univention
be open.

UCS@school

Handbuch für Administratoren

www.univention.de

Version 4.1 v1
Stand: 09. Oktober 2015

Alle Rechte vorbehalten./ All rights reserved.
(c) 2002-2015
Univention GmbH
Mary-Somerville-Straße 1
28359 Bremen
Deutschland
feedback@univention.de

Jede aufgeführte Marke und jedes Warenzeichen steht im Eigentum ihrer jeweiligen eingetragenen Rechtsinhaber. Linux ist ein eingetragenes Warenzeichen von Linus Torvalds.

The mentioned brand names and registered trademarks are owned by the respective legal owners in each case. Linux is a registered trademark of Linus Torvalds.

univention
be open.

Inhaltsverzeichnis

1. Einführung 7
2. Aufbau einer UCS@school-Umgebung 9
    2.1. UCS@school-Benutzerrollen 9
    2.2. Aufteilung von UCS@school 10
        2.2.1. Replikation der LDAP-Daten auf die Schul-Standorte 10
    2.3. Verwaltungsnetz und Edukativnetz 10
    2.4. UCS@school-Objekte im LDAP-Verzeichnisdienst 11
        2.4.1. Struktur einer UCS@school-OU 11
        2.4.2. Weitere UCS@school-Objekte 13
3. Installation 15
    3.1. Installation einer Single-Server-Umgebung 15
        3.1.1. Installation des DC Master 15
    3.2. Installation einer Multi-Server-Umgebung 16
        3.2.1. Installation des DC Master 16
        3.2.2. Installation eines DC Backup (optional) 17
        3.2.3. Installation eines Schulservers 17
    3.3. (Erneuter) Domänenbeitritt eines Schulservers 18
    3.4. Umwandlung einer Single-Server-Umgebung in eine Multi-Server-Umgebung 19
4. Verwaltung von Schulen über die Univention Management Console 21
    4.1. Verwaltung von Schulen 21
        4.1.1. Anlegen von Schulen 21
        4.1.2. Bearbeiten von Schulen 22
        4.1.3. Löschen von Schulen 22
    4.2. Verwaltung einzelner Benutzerkonten 22
        4.2.1. Anlegen eines Benutzerkontos 22
        4.2.2. Bearbeiten eines Benutzerkontos 23
        4.2.3. Löschen von Benutzerkonten 23
    4.3. Pflege von Benutzerkonten über CSV-Dateien 23
        4.3.1. Import von CSV-Dateien 23
    4.4. Verwaltung von Schulklassen 28
        4.4.1. Anlegen von Schulklassen 28
        4.4.2. Bearbeiten von Schulklassen 28
        4.4.3. Löschen von Schulklassen 28
    4.5. Verwaltung von Rechnern 29
        4.5.1. Anlegen von Rechnerkonten 29
        4.5.2. Bearbeiten von Rechnerkonten 29
        4.5.3. Löschen von Rechnerkonten 30
5. Verwaltung von Schulen über Importskripte 31
    5.1. Pflege von Benutzerkonten für Schüler, Lehrer und Mitarbeiter 31
    5.2. Import von Schulklassen 33
    5.3. Vorgehen zum Schuljahreswechsel 34
    5.4. Skriptbasierter Import von Netzwerken 35
    5.5. Import von Rechnerkonten für Windows-PCs 35
        5.5.1. Skriptbasierter Import von PCs 36
    5.6. Konfiguration von Druckern an der Schule 37
6. Erweiterte Konfiguration 39
    6.1. Einrichtung der Druckmoderation 39
        6.1.1. Anlegen eines PDF-Druckers für die Druckermoderation 39
    6.2. Windows-spezifische Benutzereinstellungen 40
    6.3. Anlegen von Freigaben 41
    6.4. Lehrerzugriff auf Benutzerfreigaben 41
    6.5. Anlegen von Benutzerkonten für Schuladministratoren 42

6.6. Konfiguration der Helpdesk-Kontaktadresse 42
7. Integration und Verwaltung von Microsoft Windows-Clients 43
7.1. Anmeldedienste mit Samba 43
7.2. Server für Dateifreigaben 44
7.3. Netlogon-Skripte für Samba4-Umgebung 44
7.4. iTALC-Installation auf Windows-Clients 45
8. Übersicht über die schulspezifischen Anwendungen 47
8.1. Modulübersicht 47
9. Web-Proxy auf den Schulservern 49
9.1. Einbindung von externen Blacklisten 49
10. Authentifizierung des WLAN-Zugriffs über RADIUS 51
10.1. Installation und Konfiguration des RADIUS-Servers 51
10.2. Konfiguration der *Access Points* 51
10.3. Konfiguration der zugreifenden Clients 51
10.4. Freigabe des WLAN-Zugriffs in der Univention Management Console 52
10.5. Fehlersuche 52
11. Klassenarbeitsmodus 53
11.1. Technische Hintergründe 53
11.2. Konfiguration 54
11.3. Beispiele für Gruppenrichtlinien 55
11.3.1. Generelle Hinweise zu Gruppenrichtlinien und Administrativen Vorlagen 56
11.3.2. Windows-Anmeldung im Prüfungsraum auf Mitglieder der Klassenarbeitsgruppe beschränken 56
11.3.2.1. Anwendungsbereich der GPO auf Klassenarbeitscomputer einschränken 57
11.3.2.2. Einschränkung der Windows-Anmeldung auf Klassenarbeitsbenutzerkonten und Lehrer 57
11.3.3. Zugriff auf USB-Speicher und Wechselmedien einschränken 58
11.3.3.1. Zugriff auf USB-Speicher an Windows XP einschränken 58
11.3.3.2. Installation neuer Gerätetreiber für USB-Speicher an Windows XP verbieten 58
11.3.3.3. Zugriff auf USB-Speicher an Windows 7 einschränken 59
11.3.3.4. Installation neuer Gerätetreiber für USB-Speicher an Windows 7 Clients verbieten 59
11.3.4. Vorgabe von Proxy-Einstellungen für den Internetzugriff 60
11.3.4.1. Proxy-Vorgabe für den Internet Explorer 60
11.3.4.2. Sperrung der Proxyeinstellung für den Internet Explorer 60
11.3.4.3. Proxy-Vorgabe für Google Chrome 61
11.3.4.4. Proxy-Vorgabe für Mozilla Firefox 61
11.3.5. Zugriff auf bestimmte Programme einschränken 62
11.3.5.1. Kommandoeingabeaufforderung deaktivieren 62
11.3.5.2. Zugriff auf Windows-Registry-Editor deaktivieren 63
11.3.5.3. Konfiguration von *Software Restriction Policies* (SRP) 63
11.3.6. Verwendung temporärer Benutzerprofil-Kopien 64
12. Integration und Verwaltung von Univention Corporate Client-Systemen 67
12.1. Installation von UCC 68
12.2. Konfigurationseinstellungen für UCC-Systeme 68
12.3. Ausrollen von neuen UCC-Systemen 69
13. Pre- und Post-Hook-Skripte für den Import 71
13.1. Erweiterung von Importdateien 72
13.2. Beispiel-Hook-Skript: automatische Erstellung der Marktplatzfreigabe 72
13.3. Beispiel-Hook-Skript: Setzen des LDAP-Containers für DHCP-Objekte 73
14. Hinweise für große UCS@school-Umgebungen 75
14.1. Skalierung von UCS@school Samba 4 Umgebungen 75
14.1.1. Installation zusätzlicher Memberserver 75

14.1.2. Installation zusätzlicher Anmeldeserver 76
Literaturverzeichnis 77

Kapitel 1. Einführung

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 ein zusätzliches Dokument [ucs-school-teacher] bereit.

Kapitel 2. Aufbau einer UCS@school-Umgebung

2.1. UCS@school-Benutzerrollen 9
2.2. Aufteilung von UCS@school 10
2.2.1. Replikation der LDAP-Daten auf die Schul-Standorte 10
2.3. Verwaltungsnetz und Edukativnetz 10
2.4. UCS@school-Objekte im LDAP-Verzeichnisdienst 11
2.4.1. Struktur einer UCS@school-OU 11
2.4.2. Weitere UCS@school-Objekte 13

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.

2.1. UCS@school-Benutzerrollen

Feedback

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:

- *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* 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.

- Vollen Zugriff auf die Administrationsfunktionen von UCS@school erhalten die *Schuladministratoren*. Sie können z.B. Computer zu Rechnergruppen zusammenfassen, neue Internetfilter definieren oder auch Lehrerpasswörter zurücksetzen.

- 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 Abschnitt 2.3).

- 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 ein, die üblicherweise aus vorhandenen Schulverwaltungssystemen extrahiert werden können und so einen automatisierten Abgleich ermöglichen.

2.2. Aufteilung von UCS@school

Feedback

Für den Betrieb von UCS@school an einer einzelnen Schule reicht ein Serversystem aus (dieses wird dann in der UCS-Systemrolle Domänencontroller Master 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 Domänencontroller Master als der primäre Server zur Datenverwaltung genutzt. Für jeden Schul-Standort wird dann ein Domänencontroller Slave installiert, nachfolgend als *Schulserver* bezeichnet.

Achtung

UCS@school unterstützt derzeit nur einen Schulserver pro Standort. Darüber hinaus können weitere UCS-Systeme mit Samba 4 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 Abschnitt 2.2.1). Die Einrichtung zusätzlicher UCS-Systeme wird in Abschnitt 14.1 beschrieben.

2.2.1. Replikation der LDAP-Daten auf die Schul-Standorte

Feedback

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 Domänencontroller Master fortlaufend repliziert und aktualisiert wird. Dies gewährleistet einen reibungslosen Betrieb, auch wenn die Verbindung zwischen Schulserver und dem zentralen Domänencontroller Master einmal ausfallen sollte.

Aus Sicherheitsgründen speichern die Schulservern 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 werden auf den Schul-Server übertragen.

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.

Seit UCS@school 3.2 R2 wird zwischen dem Namen einer Schule und dem Schulkürzel (OU-Namen) unterschieden. 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.

2.3. Verwaltungsnetz und Edukativnetz

Feedback

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 Abschnitt 2.2.1 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.

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 Abschnitt 3.2.3 werden diese ausführlich beschrieben.

Anmerkung

Die Einrichtung eines Verwaltungsnetzes ist in einer Single-Server-Umgebung nicht möglich. Hier werden alle Benutzerkonten auf dem Domänencontroller Master vorgehalten.

Achtung

Voraussetzung für diese Unterteilung ist eine physikalische Trennung der beiden Netzwerksegmente. D.h. das edukative Netz und das Verwaltungsnetz können nicht gleichzeitig im gleichen Netzwerksegment verwendet werden.

2.4. UCS@school-Objekte im LDAP-Verzeichnisdienst

Feedback

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 Abschnitt 2.2.1 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.

2.4.1. Struktur einer UCS@school-OU

Feedback

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.

Anmerkung

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

2.4.2. Weitere UCS@school-Objekte

Feedback

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 OU-spezifisch. Sie enthalten (entsprechend ihrem Namen) als Gruppenmitglieder die Schul-DCs oder die Memberserver der Schulstandorte, wobei diese jeweils nach Verwaltungsnetz und Edukativnetz getrennt werden. Domaincontroller Master und Domaincontroller Backup 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 Memberserver der jeweiligen OU (hier *gymmitte*), wobei diese jeweils nach Verwaltungsnetz und Edukativnetz getrennt werden. Domaincontroller Master und Domaincontroller Backup 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 Abschnitt 6.5.

Kapitel 3. Installation

3.1. Installation einer Single-Server-Umgebung 15
3.1.1. Installation des DC Master 15
3.2. Installation einer Multi-Server-Umgebung 16
3.2.1. Installation des DC Master 16
3.2.2. Installation eines DC Backup (optional) 17
3.2.3. Installation eines Schulservers 17
3.3. (Erneuter) Domänenbeitritt eines Schulservers 18
3.4. Umwandlung einer Single-Server-Umgebung in eine Multi-Server-Umgebung 19

UCS@school basiert auf Univention Corporate Server (UCS). UCS@school wird dabei als Repository-Komponente eingebunden. Die Installation von UCS ist im UCS-Handbuch 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: die Installation als Single-Server-Umgebung und die Installation als Multi-Server-Umgebung mit einem Domänencontroller Master und mindestens einem Schulserver. Die nachträgliche Umwandlung einer Single-Server-Umgebung in eine Multi-Server-Umgebung wird unterstützt und in Abschnitt 3.4 genauer beschrieben.

3.1. Installation einer Single-Server-Umgebung

Feedback

3.1.1. Installation des DC Master

Feedback

Bei der UCS-Installation muss die Systemrolle *Domänencontroller Master* ausgewählt werden. Nach der UCS-Installation kann in Univention Management Console das Modul **App Center** geöffnet und dort die Applikation *UCS@school* nachinstalliert werden. Nach Abschluss der Installation wird in Univention Management Console ein neues Modul angezeigt, mit welchem die wizardgesteuerte Konfiguration von UCS@school durchgeführt wird:

- Das Konfigurationsmodul fragt auf dem DC Master zunächst nach der Art der UCS@school-Umgebung, die installiert werden soll. Hier ist der Eintrag *Single-Server-Umgebung* auszuwählen.

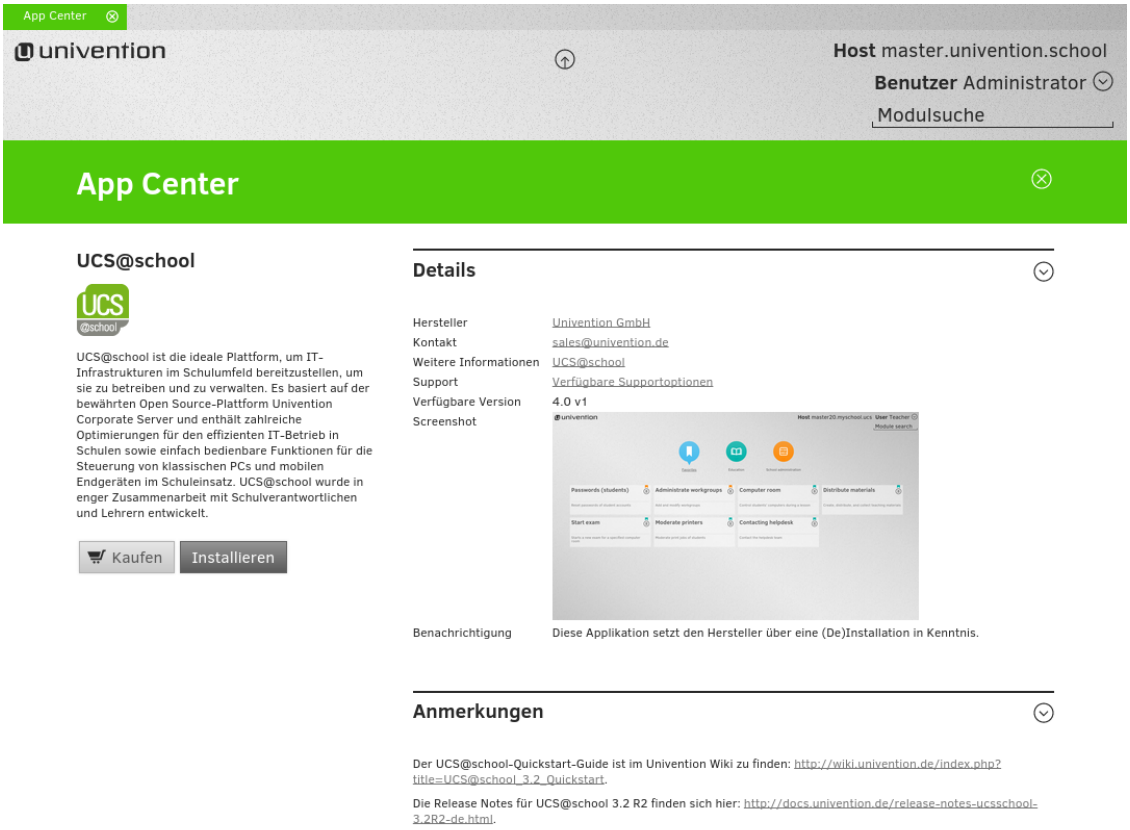
- UCS@school benötigt für die Bereitstellung von Datei- und Drucker-Freigaben den Samba-Dienst. Sofern auf dem DC Master noch kein Samba-Dienst installiert ist, kann zwischen *Samba 3* und *Samba 4* ausgewählt werden.

- Die Daten eines Schulservers werden im Verzeichnisdienst in Organisationseinheiten (OU) gespeichert (siehe auch Kapitel 2). Im letzten Schritt des Konfigurationsassistenten wird nach dem Namen der Schule gefragt. Dieser ist ein frei wählbarer Bezeichner (wie z.B. *Gymnasium Mitte*), der primär in den UMC-Modulen verwendet wird. Das ebenfalls abgefragte Schulkürzel entspricht dem eigentlichen Namen der Organisationseinheit, welche vom UMC-Modul im Zuge der Konfiguration automatisch angelegt wird. Das Schulkürzel sollte ausschließlich aus Buchstaben (a-z und A-Z), Ziffern (0-9) 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. Nach der Eingabe des Schulnamens wird automatisch ein Vorschlag für ein Schulkürzel gemacht, welcher jedoch manuell angepasst werden kann.

Während der Konfiguration werden benötigte Softwarepakete automatisch aus dem Univention App Center heruntergeladen und installiert. Somit sind nach der Konfiguration alle für die Datenpflege und Steuerung von UCS@school benötigten Pakete auf dem DC Master zugreifbar.

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 Kapitel 4 und Kapitel 5.

Abbildung 3.1. Installation von UCS@school über das Univention App Center



Wurde während der Installation des DC Masters ein DHCP-Server installiert, verschiebt der UCS@school-Konfigurationsassistent das DHCP-Server-Objekt des DC Masters (zu finden unter `cn=dhcp,`*`LDAPBASIS`*) automatisch in den entsprechenden DHCP-Container der OU (`cn=dhcp,ou=`*`OUNAME`*`,`*`LDAPBASIS`*). Dies ist für die korrekte Funktion des DHCP-Servers notwendig.

3.2. Installation einer Multi-Server-Umgebung

Feedback

3.2.1. Installation des DC Master

Feedback

Bei der UCS-Installation muss die Systemrolle *Domänencontroller Master* ausgewählt werden. Nach der UCS-Installation kann in Univention Management Console das Modul **App Center** geöffnet und dort die Applikation *UCS@school* nachinstalliert werden. Nach Abschluss der Installation wird in Univention Management Console ein neues Modul angezeigt, mit welchem die wizardgesteuerte Konfiguration von UCS@school durchgeführt wird:

- Das Konfigurationsmodul fragt auf dem DC Master zunächst nach der Art der UCS@school-Umgebung, die installiert werden soll. Hier ist der Eintrag *Multi-Server-Umgebung* auszuwählen.
- Weitere Konfigurationsoptionen werden in einer Multi-Server-Umgebung auf dem DC Master nicht benötigt.

Während der Konfiguration werden benötigte Softwarepakete automatisch aus dem Univention App Center heruntergeladen und installiert. Somit sind nach der Konfiguration alle für die Datenpflege benötigten Pakete auf dem DC Master zugreifbar.

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

3.2.2. Installation eines DC Backup (optional)

Feedback

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

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

Die Installation von UCS@school auf einem DC Backup erfolgt analog zur in Abschnitt 3.2 beschriebenen Installation des DC Master.

Achtung

Sofern DC Backup-Systeme in der UCS-Domäne vorhanden sind, muss dort ebenfalls UCS@school installiert und konfiguriert werden. Sollte dies nicht der Fall sein, kann es zu schweren Replikationsproblemen auf den Schulservern kommen.

3.2.3. Installation eines Schulservers

Feedback

An jedem Schul-Standort muss ein Schulserver installiert werden.

Bei der UCS-Installation muss die Systemrolle *Domänencontroller Slave* (kurz DC Slave) ausgewählt werden. Nach der UCS-Installation kann in Univention Management Console das Modul **App Center** geöffnet und dort die Applikation *UCS@school* nachinstalliert werden. Nach Abschluss der Installation wird in Univention Management Console ein neues Modul angezeigt, mit welchem die wizardgesteuerte Konfiguration von UCS@school auf dem DC Slave durchgeführt wird:

- Das Konfigurationsmodul kann auf einem DC Slave nur dann erfolgreich durchlaufen werden, wenn die Konfiguration des DC Masters bereits über das dort installierte Konfigurationsmodul abgeschlossen wurde.
- Nach der Konfiguration ist es erforderlich, dass der DC Slave erneut der Domäne beitritt. Im zweiten Schritt werden die für den erneuten Beitritt notwendigen Anmeldedaten (Benutzername, Passwort) abgefragt. Hier kann der Benutzer `Administrator` oder ein Mitglied der Gruppe `Domain Admins` angegeben werden. Der vollqualifizierte Rechnername (FQDN) des DC Masters wird üblicherweise automatisch ermittelt und vorausgefüllt. Sollte dies nicht möglich sein, muss der vollständige Rechnername inkl. DNS-Domäne angegeben werden, z.B. `master.example.com`.
- UCS@school benötigt für die Bereitstellung von Datei- und Drucker-Freigaben den Samba-Dienst. Sofern auf dem DC Master noch kein Samba-Dienst installiert ist, kann zwischen *Samba 3* und *Samba 4* ausgewählt werden.
- Die Daten eines Schulservers werden im Verzeichnisdienst in Organisationseinheiten (OU) gespeichert (siehe auch Kapitel 2). Daher wird im Konfigurationsassistenten nach dem Namen der Schule gefragt. Dieser ist ein frei wählbarer Bezeichner (wie z.B. *Gymnasium Mitte*), der primär in den UMC-Modulen verwendet wird. Das ebenfalls abgefragte Schulkürzel entspricht dem eigentlichen Namen der Organisationseinheit, welche vom UMC-Modul im Zuge der Konfiguration automatisch angelegt wird. 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. Nach der Eingabe des Schul-

namens wird automatisch ein Vorschlag für ein Schulkürzel gemacht, welcher jedoch manuell angepasst werden kann.

- Nach der Angabe des Schulnamens ist die Art des Schulservers anzugeben. Es kann zwischen einem Schulserver für das Edukativnetz (**Edukativer Schulserver**) und einem Schulserver für das Verwaltungsnetz (**Verwaltungsserver**) gewählt werden. Die Funktionen für den IT-gestützten Unterricht werden dabei nur von den Schulservern im Edukativnetz bereitgestellt.

- Sollte an einem Schulstandort der Schulserver des Verwaltungsnetzes vor dem edukativen Schulserver konfiguriert werden, fragt der Konfigurationsassistent zusätzlich den Namen des zukünftigen edukativen Schulservers ab. Sollte der hier angegebene Name des Schulservers nicht korrekt sein, muss vor dem Import von Benutzern der Freigabeserver für die Benutzer-Heimatverzeichnisse korrigiert werden (siehe auch Abschnitt 4.1.2).

Achtung

Für den Verwaltungsserver muss ein vom edukativen Netz physikalisch getrenntes Netzwerksegment sowie ein eigenes IP-Subnetz verwendet wird, um Konflikte mit dem Schulserver des Edukativnetzes zu vermeiden (siehe auch Abschnitt 2.3).

Während der Konfiguration werden benötigte Softwarepakete automatisch aus dem Univention App Center installiert und ein erneuter Domänenbeitritt durchgeführt. Somit sind nach der Konfiguration alle für die Steuerung von UCS@school benötigten Pakete auf dem DC Slave zugreifbar.

Wurde während der Installation des DC Slaves ein DHCP-Server installiert, verschiebt der UCS@school-Konfigurationsassistent das DHCP-Server-Objekt des DC Slaves (zu finden unter `cn=dhcp,`*`LDAPBASIS`*) automatisch in den entsprechenden DHCP-Container der OU (`cn=dhcp,ou=`*`OUNAME`*`,`*`LDAPBASIS`*). Dies ist für die korrekte Funktion des DHCP-Servers notwendig, da jeder Schulserver eine individuelle LDAP-Suchbasis verwendet.

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

3.3. (Erneuter) Domänenbeitritt eines Schulservers

Feedback

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

- Vor dem Domänenbeitritt des Schulservers muss die Schule (OU) des Schulservers in der Univention Management Console des DC Masters angelegt werden (siehe Abschnitt 4.1). Das Anlegen der Schule (OU) erfolgt üblicherweise automatisch durch das UMC-Konfigurationsmodul und muss nur dann manuell durchgeführt werden, wenn die Schule (OU) im LDAP-Verzeichnis noch fehlt.

- Anschließend muss das System erneut der Domäne beitreten. Dies erfolgt auf der Kommandozeile durch Aufruf des Befehls `univention-join`.

- Der Domänencontroller Master wird im Regelfall durch eine DNS-Abfrage ermittelt. Wenn das nicht möglich sein sollte, kann der Rechnername des DC Master auch durch den Parameter `-dcname` *`HOSTNAME`* direkt angegeben werden. Der Rechnername muss dabei als vollqualifizierter Name angegeben werden, also beispielsweise `master.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.

Anmerkung

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.

3.4. Umwandlung einer Single-Server-Umgebung in eine Multi-Server-Umgebung

Feedback

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 DC Masters auszuführen, die einen Austausch des UCS@school-Metapakets sowie eine Konfigurationsänderung durchführen (Bitte das Minuszeichen hinter dem zweiten Paketnamen beachten):

```
univention-install ucs-school-master ucs-school-singlemaster-
ucr unset ucsschool/singlemaster
```

Mit der Deinstallation des Pakets ***ucs-school-singlemaster*** werden die nachfolgenden UCS@school-spezifischen Pakete (z.B. UMC-Module), die normalerweise nicht auf einem DC Master der Multi-Server-Umgebung installiert sind, automatisch zur Löschung vorgesehen. Die eigentliche Löschung 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-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-netlogon
ucs-school-netlogon-user-logonscripts
ucs-school-old-homedirs
ucs-school-old-sharedirs
ucs-school-ucc-integration
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, sollte auf ihre Einstellungen hin überprüft werden. Dies betrifft unter anderem die DHCP-DNS-Einstellungen sowie die Einstellungen für UCC-Systeme (siehe auch Abschnitt 12.2).

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

```
invoke-rc.d univention-management-console-server restart
```

Achtung

Es ist zu beachten, dass auch nach der abgeschlossenen Umwandlung in eine Multi-Server-Umgebung der auf dem DC Master installierte Samba3- oder Samba4-Dienst bestehen bleibt und nicht automatisch deinstalliert wird.

Kapitel 4. Verwaltung von Schulen über die Univention Management Console

4.1. Verwaltung von Schulen 21
4.1.1. Anlegen von Schulen 21
4.1.2. Bearbeiten von Schulen 22
4.1.3. Löschen von Schulen 22
4.2. Verwaltung einzelner Benutzerkonten 22
4.2.1. Anlegen eines Benutzerkontos 22
4.2.2. Bearbeiten eines Benutzerkontos 23
4.2.3. Löschen von Benutzerkonten 23
4.3. Pflege von Benutzerkonten über CSV-Dateien 23
4.3.1. Import von CSV-Dateien 23
4.4. Verwaltung von Schulklassen 28
4.4.1. Anlegen von Schulklassen 28
4.4.2. Bearbeiten von Schulklassen 28
4.4.3. Löschen von Schulklassen 28
4.5. Verwaltung von Rechnern 29
4.5.1. Anlegen von Rechnerkonten 29
4.5.2. Bearbeiten von Rechnerkonten 29
4.5.3. Löschen von Rechnerkonten 30

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 Kapitel 5 näher beschrieben).

4.1. Verwaltung von Schulen

Feedback

Die Daten einer Schule werden in einer Organisationseinheit (OU) - einem Teilbaum des LDAP-Verzeichnisdienstes - gespeichert (siehe auch Kapitel 2). 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.

4.1.1. Anlegen von Schulen

Feedback

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 ein 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 Schulservernamens 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 Abschnitt 6.2 und Abschnitt 7.2).

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

Anmerkung

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

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.

4.1.2. Bearbeiten von Schulen

Feedback

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 Abschnitt 6.2 und Abschnitt 7.2 beschrieben.

4.1.3. Löschen von Schulen

Feedback

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

Achtung

Das Löschen einer Schule umfasst auch das Entfernen aller damit verbundenen Objekte wie Benutzerkonten, Klassen, Arbeitsgruppen, Rechner, DHCP-Leases, Drucker und Freigaben! Das Löschen einer Schule kann nicht rückgängig gemacht werden!

4.2. Verwaltung einzelner Benutzerkonten

Feedback

Für die manuelle Pflege von einzelnen Benutzerkonten wird auf dem Domänencontroller Master 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.

4.2.1. Anlegen eines Benutzerkontos

Feedback

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.

Die erste Seite des Assistenten fragt zunächst die gewünschte Benutzerrolle für das neue Benutzerkonto ab. Zur Auswahl stehen die vier Benutzerrollen *Schüler*, *Lehrer*, *Lehrer und Mitarbeiter* und *Mitarbeiter*. Die einzelnen Benutzerrollen werden in Abschnitt 2.1 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: *Vorname*, *Nachname*, *Benutzername*, ggf. *Klasse*, *E-Mail-Adresse* und *Passwort*. 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. Die Angabe von E-Mail-Adresse und Passwort ist optional. Ist kein Passwort vergeben, muss das Passwort vom Administrator (oder Lehrer) zurückgesetzt werden, bevor das Benutzerkonto vom Benutzer erstmalig verwendet werden kann.

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.

Anmerkung

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

4.2.2. Bearbeiten eines Benutzerkontos

Feedback

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.

4.2.3. Löschen von Benutzerkonten

Feedback

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.

4.3. Pflege von Benutzerkonten über CSV-Dateien

Feedback

Zusätzlich zum UMC-Modul **Benutzer (Schulen)**, welches die Pflege einzelner Benutzerkonten erlaubt, bringt UCS@school den Assistenten **CSV-Import** für die Pflege von Benutzerkonten über CSV-Dateien mit.

Der Assistent erlaubt es, eine CSV-Datei mit Benutzerinformationen einzulesen. Die eingelesenen Daten werden z.B. auf Schreibfehler oder Konflikte geprüft und werden vor dem eigentlichen Import innerhalb des Assistenten noch einmal angezeigt. Dort können die Daten nachträglich bearbeitet werden. Neben dem Anlegen neuer Benutzerkonten ist es auch möglich, vorhandene Benutzerkonten zu modifizieren oder zu löschen.

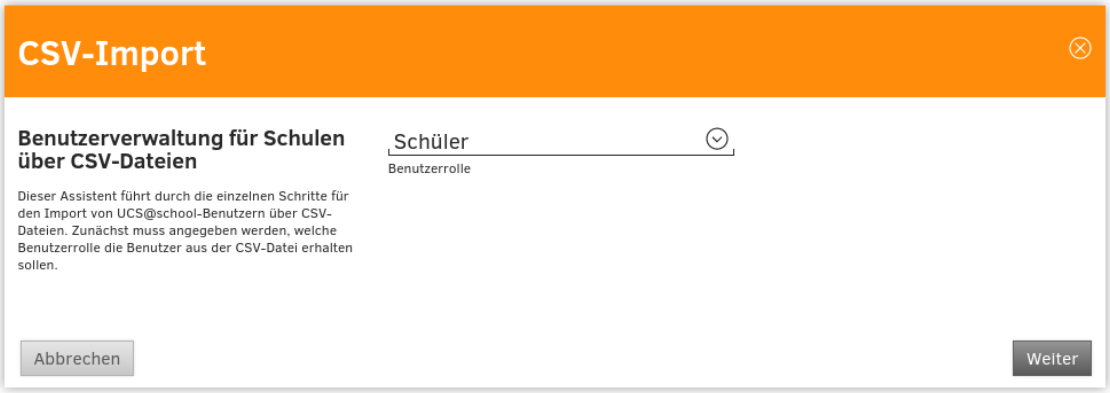
4.3.1. Import von CSV-Dateien

Feedback

Für den Import einer CSV-Datei muss das UMC-Modul **CSV-Import** aus der UMC-Modulgruppe **Schul-Administration** geöffnet werden. Der Assistent sieht vor, dass durch eine CSV-Datei nur Benutzer einer

bestimmten Benutzerrolle importiert werden können. Der gleichzeitige Import von z.B. Schülern und Lehrern durch den Import einer einzelnen CSV-Datei ist also nicht möglich. Auf der ersten Seite des Assistenten ist daher die gewünschte Benutzerrolle auszuwählen (siehe Abbildung 4.1). Sind mehrere Schulen in der UCS@school-Umgebung eingerichtet, wird zusätzlich abgefragt, in welche Schule die CSV-Datei importiert werden soll.

Abbildung 4.1. CSV-Import: Auswahl der Benutzerrolle

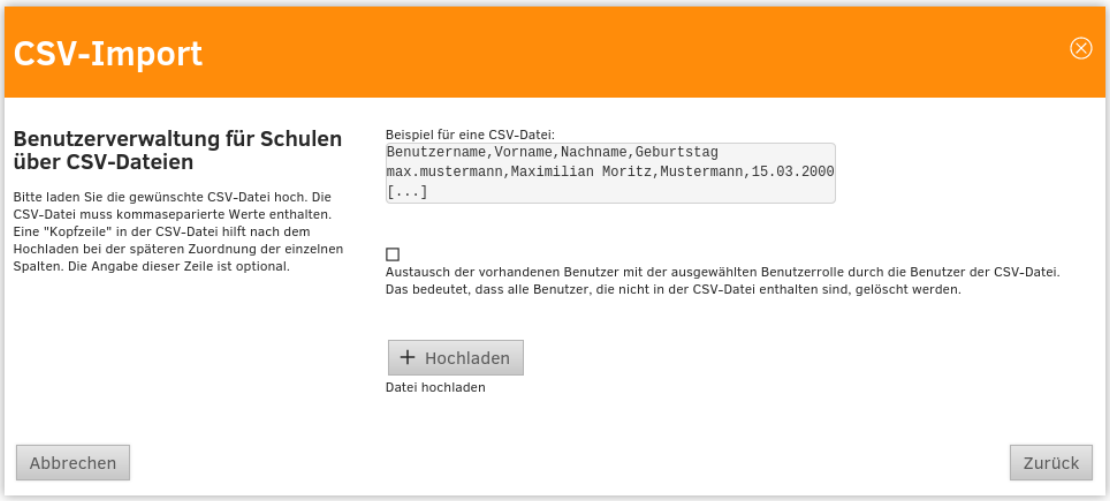


Nach dem Auswählen der Schaltfläche **Weiter** ist auf der zweiten Seite der Import-Modus auszuwählen sowie die CSV-Datei hochzuladen.

In der Standardeinstellung werden die in der CSV-Datei angegebenen Benutzerkonten hinzugefügt. Sollten gleichlautende Benutzerkonten schon im Verzeichnisdienst existieren, werden sie entsprechend der CSV-Datei modifiziert. Dieser Import-Modus ist für den Erstimport von Benutzerkonten (z.B. ein einzelner Klassensatz) oder das nachträgliche Modifizieren einer Teilmenge der vorhandenen Benutzerkonten gedacht.

Liegt eine CSV-Datei mit allen gültigen Benutzern vor, kann alternativ der zweite Import-Modus verwendet werden. In diesem Modus werden (zusätzlich zum vorher beschriebenen Verhalten) alle Benutzerkonten gelöscht, die im Verzeichnisdienst, aber nicht in der CSV-Datei enthalten sind. Zum Beispiel kann so zum Schuljahreswechsel ein CSV-Komplettexport der Schülerdatenbank aus der Schulverwaltungssoftware durchgeführt und die CSV-Datei in UCS@school importiert werden: für neue Schüler werden Benutzerkonten erstellt, die Benutzerkonten von vorhandenen Schülern werden aktualisiert und die Benutzerkonten von abgegangenen Schülern werden gelöscht. Für den zweiten Import-Modus ist die Checkbox **Austausch der vorhandenen Benutzer mit der ausgewählten Benutzerrolle durch die Benutzer der CSV-Datei** zu aktivieren.

Abbildung 4.2. CSV-Import: Upload der CSV-Datei



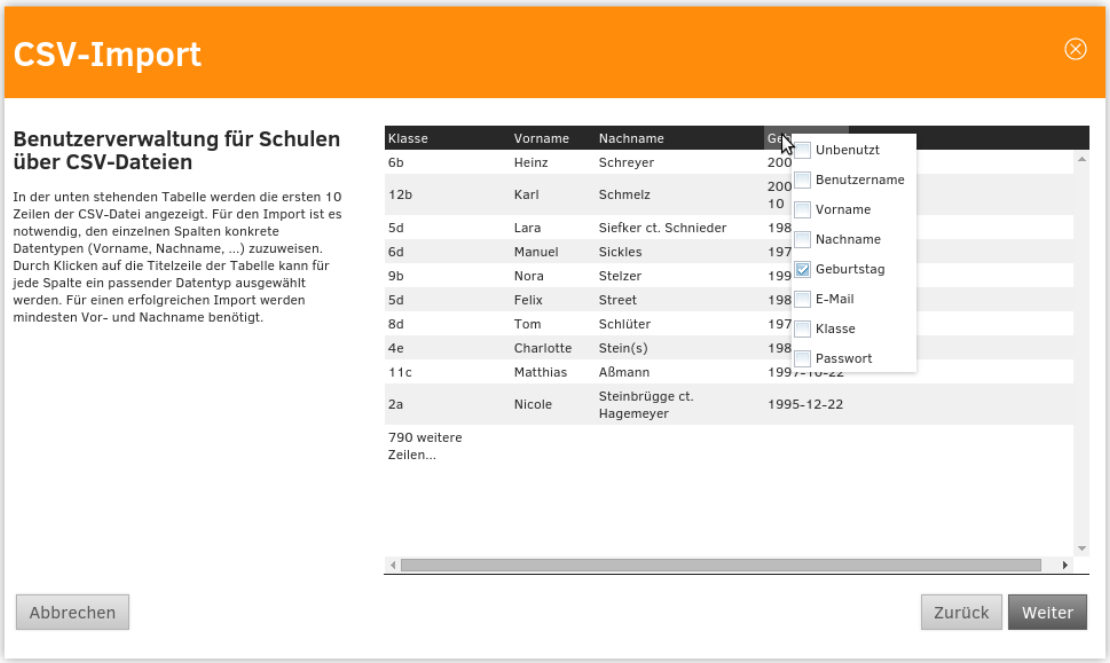
Mit dem **Hochladen** einer CSV-Datei wechselt der Assistent automatisch zum dritten Schritt, in dem eine Zuordnung der Spalten der CSV-Datei zu konkreten Benutzerattributen erfolgt. Folgende Benutzerattribute stehen für die Zuordnung zur Verfügung:

- Benutzername
- Vorname
- Nachname
- Geburtstag
- E-Mail
- Klasse
- Passwort

Für die einfachere Zuordnung zeigt der Assistent die ersten 10 Zeilen der CSV-Datei an. Mit einem Klick auf den Titel der jeweiligen Spalte kann die Zuordnung geändert werden (siehe Abbildung 4.3).

Für den Import wird mindestens die Zuordnung der Benutzerattribute *Vorname* und *Nachname* benötigt. Wurde dem Attribut *Benutzername* keine Spalte aus der CSV-Datei zugeordnet, wird der Benutzername automatisch aus dem Vornamen und dem Nachnamen generiert (<*Vorname*>.<*Nachname*>). Bei jedem weiteren Import wird der Benutzername erneut generiert und ggf. anhand von zusätzlich angegebenen Attributen einem bestehenden Benutzerkonto zugeordnet.

Abbildung 4.3. CSV-Import: Zuordnung der Benutzerattribute



Auf der letzten Seite des Assistenten werden zur Prüfung alle vorgesehenen Änderungsschritte in einer Tabelle angezeigt. Jede Zeile der Tabelle repräsentiert ein Benutzerkonto und enthält die folgenden Angaben:

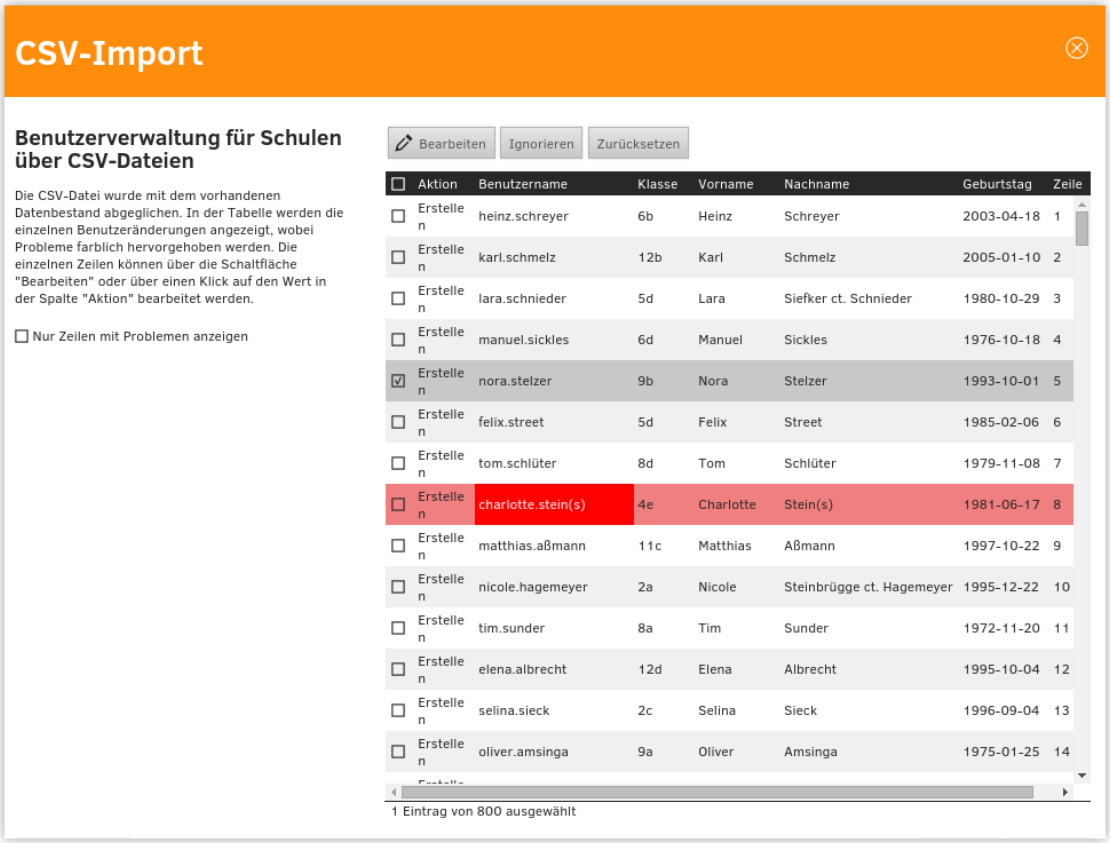
- den Benutzernamen (ggf. automatisch generiert, falls nicht zugeordnet),
- die zugeordneten Attribute aus der CSV-Datei,
- die vorgesehene **Aktion** für das Benutzerkonto, welche angibt, ob das betreffende Benutzerkonto neu angelegt werden soll (**Erstellen**), bereits existiert und modifiziert werden soll (**Ändern**) oder gelöscht werden soll (**Löschen**). Darüber hinaus können Einträge während des Imports auch manuell ausgelassen werden (**Ignorieren**).
- der Angabe der betreffenden Zeile in der CSV-Datei

Werden bei der automatischen Prüfung der CSV-Datei Unstimmigkeiten oder Probleme erkannt, werden die betreffenden Attributfelder farblich hervorgehoben:

- Gelbe Zellen weisen auf ungewöhnliche Änderungen hin (z.B. eine Änderung des Geburtsdatums). Die betreffenden Zeilen sollten manuell geprüft werden. Sie stellen jedoch kein Hindernis für einen Import dar.
- Rot markierte Zellen enthalten ein gravierendes Problem, wie z.B. die doppelte Vergabe eines Benutzernamens oder die ungültige Schreibweise eines Geburtsdatums. Probleme, die durch die roten Zellen angezeigt werden, müssen korrigiert werden (siehe unten), da ansonsten der Import verweigert wird. Alternativ kann die betroffene Zeile markiert und über die Schaltfläche **Ignorieren** komplett ignoriert werden.

Beim Verweilen des Mauszeigers über einer farblich markierten Zeile wird ein Tooltip mit näheren Informationen zu erkannten Problemen angezeigt. Über die Checkbox **Nur Zeilen mit Problemen anzeigen** kann die Anzeige auf Einträge mit gelb oder rot markierten Zellen beschränkt werden.

Abbildung 4.4. CSV-Import: Überprüfung der bevorstehenden Änderungen

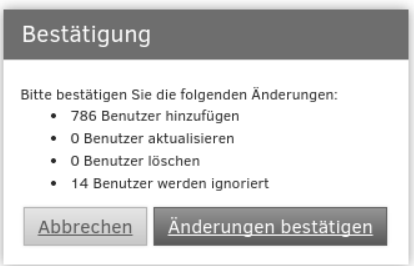


Um fehlerhafte Werte einer Zeile zu korrigieren, muss die betroffene Zeile zunächst ausgewählt und anschließend die Schaltfläche **Bearbeiten** angeklickt werden. Es öffnet sich ein Bearbeitungsdialog, in dem alle Werte einer Tabellenzeile angezeigt werden. Alternativ kann in der Tabelle mit einem Doppelklick auf die betreffende Zelle ebenfalls der Dialog zum Bearbeiten eines Eintrags geöffnet werden.

Über die Schaltfläche **Zurücksetzen** können nach einer Modifikation die markierten Zeilen wieder auf die Originalwerte aus der CSV-Datei zurückgesetzt werden.

Nach Abschluss der manuellen Prüfung und möglicher Korrekturen kann über die Schaltfläche **Weiter** eine Zusammenfassung über die bevorstehenden Änderungen im Verzeichnisdienst angezeigt werden (siehe Abbildung 4.5). Nach der Bestätigung der bevorstehenden Änderungen werden diese in den Verzeichnisdienst eingepflegt. Je nach Menge der zu importierenden Daten kann dies einen Moment dauern. Ein Fortschrittsbalken informiert über den aktuellen Fortschritt.

Abbildung 4.5. CSV-Import: Abschließende Zusammenfassung



Nach Abschluss des Imports wird eine kurze Rückmeldung zum Import angezeigt. Die angelegten bzw. geänderten Benutzerkonten stehen nach Abschluss der Verzeichnisdienstreplikation auf den betreffenden UCS@school-Systemen zur Verfügung.

4.4. Verwaltung von Schulklassen

Feedback

Auf dem Domaincontroller Master 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**.

4.4.1. Anlegen von Schulklassen

Feedback

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*). 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.

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.

4.4.2. Bearbeiten von Schulklassen

Feedback

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.

Anmerkung

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.

4.4.3. Löschen von Schulklassen

Feedback

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.

Anmerkung

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.

4.5. Verwaltung von Rechnern

Feedback

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.

4.5.1. Anlegen von Rechnerkonten

Feedback

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
- **Univention Corporate Client** ist nur verfügbar, wenn über das Univention App Center die Applikation *Univention Corporate Client* installiert wurde - siehe dazu auch Kapitel 12.

Auf der nächste Seite des Assistenten müssen **Name**, **IP-Adresse** und **MAC-Adresse** des neuen Rechnerkontos angegeben werden. 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.

Anmerkung

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.

4.5.2. Bearbeiten von Rechnerkonten

Feedback

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.

4.5.3. Löschen von Rechnerkonten

Feedback

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.

Kapitel 5. Verwaltung von Schulen über Importskripte

5.1. Pflege von Benutzerkonten für Schüler, Lehrer und Mitarbeiter 31
5.2. Import von Schulklassen 33
5.3. Vorgehen zum Schuljahreswechsel 34
5.4. Skriptbasierter Import von Netzwerken 35
5.5. Import von Rechnerkonten für Windows-PCs 35
5.5.1. Skriptbasierter Import von PCs 36
5.6. Konfiguration von Druckern an der Schule 37

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 Kapitel 4 beschrieben). Ergänzend hierzu gibt es Programme für die Kommandozeile, die auch eine automatisierte Pflege der UCS@school-Umgebung zulassen.

Achtung

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

5.1. Pflege von Benutzerkonten für Schüler, Lehrer und Mitarbeiter

Feedback

Die Verwaltung der Schüler-, Lehrer und Mitarbeiterdaten und deren Aktualisierung zum Schuljahreswechsel (Versetzungen, Schulabgänge etc.) erfolgt in der Regel durch die Schulverwaltung. Hierbei wird eine große Anzahl an Lösungen zur Datenpflege eingesetzt, die sich von Schulträger zu Schulträger unterscheidet.

Die Benutzerverwaltung von UCS@school ist darauf ausgelegt, dass die primäre Verwaltung der Schuldaten weiterhin durch die Schulverwaltung erfolgen kann. Diese Daten werden dann in eine Datei im CSV-Format exportiert und kommandozeilenbasiert in UCS@school importiert. Die einzelnen Felder der CSV-Datei sind durch ein Tabulatorzeichen zu trennen.

Für punktuelle Anpassungen - etwa ein Schulwechsel mitten im Schuljahr - besteht die Möglichkeit einzelne Schüler manuell zu bearbeiten. Dies wird in Abschnitt 4.2 beschrieben.

Der Import der Schuldaten ist bei Single- und Multi-Server-Umgebungen identisch.

Der Import von Benutzern erfolgt über das Skript `/usr/share/ucs-school-import/scripts/import_user`, das auf dem Domänencontroller Master als Benutzer `root` gestartet werden muss. Es erwartet den Namen einer CSV-Datei als ersten Parameter. Das Format der Eingabedatei ist wie folgt aufgebaut:

Tabelle 5.1. Aufbau der Datenzeilen für den Benutzer-Import

Feld	Beschreibung	Mögliche Werte	Beispiel
Aktion	Art der Benutzermodifikation	`A`=Hinzufügen, `M`=Modifizieren, `D`=Löschen	**`A`**
Benutzername	Der zum Login verwendete Benutzername	---	**`m.mustermann`**

Feld	Beschreibung	Mögliche Werte	Beispiel
Nachname	Der Nachname des Benutzers	---	`Mustermann`
Vorname	Der Vorname des Benutzers	---	`Michael`
OU	Die OU, unter der der Benutzer angelegt werden soll	---	`g123m`
Klasse	Name der Klasse des Benutzers; nur Lehrer können in mehreren Klassen vertreten sein!	---	`g123m-1A,g123m-1B, g123m-2A,g123m-4C`
Rechte	derzeit ungenutzt; das Feld sollte leer bleiben, so dass 2 Tabulator-Zeichen aufeinander folgen	---	
Email-Adresse	Mailadresse des Benutzers	---	`m.musterm@beispiel.edu`
(Lehrer)	Definiert, ob der Benutzer ein Lehrer ist	`0`=Kein Lehrer, `1`=Lehrer	`1`
(Aktiv)	Definiert, ob das Benutzerkonto beim Anlegen sofort aktiviert wird	`0`=nicht aktivieren, `1`=aktivieren	`1`
(Mitarbeiter)	Definiert, ob der Benutzer ein Mitarbeiter ist	`0`=Kein Mitarbeiter, `1`=Mitarbeiter	`0`

Ein Beispiel für eine Importdatei:

```
A  max   Meyer  Max     g123m  g123m-1A           max@schule.edu   0 1 0
M  m.we  Weber  Moritz  g123m  g123m-1A,g123m-2D  mw@schule.edu    1 1 0
D  a.la  Lang   Anke    g123m  g123m-4C           a.la@schule.edu  1 1 1
```

Über das Feld *Aktion* kann die Art der Benutzermodifikation gesteuert werden. Folgende Aktionen sind definiert:

Aktion	Beschreibung
A	Hinzufügen
M	Modifizieren
D	Löschen

Auch beim Löschen (Aktion `D`) müssen gültige Werte übergeben werden.

Die Angabe von Klassen bezieht sich bei Schülern in der Regel auf eine einzelne Klasse. Lehrer können dagegen in mehreren Klassen vertreten sein. Diese sollten auch angegeben werden (kommasepariert), damit die Benutzerkonten der Lehrer automatisch in die jeweilige Klassengruppe eingetragen werden und sie somit auch Zugriff auf die jeweilige Dateifreigabe der Klasse erhalten. Bei Mitarbeitern ist das Feld Klasse leer zu lassen.

Anmerkung

Bei der Angabe von Schulklassen ist zu beachten, dass die Klassennamen domänenweit eindeutig sein müssen. Das heißt, eine Klasse *1A* kann nicht in mehreren OUs verwendet werden. Bei der Erstellung von Klassen über das UMC-Modul *Klassen (Schulen)* wird daher automatisch die OU und ein Bindestrich dem Klassennamen als Präfix vorangestellt. Dieses Vorgehen wird auch für den Import auf der Kommandozeile empfohlen.

Die optionalen Felder *Lehrer* und *Mitarbeiter* bestimmen die Rolle des Benutzers im System. Werden die Werte nicht angegeben, so wird der Benutzer mit der Rolle Schüler angelegt. Es ist möglich einem Benutzer sowohl die Rollen Lehrer und Mitarbeiter zu geben.

Über das optionale Feld *Aktiv* wird gesteuert, ob das Benutzerkonto aktiviert werden soll. Ist kein Wert angegeben, wird das Konto automatisch aktiviert.

Die Benutzerkonten werden mit zufälligen, unbekannten Passwörtern initialisiert. Mehrere Personengruppen können die Konten anschließend freischalten:

- Das Konto eines Schuladministrators kann durch Benutzer der Gruppe `Domain Admins` in der Univention Management Console erstellt und modifiziert werden.
- Die Konten von Mitarbeitern können durch Benutzer der Gruppe `Domain Admins` in der Univention Management Console durch die Vergabe eines Passworts freigeschaltet werden.
- Die Konten von Lehrern können durch den Schuladministrator über das Modul **Passwörter (Schüler)** durch die Vergabe eines Passworts freigeschaltet werden.
- Die Konten von Schülern können durch Lehrer über das Modul **Passwörter (Lehrer)** klassenweise durch die Vergabe eines Passworts freigeschaltet werden.

Mit den folgenden Univention Configuration Registry-Variablen kann für Schüler, Lehrer, Schuladministratoren und Mitarbeiter eine UMC-Richtlinie zugewiesen werden, die festlegt, welche UMC-Module bei einer Anmeldung der entsprechenden Benutzergruppe angezeigt werden. Hierbei muss der LDAP-DN (*Distinguished Name*) der Richtlinie angegeben werden.

- `ucsschool/ldap/default/policy/umc/pupils` gilt für Anmeldungen von Schülern
- `ucsschool/ldap/default/policy/umc/teachers` gilt für Anmeldungen von Lehrern
- `ucsschool/ldap/default/policy/umc/admins` gilt für Anmeldungen von Schuladministratoren
- `ucsschool/ldap/default/policy/umc/staff` gilt für Anmeldungen von Mitarbeitern

Wenn die UCR-Variablen auf den Wert `None` gesetzt sind, wird für den jeweiligen Benutzertyp keine Richtlinie verknüpft. Es müssen dann eigene Richtlinien an die Container gebunden werden.

Achtung

Bei der Verwendung von Samba 4 benötigt der S4-Connector einige Zeit, um die Benutzer in die Samba 4-Benutzerdatenbank zu synchronisieren. Je nach Menge der Importdaten und der verwendeten Hardware kann die Synchronisation einige Stunden benötigen. Währenddessen kann es zu Verzögerungen in der Synchronisation von nicht-import-abhängigen Änderungen im LDAP oder Active Directory kommen (z.B. interaktive Änderung von Benutzerpasswörtern).

5.2. Import von Schulklassen

Feedback

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
gym123-2A
gym123-Igel
```

Der Import von Benutzern erfolgt über das Skript `/usr/share/ucs-school-import/scripts/import_group`, das auf dem Domänencontroller Master 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:

Tabelle 5.2. 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	---	**`g123m`**
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
```

5.3. Vorgehen zum Schuljahreswechsel

Feedback

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 Abschnitt 5.1). 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 Domänencontroller Master 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.

   ### Anmerkung

   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 Abschnitt 5.1).

4. Eine Liste aller Neuzugänge wird aus der Schulverwaltungssoftware exportiert und über das Import-Skript importiert (Aktion A, siehe Abschnitt 5.1).

5.4. Skriptbasierter Import von Netzwerken

Feedback

Durch den Import von Netzwerken können IP-Subnetze im LDAP angelegt werden und diverse Voreinstellungen wie Adressen von Router, DNS-Server etc. für diese Subnetze konfiguriert werden. Darunter fällt z.B. auch ein Adressbereich aus dem für neuangelegte Systeme automatisch IP-Adressen vergeben werden können.

Das Importieren von Subnetzen empfiehlt sich in größeren UCS@school-Umgebungen. Kleinere Umgebungen können diesen Schritt häufig überspringen, da fehlende Netzwerke beim Import von Rechnerkonten automatisch angelegt werden.

Netzwerke können derzeit nur auf der Kommandozeile über das Skript `/usr/share/ucs-school-import/scripts/import_networks` importiert werden. Das Skript muss auf dem Domänencontroller Master als Benutzer `root` aufgerufen werden. Das Format der Import-Datei ist wie folgt aufgebaut:

Feld	**Beschreibung**	**Mögliche Werte**
OU	OU des zu modifizierenden Netzwerks	**`g123m`**
Netzwerk	Netzwerk und Subnetzmaske	**`10.0.5.0/ 255.255.255.0`**
(IP-Adress-Bereich)	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`**

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
```

Wird für das Feld *Netzwerk* keine Netzmaske angegeben, so wird automatisch die Netzmaske `255.255.255.0` verwendet. Sollte der *IP-Adressbereich* nicht explizit angegeben worden sein, wird der Bereich *X.Y.Z.20-X.Y.Z.250* verwendet.

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`.

5.5. Import von Rechnerkonten für Windows-PCs

Feedback

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 Windows-PCs über den im UCS-Handbuch beschriebenen Weg der Domäne beitreten.

5.5.1. Skriptbasierter Import von PCs

Feedback

Der Import mehrerer PCs erfolgt über das Skript `/usr/share/ucs-school-import/scripts/import_computer`, das auf dem Domänencontroller Master 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
Rechnertyp	Typ des Rechnerobjektes	`ipmanagedclient`, `macos`, `ucc`, `windows`	**`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`**
(Zone)	Optionale Zone	`edukativ`, `verwaltung`	**`edukativ`**

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
ipmanagedclient  printerg123m-01  10:00:ee:ff:cc:04  g123m  10.0.5.250
ucc              uccg123m-01      10:00:ee:ff:cd:e2  g123m  10.0.5.10
```

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.

5.6. Konfiguration von Druckern an der Schule

Feedback

Der Import der Drucker kann skriptbasiert über das Skript `/usr/share/ucs-school-import/scripts/import_printer` erfolgen, das auf dem Domänencontroller Master 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 Druckermodifkation	`A`=Hinzufügen, `M`=Modifizieren, `D`=Löschen	**`A`**
OU	OU, in der das Druckerobjekt modifiziert werden soll	---	**`g123m`**
Druckserver	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 im Druckdienste-Kapitel des UCS-Handbuchs beschrieben.

Kapitel 6. Erweiterte Konfiguration

6.1. Einrichtung der Druckmoderation 39
6.1.1. Anlegen eines PDF-Druckers für die Druckermoderation 39
6.2. Windows-spezifische Benutzereinstellungen 40
6.3. Anlegen von Freigaben 41
6.4. Lehrerzugriff auf Benutzerfreigaben 41
6.5. Anlegen von Benutzerkonten für Schuladministratoren 42
6.6. Konfiguration der Helpdesk-Kontaktadresse 42

6.1. Einrichtung der Druckmoderation

Feedback

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 Abschnitt 5.6 beschrieben, Druckfreigaben für die zu verwendenden, physikalisch existierenden Drucker angelegt werden.

An den Druckerfreigabeobjekten (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 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.

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 können auch die Druckmodi *Drucken deaktiviert* und *Drucken möglich* ausgewählt werden, die das Drucken von den Rechnern des Computerraums entweder vollständig untersagen oder - unabhängig der gemachten Voreinstellungen - auf allen physikalischen Druckern erlauben.

6.1.1. Anlegen eines PDF-Druckers für die Druckermoderation

Feedback

Druckerfreigaben werden, wie in einer Standard-UCS-Installation, über das UMC-Modul **Drucker** auf dem Domänencontroller Master angelegt. Weiterführende Dokumentation findet sich im Druckdienste-Kapitel des UCS-Handbuchs [ucs-handbuch].

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 Joinskripte.

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 Joinskript *80ucs-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`**

6.2. Windows-spezifische Benutzereinstellungen

Feedback

Neben den in Abschnitt 4.2 und Abschnitt 5.1 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.

  ### Anmerkung

  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.

- Darüber hinaus wird auch automatisch der Pfad zum Heimatverzeichnis des Benutzers gesetzt. In einer Single-Server-Umgebung wird automatisch der Domaincontroller Master 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 Abschnitt 4.1.2). Der dort definierte Dateiserver wird beim Anlegen eines Benutzers ausgelesen und der UNC-Pfad am Benutzerobjekt entsprechend gesetzt (Beispiel: `\\server3.example.com\benutzer123`).

Anmerkung

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.

6.3. Anlegen von Freigaben

Feedback

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/markt-platz` 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 Domänencontroller Master angelegt. Weiterführende Dokumentation findet sich im Freigaben-Kapitel des UCS-Handbuchs [ucs-handbuch].

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.

6.4. Lehrerzugriff auf Benutzerfreigaben

Feedback

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 Joinskript 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`.

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 Domänencontroller Master 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.

6.5. Anlegen von Benutzerkonten für Schuladministratoren

Feedback

Benutzerkonten von Lehrern können durch eine zusätzliche Gruppenmitgliedschaft zu Schuladministratoren umgewandelt werden. Sie unterliegen dann jedoch der Einschränkung, dass die Benutzerkonten der Lehrer-Schuladministratoren nur auf den edukativen Schulserver und nicht auf den Schulserver des Verwaltungsnetzes repliziert werden.

Die zusätzliche Gruppenmitgliedschaft muss manuell über das UMC-Modul **Benutzer** auf dem Domänencontroller Master hinzugefügt werden. Auf dem Reiter **Gruppen** muss das Benutzerkonto in die Gruppe `admins-`*`OU`* (bei der OU *gym17* ist dies die Gruppe `admins-gym17`) aufgenommen werden.

Soll das Benutzerkonten des Schuladministrators auch auf den Systemen des Verwaltungsnetzes verfügbar sein, so reicht es nicht aus, die Gruppenmitgliedschaft zu ändern. Es muss manuell ein neues Benutzerkonto über das UMC-Modul **Benutzer** auf dem Domänencontroller Master angelegt werden.

Die Benutzerkonten der Schuladministratoren müssen unterhalb der OU der Schule im Container `cn=admins,cn=users` angelegt werden. Die Auswahl findet mit der Option **Container** beim Anlegen eines Benutzers statt. Bei einer OU *gym17* muss beispielsweise der Container **gym17/users/admins** ausgewählt werden.

Der Benutzer muss außerdem im Reiter **Gruppen** in die Gruppe `admins-`*`OU`*, also z.B. `admins-gym17` aufgenommen werden.

Sollte der 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 Abschnitt 6.2).

6.6. Konfiguration der Helpdesk-Kontaktadresse

Feedback

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-Mail-Adresse des zuständigen Helpdesk-Teams gesetzt werden.

Kapitel 7. Integration und Verwaltung von Microsoft Windows-Clients

7.1. Anmeldedienste mit Samba 43
7.2. Server für Dateifreigaben 44
7.3. Netlogon-Skripte für Samba4-Umgebung 44
7.4. iTALC-Installation auf Windows-Clients 45

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 Abschnitt 7.1.

Die Netzkonfiguration der Clients kann zentral über in UCS integrierte DNS- und DHCP-Dienste durchgeführt werden. Weitere Hinweise finden sich in Abschnitt 5.5.1.

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 Abschnitt 6.2.

Auf den Windows-Clients der Schüler kann die Software *iTALC* 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 iTALC wird in Abschnitt 7.4 beschrieben.

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

7.1. Anmeldedienste mit Samba

Feedback

In Univention Corporate Server 3.x stehen zwei verschiedene Samba-Varianten zur Auswahl:

- *Samba 3* implementiert Domänendienste auf Basis der Domänen-Technologie von Microsoft Windows NT. Samba 3 ist die aktuelle stabile und bewährte Haupt-Release-Serie des Samba-Projekts und ist seit vielen Jahren in UCS integriert.
- *Samba 4* ist die nächste Generation der Samba-Suite. Die wichtigste Neuerung von Samba 4 besteht in der Unterstützung von Domänen-, Verzeichnis- und Authentifizierungsdiensten, die kompatibel zu Microsoft Active Directory sind. Mit Samba 4 lassen sich deswegen Active Directory-kompatible Windows-Domänen aufbauen. Diese ermöglichen auch die Verwendung der von Microsoft bereit gestellten Werkzeuge beispielsweise für die Verwaltung von Benutzern oder Gruppenrichtlinien (GPOs). Die aktuell vom Samba-Projekt veröffentlichten Versionen von Samba 4 unterliegen in der Weiterentwicklung noch stärkeren Änderungen als Samba 3. 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. Parallel dazu wurde für UCS Samba 3 mit Samba 4 integriert. Somit werden auch bei Verwendung der Active Directory kompatiblen Domänendienste die erprobten Datei- und Druckdienste aus Samba 3 verwendet.

Achtung

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, 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 Schulserver (bzw. dem Domänencontroller Master bei Single-Server-Umgebungen) 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
```

Bei Neuinstallationen von UCS@school wird standardmäßig Samba 4 empfohlen. Umgebungen, die von einer Vorversion aktualisiert wurden, können von Samba 3 auf Samba 4 migriert werden. Das dafür notwendige Vorgehen ist unter der folgenden URI dokumentiert:

http://wiki.univention.de/index.php?title=UCS%40school_Samba_3_to_Samba_4_Migration

Weiterführende Hinweise zur Konfiguration von Samba finden sich im UCS-Handbuch [ucs-handbuch].

7.2. Server für Dateifreigaben

Feedback

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 Domänencontroller Master als Dateiserver konfiguriert.

7.3. Netlogon-Skripte für Samba4-Umgebung

Feedback

In UCS-Umgebungen mit mehreren Samba4-Domänencontrollern werden in der Standardeinstellung alle Dateien der `NETLOGON`-Dateifreigabe automatisch (durch die `SYSVOL`-Replikation) zwischen allen Samba4-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 Samba4-Domänencontrollern gesetzt werden. Dies kann z.B. in der UMC über eine UCR-Richtlinien global definiert werden. Nach der Änderung müssen die Dienste `samba4` und `univention-directory-listener` neu gestartet werden:

```
invoke-rc.d samba4 restart
invoke-rc.d univention-directory-listener restart
```

7.4. iTALC-Installation auf Windows-Clients

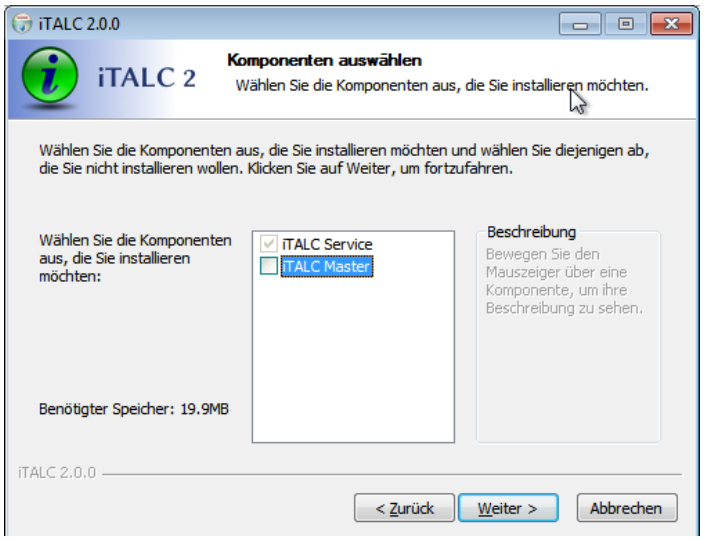
Feedback

Für die Kontrolle und Steuerung der Schüler-PCs integriert UCS@school optional die Software iTALC. Dieses Kapitel beschreibt die Installation von iTALC auf den Schüler-PCs. Die Administration durch die Lehrkräfte ist in der UCS@school-Lehrerdokumentation [ucs-school-teacher] beschrieben.

Für die Nutzung der Rechnerüberwachungs- und Präsentationsfunktionen in der Computerraumverwaltung (siehe Abschnitt 8.1) wird vorausgesetzt, dass auf den Windows-Clients die Software iTALC installiert wurde.

Seit UCS@school 3.1 R2 sind Windows-Binärpakete für die Open Source-Software iTALC in UCS@school enthalten. Die Binärpakete sind direkt über die Samba-Freigabe *iTALC-Installation* abruf- und installierbar. Alternativ finden sich die Installationdateien für 32- und 64bit-Versionen von iTALC auf dem Schulserver im Verzeichnis `/usr/share/italc-windows/`. Interoperabilitätstests zwischen UCS@school und iTALC wurden ausschließlich mit der von UCS@school mitgelieferten iTALC-Version unter Windows XP und Windows 7 (32 und 64 Bit) durchgeführt.

Abbildung 7.1. iTALC-Installation: Auswahl der Komponenten



iTALC bringt ein Installationsprogramm mit, das durch alle notwendigen Schritte führt. Während der Installation sollte nur der *iTALC Service* installiert und der *iTALC Master* abgewählt werden.

Nach der Installation von iTALC auf dem Windows-Client muss der öffentliche Schlüssel importiert werden, damit der Schulserver Zugriff auf das installierte iTALC-Backend erhält. Dies erfolgt durch Aufruf der iTALC Management Console unter **Authentifizierung -> Schlüsseldatei-Assistent starten -> Öffentlichen Schlüssel importieren (Client-Computer) -> Lehrer**. Unter **Bitte geben Sie den Ort des öffentlichen Zugriffsschlüssels an, der importiert werden soll** ist der iTALC-Schlüssel des Schulservers anzugeben. Der Schlüssel wird automatisch auf der SYSVOL-Freigabe des Schulservers unter dem Namen der Schuldomäne unter `scripts` abgelegt (Kommt Samba 3 zum Einsatz, wird der Schlüssel auf der Netlogon-Freigabe abgelegt). Der Dateiname der Schlüsseldatei enthält den Namen des Schulservers für den sie generiert wurde, um Namenskonflikte auf der SYSVOL-Freigabe bei der Verwendung von Samba 4

zu vermeiden. Damit der iTALC-Assistent die Schlüsseldatei selbständig erkennt, sollte die Datei `italc-key_`*`SERVERNAME`*`.pub.key.txt` verwendet werden.

Außerdem sollte auf den Windows-Clients sichergestellt werden, dass die installierte System-Firewall so konfiguriert ist, dass Port *11100* nicht blockiert wird. Dies ist Voraussetzung für eine funktionierende Umgebung, da iTALC diesen Port für die Kommunikation mit dem Schulserver bzw. anderen Computern verwendet.

Kapitel 8. Übersicht über die schulspezifischen Anwendungen

8.1. Modulübersicht 47

8.1. Modulübersicht

Feedback

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 im separaten Handbuch für Lehrer [ucs-school-teacher].

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

- *Passwörter (Schüler)* erlaubt Lehrern das Zurücksetzen von Schüler-Passwörtern. Die bestehenden Schüler-Passwörter können aus Sicherheitsgründen nicht ausgelesen werden; wenn Schüler ihr Passwort vergessen, muss ein neues Passwort vergeben werden. Schuladministratoren dürfen außerdem die Passwörter von Lehrern zurücksetzen.

- Das Modul *Computerraum* erlaubt die Kontrolle der Schüler-PCs und des Internetzugangs während einer Schulstunde. Der Internetzugang kann gesperrt oder freigegeben werden und einzelne Internetseiten können gezielt freigegeben werden. Wenn eine entsprechende Software (iTALC) 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 Bildschiminhalt eines PCs auf andere Systeme übertragen werden. Dies erlaubt es Lehrern, auch ohne einen Beamer Präsentationen durchzuführen.

- 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-Mail-Anfrage stellen. Die Konfiguration des Helpdesk-Moduls wird in Abschnitt 6.6 beschrieben.

- 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.

- 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.

- 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.

- 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.
- Das Modul *Unterrichtszeiten* erlaubt es, die Zeiträume der jeweiligen Schulstunden pro Schule zu definieren.
- 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.
- 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 Kapitel 9 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 der Funktion **Internetregeln definieren** können die Regeln verwaltet werden.

Kapitel 9. Web-Proxy auf den Schulservern

9.1. Einbindung von externen Blacklisten 49

In der Grundeinstellung läuft auf jedem Schulserver (bzw. im Single-Server-Betrieb auf dem Domänencontroller Master) ein Proxy-Server auf Basis von Squid im Zusammenspiel mit squidGuard. Der Proxy erlaubt Lehrern in Schulstunden den Zugriff auf einzelne Webseiten zu beschränken oder auch generell bestimmte Webseiten zu sperren. Dies ist in der UCS@school-Lehrerdokumentation [ucs-school-teacher] beschrieben.

Der Proxyserver muss zwingend auf dem jeweiligen Schulserver betrieben werden.

Die Proxykonfiguration wird in der Grundeinstellung durch DHCP verteilt, diese Einstellung 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 Konfigurationparameter zusammengestellt. Die PAC-Datei eines Schulservers steht unter der folgenden URL bereit:

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

Im Internet Explorer 8 wird die PAC-Datei beispielsweise unter **Internetoptionen -> Reiter Verbindungen -> LAN-Einstellungen -> Automatisches Konfigurationsskript verwendet** zugewiesen.

In Firefox 10 kann die PAC-Datei im Menü unter **Bearbeiten -> Einstellungen -> Erweitert -> Netzwerk -> Verbindungen -> Einstellungen -> Automatische Proxy-Konfigurations-URL** zugewiesen werden.

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

9.1. Einbindung von externen Blacklisten

Feedback

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 zwei UCR-Variablen: `proxy/filter/global/blacklists/domains` und `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.

Anmerkung

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.

Anmerkung

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 10. Authentifizierung des WLAN-Zugriffs über RADIUS

10.1. Installation und Konfiguration des RADIUS-Servers 51
10.2. Konfiguration der *Access Points* 51
10.3. Konfiguration der zugreifenden Clients 51
10.4. Freigabe des WLAN-Zugriffs in der Univention Management Console 52
10.5. Fehlersuche 52

RADIUS ist ein Authentifizierungsprotokoll für Rechner 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* 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.

10.1. Installation und Konfiguration des RADIUS-Servers

Feedback

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.

Nun müssen alle *Access Points* der Schule in der Konfigurationsdatei `/etc/freeradius/clients.conf` registriert werden. 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 für einen *Access Point*:

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

10.2. Konfiguration der *Access Points*

Feedback

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 `/etc/freeradius/clients.conf` hinterlegte Passwort

10.3. Konfiguration der zugreifenden Clients

Feedback

Der zugreifende Client muss zunächst das UCS-Wurzelzertifikat importieren. Es kann z.B. von der Startseite des Domänencontroller Master 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. Im Univention Wiki findet sich eine exemplarische Schritt-für-Schritt-Anleitung für die Einrichtung unter Windows XP: http://wiki.univention.de/index.php?title=Einrichtung-WLAN-Authentifizierung-WinXP, sowie für die Einrichtung unter Windows 7: http://wiki.univention.de/index.php?title=Einrichtung-WLAN-Authentifizierung-Win7.

10.4. Freigabe des WLAN-Zugriffs in der Univention Management Console

Feedback

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 der UCS@school-Lehrerdokumentation [ucs-school-teacher].

10.5. Fehlersuche

Feedback

Im Fehlerfall sollte die Logdatei `/var/log/freeradius/radius.log` geprüft werden. Erfolgreiche Logins führen zu einem Logeintrag `Auth: Login OK` und eine fehlgeschlagene Authentifizierung beispielsweise zu `Auth: Login incorrect`.

Kapitel 11. Klassenarbeitsmodus

11.1. Technische Hintergründe 53
11.2. Konfiguration 54
11.3. Beispiele für Gruppenrichtlinien 55
11.3.1. Generelle Hinweise zu Gruppenrichtlinien und Administrativen Vorlagen 56
11.3.2. Windows-Anmeldung im Prüfungsraum auf Mitglieder der Klassenarbeitsgruppe beschränken 56
11.3.2.1. Anwendungsbereich der GPO auf Klassenarbeitscomputer einschränken 57
11.3.2.2. Einschränkung der Windows-Anmeldung auf Klassenarbeitsbenutzerkonten und Lehrer 57
11.3.3. Zugriff auf USB-Speicher und Wechselmedien einschränken 58
11.3.3.1. Zugriff auf USB-Speicher an Windows XP einschränken 58
11.3.3.2. Installation neuer Gerätetreiber für USB-Speicher an Windows XP verbieten..... 58
11.3.3.3. Zugriff auf USB-Speicher an Windows 7 einschränken 59
11.3.3.4. Installation neuer Gerätetreiber für USB-Speicher an Windows 7 Clients verbieten 59
11.3.4. Vorgabe von Proxy-Einstellungen für den Internetzugriff 60
11.3.4.1. Proxy-Vorgabe für den Internet Explorer 60
11.3.4.2. Sperrung der Proxyeinstellung für den Internet Explorer 60
11.3.4.3. Proxy-Vorgabe für Google Chrome 61
11.3.4.4. Proxy-Vorgabe für Mozilla Firefox 61
11.3.5. Zugriff auf bestimmte Programme einschränken 62
11.3.5.1. Kommandoeingabeaufforderung deaktivieren 62
11.3.5.2. Zugriff auf Windows-Registry-Editor deaktivieren 63
11.3.5.3. Konfiguration von *Software Restriction Policies* (SRP) 63
11.3.6. Verwendung temporärer Benutzerprofil-Kopien 64

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 Abschnitt 11.1 und mögliche Konfigurationsschnittstellen in Abschnitt 11.2 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 Abschnitt 11.3 beispielhaft beschrieben.

11.1. Technische Hintergründe

Feedback

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 Loginname für das Klassenarbeitskonto setzt sich aus einem festgelegten Präfix (standardmäßig `exam-`) und dem normalen Benutzernamen zusammen. Bspw. 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.

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 Abschnitt 11.3).

Anmerkung

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, empfehlen wir, bspw. ein optisch klar zu unterscheidendes Hintergrundbild über die Richtlinien zuzuweisen.

11.2. Konfiguration

Feedback

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 Domänencontroller Master 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.
- `ucsschool/ldap/default/container/exam` ist der Name 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.

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 standardmäßig der alphabetisch erste Raum ausgewählt.

- `ucsschool/exam/default/shares` gibt den vorausgewählten Freigabezugriff für eine neue Klassenarbeit an. Mögliche Werte sind `all` für Zugriff auf alle Freigaben ohne Einschränkungen sowie `home` für eingeschränkten Zugriff auf lediglich das Heimatverzeichnis des (Klassenarbeits-)Benutzerkonto. 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) oder `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) oder `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) oder `false` (Auswahlkästchen nicht vorausgewählt).

11.3. Beispiele für Gruppenrichtlinien

Feedback

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 werden 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 Computer-Konten 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.

Anmerkung

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.“ [1]

11.3.1. Generelle Hinweise zu Gruppenrichtlinien und Administrativen Vorlagen

Feedback

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.

11.3.2. Windows-Anmeldung im Prüfungsraum auf Mitglieder der Klassenarbeitsgruppe beschränken

Feedback

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 einzuschrän-

[1] http://technet.microsoft.com/de-de/library/cc785665(v=ws.10).aspx

ken, 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.

11.3.2.1. Anwendungsbereich der GPO auf Klassenarbeitscomputer einschränken

Feedback

- In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
- In der Baumdarstellung der Gruppenrichtlinienverwaltung die Gruppenrichtlinie anklicken.
- Auf dem geöffneten Reiter *Bereich* im Abschnitt *Sicherheitsfilterung* die Schaltfläche *Hinzufügen* betätigen.
- 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.
- Auf dem geöffneten Reiter *Bereich* im Abschnitt *Sicherheitsfilterung* die Gruppe *Authenticated Users* auswählen und die Schaltfläche *Entfernen* betätigen.

11.3.2.2. Einschränkung der Windows-Anmeldung auf Klassenarbeitsbenutzerkonten und Lehrer

Feedback

- In der Gruppenrichtlinienverwaltung das Gruppenrichtlinienobjekt zur Bearbeitung öffnen (Kontextmenü des GPO in der Baumdarstellung).
- Im neu geöffneten Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:

  Computerkonfiguration -> Richtlinien -> Windows-Einstellungen -> Sicherheitseinstellungen -> Lokale Richtlinien -> Zuweisen von Benutzerrechten
- Im neu geöffneten Richtlinien-Dialog *Eigenschaften von Lokal anmelden zulassen* auf dem Reiter *Sicherheitsrichtlinie* die Option *Diese Richtlinieneinstellung definieren* aktivieren.
- Dann die Schaltfläche *Benutzer oder Gruppe hinzufügen* betätigen.
- In das Eingabefeld *Benutzer und Gruppennamen* den Namen **`Administratoren`** eintragen und den Dialog mit *OK* schließen.
- Erneut die Schaltfläche *Benutzer oder Gruppe hinzufügen* betätigen.
- Im neu geöffneten Dialog die Schaltfläche *Durchsuchen* betätigen.
- 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.
- Den Dialog *Benutzer oder Gruppe hinzufügen* ebenfalls mit *OK* schließen.
- Erneut die Schaltfläche *Benutzer oder Gruppe hinzufügen* betätigen.

- Im neu geöffneten Dialog die Schaltfläche *Durchsuchen* betätigen.
- 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.
- Den Dialog *Benutzer oder Gruppe hinzufügen* ebenfalls mit *OK* schließen.
- Den Richtlinien-Dialog *Eigenschaften von Lokal anmelden zulassen* mit *OK* schließen.

11.3.3. Zugriff auf USB-Speicher und Wechselmedien einschränken

Feedback

Zur Einschränkung des Zugriffs auf USB-Speicher und Wechselmedien sind je nach Windowsversion zwei Fälle zu beachten: einerseits die Einschränkung der Benutzung bereits installierter Gerätetreiber und andererseits 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.

Anmerkung

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:

- http://technet.microsoft.com/de-de/library/hh125922%28v=ws.10%29.aspx.

11.3.3.1. Zugriff auf USB-Speicher an Windows XP einschränken

Feedback

Diese Richtlinie wird über eine Administrative Vorlage (ADMX) definiert, die in Microsoft Knowledgebase Artikel 555324. [2] 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 Abschnitt 11.3.1).

- In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:

  Computerkonfiguration -> Richtlinien -> Administrative Vorlagen -> Spezielle Einstellungen -> Treiber einschränken

- Richtlinie *USB Sperren* öffnen, *Aktiviert* auswählen und mit *OK* bestätigen.

Anmerkung

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

11.3.3.2. Installation neuer Gerätetreiber für USB-Speicher an Windows XP verbieten

Feedback

Diese Richtlinie definiert eingeschränkte Dateisystemberechtigungen gemäß Microsoft Knowledgebase Artikel 823732 [3].

[2] http://support.microsoft.com/kb/555324
[3] http://support.microsoft.com/kb/823732

- In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:

  Computerkonfiguration -> Richtlinien -> Windows-Einstellungen -> Sicherheitseinstellungen -> Dateisystem
- Rechtsklick auf *Datei hinzufügen...*
- Das Verzeichnis `C:\Windows\Inf` ansteuern und dort die Datei `usbstor.inf` auswählen und mit *OK* bestätigen (ggf. wird die Dateiendung `.inf` nicht mit angezeigt).
- In dem neu geöffneten Dialog *Datenbanksicherheit für ...* in der oberen Liste *Gruppen- oder Benutzernamen* die Schaltfläche *Hinzufügen* betätigen und den Namen der Klassenarbeitsgruppe hinzufügen,
- In der darunter angezeigten Liste *Berechtigungen für ...* in der Zeile *Vollzugriff*, Spalte *Verweigern* ein Häkchen setzen und mit *OK* bestätigen.
- Den Dialog *Datenbanksicherheit für ...* mit *OK* schließen.
- Das neue Dialogfenster *Windows-Sicherheit* mit *Ja* bestätigen.
- Das neue Dialogfenster *Objekt hinzufügen* mit *OK* schließen.
- Analog sollten Einstellungen für `%SystemRoot%\inf\usbstor.pnf` und `%SystemRoot%\system32\drivers\usbstor.sys` definiert werden.

11.3.3.3. Zugriff auf USB-Speicher an Windows 7 einschränken

Feedback

- In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:

  Benutzerkonfiguration -> Richtlinien -> Administrative Vorlagen -> System -> Wechselmedienzugriff
- Z.B. Richtlinie *Wechseldatenträger: Lesezugriff verweigern* öffnen, *Aktiviert* auswählen und mit *OK* bestätigen.

Anmerkung

Weitere Informationen zu diesem Thema liefert z.B. http://technet.microsoft.com/de-de/library/cc771759%28v=ws.10%29.aspx.

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

Feedback

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.

- In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:

Computerkonfiguration -> Richtlinien -> Administrative Vorlagen -> System -> Geräteinstallation -> Einschränkungen bei der Geräteinstallation

- Hier kann die Installation von Treibern für bestimmte Geräteklassen, Geräte-IDs oder alle Wechselgeräte eingeschränkt werden.
- 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.

Anmerkung

Weitere Informationen zu diesem Thema liefert z.B. http://technet.microsoft.com/de-de/library/cc731387%28v=ws.10%29.aspx.

11.3.4. Vorgabe von Proxy-Einstellungen für den Internetzugriff

Feedback

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 Benutzer-Zugriffs auf eben diese Einstellungen sinnvoll. Dazu gibt es zwei unterschiedliche Ansätze: Im Fall des Internet Explorers bietet die Administrative Vorlage die Möglichkeit, das entsprechende Einstellungsfenster zu sperren. 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 die beiden letztgenannten Browser ist es daher wichtig darauf zu achten, die Einstellungen, wo nötig, im Zweig *Computerkonfiguration* des Gruppenrichtlinieneditors statt im Zweig *Benutzerkonfiguration* zu treffen.

11.3.4.1. Proxy-Vorgabe für den Internet Explorer

Feedback

- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:

  Benutzerkonfiguration -> Richtlinien -> Windows-Einstellungen -> Internet Explorer-Wartung -> Verbindung

- Richtlinie *Proxyeinstellungen* öffnen, *Aktiviert* auswählen und bestätigen.
- Proxyadresse für *HTTP* sowie *Secure* und das entsprechende *Port*-Feld ausfüllen (Wert der Univention Configuration Registry-Variable `squid/httpport`, Standard 3128)
- Ggf. *Für alle Adressen denselben Proxyserver verwenden* aktivieren.

11.3.4.2. Sperrung der Proxyeinstellung für den Internet Explorer

Feedback

- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:

  Computerkonfiguration -> Richtlinien -> Administrative Vorlagen: Vom zentralen Computer abgerufene Richtliniendefinitionen (ADMX-Dateien) -> Windows-Komponenten -> Internet Explorer -> Internetsystemsteuerung

- Richtlinie *Verbindungsseite deaktivieren* öffnen und *Aktiviert* auswählen und bestätigen.

11.3.4.3. Proxy-Vorgabe für Google Chrome

Feedback

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.

- In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:

  Computerkonfiguration -> Richtlinien -> Administrative Vorlagen: Vom zentralen Computer abgerufene Richtliniendefinitionen (ADMX-Dateien) -> Google -> Google Chrome -> Proxy-Server
- Richtlinie *Auswählen, wie Proxy-Server-Einstellungen angegeben werden* öffnen und *Aktiviert* auswählen,
- Im Dropdown *System-Proxy-Einstellungen verwenden* auswählen und bestätigen.

11.3.4.4. Proxy-Vorgabe für Mozilla Firefox

Feedback

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.

- In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:

  Computerkonfiguration -> Richtlinien -> Administrative Vorlagen: Vom zentralen Computer abgerufene Richtliniendefinitionen (ADMX-Dateien) -> Mozilla Firefox Locked Settings -> General
- Richtlinie *Proxy Settings* öffnen und *Aktiviert* auswählen,
- Im Dropdown *Preference State* die Einstellung *Locked* auswählen,
- Im Dropdown *Proxy Setting* die Einstellung *Manual Proxy Configuration* auswählen,
- Im Feld *Proxy Setting* die Einstellung *Manual Setting - HTTP Proxy* eintragen,
- Im Feld *HTTP Proxy Port* den Proxy Port eintragen (Wert der Univention Configuration Registry-Variable `squid/httpport`, Standard 3128)
- 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.

- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:

  Computerkonfiguration -> Windows-Einstellungen -> Skripts (Start/Herunterfahren)

- Richtlinie *Starten* öffnen,
- Im Dialog *Eigenschaften von Starten* auf dem Reiter *Skripts* die Schaltfläche *Dateien anzeigen* betätigen,
- In das vom automatisch geöffneten Windows Explorer angezeigte (leere) Verzeichnis (`Machine\Scripts\Startup` im betreffenden GPO-Verzeichnis) die Datei `firefox_startup.vbs` kopieren und das Explorer-Fenster schließen.
- Im Dialog *Eigenschaften von Starten* die Schaltfläche *Hinzufügen* betätigen,
- Im neu geöffneten Dialog *Hinzufügen eines Skripts* neben dem Feld *Skriptname* den Namen `firefox_startup.vbs` eintragen und Dialog mit *OK* bestätigen.
- Im Dialog *Eigenschaften von Starten* den Dialog mit *OK* bestätigen.
- Richtlinie *Herunterfahren* öffnen, und dort analog zu dem Vorgehen bei *Starten* das Skript `firefox_shutdown.vbs` eintragen. Im Detail also:
- Im Dialog *Eigenschaften von Herunterfahren* die Schaltfläche *Hinzufügen* betätigen,
- In das vom automatisch geöffneten Windows Explorer angezeigte (leere) Verzeichnis (`Machine\Scripts\Shutdown` im betreffenden GPO-Verzeichis) die Datei `firefox_shutdown.vbs` kopieren und das Explorer-Fenster schließen.
- Im neu geöffneten Dialog *Hinzufügen eines Skripts* neben dem Feld *Skriptname* den Namen `firefox_shutdown.vbs` eintragen und Dialog mit *OK* bestätigen.
- Im Dialog *Eigenschaften von Herunterfahren* den Dialog mit *OK* bestätigen.

11.3.5. Zugriff auf bestimmte Programme einschränken

Feedback

Anmerkung

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:

- http://technet.microsoft.com/en-us/library/bb457006.aspx#EGAA.
- http://technet.microsoft.com/en-us/library/hh994606.aspx.

11.3.5.1. Kommandoeingabeaufforderung deaktivieren

Feedback

- In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:

  Benutzerkonfiguration -> Richtlinien -> Administrative Vorlagen -> System

- Richtlinie *Zugriff auf Eingabeaufforderung verhindern* öffnen und *Aktiviert* auswählen und bestätigen.

11.3.5.2. Zugriff auf Windows-Registry-Editor deaktivieren

Feedback

- In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:

  Benutzerkonfiguration -> Richtlinien -> Administrative Vorlagen -> System
- Richtlinie *Zugriff auf Programme zum Bearbeiten der Registrierung verhindern* öffnen
- *Aktiviert* auswählen und den Dialog mit *OK* bestätigen.

11.3.5.3. Konfiguration von *Software Restriction Policies* (SRP)

Feedback

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 [4].

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.

Anmerkung

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:

- http://technet.microsoft.com/en-us/library/bb457006.aspx#EGAA.
- http://technet.microsoft.com/en-us/library/hh994606.aspx.

- In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:

  Benutzerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen -> Richtlinien für Softwareeinschränkung
- Rechtsklick auf *Neue Richtlinien für Softwareeinschränkung erstellen*
- Im rechten Fensterteil *Erzwingen* öffnen,
- Einstellung *Alle Benutzer außer den lokalen Administratoren* auswählen und mit *OK* bestätigen.
- Im rechten Fensterteil *Sicherheitsstufen* öffnen.
- *Nicht erlaubt* per Doppelklick öffnen.
- *Als Standard* auswählen und mit *OK* bestätigen.
- Im rechten Fensterteil *Zusätzliche Regeln* öffnen.
- Rechtsklick auf *Neue Pfadregel...*

[4] Weitere sinnvolle Hinweise zur Analyse und Pflege der Software Restriction Policies liefert z.B. http://www.nsa.gov/ia/_files/os/win2k/Application_Whitelisting_Using_SRP.pdf

- In das Eingabefeld *Pfad* den UNC-Pfad `\\%USERDNSDOMAIN%\SysVol` eingeben, damit Logon- und GPO-Skripte ausgeführt werden können.
- In der Dropdown-Liste *Nicht eingeschränkt* auswählen und mit *OK* bestätigen.

Tabelle 11.1. Beispiele für weitere Pfadregeln

Pfad	Sicherheitsstufe
`\\%USERDNSDOMAIN%\SysVol`	Nicht eingeschränkt
`\\%LogonServer%\SysVol`	Nicht eingeschränkt
`\\%LogonServer%\netlogon`	Nicht eingeschränkt
`\\%COMPUTERNAME%\Templates$\*`	Nicht eingeschränkt
`%UserProfile%\Local Settings\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

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

Tabelle 11.2. Beispiele für weitere Pfadregeln

Pfad	Sicherheitsstufe
`%UserProfile%\Local Settings\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

- 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 [5].

11.3.6. Verwendung temporärer Benutzerprofil-Kopien

Feedback

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.

[5] Weitere sinnvolle Hinweise zur Analyse und Pflege der Software Restriction Policies liefert z.B. http://www.nsa.gov/ia/_files/os/win2k/Application_Whitelisting_Using_SRP.pdf

- In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:

  Computerkonfiguration -> Richtlinien -> Administrative Vorlagen -> System -> Benutzerprofile
- Richtlinie *Zwischengespeicherte Kopien von servergespeicherten Profilen löschen* öffnen und *Aktiviert* auswählen und bestätigen.

Kapitel 12. Integration und Verwaltung von Univention Corporate Client-Systemen

12.1. Installation von UCC 68
12.2. Konfigurationseinstellungen für UCC-Systeme 68
12.3. Ausrollen von neuen UCC-Systemen 69

Univention Corporate Client (UCC) ist wie UCS@school eine aus dem Univention App Center heraus installierbare Erweiterung für Univention Corporate Server. UCC enthält eine optimierte Desktop-Umgebung auf Basis von Linux (Ubuntu), die eine Anpassung des Desktops an die jeweilige Hardware und den Einsatzzweck zulässt. Der Rollout der UCC-Systeme wird über ein imagebasiertes Verfahren durchgeführt. Dabei kann entweder auf offiziell bereitgestellte Images (ThinClient oder Desktop) zurückgegeriffen werden oder es können speziell an die eigene Umgebung angepasste Images erstellt werden. Die Verwaltung der UCC-Systeme erfolgt über die Univention Management Console.

UCS@school bietet die Möglichkeit, UCC-Desktop-Systeme ähnlich wie Windows-Systeme in die UCS@school-Umgebung einzubinden. Die dafür notwendigen Konfigurationsschritte werden durch spezielle Integrationspakete für UCS@school und UCC auf ein Minimum reduziert. Nach dem Einbinden der UCC-Systeme stehen in Verbindung mit UCS@school unter anderem die folgenden Features auf den UCC-Systemen zur Verfügung:

- Automatisches Einbinden der Heimatverzeichnisse der Benutzer während des Anmeldevorgangs und der Zugriff auf Klassen- und Arbeitsgruppen-Dateifreigaben über eine Verknüpfung auf dem Desktop
- Automatische Einbindung der CUPS-Druckerfreigaben vom Schulserver
- Automatischer Start von iTALC auf den UCC-Systemen, welches die Verwendung der Bildschirm- bzw. Eingabegerätesperre über das UMC-Modul *Computerraum* ermöglicht
- Über Univention Configuration Registry-Richtlinien gesteuerte Einrichtung des Proxy-Servers für KDE-Anwendungen und Firefox inklusive einer transparenten Authentifizierung gegenüber dem HTTP-Proxy (Squid) des Schulservers

Für die Integration von UCC in UCS@school gelten die folgenden Einschränkungen:

- Für die Integration von UCC-Desktop-Systemen in UCS@school ist die Verwendung von Samba 4 auf dem UCS@school-Schulserver erforderlich.
- Die UCC-Systeme müssen mit dem offiziellen Desktop-Image (oder einem äquivalenten, selbst erstellten Image) installiert werden. UCC-ThinClient-Systeme bzw. UCC-Terminalserver werden in Verbindung mit UCS@school nicht unterstützt.
- Der über iTALC realisierte Präsentationsmodus sowie das Beaufsichtigen von Systemen über das UMC-Modul *Computerraum* werden für UCC-Systeme derzeit nicht unterstützt.
- Die über CUPS eingebundenen Druckerfreigaben unterstützen nicht alle Kombinationen für Zugriffsberechtigungen. Das Freigeben aller Drucker über das Computerraum-Modul hat daher keine Auswirkung auf UCC-Systeme.
- Der Klassenarbeitsmodus von UCS@school wird auf UCC-Systemen nicht unterstützt.

Weitere Informationen zu UCC finden sich im UCC-Handbuch [ucc-handbuch].

12.1. Installation von UCC

Feedback

Im Folgenden wird die Installation von Univention Corporate Client (UCC) auf einem UCS@school-Schulserver beschrieben. Dabei wird die Kenntnis des UCC-Handbuchs [ucc-handbuch] vorausgesetzt und neben einer Kurzanleitung für die Installation nur abweichende Installationsschritte beschrieben.

Die Installation von UCC erfolgt über das Univention App Center in der Univention Management Console. Die Applikation *Univention Corporate Client* muss auf dem UCS@school-Schulserver installiert werden. Dies ist in einer Single-Server-Umgebung der Domänencontroller Master und in einer Multi-Server-Umgebung der Domänencontroller Slave. Die notwendigen Installationsschritte sind auf beiden UCS-Systemrollen gleich und werden daher im folgenden gemeinsam beschrieben. Vor der Installation von UCC muss zunächst die UCS@school-Umgebung fertig installiert und konfiguriert werden.

Achtung

Die Verwendung von UCC in UCS@school setzt die Verwendung des offiziellen UCC-Desktop-Images oder eines selbsterstellten Desktop-Images voraus. Das offizielle UCC-Desktop-Image wird während der Installation vom Univention UCC-Repository-Server heruntergeladen und hat im gepackten Zustand eine Größe von ca. 1 GB. Es ist daher, je nach Art und Geschwindigkeit der Internetanbindung, mit längeren Downloadzeiten zu rechnen. Nach erfolgreichem Download wird das Image entpackt. Daher muss vor der Installation von UCC auf dem Schulserver sichergestellt werden, dass mindestens mindestens 22 GB an freiem Speicherplatz vorhanden sind.

Auf dem Schulserver sind für die Installation von UCC die folgenden Schritte durchzuführen:

- Die Installation von UCC erfolgt über das Univention App Center. Dafür muss auf dem betreffenden System im Univention App Center die Applikation Univention Corporate Client ausgewählt und installiert werden. Der *UCC-Setup*-Assistent ist nicht für die Einrichtung von UCS@school geeignet!

- Nun muss das offizielle UCC-Desktop-Image installiert werden. Dazu wird das Univention Management Console-Modul **UCC-Images** geöffnet und **UCC 2.0 desktop image** ausgewählt. Nach einem Klick auf **Herunterladen** wird das Image heruntergeladen.

- Nach Abschluss der Installation von UCC und des UCC-Desktop-Images sind ggf. neue Joinskripte auf dem System installiert worden, die noch nicht ausgeführt wurden. Daher ist es wichtig, die noch nicht ausgeführten Joinskripte jetzt über das UMC-Modul *Domänenbeitritt* zu starten. Alternativ kann das Starten der Joinskripte auch auf der Kommandozeile über den Befehl `univention-run-join-scripts` erfolgen.

12.2. Konfigurationseinstellungen für UCC-Systeme

Feedback

Im Folgenden werden die UCS@school-spezifischen Konfigurationseinstellungen beschrieben, die von regulären UCC-Systemen abweichen. Weitergehende Konfigurationsmöglichkeiten werden im UCC-Handbuch [ucc-handbuch] beschrieben.

Für die korrekte Funktion der UCC-Systeme ist sicherzustellen, dass die UCC-Systeme den Domänencontroller Master (nur bei Single-Server-Umgebungen!) bzw. den Domänencontroller Slave (Multi-Server-Umgebung) als DNS-Server verwenden. In der Standardeinstellung wird automatisch eine DHCP-DNS-Richtlinie `cn=dhcp-dns-SCHULNAME,cn=policies,ou=SCHULNAME,dc=example,dc=com` erstellt und mit dem Container `cn=dhcp,ou=SCHULNAME,dc=example,dc=com` verknüpft, die die IP-Adresse des Schulservers als DNS-Server über DHCP konfiguriert. Das automatische Erstellen und Verknüpfen der DHCP-DNS-Richtlinie kann durch das Setzen der UCR-Variable `ucsschool/import/genera-`

`te/policy/dhcp/dns/set_per_ou=false` auf Domänencontroller Master- *und* Domänencontroller Slave-Systemen deaktiviert werden.

Die Konfiguration der UCC-Systeme erfolgt in der Standardeinstellung über eine automatisch vom Schulserver generierte UCR-Richtlinie. Diese trägt den Namen `ou-default-ucr-policy` und wird für jede Schul-OU unter dem DN `cn=ou-default-ucr-policy,cn=policies,ou=SCHULNAME,dc=example,dc=com` im LDAP-Verzeichnis abgelegt. Diese UCR-Richtlinie wird automatisch bei der Installation des Schulservers mit geeigneten Werten vordefiniert, welche nachfolgend beschrieben werden:

- Die UCR-Variable `ucc/mount/cifshome/server` definiert den Server, von dem das Samba-Heimatverzeichnis des sich anmeldenden Benutzers gemountet wird. In der Variable ist der FQDN anzugeben (Beispiel: **`ucc/mount/cifshome/server=schulserver1.example.com`**).

- Analog zur aus UCS bereits bekannten UCR-Variable `proxy/http` kann über die Variable `ucc/proxy/http` der HTTP-Proxy für die UCC-Systeme definiert werden (Beispiel: **`ucc/proxy/http=http://schulserver1.example.com:3128`**).

- Der CUPS-Druckserver für UCC-Systeme wird über die UCR-Variable `ucc/cups/server` festgelegt. Auch hier ist der FQDN des Druckservers anzugeben (Beispiel: **`ucc/cups/server=schulserver1.example.com`**).

- Für die Verwendung von iTALC wird auf den UCC-Systemen der iTALC-Schlüssel des Schulservers zur automatischen Authentifizierung benötigt. Die folgenden zwei Variablen definieren eine Samba-Freigabe sowie den Dateinamen der iTALC-Schlüsseldatei, über die das UCC-System die Schlüsseldatei beziehen kann: `ucc/italc/key/sambasource` und `ucc/italc/key/filename`. In der Standardeinstellung wird der iTALC-Schlüssel auf der *NETLOGON*-Freigabe des Schulservers abgelegt. Die Schlüsseldatei enthält dabei den Namen des Schulservers (Beispiel: **`ucc/italc/key/sambasource=\\schulserver1\netlogon`** und **`ucc/italc/key/filename=italc-key_schulserver1.pub`**).

Das automatische Erstellen und Verknüpfen der UCR-Richtlinie `ou-default-ucr-policy` kann durch das Setzen der UCR-Variable `ucsschool/import/generate/policy/ucc/settings=false` auf Domänencontroller Master- *und* Domänencontroller Slave-Systemen deaktiviert werden.

Die UCC-Systeme können Kerberos als Authentifizierungsmethode für die transparente Authentifizierung gegenüber dem HTTP-Proxy (Squid) des Schulservers verwenden. Diese Authentifizierungsmethode ist in der Standardeinstellung im HTTP-Proxy des Schulservers deaktiviert und muss manuell durch das Setzen der Univention Configuration Registry-Variable `squid/krb5auth=yes` aktiviert werden. Anschließend ist auf dem Schulserver ein Neustart des Dienstes `squid` notwendig, der entweder über das UMC-Modul *Systemdienste* oder auf der Kommandozeile über das Kommando `invoke-rc.d squid3 restart` durchgeführt werden kann.

12.3. Ausrollen von neuen UCC-Systemen

Feedback

Sind Installation und Konfiguration von UCC auf dem Schulserver abgeschlossen, können neue UCC-Desktop-Systeme installiert und für UCS@school eingerichtet werden. Die nachfolgenden Schritte für den Rollout wurden auf ein Minimum reduziert und beinhalten abweichende Schritte zum regulären UCC-Rollout. Hinweise zu Rollout und Konfiguration von UCC-Desktop-Systemen können dem UCC-Handbuch [ucc-handbuch] entnommen werden.

- Für die Installation eines UCC-Desktop-Systems muss zunächst für jedes zu installierende System ein UCC-Objekt im LDAP-Verzeichnis erstellt werden. Hierzu werden Angaben wie IP-Adresse und MAC-Adresse benötigt. Das UCC-Objekt muss entweder in der Univention Management Console über das Modul *Rechner (Schulen)* oder auf der Kommandozeile über das UCS@school-Importskript `import_computer` ange-

legt werden. Bei beiden Varianten ist darauf zu achten, dass als Rechnertyp *Univention Corporate Client* bzw. *ucc* angegeben wird. Hinweise zum Importskript `import_computer` finden sich in Abschnitt 5.5.1.

- Nach dem Anlegen des UCC-Objektes muss das Rechner-Objekt in der Univention Management Console geöffnet und auf den Reiter *Images* gewechselt werden. Dort sollte als Startvariante *Installation: Neupartitionierung und Image-Rollout* und das gewünschte UCC-Desktop-Image ausgewählt werden. Diese Einstellungen beziehen sich ausschließlich auf den erstmaligen Rollout des UCC-Images auf ein neues System. Der Rechner muss nun neu gestartet und ein PXE-Boot initiiert werden. Dabei werden im Rahmen des Rollouts alle vorhandenen Daten des Systems überschrieben!

- Die Installation der notwendigen Integrationspakete auf dem UCC-System kann manuell auf der Kommandozeile des UCC-Systems erfolgen (`apt-get install univention-ucc-ucs-school-integration`). Sollen mehrere UCC-Systeme ausgerollt werden, wird empfohlen, am Container `cn=computers,ou=SCHULNAME,dc=example,dc=com` eine neue Richtlinie vom Typ *UCC Software-Update-Einstellungen* zu verknüpfen, über die das Paket ***univention-ucc-ucsschool-integration*** automatisch beim Systemstart installiert wird.

- Wurden die vorgenannten Schritte durchgeführt, kann das UCC-System gestartet werden. Während des PXE-Boot-Vorgangs wird automatisch eine Repartitionierung und die Installation des UCC-Desktop-Images vorgenommen. Dabei werden vom UCC-System Informationen für den Domänenbeitritt abgefragt. Sofern die oben genannte Richtlinie eingerichtet wurde, wird beim Starten des UCC-Systems das Integrationspaket nachinstalliert.

  ## Achtung

  Für die Nachinstallation des Integrationspakets muss das UCC-System Zugriff auf die offiziellen Univention-UCC-Repository-Server erhalten. Die dafür notwendigen DHCP-Routing-Einstellungen müssen ggf. vor dem ersten Bootvorgang eingerichtet werden.

- Nach Abschluss der manuellen bzw. automatischen Installation des Integrationspakets müssen einmalig auf dem UCC-System noch nicht ausgeführte Joinskripte aufgerufen werden. Dazu ist auf dem UCC-System auf der Kommandozeile der Befehl `univention-run-join-scripts` auszuführen. Dabei wird z.B. der iTALC-Schlüssel vom Schulserver auf das UCC-System kopiert.

- Zum Abschluss sollte das UCC-System neu gestartet werden.

Kapitel 13. Pre- und Post-Hook-Skripte für den Import

13.1. Erweiterung von Importdateien 72
13.2. Beispiel-Hook-Skript: automatische Erstellung der Marktplatzfreigabe 72
13.3. Beispiel-Hook-Skript: Setzen des LDAP-Containers für DHCP-Objekte 73

Während des Datenimports kann es notwendig sein, dass in Abhängigkeit von der jeweiligen Umgebung zusätzlich einige weitere Einstellungen vorgenommen werden müssen. Mit den Pre- und Post-Hook-Skripten besteht die Möglichkeit vor und nach dem Import eines Objektes, Skripte auszuführen. Zu allen Objekten und den davon jeweils unterstützten Operationen können mehrere Skripte definiert werden, die dann vor und nach den Operationen Anpassungen vornehmen.

Damit die Import-Skripte die Hook-Skripte finden können, müssen diese unterhalb des Verzeichnisses `/usr/share/ucs-school-import/hooks/` abgelegt werden. Dort gibt es für jede unterstützte Operation ein eigenes Unterverzeichnis. Beispielsweise gibt es das Verzeichnis `user_create_pre.d`, das alle Skripte enthalten muss, die vor dem Import eines Benutzers ausgeführt werden sollen. Alle weiteren Verzeichnisse sind nach dem gleichen Schema benannt: `<Objekt>_<Operation>_pre.d` für die Skripte, die *vor* einer Operation ausgeführt werden sollen und `<Objekt>_<Operation>_post.d` für die Skripte, die nach einer Operation ausgeführt werden sollen. Das Paket ***ucs-school-import*** bringt diese Verzeichnisse bereits mit. Skripte, die bei der Ausführung berücksichtigt werden sollen, müssen zwei Bedingungen erfüllen. Der Name darf nur aus Ziffern, Buchstaben und Unter- und Bindestrichen bestehen und die Ausführungsrechte müssen für die Datei gesetzt sein. Alle anderen Dateien in diesen Verzeichnissen werden ignoriert.

Die Hook-Skripte werden derzeit für die Objekttypen `ou`, `user`, `group`, `printer`, `computer`, `network` und `router` für die Operationen `create`, `modify` und `remove` ausgeführt. Dabei ist zu beachten, dass für Rechner (*computer*), Netzwerke, Router und Schul-OUs nur die Operation zum Erzeugen (`create`) definiert ist und daher auch nur dafür Hook-Skripte definiert werden können.

Die Pre-Hook-Skripte werden mit einem Parameter aufgerufen. Dieser enthält den Namen einer Datei in der die Zeile des als nächstes zu bearbeitenden Objektes aus der Import-Datei gespeichert ist. Darüber können die Skripte jede Einstellung für das Objekt auslesen; allerdings ist zu berücksichtigen, dass zu diesem Zeitpunkt die Daten noch nicht durch das Import-Skript geprüft worden sind. Die Post-Hook-Skripte bekommen als zusätzlichen Parameter noch den LDAP-DN des gerade bearbeiteten Objektes übergeben.

Das folgende Beispiel-Skript soll ausgeführt werden, nachdem eine neue Schul-OU angelegt wurde. Dafür muss das Skript in das Verzeichnis `/usr/share/ucs-school-import/hooks/ou_create_post.d/` kopiert werden. Die Aufgabe des Skriptes soll es sein, die LDAP-Basis für den DHCP-Server der Schule per Univention Configuration Registry-Richtlinie auf den Container `cn=dhcp` unterhalb der LDAP-Basis der Schule zu setzen.

```
#!/bin/sh
ldap_base="$(ucr get ldap/base)"
# Auslesen der ersten Spalte (OU-name) der Importdatei
ou="$(awk -F '\t' '{print $1}' "$1")"
# Den Standard-Schul-DC-Namen erzeugen
host="dc${ou}-01.$(ucr get domainname)"
# Eine UCR-Richtlinie erstellen und mit dem Schul-DC verbinden
udm policies/registry create \
  --position "cn=policies,ou=$ou,$ldap_base" \
  --set name=dhcpd_ldap_base \
  --append "registry=dhcpd/ldap/base=cn=dhcp,ou=$ou,$ldap_base"
```

```
udm computers/domaincontroller_slave \
  --dn "cn=dc${ou}-01,cn=dc,cn=computers,ou=$ou,$ldap_base" \
  --policy-reference "cn=dhcpd_ldap_base,cn=policies,ou=$ou,$ldap_base"
echo "$(basename $0): Added policy dhcpd_ldap_base ."
```

Obwohl das Skript `create_ou` keine Eingabedatei übergeben bekommt, wird für die Hook-Skripte eine generiert, die in der Zeile den Namen der OU enthält. Wenn ein vom Standard abweichender Schul-DC-Name angegeben wurde, wird dieser als zweiter Wert übergeben. Für alle anderen Operationen auf den Objekten können Hook-Skripte auf äquivalente Weise erstellt werden.

13.1. Erweiterung von Importdateien

Feedback

Eine weitere Funktion von den Hook-Skripten ist die Möglichkeit mit Erweiterungen in den Import-Dateien umzugehen, d.h. wenn in den Importdateien mehr Felder eingetragen sind, als durch die Import-Skripte selbst verarbeitet werden, so können die erweiterten Attribute in den Hook-Skripten ausgelesen und verarbeitet werden. Als Beispiel könnten bei den Benutzern Adressinformationen oder eine Abteilung gespeichert werden. Die zusätzlichen Felder werden in den Importdateien jeweils hinten an die Zeilen getrennt durch einen Tabulator angehängt. Da die Hook-Skripte die komplette Zeile übergeben bekommen, kann ein Post-Hook-Skript genutzt werden, um die neuen Felder auszulesen und die Informationen z.B. an dem gerade erzeugten Benutzer zu ergänzen.

13.2. Beispiel-Hook-Skript: automatische Erstellung der Marktplatzfreigabe

Feedback

Um den Austausch von Dokumenten zwischen Benutzern zu erleichtern, wird empfohlen, die Freigabe *Marktplatz* auf den jeweiligen Schul-DCs anzulegen, auf die alle Benutzer Zugriff erhalten.

Das Hook-Skript `ou_create_post.d/52marktplatz_create` wird ab UCS@school für UCS 2.4 mitgeliefert und legt beim Aufruf von `create_ou` die Freigabe ``Marktplatz'' automatisch an. Über die Univention Configuration Registry-Variable `ucsschool/import/generate/share/marktplatz` kann der Hook de-/aktiviert werden, indem der Variable der Wert `no` bzw. `yes` zugeordnet wird.

Über drei weitere Univention Configuration Registry-Variablen kann das Verhalten des Hooks gesteuert werden:

- `ucsschool/import/generate/share/marktplatz/sharepath`

  Diese Variable definiert das Verzeichnis auf dem Server, welches als Freigabe `Marktplatz` freigegeben wird. In der Standardeinstellung wird das Verzeichnis `/home/<OU>/groups/Marktplatz` verwendet.

- `ucsschool/import/generate/share/marktplatz/group`

  Beim Anlegen der Freigabe wird die in dieser Variable definierte Gruppe als Gruppenbesitzer der Freigabe festgelegt. In der Standardeinstellung ist dies die Gruppe `Domain Users`. Es ist zu beachten, dass abweichend vom UCS-Standard die über die Importskripte angelegten Benutzer nicht in der Gruppe `Domain Users` enthalten sind.

- `ucsschool/import/generate/share/marktplatz/permissions`

  Die Zugriffsrechte der Freigabe sind in oktaler Schreibweise anzugeben (z.B. 0777). In der Standardeinstellung erhalten der Benutzer `root`, die vordefinierte Gruppe (z.B. `Domain Users`) sowie alle sonstigen Benutzer Lese- und Schreibrechte (0777).

13.3. Beispiel-Hook-Skript: Setzen des LDAP-Containers für DHCP-Objekte

Feedback

Auf den Schul-DCs wird ein abweichender Container für DHCP-Objekte verwendet, weshalb die Univention Configuration Registry-Variable `dhcpd/ldap/base` entsprechend gesetzt werden muss. Um das manuelle Setzen der UCR-Variable für jede neue OU bzw. jeden neuen Schul-DC zu vermeiden, wird über den Standard-Hook `ou_create_post.d/40dhcpsearchbase_create` automatisch beim Erstellen einer OU die UCR-Richtlinie `ou-default-ucr-policy` im Container `cn=policies,ou=`*`XXX`*`,`*`LDAPBASIS`* angelegt und anschließend mit dem OU-Objekt `ou=`*`XXX`*`,`*`LDAPBASIS`* verknüpft. Über die Richtlinie wird die Univention Configuration Registry-Variable `dhcpd/ldap/base` entsprechend gesetzt. Dadurch wird sichergestellt, dass die in der Richtlinie gesetzten UCR-Variablen auf allen UCS-Systemen der OU automatisch übernommen werden.

Kapitel 14. Hinweise für große UCS@school-Umgebungen

14.1. Skalierung von UCS@school Samba 4 Umgebungen 75
14.1.1. Installation zusätzlicher Memberserver 75
14.1.2. Installation zusätzlicher Anmeldeserver 76

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 im *UCS performance guide* [ucs-performance-guide] 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.

14.1. Skalierung von UCS@school Samba 4 Umgebungen

Feedback

14.1.1. Installation zusätzlicher Memberserver

Feedback

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

Um einen solchen zusätzlichen Memberserver an einem Schulstandort zu installieren und zu joinen, müssen vorbereitende Schritte durchgeführt werden:

- Für den neuen Memberserver 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 Memberserver installiert wurde.

- Der Memberserver muss in die Gruppen `Member-Edukativnetz` und `OU<OUNAME>-Member-Edukativnetz` aufgenommen werden.

- Im Univention Directory Manager sollte eine Univention Configuration Registry Richtlinie angelegt werden, die die UCR-Variable `ldap/server/name` 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 Memberservers positioniert ist.

- Auf dem Memberserver selbst muss vor dem Domänenbeitritt die UCR-Variable `nameserver1` auf die IP-Adresse des Schulservers gesetzt werden. Die UCR-Variablen `nameserver2` und `nameserver3` dürfen nicht gesetzt sein.
- Nach diesen Schritten kann der Memberserver wie gewohnt der Domäne beitreten.

14.1.2. Installation zusätzlicher Anmeldeserver

Feedback

In UCS@school-Umgebungen in denen Samba 4 Active Directory-kompatible Dienste bereitstellt, kann zur Skalierung der Anmeldedienste ein zusätzlicher UCS DC Slave an einem Schulstandort installiert werden. Dieser zusätzliche, sekundäre Domänencontroller wird als normaler UCS DC Slave installiert und muss danach durch Ausführung eines speziellen Skripts an dem Schulstandort der Domäne beitreten. Auf diesem sekundären Domänencontroller wird nicht die UCS@school App installiert.

Zwischen dem Samba4-Verzeichnisdienst auf dem neuen UCS DC Slave und dem UCS@school-Server wird die DRS Replikation eingesetzt, die Samba 4 auch im Standard-UCS verwendet. Die für UCS@school charakteristische selektive LDAP-Replikation von Verzeichnisdaten findet wie üblich weiter vom UCS DC Master zu den DC Slave-Systemen statt. Allerdings findet die Synchronisation mit dem Samba4-Verzeichnisdienst nur auf dem primären Schulserver statt.

Achtung

Der sekundäre Domänencontroller stellt nur redundante Anmeldedienste zur Verfügung, UCS@school-spezifische Dienste und UMC-Module stellt er nicht bereit.

Damit in diesem Setup der Domänenbeitritt von Windows-Clients problemlos funktioniert, sollten für diese immer über die UCS@school-spezifischen Import-Werkzeuge Rechnerobjekte in der Univention Management Console angelegt werden. Wenn dies nicht vor dem Domänenbeitritt eines Windows-Clients erfolgt, kann der Domänenbeitritt mit einer Windows-Fehlermeldung abbrechen. Dies ist darauf zurückzuführen, dass zur Konfliktvermeidung im Samba-Verzeichnisdienst auf dem sekundären Schul-DC per Voreinstellung keine neuen Maschinenkonten angelegt werden können.

Um einen solchen sekundären Domänencontroller an einem Schulstandort zu installieren und in die Domäne aufzunehmen, müssen auf dem Master folgende vorbereitende Schritte als `root` durchgeführt werden:

- ```
  /usr/share/ucs-school-import/scripts/create_ou \
      <Schul-OU> <Name des neuen Schul-DCs>
  ```
- ```
  /usr/share/ucs-school-import/scripts/move_domaincontroller_to_ou \
      --ou <Schul-OU> --dcname <Name des neuen Schul-DCs>
  ```
- ```
  cd /usr/share/ucs-school-import/scripts
  scp ucs-school-join-secondary-samba4 root@<Name des neuen Schul-DCs>:
  ```

Danach muss auf dem neuen DC Slave für den Domänenbeitritt folgender Schritt als Benutzer `root` ausgeführt werden:

- ```
  /root/ucs-school-join-secondary-samba4 <IP des primären Schul-DCs>
  ```

Literaturverzeichnis

[ucs-handbuch] Univention GmbH. 2015. *Univention Corporate Server - Handbuch für Benutzer und Administratoren*. https://docs.software-univention.de/handbuch-4.1.html.

[ucc-handbuch] Univention GmbH. 2014. *Univention Corporate Client - Manual for administrators*. https://docs.software-univention.de/ucc-manual.html.

[ucs-school-teacher] Univention GmbH. 2012. *UCS@school - Handbuch für Lehrkräfte und Schuladministratoren*. https://docs.software-univention.de/ucsschool-lehrer-handbuch-4.0.pdf.

[ucs-performance-guide] Univention GmbH. 2015. *UCS performance guide*. https://docs.software-univention.de/performance-guide-4.1.html.