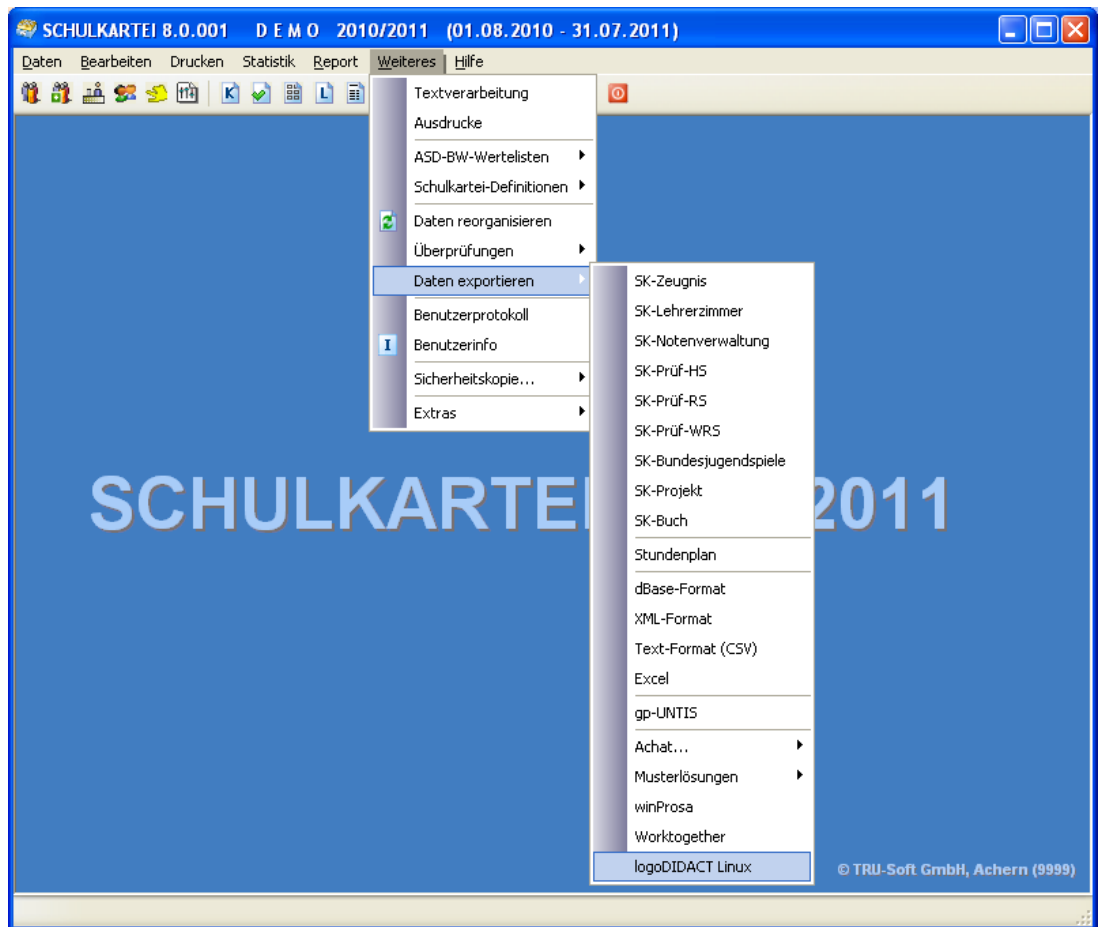


Abbildung B.20. Dateimenu zum Daten-Export („LogoDIDACT Linux“)

Im angegebenen Verzeichnis (installationsabhängig) finden Sie dann die beiden exportierten Dateien:

1. logoDIDACT_Schueler.TXT
2. logoDIDACT_Lehrer.TXT

Wenn Sie möchten, können Sie die Benutzerlisten anschließend noch auf einen Wechseldatenträger speichern. Klicken Sie dazu auf „Ja“. Im Beispiel sollen die Text-Dateien direkt nach C : \ gespeichert werden.

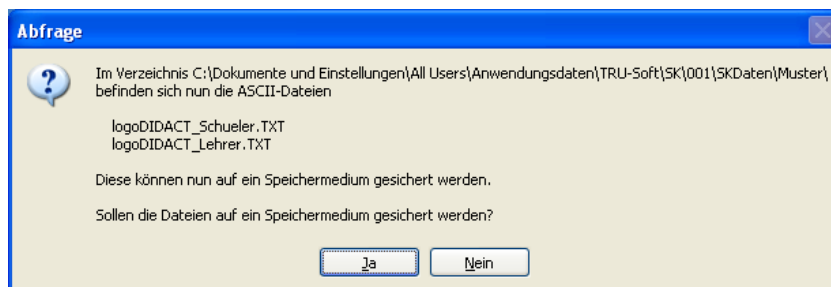


Abbildung B.21. Speichern der Text-Dateien (Schüler- und Lehrerliste)

Wählen Sie den passenden Laufwerksbuchstaben für Ihren Wechseldatenträger (sofern angebunden) oder alternativ „alle Laufwerke anzeigen“ für lokale Festplatten, Netzlaufwerke o.ä.

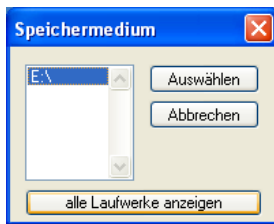


Abbildung B.22. Festlegen des Laufwerksbuchstaben

Nachdem Sie sich für einen Laufwerksbuchstaben entschieden haben, klicken Sie auf „**Auswählen**“.

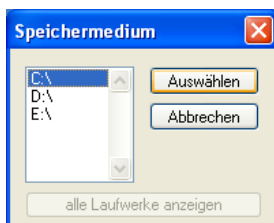


Abbildung B.23. Auswählen des Laufwerksbuchstaben

Im Beispiel werden die benötigten Unterverzeichnisse auf C : \ angelegt. Bestätigen Sie die nachfolgenden Info-Dialoge einfach mit „**OK**“.

1. Unterverzeichnis C : \SK-Export

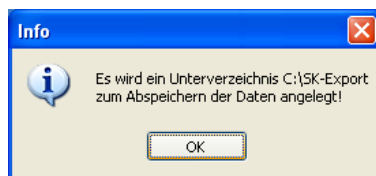


Abbildung B.24. Anlegen der Unterverzeichnisse SK-Export

2. Unterverzeichnis C : \SK-Export\logoDIDACTLinux

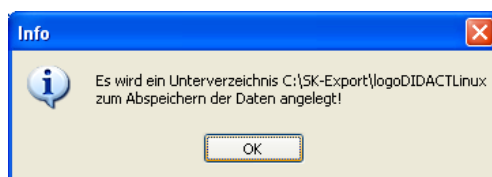


Abbildung B.25. Anlegen der Unterverzeichnisse SK-Export\logoDIDACTLinux

Abschließend erhalten Sie noch eine Meldung mit Hinweisen zu Fehlern, die ggf. beim Speichern aufgetreten sind.

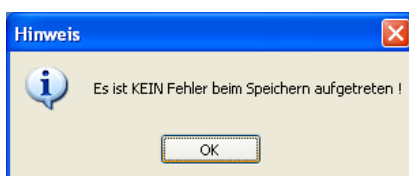


Abbildung B.26. Speichern der Text-Dateien OHNE Fehler