univention
be open.

UCS@school - Handbuch für Administratoren

Release 5.0

04.06.2025

Inhalt

UCS@school ist eine auf Univention Corporate Server (UCS) basierende IT-Komplettlösung mit zahlreichen Zusatzkomponenten für Nutzung, Betrieb und Management von Informationstechnologie (IT) in Schulen. UCS@school vereint die Stärken des Enterprise-Betriebssystems UCS im Bereich einfacher und zentraler Verwaltung von IT-Umgebungen mit den Vorteilen klassischer Schulsoftware für den Computereinsatz im Unterricht.

UCS ist die ideale Plattform für Schulen und Schulträger, um IT gemeinsam mit den dazu gehörenden Service- und Supportprozessen für eine oder mehrere Schulen zentral und wirtschaftlich bereitzustellen. UCS@school ergänzt UCS um zahlreiche Komponenten für den IT-Betrieb und den IT-gestützten Unterricht in der Schule.

Die Univention Management Console ermöglicht die zentrale, web-basierte Verwaltung aller Domänendaten (z.B. Benutzer, Gruppen, Rechner, DNS/DHCP). Die Speicherung der Daten erfolgt in einem Verzeichnisdienst auf Basis von OpenLDAP. Da viele Schuldaten primär in schulträgerspezifischen Systemen erfasst werden, bringt UCS@school unter anderem eine CSV-Datei-basierte Importschnittstelle für Schülerdaten mit.

Um den IT-gestützten Unterricht zu ergänzen, wurde die Benutzeroberfläche der Univention Management Console an die Anforderungen von Lehrern angepasst. Dies ermöglicht zum Beispiel die Organisation der Unterrichtsvorbereitung und Klassenraumplanung sowie die temporäre Sperrung des Internetzugangs für ausgewählte Computer. Lehrern ist es auch möglich, den Bildschirminhalt eines Schüler-PCs einzusehen, via Netzwerk individuelle Hilfestellungen zu geben oder einen beliebigen Desktop auf alle anderen Computer in der Klasse oder per Beamer zu übertragen. Auch bei im Schulalltag wiederkehrenden Tätigkeiten, wie dem Zurücksetzen von Passwörtern für Schüler-Benutzerkonten, werden Lehrer unterstützt.

Für die Bedienung der UCS@school-spezifischen Module der Univention Management Console steht *UCS@school - Handbuch für Lehrkräfte und Schuladministratoren* [1] bereit.

KAPITEL 1

Aufbau einer UCS@school-Umgebung

Univention Corporate Server (UCS) bietet ein plattformübergreifendes Domänenkonzept mit einem gemeinsamen Vertrauenskontext zwischen Linux- und Windows-Systemen. Innerhalb einer UCS-Domäne ist ein Benutzer mit seinem Benutzernamen und Passwort auf allen Systemen bekannt, und kann für ihn freigeschaltete Dienste nutzen.

UCS@school baut auf das flexible Domänenkonzept von UCS auf und integriert einige schulspezifische Erweiterungen.

1.1 UCS@school-Benutzerrollen

In einer Standard-UCS-Installation sind alle Benutzerkonten vom selben Typ und unterscheiden sich nur anhand ihrer Gruppenmitgliedschaften. In einer UCS@school-Umgebung ist jeder Benutzer einer *Rolle* zugeordnet, aus der sich Berechtigungen in der UCS@school-Verwaltung ergeben:

Schüler
: *Schülern* wird in der Standardeinstellung kein Zugriff auf die Administrationsoberflächen gewährt. Sie können sich mit ihren Benutzerkonten nur an Windows-Clients anmelden und die für sie freigegebenen Dateifreigaben und Drucker verwenden.

Lehrer
: *Lehrer* erhalten gegenüber Schülern zusätzliche Rechte, um z.B. auf UMC-Module zuzugreifen, die das Zurücksetzen von Schülerpasswörtern oder das Auswählen von Internetfiltern ermöglichen. Die einem Lehrer angezeigten Module können individuell definiert werden, Lehrer erhalten in der Regel aber nur Zugriff auf einen Teil der von der Univention Management Console bereitgestellten Funktionen.

Schuladministrator
: *Schuladministratoren* erhalten, auf den Servern ihrer jeweiligen Schule, administrativen Zugriff auf die UCS@school-UMC-Module. Sie können z.B. Computer zu Rechnergruppen zusammenfassen, neue Internetfilter definieren oder auch Lehrerpasswörter zurücksetzen. Schuladministratoren, die mit dem UCS@school-UMC-Modul erstellt werden, besitzen nicht die Option *UCS@school-Lehrer* und befinden sich nicht in der Gruppe `lehrer-OU` (siehe auch *Anlegen von Benutzerkonten für Schuladministratoren* (Seite 40)).

Mitarbeiter
: Der Benutzertyp *Mitarbeiter* kommt häufig im Umfeld der Schulverwaltung zum Einsatz. Er besitzt in der Standardeinstellung ähnliche Zugriffsrechte wie ein Schülerkonto, kann jedoch mit zusätzlichen Rechten ausgestattet werden (siehe auch *Verwaltungsnetz und Edukativnetz* (Seite 6)).

System-Administrator
: Die *System-Administratoren* sind Mitarbeiter mit vollem administrativen Zugriff auf die UCS@school-Systeme, also beispielweise ein IT-Dienstleister, der die Schule beim Betrieb der Server unterstützt.

Überschneidungen der Benutzertypen Lehrer, Mitarbeiter und Schuladministrator sind möglich. So können z.B. Benutzerkonten erstellt werden, die eine Nutzung des Kontos als Lehrer und Mitarbeiter ermöglichen.

Für die Pflege der Benutzerkonten stehen mehrere Möglichkeiten zur Verfügung. Die Bearbeitung von Benutzerkonten kann über die Univention Management Console erfolgen. Darüber hinaus bringt UCS@school flexible Importskripte mit. Sie lesen Tabulator-getrennte Importdateien oder CSV-Dateien ein, die üblicherweise aus vorhandenen Schulverwaltungssystemen extrahiert werden können und so einen automatisierten Abgleich ermöglichen.

1.2 Aufteilung von UCS@school

Für den Betrieb von UCS@school an einer einzelnen Schule reicht ein Serversystem aus (dieses wird dann in der UCS-Systemrolle *Primary Directory Node* installiert). Ein solches Szenario wird nachfolgend auch als *Single-Server-Umgebung* bezeichnet.

Für Schulträger oder große Schulen mit mehreren Standorten oder mit einer großen Anzahl an Clients, kann die UCS@school-Installation auf mehrere Server verteilt werden (*Multi-Server-Umgebung*). Dabei wird ein Primary Directory Node als der primäre Server zur Datenverwaltung genutzt. Für jeden Schul-Standort wird dann ein Replica Directory Node installiert, nachfolgend als *Schulserver* bezeichnet.

Vorsicht: UCS@school unterstützt derzeit für Edukativ- und Verwaltungsnetz jeweils nur einen Schulserver pro Standort.

Darüber hinaus können UCS-Systeme mit der Rolle *Managed-Node-Server* installiert und an den Schul-Standorten betrieben werden. Diese zusätzlichen UCS-Systeme können jedoch nicht in Verbindung mit UCS@school-Funktionalitäten eingesetzt werden; z.B. wird das Sperren von Dateifreigaben über die UCS@school-UMC-Module auf den zusätzlichen UCS-Systemen nicht unterstützt.

Zusätzlich müssen die Rechnerobjekte der zusätzlichen UCS-Systeme vor dem Domänenbeitritt unterhalb der Organisationseinheit (OU) der Schule angelegt werden (siehe auch *Replikation der LDAP-Daten auf die Schul-Standorte* (Seite 4)). Die Einrichtung zusätzlicher UCS-Systeme wird in *Skalierung von UCS@school Samba 4 Umgebungen* (Seite 89) beschrieben.

1.2.1 Replikation der LDAP-Daten auf die Schul-Standorte

Ein Schulserver bietet alle an einem Standort verwendeten Dienste an. Die Anfragen an den LDAP-Verzeichnisdienst erfolgen dabei gegen einen lokalen LDAP-Server, der automatisch gegen den Primary Directory Node fortlaufend repliziert und aktualisiert wird. Dies gewährleistet einen reibungslosen Betrieb, auch wenn die Verbindung zwischen Schulserver und dem zentralen Primary Directory Node einmal ausfallen sollte.

Aus Sicherheitsgründen speichern die Schulserver nur eine Teilreplikation des LDAP-Verzeichnisses. Nur die für den Schulserver relevanten Teile (z.B. Benutzer und Gruppen der jeweiligen Schule) sowie die globalen Strukturen des LDAP-Verzeichnisses, inklusive deren Benutzer und Gruppen, werden auf den Schul-Server übertragen.

Vorsicht: Benutzer, deren Benutzerkonto nicht unterhalb einer Organisationseinheit der Schule (Schul-OU) liegt, können ihr Passwort nur über die UMC des Primary Directory Node oder eines Backup Directory Node ändern (nicht über den Schulserver am Standort bzw. einem dort angebundenen Windows-Client).

Ebenso dürfen Benutzer, deren Benutzerkonto unterhalb einer Schul-Organisationseinheit liegt, aus Sicherheitsgründen nicht Mitglied der Gruppe `Domain Admins` sein.

In UCS@school werden schulübergreifende Benutzerkonten unterstützt. Ein Benutzerobjekt existiert im LDAP-Verzeichnis nur einmal an seiner primären Schule. An die weiteren Schulen wird nur ein Ausschnitt des

LDAP-Verzeichnisses dieser Schule repliziert: sein Benutzerobjekt und die Standardgruppen. Verlässt der Benutzer die Schule, wird sein Benutzerobjekt dort gelöscht bzw. nicht mehr dorthin repliziert. Schulübergreifende Benutzerkonten können nur mit Importskripten verwaltet werden.

Zur Unterteilung der im LDAP-Verzeichnisdienst hinterlegten Objekte und Einstellungen wird für jede Schule im LDAP-Verzeichnis eine eigene *Organisationseinheit* (OU) angelegt. Unterhalb dieser OU werden Container für z.B. Benutzerobjekte, Gruppen, DHCP-Einstellungen, usw. angelegt. Diese OUs werden direkt unterhalb der LDAP-Basis angelegt.

UCS@school unterscheidet in seinem Verzeichnisdienst zwischen dem Namen einer Schule und dem Schulkürzel (OU-Namen). Der Name einer Schule kann frei gewählt werden und wird primär in den UMC-Modulen angezeigt (in anderem Kontexten wird dieser Wert häufig auch als Anzeigename bezeichnet). Der eigentliche Name der Organisationseinheit (OU) wird nachfolgend auch als Schulkürzel bezeichnet. Das Schulkürzel sollte ausschließlich aus Buchstaben, Ziffern oder dem Bindestrich bestehen, da es unter anderem die Grundlage für Gruppen-, Freigabe- und Rechnernamen bildet. Häufig kommen hier Schulnummern wie *340* oder zusammengesetzte Kürzel wie `g123m` oder `gymmitte` zum Einsatz.

1.2.2 Replikation mehrerer Schulen auf einen Schulserver

Im Normalfall repliziert ein Schulserver die LDAP-Daten für genau eine Schule. Es gibt jedoch Szenarien, in denen es wünschenswert ist, wenn die LDAP-Daten (Benutzerkonten, Gruppen, Rechnerkonten, Räume, …) von mehreren Schulen auf einem Schulserver vorgehalten werden. Beginnend mit UCS@school 4.4v5 bietet UCS@school die Möglichkeit an, dass sich mehrere Schulen einen Schulserver teilen.

Dabei sind einige Randbedingungen zu beachten:

- Jede Schule darf nur auf *einen* Schulserver repliziert werden. Die Replikation einer Schule auf mehrere Schulserver ist nicht erlaubt und wird nicht unterstützt.
- Direkt nach dem Hinzufügen eines existierenden Schulservers zu einer neuen Schule muss der Schulserver erneut der Domäne beitreten (auf der Kommandozeile über den Befehl **`univention-join`**). Anderenfalls kann es zu Inkonsistenzen im LDAP-Verzeichnis aufgrund geänderter Zugriffsberechtigungen kommen.
- Der DHCP-Dienst wird auf Schulservern, die mehrere Schulen vorhalten, *nicht* unterstützt. Hier kann es in den Logdateien auf dem Schulserver ggf. zu Fehlermeldungen des DHCP-Dienstes kommen, die in diesem Szenario ignoriert werden können.
- Lehrkräfte können in der Univention Management Console nur die Benutzer, Klassen, Arbeitsgruppen, Druckaufträge, Computerräume und Rechner der Schulen sehen, in denen sie auch Mitglied sind. Eine Ausnahme bilden die UMC-Module *Klassenarbeiten* und *Materialien verteilen*, welche die Klassenarbeiten und Verteilungsprojekte aller Schulen anzeigen, die auf diesem Schulserver verwaltet werden, unabhängig davon, ob die Lehrkräfte Mitglied der jeweiligen anderen Schulen sind.
- Ein Computerraum kann nur einer einzelnen Schule zugeordnet werden. D.h er kann nicht von mehreren Schulen aus genutzt bzw. geteilt werden. Werden zwei Räume mit dem gleichen Namen an unterschiedlichen Schulen erstellt, handelt es sich für UCS@school um zwei vollkommen unabhängige Räume.
- Die Freigaben aller dem Schulserver zugeordneten Schulen werden von dem Dateiserver Samba angezeigt. Die Namen der Freigaben entsprechen i.d.R. dem Schema `$OU-$CLASS` bzw. `$OU-$WORKGROUP`. Der Zugriff auf die automatisch erstellten Freigaben wird über die Gruppenmitgliedschaften (Arbeitsgruppen/Klassen) gesteuert.
- Da der Schulserver die Authentifizierung für die Windows-Rechner durchführt, ist es allen Benutzern der Schulen eines Schulservers möglich, sich auf allen Windows-Rechnern anzumelden, die gegen den Schulserver gejoined wurden.
- Das Teilen eines Schulservers durch mehrere Schulen beschränkt sich auf die Schulserver des Edukativnetzes. Der Betrieb von mehreren Schulen auf einem Server des Verwaltungsnetzes wird nicht unterstützt!

  Nähere Informationen zu Verwaltungs- und Edukativnetzen finden sich in *Verwaltungsnetz und Edukativnetz* (Seite 6).

Die Einrichtung mehrerer Schulen auf einem Schulserver wird in *Mehrere Schulen auf einem Schulserver verwalten* (Seite 23) beschrieben.

1.3 Verwaltungsnetz und Edukativnetz

Die Netze für den edukativen Bereich und für die Schulverwaltung müssen aus organisatorischen oder rechtlichen Gründen in der Regel logisch und/oder physikalisch getrennt werden. In UCS@school kann daher zusätzlich zur Unterteilung in Organisationseinheiten (OU) noch eine Unterteilung der OU in Verwaltungsnetz und Edukativnetz erfolgen.

Diese optionale Unterteilung findet auf Ebene der Serversysteme bzw. der Netzwerksegmente statt und sieht vor, dass in einer Schule ein Schulserver für das edukative Netz und ein Schulserver für das Verwaltungsnetz betrieben wird. Diese Server verwenden für ihre Client-Systeme (Schülerrechner bzw. Rechner der Verwaltung) jeweils ein eigenes IP-Subnetz.

Auch bei der Unterteilung in Verwaltungsnetz und Edukativnetz findet eine selektive Replikation statt, wie sie in *Replikation der LDAP-Daten auf die Schul-Standorte* (Seite 4) beschrieben wird. Zusätzlich wird jedoch bei der Replikation der Benutzerkonten anhand ihrer Benutzerrolle(n) unterschieden.

Auf den Schulserver des edukativen Netzes werden die Benutzerkonten mit den Benutzerrollen *Schüler*, *Lehrer*, *Schuladministrator* und *System-Administrator* repliziert. Auf den Schulserver der Verwaltung werden die Benutzerkonten mit den Benutzerrollen *Mitarbeiter*, *Schuladministrator* und *System-Administrator* repliziert. Die gemeinsame Verwendung der Benutzerrollen *Lehrer* und *Mitarbeiter* für ein Benutzerkonto ist möglich, z.B. für Benutzerkonten der Schulleitung, die neben ihrer Verwaltungstätigkeit auch lehrend tätig sind.

Bemerkung: Die Einrichtung eines Verwaltungsnetzes ist in einer Single-Server-Umgebung nicht möglich. Hier werden alle Benutzerkonten auf dem Primary Directory Node vorgehalten.

Vorsicht: UCS@school setzt für die Unterteilung in Edukativ- und Verwaltungsnetz eine physikalische Trennung der beiden Netzwerksegmente voraus. D.h. das edukative Netz und das Verwaltungsnetz können nicht gleichzeitig im gleichen Netzwerksegment verwendet werden. Ergänzend dazu müssen auch die Hinweise zu DHCP-DNS-Richtlinien in *Installation eines Schulservers* (Seite 17) beachtet werden.

1.3.1 Mitarbeiter im Edukativnetz

Benutzerkonten mit der Benutzerrolle *Mitarbeiter* aus dem Verwaltungsnetz können explizit auf Schulserver im Edukativnetz repliziert werden. Benutzer in dieser Rolle können sich anschließend gegen den Schulserver im Edukativnetz authentifizieren und so zum Beispiel Zugriff auf Dateifreigaben erhalten oder sich an einem Client anmelden, der Teil der lokalen Domäne ist. Sie können zu Arbeitsgruppen hinzugefügt werden. Mitarbeiter können keine edukativen UMC Module verwenden, wie zum Beispiel die Computerraumverwaltung oder den Klassenarbeitsmodus.

Folgende Schritte sind nötig, um die Replikation von Benutzern in der Rolle *Mitarbeiter* auf Schulserver im Edukativnetz zu aktivieren:

1. Auf dem Primary Directory Node und *allen* Backup Directory Nodes müssen die LDAP ACLs angepasst und der LDAP-Server neu gestartet werden:

```
$ ucr set ucsschool/ldap/replicate_staff_to_edu="true"
$ ucr commit /etc/ldap/slapd.conf
$ systemctl restart slapd
```

2. Nach der Änderung der LDAP ACLs werden nur modifizierte und neu erstellte Benutzerkonten *automatisch* repliziert, solange kein erneuter Domänenbeitritt durchgeführt wird. Um *bestehende* Benutzerkonten zu replizieren, müssen die Schulserver im Edukativnetz der Domäne erneut beitreten. Nach der Aktivierung zusätzlicher LDAP ACLs können alle Schulserver im Edukativnetz die Benutzerkonten der Rolle *Mitarbeiter* vom Primary Directory Node und den Backup Directory Nodes lesen.

Vorsicht: Wenn alle bestehenden Benutzerkonten der Rolle *Mitarbeiter* in einem Lauf repliziert werden sollen, müssen edukative Schulserver mit `univention-join` der Domäne erneut beitreten. Hierbei ist zu beachten, dass der erneute Domänenbeitritt eines edukativen Schulservers einige Zeit in Anspruch nimmt und in der Zwischenzeit nicht verwendet werden kann. Planen Sie dafür ein Wartungsfenster ein.

1.3.2 Schulserver im Verwaltungsnetz

Auf den Schulservern des Verwaltungsnetzes werden keine speziellen Dienste oder UMC-Module angeboten. Sie dienen den Verwaltungsrechnern hauptsächlich als Anmelde-, Druck- und Dateiserver. Die Benutzerkonten mit der Benutzerrolle *Mitarbeiter* haben entsprechend keinen Zugriff auf die UCS@school-spezifischen UMC-Module des edukativen Netzes. Im Gegensatz zu den Benutzern des edukativen Netzes werden für die Benutzer des Verwaltungsnetzes keine automatischen Einstellungen für Windows-Profilverzeichnis oder Windows-Heimatverzeichnis gesetzt.

Die Installationsschritte für Schulserver des Edukativnetzes und des Verwaltungsnetzes sind sehr ähnlich. In *Installation eines Schulservers* (Seite 17) werden diese ausführlich beschrieben.

1.4 UCS@school-Objekte im LDAP-Verzeichnisdienst

UCS@school erstellt zur Verwaltung der schulspezifischen Erweiterungen zusätzliche Strukturen im LDAP-Verzeichnisdienst. Im Folgenden werden einige Funktionen dieser Container und Objekte genauer vorgestellt.

Wie bereits im *Replikation der LDAP-Daten auf die Schul-Standorte* (Seite 4) beschrieben wurde, wird für jede Schule direkt unterhalb der LDAP-Basis eine eigene Organisationseinheit (OU) angelegt. Unterhalb dieser OU werden Container für Benutzerobjekte, Gruppen und weitere UCS@school-relevante Objekte erstellt. Darüber hinaus werden einige neue Objekte in den bereits bestehenden UCS-Strukturen des LDAP-Verzeichnisses angelegt.

1.4.1 Struktur einer UCS@school-OU

Der Aufbau einer Schul-OU wird nachfolgend am Beispiel der Schul-OU `gymmitte` in einem LDAP-Verzeichnis mit der LDAP-Basis `dc=example,dc=com` erläutert.

- `cn=computers,ou=gymmitte,dc=example,dc=com`

  In diesem Container werden Rechnerobjekte abgelegt, die von der OU verwaltet werden. Dies können z.B. Objekte vom Typ *Windows-Client* oder *IP-Managed-Client* sein. Die Rechnerobjekte für Schulserver (Verwaltungs- und Edukativnetz) werden in dem Untercontainer `cn=dc,cn=server,cn=computers,ou=gymmitte,dc=example,dc=com` abgelegt.

- `cn=examusers,ou=gymmitte,dc=example,dc=com`

  Dieser Container enthält temporäre Prüfungsbenutzer, die für den Klassenarbeitsmodus benötigt werden. Sie werden zu Beginn bzw. nach Beendigung des Klassenarbeitsmodus automatisch erstellt bzw. wieder gelöscht.

- `cn=groups,ou=gymmitte,dc=example,dc=com`

  `cn=raeume,cn=groups,ou=gymmitte,dc=example,dc=com`

  `cn=schueler,cn=groups,ou=gymmitte,dc=example,dc=com`

  `cn=klassen,cn=schueler,cn=groups,ou=gymmitte,dc=example,dc=com`

  In den aufgeführten Containern werden Gruppenobjekte für UCS@school vorgehalten. Im Container `cn=groups` werden automatisch einige Standard-Gruppen angelegt, die alle Schüler, Lehrer bzw. Mitarbeiter der Schul-OU als Gruppenmitglied enthalten. Diese Gruppen werden bei der Verwendung der UCS@school-Import-Mechanismen automatisch gepflegt. Beim Import von Benutzern über die Importskripte oder über die UMC-Module wird den Benutzern je nach ihrer Benutzerrolle eine der drei Gruppen automatisch als primäre Gruppe zugeordnet. Die Namen der drei Gruppen lauten `schueler-gymmitte`, `lehrer-gymmitte` und `mitarbeiter-gymmitte`.

Gruppenobjekte für Schulklassen müssen im Untercontainer `cn=klassen` abgelegt werden, damit diese von UCS@school korrekt als Klassengruppe erkannt werden. Im übergeordneten Container `cn=schueler` werden von den UCS@school-Modulen Gruppenobjekte für klassenübergreifende Arbeitsgruppen (z.B. Musik-AG) gepflegt, die z.B. über das UMC-Modul *Arbeitsgruppen verwalten* erstellt werden.

Beim Anlegen von Räumen über das UMC-Modul *Computerräume verwalten* werden ebenfalls Gruppenobjekte erstellt, die im Container `cn=raeume` abgelegt werden. Diese Gruppenobjekte enthalten üblicherweise ausschließlich Rechnerobjekte als Gruppenmitglieder.

- `cn=shares,ou=gymmitte,dc=example,dc=com`

  `cn=klassen,cn=shares,ou=gymmitte,dc=example,dc=com`

  Die beiden Container enthalten allgemeine bzw. klassenspezifische Freigabeobjekte für die Schul-OU.

- `cn=users,ou=gymmitte,dc=example,dc=com`

  Die Benutzerobjekte für UCS@school müssen entsprechend ihrer Benutzerrolle in einem der vier Untercontainer `cn=schueler`, `cn=lehrer`, `cn=lehrer und mitarbeiter`, `cn=mitarbeiter` oder `cn=admins` erstellt werden.

- `cn=dhcp,ou=gymmitte,dc=example,dc=com`

  `cn=networks,ou=gymmitte,dc=example,dc=com`

  `cn=policies,ou=gymmitte,dc=example,dc=com`

  `cn=printers,ou=gymmitte,dc=example,dc=com`

  Die genannten Container enthalten (analog zu ihrem globalem Pendant direkt unterhalb der LDAP-Basis) die DHCP-, Netzwerk-, Richtlinien- und Drucker-Objekte für die jeweilige Schul-OU.

Bemerkung: UCS@school unterstützt aktuell keine weitere Strukturierung der LDAP-Objekte durch Untercontainer oder Unter-OUs in den oben angegebenen Containern.

1.4.2 Weitere UCS@school-Objekte

Für die Steuerung von Zugriffsrechten auf UCS@school-Funktionen und das LDAP-Verzeichnis werden mit dem Erstellen einer neuen Schul-OU automatisch einige Gruppen erstellt. Auch diese Gruppen werden am Beispiel der OU `gymmitte` in einem LDAP-Verzeichnis mit der LDAP-Basis `dc=example,dc=com` erläutert.

- `cn=DC-Edukativnetz,cn=ucsschool,cn=groups,dc=example,dc=com`

  `cn=DC-Verwaltungsnetz,cn=ucsschool,cn=groups,dc=example,dc=com`

  `cn=Member-Edukativnetz,cn=ucsschool,cn=groups,dc=example,dc=com`

  `cn=Member-Verwaltungsnetz,cn=ucsschool,cn=groups,dc=example,dc=com`

  Diese Gruppen werden beim Erstellen der ersten Schul-OU einmalig angelegt und sind nicht spezifisch für eine bestimmte OU. Sie enthalten (entsprechend ihrem Namen) als Gruppenmitglieder die Schul-DCs oder die Managed Node Server der Schulstandorte, wobei diese jeweils nach Verwaltungsnetz und Edukativnetz getrennt werden. Über diese Gruppen werden Zugriffsrechte von UCS@school-Systemen auf die UCS@school-Objekte im LDAP gesteuert. Primary Directory Node und Backup Directory Node dürfen **kein** Mitglied in einer dieser Gruppen sein.

- `cn=OUgymmitte-DC-Edukativnetz,cn=ucsschool,cn=groups,dc=example,dc=com`

  `cn=OUgymmitte-DC-Verwaltungsnetz,cn=ucsschool,cn=groups,dc=example,dc=com`

  `cn=OUgymmitte-Member-Edukativnetz,cn=ucsschool,cn=groups,dc=example,dc=com`

  `cn=OUgymmitte-Member-Verwaltungsnetz,cn=ucsschool,cn=groups,dc=example,dc=com`

Diese OU-spezifischen Gruppen werden während des Anlegens der Schul-OU erstellt. Sie enthalten (entsprechend ihrem Namen) als Gruppenmitglieder die Schul-DCs oder die Managed Node Server der jeweiligen OU (hier `gymmitte`), wobei diese jeweils nach Verwaltungsnetz und Edukativnetz getrennt werden. Primary Directory Node und Backup Directory Node dürfen **kein** Mitglied in einer dieser Gruppen sein.

- `cn=OUgymmitte-Klassenarbeit,cn=ucsschool,cn=groups,dc=example,dc=com`

  Während eines laufenden Klassenarbeitsmodus werden die beteiligten Benutzer und Rechner als Gruppenmitglieder zu dieser Gruppe hinzugefügt. Sie wird z.B. für die Steuerung von speziellen Einstellungen für den Klassenarbeitsmodus verwendet.

- `cn=admins-gymmitte,cn=ouadmins,cn=groups,dc=example,dc=com`

  Benutzer, die Mitglied dieser Gruppe sind, werden von UCS@school in der betreffenden OU automatisch als Schuladministrator behandelt. Siehe dazu auch *Anlegen von Benutzerkonten für Schuladministratoren* (Seite 40).

KAPITEL 2

Installation

UCS@school basiert auf Univention Corporate Server (UCS) und wird dabei als Repository-Komponente aus dem Univention App Center eingebunden. Die Installation von UCS[1] ist *Univention Corporate Server - Handbuch für Benutzer und Administratoren* [2] dokumentiert. Nachfolgend wird nur auf ggf. auftretende Unterschiede zur Grundinstallation von Univention Corporate Server sowie die Installation von UCS@school selbst eingegangen.

Im Folgenden werden zwei Installationsvarianten beschrieben:

1. Die Installation als Single-Server-Umgebung
2. Die Installation als Multi-Server-Umgebung mit einem Primary Directory Node und mindestens einem Schulserver.

In beiden Fällen wird empfohlen, während des Installationsprozesses von UCS@school keine weiteren Aktionen in der UMC oder auf der Kommandozeile auszuführen. Sollten Sie das Fenster im Browser während des Installationsprozesses von UCS@school schließen, läuft die Installation selbst dennoch auf dem System weiter. Um den Status der Installation dann noch zu überprüfen, können Sie die Logdatei in `/var/log/univention/management-console-module-schoolinstaller.log` konsultieren.

Die nachträgliche Umwandlung einer Single-Server-Umgebung in eine Multi-Server-Umgebung wird unterstützt und in *Umwandlung Single-Server- in Multi-Server-Umgebung* (Seite 19) genauer beschrieben.

In beiden Varianten wird standardmäßig bei der Erstinstallation von UCS@school auf dem Primary Directory Node eine Demonstrationsschule inklusive Testnutzern konfiguriert. Die Schule trägt den Namen *DEMOSCHOOL* und kann für eigene Tests verwendet werden. Das Passwort für die automatisch angelegten Nutzer `demo_student`, `demo_teacher` und `demo_admin` befindet sich in der Datei `/etc/ucsschool/demoschool.secret`. Um das Anlegen der Demonstrationsschule zu verhindern, muss die UCR-Variable `ucsschool/join/create_demo` auf den Wert `no` gesetzt werden, **bevor** der UCS@school-Konfigurationsassistent durchlaufen wird. Das Setzen der UCR-Variable ist entweder über das UMC-Modul *Univention Configuration Registry* oder auf der Kommandozeile mit dem Befehl **`ucr set ucsschool/join/create_demo=no`** möglich.

Neu in Version 4.4: Der Installationsprozess nutzt seit UCS@school 4.4 das Feature *Join-Hooks*.

Join-Hooks werden in einer UCS@school-Umgebung vom Primary Directory Node im LDAP-Verzeichnis hinterlegt und automatisch während des Join-Vorgangs bzw. während der Ausführung von Join-Skripten ausgeführt. Der UCS@school-Join-Hook installiert auf allen Systemen der Domäne automatisch die App **`UCS@school`** aus dem Univention App Center und installiert die auf dem jeweiligen System benötigten UCS@school-Pakete, sofern diese fehlen. Für die Erstinstallation der Pakete wird der Join-Hook je nach Rolle des Systems und dessen Systemperformance mehrere Minuten benötigen. Der Join-Vorgang darf dabei nicht abgebrochen werden.

[1] https://docs.software-univention.de/manual/5.0/de/installation.html#installation-chapter

Der Hostname darf nur aus Kleinbuchstaben, Ziffern sowie dem Bindestrich bestehen (`a-z`, `0-9` und `-`) und zur Trennung nur einzelne Punkte enthalten. Der Hostname darf außerdem nur mit einem Kleinbuchstaben beginnen, mit einem Kleinbuchstaben oder einer Ziffer enden und ist auf eine Länge von 13 Zeichen beschränkt.

2.1 Installation einer Single-Server-Umgebung

Zunächst muss ein UCS System mit der Systemrolle *Primary Directory Node* (kurz: Primary) installiert werden. Die Installation von UCS[2] ist in *Univention Corporate Server - Handbuch für Benutzer und Administratoren* [2] beschrieben. Es ist empfohlen während der Installation keine zusätzliche Software auszuwählen.

Nach der erfolgreichen UCS-Installation muss die App **`UCS@school`** installiert werden. Jedes UCS-System bietet ein webbasiertes Konfigurationsinterface an, Univention Management Console, kurz UMC. Dies ist via Webbrowser erreichbar, dazu kann einfach der Name oder die IP-Adresse des Servers in die Adresszeile des Webbrowsers eingegeben werden. Es erscheint eine Kachel mit der Bezeichnung *System- und Domäneneinstellungen*. Nach einem Klick auf die Kachel wird eine Anmeldemaske angezeigt. Dort erfolgt die Anmeldung mit dem Benutzer `Administrator`. Sofern noch nicht geändert, entspricht das Passwort dem während der UCS-Installation vergebenen Passwort für den Benutzer `root`.

Nun kann die Kachel *App Center* geöffnet und dort die Applikation *UCS@school* installiert werden. Für die Installation ist den Anweisungen zu folgen, bspw. kann eine Lizenzaktivierung notwendig sein. Details dazu sind im *Univention Corporate Server - Handbuch für Benutzer und Administratoren* [2] zu finden.

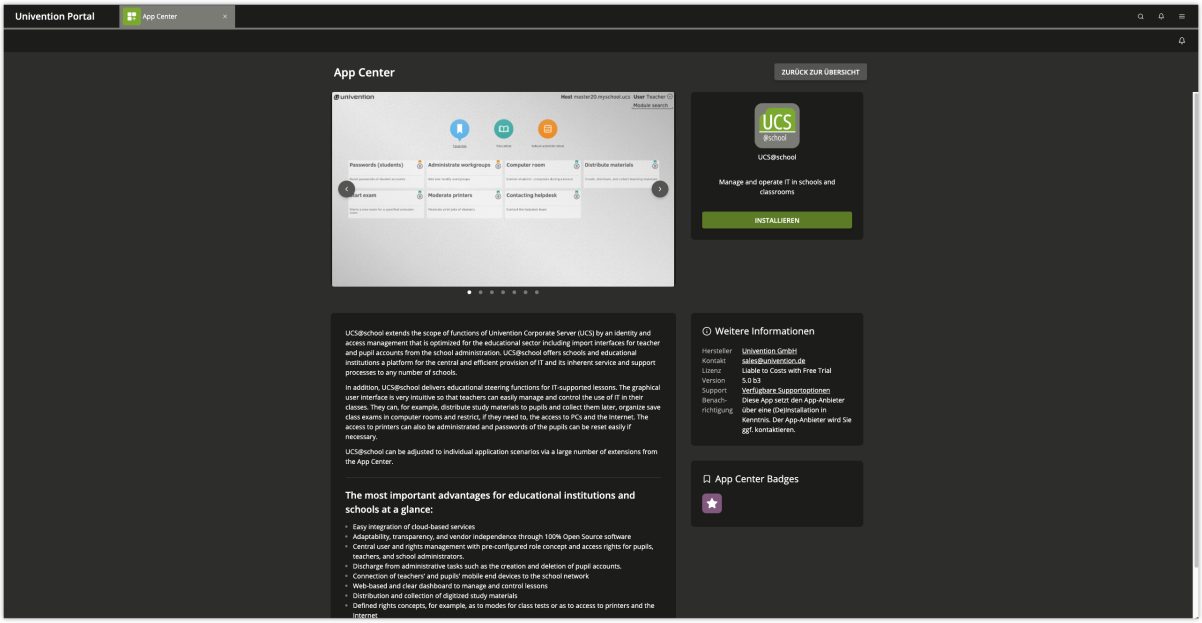

Abb. 2.1: Installation von UCS@school über das Univention App Center

Nach dem Abschluss der Installation über das App Center erfolgt die Konfiguration von UCS@school. Diese wird mit dem UCS@school Konfigurationsassistenten durchgeführt. Dieser ist in UMC über den Bereich *Schul-Administration* erreichbar.

Auf der ersten Seite fragt der Konfigurationsassistent nach dem Installationsszenario. Hier ist die `Single-Server-Umgebung` auszuwählen.

Auf der zweiten Seite muss der Name der Schule und das Schulkürzel eingegeben werden. Innerhalb von UCS@school wird dieser Name immer wieder angezeigt. Sobald der Name der Schule eingetragen ist und in das Feld für das Schulkürzel geklickt wird, wird ein Wert für das Schulkürzel vorgeschlagen. Dieser Wert kann entsprechend angepasst werden.

- Der Name der Schule kann dabei Leerzeichen und Sonderzeichen enthalten.

[2] https://docs.software-univention.de/manual/5.0/de/installation.html#installation-chapter

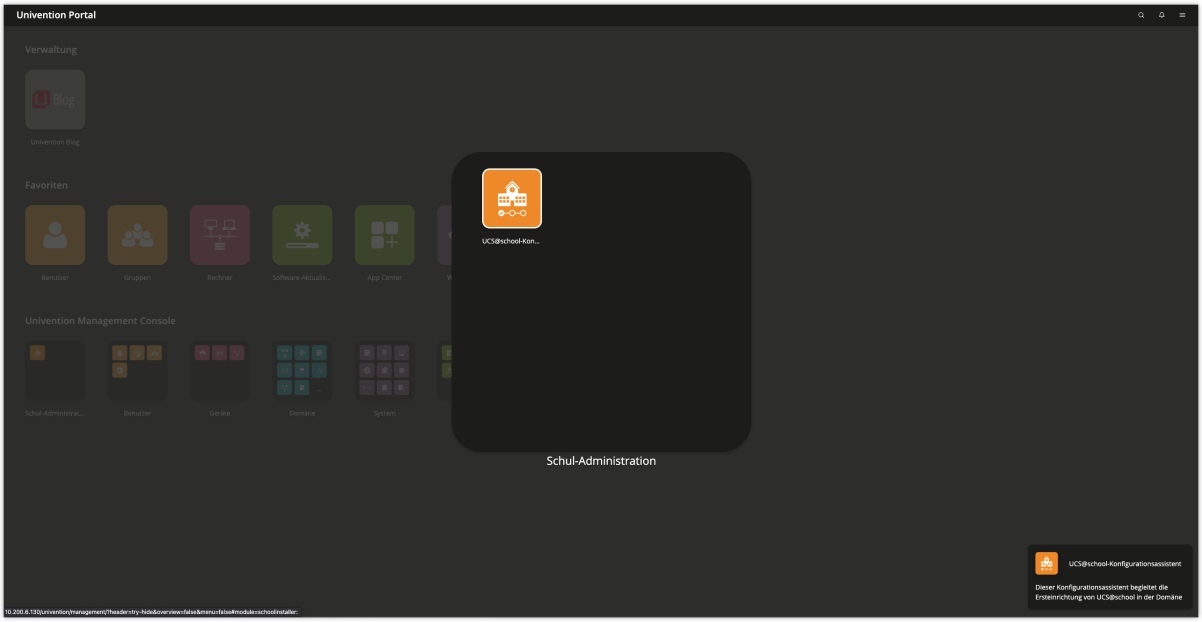

Abb. 2.2: Starten des UCS@school-Konfigurationsassistenten

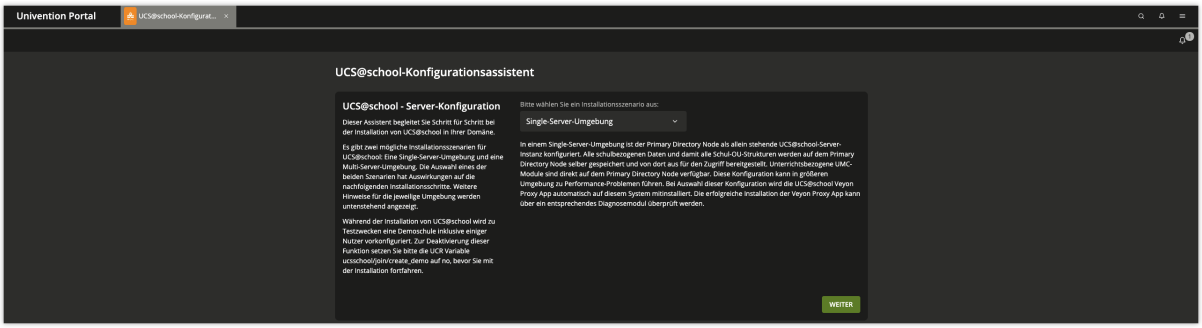

Abb. 2.3: Single-Server-Umgebung

- Das Schulkürzel darf nur aus Buchstaben, Zahlen und Unterstrichen bestehen.

Das Schulkürzel wird im Verzeichnisdienst als Name für die Organisationseinheiten (OU) verwendet (siehe auch *Aufbau einer UCS@school-Umgebung* (Seite 3)), zusätzlich wird das Schulkürzel als Grundlage für Gruppen-, Freigabe- und Rechnernamen verwendet.

Wichtig: Das Schulkürzel kann nach der initialen Konfiguration von UCS@school nicht mehr modifiziert werden.

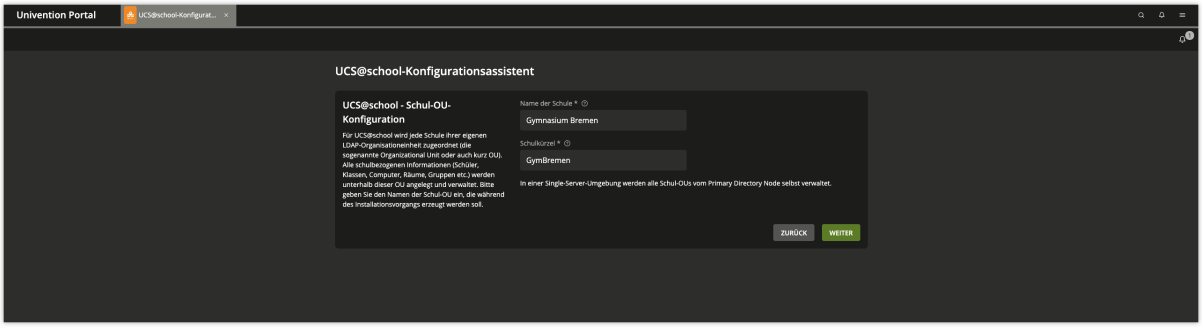

Abb. 2.4: Eingabe der Schuldaten

Nach der abschließenden Bestätigung startet die Konfiguration von UCS@school. Dabei werden diverse Pakete installiert und konfiguriert. Die Dauer schwankt je nach Geschwindigkeit der Internetverbindung und Serverausstattung.

Installation und Konfiguration von UCS@school sollten mit einem Neustart des Systems abgeschlossen werden. Im Anschluss kann die weitere Konfiguration der Schule vorgenommen werden, siehe *Verwaltung von Schulen über Importskripte* (Seite 31).

Wichtig: Nach Abschluss der Installation auf dem Primary Directory Node muss auf allen anderen gejointen Systemen der Domäne der Befehl **`univention-run-join-scripts`** ausgeführt werden, damit der installierte UCS@school-Join-Hook benötigte Konfigurationspakete auf den Systemen nachinstallieren kann.

Dieser Vorgang kann je nach Rolle des Systems und dessen Systemperformance mehrere Minuten dauern und darf nicht unterbrochen werden.

2.2 Installation einer Multi-Server-Umgebung

Das Konzept der Multi-Server-Umgebung von UCS@school sieht zentrale Server für Cloud-Dienste wie Portal, Mail, Kalender, Dateiablage usw. kombiniert mit lokalen Schulservern für Anmeldedienste, IT-Infrastruktur und pädagogischen Funktionen vor. Eine Übersicht an möglichen Szenarien wird in *UCS@school - Szenarien zum Einsatz von UCS@school* [3] dargestellt.

Der Installationsprozess für die unterschiedlichen Rechnerrollen in der UCS@school-Domäne wird in den nachfolgenden Abschnitten genauer beschrieben.

2.2.1 Installation des Primary Directory Node

Zunächst muss ein UCS System mit der Systemrolle *Primary Directory Node* installiert werden. Die Installation von UCS[3] ist in *Univention Corporate Server - Handbuch für Benutzer und Administratoren* [2] beschrieben. Sofern der Primary Directory Node als Active Directory-kompatibler Domänencontroller genutzt werden soll, so kann die Software bereits während der UCS-Installation ausgewählt werden.

Nach der erfolgreichen UCS-Installation muss die App **`UCS@school`** installiert werden. Jedes UCS System bietet ein webbasiertes Konfigurationsinterface an, Univention Management Console, kurz UMC. Dies ist via Webbrowser erreichbar, dazu kann einfach der Name oder die IP-Adresse des Servers in die Adresszeile des Webbrowsers eingegeben werden. Es erscheint eine Kachel mit der Bezeichnung System- und Domäneneinstellungen. Nach einem Klick auf die Kachel wird eine Anmeldemaske angezeigt. Dort erfolgt die Anmeldung mit dem Benutzer `Administrator` und dem während der UCS-Installation vergebenen Passwort für den Benutzer `root`.

Nun kann die Kachel *App Center* geöffnet und dort die Applikation **`UCS@school`** installiert werden. Für die Installation ist den Anweisungen zu folgen, bspw. kann eine Lizenzaktivierung notwendig sein. Details dazu sind im *Univention Corporate Server - Handbuch für Benutzer und Administratoren* [2] unter Univention App Center[4] zu finden.

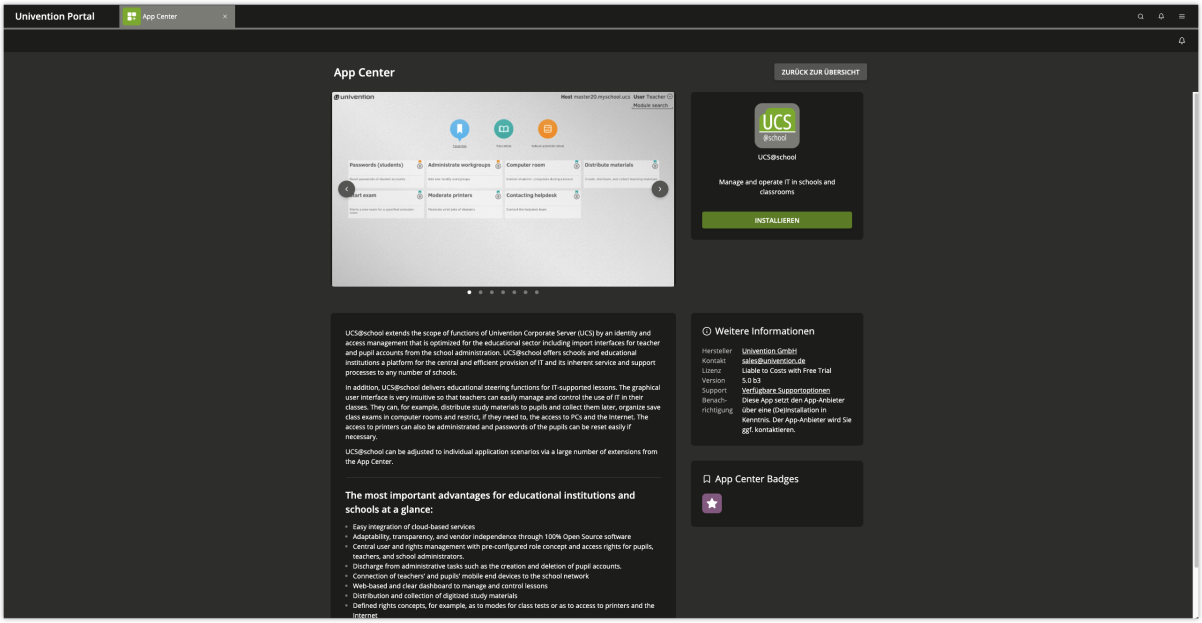

Abb. 2.5: Installation von UCS@school über das Univention App Center

Nach dem Abschluss der Installation über das App Center erfolgt die Konfiguration von UCS@school. Diese wird mit dem UCS@school-Konfigurationsassistenten durchgeführt. Dieser ist in UMC über den Bereich *Schul-Administration* erreichbar.

Auf der ersten Seite fragt der Konfigurationsassistent nach dem Installationsszenario. Hier ist die `Multi-Server-Umgebung` auszuwählen.

Nach der abschließenden Bestätigung startet die Konfiguration von UCS@school. Dabei werden diverse Pakete installiert und konfiguriert. Die Dauer schwankt je nach Geschwindigkeit der Internetverbindung und Serverausstattung.

Installation und Konfiguration von UCS@school sollten mit einem Neustart des Systems abgeschlossen werden.

Wichtig: Nach Abschluss der Installation auf dem Primary Directory Node muss auf allen anderen gejointen Systemen der Domäne der Befehl **`univention-run-join-scripts`** ausgeführt werden, damit der installierte UCS@school-Join-Hook benötigte Konfigurationspakete auf den Systemen nachinstallieren kann.

[3] https://docs.software-univention.de/manual/5.0/de/installation.html#installation-chapter
[4] https://docs.software-univention.de/manual/5.0/de/software/app-center.html#software-appcenter

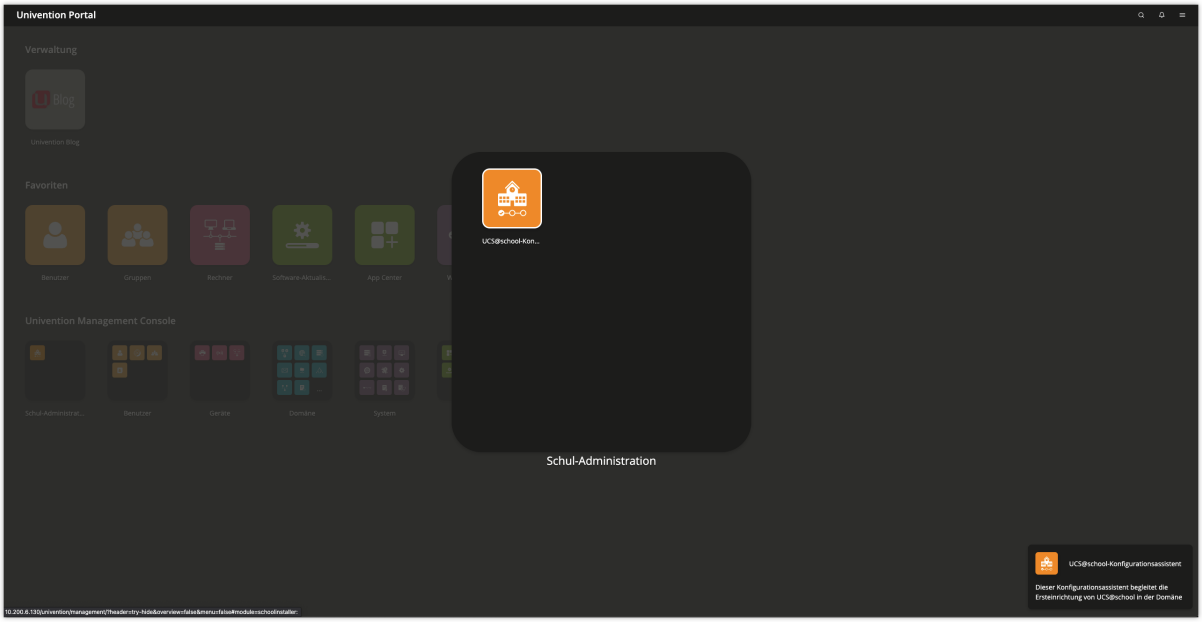

Abb. 2.6: Starten des UCS@school-Konfigurationsassistenten

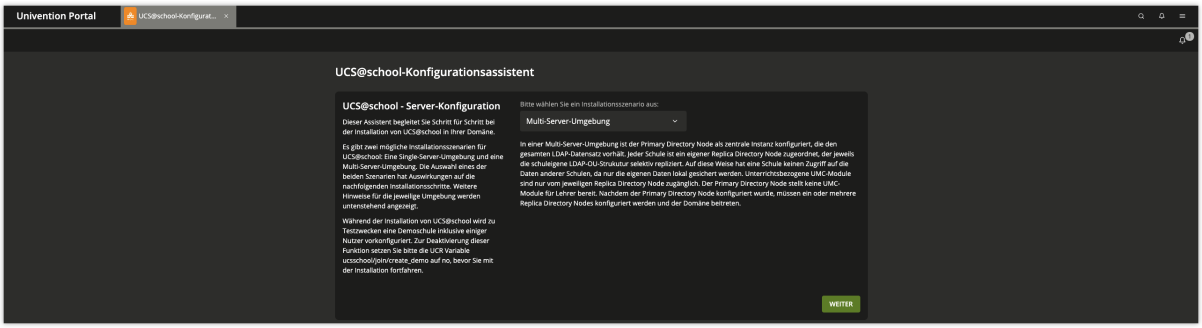

Abb. 2.7: Multi-Server-Umgebung

Dieser Vorgang kann je nach Rolle und Systemperformance mehrere Minuten dauern und darf nicht unterbrochen werden.

2.2.2 Installation eines Backup Directory Node (optional)

Auf Servern mit der Rolle *Backup Directory Node* (kurz: Backup) werden alle Domänendaten und SSL-Sicherheitszertifikate als Nur-Lese-Kopie gespeichert.

Ein Backup Directory Node dient als Fallback-System des Primary Directory Node. Sollte dieser ausfallen, kann ein Backup Directory Node die Rolle des Primary Directory Node dauerhaft übernehmen. Der Einsatz eines Backup Directory Node ist optional.

Es muss ein neues Backup Directory Node System installiert werden. Während des Domänenbeitritts (oder der Ausführung von **`univention-run-join-scripts`**) werden auf diesem System durch den in den vorigen Abschnitten bereits erwähnten UCS@school-Join-Hook automatisch die gleichen Pakete wie auf dem Primary Directory Node installiert. Es werden dabei jedoch nur die Softwarepakete installiert. Falls nach der Installation Änderungen an der Konfiguration auf dem Primary Directory Node vorgenommen werden, müssen diese manuell auf den/die Backup-Systeme übertragen werden, damit diese in einem *Backup2Master*-Szenario die Rolle des Primary Directory Node ohne Probleme übernehmen können.

Je nach Systemperformance und Netzanbindung wird der Domänenbeitritt einige Minuten länger dauern als in reinen UCS-Domänen ohne UCS@school.

Nach dem Domänenbeitritt (und damit der Installation von UCS@school) sollte das System neu gestartet werden.

2.2.3 Installation eines Schulservers

Der edukative Schulserver, im folgenden Schulserver genannt, liefert die Anmeldedienste für Schüler und Lehrer an einer Schule.

Zusätzlich bietet der Schulserver die Funktionen für den IT-gestützten Unterricht. Ob die Installation eines Schulservers für die jeweilige UCS@school-Umgebung notwendig ist, kann *UCS@school - Szenarien zum Einsatz von UCS@school* [3] entnommen werden, welches unterschiedliche Anwendungsszenarien aufzeigt.

Soll ein Schulserver installiert werden, muss zunächst für diesen Schulserver eine Schule angelegt werden. Das Anlegen von Schulen wird in *Anlegen von Schulen* (Seite 22) ausführlich beschrieben. Dieser Schritt muss zwingend *vor* der Installation des Schulservers bzw. seinem Domänenbeitritt erfolgen, da dieser sonst als normales UCS-System ohne spezielle UCS@school-Funktionalitäten eingerichtet wird.

Nach dem Anlegen der Schule muss ein UCS-System mit der Systemrolle *Replica Directory Node* installiert werden. Die Installation von UCS[5] ist in *Univention Corporate Server - Handbuch für Benutzer und Administratoren* [2] beschrieben. Während der Installation ist darauf zu achten, dass der Rechnername bei der Installation mit dem Namen des Schulservers übereinstimmt, der beim Anlegen der Schule angegeben wurde.

Nach der Angabe des Schulservernamens wird vom UCS-Installer ab UCS 4.4-1 die Rolle abgefragt, die der Schulserver in der UCS@school-Domäne übernehmen soll. Für einen edukativen Schulserver ist hier `Schulserver im Edukativnetz` auszuwählen. Der UCS-Installer gleicht die gemachte Angabe mit der Konfiguration der bereits angelegten Schule ab und weist ggf. auf Widersprüche hin. Für die Installation von UCS@school muss im UCS-Installer keine zusätzliche Software ausgewählt werden. Für UCS@school notwendige Softwarepakete werden automatisch mitinstalliert.

Nach der UCS-Installation und erfolgreichem Domänenbeitritt ist auf dem System auch die App **`UCS@school`** installiert.

Jedes UCS-System bietet ein webbasiertes Konfigurationsinterface an, Univention Management Console, kurz UMC. Dies ist via Webbrowser erreichbar, dazu kann einfach der Name oder die IP-Adresse des Servers in die Adresszeile des Webbrowsers eingegeben werden. Es erscheint eine Kachel mit der Bezeichnung *Systemeinstellungen*. Nach einem

[5] https://docs.software-univention.de/manual/5.0/de/installation.html#installation-chapter

Klick auf die Kachel wird eine Anmeldemaske angezeigt. Dort erfolgt die Anmeldung mit dem Benutzer `Administrator`, sofern noch nicht geändert, entspricht das Passwort dem während der Primary Directory Node Installation vergebenen Passwort für den Benutzer `root`.

Vorsicht: Die *nachträgliche* Installation von UCS@school auf einem bestehenden Replica Directory Node und die Verwendung als Schulserver ist nicht möglich. Der Verwendungszweck des Systems wird während des Domänenbeitritts festgelegt.

Falls das Anlegen der Schule und das Hinterlegen des Rechnernamens an der Schule versäumt wurde, wird das System während des Domänenbeitritts als normaler Replica Directory Node ohne spezielle UCS@school-Funktionalität eingerichtet.

Soll das System trotzdem als Schulserver im Edukativ- oder Verwaltungsnetz eingesetzt werden, muss zunächst das existierende Rechnerobjekt im LDAP-Verzeichnisdienst entfernt werden. Anschließend ist der Rechnername, wie in *Bearbeiten von Schulen* (Seite 24) beschrieben, an der Schule zu hinterlegen. Abschließend muss das System von Grund auf neu mit UCS installiert werden und danach der UCS@school-Domäne neu beitreten.

2.2.4 Installation eines Verwaltungsservers (optional)

Der Verwaltungsserver bietet Anmeldedienste für Mitarbeiter in der Verwaltung an. Es ist nicht zwingend erforderlich, dass (an jeder Schule) ein Verwaltungsserver installiert wird.

Für den Verwaltungsserver muss ein vom edukativen Netz physikalisch getrenntes Netzwerksegment sowie ein eigenes IP-Subnetz verwendet werden, um Konflikte mit dem Schulserver des Edukativnetzes zu vermeiden (siehe auch *Verwaltungsnetz und Edukativnetz* (Seite 6)).

Die Installation eines Verwaltungsserver erfolgt analog zur in *Installation eines Schulservers* (Seite 17) beschriebenen Installation des Schulservers. Auch hier muss **vor** dem Domänenbeitritt der Rechnername des Verwaltungsservers an der Schule eingetragen werden. *Bearbeiten von Schulen* (Seite 24) beschreibt dies für bestehende Schulen. Abweichend zur Installation eines edukativen Schulservers muss bei der Installation eines Verwaltungsservers (ab UCS 4.4-1) als Rolle `Schulserver im Verwaltungsnetz` ausgewählt werden. Auch hier wird ggf. bei festgestellten Widersprüchen ein Hinweis angezeigt.

Bemerkung: Bei der Verwendung des Verwaltungsnetzes muss vor dem Anlegen der ersten Schule bzw. vor der Installation des ersten Schulservers bzw. Verwaltungsservers darauf geachtet werden, dass auf allen UCS@school-Systemen die UCR-Variable `ucsschool/import/generate/policy/dhcp/dns/set_per_ou` auf den Wert `false` gesetzt wird. Dies lässt sich am besten über eine UCR-Richtlinie für die gesamte UCS@school-Domäne erledigen.

IP-Subnetze sowie DNS-Server müssen über das Importskript **`import_networks`** (siehe in *Skriptbasierter Import von Netzwerken* (Seite 33)) importiert bzw. gesetzt werden, um einen fehlerfreien Betrieb zu gewährleisten.

2.2.5 (Erneuter) Domänenbeitritt eines Schulservers

Die Einrichtung eines Schulservers ist auch ohne das oben beschriebene UMC-Konfigurationsmodul möglich bzw. notwendig, wenn während des Konfigurationsprozesses Probleme auftreten sollten. Nur in einem solchen Szenario müssen die in diesem Abschnitt beschriebenen Schritte manuell durchgeführt werden:

- Das System muss erneut der Domäne beitreten. Dies erfolgt auf der Kommandozeile durch Aufruf des Befehls **`univention-join`**.
- Der Primary Directory Node wird im Regelfall durch eine DNS-Abfrage ermittelt. Wenn das nicht möglich sein sollte, kann der Rechnername des Primary Directory Node auch durch den Parameter `-dcname` *`HOSTNAME`* direkt angegeben werden. Der Rechnername muss dabei als vollqualifizierter Name angegeben werden, also beispielsweise `primary.example.com`.

- Als Join-Account wird ein Benutzerkonto bezeichnet, das berechtigt ist, Systeme der UCS-Domäne hinzuzufügen. Standardmäßig ist dies der Benutzer `Administrator` oder ein Mitglied der Gruppe `Domain Admins`. Der Join-Account kann durch den Parameter `-dcaccount` *ACCOUNTNAME* an **univention-join** übergeben werden.

Bemerkung: Der Name des Schulservers darf nur aus Kleinbuchstaben, Ziffern sowie dem Bindestrich bestehen (`a-z`, `0-9` und `-`). Der Name darf nur mit einem Kleinbuchstaben beginnen, mit einem Kleinbuchstaben oder einer Ziffer enden und ist auf eine Länge von 12 Zeichen beschränkt. Bei Abweichungen von diesen Vorgaben kann es zu Problemen bei der Verwendung von Windows-Clients kommen.

2.2.6 Installation sonstiger Systeme (optional)

Während des Domänenbeitritts sonstiger Systeme (Replica Directory Node ohne UCS@school oder Managed Node) wird (sofern notwendig) über den UCS@school-Join-Hook automatisch die Installation der UCS@school-App und notwendiger UCS@school-Pakete veranlasst. Weitere manuelle Schritte sind zunächst nicht zu beachten.

2.3 Umwandlung Single-Server- in Multi-Server-Umgebung

UCS@school-Umgebungen, die als Single-Server-Umgebung installiert/eingerichtet wurden, können bei Bedarf nachträglich in eine Multi-Server-Umgebung umgewandelt werden. Die Umwandlung ermöglicht die Aufnahme von Schulservern in die Domäne.

Für die Umwandlung sind einige Befehle auf der Kommandozeile des Primary Directory Nodes auszuführen, die einen Austausch des UCS@school-Meta-Pakets sowie eine Konfigurationsänderung durchführen. Bitte beachten Sie das Minuszeichen hinter dem zweiten Paketnamen am Ende der ersten Zeile:

```
$ univention-install ucs-school-multiserver ucs-school-singleserver-
$ ucr unset ucsschool/singlemaster
```

Durch die beiden Befehle wird das Meta-Paket **ucs-school-singleserver** deinstalliert und im gleichen Zug das Paket **ucs-school-multiserver** installiert.

Mit der Deinstallation des Pakets **ucs-school-singleserver** werden die nachfolgenden UCS@school-spezifischen Pakete (z.B. UMC-Module), die normalerweise nicht auf einem Primary Directory Node der Multi-Server-Umgebung installiert sind, automatisch zur Löschung vorgesehen. Die eigentliche Löschung der betroffenen Pakete findet während des nächsten Updates oder durch den manuellen Aufruf von **apt-get autoremove** statt. Dabei ist zu beachten, dass neben den genannten Paketen ggf. auch ungenutzte Paketabhängigkeiten entfernt werden.

```
ucs-school-branding
ucs-school-netlogon
ucs-school-netlogon-user-logonscripts
ucs-school-old-homedirs
ucs-school-old-sharedirs
ucs-school-umc-computerroom
ucs-school-umc-distribution
ucs-school-umc-exam
ucs-school-umc-helpdesk
ucs-school-umc-internetrules
ucs-school-umc-lessontimes
ucs-school-umc-printermoderation
ucs-school-webproxy
univention-squid-kerberos
```

Um die Löschung einzelner Pakete zu vermeiden, kann der folgende Befehl verwendet werden, bei dem *$PAKETNAME* durch den gewünschten Paketnamen auszutauschen ist:

```
$ apt-get unmarkauto $PAKETNAME
```

Richtlinien, die (ggf. automatisch von UCS@school) an Container der Schul-OUs verknüpft wurden, sollten auf ihre Einstellungen hin überprüft werden. Dies betrifft unter anderem die DHCP-DNS-Einstellungen.

Nachdem die oben genannten Schritte ausgeführt wurden, sollte abschließend der UMC-Server auf dem Primary Directory Node neu gestartet werden:

```
$ service univention-management-console-server restart
```

Vorsicht: Es ist zu beachten, dass auch nach der abgeschlossenen Umwandlung in eine Multi-Server-Umgebung der auf dem Primary Directory Node installierte Dienst *Samba 4* bestehen bleibt und nicht automatisch deinstalliert wird.

2.4 Integration mit Self-Service App

Um die *Self-Service App* in einer UCS@school-Umgebung einzusetzen, wird empfohlen das Paket **ucs-school-selfservice-support** auf dem Primary Directory Node und den Backup Directory Node zu installieren. Dies sorgt automatisch dafür, dass den Benutzern aller Schulen, die in den Gruppen `Domain Users` *OUNAME* Mitglied sind, die Benutzung des *Self-Service* Moduls erlaubt wird. Es wird automatisch die UCR-Variable `umc/self-service/passwordreset/whitelist/groups` beim Erstellen von neuen Schul-OUs aktuell gehalten.

Die Installation wird folgendermaßen durchgeführt:

```
$ univention-install ucs-school-selfservice-support
```

KAPITEL 3

Verwaltung von Schulen über die Univention Management Console

UCS@school bietet für viele der regelmäßig wiederkehrenden Verwaltungsaufgaben spezielle UMC-Module und -Assistenten an, die beim Anlegen, Modifizieren und Löschen von z.B. Schulen, Benutzerkonten und Rechnern unterstützen.

Ergänzend hierzu gibt es Programme für die Kommandozeile, die auch eine automatisierte Pflege der UCS@school-Umgebung zulassen. Diese werden in *Verwaltung von Schulen über Importskripte* (Seite 31) näher beschrieben.

Wichtig: Das Bearbeiten von UCS@school Objekten außerhalb der UCS@school-UMC-Module oder des Benutzer-Imports kann zu fehlerhaften Objekten führen.

Um diese Objekte sichtbar zu machen, werden ab UCS@school 4.4 v8 Objekte validiert, die aus dem Verzeichnisdienst in UCS@school geladen werden.

Zusätzlich zu den Fehlermeldungen in den regulären Log Dateien wird eine Ausgabe des gesamten Objekts in die nur vom Benutzer `root` lesbare Datei `/var/log/univention/ucs-school-validation.log` geschrieben.

Mit der Univention Configuration Registry Variable `ucsschool/validation/logging/backupcount` kann gesetzt werden, wie viele Kopien dieser Datei in Rotation gehalten werden, bevor die erste gelöscht wird. Als Standard ist `60` gesetzt.

Mit der Univention Configuration Registry Variable `ucsschool/validation/logging/enabled` kann an- und abgeschaltet werden, ob in die beiden Dateien `/var/log/univention/ucs-school-validation.log` und `/var/log/univention/management-console-module-schoolwizards.log` geloggt werden soll. Als Standard ist `yes` gesetzt.

3.1 Verwaltung von Schulen

Die Daten einer Schule werden in einer Organisationseinheit (OU) - einem Teilbaum des LDAP-Verzeichnisdienstes - gespeichert (siehe auch *Aufbau einer UCS@school-Umgebung* (Seite 3)). Die Verwaltung der logischen Einheit *Schule* kann in der Univention Management Console über das Modul *Schulen* erfolgen, welches sich in der Modulgruppe *Schul-Administration* befindet. Es ermöglicht das Suchen nach, sowie das Anlegen, Bearbeiten und Löschen von Schulen in der UCS@school-Umgebung.

Bevor ein neuer Schulserver der UCS@school-Domäne beitreten kann, muss die dazugehörige Schule angelegt werden.

3.1.1 Anlegen von Schulen

Um den Assistenten für das Hinzufügen einer neuen Schule zu starten, ist die Schaltfläche *Hinzufügen* oberhalb der Tabelle auszuwählen. Bei Neuinstallationen ohne bestehende Schulen fragt das UMC-Modul automatisch beim Öffnen, ob jetzt die erste Schule angelegt werden soll.

Der Assistent fragt in jeder UCS@school-Umgebung mindestens die beiden Werte *Name der Schule* und *Schulkürzel* ab. In Multi-Server-Umgebungen wird zusätzlich der Name des edukativen Schulservers abgefragt, welcher später die Dienste für die neue Schule bereitstellen soll.

Im Eingabefeld *Name der Schule* ist eine beliebige Beschreibung für die Schule (z.B. *Gymnasium Mitte*) anzugeben, die keiner Zeichenlimitierung unterliegt. Sie wird später in den UCS@school-Modulen angezeigt, wenn zwischen unterschiedlichen Schulen zu wählen ist. Nachdem ein Wert eingetragen wurde, wird beim Wechsel in das nächste Eingabefeld automatisch ein Vorschlag für das *Schulkürzel* generiert.

Das Schulkürzel ist i.d.R. ein kurzer Bezeichner für die Schule, der sich später an unterschiedlichen Stellen wiederfindet. Es wird automatisch u.a. als Präfix für Gruppen- und Freigabenamen verwendet. Darüber hinaus wird das Schulkürzel als Name für die Organisationseinheit (OU) im Verzeichnisdienst verwendet. Häufig kommen hier Schulnummern wie `340` oder zusammengesetzte Kürzel wie `g123m` oder `gymmitte` zum Einsatz.

In Single-Server-Umgebungen ist die Angabe eines Rechnernamens für Schulserver nicht erforderlich, während in Multi-Server-Umgebungen der *Rechnername des Schulservers* angegeben werden muss. Der eingetragene Schulserver wird automatisch als Dateiserver für Klassen- und Benutzerfreigaben verwendet (siehe *Windows-spezifische Benutzereinstellungen* (Seite 38) und *Server für Dateifreigaben* (Seite 46)). Optional kann auch der *Rechnername des Verwaltungsservers* angegeben werden, sofern dieser verwendet werden soll.

Nach dem erfolgreichen Anlegen der Schule über die Schaltfläche *Speichern* erscheint eine Statusmeldung im oberen Teil der Univention Management Console.

Vorsicht: Bei Schulservern bzw. Verwaltungsservern muss die Schule **vor** dem Domänenbeitritt des Systems angelegt und der Rechnername des Schulservers bzw. Verwaltungsservers an der Schule hinterlegt werden.

Stimmen hinterlegter Rechnername und der Name des beitretenden Systems nicht überein, wird ein Replica Directory Node ohne UCS@school-Funktionalität installiert und eingerichtet.

Wichtig: Das Schulkürzel darf ausschließlich aus Buchstaben (`a-z` und `A-Z`), Ziffern (`0-9`) und dem Bindestrich (`-`) bestehen, da es unter anderem die Grundlage für Gruppen-, Freigabe- und Rechnernamen bildet.

Der Name des Schulservers bzw. Verwaltungsservers darf nur aus Kleinbuchstaben, Ziffern sowie dem Bindestrich bestehen (`a-z`, `0-9` und `-`). Der Name darf nur mit einem Kleinbuchstaben beginnen, mit einem Kleinbuchstaben oder einer Ziffer enden und ist auf eine Länge von 12 Zeichen beschränkt. Bei Abweichungen von diesen Vorgaben kann es zu Problemen bei der Verwendung von Windows-Clients kommen.

3.1.2 Mehrere Schulen auf einem Schulserver verwalten

Wie in *Replikation mehrerer Schulen auf einen Schulserver* (Seite 5) bereits beschrieben wurde, können mehrere Schulen auf einen Schulserver repliziert werden. Für die Einrichtung sind zusätzliche Schritte notwendig, die nachfolgend beschrieben werden:

- In der UMC kann die Zuweisung eines Schulservers zu einer Schule nur beim Anlegen der Schule erfolgen. Damit mehrere Schulen vom gleichen Schulserver verwaltet werden, muss beim Anlegen der betreffenden Schulen im Feld *Rechnername des Schulservers im Edukativnetz* der gleiche Name des Schulservers angegeben werden (siehe *Anlegen einer neuen Schule* (Seite 23)).

  Auf der Kommandozeile ist die Zuweisung über das Kommando **`create_ou`** beim Anlegen einer Schule möglich. Im folgenden Beispiel werden die Schulen `gymwest` und `bswest` angelegt, die den Schulserver `dcwest` verwenden sollen.

```
$ cd /usr/share/ucs-school-import/scripts/
$ ./create_ou gymwest dcwest
$ ./create_ou bswest dcwest
```

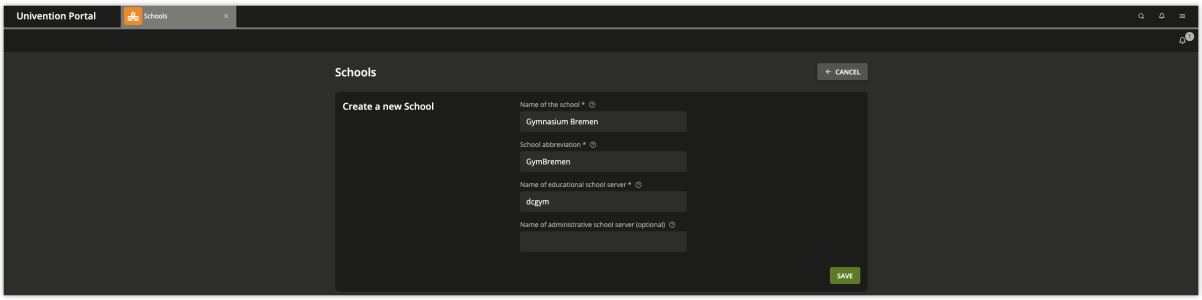

Abb. 3.1: Anlegen einer neuen Schule

- Nach dem Anlegen der Schulen bzw. dem Zuweisen der Schulserver zu den Schulen ist im UMC-Modul *Schulen* die betreffende Schule zu öffnen und dort unter *Erweiterte Einstellungen* zu prüfen, ob die korrekten Dateiserver für Heimatverzeichnisse und Klassenfreigaben hinterlegt sind (siehe *Das Setzen von Dateiservern für eine Schule* (Seite 23)). Diese Werte sind auch zu prüfen, wenn diese in der Vergangenheit bereits korrekt waren, da sie ggf. während der Schulserver-Zuweisung neu gesetzt werden.

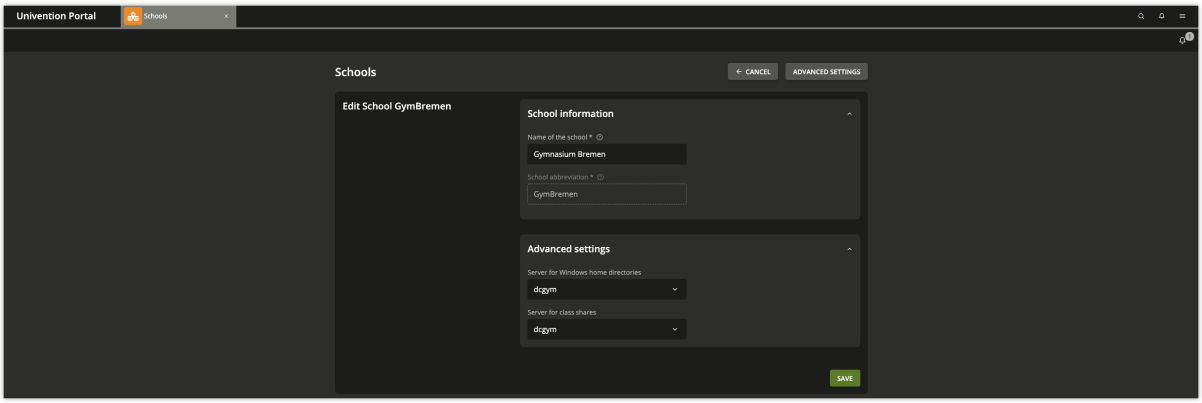

Abb. 3.2: Das Setzen von Dateiservern für eine Schule

- Es ist zu beachten, dass bereits während des Anlegens einer neuen Schule für den betroffenen Schulserver neue Zugriffsberechtigungen auf das LDAP-Verzeichnis gesetzt werden, die den laufenden Betrieb auf einem Schulserver negativ beeinflussen können. Die Zuweisung bzw. das Anlegen der Schule sollte daher in einem geeigneten Wartungsfenster stattfinden.

  Falls ein bereits existierender Schulserver einer weiteren Schule zugewiesen wurde, der bereits erfolgreich der UCS@school-Domäne beigetreten ist, *muss* dieser Schulserver den Domänenbeitritt erneut durchführen, um

einen konsistenten Zustand des LDAP-Verzeichnisses auf dem Schulserver herzustellen.

Warnung: Die Verwendung des DHCP-Servers auf einem Schulserver, dem mehrere Schulen zugewiesen wurden, wird nicht unterstützt.

3.1.3 Bearbeiten von Schulen

Zum Bearbeiten einer bestimmten Schule ist diese in der Tabelle auszuwählen und die Schaltfläche *Bearbeiten* anzuklicken. Im folgenden Dialog kann der Name der Schule angepasst werden. Das nachträgliche Ändern des Schulkürzels ist nicht möglich.

Darüber hinaus können durch einen Klick auf *Erweiterte Einstellungen* die für die Schule zuständigen Freigabeserver eingesehen und modifiziert werden. Die genaue Funktion dieser Freigabeserver wird in *Windows-spezifische Benutzereinstellungen* (Seite 38) und *Server für Dateifreigaben* (Seite 46) beschrieben.

Das nachträgliche Hinzufügen von Schulservern für das Verwaltungsnetz ist derzeit nicht über die UMC möglich. Auf der Kommandozeile kann dies jedoch über das Tool **`create_ou`** erreicht werden. Diesem Tool sind als Parameter der OU-Name, der Rechnername des existierenden Schulservers im Edukativnetz und der noch fehlende Rechnername für den Schulserver im Verwaltungsnetz zu übergeben.

Im folgenden Beispiel wird für die Schule `gymmitte`, die bereits den Schulserver `dcgymmitte` im Edukativnetz einsetzt, zusätzlich der Schulserver `admgymmitte` für das Verwaltungsnetz hinterlegt:

```
$ cd /usr/share/ucs-school-import/scripts/
$ ./create_ou gsmitte dcgymmitte admgymmitte
```

3.1.4 Löschen von Schulen

Zum Löschen einer bestimmten Schule ist diese in der Tabelle auszuwählen und die Schaltfläche *Löschen* anzuklicken.

Gefahr: Das Löschen einer Schule umfasst auch das unwiderrufliche Entfernen aller damit verbundenen Objekte wie Benutzerkonten, Klassen, Arbeitsgruppen, Rechner, DHCP-Leases, Drucker und Freigaben.

Das Löschen einer Schule kann nicht rückgängig gemacht werden.

3.2 Verwaltung einzelner Benutzerkonten

Für die manuelle Pflege von einzelnen Benutzerkonten wird auf dem Primary Directory Node das UMC-Modul *Benutzer (Schulen)* bereitgestellt, welches sich in der UMC-Modulgruppe *Schul-Administration* befindet. Es ermöglicht das Suchen nach, sowie das Anlegen, Bearbeiten und Löschen von Schülern, Lehrern und Mitarbeitern in der UCS@school-Umgebung.

3.2.1 Anlegen eines Benutzerkontos

Um den Assistenten für das Hinzufügen eines neuen Benutzers zu starten, ist die Schaltfläche *Hinzufügen* oberhalb der Tabelle auszuwählen. In UCS@school-Umgebungen ohne bestehende Benutzer fragt das Modul automatisch beim Öffnen, ob jetzt der erste Benutzer angelegt werden soll.

Wichtig: Es ist wichtig, dass beim Anlegen einzelner Benutzer für UCS@school das UMC-Modul *Benutzer (Schulen)* verwendet wird, weil sich UCS@school Benutzer von regulären UCS Benutzern unterscheiden.

Detaillierte Informationen zu den Unterschieden der Benutzerkonten finden sich in KB 15630 - How a UCS@school user should look like[6].

Die erste Seite des Assistenten fragt zunächst die gewünschte Benutzerrolle für das neue Benutzerkonto ab. Zur Auswahl stehen die folgenden Benutzerrollen:

- *Schüler*
- *Lehrer*
- *Lehrer und Mitarbeiter*
- *Mitarbeiter*

Die einzelnen Benutzerrollen werden in *UCS@school-Benutzerrollen* (Seite 3) genauer beschrieben. Sind mehrere Schulen in der UCS@school-Umgebung eingerichtet, wird zusätzlich abgefragt, in welcher Schule das Benutzerkonto angelegt werden soll.

Über die Schaltfläche *Weiter* gelangt man auf die zweite Seite des Assistenten. Dort werden die für UCS@school relevanten Benutzerattribute abgefragt. Die folgenden Attribute müssen angegeben werden:

- *Vorname*
- *Nachname*
- *Benutzername*
- *Klasse*

Über die Schaltfläche *Neue Klasse erstellen* ist es möglich, direkt in das UMC-Modul *Klassen (Schule)* zu wechseln, um dort eine weitere Schulklasse anlegen zu können. Ein Benutzer in der Rolle Schüler benötigt immer eine Schulklasse. Benutzerkontodaten werden an anderen Stellen weiter verarbeitet. Wenn die Angabe für die Klasse eines Schülers fehlt, kann die Weiterverarbeitung gestört werden.

Die folgenden Attribute sind optional:

- *E-Mail*
- *Passwort*
- *deaktiviert*
- *Geburtstag*

Ist kein Passwort vergeben, muss das Passwort vom Administrator (oder Lehrer) zurückgesetzt werden, bevor das Benutzerkonto vom Benutzer erstmals verwendet werden kann.

Bemerkung: Ab UCS@school Version 5.0 v3 kann über die Univention Configuration Registry Variable `ucsschool/wizards/schoolwizards/users/check-password-policies` die Evaluierung von Passwort Richtlinien während des Anlegens neuer Benutzer eingeschaltet werden. Gültige Werte sind `yes` und `no`. Die Evaluierung ist standardmäßig ausgeschaltet. Passwort Richtlinien werden beim Bearbeiten von Benutzern immer evaluiert.

Nach dem Anklicken der Schaltfläche *Speichern* wird das Benutzerkonto im Verzeichnisdienst angelegt und eine Benachrichtigung über den Erfolg der Aktion angezeigt. Anschließend wird wieder die zweite Seite des Assistenten angezeigt, um weitere Benutzerkonten anlegen zu können. Die Einstellungen für Schule und Benutzerrolle bleiben dabei erhalten. Mit der Verwendung der Schaltfläche *Abbrechen* gelangt man zurück zum zentralen Suchdialog des UMC-Moduls.

Wichtig: Die Benutzernamen müssen schulübergreifend eindeutig sein. D.h. es ist nicht möglich, den gleichen Benutzernamen an zwei unterschiedlichen Schulen zu verwenden.

[6] https://help.univention.com/t/15630

Wichtig: Benutzernamen dürfen keine von Windows reservierten Namen enthalten. Siehe Microsoft Dokumentation[7] für weitere Informationen. Benutzernamen, die diesen Regeln nicht entsprechen, sind als veraltet anzusehen. Ab UCS 5.2 sind diese Benutzernamen nicht mehr unterstützt und müssen geändert werden.

Bemerkung: Über die Univention Configuration Registry Variable `ucsschool/wizards/schoolwizards/users/optional_visible_fields` können die angezeigten optionalen Felder angepasst werden. Ab UCS@school 4.4 v9 kann hier auch das Ablaufdatum (*expiration_date*) hinzugefügt werden werden.

3.2.2 Bearbeiten eines Benutzerkontos

Zum Bearbeiten eines Benutzerkontos ist dieses in der Tabelle auszuwählen und die Schaltfläche *Bearbeiten* anzuklicken. Im folgenden Dialog können die Attribute des Benutzerkontos bearbeitet werden. Das nachträgliche Ändern des Benutzernamens ist nicht möglich.

Sofern der angemeldete UMC-Benutzer die Rechte für das UMC-Modul *Benutzer* aus der Modulgruppe *Domäne* besitzt, wird zusätzlich die Schaltfläche *Erweiterte Einstellungen* angezeigt. Über sie kann das UMC-Modul *Benutzer* geöffnet werden, in dem viele erweiterte Einstellungen für das Benutzerkonto möglich sind.

3.2.3 Löschen von Benutzerkonten

Zum Löschen von Benutzerkonten sind diese in der Tabelle auszuwählen und anschließend die Schaltfläche *Löschen* anzuklicken. Nach dem Bestätigen werden die Benutzerkonten aus dem Verzeichnisdienst entfernt.

3.3 Verwaltung von Schulklassen

Auf dem Primary Directory Node kann das Anlegen und Entfernen von Schulklassen über das UMC-Modul *Klassen (Schulen)* erfolgen. Das Anlegen einer Schulklasse ist erforderlich, bevor das erste Schüler-Benutzerkonto erstellt werden kann.

Die eigentliche Zuordnung von Schülern zu einer Klasse erfolgt über das UMC-Modul *Benutzer (Schulen)* am Schüler-Benutzerobjekt oder während des CSV-Imports.

Die Zuordnung von Lehrern zu Klassen erfolgt über das UMC-Modul *Lehrer Klassen zuordnen*.

3.3.1 Anlegen von Schulklassen

Im zentralen Suchdialog des UMC-Moduls ist oberhalb der Tabelle die Schaltfläche *Hinzufügen* auszuwählen, um eine neue Klasse zu erstellen. Sind mehrere Schulen in der UCS@school-Umgebung eingerichtet, wird zunächst abgefragt, in welcher Schule die Klasse angelegt werden soll. Wurde nur eine Schule eingerichtet, wird dieser Schritt automatisch übersprungen.

Anschließend wird für die neue Klasse ein Name sowie eine Beschreibung erfragt. Sprechende Namen, wie zum Beispiel `Igel` oder `BiologieLK` sind als Namen ebenso möglich wie Buchstaben-Ziffern-Kombinationen (`10R`). Aufeinander folgende Leerzeichen werden nicht unterstützt. Über die Schaltfläche *Speichern* wird die neue Klasse im Verzeichnisdienst angelegt.

Die Klassennamen in UCS@school müssen schulübergreifend eindeutig sein. Um trotzdem z.B. die Klasse *7A* in mehreren Schule verwenden zu können, wird dem Klassennamen im Verzeichnisdienst automatisch das jeweilige Schulkürzel als Präfix vorangestellt. Für die Klasse *7A* an der Schule mit dem Schulkürzel `gymmitte` wird daher das Klassenobjekt `gymmitte-7A` erstellt. Dieser Name mit Präfix zeigt sich z.B. später bei der Administration von Datei- und Verzeichnisberechtigungen auf Windows-Rechnern.

[7] https://learn.microsoft.com/en-us/windows/win32/fileio/naming-a-file

Um innerhalb einer Klasse den Austausch von Dokumenten zu vereinfachen, wird mit dem Anlegen einer neuen Klasse auch automatisch eine neue Freigabe erstellt, die den gleichen Namen trägt, wie das Klassenobjekt (z.B. `gymmitte-7A`). Die Freigabe wird auf dem Dateiserver angelegt, welcher an dem Schulobjekt unter *Erweiterte Einstellungen* als *Server für Klassenfreigaben* hinterlegt ist. Der Zugriff auf diese Freigabe ist auf die Benutzer der Klasse beschränkt.

3.3.2 Bearbeiten von Schulklassen

Zum Bearbeiten einer Klasse ist diese in der Tabelle auszuwählen und die Schaltfläche *Bearbeiten* anzuklicken. Im folgenden Dialog können Name und Beschreibung der Klasse bearbeitet werden.

Bemerkung: Beim Ändern des Namens werden Klassengruppe, Klassenfreigabe und Freigabeverzeichnis automatisch umbenannt.

Gegebenenfalls ist auf Windows-Rechner ein erneutes Anmelden notwendig, um wieder Zugriff auf die Freigabe zu erhalten.

Sofern der angemeldete UMC-Benutzer die Rechte für das UMC-Modul *Gruppen* aus der Modulgruppe *Domäne* besitzt, wird zusätzlich die Schaltfläche *Erweiterte Einstellungen* angezeigt. Über sie kann das UMC-Modul *Gruppen* geöffnet werden, in dem viele erweiterte Einstellungen für die Gruppe möglich sind.

3.3.3 Löschen von Schulklassen

Zum Löschen von Klassen sind diese in der Tabelle auszuwählen und anschließend die Schaltfläche *Löschen* anzuklicken. Nach dem Bestätigen werden die Klassen aus dem Verzeichnisdienst entfernt.

Bemerkung: Mit dem Löschen der Klassen wird auch automatisch die jeweilige Klassenfreigabe entfernt.

In der Standardkonfiguration von UCS@school wird das Freigabeverzeichnis auf dem Dateiserver automatisch in das Backup-Verzeichnis `/home/backup/groups/` verschoben.

3.4 Verwaltung von Rechnern

Für die Anbindung von Arbeitsplatzrechnern in Form von z.B. Windows-Rechnern werden im Verzeichnisdienst Rechnerkonten benötigt.

Rechnerkonten werden z.B. von Windows-Rechnern automatisch beim Domänenbeitritt angelegt. Sie können aber auch vor dem Domänenbeitritt manuell über das UMC-Modul *Rechner (Schulen)* eingepflegt werden. Dies ist unter anderem für *IP-Managed-Clients* wie z.B. Netzwerkdrucker notwendig.

Das Anlegen der Rechnerkonten vor der Inbetriebnahme bringt den Vorteil, dass z.B. die für DHCP notwendigen Informationen wie IP- und MAC-Adresse schon hinterlegt sind.

3.4.1 Anlegen von Rechnerkonten

Im zentralen Suchdialog des UMC-Moduls ist oberhalb der Tabelle die Schaltfläche *Hinzufügen* auszuwählen, um den Assistenten für ein neues Rechnerkonto zu starten.

Sind mehrere Schulen in der UCS@school-Umgebung eingerichtet, ist zunächst auszuwählen, in welcher Schule das Rechnerkonto angelegt werden soll. Wurde nur eine Schule eingerichtet, wird dieses Auswahlfeld automatisch ausgeblendet.

Im Auswahlfeld *Rechnertyp* stehen bis zu vier Rechnertypen zur Auswahl:

- `Windows-System` für Windows-Rechner ab Windows XP
- `Mac OS X`
- `Gerät mit IP-Adresse` für z.B. Netzwerkdrucker mit eigener IP-Adresse

Auf der nächste Seite des Assistenten müssen folgende Attribute des neuen Rechnerkontos angegeben werden:

- *Name*,
- *IP-Adresse*
- *MAC-Adresse*

Um Probleme beim Domänenbeitritt zu vermeiden, muss der Name des Rechnerkontos mit dem Namen des Rechners übereinstimmen. Die *Subnetzmaske* kann in den meisten Fällen auf der Voreinstellung belassen werden. Die MAC-Adresse wird unter anderem für die statische Vergabe der IP-Adressen per DHCP verwendet. Die Angabe der Inventarnummer ist optional.

Bemerkung: Als IP-Adresse kann auch die Adresse des Subnetzes angegeben werden (z.B. `192.168.2.0` bei einer Subnetzmaske von `255.255.255.0`). Der Assistent wählt dann automatisch eine freie IP-Adresse aus dem angegebenen Subnetz aus (z.B. `192.168.2.20`) und weist sie dem neuen Rechnerkonto zu.

3.4.2 Bearbeiten von Rechnerkonten

Zum Bearbeiten eines Rechnerkontos ist dieses in der Tabelle auszuwählen und die Schaltfläche *Bearbeiten* anzuklicken. Im folgenden Dialog können IP-Adresse, MAC-Adresse, Subnetzmaske und Inventarnummer angepasst werden.

Das Bearbeiten des Rechnernamens ist nicht möglich.

Sofern der angemeldete UMC-Benutzer die Rechte für das UMC-Modul *Rechner* aus der Modulgruppe *Domäne* besitzt, wird zusätzlich die Schaltfläche *Erweiterte Einstellungen* angezeigt. Über sie kann das UMC-Modul *Rechner* geöffnet werden, in dem viele erweiterte Einstellungen für das Rechnerkonto möglich sind.

3.4.3 Löschen von Rechnerkonten

Zum Löschen von Rechnerkonten sind diese in der Tabelle auszuwählen und anschließend die Schaltfläche *Löschen* anzuklicken. Nach dem Bestätigen werden die Rechnerkonten aus dem Verzeichnisdienst entfernt.

3.5 UCS@school Kelvin REST API

Die App **`UCS@school Kelvin REST API`** installiert eine REST Schnittstelle zur Verwaltung von UCS@school-Objekten wie zum Beispiel Schulen, Rollen, Klassen und Benutzern. Die Objekte können über die Schnittstelle gelesen und abgefragt, verändert und gelöscht werden. Die Schnittstelle dient dazu, den Verzeichnisdienst in UCS@school per Netzwerkschnittstelle anzusprechen, zum Beispiel von einer Schulverwaltungssoftware oder einem Bildungsangebot.

Weitere Informationen finden sich in der Entwicklerdokumentation der Schnittstelle[8] (nur in Englisch verfügbar).

[8] https://docs.software-univention.de/ucsschool-kelvin-rest-api/index.html

KAPITEL 4

Verwaltung von Schulen über Importskripte

UCS@school bietet für viele der regelmäßig wiederkehrenden Verwaltungsaufgaben spezielle UMC-Module und Assistenten an, die beim Anlegen, Modifizieren und Löschen von z.B. Schulen, Benutzerkonten und Rechnern unterstützen. Diese werden in *Verwaltung von Schulen über die Univention Management Console* (Seite 21) beschrieben).

Ergänzend hierzu gibt es Programme für die Kommandozeile, die auch eine automatisierte Pflege der UCS@school-Umgebung zulassen und werden nachfolgend beschrieben.

Vorsicht: Seit der UCS@school-Version 3.2 R2 halten die kommandozeilenbasierten Importskripte zu Beginn des jeweiligen Imports den Univention Directory Notifier auf dem Primary Directory Node an. Nach Abschluss des Imports wird der Univention Directory Notifier wieder gestartet.

4.1 Pflege von Benutzerkonten für Schüler, Lehrer und Mitarbeiter

Für UCS@school gibt es momentan mehrere Möglichkeiten Nutzer in das System zu importieren.

Die Konfiguration des kommandozeilenbasierten Benutzerimports ist in *UCS@school - Handbuch zur CLI-Import-Schnittstelle* [4] beschrieben.

4.2 Import von Schulklassen

Beim Import schon Schulklassen ist zu beachten, dass die Klassennamen domänenweit eindeutig sein müssen. Das heißt, eine Klasse *1A* kann nicht in mehreren OUs verwendet werden. Daher sollte jedem Klassennamen die OU und ein Bindestrich vorangestellt werden.

Bei der Erstellung von Klassen über das UMC-Modul *Klassen (Schulen)* geschieht dies automatisch. Sprechende Namen, wie zum Beispiel `Igel` oder `BiologieAG`, sind für Klassennamen ebenso möglich wie Buchstaben-Ziffern-Kombinationen (`10R`).

Beispiele für die Schule `gym123`:

```
gym123-1A
gym123-1B
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
gym123-2A
gym123-Igel
```

Der Import von Benutzern erfolgt über das Skript **/usr/share/ucs-school-import/scripts/import_group**, das auf dem Primary Directory Node als Benutzer `root` gestartet werden muss. Es erwartet den Namen einer CSV-Datei als ersten Parameter. Das Dateiformat für die Gruppen-Importdatei ist wie folgt aufgebaut:

Tab. 4.1: Aufbau der Datenzeilen für den Gruppen-Import

Feld	Beschreibung	Mögliche Werte	Beispiel
Aktion	Art der Gruppenmodifikation	`A`=Hinzufügen, `M`=Modifizieren, `D`=Löschen	`A`
OU	OU, in der die Gruppe modifiziert werden soll	—	`g123`
Gruppenname	Der Name der Gruppe	—	`g123m-1A`
(Beschreibung)	Optionale Beschreibung der Gruppe	—	`Klasse 1A`

Ein Beispiel für eine Importdatei:

```
A     g123m     g123m-1A          Klaaassen 1A
A     g123m     g123m-LK-Inf      Leistungskurs Informatik
M     g123m     g123m-1A          Klasse 1A
D     g123m     g123m-LK-Inf      Leistungskurs Informatik
D     g123m     g123m-R12         Klasse R12
```

4.3 Vorgehen zum Schuljahreswechsel

Zum Schuljahreswechsel stehen zahlreiche Änderungen in den Benutzerdaten an. Schüler werden in eine höhere Klasse versetzt, der Abschlussjahrgang verlässt die Schule und ein neuer Jahrgang wird eingeschult.

Ein Schuljahreswechsel erfolgt in vier Schritten:

1. Eine Liste aller Schulabgänger wird aus der Schulverwaltungssoftware exportiert und die Konten werden über das Import-Skript entfernt (Aktion D, siehe *Pflege von Benutzerkonten für Schüler, Lehrer und Mitarbeiter* (Seite 31)). Die Klassen der Schulabgänger müssen ebenfalls über das Import-Skript für Gruppen entfernt werden.

2. Die bestehenden Klassen sollten umbenannt werden. Dies stellt sicher, dass Dateien, die auf einer Klassenfreigabe gespeichert werden und somit einer Klasse zugeordnet sind, nach dem Schuljahreswechsel weiterhin der Klasse unter dem neuen Klassennamen zugeordnet sind.

   Die ältesten Klassen (die der Abgänger zum Schulende) müssen zuvor gelöscht werden. Die Umbenennung erfolgt über das Skript **/usr/share/ucs-school-import/scripts/rename_class**, das auf dem Primary Directory Node als Benutzer `root` aufgerufen werden muss. Es erwartet den Namen einer tab-separierten CSV-Datei als ersten Parameter. Die CSV-Datei enthält dabei pro Zeile zuerst den alten und dann den neuen Klassennamen, z.B.

   ```
   gymmitte-6B     gymmitte-7B
   gymmitte-5B     gymmitte-6B
   ```

   Die Reihenfolge der Umbenennung ist wichtig, da die Umbenennung sequentiell erfolgt und der Zielname nicht existieren darf.

Bemerkung: Beim Umbenennen der Klassen-Freigaben werden auch deren Werte für *Samba-Name* sowie die *erzwungene Gruppe* automatisch angepasst, sofern diese noch die Standardwerte des UCS@school-Importskriptes aufweisen.

Bei manuellen Änderungen müssen diese Werte nach dem Umbenennen der Klasse nachträglich manuell angepasst werden.

3. Eine aktuelle Liste aller verbleibenden Schülerdaten wird über das Import-Skript neu eingelesen (Aktion `M`, siehe *Pflege von Benutzerkonten für Schüler, Lehrer und Mitarbeiter* (Seite 31)).
4. Eine Liste aller Neuzugänge wird aus der Schulverwaltungssoftware exportiert und über das Import-Skript importiert (Aktion `A`, siehe *Pflege von Benutzerkonten für Schüler, Lehrer und Mitarbeiter* (Seite 31)).

4.4 Skriptbasierter Import von Netzwerken

Der skriptbasierte Import von Netzwerken legt IP-Subnetze im LDAP an und konfiguriert diverse Voreinstellungen wie zum Beispiel Adressen von Routern (Gateways), DNS-Server und WINS-Server für diese Subnetze. Darunter fällt zum Beispiel auch ein Adressbereich, aus dem für neuangelegte Systeme automatisch IP-Adressen vergeben werden können.

Der skriptbasierte Import ist insbesondere in Szenarien empfehlenswert, wo UCS für die Verteilung der Netzwerkkonfiguration über DHCP zum Einsatz kommt und damit die Netzwerkkonfiguration von Clients übernimmt. Insbesondere größere UCS@school-Umgebungen profitieren vom skriptbasierten Import von Netzwerken.

In kleineren Umgebungen kann es flexibler sein, wenn Administratoren die Netzwerkeinstellungen über die Univention Management Console vornehmen. UCS erstellt automatisch entsprechende Netzwerkobjekte für das Netzwerk eines Rechnerkontos. Bei der Verwendung von DHCP über UCS und im Unterschied zum skriptbasierten Import müssen Administratoren über die Univention Management Console die DHCP-Richtlinie für Rechnerkonten mit Vorgaben zu Gateway, DNS-Server oder WINS-Server manuell anlegen.

Siehe auch:

Univention Corporate Server - Handbuch für Benutzer und Administratoren [2]:

Konfiguration von Clients durch DHCP-Richtlinien[9]
zum Anlegen einer DHCP Richtlinie mit Vorgaben zu Gateway, DNS-Server oder WINS-Server

Verwaltung der Rechnerkonten über Univention Management Console Modul[10]
zum Anlegen von Rechnerkonten

Administratoren können Netzwerke auf der Kommandozeile über das Skript **`/usr/share/ucs-school-import/scripts/import_networks`** aus einer CSV Datei importieren, indem sie es auf dem Primary Directory Node als Benutzer `root` starten. Das Skript erstellt Netzwerkobjekte **inklusive** einer DHCP-Richtlinie mit Vorgaben zu Gateway, DNS-Server und WINS-Server.

Tab. 4.2 zeigt das Format der Import-Datei. Das Skript **`import_networks`** erwartet Tabulatorzeichen zur Trennung der einzelnen Felder. Optionale Felder stehen in Klammern und dürfen in der Import-Datei leer bleiben, zum Beispiel *(IP-Adressbereich)*. Quellcode 4.1 zeigt ein Beispiel.

Tab. 4.2: Format der Import-Datei für **`import_networks`**

Feld	Beschreibung	Mögliche Werte
OU	OU des zu modifizierenden Netzwerks	`g123m`
Netzwerk	Netzwerk und Subnetzmaske	`10.0.5.0/255.255.255.0`
(IP-Adressbereich)	Bereich, aus dem IP-Adressen für neuangelegte Systeme automatisch vergeben werden	`10.0.5.10-10.0.5.140`
(Router)	IP-Adresse des Routers	`10.0.5.1`
(DNS-Server)	IP-Adresse des DNS-Servers	`10.0.5.2`
(WINS-Server)	IP-Adresse des WINS-Servers	`10.0.5.2`

[9] https://docs.software-univention.de/manual/5.0/de/ip-config/dhcp.html#networks-dhcp-policies
[10] https://docs.software-univention.de/manual/5.0/de/computers/umc.html#computers-hostaccounts

Bemerkung: Quellcode 4.1 verwendet Tabulatorzeichen zur Trennung der Felder. Nutzen Sie den Link zum Herunterladen der `Importdatei` für die weitere Verwendung.

Quellcode 4.1: Beispiel für eine `Importdatei`

```
g123m   10.0.5.0        10.0.5.1    10.0.5.2    10.0.5.2
g123m   10.0.6.0/25 10.0.6.5-10.0.6.120 10.0.6.1    10.0.6.2    10.0.6.15
```

Das Skript **`import_networks`** verwendet Voreinstellungen, wenn folgende Angaben in der CSV Datei für den Netzwerkimport fehlen:

- Netzmaske `255.255.255.0`, wenn im Feld *Netzwerk* keine Angabe über die Netzmaske vorliegt.
- IP Adressbereich `X.Y.Z.20-X.Y.Z.250`, wenn im Feld *IP-Adressbereich* keine Angabe über den Adressbereich vorliegt.

Zur Vereinfachung der Administration der Netzwerke steht zusätzlich das Skript **`import_router`** zur Verfügung, das nur den Default-Router für das angegebene Netzwerk neu setzt. Es verwendet das gleiche Format wie **`import_networks`**.

4.5 Import von Rechnerkonten

Rechnerkonten können entweder einzeln über ein spezielles UMC-Modul oder über ein spezielles Import-Skript als Massenimport angelegt werden. Die Rechnerkonten sollten vor dem Domänenbeitritt von z.B. Windows-PCs angelegt werden, da so sichergestellt wird, dass die für den Betrieb von UCS@school notwendigen Informationen im LDAP-Verzeichnis vorhanden sind und die Objekte an der korrekten Position im LDAP-Verzeichnis abgelegt wurden.

Nach dem Anlegen der Rechnerkonten können die PCs über den im UCS-Handbuch beschriebenen Weg der Domäne beitreten.

4.5.1 Skriptbasierter Import von PCs

Der Import mehrerer PCs erfolgt über das Skript **`/usr/share/ucs-school-import/scripts/import_computer`**, das auf dem Primary Directory Node als Benutzer `root` aufgerufen werden muss. Es erwartet den Namen einer CSV-Datei als ersten Parameter, die in folgender Syntax definiert wird. Die einzelnen Felder sind durch ein Tabulatorzeichen zu trennen.

Es ist zu beachten, dass Computernamen domänenweit eindeutig sein müssen. Das heißt, ein Computer `windows01` kann nicht in mehreren OUs verwendet werden.

Um die Eindeutigkeit zu gewährleisten, wird empfohlen, jedem Computernamen die OU voranzustellen oder zu integrieren (z.B. `340win01` für Schule *340*).

Feld	Beschreibung	Mögliche Werte	Beispiel
Rechnertype	Typ des Rechnerobjektes	`ipmanagedclient`, `macos`, `windows`, `ubuntu`, `linux`	`windows`
Name	zu verwendender Rechnername	—	`wing123m-01`
MAC-Adresse	MAC-Adresse (wird für DHCP benötigt)	—	`00:0c:29:12:23:34`
OU	OU; in der das Rechnerobjekt modifiziert werden soll	—	`g123m`
IP-Adresse (/Netzmaske) oder IP Subnetz	IP-Adresse des Rechnerobjektes und optional die passende Netzmaske; alternativ das Ziel-IP-Subnetz	—	`10.0.5.45/255.255.255.0`
(Inventarnr.)	Optionale Inventarnummer	—	`TR47110815-XA-3`
(Weitere Felder)	Optionale zusätzliche Attribute	—	`description`

Die Subnetzmaske kann sowohl als Präfix (`24`) als auch in Oktettschreibweise (`255.255.255.0`) angegeben werden. Die Angabe der Subnetzmaske ist optional. Wird sie weggelassen, wird die Subnetzmaske `255.255.255.0` angenommen.

Wird im Feld *IP-Adresse (/ Netzmaske)* nur ein Subnetz angegeben (z.B. `10.0.5.0`), wird dem Computerobjekt automatisch die nächste freie IP-Adresse aus diesem IP-Subnetz zugewiesen.

Beispiel für eine Importdatei:

```
ipmanagedclient  routerg123m-01   10:00:ee:ff:cc:02  g123m  10.0.5.1
windows          wing123m-01      10:00:ee:ff:cc:00  g123m  10.0.5.5
windows          wing123m-02      10:00:ee:ff:cc:01  g123m  10.0.5.6
macos            macg123m-01      10:00:ee:ff:cc:03  g123m  10.0.5.7
ubuntu           ubuntug123m-01   10:00:ee:ff:cc:04  g123m  10.0.5.8
linux            linuxg123m-01    10:00:ee:ff:cc:05  g123m  10.0.5.9
ipmanagedclient  printerg123m-01  10:00:ee:ff:cc:06  g123m  10.0.5.250
```

Die importierten Rechner werden so konfiguriert, dass ihnen die angegebene IP-Adresse automatisch per DHCP zugeordnet wird, sofern auf dem Schulserver der DHCP-Dienst installiert ist, und der angegebene Rechnername über das Domain Name System (DNS) aufgelöst werden kann.

Ab UCS@school 5.0 v2 wird das Ausführen von Python Hooks während des Computer Imports unterstützt (siehe *Python-Hooks* (Seite 83)).

Ab UCS@school 5.0 v3 wird das Ausführen von Python Hooks unterstützt, die ausschließlich während des Computer Imports ausgeführt werden. Sie werden vor bzw. nach den Python Hooks beim Erstellen der UCS@school Objekte ausgeführt.

Ähnlich wie bei den *Python-Hooks* (Seite 83), muss zur Nutzung der Hook-Funktionalität eine Python-Klasse erstellt werden, die von `ucsschool.importer.utils.computer_pyhook.ComputerPyHook` ableitet. Der Name der Datei mit der abgeleiteten Klasse muss auf `.py` enden und die Datei im Verzeichnis `/usr/share/ucs-school-import/pyhooks` abgespeichert werden. Neben den Funktionalitäten der Python Hooks steht in den Hook Methoden der Parameter `row` als Liste zur Verfügung, der die Werte der CSV Zeile als Liste enthält. Dies erlaubt es zusätzliche Werte zu setzen.

`class SchoolComputerImportHook`

```
from typing import List
from ucsschool.lib.models.computer import SchoolComputer
from ucsschool.importer.utils.computer_pyhook import ComputerPyHook

 class SchoolComputerImportHook(ComputerPyHook):
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
    model = SchoolComputer
    priority = {
        "pre_create": 10,
        "post_create": 20,
    }

    def post_create(self, obj: SchoolComputer, row: List[str]) -> None:
        ...

    def post_create(self, obj: SchoolComputer, row: List[str]) -> None:
        ...
```

4.6 Konfiguration von Druckern an der Schule

Der Import der Drucker kann skriptbasiert über das Skript **`/usr/share/ucs-school-import/scripts/import_printer`** erfolgen, das auf dem Primary Directory Node als Benutzer `root` aufgerufen werden muss. Es erwartet den Namen einer CSV-Datei als ersten Parameter, die in folgender Syntax definiert wird. Die einzelnen Felder sind durch ein Tabulatorzeichen zu trennen.

Feld	Beschreibung	Mögliche Werte	Beispiel
Aktion	Art der Druckermodifikation	`A`=Hinzufügen, `M`=Modifizieren, `D`=Löschen	`A`
OU	OU, in der das Druckerobjekt modifiziert werden soll	—	`g123m`
Druckerserver	Name des zu verwendenden Druckservers	—	`dcg123m-01`
Name	Name der Druckerwarteschlange	—	`laserdrucker`
URI	URI, unter dem der Drucker erreichbar ist	—	`lpd://10.0.5.250`

Die Druckerwarteschlange wird beim Anlegen eines neuen Druckers auf dem im Feld *Druckserver* angegebenen Druckserver eingerichtet. Das URI-Format unterscheidet sich je nach angebundenem Drucker und ist in Konfiguration von Druckerfreigaben[11] in *Univention Corporate Server - Handbuch für Benutzer und Administratoren* [2] beschrieben.

[11] https://docs.software-univention.de/manual/5.0/de/print-services/share.html#print-shares

KAPITEL 5

Erweiterte Konfiguration

5.1 Einrichtung der Druckmoderation

Um unnötige oder fehlerhafte Druckaufträge zu minimieren, bietet UCS@school den Lehrern die Möglichkeit, Druckaufträge zu moderieren. Dafür werden die Druckaufträge zunächst über einen speziellen PDF-Drucker (Druckerfreigabe `PDFDrucker`) auf dem Schüler-/Lehrerrechner gedruckt und anschließend durch den Lehrer im UMC-Modul *Drucker moderieren* betrachtet, verworfen oder für den Druck freigegeben.

In UCS@school gibt es vielfältige Möglichkeiten, die Druckmoderation zu konfigurieren und einzusetzen. Nachfolgend wird die Einrichtung eines einzelnen Szenarios beschrieben, welches leicht an die Bedürfnisse der eigenen Schulumgebung angepasst werden kann. In dem beschriebenen Szenario wird der Zugriff auf die physikalischen Drucker für alle Schüler gesperrt.

Für die Druckmoderation ist es erforderlich, dass zunächst wie in *Konfiguration von Druckern an der Schule* (Seite 36) beschrieben, Druckerfreigaben für die zu verwendenden, physikalisch existierenden Drucker angelegt werden.

An den Druckerfreigabeobjekten im UMC-Modul *Drucker* können spezielle Zugriffsrechte gesetzt werden. Dabei kann der Zugriff für einzelne Benutzer oder ganze Gruppen erlaubt bzw. gesperrt werden. Um den Schülern den Zugriff auf die physikalischen Drucker zu verbieten, muss an den Druckerfreigaben für diese Drucker der Zugriff durch Benutzer der OU-spezifischen Gruppe `schueler-`*`OU`* (z.B. `schueler-gsmitte`) verboten werden. Für den PDF-Drucker `PDFDrucker` sollten keine Einschränkungen gemacht werden.

Schüler haben damit nur noch die Möglichkeit Druckaufträge an den `PDFDrucker` zu senden. Im UMC-Modul *Drucker moderieren* können die Druckaufträge anschließend durch den Lehrer aufgelistet und in Form einer PDF-Datei betrachtet werden. Dafür ist ein geeignetes Programm zur Anzeige von PDF-Dateien auf den Lehrerrechnern erforderlich. Die Druckaufträge können dann durch den Lehrer an einen beliebigen physikalischen Drucker der Schule weitergeleitet oder auch verworfen werden.

Lehrer können in dem UMC-Modul grundsätzlich nur die Druckaufträge der Schüler oder ihre eigenen Druckaufträge betrachten. Druckaufträge von anderen Lehrern werden von dem UMC-Modul nicht angezeigt.

Um Ausnahmen von dieser strikte Regelung zu ermöglichen, kann der Lehrer im UMC-Modul *Computerraum* über den Punkt *Einstellungen ändern* den Druckmodus für einen einzelnen Computerraum beeinflussen. Die oben beschriebenen Einschränkungen für Schüler werden dabei als *Standard (globale Einstellungen)* beschrieben. Darüber hinaus kann auch der Druckmodus *Drucken deaktiviert* ausgewählt werden, der das Drucken von den Rechnern des Computerraums vollständig untersagt.

5.1.1 Anlegen eines PDF-Druckers für die Druckermoderation

Druckerfreigaben werden, wie in einer Standard-UCS-Installation, über das UMC-Modul *Drucker* auf dem Primary Directory Node angelegt. Weiterführende Dokumentation findet sich in Druckdienste[12] in *Univention Corporate Server - Handbuch für Benutzer und Administratoren* [2].

Die Drucker müssen unterhalb der OU der Schule angelegt werden. Die Auswahl findet mit der Option *Container* beim Anlegen eines Drucker statt. Bei der OU `gym17` muss beispielsweise `gym17/printers` ausgewählt werden.

Für die Verwendung der Druckermoderation muss ein PDF-Drucker unterhalb der OU der Schule angelegt werden. Dies geschieht in der Regel automatisch bei der Installation von UCS@school bzw. dem Ausführen der Join-Skripte.

Sollte der PDF-Drucker für eine OU fehlen, gibt es zwei Möglichkeiten dieses für eine OU zu erstellen:

- Auf dem Schulserver kann über das UMC-Modul *Domänenbeitritt* das Join-Skript *99ucs-school-umc-printermoderation* (erneut) ausgeführt werden.
- Alternativ kann das LDAP-Objekt im zuständigen Container für Druckerfreigaben der betreffenden OU (siehe oben) angelegt werden. Dabei müssen folgende Werte am Druckerfreigabe-Objekt gesetzt werden:

  Server
  Name des Schulservers

  Protokoll
  `cups-pdf:/`

  Ziel
  leer

  Drucker-Hersteller
  `PDF`

  Drucker-Modell
  `Generic CUPS-PDF Printer`

5.2 Windows-spezifische Benutzereinstellungen

Neben den in *Verwaltung einzelner Benutzerkonten* (Seite 24) und *Pflege von Benutzerkonten für Schüler, Lehrer und Mitarbeiter* (Seite 31) genannten Attributen für Benutzer werden beim Anlegen eines Benutzers auch automatisch einige Windows-spezifische Einstellungen vorgenommen:

- Für die Verwendung von Samba ist es notwendig, dass für jeden Benutzer ein UNC-Pfad für das Windows-Benutzerprofil vorgegeben wird. In der Standardeinstellung von UCS@school wird der jeweilige Logonserver als Ablageort für das Benutzerprofil definiert (`%LOGONSERVER%\%USERNAME%\windows-profiles\default`).

  Falls die Benutzerprofile statt auf dem Logonserver auf einem anderen Dateiserver gespeichert werden sollen, kann in der Univention Management Console am Rechnerobjekt des gewünschten Dateiservers der Dienst *Windows Profile Server* gesetzt werden. Es wird dann ein UNC-Pfad nach dem Schema `\\DATEISERVERNAME\%USERNAME%\windows-profiles\default` am Benutzerobjekt gespeichert.

  Bemerkung: Falls ein alternativer Dateiserver für den Benutzerprofilpfad verwendet werden soll, muss das entsprechende Rechnerobjekt unterhalb der Schul-OU im LDAP-Verzeichnisdienst liegen.

  Für den reibungslosen Betrieb darf der Dienst *Windows Profile Server* nur an einem Dateiserver pro OU gesetzt werden.

  Weiterhin ist der Dienst *Windows Profile Server* veraltet und wird in einer zukünftigen UCS@school-Version entfernt bzw. durch einen äquivalenten Mechanismus ersetzt.

  ---

[12] https://docs.software-univention.de/manual/5.0/de/print-services/index.html#print-general

- Darüber hinaus wird auch automatisch der Pfad zum Heimatverzeichnis des Benutzers gesetzt. In einer Single-Server-Umgebung wird automatisch der Primary Directory Node als Dateiserver eingetragen. In Multi-Server-Umgebungen ist der für die OU zuständige Dateiserver am Schul-OU-Objekt hinterlegt.

  Um diesen zu ändern, muss in der Univention Management Console das OU-Objekt geöffnet werden und auf dem Reiter *UCS@school* im Auswahlfeld *Server für Windows-Heimatverzeichnisse* ein geeigneter Dateiserver ausgewählt werden (siehe auch *Bearbeiten von Schulen* (Seite 24)). Der dort definierte Dateiserver wird beim Anlegen eines Benutzers ausgelesen und der UNC-Pfad am Benutzerobjekt entsprechend gesetzt (Beispiel: `\\server3.example.com\benutzer123`).

Bemerkung: Die Windows-spezifischen Einstellungen werden nur beim Anlegen eines Benutzers gesetzt und am Benutzerobjekt gespeichert.

Ein nachträgliches Modifizieren des Benutzers über die Importskripte hat keinen Einfluss auf diese Einstellungen. Änderungen müssen manuell z.B. über das UMC-Modul *Benutzer* erfolgen.

5.3 Anlegen von Freigaben

Die meisten Freigaben in einer UCS@school-Umgebung werden automatisch erstellt. Jede Klasse oder Arbeitsgemeinschaft verfügt über eine gemeinsame Freigabe. Weiterhin existiert mit der *Marktplatz*-Freigabe je Schule eine schulweite Freigabe. Das Erstellen der Marktplatzfreigabe beim Anlegen einer OU kann durch das Setzen der Univention Configuration Registry Variable `ucsschool/import/generate/marktplatz` auf den Wert `no` verhindert werden.

Diese Freigaben müssen zwingend auf dem Schulserver bereitgestellt werden, um die von UCS@school bereitgestellten Funktionen nutzen zu können.

Weitere Freigaben werden, wie in einer Standard-UCS-Installation, über das UMC-Modul *Freigaben* auf dem Primary Directory Node angelegt. Weiterführende Dokumentation findet sich in Verwaltung von Freigaben[13] in *Univention Corporate Server - Handbuch für Benutzer und Administratoren* [2].

Die Freigaben müssen unterhalb der OU der Schule angelegt werden. Die Auswahl findet mit der Option *Container* beim Anlegen einer Freigabe statt. Für die OU `gym17` muss beispielsweise der Container `gym17/shares` ausgewählt werden.

Neu in Version 4.1: R2 v5

Seit UCS@school 4.1 R2 v5 werden neue Freigaben (sowohl automatisch, als auch manuell erstellte) standardmäßig nur noch per Samba/CIFS freigegeben. Um neue Freigaben standardmäßig auch per NFS zu exportieren, muss die Univention Configuration Registry Variable `ucsschool/default/share/nfs` auf allen UCS@school-Systemen auf den Wert `yes` gesetzt werden.

Um den NFS-Export einer Freigabe manuell ein- oder auszuschalten, kann im UMC-Modul *Freigaben* für jede Freigabe die Option *Für NFS-Clients exportieren (NFSv3 und NFSv4)* (de)aktiviert werden.

5.4 Lehrerzugriff auf Benutzerfreigaben

Lehrern kann der Zugriff auf alle Heimatverzeichnisse von Schülern an einer Schule freigeschaltet werden. Dies geschieht durch Installation des Pakets **`ucs-school-roleshares`** auf dem jeweiligen Schulserver. Der Zugriff kann dann über eine spezielle Dateifreigabe erfolgen.

Das Paket installiert das Skript **`/usr/share/ucs-school-import/scripts/create_roleshares`**, welches über das Join-Skript automatisch aufgerufen wird und später auch manuell aufgerufen werden kann. Mit der Standardoption `--create student` aufgerufen, legt es für alle Dateiserver des Schulstandorts jeweils eine Freigabe mit dem Namensschema `schueler-`*`OU`* an. Die Freigabe erlaubt der Gruppe `lehrer-`*`OU`* den administrativen Zugriff auf das Basisverzeichnis `/home/`*`OU`*`/schueler`.

[13] https://docs.software-univention.de/manual/5.0/de/shares/index.html#shares-general

Per Voreinstellung wird der Lehrergruppe Lesezugriff gewährt. Die Freigabe wird vom jeweiligen Dateiserver nicht explizit angezeigt. Eine an einem Windows-Arbeitsplatz angemeldete Lehrkraft sollte automatisch eine Verknüpfung zu dieser Freigabe angezeigt bekommen.

Die Freigabe-Einstellungen dieser Freigabe können wie üblich über die Univention Management Console auf dem Primary Directory Node angepasst werden, z.B. um Lehrern auch Schreibzugriff zu gewähren.

Voraussetzung für diese Funktion ist, dass die Heimatverzeichnisse der Benutzerkonten in entsprechend strukturierten Unterverzeichnissen angelegt wurden. Dies geschieht in Domänen die mit UCS@school 3.2 R2 oder später installiert wurden automatisch. In älteren Umgebungen wird dies dadurch verhindert, dass dort Univention Configuration Registry Variable `ucsschool/import/roleshare` automatisch auf `no` gesetzt wurde. Dies gewährleistet eine einheitliche Anlage der Heimatverzeichnisse und sollte erst nach einer manuellen Migration der Heimatverzeichnisse geändert werden.

5.5 Anlegen von Benutzerkonten für Schuladministratoren

Ab UCS@school 4.4 v8 können Benutzerkonten für Schuladministratoren direkt über das UCS@school UMC-Modul angelegt werden. Diese Option ist standardmäßig abgeschaltet. Um das Verhalten zu aktivieren, muss der Wert `schoolAdmin` aus der Univention Configuration Registry Variable `ucsschool/wizards/schoolwizards/users/roles/disabled` entfernt werden. Schuladministratoren, die mit dem UCS@school UMC-Modul erstellt werden, besitzen nicht die Option *UCS@school-Lehrer* und befinden sich nicht in der Gruppe *lehrer-OU*.

Benutzerkonten von Lehrern können durch eine zusätzliche Gruppenmitgliedschaft und das Einschalten einer Option zu Schuladministratoren umgewandelt werden.

- Die zusätzliche Gruppenmitgliedschaft muss manuell über das Univention Management Console-Modul *Benutzer* auf dem Primary Directory Node hinzugefügt werden. Auf dem Reiter *Gruppen* muss das Benutzerkonto in die Gruppe `admins-`*OU* (für die OU *gym17* ist dies die Gruppe `admins-gym17`) aufgenommen werden.
- Im Univention Management Console-Modul *Benutzer* muss außerdem im Reiter *Optionen* die Option *UCS@school-Administrator* eingeschaltet werden.

Warnung: Es ist nicht möglich, ein Benutzerkonto einzurichten, das mit der Rolle *Schuladministrator* an einer Schule und mit der Rolle *Lehrer* an einer anderen Schule agiert.

Ein Benutzerkonto mit der Option *UCS@school-Administrator* verfügt standardmäßig über einige Schuladministrator-Berechtigungen für alle Schulen, an denen es Mitglied ist. Das gilt auch, wenn das Benutzerkonto kein Mitglied der Gruppe `admins-`*OU* für die jeweilige Schule ist. Die Gruppenmitgliedschaft des Benutzerkontos in `admins-`*OU* fügt für die jeweilige Schule weitere Schuladministrator-Berechtigungen hinzu.

Ein Benutzerkonto mit aktivierter *UCS@school-Administrator*-Option muss für alle Schulen, in denen das Benutzerkonto Mitglied ist, auch zu den Gruppen `admins-`*OU* hinzugefügt werden. Auf diese Weise finden Schuladministratoren an allen Schulen das gleiche, konsistente Verhalten für administrative Tätigkeiten im Rahmen ihrer Schuladministrator-Berechtigungen vor. Systemadministratoren erkennen besser, welche Benutzerkonten die Schuladministrator-Berechtigung haben.

Fungiert das Benutzerkonto nicht mehr als Lehrer, sondern nur noch als Schuladministrator, so kann im Reiter *Optionen* die Option *UCS@school-Lehrer* deaktiviert und dem Benutzer die Gruppe `lehrer-`*OU* entzogen werden.

Soll ein Schuladministrator auch als Lehrer tätig sein, muss zusätzlich die Gruppe `lehrer-`*OU*, also z.B. `lehrer-gym17`, hinzugefügt werden. Abschließend müssen die Angaben für Profilpfad und Heimatverzeichnispfad am Benutzerobjekt gesetzt werden, um das gleiche Verhalten wie bei Schüler- und Lehrerkonten zu erhalten (siehe dazu auch *Windows-spezifische Benutzereinstellungen* (Seite 38)).

5.6 Konfiguration der Helpdesk-Kontaktadresse

Über das Helpdesk-Modul können Lehrer per E-Mail Kontakt zum Helpdesk-Team einer Schule aufnehmen. Damit dieses Modul genutzt werden kann, muss auf dem jeweiligen Server die Univention Configuration Registry Variable `ucsschool/helpdesk/recipient` auf die E-Mailadresse des zuständigen Helpdesk-Teams gesetzt werden.

5.7 Konfiguration des Computerraum-Moduls

Im UMC-Modul *Computerraum* kann z.B. über die Funktion *Beobachten* eine verkleinerte Desktop-Ansicht der aufgelisteten Windows-Rechner angezeigt werden. Dabei ist es möglich, die Desktops bestimmter Benutzergruppen von dieser Anzeige auszuschließen. In der Standardkonfiguration ist dies die Gruppe `Domain Admins`.

Über die Univention Configuration Registry-Variable `ucsschool/umc/computerroom/hide_screenshots/groups` kann eine abweichende kommaseparierte Liste mit Gruppennamen konfiguriert werden, z.B. `Domain Admins,Helpdesk`. Da UCS@school für jede Schule für die dort agierenden Lehrer eine eigene Benutzergruppe anlegt, wurde zur Vereinfachung eine weitere Univention Configuration Registry-Variable `ucsschool/umc/computerroom/hide_screenshots/teachers` eingeführt. Wird in dieser Variable der Wert `yes` hinterlegt, ist das Betrachten der Desktop-Ansicht von Rechnern, an denen Lehrer angemeldet sind, nicht mehr möglich.

Über die Univention Configuration Registry-Variable `ucsschool/umc/computerroom/screenshot_dimension` kann eine gewünschte Auflösung für Screenshots zur Überwachung der einzelnen Computer im Computerraum angegeben werden. Bei Benutzung der Standardeinstellung (nicht gesetzt) wird die Auflösung des Zielrechners verwendet. Soll eine andere Auflösung verwendet werden, muss die Variable gesetzt werden. Hierbei wird ein String des Formats `<Breite>x<Höhe>` erwartet.

Vorsicht: Die Anpassung der Univention Configuration Registry-Variable `ucsschool/umc/computerroom/screenshot_dimension` erlaubt die Optimierung der Bandbreiten und CPU-Auslastung. Die Auflösung wird an die Veyon WebAPI weitergereicht, es werden aber nicht alle Auflösungen unterstützt. Im Falle einer nicht unterstützten Auflösung wird kein Screenshot als Antwort ausgegeben. Daher ist die Verwendung von Standardauflösungen empfohlen. Die geringste, funktionstüchtige Auflösung ist *240p* (320x240 Pixel).

Über die Aktion *Computer einschalten* können *WakeOnLAN*-Pakete an die betreffenden Rechner verschickt werden, um diese einzuschalten. Ab UCS@school 4.4v4 werden diese *WakeOnLAN*-Pakete über alle Netzwerkschnittstellen des UCS@school-Systems verschickt.

Falls die Pakete auf bestimmten Netzwerkschnittstellen nicht verschickt werden sollen, können diese Schnittstellen über die UCR-Variablen `ucsschool/umc/computerroom/wakeonlan/blacklisted/interfaces` und `ucsschool/umc/computerroom/wakeonlan/blacklisted/interface_prefixes` festgelegt werden. Dabei sind die einzelnen Werte durch Leerzeichen zu trennen, z.B. `tun docker`. Wenn sich die Zielrechner in einem anderen Netzwerk befinden, können über die UCR-Variable `ucsschool/umc/computerroom/wakeonlan/target_nets` die Subnetze angepasst werden, an die Pakete gesendet werden. Dabei sind die einzelnen Werte durch Leerzeichen zu trennen, z.B. `255.255.255.255 10.200.18.255`.

Neu in Version 4.4: v4

Ab Version 4.4 v4 prüft das Computerraum-Modul von UCS@school in der Standardeinstellung regelmäßig, ob alle gesperrten Rechner weiterhin noch gesperrt sind, um z.B. Rechner nach deren Neustart wieder in den gesperrten Zustand zu versetzen. Das Intervall, in dem die Überprüfung läuft, kann durch die Univention Configuration Registry-Variable `ucsschool/umc/computerroom/screenlock/interval` konfiguriert werden. In der Standardkonfiguration wird die Prüfung alle 5 Sekunden durchgeführt. Wird der Wert der Variable auf 0 gesetzt, wird die Prüfung abgeschaltet.

Neu in Version 4.4: v8

Ab UCS@school 4.4v8 werden Rechner mit mehreren IP-Adressen unterstützt. Die IP-Adressen des jeweiligen Rechners werden durchlaufen und die erste verwendet, die erreicht werden kann. Dies kann zu längeren Wartezeiten

führen, wenn Rechner innerhalb des Computerraums ausgeschaltet sind oder eine Firewall den Befehl blockiert. Das Verhalten ist standardmäßig deaktiviert und kann durch Setzen der Univention Configuration Registry-Variable `ucsschool/umc/computerroom/ping-client-ip-addresses` aktiviert werden.

Vorsicht: Ab UCS@school 5.0 wird *Veyon* als Computerraum Backend eingesetzt. In den UMC-Modulen *Computerraum* und *Klassenarbeiten* werden fortan nur noch Computerräume angezeigt, deren Backend auf *Veyon* gesetzt ist.

Für die Zeit der Migration in Multi-Server-Umgebungen können Computerräume, die iTALC als Backend verwenden und auf Replica Directory Node betrieben werden, die noch UCS@school 4.4v9 verwenden, weiter verwendet werden. Die Migration von iTALC auf *Veyon* in diesen Mischumgebungen erfolgt im UMC-Modul *Computerräume verwalten* auf dem entsprechenden Replica Directory Node (und nicht auf dem Primary Directory Node). Die Schritte der Migration von iTALC zu *Veyon* sind in Univention Help 16937 - „Migration of the computer room backend iTALC to Veyon“[14] beschrieben.

5.8 Konfiguration des Klassenlisten-Moduls

Über das UMC-Modul *Klassenlisten* können Listen mit Schülerdaten einer ausgewählten Klasse exportiert werden. In der Standardkonfiguration werden die UDM Attribute `firstname`, `lastname` und `username` sowie die ausgewählte Klasse angezeigt.

Mit der Univention Configuration Registry Variable `ucsschool/umc/lists/class/attributes` können die angezeigten Attribute angepasst werden. Die Variable beschreibt eine Zuordnung der anzuzeigenden UDM Attribute zu den angezeigten Spaltennamen. Dabei sind die Zuordnung durch Kommata zu trennen, z.B. `firstname Vorname,lastname Nachname,Class Klasse,username Username`. Für `Class` wird dabei die ausgewählte Klasse eingesetzt.

5.9 Konfiguration der Materialverteilung

Neu in Version 5.0v5: Ab UCS@school 5.0v5 ist es möglich Lehrer bei der Materialverteilung und -Einsammlung auszuschließen.

Um diese Einstellung zu aktivieren, muss die Univention Configuration Registry Variable `ucsschool/datadistribution/exclude_teachers` auf `True` gesetzt werden. Dadurch werden Lehrkräfte, die sich in Klassen oder Arbeitsgruppen befinden, bei der Verteilung und dem Einsammeln der Materialien ignoriert.

5.10 Konfiguration von Email-Adressen für Arbeitsgruppen

Neu in Version 4.4v7: Ab UCS@school 4.4v7 ist es möglich die Aktivierung von E-Mailadressen für Arbeitsgruppen über das Modul *Arbeitsgruppen verwalten* zu erlauben.

Um dieses Feature zu aktivieren, muss die Univention Configuration Registry Variable `ucsschool/workgroups/mailaddress` gesetzt werden. Der eingetragene Wert bestimmt das Muster, nach dem die E-Mailadresse einer Arbeitsgruppe berechnet wird.

Es stehen folgende Platzhalter-Werte zur Verfügung:

- `{ou}`
- `{name}`

Ist der Wert der Univention Configuration Registry Variable beispielsweise `{ou}-{name}@schule-univention.de`, so wird für eine Arbeitsgruppe mit dem Namen `AG1` an der Schule `DEMOSCHOOL` die E-Mailadresse `DEMOSCHOOL-AG1@schule-univention.de` berechnet.

[14] https://help.univention.com/t/16937

5.11 Provisionierung von Benutzern zu Apple School Manager

Die Apple School Manager Connector App für UCS@school synchronisiert automatisch Benutzer zu Apple School Manager (ASM). Das UCS@school Identity Management übernimmt die Rolle des Studierendeninformationssystems und verwendet die SFTP-Schnittstelle, wie sie von Apple bereit gestellt wird.

KAPITEL 6

Integration und Verwaltung von Microsoft Windows-Clients

Microsoft Windows-Clients werden in Univention Corporate Server (UCS) mithilfe von Samba integriert und verwaltet. Die Windows-Clients authentifizieren sich dabei gegen den Samba-Server. Auch Datei- und Druckdienste werden für die Windows-Clients über Samba bereitgestellt. Weitere Hinweise finden sich in *Anmeldedienste mit Samba* (Seite 46).

Die Netzkonfiguration der Clients kann zentral über in UCS integrierte DNS- und DHCP-Dienste durchgeführt werden. Weitere Hinweise finden sich in *Skriptbasierter Import von PCs* (Seite 34).

Beim Import von neuen Benutzern des Edukativnetzes über die Importskripte oder über den Assistenten in der UMC werden automatisch windows-spezifische Einstellungen zum Profilpfad und zum Heimatverzeichnispfad vorgenommen. Weitere Hinweise finden sich in *Windows-spezifische Benutzereinstellungen* (Seite 38).

Auf den Windows-Clients der Schüler kann die Software *Veyon* installiert werden. Sie erlaubt es Lehrern, über ein UMC-Modul den Desktop der Schüler einzuschränken und z.B. Bildschirme und Eingabegeräte zu sperren. Außerdem kann ein Übertragungsmodus aktiviert werden, der die Bildschirmausgabe des Desktops des Lehrers auf die Schülerbildschirme überträgt. Die Installation von *Veyon* wird in *Computerraumüberwachung in UCS@school mit Veyon* (Seite 47) beschrieben.

Aufgrund einiger Limitierungen (u.a. von *Veyon*) kann auf Windows-Terminalservern nicht der volle Funktionsumfang von UCS@school genutzt werden. Die Verwendung von Terminalservern mit UCS@school wird daher nicht unterstützt.

Wichtig: Die App **`UCS@school Veyon Proxy`** wird in Single-Server-Umgebungen, sowie auf edukativen Schulservern automatisch installiert. Sie wird von UCS@school angesprochen und ist nicht zur manuellen Verwendung gedacht.

Die App **darf nicht** manuell deinstalliert werden.

6.1 Anmeldedienste mit Samba

UCS@school integriert *Samba 4*. Die Unterstützung von Domänen-, Verzeichnis- und Authentifizierungsdiensten, die kompatibel zu Microsoft Active Directory sind, erlauben den Aufbau von Active Directory-kompatiblen Windows-Domänen. Diese ermöglichen u.a. die Verwendung der von Microsoft bereit gestellten Werkzeuge beispielsweise für die Verwaltung von Benutzern oder Gruppenrichtlinien (GPOs). Univention hat die benötigten Komponenten für die Bereitstellung von Active Directory kompatiblen Domänendiensten mit Samba 4 getestet und in enger Zusammenarbeit mit dem Samba-Team in UCS integriert.

Vorsicht: Bei der Verwendung von Samba 4 in einer Multi-Server-Umgebung ist es zwingend erforderlich, dass alle Windows-Clients ihren jeweiligen Schul-DC als DNS-Server verwenden, um einen fehlerfreien Betrieb zu gewährleisten.

Windows-Clients des Edukativnetzes, die ihre DNS-Einstellungen über DHCP beziehen, erhalten in der Standardeinstellung automatisch die IP-Adresse des Schul-DCs als DNS-Server zugewiesen. Dafür wird beim Joinen eines Schulservers automatisch am unter dem Schul-OU-Objekt liegenden DHCP-Container eine DHCP-DNS-Richtlinie verknüpft. Das automatische Verknüpfen dieser Richtlinie kann über das Setzen einer UCR-Variable auf dem Primary Directory Node *und* dem Schulserver deaktiviert werden. Die folgende Variable muss vor der Installation von UCS@school oder dem Update des Systems gesetzt werden:

```
$ ucr set ucsschool/import/generate/policy/dhcp/dns/set_per_ou=false
```

Dies lässt sich am besten über eine UCR-Richtlinie für die gesamte UCS@school-Domäne erledigen. Wurde die Variable versehentlich nicht gesetzt, werden automatisch fehlende DHCP-DNS-Richtlinien wieder angelegt und mit den entsprechenden DHCP-Container der Schul-OU-Objekte verknüpft. Dies kann gerade in Verwaltungsnetzen zu Fehlfunktionen führen (siehe auch *Verwaltungsnetz und Edukativnetz* (Seite 6)).

Bei Neuinstallationen von UCS@school wird standardmäßig Samba 4 installiert. Umgebungen, die von einer Vorversion aktualisiert werden, müssen von Samba 3 auf Samba 4 migriert werden. Das dafür notwendige Vorgehen ist unter der folgenden URI dokumentiert: Univention Help 21846 - „UCS@school Samba 3 to Samba 4 Migration“[15].

Weiterführende Hinweise zur Konfiguration von Samba finden sich in Services für Windows[16] in *Univention Corporate Server - Handbuch für Benutzer und Administratoren* [2].

6.2 Server für Dateifreigaben

Beim Anlegen einer neuen Klasse bzw. eines Benutzers wird automatisch eine Klassenfreigabe für die Klasse bzw. eine Heimatverzeichnisfreigabe für den Benutzer eingerichtet. Der für die Einrichtung der Freigabe notwendige Dateiserver wird in den meisten Fällen ohne manuellen Eingriff bestimmt. Dazu wird am Schul-OU-Objekt bei der Registrierung einer Schule automatisch der in der Univention Management Console angegebene Schulserver als Dateiserver jeweils für Klassen- und Benutzerfreigaben hinterlegt.

Die an der Schul-OU hinterlegte Angabe bezieht sich ausschließlich auf neue Klassen- und Benutzerobjekte und hat keinen Einfluss auf bestehende Objekte im LDAP-Verzeichnis. Durch das Bearbeiten der entsprechenden Schul-OU im UMC-Modul *LDAP-Verzeichnis* können die Standarddateiserver für die geöffnete Schul-OU nachträglich modifiziert werden.

Es ist zu beachten, dass die an der Schul-OU hinterlegten Dateiserver nur in einer Multi-Server-Umgebung ausgewertet werden. In einer Single-Server-Umgebung wird für beide Freigabetypen beim Anlegen neuer Objekte immer der Primary Directory Node als Dateiserver konfiguriert.

[15] https://help.univention.com/t/21846
[16] https://docs.software-univention.de/manual/5.0/de/windows/index.html#windows-services-for-windows

6.3 Netlogon-Skripte für Samba 4 Umgebung

In UCS-Umgebungen mit mehreren Samba 4 Domänencontrollern werden in der Standardeinstellung alle Dateien der *NETLOGON*-Dateifreigabe automatisch (durch die *SYSVOL*-Replikation) zwischen allen Samba 4 Domänencontrollern repliziert. Beim Einsatz von UCS@school kann es bei der Verwendung von domänenweiten Benutzerkonten und benutzerspezifischen Netlogon-Skripten zu Synchronisationskonflikten kommen. Konflikte können ebenfalls bei eigenen, standortbezogenen Netlogon-Skripten auftreten.

In diesen Fällen ist es ratsam, die Synchronisation der *NETLOGON*-Freigabe zu unterbinden, indem ein abweichendes Verzeichnis für die *NETLOGON*-Freigabe definiert wird. Das Verzeichnis darf dabei nicht unterhalb der *SYSVOL*-Dateifreigabe (`/var/lib/samba/sysvol/REALM/`) liegen.

Das folgende Beispiel setzt das Verzeichnis der *NETLOGON*-Freigabe auf `/var/lib/samba/netlogon/` und passt ebenfalls das Verzeichnis für die automatisch generierten Benutzer NETLOGON-Skripte an:

```
$ ucr set samba/share/netlogon/path=/var/lib/samba/netlogon
$ ucr set ucsschool/userlogon/netlogon/path=/var/lib/samba/netlogon/user
```

Die zwei UCR-Variablen müssen auf allen Samba 4 Domänencontrollern gesetzt werden. Dies kann z.B. in der UMC über eine UCR-Richtlinien global definiert werden. Nach der Änderung müssen die Dienste `samba` und `univention-directory-listener` neu gestartet werden:

```
$ service samba restart
$ service univention-directory-listener restart
```

6.4 Computerraumüberwachung in UCS@school mit Veyon

Veyon[17] ist eine freie und quelloffene Software zur plattformübergreifenden Überwachung und Steuerung von Computern. In UCS@school können Sie *Veyon* verwenden, um in Computerräumen die Computer von Schülern zu steuern und zu überwachen.

Sie können *Veyon* mit den folgenden Möglichkeiten nutzen:

- über die integrierte UCS@school-Web-Oberfläche
- direkt über die von *Veyon* bereitgestellte Windows Applikation **`Veyon Master`**.

Damit Sie die Web-Oberfläche nutzen können, müssen Sie die folgenden Installations- und Konfigurationsschritte abschließen:

1. *Veyon Installation auf Windows-Clients von Schülern* (Seite 48)
2. *Veyon Konfiguration für die UCS@school Web-Oberfläche* (Seite 49)

Alternativ können Sie die Rechner so einrichten, dass Sie die Windows Applikation **`Veyon Master`** verwenden. Für **`Veyon Master`** müssen Sie die folgenden Schritte abschließen:

1. *Veyon Installation auf Windows-Clients von Schülern* (Seite 48)
2. *Veyon Installation auf Windows-Clients von Lehrern* (Seite 53)
3. *Einrichten des Veyon Master* (Seite 54)

Lehrende, die den **`Veyon Master`** verwenden, finden Informationen im Veyon-Benutzerhandbuch[18].

Welche Möglichkeit Sie wählen, hängt neben den verfügbaren Features auch von der Anzahl der gleichzeitig zu überwachenden Computer bzw. Computerräume ab.

Wichtig: Auf den Windows-Clients muss in jedem Fall sichergestellt werden, dass die installierte System-Firewall den Port `11100` nicht blockiert. Der offene Port `11100` ist Voraussetzung für eine funktionierende

[17] https://veyon.io/de/
[18] https://docs.veyon.io/de/latest/user/index.html

Veyon-Umgebung, da Veyon diesen Port für die Kommunikation mit dem Schulserver bzw. anderen Computern verwendet.

Siehe auch:

Import/Export der Konfiguration[Seite 48, 19] **im Veyon-Administrationshandbuch**
für Information über Werkzeuge, die die Übertragung von Konfigurationen erleichtern.

6.4.1 Systemanforderungen des UCS@school Veyon Proxy

Wenn Sie die integrierte Web-Oberfläche zur Überwachung der Computerräume verwenden, steigen die Hardwareanforderungen an den Schulserver. Tab. 6.1 liefert eine Orientierung über die Hardwareanforderungen.

Ein Computer gilt dabei als aktiv, wenn er angeschaltet ist und sich in einem Computerraum befindet, welcher zu diesem Zeitpunkt überwacht wird.

Computer, die nicht aktiv überwacht werden, spielen für die Performance nur eine untergeordnete Rolle.

Warnung: Es gilt zu beachten, dass es sich hierbei um Messungen unter Laborbedingungen handelt. Die tatsächlichen Hardwareanforderungen können mitunter stark von den Angaben abweichen und sind zum Beispiel von der Bildschirmauflösung und aktiver Nutzung der Windowsrechner, sowie der tatsächlichen Leistung der Prozessorkerne abhängig.

Tab. 6.1: Minimale Systemressourcen unter Last

Anzahl gleichzeitig aktiver Computer	Arbeitsspeicher	Ausgelastete Prozessoren
20	500 MB	2 vCPU / Threads
40	1000 MB	3 vCPU / Threads
80	2000 MB	6 vCPU / Threads
120	3000 MB	8 vCPU / Threads
200	5000 MB	12 vCPU / Threads

Die aufgeführten benötigten Systemressourcen wurden mit einem `Intel® Xeon® Silver 4314 Prozessor` gemessen. Die Hardwareanforderungen können je nach Umgebung reduziert werden, indem die Einstellungen der Veyon Proxy App und des Computerraum Moduls angepasst werden, wie in *Performance-Optimierungen der App UCS@school Veyon Proxy* (Seite 51) beschrieben. Für diese Messungen wurden die Einstellungen nicht angepasst.

Bemerkung: Bei mehr als 200 gleichzeitig aktiven Computern empfehlen wir den direkten Einsatz von **`Veyon Master`**, siehe *Einrichten des Veyon Master* (Seite 54).

6.4.2 Veyon Installation auf Windows-Clients von Schülern

Dieser Abschnitt beschreibt die Installation von *Veyon* auf den Schüler-PCs. Für Informationen über die Administration über die UCS@school Web-Oberfläche durch Lehrkräfte, siehe *UCS@school - Handbuch für Lehrkräfte und Schuladministratoren* [1].

Für die Nutzung der Rechnerüberwachungs- und Präsentationsfunktionen in der Computerraumverwaltung (siehe *Modulübersicht* (Seite 59)) wird vorausgesetzt, dass auf den Windows-Clients die Software *Veyon* installiert wurde und als Computerraum Backend des entsprechenden Computerraums *Veyon* gesetzt ist (siehe *Konfiguration des Computerraum-Moduls* (Seite 41)).

[19] https://docs.veyon.io/de/latest/admin/configuration.html#confimportexport

Neu in Version 4.4v9: Seit UCS@school 4.4 v9 sind Windows-Binärpakete für die Open Source-Software *Veyon* in UCS@school enthalten.

Die Binärpakete sind direkt über die Samba-Freigabe *Veyon-Installation* abruf- und installierbar. Die Installationsdatei der 64-Bit Version von *Veyon* findet sich auf dem Schulserver im Verzeichnis `/usr/share/ucs-school-veyon-windows/`.

Interoperabilitätstests zwischen UCS@school und *Veyon* wurden ausschließlich mit der von UCS@school mitgelieferten *Veyon* Version unter Windows 7 und Windows 10 (64 Bit) durchgeführt.

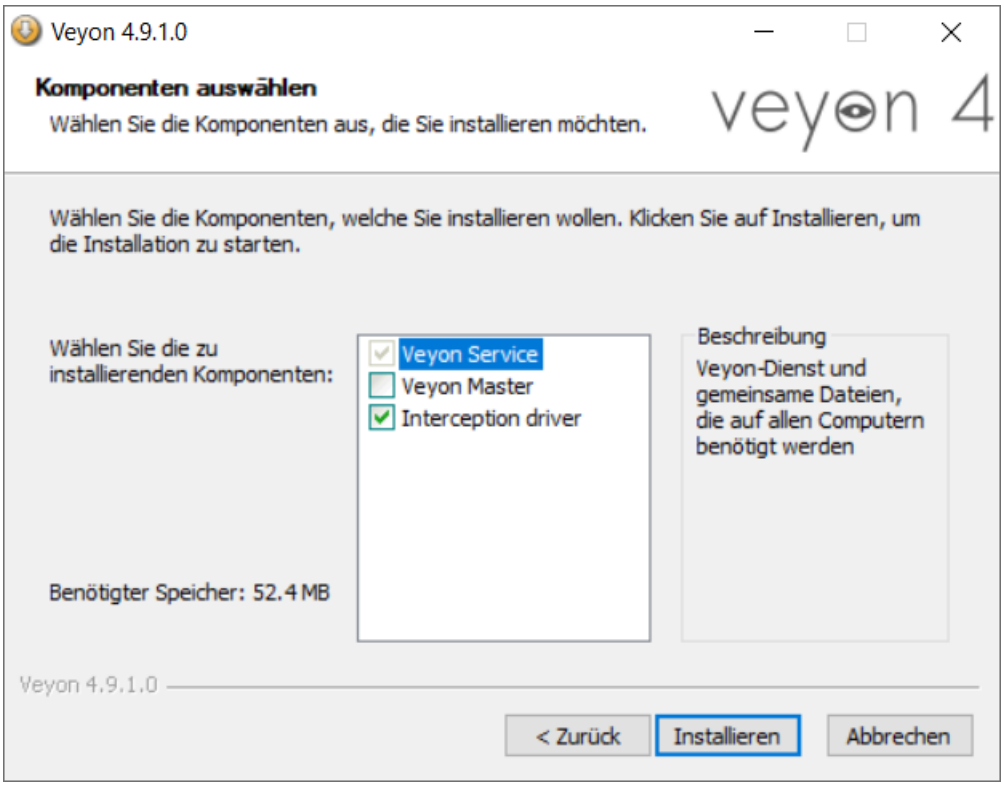

Abb. 6.1: *Veyon* Installation: Auswahl der Komponenten

Veyon bringt ein Installationsprogramm mit, das durch alle notwendigen Schritte führt. Installieren Sie *Veyon Service* sowie *Interception driver*. Auf den Schüler-PCs ist kein **`Veyon Master`** nötig.

6.4.3 Veyon Konfiguration für die UCS@school Web-Oberfläche

Falls eine direkte Steuerung über den **`Veyon Master`** gewünscht ist, ist dieser Abschnitt nicht notwendig und kann übersprungen werden.

Nach der Installation von *Veyon* auf dem Windows-Client muss das Programm mit dem installierten *Veyon Configurator* für eine Schlüsseldatei-Authentifizierung konfiguriert werden. Zunächst muss im *Veyon Configurator* unter *Allgemein* ‣ *Authentifizierung* die Methode Schlüsseldatei-Authentifizierung ausgewählt werden. Anschließend muss unter *Allgemein* ‣ *Benutzergruppen* die Checkbox *Benutzergruppen von Domain einbeziehen* aktiviert werden. Als *Benutzergruppen-Backend* wird der Standard *Systembenutzergruppen* verwendet.

Bemerkung: Falls ein *Veyon Configurator* mit Version 4.7 oder 4.8 verwendet wird, muss anstatt der Checkbox *Benutzergruppen von Domain einbeziehen* unter *Allgemein* ‣ *Benutzergruppen* die Checkbox *Verwendung von Domaingruppen aktivieren* unter *Zugriffskontrolle* aktiviert werden.

Schließlich muss der öffentliche Schlüssel importiert werden, damit der Schulserver Zugriff auf das installierte *Veyon* Backend erhält. Der Import kann mit *Authentifizierungsschlüssl* ‣ *Schlüssel importieren* durchgeführt werden. Dort ist der *Veyon* Schlüssel des Schulservers anzugeben.

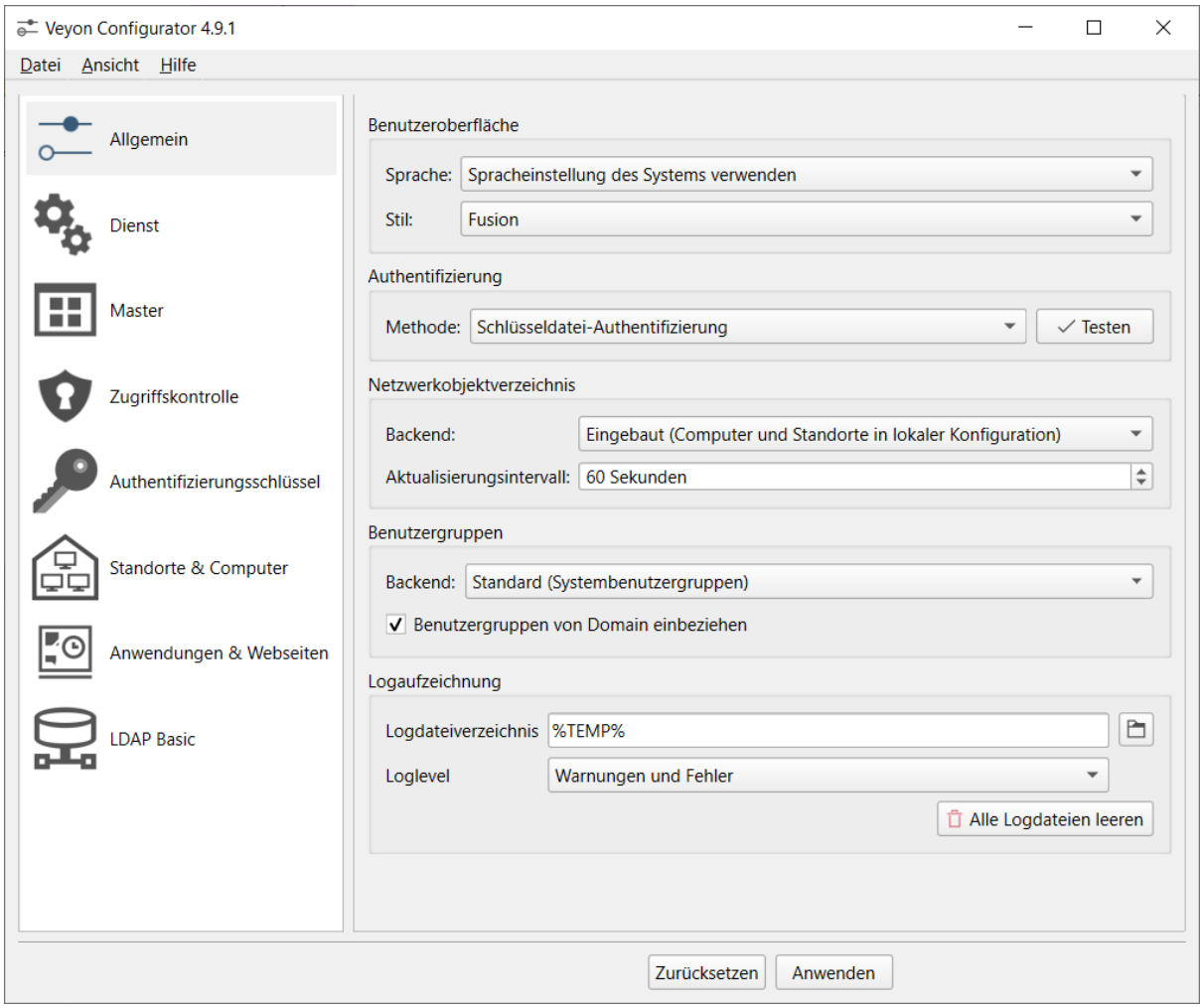

Abb. 6.2: *Veyon* Konfiguration: Auswahl der Authentifizierungs-Methode

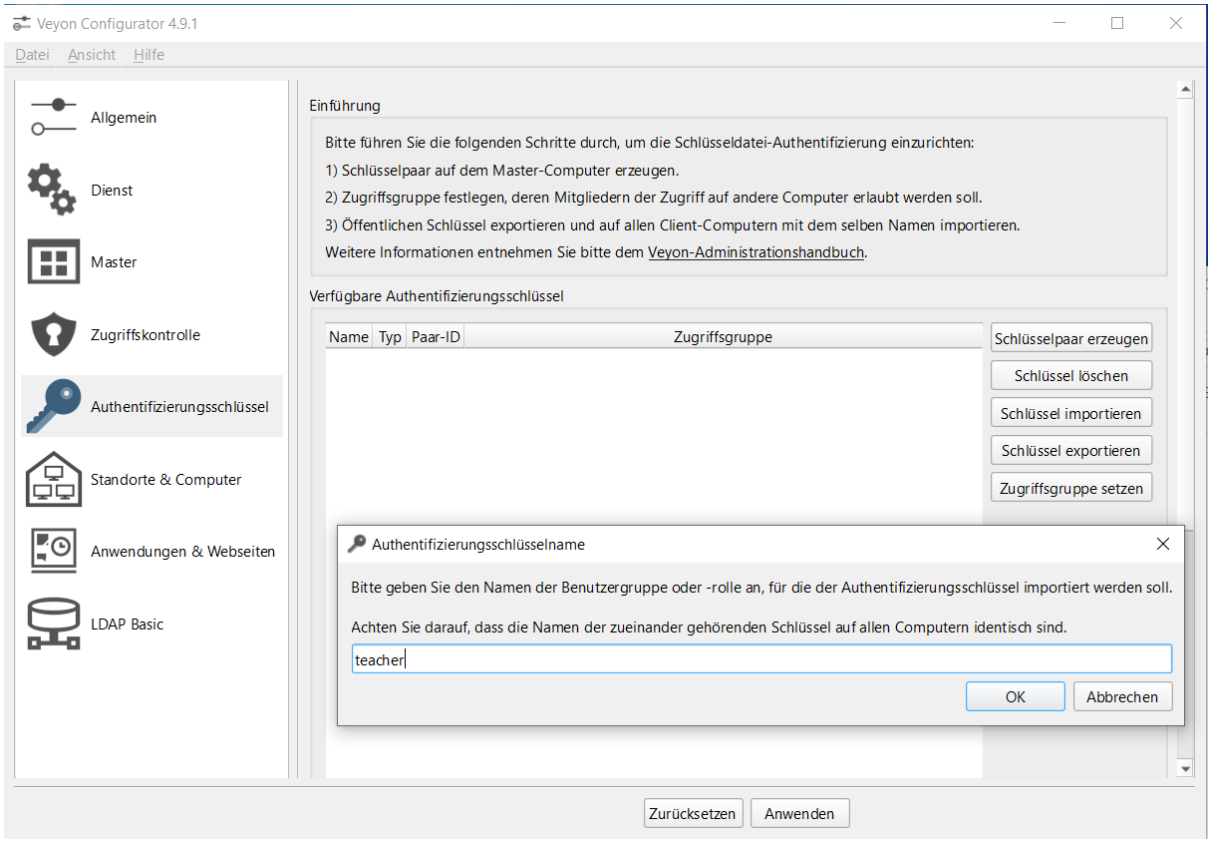

Abb. 6.3: *Veyon* Konfiguration: Schlüsselimport

Der Schlüssel wird automatisch auf der SYSVOL-Freigabe des Schulservers unter dem Namen der Schuldomäne unter `scripts/veyon-cert_SERVERNAME.pem` abgelegt. (U.U. liegt dort zusätzlich eine Datei `veyon-cert.pem` *ohne* den Namen des Servers. Diese sollte nicht verwendet werden.) Im Dialog *Authentifizierungsschlüsselname* muss der Name *teacher* angegeben werden. Außer den beschriebenen Konfigurationen müssen keine weiteren Anpassungen vorgenommen werden.

Der Konfigurationstest im *Veyon Configurator* unter *Allgemein* ‣ *Authentifizierung* ‣ *Testen* wird trotz korrekter Einrichtung fehlschlagen. Die korrekte Einrichtung kann im *Computerraum* Modul überprüft werden. Hier sollte sich der Punkt neben dem Namen des eingerichteten Windows Clients dunkelgrau färben.

6.4.4 Performance-Optimierungen der App `UCS@school Veyon Proxy`

Vorsicht: Dieser Abschnitt beschreibt ausschließlich Experteneinstellungen zur Optimierung und kann bei einer regulären Installation übersprungen werden. Die weiter unten beschriebenen Einstellung zum **`UCS@school Veyon Proxy`** werden ohne Verifikation direkt an den im Docker-Container enthaltenen Veyon Master weitergereicht.

Bemerkung: Alle Einstellungen müssen auf dem edukativen Schulservern gemacht werden.

Ab Version *4.8.3.8-ucs1* des **`UCS@school Veyon Proxy`** stehen neue App-Einstellungen zur Verfügung um Performance-Optimierungen zu definieren.

Die Einstellungen steuern die Verbindung zwischen **`UCS@school Veyon Proxy`** und den Windows-Clients.

- `veyon/Master/ComputerMonitoringUpdateInterval`

- veyon/Master/ComputerMonitoringImageQuality
- veyon/Core/ComputerStatePollingInterval
- veyon/WebAPI/ConnectionIdleTimeout

Quellcode 6.1: App-Einstellungen werden wie folgt geändert, die App wird dabei neu gestartet.

```
univention-app configure ucsschool-veyon-proxy --set veyon/WebAPI/
↪ConnectionIdleTimeout=60
```

Die Einstellung veyon/Master/ComputerMonitoringImageQuality bietet die Möglichkeit die Qualität der VNC Verbindung zwischen den Windows-Clients und dem **UCS@school Veyon Proxy** zu ändern. Der Wert ist von 0 (höchste Qualität) bis 4 (niedrigste Qualität) begrenzt. Auf Stufe 4 können Kompressionsartefakte erkennbar sein, ein Unterschied zwischen den Stufen ist meist nur im direkten Vergleich erkennbar. Ist die Qualität niedrig eingestellt reduziert dies die Datenmenge, die über die VNC Verbindung zwischen Windows-Clients und dem **UCS@school Veyon Proxy** übertragen wird. Wir empfehlen Stufe 4 als Standardeinstellung.

Die Einstellungen veyon/Master/ComputerMonitoringUpdateInterval und veyon/Core/ComputerStatePollingInterval steuern den Intervall, in dem der **UCS@school Veyon Proxy** neue Screenshots und Statusupdates von Zielrechnern abfragt und ist in Millisekunden angegeben. Hierbei beträgt der maximal Wert 10000 msec, der Standardwert beträgt 1000 msec. Das Minimum beider Werte bestimmt wie oft der **UCS@school Veyon Proxy** einen neuen Screenshot erzeugt. Durch erhöhen der Werte kann die Prozessor- und Netzwerklast, des Systems, reduziert werden.

Die Einstellung veyon/WebAPI/ConnectionIdleTimeout definiert die Zeit in Sekunden, nach der eine inaktive VNC-Verbindung zwischen dem **UCS@school Veyon Proxy** und einem Windows-Client geschlossen wird. Wir empfehlen 60 Sekunden, der Wert sollte jedoch immer höher sein als die folgenden Computerraum Modul Einstellungen, um zu Vermeiden das Verbindungen neu auf gebaut werden.

6.4.5 Performance-Optimierungen des Computerraum Moduls

Auch das Computerraum Modul bietet einige Einstellungen zur Performance-Optimierung. Dabei zielen alle Einstellungen darauf, den **UCS@school Veyon Proxy** zu entlasten, indem die Anzahl von Anfragen an den Proxy reduziert werden.

Die Einstellungen steuern die Verbindung zwischen Univention Management Console und dem **UCS@school Veyon Proxy**. Statusupdates und Screenshots werden vom **UCS@school Veyon Proxy** zwischen gespeichert. Die folgenden UCR-Variablen steuern wie oft dieser Zwischenspeicher (Cache) abgefragt wird.

- ucsschool/umc/computerroom/update-interval
- ucsschool/umc/computerroom/screenshot/interval

Die Einstellung ucsschool/umc/computerroom/update-interval steuert das Intervall in Sekunden, mit dem der Computerraum Informationen zum eingeloggten Benutzer, sowie dem Sperrzustand von Monitor und Eingabegeräten, an der App, abfragt. Die Standardeinstellung beträgt 1 Sekunde.

Die Einstellung ucsschool/umc/computerroom/screenshot/interval steuert das Intervall in Sekunden, mit dem der Computerraum einen Screenshot des Computers abfragt. Der Standardwert beträgt 5 Sekunden. Der Inhalt des Screenshots ändert sich nur, wenn die App einen neuen Screenshot zwischenspeichert.

Quellcode 6.2: Computerraum Einstellungen werden als UCR-Variablen gesetzt. Die UMC muss manuell neu gestartet und die UMC im Browser muss neu geladen werden, damit die Einstellungen greifen.

```
ucr set ucsschool/umc/computerroom/update-interval=1
service univention-management-console-server restart
```

6.4.6 Veyon Installation auf Windows-Clients von Lehrern

Dieser Abschnitt beschreibt die Installation von *Veyon* auf Lehrer-PCs. Wenn Sie nur die UCS@school Web-Oberfläche verwenden, können Sie diesen Abschnitt überspringen.

Sie können die *Veyon* Binärpakete direkt über die Samba-Freigabe *Veyon-Installation* abrufen und installieren. Die Installationsdatei der 64-Bit Version von *Veyon* finden Sie auf dem Schulserver im Verzeichnis `/usr/share/ucs-school-veyon-windows/`.

Univention hat Interoperabilitätstests zwischen UCS@school und *Veyon* mit der von UCS@school mitgelieferten *Veyon* Version unter Windows 7 und Windows 10 (64 Bit) durchgeführt.

Veyon bringt ein Installationsprogramm mit, das durch alle notwendigen Schritte führt. Während der Installation müssen Sie alle aufgelisteten Komponenten installieren.

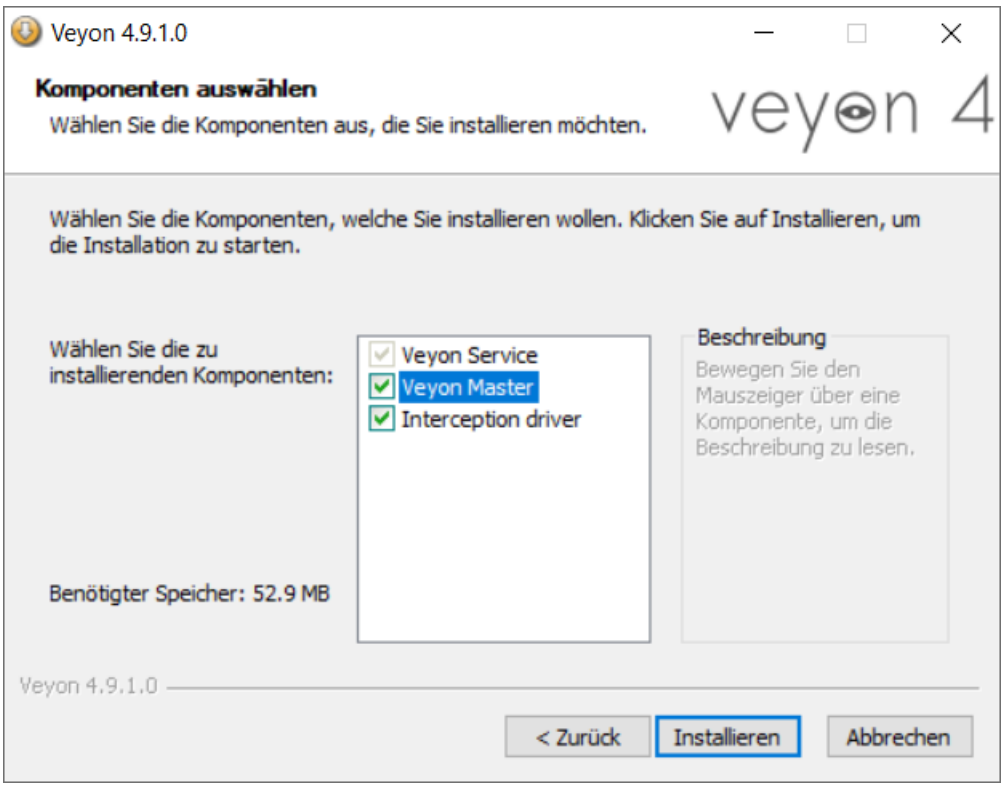

Abb. 6.4: *Veyon* Installation: Auswahl der Komponenten

Für eine erfolgreiche Authentifizierung zwischen Lehrer- und Schüler-PCs zur Überwachung und Steuerung wählen Sie entweder die *Anmeldeauthentifizierung* oder die *Schlüsselauthentifizierung* im Abschnitt *Allgemein* des *Veyon Configurator*, sowohl auf den Lehrer- als auch auf den Schüler-PCs. Weitere Details finden Sie unter Authentifizierung[20] im Veyon-Administrationshandbuch.

Tipp: Bei einer Migration von der UCS@school Web-Oberfläche hin zum **`Veyon Master`** können Sie die bestehenden Schlüssel wiederverwenden. Kopieren Sie den privaten Schlüssel `/etc/ucsschool-veyon/key.pem` von dem Schulserver auf den Lehrer-Computer und importieren Sie diesen mit dem *Veyon Configurator*. Eine Änderung der Schüler-PCs ist damit nicht notwendig.

---

[20] https://docs.veyon.io/de/latest/admin/configuration.html#confauthentication

6.4.7 Einrichten des `Veyon Master`

Alternativ zur Kontrolle von Computern über die Computerraum-Weboberfläche von UCS@school können Sie **`Veyon Master`** direkt verwenden. Gehen Sie durch die nachfolgenden Konfigurationsschritte, um **`Veyon Master`** auf mehreren Computern einzurichten.

Tipp: Es gibt Integrationstests für *Veyon*, die Sie nach Abschluss aller Konfigurationsschritte im Veyon Configurator durchführen können. Die Tests müssen erfolgreich sein. Die Tests finden Sie auf der letzten Seite der *LDAP-Basic* Einstellungen.

Bemerkung: Zu allen Bildern der grafischen Benutzerschnittstelle des Veyon Configurator enthält dieses Kapitel ergänzend Programmblöcke in PowerShell, die auf die Veyon CLI zurückgreifen. Sie können die Programmblöcke z.B. als Bausteine zur Automatisierung verwenden.

Erstellen eines Veyon Benutzers

Erstellen Sie ein einfaches Authentisierungskonto[21] auf dem Primary Directory Node mit dem UMC-Modul *Benutzer*. *Veyon* verwendet das Authentisierungskonto für die LDAP-Verbindung. Quellcode 6.3 zeigt die Erstellung des Kontos auf der Kommandozeile.

Quellcode 6.3: Einrichten eines einfachen Authentisierungskonto mit UDM.

```
VEYON_PASSWORD="veyon-user-account-password"  # Passen Sie dieses Passwort an!
SCHOOL_NAME="school1"

udm users/ldap create --position "cn=users,ou="$SCHOOL_NAME",$(ucr get ldap/base)"␣
↪\
   --set username="veyon-$SCHOOL_NAME" \
   --set lastname="veyon-$SCHOOL_NAME" \
   --set password="$VEYON_PASSWORD"
```

LDAP-Basiseinstellungen

Als nächstes müssen Sie die Einstellungen für die Authentisierung setzen. Hierfür können Sie sowohl den *Veyon Configurator* als auch die `veyon-cli` Kommandozeilen-Schnittstelle verwenden. Beide Werkzeuge wurden in den vorangegangenen Schritten mit *Veyon* auf den Windows-Clients installiert. Viele der Einstellungen in diesem Abschnitt hängen von der Umgebung ab und müssen angepasst werden. Die Kommentare am Ende einer Zeile mit `veyon-cli config set ...` verweisen auf die Kennzeichnung in der grafischen Benutzeroberfläche des *Veyon Configurator*.

Vor der Ausführung der Befehle in Quellcode 6.4 müssen Sie das öffentliche Zertifikat der Zertifizierungsstelle der UCS Domäne auf den lokalen Rechner kopieren. Das Wurzelzertifikat können Sie über die Univention Management Console herunterladen. Setzen Sie anschließend die Variable `$CA_CERTIFICATE_PATH` auf den Wert, der dem Pfad des Zertifikats entspricht. Wenn Sie die grafische Benutzeroberfläche zur Konfiguration verwenden, muss der Dateipfad manuell eingetragen werden, da bei der interaktiven Dateiauswahl nur PEM-Dateien angezeigt werden.

Quellcode 6.4: Setzen der LDAP-Basiseinstellungen über die Veyon Kommandozeilen-Schnittstelle

```
# Diese Variablen müssen auf das Zielsystem angepasst werden:
$LDAP_BASE = 'dc=univention,dc=de'
$SCHOOL_FQDN = 'school1.univention.de'
$VEYON_USER = "uid=veyon-school1,cn=users,ou=school1,$LDAP_BASE"
```

(Fortsetzung auf der nächsten Seite)

[21] https://docs.software-univention.de/manual/5.0/de/user-management/index.html#users-general

(Fortsetzung der vorherigen Seite)

```
$VEYON_PASSWORD = 'veyon-user-account-password'  # Passen Sie dieses Passwort an!
$CA_CERTIFICATE_PATH = 'path-to-tls-ldap-certificate'

cd 'C:\Program Files\Veyon\'

.\veyon-cli config set LDAP/ServerHost "$SCHOOL_FQDN"  # LDAP-Server
.\veyon-cli config set LDAP/ServerPort 7389  # LDAP-Port
.\veyon-cli config set LDAP/BindPassword $VEYON_PASSWORD # Bind-Passwort
.\veyon-cli config set LDAP/BindDN "$VEYON_USER"  # Bind-DN

.\veyon-cli config set LDAP/ConnectionSecurity 1  # Verschlüsselungsprotokoll (1 =␣
↪TLS)
.\veyon-cli config set LDAP/TLSVerifyMode 2  # TLS-Zertifikatsüberprüfung
.\veyon-cli config set LDAP/TLSCACertificateFile "$CA_CERTIFICATE_PATH"  #␣
↪Benutzerdefinierte CA-Zertifikatsdatei
.\veyon-cli config set LDAP/UseBindCredentials true  # Bind-Zugangsdaten verwenden

.\veyon-cli config set LDAP/BaseDN "$LDAP_BASE"  # Fester Base-DN
.\veyon-cli config set NetworkObjectDirectory/Plugin '{6f0a491e-c1c6-4338-8244-
↪f823b0bf8670}'  # Backend (Setzt das Netzwerkobjektverzeichnis zu "LDAP Basic ...
↪")
```

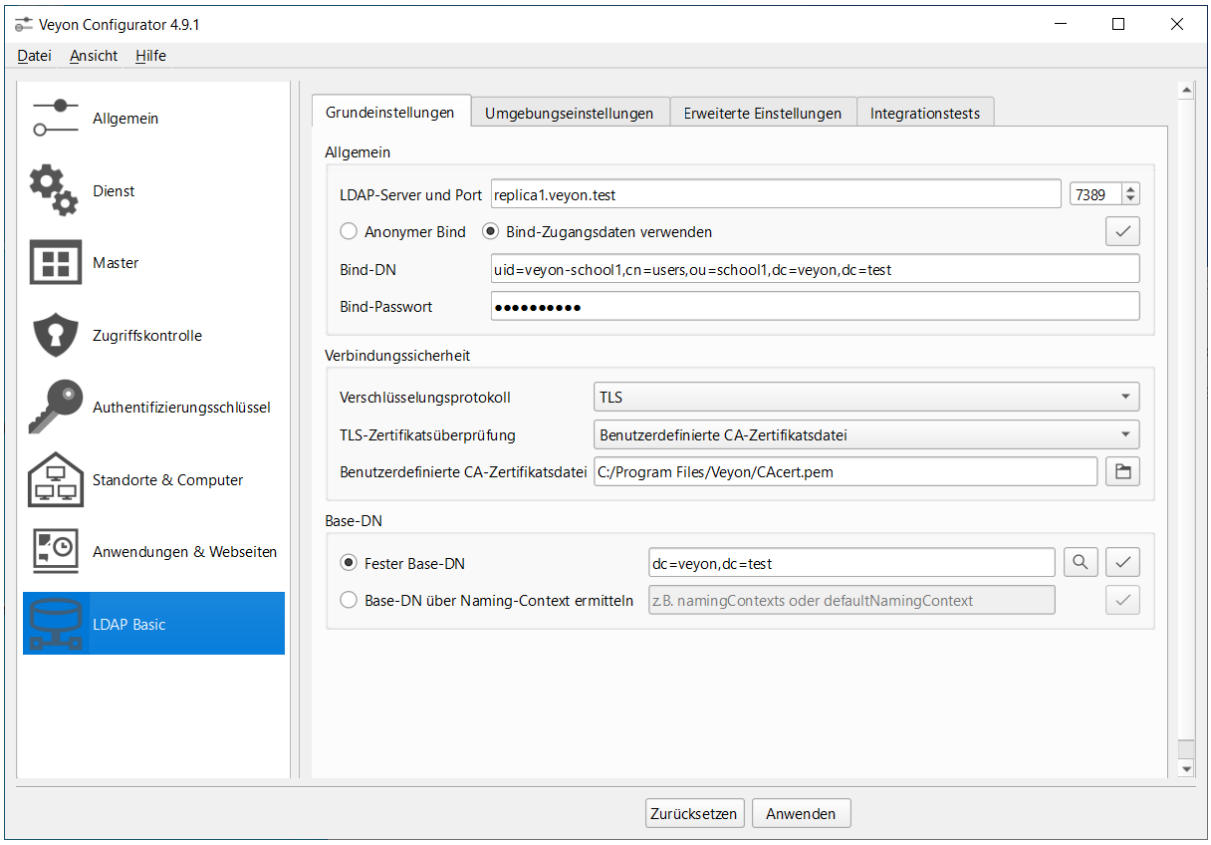

Abb. 6.5: **Veyon Master** Konfiguration: Beispiel für LDAP Grundeinstellungen

LDAP-Umgebungseinstellungen

Die folgenden Einstellungen sind so gewählt, dass Standorte im **Veyon Master** den Computerräumen von UCS@school entsprechen.

Quellcode 6.5: Setzen der LDAP-Umgebungseinstellungen über die Veyon Kommandozeilen-Schnittstelle

```
cd 'C:\Program Files\Veyon\'

.\veyon-cli config set LDAP/RecursiveSearchOperations true  # Rekursive␣
↪Suchoperationen in Objektbäumen durchführen
.\veyon-cli config set LDAP/UserLoginNameAttribute uid  # Attribut␣
↪Benutzeranmeldename
.\veyon-cli config set LDAP/GroupMemberAttribute uniqueMember  # Attribut␣
↪Gruppenmitglied
.\veyon-cli config set LDAP/ComputerDisplayNameAttribute displayName  # Attribut␣
↪Computeranzeigename
.\veyon-cli config set LDAP/ComputerHostNameAttribute cn  # Attribut␣
↪Computerhostname
.\veyon-cli config set LDAP/ComputerHostNameAsFQDN false  # Hostnamen sind als␣
↪vollqualifizierte Domainnamen gespeichert
.\veyon-cli config set LDAP/ComputerMacAddressAttribute macAddress  # macAddress
.\veyon-cli config set LDAP/LocationNameAttribute cn  # Attribute Standortname
```

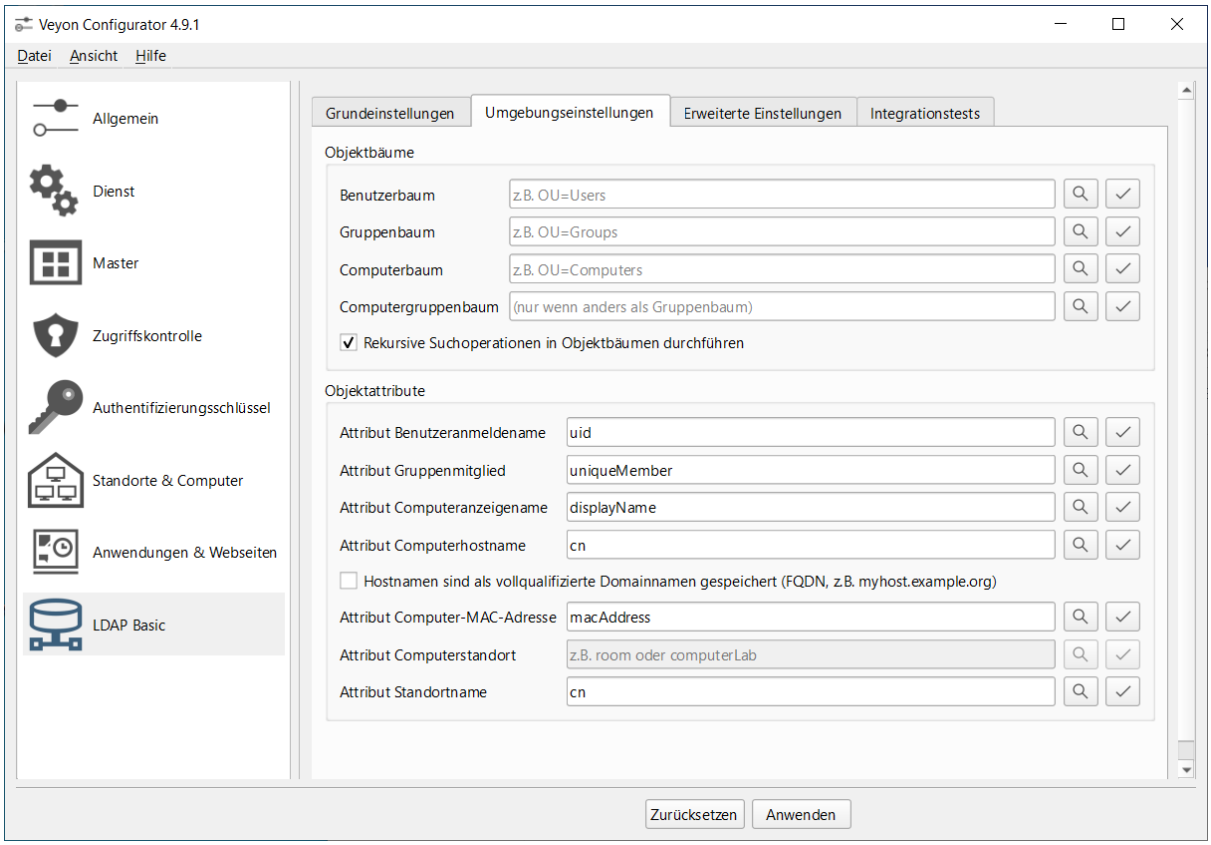

Abb. 6.6: **Veyon Master** Konfiguration: LDAP Umgebungseinstellungen

Erweiterte Einstellungen

Dieser Abschnitt zeigt, wie Sie die erweiterten LDAP Einstellungen setzen müssen, um relevante Benutzer, Gruppen und Computer zu identifizieren. Die folgenden Einstellungen sind so gewählt, dass Standorte im **Veyon Master** den Computerräumen von UCS@school entsprechen:

Quellcode 6.6: Setzen der erweiterten LDAP-Einstellungen über die Veyon Kommandozeilen-Schnittstelle

```
cd 'C:\Program Files\Veyon\'

.\veyon-cli config set LDAP/UsersFilter
↪'(|(ucsschoolRole=student*)(ucsschoolRole=teacher*))' # Filter für Benutzer
.\veyon-cli config set LDAP/UserGroupsFilter '(objectClass=ucsschoolGroup)'  #␣
↪Filter für Benutzergruppen
.\veyon-cli config set LDAP/ComputersFilter '(objectClass=ucsschoolComputer)'  #␣
↪Filter für Computer
.\veyon-cli config set LDAP/QueryNestedUserGroups false  # Verschachtelte␣
↪Benutzergruppen abfragen
.\veyon-cli config set LDAP/IdentifyGroupMembersByNameAttribute false  #␣
↪Identifizierung von Gruppenmitgliedern
.\veyon-cli config set LDAP/ComputerGroupsFilter '(&(ucsschoolRole=computer_
↪room:school:*)(!(cn=*all-windows-hosts*)))' # Filter für Computergruppen
.\veyon-cli config set LDAP/ComputerLocationsByContainer false  #␣
↪Computercontainer oder OUs
.\veyon-cli config set LDAP/ComputerLocationsByAttribute false  # Attribut␣
↪Standort in Computerobjekten
```

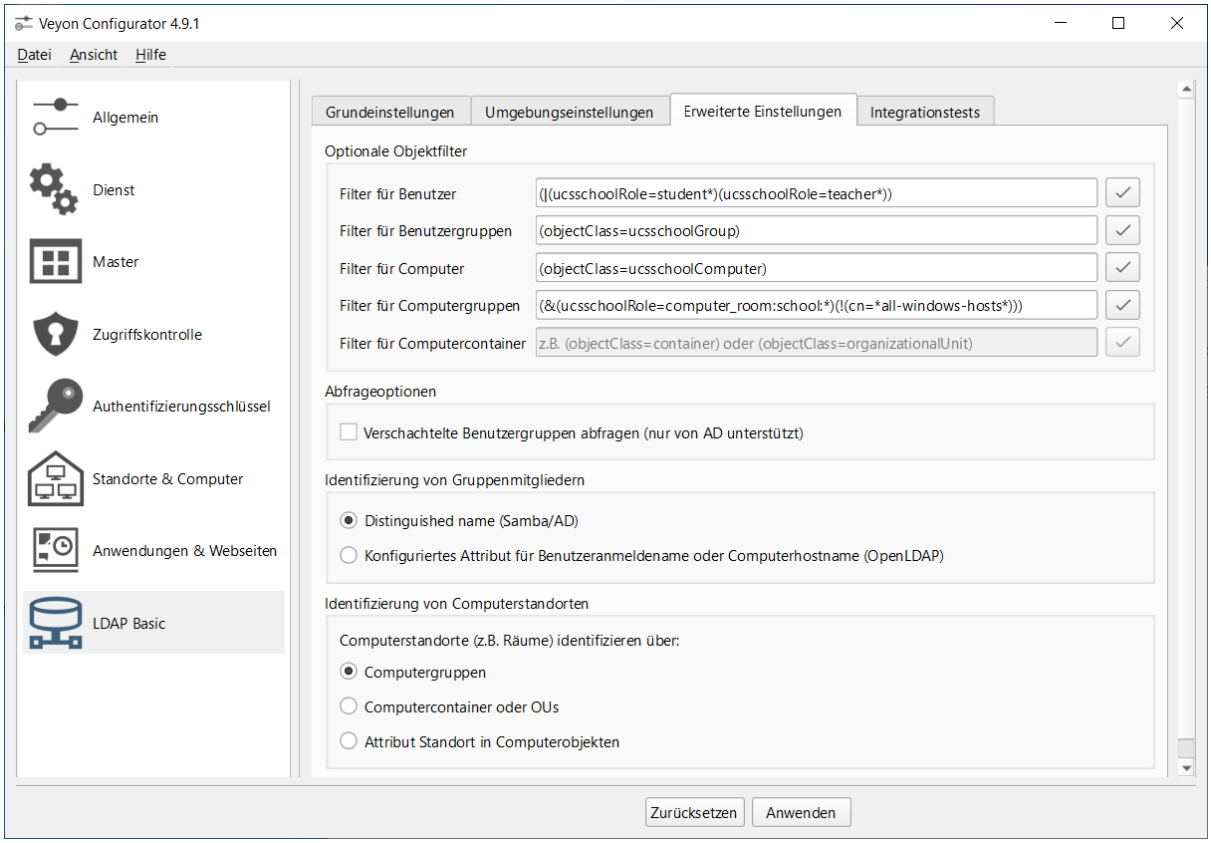

Abb. 6.7: **Veyon Master** Konfiguration: LDAP Erweiterte Einstellungen

Verhaltenseinstellungen des `Veyon Master`

Dieser Abschnitt zeigt optionale empfohlene Einstellungen. In Umgebungen mit vielen Computerräumen kann es sinnvoll sein, nur den Standort bzw. Computerraum anzuzeigen, in welchem sich auch der aktuell genutzte Computer befindet. Bei Umgebungen mit vielen Computerräumen kann es sonst unübersichtlich werden. Die Einstellung `HideLocalComputer` verbirgt den eigenen Computer in der Darstellung.

Quellcode 6.7: Setzen der **`Veyon Master`** Verhaltens-Einstellungen über die Veyon Kommandozeilen-Schnittstelle

```
cd 'C:\Program Files\Veyon\'

.\veyon-cli config set Master/ShowCurrentLocationOnly true  # Nur aktuellen␣
↪Standort anzeigen
.\veyon-cli config set Master/HideLocalComputer true  # Lokalen Computer ausblenden
```

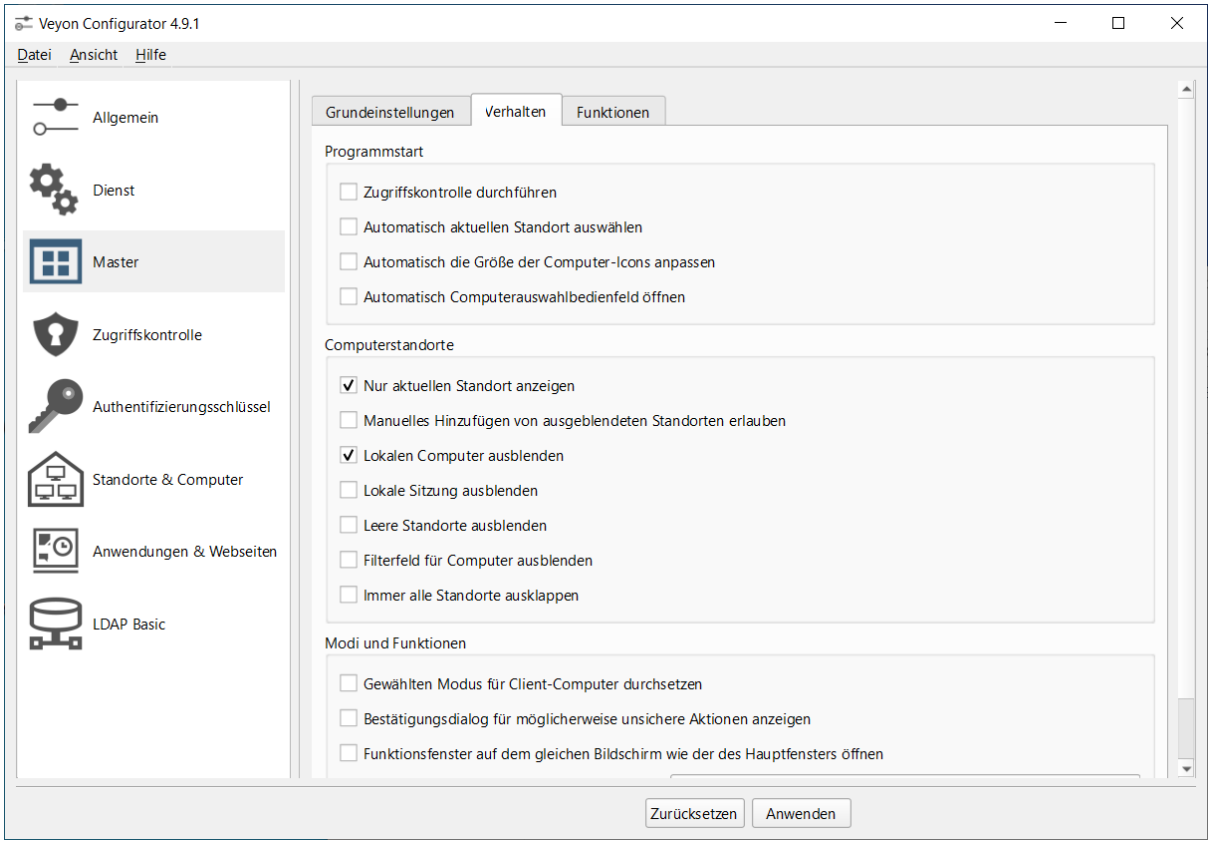

Abb. 6.8: **`Veyon Master`** Konfiguration: Verhalten des **`Veyon Master`**

KAPITEL 7

Übersicht über die schulspezifischen Anwendungen

7.1 Modulübersicht

UCS@school stellt eine Reihe von Modulen für die Univention Management Console bereit, die für den IT-gestützten Unterricht verwendet werden können.

Im folgenden werden die Module kurz beschrieben. Eine ausführliche Beschreibung der Verwendung der Module findet sich in *UCS@school - Handbuch für Lehrkräfte und Schuladministratoren* [1].

Einige Module stehen Lehrern und Schuladministratoren zur Verfügung während andere Module nur Schuladministratoren vorbehalten sind:

Passwörter (Schüler)
Passwörter (Schüler) erlaubt Lehrern das Zurücksetzen von Schüler-Passwörtern.

Passwörter (Lehrer)
Passwörter (Lehrer) erlaubt Schuladministratoren das Zurücksetzen von Lehrer-Passwörtern.

Passwörter (Mitarbeiter)
Passwörter (Mitarbeiter) erlaubt Schuladministratoren das Zurücksetzen von Mitarbeiter-Passwörtern.

Computerraum
Das Modul *Computerraum* erlaubt die Kontrolle der Schüler-PCs und des Internetzugangs während einer Unterrichtsstunde. Der Internetzugang kann gesperrt oder freigegeben werden und einzelne Internetseiten können gezielt freigegeben werden.

Wenn eine entsprechende Software (*Veyon*) auf den Schüler-PCs installiert ist, besteht auch die Möglichkeit diese PCs zu steuern. So kann beispielsweise der Bildschirm gesperrt werden, so dass in einer Chemie-Stunde die ungeteilte Aufmerksamkeit auf ein Experiment gelenkt werden kann.

Außerdem kann der Bildschirminhalt eines PCs auf andere Systeme übertragen werden. Dies erlaubt es Lehrern, auch ohne einen Beamer Präsentationen durchzuführen.

Helpdesk kontaktieren
Jede Schule wird durch einen Helpdesk betreut. Der Helpdesk kann z.B. durch eine Support-Organisation beim Schulträger oder durch technisch versierte Lehrer an den Schulen umgesetzt werden. Über das Modul *Helpdesk kontaktieren* können Lehrer und Schuladministratoren eine E-Mailanfrage stellen. Die Konfiguration des Helpdesk-Moduls wird in *Konfiguration der Helpdesk-Kontaktadresse* (Seite 41) beschrieben.

Arbeitsgruppen verwalten
Jeder Schüler ist Mitglied seiner Klasse. Darüber hinaus gibt es die Möglichkeit mit dem Modul *Arbeitsgruppen*

verwalten Schüler und Lehrer in klassenübergreifende Arbeitsgruppen einzuordnen.

Das Anlegen einer Arbeitsgruppe legt automatisch einen Datenbereich auf dem Schulserver (Dateifreigabe) an, auf den alle Mitglieder der Arbeitsgruppe Zugriff erhalten. Der Name der Dateifreigabe ist identisch mit dem gewählten Namen der Arbeitsgruppe.

Das Anlegen, Bearbeiten und Löschen von Arbeitsgruppen ist in der Standardkonfiguration sowohl den Lehrern als auch den Schuladministratoren erlaubt.

Drucker moderieren
Mit dem Modul *Drucker moderieren* können Ausdrucke der Schüler geprüft werden. Die anstehenden Druckaufträge können vom Lehrer betrachtet und entweder verworfen oder zum Drucken freigegeben werden. Dadurch können unnötige oder fehlerhafte Ausdrucke vermieden werden.

Materialien verteilen
Das Modul *Materialien verteilen* vereinfacht das Verteilen und Einsammeln von Unterrichtsmaterial an Klassen oder Arbeitsgruppen.

Optional kann eine Frist zum Verteilen und Einsammeln festgelegt werden. So ist es möglich, Aufgaben zu verteilen, die bis zum Ende der Unterrichtsstunde zu bearbeiten sind. Nach Ablauf der Frist werden die verteilten Materialien dann automatisch wieder eingesammelt und im Heimatverzeichnis des Lehrers abgelegt.

Computerräume verwalten
Mit dem Modul *Computerräume verwalten* werden Computer einer Schule einem Computerraum zugeordnet. Diese Computerräume können von den Lehrern zentral verwaltet werden, etwa indem der Internetzugang freigegeben wird.

Unterrichtszeiten
Das Modul *Unterrichtszeiten* erlaubt es, die Zeiträume der jeweiligen Unterrichtsstunden pro Schule zu definieren.

Lehrer Klassen zuordnen
Für jede Klasse gibt es einen gemeinsamen Datenbereich. Damit Lehrer auf diesen Datenbereich zugreifen können, müssen sie mit dem Modul *Lehrer Klassen zuordnen* der Klasse zugewiesen werden.

Internetregeln definieren
Für die Filterung des Internetzugriffs wird ein Proxy-Server eingesetzt, der bei dem Abruf einer Internetseite prüft, ob der Zugriff auf diese Seite erlaubt ist. Ist das nicht der Fall, wird eine Informationsseite angezeigt. Dies wird in *Web-Proxy auf den Schulservern* (Seite 63) weitergehend beschrieben.

Wenn Schüler beispielsweise in einer Schulstunde in der Wikipedia recherchieren sollen, kann eine Regelliste definiert werden, die Zugriffe auf alle anderen Internetseiten unterbindet. Diese Regelliste kann dann vom Lehrer zugewiesen werden.

Mit dem Modul *Internetregeln definieren* können die Regeln verwaltet werden.

7.2 Passwörter zurücksetzen

Mit den Modulen *Passwörter (Schüler)*, *Passwörter (Lehrer)* und *Passwörter (Mitarbeiter)* lassen sich Benutzerpasswörter zurücksetzen. Die Benutzeroberfläche der Module ist identisch. Es werden alle Schüler/Lehrer/Mitarbeiter der gewählten *Schule* angezeigt. Durch Auswahl einer *Klasse oder Arbeitsgruppe* und/oder Nutzung der Suchleiste lässt sich die Menge der angezeigten Nutzer weiter eingrenzen.

Durch Auswahl eines oder mehrerer Nutzer und Anklicken von *PASSWORT ZURÜCKSETZEN*, kann ein neues Passwort für die jeweiligen Nutzer festgelegt werden.

Aus Sicherheitsgründen ist es vor dem Zurücksetzen des Passwortes erforderlich, dass der aktuell eingeloggte Nutzer sein Passwort erneut eingeben muss.

Die bestehenden Schüler-Passwörter können außerdem nicht ausgelesen werden. Wenn Schüler ihr Passwort vergessen, muss ein neues Passwort vergeben werden. Schuladministratoren dürfen die Passwörter von Lehrern und Mitarbeitern zurücksetzen.

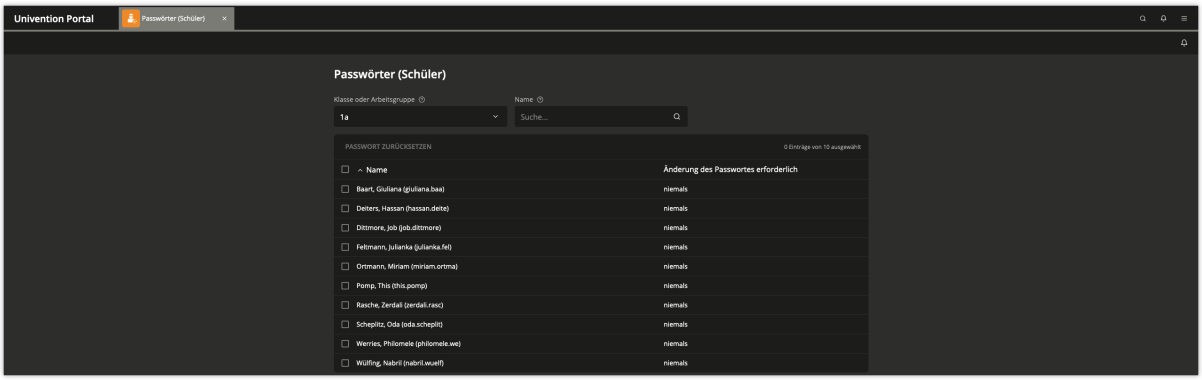

Abb. 7.1: Zurücksetzen von Schülerpasswörtern

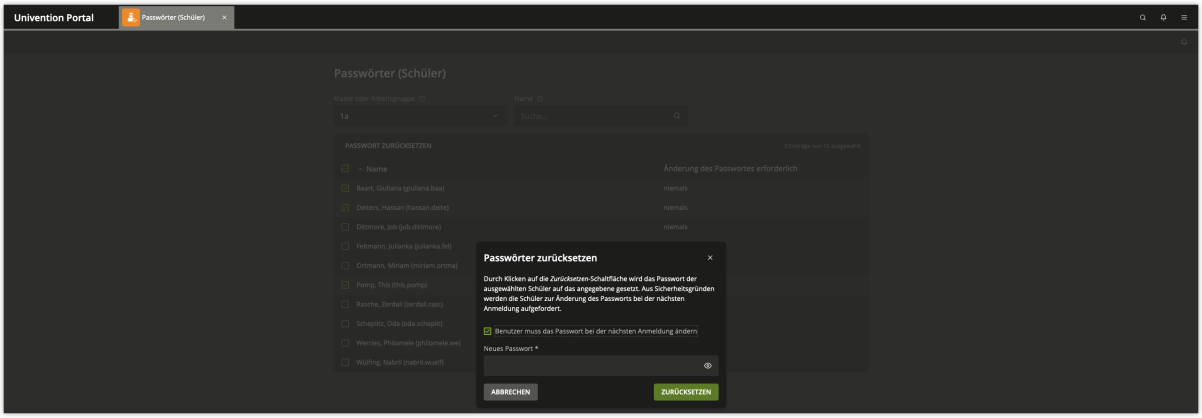

Abb. 7.2: Festlegen eines neuen Passworts

Neben dem Namen und Nutzernamen der angezeigten Nutzer wird außerdem gezeigt, bei wem eine Änderung des Passwortes bei der nächsten Anmeldung erforderlich ist. Die Passwortänderung ist dann erforderlich, wenn beim Zurücksetzen eines Passworts die Checkbox *Benutzer muss das Passwort bei der nächsten Anmeldung ändern* angewählt wurde. Das Verhalten dieser Checkbox lässt sich durch folgende UCR-Variablen ändern:

ucsschool/passwordreset/password-change-on-next-login

Wenn mit `true` eingeschaltet, wird der Wert der Checkbox standardmäßig eingeschaltet.

ucsschool/passwordreset/force-password-change-on-next-login

Wenn mit `true` eingeschaltet, wird das Ändern des Wertes in der Checkbox verhindert.

KAPITEL 8

Web-Proxy auf den Schulservern

In der Grundeinstellung läuft auf jedem Schulserver (bzw. im Single-Server-Betrieb auf dem Primary Directory Node) ein Proxy-Server auf Basis von *Squid* im Zusammenspiel mit *squidGuard*. Der Proxy erlaubt Lehrern in Unterrichtsstunden und im Klassenarbeitsmodus den Zugriff auf einzelne Webseiten zu beschränken oder auch generell bestimmte Webseiten zu sperren. Dies ist in *UCS@school - Handbuch für Lehrkräfte und Schuladministratoren* [1] beschrieben.

Der Proxyserver muss zwingend auf dem jeweiligen Schulserver betrieben werden.

8.1 Einrichtung

Die Proxykonfiguration wird in der Grundeinstellung durch DHCP über die WPAD-Option verteilt. Siehe WAPD auf Wikipedia[22].

Soll die WPAD-Option abgeschaltet werden, so muss die Option an dem betreffenden DHCP-Service-Objekt entfernt werden. Dies kann entweder im UMC-Modul *DHCP* am betreffenden DHCP-Service-Objekt auf dem Reiter *Erweiterte Einstellungen* unter *Low-level DHCP configuration* oder an der Kommandozeile geschehen.

Das DHCP-Service-Objekt trägt in der Standardkonfiguration den Namen des Schulkürzels und sollte daher in der UMC leicht identifizierbar sein. Um die richtige DN und Option auf der Kommandozeile zu finden, können zuerst alle DHCP-Service-Objekte aufgelistet werden. Die nachfolgenden Befehle sollten als Benutzer root auf dem Primary Directory Node ausgeführt werden:

```
$ udm dhcp/service list
```

So können in der folgenden Zeile *DN* und *FQDN* durch konkrete Werte ersetzt werden:

```
$ udm dhcp/service modify \
  --dn DN \
  --remove option='wpad "http://FQDN/proxy.pac"'
```

Beispiel:

```
root@primary:~# udm dhcp/service list

DN: cn=school123,cn=dhcp,ou=school123,dc=example,dc=com
```

(Fortsetzung auf der nächsten Seite)

[22] https://de.wikipedia.org/wiki/Web_Proxy_Autodiscovery_Protocol

(Fortsetzung der vorherigen Seite)

```
  option: wpad "http://replica123.example.com/proxy.pac"
  service: school123

DN: cn=example.com,cn=dhcp,dc=example,dc=com
  service: example.com

root@primary:~# udm dhcp/service modify --dn cn=school123,cn=dhcp,ou=school123,
↪dc=example,dc=com \
> --remove option='wpad "http://replica123.example.com/proxy.pac"'
Object modified: cn=school123,cn=dhcp,ou=school123,dc=example,dc=com
root@primary:~#
```

Auf dem UCS-System, auf dem der betroffene DHCP-Server läuft (in Single-Server-Umgebungen ist dies der Primary Directory Node in Multi-Server-Umgebungen i.d.R. ein konkreter Schulserver), muss anschießend eine UCR-Variable entfernt und der DHCP-Server neu gestartet werden:

```
$ ucr unset dhcpd/options/wpad/252
$ systemctl restart univention-dhcp
```

Um Domains, IP-Adressen, Netzwerke oder URLs von der Verwendung des Proxies auszunehmen, können die UCR-Variablen `proxy/pac/exclude/*` gesetzt werden. Eine Liste der möglichen Einstellungen samt Erklärungen wird angezeigt mit:

```
$ ucr search --verbose ^proxy/pac/exclude/
```

Die Verteilung der Proxykonfiguration mittels DHCP-WPAD-Option wird jedoch nicht von allen Browsern unterstützt. Die Konfiguration kann alternativ über eine Proxy-Autokonfigurationsdatei (PAC-Datei) automatisiert werden. In PAC-Dateien sind die relevanten Konfigurationsparameter zusammengestellt. Die PAC-Datei eines Schulservers steht unter der folgenden URL bereit:

`http://schulserver.domaene.de/proxy.pac`

Im Internet Explorer wird die PAC-Datei beispielsweise unter *Internetoptionen* ‣ *Reiter Verbindungen* ‣ *LAN-Einstellungen* ‣ *Automatisches Konfigurationsskript verwendet* zugewiesen.

In Firefox kann die PAC-Datei im Menü unter *Allgemein* ‣ *Einstellungen* ‣ *Verbindungs-Einstellungen* ‣ *Automatische Proxy-Konfigurations-URL* zugewiesen werden.

Bei Einsatz von Samba 4 kann die Proxy-Konfiguration alternativ auch über Gruppenrichtlinien zugewiesen werden.

Bei der PAC- und der WPAD-Datei handelt es sich um die gleiche Datei (`/var/www/proxy.pac`). Es können daher die gleichen UCR-Variablen verwendet werden um Domains, IP-Adressen, Netzwerke oder URLs von der Verwendung des Proxies auszunehmen (`proxy/pac/exclude/*`).

8.2 Einbindung von externen Blacklisten

Der Proxy von UCS@school unterstützt (ab UCS@school 4.0 R2 und mindestens UCS 4.0 Erratum 163) die Einbindung von externen Blacklisten, welche als Textdateien vorliegen müssen.

Die Textdateien dürfen jeweils nur Domänennamen oder URLs enthalten. Pro Zeile darf nur ein Eintrag (Domänenname/URL) enthalten sein. Die Textdateien müssen unterhalb des Verzeichnisses `/var/lib/ucs-school-webproxy/` abgelegt werden. Die Verwendung von weiteren Unterverzeichnissen ist möglich.

Eingebunden werden die Blacklisten über das Setzen von folgenden UCR-Variablen:

- `proxy/filter/global/blacklists/domains`
- `proxy/filter/global/blacklists/urls`.

Diese Variablen enthalten die Dateinamen der Domänen-Blacklisten bzw. URL-Blacklisten. Die Dateinamen sind relativ zum Verzeichnis `/var/lib/ucs-school-webproxy` anzugeben und müssen durch Leerzeichen voneinander getrennt werden.

Die Einbindung der folgenden, exemplarischen Blacklist-Dateien

```
/var/lib/ucs-school-webproxy/extblacklist1/domains
/var/lib/ucs-school-webproxy/extblacklist1/urls
/var/lib/ucs-school-webproxy/bl2/list-domains
/var/lib/ucs-school-webproxy/bl2/list-urls
/var/lib/ucs-school-webproxy/bl3-dom
/var/lib/ucs-school-webproxy/bl3-urls
```

kann über die nachfolgenden **ucr set**-Befehle erreicht werden:

```
$ ucr set proxy/filter/global/blacklists/domains=\
    "extblacklist1/domains bl2/list-domains bl3-dom"
$ ucr set proxy/filter/global/blacklists/urls=\
    "extblacklist1/urls bl2/list-urls bl3-urls"
```

Die Blacklisten werden vom Proxy in der Standardeinstellung mit niedriger Priorität ausgewertet, d.h. (temporäre) Whitelisten von Schuladministratoren und Lehrern haben Vorrang. Um die globalen Blacklisten vorrangig auszuwerten, kann die UCR-Variable `proxy/filter/global/blacklists/forced` auf den Wert `yes` gesetzt werden. Die Blacklisten können anschließend nicht mehr durch Schuladministratoren oder Lehrer in der UMC umgangen bzw. zeitweilig deaktiviert werden.

Vorsicht: Es ist zu beachten, dass bei einer Aktualisierung der Blacklist-Textdateien die internen Filterdatenbanken des Proxys nicht ebenfalls automatisch aktualisiert werden. Um dies zu erreichen, müssen die beiden UCR-Variablen erneut gesetzt werden.

Bemerkung: Abhängig von der Anzahl der Einträge in den eingebundenen Blacklisten, kann die Aktualisierung der internen Filterdatenbanken beim Setzen der UCR-Variablen mehrere Sekunden benötigen.

KAPITEL 9

Authentifizierung des WLAN-Zugriffs über RADIUS

RADIUS ist ein Authentifizierungsprotokoll in Computernetzen. Es wird in UCS@school für die Authentifizierung von Rechnern für den Wireless-LAN-Zugriff eingesetzt.

Der RADIUS-Server muss auf den *Access Points* entsprechend konfiguriert werden. Die vom Client übertragenen Benutzerkennungen werden dann durch den festgelegten RADIUS-Server geprüft, der wiederum für die Authentifizierung auf den UCS-Verzeichnisdienst zugreift.

9.1 Installation und Konfiguration des RADIUS-Servers

Um RADIUS-Unterstützung einzurichten, muss das Paket **ucs-school-radius-802.1x** auf dem Schulserver der Schule installiert werden, in der WLAN-Authentifizierung eingerichtet werden soll. Außerdem muss das Paket **ucs-school-webproxy** auf dem Schulserver installiert sein.

Beginnend mit UCS@school 4.4 wird während der Installation des Pakets **ucs-school-radius-802.1x** auch automatisch die App **RADIUS** mit seinen zusätzlichen Features installiert. Der entsprechende Abschnitt RADIUS[23] in *Univention Corporate Server - Handbuch für Benutzer und Administratoren* [2] ist daher auch zu prüfen.

Nun müssen alle *Access Points* der Schule in der RADIUS-Konfiguration zusammen mit einem Passwort hinterlegt werden, um einen Vertrauenskontext zwischen Access Point und RADIUS-Server zu schaffen. Dies kann ab UCS 4.4 entweder in der Univention Management Console erfolgen, sofern für jeden Access Point ein Rechnerobjekt im LDAP-Verzeichnis hinterlegt wird, oder in der Konfigurationsdatei `/etc/freeradius/3.0/clients.conf`.

Pro *Access Point* sollte ein zufälliges Passwort erstellt werden. Dies kann z.B. mit dem Befehl **makepasswd** geschehen. Die Kurzbezeichnung ist frei wählbar. Ein Beispiel für einen solchen Eintrag:

```
client AP01 {
    secret = a9RPAeVG
    ipaddr = 192.168.100.101
}
```

[23] https://docs.software-univention.de/manual/5.0/de/ip-config/radius.html#ip-config-radius

9.2 Konfiguration der *Access Points*

Nun müssen die *Access Points* konfiguriert werden. Die dafür nötigen Schritte unterscheiden sich je nach Hardwaremodell, prinzipiell müssen die folgenden vier Optionen konfiguriert werden:

- Der Authentifizierungmodus muss auf RADIUS-Authentifzierung umgestellt werden. Diese Option wird oft auch als *WPA Enterprise* bezeichnet.
- Die IP-Adresse des Schulservers muss als RADIUS-Server angegeben werden.
- Der Radius-Port ist `1812`, sofern kein abweichender Port in *FreeRADIUS* konfiguriert wurde.
- Das in der UMC bzw. in der Datei `/etc/freeradius/3.0/clients.conf` hinterlegte Passwort.

9.3 Konfiguration der zugreifenden Clients

Der zugreifende Client muss zunächst das UCS-Wurzelzertifikat importieren. Es kann z.B. von der Startseite des Primary Directory Node unter dem Link *Wurzelzertifikat* bezogen werden. Anschließend muss er eine Netzwerkverbindung mit den folgenden Parametern konfigurieren:

- Authentifizierung per WPA und TKIP als Verschlüsselungsverfahren
- `PEAP` und `MSCHAPv2` als Authentifizierungsprotokoll

Die Konfiguration unterscheidet sich je nach Betriebssystem des Clients. Eine exemplarische Schritt-für-Schritt-Anleitung findet sich unter Univention Help 21827 - „Einrichtung des WLAN-Zugriffs über RADIUS für Windows 10“[24].

9.4 Freigabe des WLAN-Zugriffs in der Univention Management Console

In der Grundeinstellung ist der WLAN-Zugriff nicht zugelassen. Um einzelnen Benutzergruppen WLAN-Zugriff zu gestatten, muss in der Univention Management Console im Modul *Internetregeln definieren* eine Regel hinzugefügt - oder eine bestehende editiert werden, in der die Option *WLAN-Authentifizierung aktiviert* aktiviert ist.

Weiterführende Dokumentation zur Freigabe des WLAN-Zugriffs finden sich in *UCS@school - Handbuch für Lehrkräfte und Schuladministratoren* [1].

9.5 Fehlersuche

Im Fehlerfall sollte die Logdatei `/var/log/freeradius/radius.log` geprüft werden:

- Erfolgreiche Logins führen zu einem Logeintrag `Auth: Login OK`.
- Fehlgeschlagene Authentifizierung führt beispielsweise zu `Auth: Login incorrect`.

Weitere Informationen zur Fehlersuche sind in *Univention Corporate Server - Handbuch für Benutzer und Administratoren* [2], im Abschnitt RADIUS[25], beschrieben.

[24] https://help.univention.com/t/21827
[25] https://docs.software-univention.de/manual/5.0/de/ip-config/radius.html#ip-config-radius

KAPITEL 10

Klassenarbeitsmodus

Der Klassenarbeitsmodus ermöglicht die gezielte Einschränkung der Computernutzung für Schüler einer Klasse. Über das UMC-Modul für den Klassenarbeitsmodus kann ein Lehrer einen Klassenraum für die exklusive Nutzung durch bestimmte Gruppen konfigurieren. Der Klassenarbeitsmodus bietet darüber hinaus auch einen direkten Zugriff auf die Funktionalitäten der Materialverteilung.

Hintergründe zur technischen Umsetzung werden in *Technische Hintergründe* (Seite 69) und mögliche Konfigurationsschnittstellen in *Konfiguration* (Seite 70) genannt.

Für die Dauer des Klassenarbeitsmodus werden die ausgewählten Schüler und Räume in eine speziell benannte Gruppe aufgenommen. Dies macht es möglich mit Hilfe von Windows-Gruppenrichtlinien spezifische Einschränkungen für die Benutzung von Windows-Rechnern im gewählten Raum zu definieren, wie z.B. die Vorgabe eines Proxy-Servers zur Filterung des Internetzugriffs, die Einschränkung den Zugriffs auf USB-Speicher und andere Wechselmedien oder auch die Sperrung bestimmter Programme. Einsatzmöglichkeiten für Gruppenrichtlinien werden in *Beispiele für Gruppenrichtlinien* (Seite 72) beispielhaft beschrieben.

10.1 Technische Hintergründe

Zur Verwendung des Klassenarbeitsmodus sind folgende Voraussetzungen zu erfüllen:

- Verwendung einer Samba 4-Domäne (AD-Domäne)
- Einsatz von Windows XP oder höher auf den Prüfungscomputern
- Import von Computerkonten und Zuordnung der Computer zu Computerräumen
- Die Verwendung des UCS@school-HTTP-Proxys durch die Prüfungscomputer zur Filterung des Internetzugriffs

Eine neue Klassenarbeit kann über das Modul *Klassenarbeit starten* begonnen werden. Beim Durchlaufen der einzelnen Schritte werden von der Lehrkraft ein Name für die Klassenarbeit und die teilnehmenden Klassen/Arbeitsgruppen ausgewählt. Zusätzlich können für die Arbeit notwendige Dateien hochgeladen sowie Computerraumeinstellungen ausgewählt werden.

Damit Schülern nicht die Möglichkeit gegeben wird, auf ihr bisheriges Heimatverzeichnis zuzugreifen, werden zum Zeitpunkt des Einrichtens der Klassenarbeit für die ausgewählten Schülerkonten spezielle Klassenarbeitskonten neu angelegt.

Der Anmeldename für das Klassenarbeitskonto setzt sich aus einem festgelegten Präfix (standardmäßig `exam-`) und dem normalen Benutzernamen zusammen. Beispielsweise wird für den Benutzer `anton123` das Klassenarbeitskonto `exam-anton123` angelegt, mit dem er sich während der Klassenarbeit anmelden muss.

Für das Klassenarbeitskonto wird ein neues Heimatverzeichnis erzeugt, Passwörter und andere Konteneinstellungen werden jedoch aus dem ursprünglichen Benutzerkonto direkt übernommen. Schüler können die Zugriffsberechtigungen ihrer Heimatverzeichnisse nicht verändern. Dadurch wird verhindert, dass ein Schüler sein Heimatverzeichnis für weitere Schüler freigegeben kann.

Um Schülern den Zugriff auf andere Dienste (z.B. Mail oder Cloud) während einer Klassenarbeit zu verwehren, kann die UCR-Variable `ucsschool/exam/user/disable` (Seite 71) aktiviert werden (siehe *Konfiguration* (Seite 70)).

Für deaktivierte Nutzerkonten wird kein Klassenarbeitskonto angelegt. Diese werden beim Hinzufügen zur Klassenarbeit ignoriert. Soll ein Schüler an einer Klassenarbeit teilnehmen, muss dessen Nutzerkonto aktiviert sein. Wie Benutzer aktiviert/deaktiviert werden können, wird in *Univention Corporate Server - Handbuch für Benutzer und Administratoren* [2] im Abschnitt Modul Benutzerverwaltung - Reiter Konto[26] beschrieben.

Nutzerkonten, die aufgrund der UCR-Variable `ucsschool/exam/user/disable` (Seite 71) bei einer laufenden Klassenarbeit deaktiviert wurden, werden erkannt und nicht ignoriert.

Alle Klassenarbeitskonten der Schüler sowie alle Rechner des Computerraumes sind für den Zeitraum der Klassenarbeit Mitglieder der Gruppe `OU`*`OU-Name`*`-Klassenarbeit`. Durch diese Gruppe können spezifische Einschränkungen für Schüler und Rechner mit Hilfe von Windows-Gruppenrichtlinien vorgenommen werden (siehe *Beispiele für Gruppenrichtlinien* (Seite 72)).

Bemerkung: Damit die Einstellungen der Gruppenrichtlinien für die Rechner entsprechend greifen, ist es wichtig, dass die Schülerrechner des Computerraumes nach dem Einrichten einer Klassenarbeit neu gestartet werden. Dieser Vorgang wird durch das UMC-Modul *Klassenarbeit starten* unterstützt, indem alle eingeschalteten Rechner automatisch neu gestartet werden können.

Zusätzlich ist es aus dem selben Grund wichtig, dass nach Beenden einer Klassenarbeit die Schülerrechner entweder ausgeschaltet oder neu gestartet werden. Nur so können die ursprünglichen Einstellungen der Gruppenrichtlinien wieder wirksam werden.

Damit leicht erkannt werden kann, dass die Gruppenrichtlinien für den Klassenarbeitsmodus an den Rechnern wirksam sind, weisen Sie zum Beispiel ein optisch klar zu unterscheidendes Hintergrundbild über die Richtlinien zu.

10.2 Konfiguration

Für die Konfiguration des Klassenarbeitsmodus gibt es eine Reihe von Univention Configuration Registry Variablen. Diese werden im folgenden aufgelistet und kurz erläutert.

Die nachfolgenden Univention Configuration Registry Variablen können geändert werden, um LDAP-Eigenschaften der Klassenarbeitskonten, -gruppen und -container anzupassen. Sofern diese Variablen manuell gesetzt werden, ist zu beachten, dass es sich dabei um globale Einstellungen handelt und diese Variablen sowohl auf dem Primary Directory Node als auch auf den Schulservern identische Werte aufweisen müssen.

`ucsschool/ldap/default/userprefix/exam`

Gibt den Präfix an, der dem ursprünglichen Benutzernamen im Klassenarbeitskonto vorangestellt wird. Er ist standardmäßig auf `exam-` gesetzt.

`ucsschool/ldap/default/groupname/exam``

Bezeichnet die Gruppe, der alle Klassenarbeitskonten sowie Klassenarbeitsrechner zugeordnet sind. Über diese Gruppe können spezifische Windows-Gruppenrichtlinien für den Klassenarbeitsmodus gesetzt werden. Der Standardname für diese Gruppe ist `OU%(ou)s-Klassenarbeit`, wobei `%(ou)s` vom System automatisch durch den Namen der OU ausgetauscht wird.

[26] https://docs.software-univention.de/manual/5.0/de/user-management/umc.html#users-management-table-account

ucsschool/ldap/default/container/exam

Definiert den Namen des Containers, unterhalb dem die Klassenarbeitskonten gespeichert werden. Standardmäßig ist der Name auf `examusers` gesetzt. Die LDAP-Position des Containers ist direkt unterhalb der Schul-OU.

ucsschool/exam/user/homedir/autoremove

Definiert, ob beim automatischen Löschen der Prüfungsbenutzer auch deren Heimatverzeichnis gelöscht werden soll. Der Standard ist `no`.

ucsschool/exam/user/disable

Definiert, ob der originale Benutzer während einer Klassenarbeit deaktiviert werden soll, um die Nutzung anderer Dienste zu verhindern. Der Standard ist `no`.

Es empfiehlt sich, das Verhalten nach der Deaktivierung eines Benutzers in allen installierten Apps vorher zu überprüfen.

Das UMC-Modul zum Einrichten einer Klassenarbeit bietet die Möglichkeit bestimmte Standardwerte zu definieren, um das Starten einer Klassenarbeit zu vereinfachen. Dazu gehören:

ucsschool/exam/default/room

Definiert den vorausgewählten Raum für eine neue Klassenarbeit. Der Eintrag beinhaltet den LDAP-Namen des Raumes (inklusive des Schul-OU-Präfxies), also bspw. `meineschule-PC Raum`. Ist die Variable nicht gesetzt, wird kein Raum vorausgewählt.

ucsschool/exam/default/shares

Gibt den vorausgewählten Freigabezugriff für eine neue Klassenarbeit an. Mögliche Werte sind:

- `all`: Zugriff auf alle Freigaben ohne Einschränkungen
- `home`: Eingeschränkten Zugriff auf lediglich das Heimatverzeichnis des (Klassenarbeits-)Benutzerkontos

Ist die Variable nicht gesetzt, wird standardmäßig nur der Zugriff auf das Homeverzeichnis freigegeben.

ucsschool/exam/default/internet

Definiert die vorausgewählte Internetregel für eine neue Klassenarbeit. Mögliche Werte umfassen die Namen aller Internetregeln wie sie im UMC-Modul *Internetregeln definieren* angezeigt werden.

Normalerweise werden die globalen Standardeinstellungen verwendet.

ucsschool/exam/default/checkbox/distribution

Definiert, ob beim Starten des Klassenarbeitsmodus das Auswahlkästchen *Unterrichtsmaterial verteilen* automatisch vorausgewählt ist. Mögliche Werte sind:

- `true`: Auswahlkästchen vorausgewählt
- `false`: Auswahlkästchen nicht vorausgewählt

ucsschool/exam/default/checkbox/proxysettings

Definiert, ob beim Starten des Klassenarbeitsmodus das Auswahlkästchen *Internetregeln definieren* automatisch vorausgewählt ist. Mögliche Werte sind:

- `true`: Auswahlkästchen vorausgewählt
- `false`: Auswahlkästchen nicht vorausgewählt

ucsschool/exam/default/checkbox/sharesettings

Definiert, ob beim Starten des Klassenarbeitsmodus das Auswahlkästchen *Freigabezugriff konfigurieren* automatisch vorausgewählt ist. Mögliche Werte sind:

- `true`: Auswahlkästchen vorausgewählt
- `false`: Auswahlkästchen nicht vorausgewählt

ucsschool/exam/default/show/restart

Definiert, ob die Seite zum Neustarten der Schülerrechner angezeigt werden soll. Standardmäßig deaktiviert.

Mit UCS@school 4.4v3 gibt es die Möglichkeit in regelmäßigen Abständen Sicherungskopien aller Schülerdaten zu speichern, während sie sich in einer Klassenarbeit befinden. Diese Sicherungskopien werden in einem separaten Ordner im Heimatverzeichnis des Lehrers gespeichert, welcher die Klassenarbeit durchführt. Diese Funktionalität ist in dieser Version standardmäßig deaktiviert und kann über die folgenden Univention Configuration Registry Variablen konfiguriert werden:

ucsschool/exam/cron/backup/activated

Definiert, ob das Skript **exam-backup** automatisch durch Cron gestartet wird. Standardmäßig deaktiviert.

ucsschool/exam/cron/backup

Definiert den Zeitpunkt, an dem das Skript **exam-backup** automatisch durch Cron gestartet wird. Standardmäßig alle 5 Minuten; Beispiel: `*/5 * * * *`)

ucsschool/exam/backup/compress

Definiert, ob das Backup der Daten eines Schülers während einer Klassenarbeit komprimiert werden soll. Standardmäßig aktiviert.

ucsschool/exam/backup/limit

Definiert die maximale Anzahl an Zwischenergebnissen, die pro Schüler und Klassenarbeit gespeichert werden. Der Standardwert ist `40` und muss mindestens `1` sein. Wenn das Limit erreicht ist, werden keine weiteren Backups gespeichert.

Vorsicht: Wenn diese Funktionalität aktiviert wird, sollte dabei dringend der Bedarf an Speicherplatz berücksichtigt werden, der hier anfällt.

Sollte beispielsweise eine Klasse von 25 Schülern eine 45 Minuten dauernde Klassenarbeit schreiben und es werden dabei alle 5 Minuten ungefähr 10 MB pro Schülerin oder Schüler gesichert, so fallen dabei ungefähr 2,2 GB an Daten an.

10.3 Beispiele für Gruppenrichtlinien

Gruppenrichtlinien werden von einem Windows System aus mit Hilfe der Gruppenrichtlinienverwaltung (GPMC) angelegt und bearbeitet. Im Folgenden ist die Konfiguration der Gruppenrichtlinien von einem Windows 7 System aus beschrieben auf dem dazu die Gruppenrichtlinienverwaltung (GPMC) aus den *Remote System Administration Tools (RSAT)* installiert sein muss.

Alle Gruppenrichtlinieneinstellungen können je nach Bedarf gesammelt über ein Gruppenrichtlinienobjekt vorgenommen oder auf separate Objekte verteilt werden. Um den Bezug zwischen einem ausgewählten Gruppenrichtlinienobjekt und Objekten im Samba-Verzeichnisdienst herzustellen, kann es mit einer Organisationseinheit (OU) verknüpft werden, z.B. der Schul-OU. Einige der hier beispielhaft beschriebenen Gruppenrichtlinieneinstellungen wirken sich nur auf Benutzer- und andere nur auf Computerkonten aus.

Da die Einstellungen eines Gruppenrichtlinienobjekts nur für Objekte ausgewertet werden, die unterhalb des speziellen Verzeichniszweigs liegen, mit dem es verknüpft wurde, ist es wichtig, dass das entsprechende Gruppenrichtlinienobjekt hinreichend hoch in der hierarchischen Objektordnung verknüpft wird.

Einige der genannten Gruppenrichtlinien-Einstellungen beziehen sich auf den Bereich der Computerkonfiguration und werden nur beim Systemstart korrekt von den entsprechenden Windows-Komponenten ausgewertet. Für solche Einstellungen ist daher ein Neustart der Windows-Arbeitsplatzsysteme nach Aktivierung des Klassenarbeitsmodus notwendig.

Bemerkung: Zu diesem Thema ist auch ein Hinweis von Microsoft zu Windows XP Systemen zu beachten:

Jede Version von Windows XP Professional stellt eine Funktion zur Optimierung für schnelles Anmelden zur Verfügung.

Computer mit diesen Betriebssystemen warten standardmäßig beim Starten nicht auf den Start des Netzwerks. Nach der Anmeldung werden die Richtlinien im Hintergrund verarbeitet, sobald das Netzwerk zur Verfügung steht.

> Dies bedeutet, dass der Computer bei der Anmeldung und beim Start weiterhin die älteren Richtlinieneinstellungen verwendet. Daher sind für Einstellungen, die nur beim Start oder bei der Anmeldung angewendet werden können (z. B. Softwareinstallation und Ordnerumleitung), möglicherweise nach dem Ausführen der ersten Änderung am Gruppenrichtlinienobjekt mehrere Anmeldungen durch den Benutzer erforderlich.
>
> Diese Richtlinie wird gesteuert durch die Einstellung in `Computerkonfiguration\Administrative Vorlagen\System\Anmeldung\Beim Neustart des Computers und bei der Anmeldung immer auf das Netzwerk warten`.
>
> Diese Funktion ist in den Betriebssystemversionen von Windows 2000 oder Windows Server 2003 nicht verfügbar."
>
> ---Quelle: *Group Policy processing and precedence* [5]

10.3.1 Generelle Hinweise zu Gruppenrichtlinien und Administrativen Vorlagen

Auf dem Schulserver sollte das Verzeichnis `/var/lib/samba/sysvol/`*`DomänenNameDerUCS@schoolUmgebung`*`/Policies/PolicyDefinitions/` angelegt werden. Sobald dieses Verzeichnis angelegt ist, bevorzugt das Windows-Programm zur Gruppenrichtlinienverwaltung die dort hinterlegten Administrativen Vorlagen im ADMX-Format vor den lokal auf dem Windows 7 System installierten Administrativen Vorlagen.

Da in den nachfolgenden Abschnitten zusätzliche Administrative Vorlagen verwendet werden, die ebenfalls in dem oben genannten Verzeichnis abzulegen sind, wird empfohlen, nach dem Erstellen des Verzeichnisses einmalig die lokal installierten Administrativen Vorlagen aus dem Verzeichnis `C:\Windows\PolicyDefinitions` in das neue Verzeichnis zu kopieren. Da das Verzeichnis serverseitig unterhalb der `SYSVOL`-Freigabe liegt, wird es per Voreinstellung auf alle Samba 4 Server der Domäne synchronisiert.

Die Administrativen Vorlagen sind an sich keine Gruppenrichtlinien, sie dienen nur zur Erweiterung der Einstellungsmöglichkeiten die das Windows Programm zur Gruppenrichtlinienverwaltung dem Administrator zur Auswahl anbietet. Für neuere Windows-Versionen, wie z.B. Windows 8, stellt Microsoft aktualisierte Administrative Vorlagen zum Download zur Verfügung.

Grundsätzlich können Gruppenrichtlinien im Samba Verzeichnisdienst mit Organisationseinheiten (OU) und der LDAP-Basis verknüpft werden. Im UCS@school-Kontext werden jedoch nur Verknüpfungen unterhalb der Schul-OU auch automatisch in das OpenLDAP-Verzeichnis synchronisiert. Verknüpfungen mit der LDAP-Basis werden z.B. durch OpenLDAP-Zugriffsbeschränkungen blockiert, damit sich eine Anpassung der damit verknüpften Gruppenrichtlinien durch einen Schul-Administrator nicht auch auf alle anderen Schulen auswirkt.

Eine solche Änderung wird im S4 Connector auf der Schule als *Reject* notiert. Wenn tatsächlich gewünscht ist, eine Änderung der Gruppenrichtlinienverknüpfung an der LDAP-Basis und unter `OU=Domain Controllers` auch in das OpenLDAP-Verzeichnis und damit an alle Schulen zu synchronisieren, kann auf dem Schulserver folgender Befehl mit dem zentralen Administrator-Passwort ausgeführt werden:

```
$ eval "$(ucr shell)"
$ /usr/share/univention-s4-connector/msgpo.py \
  --write2ucs \
  --binddn "uid=Administrator,cn=users,$ldap_base" \
  --bindpwd <password>
```

Der S4 Connector erkennt eine kurze Zeit später bei dem nächsten *Resync*, dass der *Reject* aufgelöst wurde.

10.3.2 Windows-Anmeldung im Prüfungsraum auf Mitglieder der Klassenarbeitsgruppe beschränken

Neu in Version 4.4v4: Mit UCS@school 4.4v4 werden die Windows-Anmeldungen während einer Klassenarbeit automatisch von UCS@school verwaltet.

Dabei werden über das Nutzerattribut `sambaUserWorkstations` alle Schülerkonten der Klassenarbeitsgruppe auf die Rechner des Computerraumes beschränkt. Zusätzlich wird verhindert, dass sich der originale Nutzer an einem Windowsrechner anmelden kann. Dieser Mechanismus kommt ohne die hier beschriebene Einrichtung von Windows Gruppenrichtlinien aus und erfordert daher keinen Neustart der Rechner.

Sollten keine weiteren Gruppenrichtlinien eingerichtet worden sein, müssen die Rechner vor oder nach einer Klassenarbeit überhaupt nicht mehr neugestartet werden. In diesem Fall kann die Aufforderung der Lehrer zum Neustart der Rechner während der Einrichtung von Klassenarbeiten über die Univention Configuration Registry Variable *ucsschool/exam/default/show/restart* (Seite 71) abgeschaltet werden.

Da das im folgenden konfigurierte Gruppenrichtlinienobjekt je nach Verknüpfung im Samba-Verzeichnisdienst die Anmeldung an betroffenen Windows-Arbeitsplatzsystemen einschränkt, wird dringend empfohlen, als erstes die Anwendung der neuen Gruppenrichtlinie auf solche Windows-Arbeitsplatzsysteme einzuschränken, auf die sie sich später im Klassenarbeitsmodus auswirken soll. Dies geschieht am einfachsten über die Anpassung der Sicherheitsfilterung, die im Folgenden beschrieben ist.

Damit die Gruppenrichtlinieneinstellungen von Windows-Arbeitsplatzrechnern ausgewertet werden, ist es notwendig, einen Bezug zwischen dem angelegten Gruppenrichtlinienobjekt und den Rechnerobjekten im Samba-Verzeichnisdienst herzustellen. Um dies zu erreichen, kann das Gruppenrichtlinienobjekt mit einer Organisationseinheit (OU) verknüpft werden, die den Rechnerobjekten im Verzeichnisbaum übergeordnet ist, in der Regel mit der Schul-OU.

Anwendungsbereich der GPO auf Klassenarbeitscomputer einschränken

1. In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
2. In der Baumdarstellung der Gruppenrichtlinienverwaltung die Gruppenrichtlinie anklicken.
3. Auf dem geöffneten Reiter *Bereich* im Abschnitt *Sicherheitsfilterung* die Schaltfläche *Hinzufügen* betätigen.
4. In das Eingabefeld *Geben Sie die zu verwendenden Objektnamen ein* den Namen der Klassenarbeitsgruppe (`OU`*`NameDerOU`*`-Klassenarbeit`, z.B. `OUgym17-Klassenarbeit`) eintragen und den Dialog mit *OK* schließen.
5. Auf dem geöffneten Reiter *Bereich* im Abschnitt *Sicherheitsfilterung* die Gruppe `Authenticated Users` auswählen und die Schaltfläche *Entfernen* betätigen.

Einschränkung der Windows-Anmeldung auf Klassenarbeitsbenutzerkonten und Lehrer

1. In der Gruppenrichtlinienverwaltung das Gruppenrichtlinienobjekt zur Bearbeitung öffnen (Kontextmenü des GPO in der Baumdarstellung).
2. Im neu geöffneten Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen: *Computerkonfiguration ▸ Richtlinien ▸ Windows-Einstellungen ▸ Sicherheitseinstellungen ▸ Lokale Richtlinien ▸ Zuweisen von Benutzerrechten*
3. Im neu geöffneten Richtlinien-Dialog *Eigenschaften von Lokal anmelden zulassen* auf dem Reiter *Sicherheitsrichtlinie* die Option *Diese Richtlinieneinstellung definieren* aktivieren.
4. Dann die Schaltfläche *Benutzer oder Gruppe hinzufügen* betätigen.
5. In das Eingabefeld *Benutzer und Gruppennamen* den Namen `Administratoren` eintragen und den Dialog mit *OK* schließen.
6. Erneut die Schaltfläche *Benutzer oder Gruppe hinzufügen* betätigen.

7. Im neu geöffneten Dialog die Schaltfläche *Durchsuchen* betätigen.
8. In das Eingabefeld *Geben Sie die zu verwendenden Objektnamen ein* den Namen der Klassenarbeitsgruppe (`OU`*`NameDerOU`*`-Klassenarbeit`, z.B. `OUgym17-Klassenarbeit`) eintragen und den Dialog mit *OK* schließen.
9. Den Dialog *Benutzer oder Gruppe hinzufügen* ebenfalls mit *OK* schließen.
10. Erneut die Schaltfläche *Benutzer oder Gruppe hinzufügen* betätigen.
11. Im neu geöffneten Dialog die Schaltfläche *Durchsuchen* betätigen.
12. In das Eingabefeld *Geben Sie die zu verwendenden Objektnamen ein* den Namen der Lehrergruppe (`lehrer-`*`NameDerOU`*, z.B. `lehrer-gym17`) eintragen und den Dialog mit *OK* schließen.
13. Den Dialog *Benutzer oder Gruppe hinzufügen* ebenfalls mit *OK* schließen.
14. Den Richtlinien-Dialog *Eigenschaften von Lokal anmelden zulassen* mit *OK* schließen.

10.3.3 Zugriff auf USB-Speicher und Wechselmedien einschränken

Zur Einschränkung des Zugriffs auf USB-Speicher und Wechselmedien sind je nach Windowsversion zwei Fälle zu beachten:

- Die Einschränkung der Benutzung bereits installierter Gerätetreiber
- Die Einschränkung der Installation neuer Gerätetreiber

Während für Windows XP beide Einschränkungen notwendig sind, bietet Windows 7 durch erweiterte Richtlinien vereinfachte und erweiterte Kontrollmöglichkeiten. In Mischumgebungen ist eine Kombination der skizzierten Einstellungen zu empfehlen.

Bemerkung: Die Liste der hier erwähnten Einstellungen erhebt nicht den Anspruch auf Vollständigkeit. Es ist notwendig die Einstellungen entsprechend der lokalen Gegebenheiten zu testen. Insbesondere sollte folgende Microsoft-Dokumentation beachtet werden: *Threats and Countermeasures Guide: External Storage Devices* [6].

Zugriff auf USB-Speicher an Windows XP einschränken

Diese Richtlinie wird über eine Administrative Vorlage (ADMX) definiert, die in *Verwenden von Gruppenrichtlinien zum Deaktivieren von USB-, CD-ROM-, Disketten- und LS-120-Treibern* [7] beschrieben ist. Erst nach Einbinden der Administrative Vorlage (ADMX) können folgende Einstellungen getroffen werden. Beispiele für ADMX-Dateien liegen unter `/usr/share/doc/ucs-school-umc-exam/examples/GPO`. Zum Einbinden der ADMX-Dateien müssen diese auf die `SYSVOL`-Freigabe kopiert werden (siehe *Generelle Hinweise zu Gruppenrichtlinien und Administrativen Vorlagen* (Seite 73)).

1. In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
2. Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen: *Computerkonfiguration* ‣ *Richtlinien* ‣ *Administrative Vorlagen* ‣ *Spezielle Einstellungen* ‣ *Treiber einschränken*
3. Richtlinie *USB Sperren* öffnen, *Aktiviert* auswählen und mit *OK* bestätigen.

Bemerkung: Hier stehen auch weitere Gerätetypen zur Auswahl, z.B. CD-ROM-Laufwerke.

Installation neuer Gerätetreiber für USB-Speicher an Windows XP verbieten

Diese Richtlinie definiert eingeschränkte Dateisystemberechtigungen gemäß *Wie kann ich verhindern, dass Benutzer eine Verbindung zu einem USB-Speichergerät herstellen?* [8].

1. In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
2. Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen: *Computerkonfiguration* ‣ *Richtlinien* ‣ *Windows-Einstellungen* ‣ *Sicherheitseinstellungen* ‣ *Dateisystem*
3. Rechtsklick auf *Datei hinzufügen…*
4. Das Verzeichnis `C:\Windows\Inf` ansteuern und dort die Datei `usbstor.inf` auswählen und mit *OK* bestätigen.

   Bemerkung: Gegebenenfalls wird die Dateiendung `.inf` nicht mit angezeigt.

5. In dem neu geöffneten Dialog *Datenbanksicherheit für …* in der oberen Liste *Gruppen- oder Benutzernamen* die Schaltfläche *Hinzufügen* betätigen und den Namen der Klassenarbeitsgruppe hinzufügen,
6. In der darunter angezeigten Liste *Berechtigungen für …* in der Zeile *Vollzugriff*, Spalte *Verweigern* ein Häkchen setzen und mit *OK* bestätigen.
7. Den Dialog *Datenbanksicherheit für …* mit *OK* schließen.
8. Das neue Dialogfenster *Windows-Sicherheit* mit *Ja* bestätigen.
9. Das neue Dialogfenster *Objekt hinzufügen* mit *OK* schließen.

Analog sollten Einstellungen für `%SystemRoot%infusbstor.pnf` und `%SystemRoot%system32driversusbstor.sys` definiert werden.

Zugriff auf USB-Speicher an Windows 7 einschränken

1. In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
2. Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen: *Benutzerkonfiguration* ‣ *Richtlinien* ‣ *Administrative Vorlagen* ‣ *System* ‣ *Wechselmedienzugriff*
3. Z.B. Richtlinie *Wechseldatenträger: Lesezugriff verweigern* öffnen, *Aktiviert* auswählen und mit *OK* bestätigen.

Bemerkung: Weitere Informationen zu diesem Thema liefert z.B. *Controlling the Use of Removable Devices and Media* [9].

Installation neuer Gerätetreiber für USB-Speicher an Windows 7 Clients verbieten

Zusätzliche Einschränkungen zur Installation von Gerätetreibern sind auch unter Windows 7 möglich. Die Einstellungsmöglichkeiten bieten eine größere Kontrolle, setzen aber auch konkrete Erfahrungen mit den im Einzelfall eingesetzten Geräten voraus. Daher ist dieser Abschnitt nur als Einstiegshilfe zu verstehen. Die folgende Einstellung würde die zusätzliche Installation jeglicher Treiber für Wechselgeräte deaktivieren. Es kann hier z.B. dann zusätzlich sinnvoll sein, Administratoren von dieser Einschränkung auszunehmen.

1. In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
2. Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen: *Computerkonfiguration* ‣ *Richtlinien* ‣ *Administrative Vorlagen* ‣ *System* ‣ *Geräteinstallation* ‣ *Einschränkungen bei der Geräteinstallation*

3. Hier kann die Installation von Treibern für bestimmte Geräteklassen, Geräte-IDs oder alle Wechselgeräte eingeschränkt werden.
4. Richtlinie *Installation von Wechselgeräten verhindern* öffnen, *Aktiviert* auswählen und mit *OK* bestätigen.

Die Richtlinie *Administratoren das Außerkraftsetzen der Richtlinien unter … erlauben* erlaubt Mitgliedern der Administratorengruppe die getroffenen Einschränkungen zu umgehen.

Noch stärkere Restriktionen sind möglich, indem man die Ausschlusslogik auf Whitelisting umstellt. Dies kann über die Richtlinie *Installation von Geräten verhindern, die nicht in anderen Richtlinien beschrieben sind* erreicht werden.

Bemerkung: Weitere Informationen zu diesem Thema liefert z.B. *Device Management and Installation Step-by-Step Guide: Controlling Device Driver Installation and Usage with Group Policy* [10].

10.3.4 Vorgabe von Proxy-Einstellungen für den Internetzugriff

Im Folgenden sind Vorgaben für Internet Explorer, Google Chrome und Mozilla Firefox beschrieben. Während Microsoft selbst Administrative Vorlagen mitliefert, sind für Google Chrome und Mozilla Firefox jeweils eigene Administrative Vorlagen notwendig.

Zusätzlich zur Vorgabe einer Proxyeinstellung ist für den Klassenarbeitsmodus eine Sperrung des Benutzerzugriffs auf eben diese Einstellungen sinnvoll. Dazu gibt es zwei unterschiedliche Ansätze:

1. Im Fall des Internet Explorers bietet die Administrative Vorlage die Möglichkeit, das entsprechende Einstellungsfenster zu sperren.
2. Im Fall von Google Chrome und Mozilla Firefox werden hingegen die Proxy-Einstellungen per Gruppenrichtlinie für den Arbeitsplatzrechner vorgegeben, statt für den Benutzer, und sind dadurch z.B. für Schüler nicht mehr veränderbar. Für diese Browser ist es daher wichtig darauf zu achten, die Einstellungen, wo nötig, im Zweig *Computerkonfiguration* des Gruppenrichtlinieneditors statt im Zweig *Benutzerkonfiguration* vorzunehmen.

Proxy-Vorgabe für den Internet Explorer

1. Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen: *Benutzerkonfiguration* ‣ *Richtlinien* ‣ *Windows-Einstellungen* ‣ *Internet Explorer-Wartung* ‣ *Verbindung*
2. Richtlinie *Proxyeinstellungen* öffnen, *Aktiviert* auswählen und bestätigen.
3. Proxyadresse für *HTTP* sowie *Secure* und das entsprechende *Port*-Feld ausfüllen (Wert der Univention Configuration Registry Variable `squid/httpport`[27], Standardwert: `3128`).
4. Ggf. *Für alle Adressen denselben Proxyserver verwenden* aktivieren.

Sperrung der Proxyeinstellung für den Internet Explorer

1. Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen: *Computerkonfiguration* ‣ *Richtlinien* ‣ *Administrative Vorlagen: Vom zentralen Computer abgerufene Richtliniendefinitionen (ADMX-Dateien)* ‣ *Windows-Komponenten* ‣ *Internet Explorer* ‣ *Internetsystemsteuerung*
2. Richtlinie *Verbindungsseite deaktivieren* öffnen und *Aktiviert* auswählen und bestätigen.

[27] https://docs.software-univention.de/manual/5.0/de/appendix/variables.html#envvar-squid-httpport

Proxy-Vorgabe für Google Chrome

Die Administrativen Vorlagen für Google Chrome werden durch das Zip-Archiv `policy_templates.zip` des Chromium-Projekts bereitgestellt. Die entsprechenden Dateien liegen unter `/usr/share/doc/ucs-school-umc-exam/examples/GPO/`. Der Inhalt des `admx` Verzeichnisses sollte in das Verzeichnis `PolicyDefinitions` auf den Schulserver kopiert werden, so dass dort die Datei `chrome.admx` liegt. Die `*.adml` Dateien aus den Unterverzeichnissen müssen in gleichnamige Unterverzeichnisse unter `PolicyDefinitions` kopiert werden.

1. In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
2. Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen: *Computerkonfiguration* ‣ *Richtlinien* ‣ *Administrative Vorlagen: Vom zentralen Computer abgerufene Richtliniendefinitionen (ADMX-Dateien)* ‣ *Google* ‣ *Google Chrome* ‣ *Proxy-Server*
3. Richtlinie *Auswählen, wie Proxy-Server-Einstellungen angegeben werden* öffnen und *Aktiviert* auswählen.
4. Im Dropdown *System-Proxy-Einstellungen verwenden* auswählen und bestätigen.

Proxy-Vorgabe für Mozilla Firefox

Auf dem Schulserver sollte das Verzeichnis `/var/lib/samba/sysvol/DomänenNameDerUCS@schoolUmgebung/Policies/PolicyDefinitions/` angelegt werden. Nähere Informationen sind im Abschnitt zu Google Chrome zu finden.

Die Administrativen Vorlagen für Mozilla Firefox werden durch das FirefoxADM-Projekt bereitgestellt. Es ist sinnvoll, die dort definierten ADM-Vorlagen in das ADMX-Format umzuwandeln.

Beispiele für ADMX Dateien liegen unter `/usr/share/doc/ucs-school-umc-exam/examples/GPO`. Der Inhalt des `admx` Verzeichnisses sollte in das Verzeichnis `PolicyDefinitions` auf den Schulserver kopiert werden, so dass dort die Datei `firefoxlock.admx` liegt. Die `*.adml` Dateien aus den Unterverzeichnissen müssen in gleichnamige Unterverzeichnisse unter `PolicyDefinitions` kopiert werden.

1. In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
2. Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen: *Computerkonfiguration* ‣ *Richtlinien* ‣ *Administrative Vorlagen: Vom zentralen Computer abgerufene Richtliniendefinitionen (ADMX-Dateien)* ‣ *Mozilla Firefox Locked Settings* ‣ *General*
3. Richtlinie *Proxy Settings* öffnen und *Aktiviert* auswählen.
4. Im Dropdown *Preference State* die Einstellung *Locked* auswählen.
5. Im Dropdown *Proxy Setting* die Einstellung *Manual Proxy Configuration* auswählen.
6. Im Feld *Proxy Setting* die Einstellung *Manual Setting - HTTP Proxy* eintragen.
7. Im Feld *HTTP Proxy Port* den Proxy Port eintragen (Wert der Univention Configuration Registry Variable `squid/httpport`[28], Standardwert: `3128`).
8. Den Dialog mit *OK* bestätigen.

Da Mozilla Firefox bisher nicht selbständig die über die Administrativen Vorlagen definierten Einstellungen in der Windows-Registry berücksichtigt, ist es notwendig diese Einstellungen über ein Startup- bzw. Shutdown-Skript in Mozilla-Konfigurationsdateien übersetzen zu lassen. Das FirefoxADM-Projekt stellt diese Skripte in Form von zwei `*.vbs` Dateien zur Verfügung. Deren Einbindung ist über die folgenden Schritt möglich.

1. Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen: *Computerkonfiguration* ‣ *Windows-Einstellungen* ‣ *Skripts (Start/Herunterfahren)*
2. Richtlinie *Starten* öffnen.
3. Im Dialog *Eigenschaften von Starten* auf dem Reiter *Skripts* die Schaltfläche *Dateien anzeigen* betätigen.

[28] https://docs.software-univention.de/manual/5.0/de/appendix/variables.html#envvar-squid-httpport

4. In das vom automatisch geöffneten Windows Explorer angezeigte (leere) Verzeichnis (`MachineScriptsStartup` im betreffenden GPO-Verzeichnis) die Datei `firefox_startup.vbs` kopieren und das Explorer-Fenster schließen.
5. Im Dialog *Eigenschaften von Starten* die Schaltfläche *Hinzufügen* betätigen.
6. Im neu geöffneten Dialog *Hinzufügen eines Skripts* neben dem Feld *Skriptname* den Namen `firefox_startup.vbs` eintragen und Dialog mit *OK* bestätigen.
7. Im Dialog *Eigenschaften von Starten* den Dialog mit *OK* bestätigen.
8. Richtlinie *Herunterfahren* öffnen, und dort analog zu dem Vorgehen bei *Starten* das Skript `firefox_shutdown.vbs` eintragen. Im Detail also:
    1. Im Dialog *Eigenschaften von Herunterfahren* die Schaltfläche *Hinzufügen* betätigen,
    2. In das vom automatisch geöffneten Windows Explorer angezeigte (leere) Verzeichnis (`MachineScriptsShutdown` im betreffenden GPO-Verzeichis) die Datei `firefox_shutdown.vbs` kopieren und das Explorer-Fenster schließen.
    3. Im neu geöffneten Dialog *Hinzufügen eines Skripts* neben dem Feld *Skriptname* den Namen `firefox_shutdown.vbs` eintragen und Dialog mit *OK* bestätigen.
9. Im Dialog *Eigenschaften von Herunterfahren* den Dialog mit *OK* bestätigen.

10.3.5 Zugriff auf bestimmte Programme einschränken

Bemerkung: Die Liste der hier erwähnten Einstellungen erhebt nicht den Anspruch der Vollständigkeit. Es ist notwendig die Einstellungen entsprechend der lokalen Gegebenheiten zu testen. Insbesondere sollten folgende Microsoft-Dokumentationen beachtet werden:

- *Using Software Restriction Policies to Protect Against Unauthorized Software* [11]
- *Administer Software Restriction Policies* [12].

Kommandoeingabeaufforderung deaktivieren

1. In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
2. Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen: *Benutzerkonfiguration* ‣ *Richtlinien* ‣ *Administrative Vorlagen* ‣ *System*
3. Richtlinie *Zugriff auf Eingabeaufforderung verhindern* öffnen und *Aktiviert* auswählen und bestätigen.

Zugriff auf Windows-Registry-Editor deaktivieren

1. In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
2. Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen: *Benutzerkonfiguration* ‣ *Richtlinien* ‣ *Administrative Vorlagen* ‣ *System*
3. Richtlinie *Zugriff auf Programme zum Bearbeiten der Registrierung verhindern* öffnen
4. *Aktiviert* auswählen und den Dialog mit *OK* bestätigen.

Konfiguration von *Software Restriction Policies* (SRP)

Aufgrund der Tiefe des Eingriffs der *Software Restriction Policies* ist zu empfehlen, diese zunächst in einer Testumgebung zu auszuprobieren. Bei der Analyse von Zugriffsfehlern kann die Ereignisanzeige des Windows-Clients helfen.

Die *Software Restriction Policies* greifen auch in die Bearbeitung von Login- und Logoff-Skripten ein. Alle dort verwendeten Programme bzw. Programmpfade sollten auf Ausführbarkeit getestet werden.

Bemerkung: Die Liste der hier erwähnten Einstellungen erhebt nicht den Anspruch der Vollständigkeit. Es ist notwendig die Einstellungen entsprechend der lokalen Gegebenheiten zu testen. Insbesondere sollte folgende Microsoft-Dokumentation beachtet werden:

- *Using Software Restriction Policies to Protect Against Unauthorized Software* [11].
- *Administer Software Restriction Policies* [12].

---

1. In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
2. Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen: *Benutzerkonfiguration* ‣ *Windows-Einstellungen* ‣ *Sicherheitseinstellungen* ‣ *Richtlinien für Softwareeinschränkung*
3. Rechtsklick auf *Neue Richtlinien für Softwareeinschränkung erstellen*.
4. Im rechten Fensterteil *Erzwingen* öffnen.
5. Einstellung *Alle Benutzer außer den lokalen Administratoren* auswählen und mit *OK* bestätigen.
6. Im rechten Fensterteil *Sicherheitsstufen* öffnen.
7. *Nicht erlaubt* per Doppelklick öffnen.
8. *Als Standard* auswählen und mit *OK* bestätigen.
9. Im rechten Fensterteil *Zusätzliche Regeln* öffnen.
10. Rechtsklick auf *Neue Pfadregel…*.
11. In das Eingabefeld *Pfad* den UNC-Pfad `\\%USERDNSDOMAIN%\SysVol` eingeben, damit Logon- und GPO-Skripte ausgeführt werden können.
12. In der Dropdown-Liste *Nicht eingeschränkt* auswählen und mit *OK* bestätigen.

Tab. 10.1: Beispiele für weitere Pfadregeln

Pfad	Sicherheitsstufe
`\\%USERDNSDOMAIN%\SysVol`	Nicht eingeschränkt
`\\%LogonServer%\SysVol`	Nicht eingeschränkt
`\\%LogonServer%\netlogon`	Nicht eingeschränkt
`\\%COMPUTERNAME%\Templates$\*`	Nicht eingeschränkt
`%UserProfile%\LocalSettings\Temp\*.tmp`	Nicht eingeschränkt
`%WinDir%\system32\cscript.exe`	Nicht eingeschränkt
`%WinDir%\system32\wscript.exe`	Nicht eingeschränkt
`%ProgramFiles%`	Nicht eingeschränkt
`%ProgramFiles(x86)%`	Nicht eingeschränkt
`*.lnk`	Nicht eingeschränkt

13. Es kann sinnvoll sein zusätzlich Programm-Pfade als *Nicht erlaubt* einzustufen, z.B.:

Tab. 10.2: Beispiele für weitere Pfadregeln

Pfad	Sicherheitsstufe
`%UserProfile%\LocalSettings\Temp`	Nicht erlaubt
`%SystemRoot%\temp\*`	Nicht erlaubt
`%SystemRoot%\System32\mstsc.exe`	Nicht erlaubt
`%SystemRoot%\System32\dllcache\*`	Nicht erlaubt
`%SystemRoot%\System32\command.com`	Nicht erlaubt
`%SystemRoot%\System32\cmd.exe`	Nicht erlaubt
`%SystemRoot%\repair\*`	Nicht erlaubt
`%SystemDrive%\temp\*`	Nicht erlaubt

14. Es sollte beachtet werden, dass schreibbare Verzeichnisse, auf die der Zugriff nicht per Software Restriction Policy eingeschränkt ist, Benutzern die Möglichkeit geben, Programmdateien dort abzulegen und so die definierten Regeln zu umgehen.

10.3.6 Verwendung temporärer Benutzerprofil-Kopien

Bei der Verwendung von UCS@school werden serverseitige Profile verwendet, die bei der Anmeldung eines Benutzers auf den jeweiligen Windows-Rechner kopiert werden.

In der Standardeinstellung von Windows wird bei der Abmeldung des Benutzers das Profil nicht gelöscht und eine lokale Kopie vorgehalten. Gerade in Verbindung mit dem Klassenarbeitsmodus führt dies zu einer unnötigen Auslastung der lokalen Festplatte.

Über eine Richtlinie kann Windows angewiesen werden, die lokale Profil-Kopie nach der Abmeldung des Benutzers wieder zu verwerfen.

1. In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
2. Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen: *Computerkonfiguration* ‣ *Richtlinien* ‣ *Administrative Vorlagen* ‣ *System* ‣ *Benutzerprofile*
3. Richtlinie *Zwischengespeicherte Kopien von servergespeicherten Profilen löschen* öffnen und *Aktiviert* auswählen und bestätigen.

KAPITEL 11

Python-Hooks

Neu in Version 4.4v9: Ab UCS@school 4.4 v9 kann vor und nach dem Anlegen, Ändern, Verschieben und Löschen von UCS@school Objekten Python-Code ausgeführt werden. Dies kann z.B. im Rahmen des UCS@school Imports von eingesetzt werden, um in Abhängigkeit von der jeweiligen Umgebung weitere Einstellungen vorzunehmen.

Python-Hooks, im folgenden Abschnitt abgekürzt mit *Hooks*, erlauben es Objekttypen zu unterscheiden (z.B. Schulklasse und Arbeitsgruppe oder Schüler und Lehrer) und haben Zugriff auf alle Attribute der Objekte.

Die Hooks werden für alle Klassen, von denen Objekte erzeugt werden können und die von `ucsschool.lib.models.base.UCSSchoolHelperAbstractClass` ableiten, ausgeführt. Diese Klassen finden sich in im Python Paket `ucsschool.lib.models` (z.B. `Student`, `SchoolClass`, `Workgroup`).

Vorsicht: Hooks werden nur auf dem System ausgeführt, auf dem sie installiert sind. In der Regel ist das der Primary Directory Node, sowie alle Backup Directory Node Server. Sollen Hooks auch auf Replica Directory Node Servern ausgeführt werden, so müssen sie auch dort installiert werden. Eine automatische Verteilung der Hook Dateien findet nicht statt.

Hooks für UCS@school Objekte ähneln den bekannten Hooks für den Benutzerimport (siehe *UCS@school - Handbuch zur CLI-Import-Schnittstelle* [4]), werden jedoch auch ohne den Import zu verwenden ausgeführt und haben einige andere Attribute.

Zur Nutzung der Hook-Funktionalität muss eine eigene Python-Klasse erstellt werden, die von *`ucsschool.lib.models.hook.Hook`* (Seite 84) ableitet. In der Klasse können Methoden *`pre_create()`* (Seite 84), *`post_create()`* (Seite 84), etc. definiert werden, welche zum jeweiligen Zeitpunkt ausgeführt werden. Der Name der Datei mit der abgeleiteten Klasse muss auf `.py` enden und im Verzeichnis `/var/lib/ucs-school-lib/hooks` abgespeichert werden.

Zwei Beispiele finden sich auf Servern der Rolle Primary Directory Node in `hook_example1.py` und `hook_example2.py` unter `/usr/share/doc/ucs-school-lib-common/` bzw. online auf https://github.com/…/hook_example1.py[29] und https://github.com/…/hook_example2.py[30].

Im Folgenden wird anhand des Beispiels in `hook_example2.py` erklärt, wie mit Hilfe eines Hooks jeder Schulklasse eine E-Mailadresse zugeordnet werden kann.

[29] https://github.com/univention/ucs-school/blob/5.0/ucs-school-lib/usr/share/doc/ucs-school-lib-common/hook_example1.py
[30] https://github.com/univention/ucs-school/blob/5.0/ucs-school-lib/usr/share/doc/ucs-school-lib-common/hook_example2.py

Warnung: Das Beispiel ist lauffähig, aber nicht für den Produktivbetrieb geeignet. Dafür bräuchte es u.a. zusätzlichen Code, um robust mit existierenden E-Mailadressen umzugehen.

Ein Python-Hook ist eine Klasse, die von *ucsschool.lib.models.hook.Hook* (Seite 84) ableitet und einige Attribute und Methoden definiert.

class MailForSchoolClass

```
from ucsschool.lib.models.group import SchoolClass
from ucsschool.lib.models.hook import Hook

class MailForSchoolClass(Hook):
    model = SchoolClass
    priority = {
        "post_create": 10,
        "post_modify": 10,
    }

    def post_create(self, obj):  # type: (SchoolClass) -> None
        ...

    def post_modify(self, obj):  # type: (SchoolClass) -> None
        ...
```

class ucsschool.lib.models.hook.**Hook**

model

Das Klassenattribut `model` bestimmt, für welche Objekte welchen Typs der Hook ausgeführt wird. Der Hook wird auch für Objekte von Klassen ausgeführt, die von der angegebenen ableiten. Wäre `model = Teacher` (aus `ucsschool.lib.models`), so würde der Hook auch für Objekte der Klasse `TeachersAndStaff` ausgeführt, nicht aber für solche vom Typ `Staff` oder `Student`.

priority

Das Klassenattribut `priority` bestimmt die Reihenfolge in der Methoden von Hooks des gleichen Typs (gleiches *model* (Seite 84)) ausgeführt werden bzw. deaktiviert sie.

Methoden mit höheren Zahlen werden zuerst ausgeführt. Ist der Wert `None` oder die Methode nicht aufgeführt, wird sie deaktiviert.

Angenommen es gäbe eine weitere Klasse mit einem Hook mit `model = SchoolClass` und diese würde `priority = {"post_create": 20}` definieren, so würde deren *post_create()* (Seite 84) Methode **vor** `MailForSchoolClass.post_create()` ausgeführt.

pre_create()

Alle Methoden der Klasse, z.B. *pre_create()* (Seite 84) oder *post_create()* (Seite 84), empfangen ein Objekt vom Typ, bzw. des davon abgeleiteten Typs, der in *model* (Seite 84) definiert wurde, als Argument `obj` und geben nichts zurück.

post_create()

Siehe *pre_create()* (Seite 84)

Die *post_create()* (Seite 84) Methode sieht wie folgt aus:

```
def post_create(self, obj):  # type: (SchoolClass) -> None
"""
Create an email address for the new school class.

:param SchoolClass obj: the SchoolClass instance, that was just created.
:return: None
"""
    ml_name = self.name_for_mailinglist(obj)
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
    self.logger.info("Setting email address %r on school class %r...", ml_name,␣
↪obj.name)
    udm_obj = obj.get_udm_object(self.lo)  # access the underlying UDM object
    udm_obj["mailAddress"] = ml_name
    udm_obj.modify()
```

Die Klasse `SchoolClass` bietet kein Attribut an, um eine E-Mailadresse anzugeben. Die Klassen in `ucsschool.lib.models` sind jedoch tatsächlich eine Abstraktion regulärer Univention Directory Manager Objekte. Um auf die darunter liegenden Objekte zuzugreifen, wird die Methode `get_udm_object()` verwendet. Als Argument muss ihr ein sogenanntes LDAP Verbindungsobjekt (`lo`) mitgegeben werden.

Die Instanzvariablen `self.lo`, `self.logger` und `self.ucr` sind nach der Ausführung von `__init__()` verfügbar. Es handelt sich bei ihnen um die Instanz eines LDAP Verbindungsobjekts, einer Instanz von Python `Logger`[31] und einer Instanz von Univention Configuration Registry.

Soll eigener Code zur Initialisierung ausgeführt werden, so sollte `__init__()` folgendermaßen implementiert werden:

```
class MailForSchoolClass(Hook):
    def __init__(self, lo, *args, **kwargs):
        super(MailForSchoolClass, self).__init__(lo, *args, **kwargs)
        # From here on self.lo, self.logger and self.ucr are available.
        # You code here.
```

Zwei Funktionen helfen dabei, aus dem Namen der Schulklasse und einem Domänennamen, eine E-Mailadresse zu erzeugen:

```
def name_for_mailinglist(self, obj):  # type: (SchoolClass) -> str
    return "{}@{}".format(obj.name, self.domainname).lower()

@property
def domainname(self):  # type: () -> str
    try:
        return self.ucr["mail/hosteddomains"].split()[0]
    except (AttributeError, IndexError):
        return self.ucr["domainname"]
```

Um E-Mailadresse auch für umbenannte Schulklassen zu ändern, wird `post_modify()` implementiert:

```
def post_modify(self, obj):  # type: (SchoolClass) -> None
    """
    Change the email address of an existing school class.

    :param SchoolClass obj: the SchoolClass instance, that was just modified.
    :return: None
    """
    udm_obj = obj.get_udm_object(self.lo)
    ml_name = self.name_for_mailinglist(obj)
    if udm_obj["mailAddress"] != ml_name:
        self.logger.info(
            "Changing the email address of school class %r from %r to %r...",
            obj.name,
            udm_obj["mailAddress"],
            ml_name,
        )
        udm_obj["mailAddress"] = ml_name
        udm_obj.modify()
```

Die Datei mit obigem Python Code kann nun im Verzeichnis `/var/lib/ucs-school-lib/hooks` abgespeichert werden. Soll der Hook von einem UMC-Modul verwendet werden, muss zuerst der UMC-Server neu gestartet

[31] https://docs.python.org/3.7/library/logging.html#logging.Logger

werden:

```
$ service univention-management-console-server restart
```

Um den Hook zu testen, kann eine interaktive Python Shell verwendet werden. Einige Ausgaben wurden im folgenden Beispiel zur Verbesserung der Lesbarkeit gekürzt:

```
>>> import logging
>>> from ucsschool.lib.models.group import SchoolClass
>>> from univention.admin.uldap import getAdminConnection

>>> logging.basicConfig(level=logging.DEBUG, format="%(message)s",␣
↪handlers=[logging.StreamHandler()])
>>> lo, _ = getAdminConnection()

>>> sc = SchoolClass(name="DEMOSCHOOL-igel", school="DEMOSCHOOL")
>>> sc.create(lo)

Starting SchoolClass.call_hooks('pre', 'create', lo('cn=admin,dc=exam,dc=ple'))␣
↪for SchoolClass(
    name='DEMOSCHOOL-igel', school='DEMOSCHOOL', dn='cn=DEMOSCHOOL-igel,cn=klassen,
↪cn=schueler,
    cn=groups,ou=DEMOSCHOOL,dc=exam,dc=ple').
Searching for hooks of type 'Hook' in: /var/lib/ucs-school-lib/hooks...
Found hook classes: MailForSchoolClass
Loaded hooks: {'post_modify': ['MailForSchoolClass.post_modify'], 'post_create': [
    'MailForSchoolClass.post_create']}.
Creating SchoolClass(name='DEMOSCHOOL-igel', school='DEMOSCHOOL', dn='...')
SchoolClass(name='DEMOSCHOOL-igel', school='DEMOSCHOOL', dn='...') successfully␣
↪created
Starting SchoolClass.call_hooks('post', 'create', lo('cn=admin,dc=uni,dc=dtr'))␣
↪for SchoolClass(
    name='DEMOSCHOOL-igel', school='DEMOSCHOOL', dn='...').
Running post_create hook MailForSchoolClass.post_create for SchoolClass(name=
↪'DEMOSCHOOL-igel',
    school='DEMOSCHOOL', dn='...')...
Setting email address 'demoschool-igel@uni.dtr' on SchoolClass(name='DEMOSCHOOL-
↪igel',
    school='DEMOSCHOOL', dn='...')...
True

>>> sc.name = "DEMOSCHOOL-hase"
>>> sc.modify(lo)

Starting SchoolClass.call_hooks('pre', 'modify', lo('cn=admin,dc=exam,dc=ple'))␣
↪for SchoolClass(
    name='DEMOSCHOOL-hase', school='DEMOSCHOOL', dn='cn=DEMOSCHOOL-hase,...', old_
↪dn='cn=DEMOSCHOOL-igel,...').
Modifying SchoolClass(name='DEMOSCHOOL-hase', school='DEMOSCHOOL', dn=
↪'cn=DEMOSCHOOL-hase,...',
    old_dn='cn=DEMOSCHOOL-igel,...')
SchoolClass(name='DEMOSCHOOL-hase', school='DEMOSCHOOL', dn='cn=DEMOSCHOOL-hase,...
↪') successfully modified
Starting SchoolClass.call_hooks('post', 'modify', lo('cn=admin,dc=exam,dc=ple'))␣
↪for SchoolClass(
    name='DEMOSCHOOL-hase', school='DEMOSCHOOL', dn='cn=DEMOSCHOOL-hase,...').
Running post_modify hook MailForSchoolClass.post_modify for SchoolClass(name=
↪'DEMOSCHOOL-hase',
    school='DEMOSCHOOL', dn='cn=DEMOSCHOOL-hase,...')...
Changing the email address of SchoolClass(name='DEMOSCHOOL-hase', school=
↪'DEMOSCHOOL', ...)
    from 'demoschool-igel@example.com' to 'demoschool-hase@example.com'...
True
```

Im Verzeichnis `/var/lib/ucs-school-lib/hooks/` wird nach Python-Hooks gesucht und die Klasse *`MailForSchoolClass`* (Seite 84) gefunden. Nach dem Laden aller Hooks wird angezeigt, in welcher Reihenfolge welche Methoden für welche Phase ausgeführt werden. Da es keine *`pre_create()`* (Seite 84) Hooks gibt, wird nun das Objekt angelegt. Anschließend werden *`post_create()`* (Seite 84) Hooks ausgeführt. Erneut wird zuerst nach Hook-Skripten gesucht. Anschließend wird *`MailForSchoolClass`* (Seite 84).*`post_create()`* (Seite 84) ausgeführt. Beim `sc.modify(lo)` passiert das Gleiche.

KAPITEL 12

Hinweise für große UCS@school-Umgebungen

Die Standardkonfiguration von Univention Corporate Server und UCS@school ist für Umgebungen mit bis zu 5.000 Benutzern optimiert worden. In größeren Umgebungen kann es notwendig werden, Anpassungen an der Standardkonfiguration vorzunehmen. Die meisten Schritte werden bereits in *UCS performance guide* [13] beschrieben.

Darüber hinaus sollten einige Punkte bereits bei der Planung und dem Aufbau einer UCS@school-Umgebung beachtet werden:

- Durch die Verwendung einer Multi-Server-Umgebung und einer geeigneten Unterteilung der Benutzerkonten auf mehrere Schul-OUs kann die Last der einzelnen Schulserver bei einer großen Gesamtanzahl an Benutzern erheblich reduziert werden. Zusätzlich wird durch die Unterteilung für die Nutzer das Bedienen der UCS@school-Systeme erleichtert, da zum Beispiel die Menge der angezeigten Benutzer, Klassen, Räume usw. auf die jeweilige Schul-OU eingeschränkt wird.
- Gruppen mit einer großen Anzahl an Mitgliedern können negative Auswirkungen auf die Geschwindigkeit der UCS@school-Systeme haben. Es sollte daher beim Anlegen von Benutzern vermieden werden, dass alle Benutzer Mitglied einer bestimmten Gruppe (z.B. `Domain Users`) werden. Die UCS@school-Importskripte beachten dies bereits und legen pro Schul-OU eine eigene Gruppe `Domain Users` *`OUNAME`* an, die als primäre Gruppe für die Benutzerkonten verwendet wird.

  Falls für die Rechteverwaltung eine Zusammenfassung der Benutzer notwendig ist, können mehrere dieser Gruppen über die *Gruppen in Gruppen*-Funktionalität zusammengeführt werden. Die einzelnen `Domain User` *`OUNAME`*-Gruppen können dann bei Bedarf z.B. als Mitglied in der Gruppe `Domain Users` eingetragen werden.

12.1 Skalierung von UCS@school Samba 4 Umgebungen

Bemerkung: Bei UCS@school muss das Backend für BIND zwingend auf Samba 4 gesetzt sein (UCR-Variable `dns/backend`[32] `= samba4`).

[32] https://docs.software-univention.de/manual/5.0/de/appendix/variables.html#envvar-dns-backend

12.1.1 Installation zusätzlicher Managed Node Server

In UCS@school Umgebungen in denen Samba 4 Active Directory kompatible Dienste bereitstellt, kann ein zusätzlicher Managed Node-Server an einem Schulstandort installiert werden.

Um einen solchen zusätzlichen Managed Node-Server an einem Schulstandort zu installieren und zu joinen, müssen vorbereitende Schritte durchgeführt werden:

1. Für den neuen Managed Node-Server muss im Container `cn=computers` der gewünschten Schul-OU ein Rechnerobjekt angelegt werden. Der Name des Rechnerobjekts muss mit dem Hostnamen übereinstimmen, mit dem der neue Managed Node-Server installiert wurde.
2. Der Managed Node-Server muss in die Gruppen `Member-Edukativnetz` und `OU`*`OUNAME`*`-Member-Edukativnetz` aufgenommen werden.
3. Im Univention Directory Manager sollte eine Univention Configuration Registry Richtlinie angelegt werden, die die UCR-Variable `ldap/server/name`[33] auf den Namen des gewünschten Schulservers setzt. Diese Univention Configuration Registry Richtlinie sollte dann mit der gewünschten Schul-OU oder mit dem Container verknüpft werden, in dem das Rechnerobjekt des Managed Node-Servers positioniert ist.
4. Auf dem Managed Node-Server selbst muss vor dem Domänenbeitritt die UCR-Variable `nameserver1`[34] auf die IP-Adresse des Schulservers gesetzt werden. Die UCR-Variablen `nameserver2`[35] und `nameserver3`[36] dürfen nicht gesetzt sein.
5. Nach diesen Schritten kann der Managed Node-Server wie gewohnt der Domäne beitreten.

12.1.2 Automatische Suche deaktivieren

Standardmäßig wird beim Öffnen von Modulen der Univention Management Console eine Suche nach allen Objekten durchgeführt. Je nach Größe der Umgebung kann das sehr lange dauern, wenn kein Suchfilter angegeben wird. Dieses Verhalten kann durch Setzen der folgenden Univention Configuration Registry Variablen für die jeweiligen Module deaktiviert werden.

Passwörter (Schüler), Passwörter (Lehrer), Passwörter (Mitarbeiter)
`ucsschool/passwordreset/autosearch`

Lehrer zuordnen
`ucsschool/assign-teachers/autosearch`

Klassen zuordnen
`ucsschool/assign-classes/autosearch`

Arbeitsgruppen verwalten
`ucsschool/workgroups/autosearch`

Benutzer
`ucsschool/wizards/schoolwizards/users/autosearch`

Klassen
`ucsschool/wizards/schoolwizards/classes/autosearch`

Rechner
`ucsschool/wizards/schoolwizards/computers/autosearch`

Schulen
`ucsschool/wizards/schoolwizards/schools/autosearch`

Benutzer/Klassen/Rechner/Schulen
`ucsschool/wizards/autosearch`

[33] https://docs.software-univention.de/manual/5.0/de/appendix/variables.html#envvar-ldap-server-name
[34] https://docs.software-univention.de/manual/5.0/de/appendix/variables.html#envvar-nameserver1
[35] https://docs.software-univention.de/manual/5.0/de/appendix/variables.html#envvar-nameserver2
[36] https://docs.software-univention.de/manual/5.0/de/appendix/variables.html#envvar-nameserver3

Bemerkung: Wie die automatische Suche auch für andere (nicht schulbezogene) UMC-Module deaktiviert wird, steht in Disabling automatic search[37] in *UCS performance guide* [13] (nur in Englisch verfügbar).

[37] https://docs.software-univention.de/ext-performance/5.0/en/index.html#umc-search-auto

Literaturverzeichnis

[1] *UCS@school - Handbuch für Lehrkräfte und Schuladministratoren*. Univention GmbH, 2021. URL: https://docs.software-univention.de/ucsschool-lehrer-handbuch-5.0.html.

[2] *Univention Corporate Server - Handbuch für Benutzer und Administratoren*. Univention GmbH, 2021. URL: https://docs.software-univention.de/manual/5.0/de/.

[3] *UCS@school - Szenarien zum Einsatz von UCS@school*. Univention GmbH, 2021. URL: https://docs.software-univention.de/ucsschool-scenarios/5.0/de/index.html.

[4] *UCS@school - Handbuch zur CLI-Import-Schnittstelle*. Univention GmbH, 2021. URL: https://docs.software-univention.de/ucsschool-import/5.0/de/index.html.

[5] *Group Policy processing and precedence*. Microsoft, April 2013. URL: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc785665(v=ws.10).

[6] *Threats and Countermeasures Guide: External Storage Devices*. Microsoft, 2012. URL: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/hh125922(v=ws.10).

[7] *Verwenden von Gruppenrichtlinien zum Deaktivieren von USB-, CD-ROM-, Disketten- und LS-120-Treibern*. Microsoft, September 2021. URL: https://learn.microsoft.com/en-us/troubleshoot/windows-server/group-policy/adm-template-disable-drivers.

[8] *Wie kann ich verhindern, dass Benutzer eine Verbindung zu einem USB-Speichergerät herstellen?* Microsoft, April 2018. URL: https://support.microsoft.com/kb/823732.

[9] *Controlling the Use of Removable Devices and Media*. Microsoft, 2012. URL: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc771759(v=ws.10).

[10] *Device Management and Installation Step-by-Step Guide: Controlling Device Driver Installation and Usage with Group Policy*. Microsoft, 2012. URL: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731387(v=ws.10).

[11] *Using Software Restriction Policies to Protect Against Unauthorized Software*. Microsoft, September 2009. URL: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb457006(v=technet.10).

[12] *Administer Software Restriction Policies*. Microsoft, August 2016. URL: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh994606(v=ws.11).

[13] *UCS performance guide*. Univention GmbH, 2021. URL: https://docs.software-univention.de/ext-performance/5.0/en/index.html.

Stichwortverzeichnis

V

Y