

Einsatzszenarien für Univention Corporate Server

Thema:	Dieses Dokument stellt beispielhaft vier Einsatzszenarien mit Univention Corporate Server vor	
Datum:	8. Dezember 2010	
Seitenzahl:	28	
Versionsnummer:	7414	
Autoren:	Univention GmbH	feedback@univention.de

Inhaltsverzeichnis

1	Einführung	3
2	Anwaltskanzlei	3
2.1	Ausgangslage	3
2.2	Systeme und Dienste	3
3	Mittelständische Maschinenbau-Firma	6
3.1	Ausgangslage	6
3.2	Umsetzung	7
4	Heterogene Großumgebung in Konzernverbund	13
4.1	Ausgangslage	13
4.2	Umsetzung	14
5	Schulträger	21
5.1	Ausgangslage	21
5.2	Umsetzung	21

1 Einführung

Die folgenden fiktiven Szenarien beleuchten beispielhaft Anwendungsmöglichkeiten von Univention Corporate Server in verschiedenen Installationsgrößen und Implementierungstiefen.

Am Ende jedes Kapitels finden sich Hinweise auf die entsprechende Dokumentation, in der die konkrete Umsetzung der einzelnen Komponenten beschrieben ist.

2 Anwaltskanzlei

2.1 Ausgangslage

Die Anwaltskanzlei Hemmerlein & Söhne verfügt über insgesamt zehn Mitarbeiter. Die Mitarbeiter arbeiten im Wesentlichen mit Office-Applikationen und einer juristischen Vorgangsbearbeitung, die nur für Windows verfügbar ist. Als Client-Betriebssystem wird Windows 7 eingesetzt. Alle Daten sollen zentral auf einem Server gespeichert und gesichert werden. Da nur geringes technisches Know-How verfügbar und eigenes technisches Personal nicht finanzierbar ist, wird Wert auf eine einfache Administration gelegt. Die nachfolgend beschriebenen administrativen Tätigkeiten können nach erfolgter Erstinstallation komplett durch einfach zu bedienende webbasierte Schnittstellen konfiguriert werden.

In der Firma existieren insgesamt drei Laserdrucker (zwei baugleiche Schwarz/Weiss-Modelle und ein Farblaserdrucker), die alle in einem zentralen Büro aufgebaut sind. Es werden häufig sehr große Schriftsätze mit hohem Volumen gedruckt.

2.2 Systeme und Dienste

UCS stellt die benötigten Dienste und Anwendungen "out of the box" als Komplettlösung zur Verfügung. Es kommt ein einzelnes UCS-System zum Einsatz, das für die Windows-Clients Anmelde- und Dateidienste bereitstellt, die Drucker verwaltet und das Backup der Daten automatisiert.

2.2.1 Verwaltung der Benutzerdaten

Für die zehn Mitarbeiter werden im Web-Interface des Univention Directory Manager Benutzerkonten angelegt. Jeder Mitarbeiter erhält dabei ein Passwort, das - wie alle Benutzerdaten - in einem LDAP-Verzeichnisdienst gespeichert und bei der Anmeldung am Windows-Client abgefragt wird.

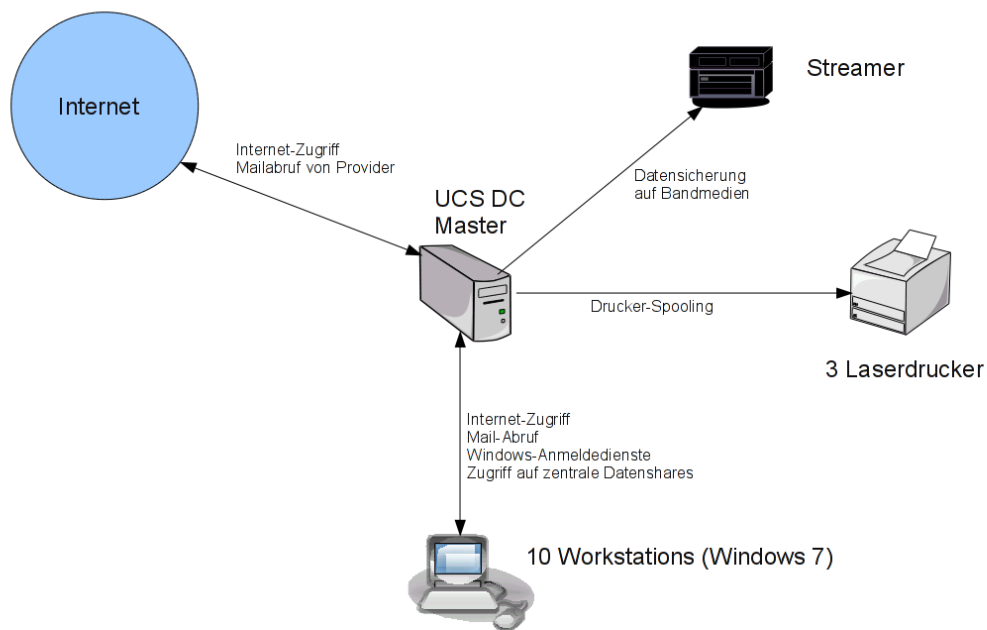


Abbildung 1: Systemübersicht der Kanzlei Hemmerlein und Söhne

2.2.2 Verwaltung der Windows-Rechner

Auf dem UCS-System wird Samba für die Anbindung der Windows-Clients eingesetzt. An der Samba-Installation müssen keine Anpassungen vorgenommen werden, Windows-Clients können direkt der durch UCS bereitgestellten Windows-Domäne beitreten. Der Domänen-Join ist aus Client-Sicht identisch mit dem Beitritt zu einer Windows-basierten Domäne.

Auf den Windows-Clients läuft die Open Source-Softwareverteilung OPSI4UCS. Sie ermöglicht eine weitgehend automatisierte Verteilung von Sicherheitsupdates und Service Packs an die Windows-Clients, so dass auch ohne dezidierten Administrator alle Systeme auf einem aktuellen und sicheren Stand betrieben werden können. Die Konfiguration von OPSI4UCS integriert sich in das UCS-Managementsystem.

2.2.3 Daten-Verwaltung

Samba stellt für jeden Benutzer auf dem UCS-System ein Heimatverzeichnis als Dateifreigabe über das CIFS-Protokoll bereit. Der Benutzer erhält so unabhängig vom angemeldeten Rechner immer dieselben Daten. Die Datenhaltung auf einer Freigabe ermöglicht außerdem eine

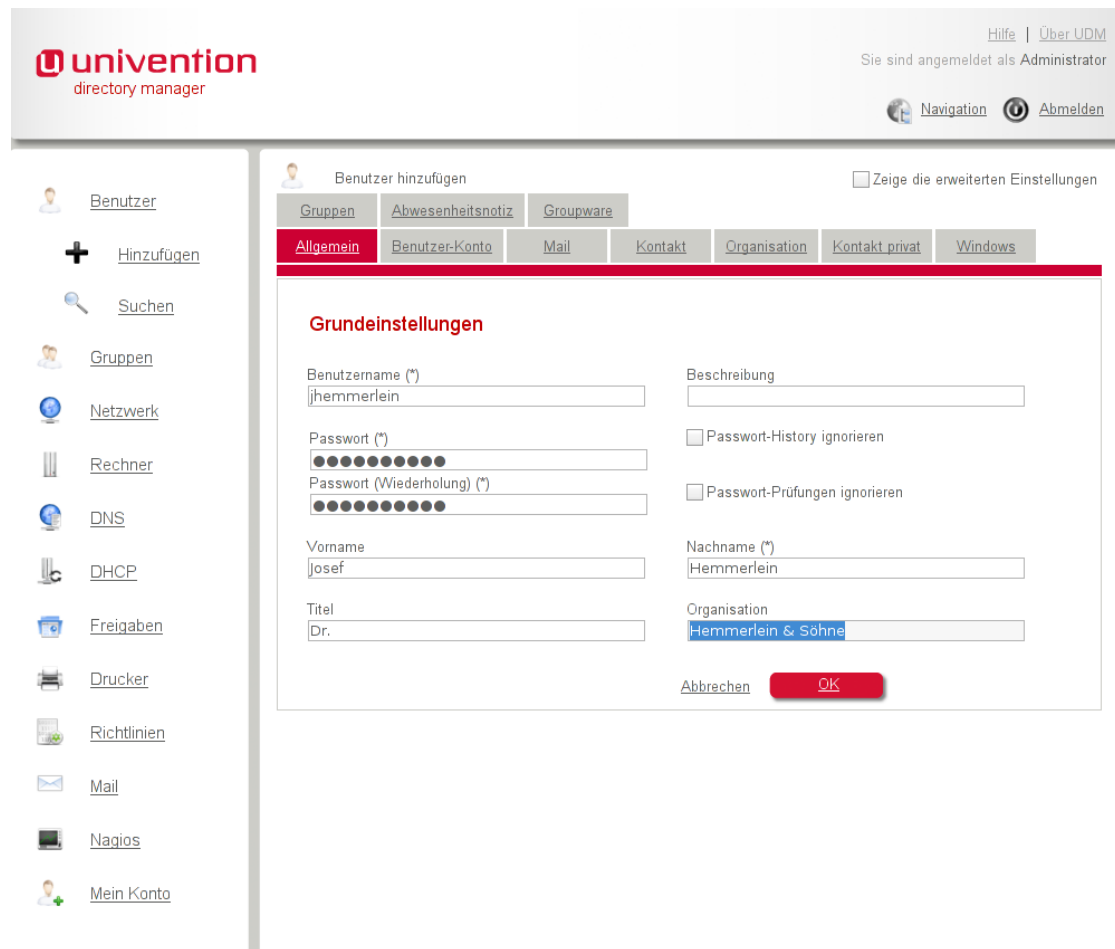


Abbildung 2: Anlegen eines Benutzers im Univention Directory Manager

zentrale Datensicherung.

Darüberhinaus existiert ein zentrale Freigabe mit juristischer Fachliteratur im PDF-Format, die auf jedem Client eingebunden wird.

Freigaben können wie Benutzer ebenfalls webbasiert im Univention Directory Manager angelegt werden.

2.2.4 Druckdienste

Das UCS-System stellt über die Software CUPS Druckdienste bereit. Es können sowohl netzwerkfähige Drucker, als auch lokal an einen Rechner angeschlossene Drucker zentral administriert werden. Die drei Drucker können bequem über den Univention Directory Manager konfiguriert werden und stehen den Benutzern auf ihren Windows-Clients direkt zur Verfügung. Die bei-

den baugleichen Laserdrucker werden dabei zu einer Druckergruppe zusammengefasst: Das bedeutet, dass die Benutzer neben der gezielten Auswahl eines Druckers auch die Möglichkeit erhalten, auf einen Pseudodrucker zu drucken. Die Druckaufträge werden dabei reihum um die beiden Drucker der Druckergruppe verteilt. Bei belegten Druckern wird auf einen freien Drucker ausgewichen, was Wartezeiten vermeidet.

2.2.5 Mailserver

Auf dem UCS-System läuft ein Mailserver, auf den die Benutzer über das IMAP-Protokoll auf ihre Mailkonten zugreifen. Virenerkennung inkl. Signaturen-Updates und Spamfilterung sind ohne weitere Folgekosten integriert. Die Verwaltung der Maileinstellungen (z.B. E-Mail-Adressen und Alias-Adressen) der Benutzer erfolgt über den Univention Directory Manager.

2.2.6 Proxy und Webfilter

Ein Webfilter auf Basis von Squid und Dansguardian ist in UCS integriert und führt mit dem integrierten Virensch scanner ClamAV eine Prüfung des Webtraffics auf Viren durch. Dadurch werden auf Webseiten versteckte Trojaner erkannt und ausgefiltert. Auch potentiell gefährliche Dateien wie EXE-Dateien können blockiert werden.

2.2.7 Backup

Alle Daten (sowohl die Daten der Benutzer im Heimatverzeichnis als auch die Daten auf der zentralen Freigabe für Fachliteratur) liegen auf dem UCS-System und können deshalb zentral auf einen Streamer gesichert werden. UCS bringt dafür die Backup-Software Bacula mit, die flexibel auf verschiedene Sicherungs- und Archivierungsstrategien angewendet werden kann.

2.2.8 Referenzen

- UCS-Handbuch
- Technisches Dokument UCS-Backup
- Technisches Dokument UCS-Proxy
- [http://wiki.univention.de/index.php?title=Opsi\(open_pc_server_integration\)](http://wiki.univention.de/index.php?title=Opsi(open_pc_server_integration))

3 Mittelständische Maschinenbau-Firma

3.1 Ausgangslage

Gunapa Technologies ist einer der wichtigsten Hersteller für Walzstahlfräsen. Am Firmensitz in Deutschland arbeiten 260 Mitarbeiter in Produktion, Verwaltung, Konstruktion und Vertrieb.

Außerdem gibt es in den USA, Argentinien und Indien lokale Standorte mit 5-10 Mitarbeitern.

Auf dem Desktop kommt überwiegend Linux zum Einsatz. Die Mitarbeiter aus Konstruktion und Entwicklung sind auf Linux-Software angewiesen und benötigen einen frei konfigurierbaren Desktop.

Für die Mitarbeiter aus der Verwaltung und dem Vertrieb soll nur eine Office-Suite, ein E-Mail-Client und ein Browser angeboten werden. Der Desktop soll von den Benutzern nicht "zerspielt" werden können.

Eine Buchhaltungssoftware, die von einigen Benutzern benötigt wird, ist nur unter Windows verfügbar. Ein Teil der Konstruktion muss mit einer CAD-Software erfolgen, die nur für Solaris verfügbar ist.

Die Administration der Rechner soll möglichst zentralisiert erfolgen. Während in der Zentrale zwei EDV-Mitarbeiter arbeiten, ist an den drei externen Standorten kein technisches Personal verfügbar.

Um Arbeitsausfälle durch Störungen zu vermeiden, muss der Großteil der angebotenen Dienste redundant bereitgestellt werden.

Um Energie zu sparen und Wartungskosten zu minimieren, sollen für die Mitarbeiter in Verwaltung und Vertrieb Thin Clients (festplattenlose Rechner) zum Einsatz kommen. Da keine lokalen Daten oder Konfigurationen gespeichert werden, kann ein defekter Thin Client problemlos auch durch nicht-technische Mitarbeiter ersetzt werden.

Ein Proxy-Server soll den Netzwerkverkehr in einem Cache zwischenspeichern und Virenschutz anbieten.

Aktuell werden nur Standard-Maildienste verwendet, später ist der Einsatz von Groupware geplant.

Alle Nutzdaten werden zentral auf einem SAN gespeichert.

3.2 Umsetzung

3.2.1 Domänencontroller / LDAP-Verzeichnis

Das Unternehmen implementiert eine Infrastruktur bestehend aus einem UCS Domänencontroller Master (DC Master), einem UCS Domänencontroller Backup (DC Backup), mehreren UCS Domänencontroller Slave (DC Slave) und Thin Clients.

Der DC Master ist das Kernstück der UCS-Domäne. Auf diesem System wird die zentrale schreibbare Kopie des LDAP-Verzeichnisdienstes vorgehalten.

Der DC Backup stellt weitgehend eine Kopie des DC Master dar. Dadurch sind alle wichtigen Dienste doppelt im Netzwerk vorhanden, die Verfügbarkeit der Dienste wird also weiter erhöht und die Last zwischen den UCS Domänencontrollern verteilt.

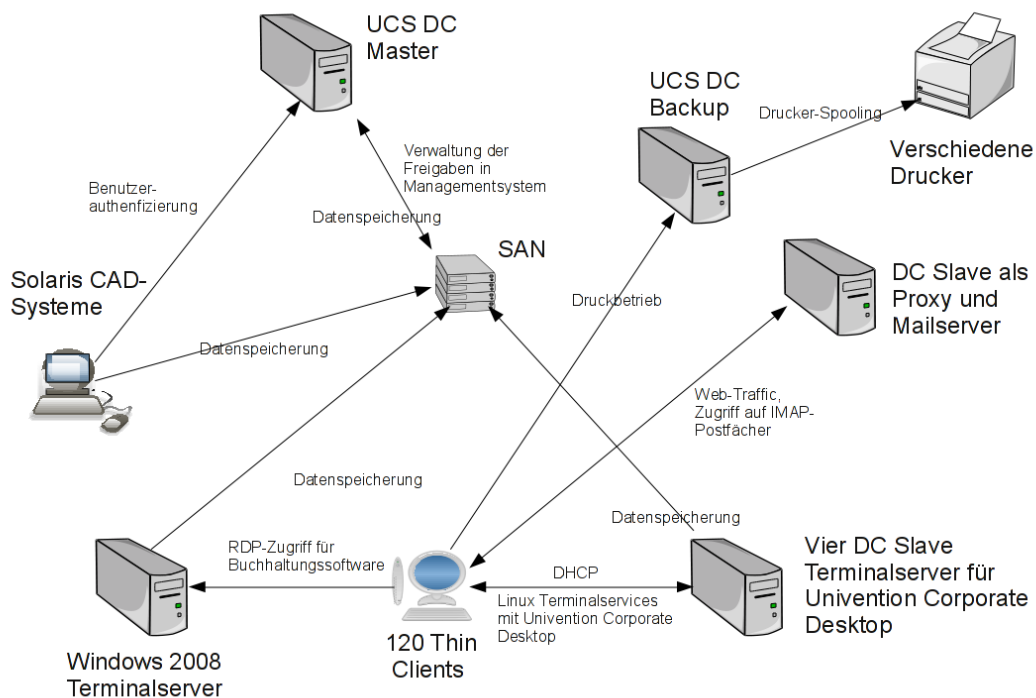


Abbildung 3: Systemübersicht von Ganupa Technologies am zentralen Standort

Sollte der DC Master durch einen Hardwaredefekt ausfallen, kann der DC Backup innerhalb kürzester Zeit zum DC Master umgewandelt werden.

Der DC Master und der DC Backup stehen in der Firmenzentrale. Die beiden UCS-Systeme betreiben einen LDAP-Server und bieten Anmeldedienste für die Domäne an. Für ein zentrales IP-Management läuft auf beiden Systemen ein mit Daten aus dem LDAP-Verzeichnis gepflegter DNS- und DHCP-Server. Auf dem DC Backup ist ein Printserver eingerichtet.

3.2.2 Linux Terminal Services

In der Firmenzentrale sind vier Domänencontroller Slave-Systeme installiert. Sie dienen als Linux-Terminalserver, auf die mit Thin Clients zugegriffen wird.

Die Anwendungen der Benutzer werden auf den Terminalservern ausgeführt, während die Thin Clients die Anwendungen lediglich darstellen und Benutzereingaben an den Terminalserver übermitteln.

Die Benutzerdaten werden auf dem zentralen SAN gespeichert. Die dafür verwendete Freigabe wird durch den Univention Directory Manager verwaltet.

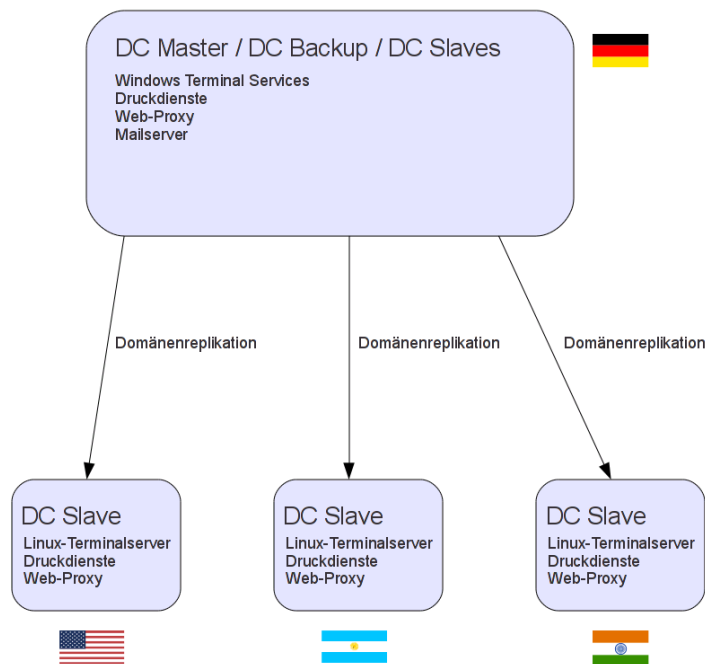


Abbildung 4: Globaler Systemaufbau von Ganupa Technologies

Auf den Linux-Terminalservern kommt Univention Corporate Desktop auf Basis von KDE 4 zum Einsatz. Alle für den Bürobetrieb wichtigen Anwendungen werden mitgeliefert (Textverarbeitung, Datenbanken, Präsentationen und Tabellenkalkulation mit OpenOffice.org, Bildverarbeitung mit Gimp, Mozilla Firefox als Web-Browser, KMail/Kontact als Groupware- und Mailclient, Multimedia-Applikationen für das Abspielen von Musik und Videos und zum Brennen von DVDs/CDs).

Das Erscheinungsbild der KDE-Oberfläche auf den Thin Clients wird über zentral verwaltete Desktop-Profile gesteuert.

Für verschiedene Benutzergruppen existieren vorkonfigurierte Desktops, in denen je nach Tätigkeit verschiedene Applikationen vorkonfiguriert sind. So verwendet etwa die Verwaltung einen Desktop, auf dem nur Mozilla Firefox und OpenOffice.org eingerichtet sind, während die technischen Mitarbeiter aus einem breiteren Applikationsumfang schöpfen können. Diese Profile werden den Benutzern durch eine Richtlinie im Univention Directory Manager zugewiesen und können optional auch vor Benutzeränderungen geschützt werden, d.h. bei jeder Anmeldung wird der Desktop wieder auf den Urzustand zurückgesetzt.

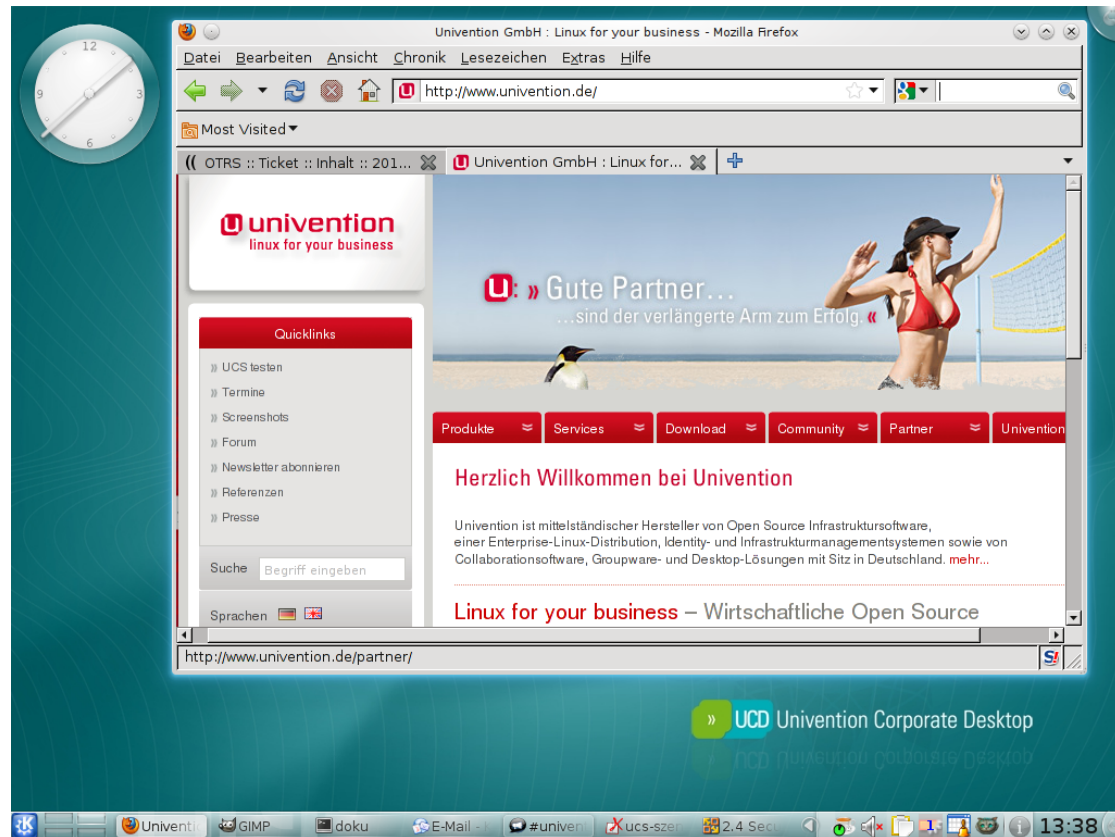


Abbildung 5: Linux-Desktop mit Univention Corporate Desktop

3.2.3 Druckdienste

Druckaufträge werden über einen Print-Server an den gewünschten Drucker weiterleitet. Die Printserver werden mit CUPS realisiert, das die verschiedenen Drucker in ein zentrales Spooling einbindet.

In einigen Großraumbüros sind mehrere Drucker zu einer Druckergruppe zusammengefasst; die Benutzer drucken einfach auf diese Gruppe, wobei die Druckaufträge gleichmässig verteilt werden und der nächste freie Drucker verwendet wird. Die Benutzer müssen so nicht prüfen ob ein Drucker gerade in Verwendung ist.

Außerdem ist jedem Drucker ein Seitenpreis zugeordnet. Dadurch können pro Benutzer die angefallenen Druckkosten ermittelt werden. Dies kann auch mit einer Limitierung von zu druckenden Seiten verbunden werden, die aber in der Umgebung nicht zum Einsatz kommt.

3.2.4 Windows-Terminalserver

Für die Windows-Programme wird durch Samba eine Windows-Domäne realisiert, in die ein Windows-Terminalserver als Mitgliedsserver eingebunden wird. Auf diesem Server wird die Buchhaltungssoftware betrieben, die nur unter Microsoft Windows läuft. Diese wird durch einen RDP-Client nahtlos auf den Linux-Desktops dargestellt.

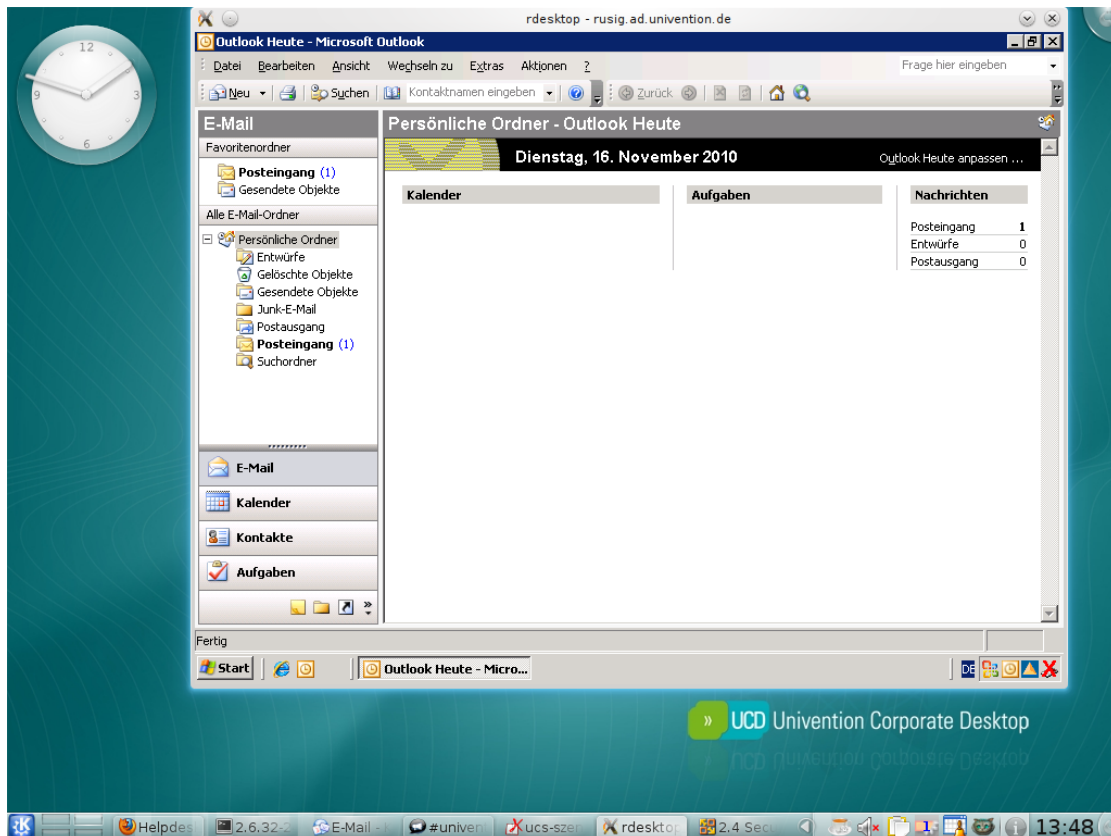


Abbildung 6: Integration einer Windows-Applikation in Univention Corporate Desktop

Ein UCS-Domänencontroller übernimmt die Funktion des primären Domänencontroller (PDC) und bietet Datei- und Druckdienste für den Windows-Terminalserver an. Die Linux- und die Samba-Domäne verwenden mit dem LDAP-Verzeichnis dieselbe Benutzerdatenbank und Benutzer können von Linux und Windows aus auf ihr Heimatverzeichnis zugreifen.

3.2.5 Einbindung von Solaris-Systemen

Eine Fachanwendung für CAD-Konstruktionen ist nur für Solaris verfügbar. Die Namensdienste auf dem Solaris-System wurden auf eine Authentifizierung gegen das UCS-LDAP angepasst, d.h. Benutzer können sich auf dem Solaris-System mit ihrer Domänen-Benutzererkennung und

-Passwort anmelden. Die zusätzliche Pflege lokaler Benutzerkonten auf dem Solaris-System entfällt so.

Das Solaris-System erhält seine IP-Adresse über DHCP von den UCS-DHCP-Servern zugewiesen. Die Datenspeicherung erfolgt auf den UCS-Fileservern über eine NFS-Freigabe.

3.2.6 Datenhaltung

Die Speicherung aller Benutzerdaten erfolgt auf einem zentralen SAN-System. Die verschiedenen Freigaben werden im Univention Directory Manager angelegt und verwaltet. Die Linux- und Solaris-Clients greifen über das Network Filesystem (NFS) auf die einzelnen Freigaben zu, die Windows-Clients über das CIFS-Protokoll.

3.2.7 Mailserver

Auf dem UCS-System läuft ein Mailserver auf Basis von Cyrus und Postfix. Die Benutzer greifen über das IMAP-Protokoll auf ihre Mailkonten zu.

Eine Virenerkennung inkl. Signaturen-Updates auf Basis von ClamAV und eine Spamerkennung auf Basis von SpamAssassin sind ohne weitere Folgekosten bereits integriert.

Die Verwaltung der Maileinstellungen (z.B. E-Mail-Adressen und Alias-Adressen) der Benutzer erfolgt über den Univention Directory Manager.

Mittelfristig ist der Einsatz einer Groupware geplant. UCS ermöglicht als herstellerübergreifende Lösung die Einbindung verschiedener Groupware-Lösungen; neben dem durch Univention bereitgestellten Kolab kann später zwischen Open-Xchange, Scalix und Zarafa gewählt werden.

3.2.8 Zentral gesteuerter Internet-Zugriff

Für einen zentral kontrollierten Internet-Zugriff bringt UCS einen Web-Proxy auf Basis von Squid und Dansguardian mit. Dieser erzwingt eine Authentifizierung der Benutzer anhand ihrer Domänenkennung. Heruntergeladene Dateien werden transparent mit dem Virenschanner ClamAV geprüft.

Dieser Proxy wird auf einem eigenständigen Domänencontroller Slave betrieben.

3.2.9 Referenzen

- UCS-Handbuch
- Kolab 2 für UCS Handbuch
- Technisches Dokument Erstellung eigener KDE-Profile
- Technisches Dokument Linux/UNIX-Systeme

- Technisches Dokument Scalix für UCS
- Technisches Dokument Squid-Webproxy-Integration
- http://www.open-xchange.com/de/ox_for_ucs/server_edition-de

4 Heterogene Großumgebung in Konzernverbund

4.1 Ausgangslage

Die Hanseatische Marineversicherung (HMV) ist ein auf den Logistikbereich spezialisierter Versicherungsdienstleister mit 1800 Mitarbeitern. Die HVM ist ein Bestandteil der Konzernmutter Vigil Insurances.

Die Konzernmutter betreibt einen eigenständigen Verzeichnisdienst auf Basis von Microsoft Active Directory, die Pflege der Benutzerdaten der einzelnen Tochterfirmen erfolgt jedoch autark.

Die Mitarbeiter arbeiten an insgesamt 36 Standorten weltweit, der grösste davon der Stammsitz in Bremen mit ca. 250 Personen. Viele der Benutzer arbeiten als Vertreter oder Gutachter mobil mit Notebooks.

Auf den Desktops kommt durchgehend Microsoft Windows zum Einsatz, auf einem Teil der Systeme noch Microsoft Windows XP, überwiegend aber Microsoft Windows 7. Die Softwareverteilung und Installation von Sicherheitsupdates erfolgt zentralisiert.

In der Zentrale soll aufgrund einer übergeordneten Konzernrichtlinie Citrix XenApp eingesetzt werden, die Benutzer greifen dann mit Thin Clients darauf zu.

Zur Abstimmung von Terminen und Kontakten soll eine Groupware eingesetzt werden. Ein Teil der Benutzer soll ausschließlich einen Web-Client verwenden, während der Rest der Benutzer Microsoft Outlook 2008 einsetzen soll.

Alle Benutzer, Rechner und Dienste sollen zentral verwaltbar sein. Kritische Systemzustände sollen zeitnah per E-Mail und SMS gemeldet werden.

Alle Serversysteme in der Zentrale sollen virtualisiert werden. Aufgrund der daraus erwachsenden erheblichen Bedeutung der Virtualisierung muss dafür eine Open Source-Lösung zum Einsatz kommen.

Die Datensicherung erfolgt zentral in Bremen.

Verschiedene internationale Compliance-Anforderungen aus dem Versicherungssektor müssen erfüllt werden.

4.2 Umsetzung

Das Unternehmen implementiert eine Infrastruktur bestehend aus einem UCS Domänencontroller Master (DC Master), einem UCS Domänencontroller Backup (DC Backup), mehreren UCS Domänencontroller Slave (DC Slave) und 150 Thin Clients.

Der DC Master ist das Kernstück der UCS-Domäne. Auf diesem System wird der zentrale, schreibbare LDAP-Verzeichnisdienst vorgehalten.

Der DC Backup stellt weitgehend eine Kopie des DC Master dar. Dadurch sind alle wichtigen Dienste doppelt im Netzwerk vorhanden, die Verfügbarkeit der Dienste wird also weiter erhöht und die Last zwischen den Domänencontrollern verteilt.

Sollte der DC Master durch einen Hardware-Defekt ausfallen, kann der DC Backup innerhalb kürzester Zeit zum DC Master umgewandelt werden.

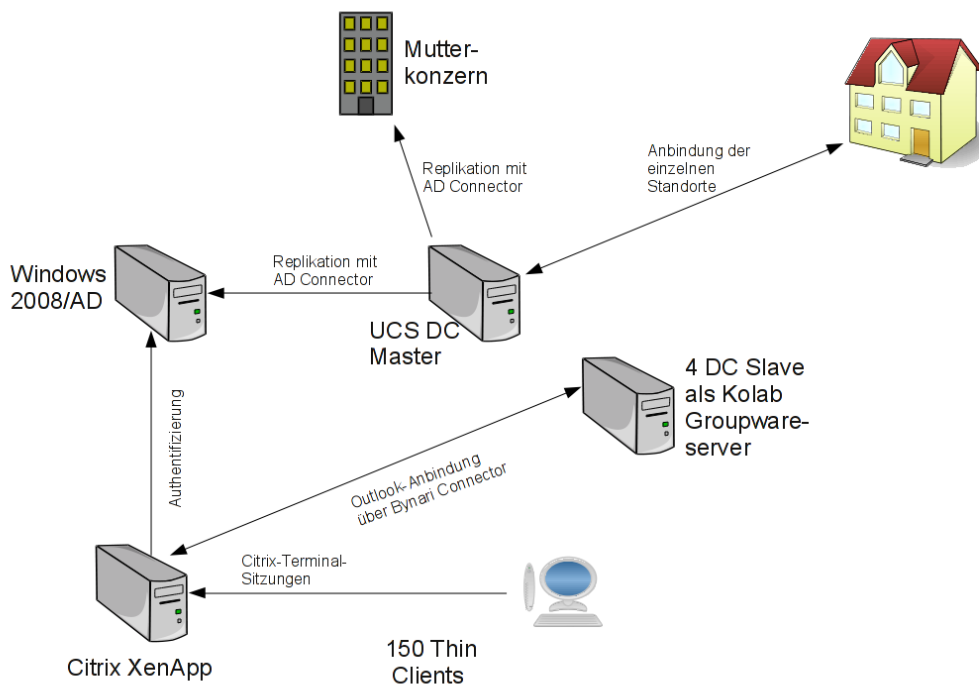


Abbildung 7: Gesamtüberblick (nicht im Bild: Storage, DNS, DHCP, Druckdienste)

Der DC Master und der DC Backup stehen in der Firmenzentrale. An den Standorten finden sich weitere UCS Domänencontroller Slave-Systeme, die Windows-Domänendienste, Druckdienste und eine Softwareverteilung bereitstellen.

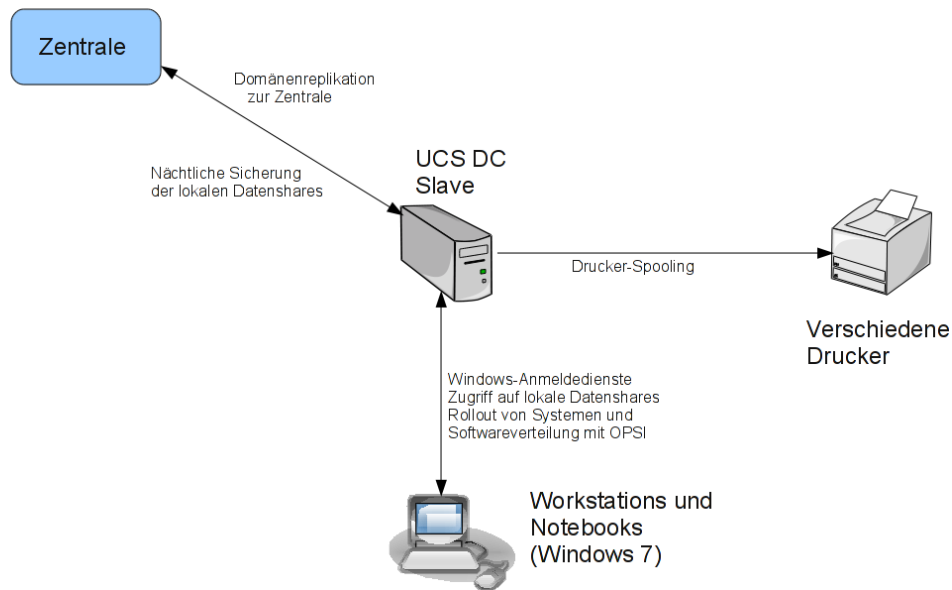


Abbildung 8: Aufbau eines Standort-Servers

4.2.1 Virtualisierung

Alle Serversysteme in der Umgebung der HVM sind mit Univention Virtual Machine Manager (UVMM) virtualisiert. Zum Einsatz kommt dabei ausschliesslich Open Source-Software.

Als Grundlage der Virtualisierung dienen Virtualisierungsserver auf UCS-Basissystemen (minimale UCS-Installationen ohne tiefere Integration in den Verzeichnisdienst). Auf diesen laufen jeweils ein bis mehrere virtuelle Maschinen mit der Virtualisierungslösung Xen. UCS- und Windows-Systeme werden paravirtualisiert betrieben, d.h. durch einen Zugriff der virtualisierten Systeme auf die Ressourcen der Wirtssysteme kann eine höhere Performance erzielt werden.

Alle virtuellen Maschinen können über den webbasierten Univention Virtual Machine Manager komfortabel angelegt und verwaltet werden. Werden Wartungsarbeiten an einem Virtualisierungsserver nötig, so können die auf diesem System laufenden virtuellen Maschinen im laufenden Betrieb auf einen anderen Server migriert werden.

Der Zugriff auf die virtuellen Maschinen wird durch eine Bibliothek abstrahiert, so dass neben Xen auch die Virtualisierungslösung KVM eingesetzt werden kann.

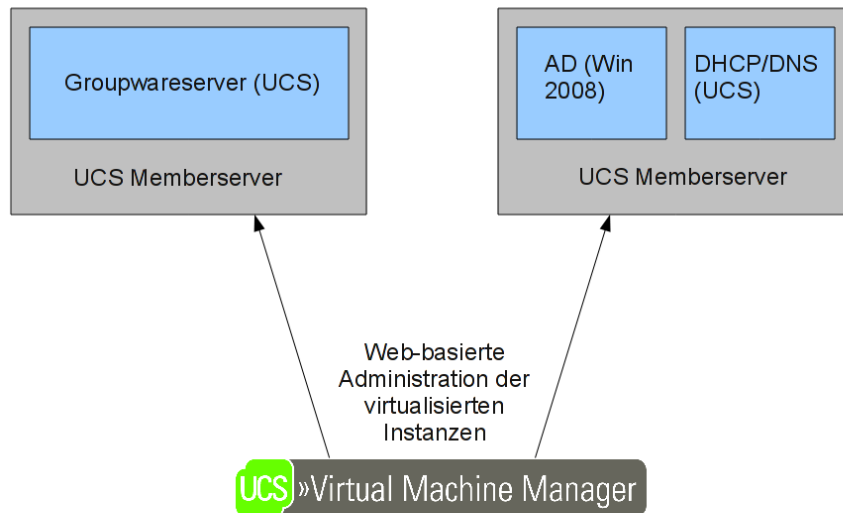


Abbildung 9: Virtualisierung der Serversysteme

4.2.2 Software-Verteilung der UCS-Systeme

Für die UCS-Domänencontroller wurden Installationsprofile erstellt. Mit diesen Profilen können mit dem Univention Net Installer PXE-basiert neue Systeme ausgerollt werden oder ggf. Systeme nach einem Hardwareausfall wieder hergestellt werden. Die Installation läuft dabei ohne weitere Benutzerinteraktion ab.

Für die Installation von Release-Updates und die Nachinstallation von Software-Paketen wird auf einem Server in der Zentrale eine zentrale Paket-Installationsquelle - das Repository - eingerichtet. Alle installierbaren Software-Pakete und -Updates werden dort vorgehalten.

Durch Richtlinien im Univention Directory Manager kann die Softwareverteilung zentral gesteuert werden. Zu einem frei wählbaren Zeitpunkt oder beim Herunterfahren/Starten des Systems werden dann Updates eingespielt oder Software-Pakete nachinstalliert.

Alle Systeme tragen die installierten Pakete automatisch in eine zentrale SQL-Datenbank ein, so dass ein Überblick über den Softwarebestand stets gewährleistet ist. Sicherheitsupdates für UCS werden zeitnah zum Download bereitgestellt und können ebenfalls automatisiert eingespielt werden.

4.2.3 Anbindung von Windows-Clients und Software-Verteilung

Für die Windows-Systeme wird durch Samba eine Windows-Domäne realisiert. Ein UCS-Domänencontroller übernimmt die Funktion des primären Domänencontroller (PDC) und bietet Datei- und Druckdienste an. Die Samba-Domäne verwendet die Benutzerdaten des UCS-LDAP-Verzeichnisses.

Wenn ein Benutzer unter Microsoft Windows sein Passwort ändern möchte, ruft er die gewohnte Windows-Funktion dafür auf. Der Änderungswunsch wird automatisch an das LDAP-Verzeichnis des DC Master in der Zentrale weitergeleitet, dort umgesetzt und von dort an alle Samba-Systeme repliziert.

Das geänderte Passwort gilt nicht nur für die Windows-Anmeldung, sondern automatisch für alle Domänendienste, also z.B. auch für das Abrufen von E-Mails.

Auf den Windows-Clients läuft die Open Source-Softwareverteilung OPSI4UCS. Sie ermöglicht auf den Windows-Clients eine weitgehend automatisierte Verteilung von Sicherheitsupdates und Windows-Updates sowie den Rollout von Software-Paketen, so dass auch ohne dezidierten Administrator alle Systeme auf einem sicheren Stand betrieben werden. Die Konfiguration von OPSI4UCS integriert sich in das UCS-Managementsystem.

OPSI wird auch für den Rollout neuer Windows-Systeme verwendet. Diese werden über PXE automatisch installiert.

4.2.4 Kolab-Groupware

Zur Koordination von Terminen und zur Pflege firmenweiter Kontakte kommt Kolab zum Einsatz. Kolab integriert sich nahtlos in die Benutzerverwaltung des Univention Directory Manager, so dass die Groupware-Einstellungen direkt in den Benutzereinstellungen konfiguriert werden können.

Die Benutzer greifen auf zwei Wegen auf ihre Groupware-Daten zu: Primär erfolgt der Zugriff von den Windows-Systemen durch Microsoft Outlook 2008. Da Outlook Kolab nicht direkt unterstützt, wird es mit einem Connector (Bynari Connector) an Kolab angebunden. Außerdem steht für mobilen Zugriff oder Zugriff aus dem Home Office ein Webclient zur Verfügung, der den kompletten Groupware-Funktionsumfang über eine HTTPS-Verbindung bereitstellt.

Auf der Serverseite wird der Kolab-Groupware-Server auf zwei Domänencontroller Slave-Systemen umgesetzt. Bei Kolab erfolgt die Speicherung der Groupware-Daten intern in IMAP-Ordern. Diese werden durch den Cyrus-IMAP-Server bereitgestellt. Die Groupware-Daten werden mit Cyrus Murder redundant über beide Groupware-Server repliziert.

Spam-Mails werden mit der Klassifizierungssoftware Spamassassin klassifiziert und aussortiert. Nicht erkannte Spam-Mails können an Spamassassin übergeben werden, um die Erkennung weiter zu verbessern.

Viren werden über die Open Source-Lösung ClamAV erkannt und blockiert. Die Viren-Signaturen werden mehrmals täglich kostenfrei von einem Server aus dem Internet bezogen. Die zusätzliche Einbindung kommerzieller Malware-Scanner ist möglich.

Alle Benutzerinformationen aus dem UCS-Verzeichnisdienst werden automatisch in einen Kontakte-Ordner repliziert. So stehen die allgemeinen LDAP-Stammdaten der Benutzer automatisch in der Groupware zur Verfügung.

4.2.5 Active Directory-Anbindung

Der Univention Active Directory Connector (kurz AD Connector) ermöglicht eine Synchronisation von Verzeichnisdienstobjekten zwischen einem Microsoft Windows 2000/2003/2008 Server mit Microsoft Active Directory (AD) und dem OpenLDAP-Verzeichnisdienst in Univention Corporate Server.

Die Synchronisationseinstellungen können individuell festgelegt werden. Der Administrator erhält dadurch die Möglichkeit, die Synchronisation exakt zu steuern und nur ausgewählte Objekte und Attribute zu synchronisieren.

In der Umgebung der HMV erfolgen zwei Synchronisationen: Neben der UCS-Domäne existiert eine lokale Microsoft Windows Server 2008 Active Directory-Domäne. In diese werden alle Container, Organisationseinheiten, Benutzer und Gruppen synchronisiert. Die Benutzer nehmen eine Sonderstellung ein, da das Passwort im Microsoft Active Directory nicht über das LDAP-Protokoll abgefragt werden kann. Hierfür wird ein zusätzlicher Dienst auf dem Windows-Server installiert, der diese Passwortsynchronisation ermöglicht. Die Rechnerkonten werden nicht synchronisiert, da Windows-Rechner nur in eine Domäne eingebunden sein können. Alle Windows-Clients sind in die UCS-Samba-Domäne gejoint.

Da in beiden Domänen die gleichen Benutzereinstellungen greifen, können Benutzer transparent auf Dienste beider Umgebungen zugreifen. So kann etwa ein Benutzer sich sowohl an seinem Notebook am UCS-Verzeichnisdienst als auch am Citrix-Server im Microsoft Active Directory mit dem selben Benutzernamen und Kennwort anmelden.

Nachdem eine Domänenanmeldung an einer UCS-Domäne durchgeführt wurde, ist anschließend eine Verbindung zu einer Dateifreigabe mit Microsoft Active Directory ohne erneute Passwortabfrage möglich. Auf den Ressourcen der anderen Domäne finden Benutzer und Administratoren gleichnamige Benutzer und Gruppen vor und können so mit den gewohnten Rechtsstrukturen arbeiten.

Neben der Synchronisation der UCS-Daten in die lokale AD-Domäne erfolgt außerdem eine Replikation in das Microsoft Active Directory-Verzeichnis des Mutterkonzerns.

4.2.6 Compliance-Anforderungen

Die HMV muss eine Reihe von Compliance-Anforderungen im Versicherungswesen erfüllen:

- Alle LDAP-Schreibzugriffe müssen verifizierbar sein. Hierzu wird der Univention Directory Logger eingesetzt. Dieser schreibt jede LDAP-Änderung in eine gesicherte Transaktions-Logdatei, die über Prüfsummen revisionssicher protokolliert wird.

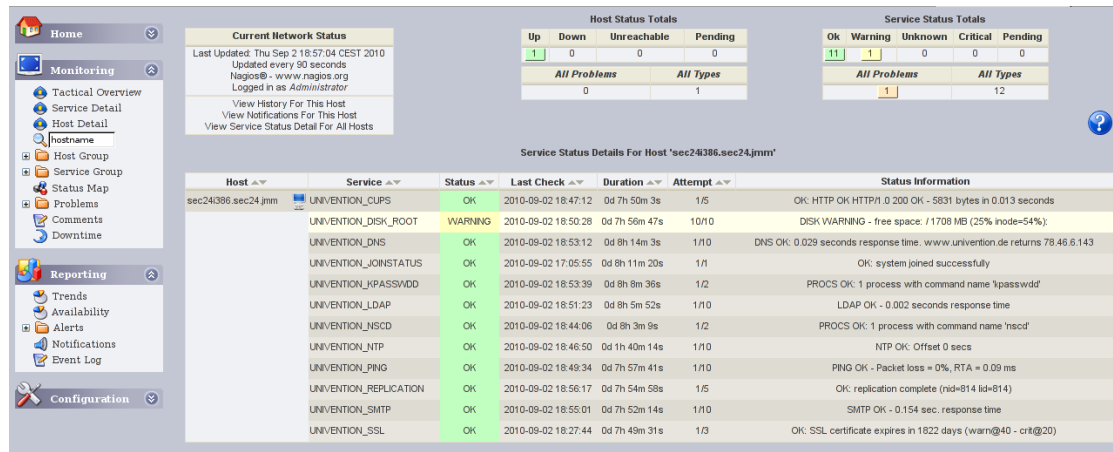
- Die Benutzerdaten müssen zeitnah für eine Betriebsprüfung abrufbar sein. Hierfür kann über Univention Directory Reports aus dem Univention Directory Manager heraus ein PDF-Dokument oder eine CSV-Datei über alle oder einige Benutzer und Gruppen erstellt werden.
- Es müssen Qualitätsstandards für Passwörter etabliert werden. In UCS kann für Passwörter beispielsweise eine Mindestanzahl von Klein- und Großbuchstaben, Sonderzeichen oder Ziffern konfiguriert werden. Außerdem können Passwörter gegen Listen unsicherer Passwörter (z.B. "secret") abgeglichen werden.

4.2.7 System-Monitoring mit Nagios

UCS integriert die Systemüberwachungssoftware Nagios, die die Überwachung komplexer IT-Strukturen aus Netzen, Rechnern und Diensten ermöglicht. Nagios bringt eine umfassende Sammlung an Überwachungsmodulen mit, die ggf. auch noch erweitert werden können.

Die Konfiguration von Nagios erfolgt weitestgehend im Univention Directory Manager.

Über eine webbasierte Oberfläche kann der Zustand der überwachten Objekte einfach abgefragt werden. Darüber hinaus wird Nagios so konfiguriert, dass beim Auftreten von Fehlern E-Mails an die Administratoren verschickt werden. Für gravierende Fehler werden SMS-Kurznachrichten verschickt.



The screenshot shows the Nagios web interface. At the top, there are summary boxes for 'Current Network Status', 'Host Status Totals', and 'Service Status Totals'. The 'Host Status Totals' box shows 11 Up, 0 Down, 0 Unreachable, and 0 Pending. The 'Service Status Totals' box shows 11 Ok, 1 Warning, 0 Unknown, 0 Critical, and 0 Pending. Below these is a table titled 'Service Status Details For Host 'sec24386.sec24.jmm''.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
sec24386.sec24.jmm	UNIVENTION_CUPS	OK	2010-09-02 18:47:12	0d 7h 50m 3s	1/5	OK: HTTP OK HTTP/1.0 200 OK - 5831 bytes in 0.013 seconds
	UNIVENTION_DISK_ROOT	WARNING	2010-09-02 18:50:28	0d 7h 56m 47s	10/10	DISK WARNING - free space: /1708 MB (25% inode=54%)
	UNIVENTION_DNS	OK	2010-09-02 18:53:12	0d 8h 14m 3s	1/10	DNS OK: 0.029 seconds response time: www.univention.de returns 78.46.6.143
	UNIVENTION_JOINSTATUS	OK	2010-09-02 17:05:55	0d 8h 11m 20s	1/1	OK: system joined successfully
	UNIVENTION_KPASSWD	OK	2010-09-02 18:53:39	0d 8h 8m 36s	1/2	PROCS OK: 1 process with command name 'kpasswd'
	UNIVENTION_LDAP	OK	2010-09-02 18:51:23	0d 8h 5m 52s	1/10	LDAP OK - 0.002 seconds response time
	UNIVENTION_NSCD	OK	2010-09-02 18:44:06	0d 8h 3m 9s	1/2	PROCS OK: 1 process with command name 'nscd'
	UNIVENTION_NTP	OK	2010-09-02 18:46:50	0d 1h 40m 14s	1/10	NTP OK: Offset 0 secs
	UNIVENTION_PING	OK	2010-09-02 18:49:34	0d 7h 57m 41s	1/10	PING OK - Packet loss = 0%, RTA = 0.09 ms
	UNIVENTION_REPLICATION	OK	2010-09-02 18:56:17	0d 7h 54m 58s	1/5	OK: replication complete (rid=614 lid=614)
	UNIVENTION_SMTP	OK	2010-09-02 18:55:01	0d 7h 52m 14s	1/10	SMTP OK - 0.154 sec. response time
	UNIVENTION_SSL	OK	2010-09-02 18:27:44	0d 7h 49m 31s	1/3	OK: SSL certificate expires in 1822 days (warn@40 - crit@20)

Abbildung 10: Systemüberwachung auf einem Server

Nagios-Prüfungen können zeitlich eingeschränkt werden, so dass unkritische Werte beispielsweise nachts keine Meldungen auslösen.

4.2.8 Citrix Terminal Services

In der Zentrale arbeiten 150 Benutzer mit Terminaldiensten auf Basis von Citrix-XenApp 6.0. Der XenApp-Terminalserver läuft auf einem Memberserver, der in die lokale Microsoft Active Directory-Domäne gejoint wurde.

Der Zugriff auf die Citrix-Server erfolgt durch Thin Clients, die mit den UCS Thin Client Services betrieben werden: Die Thin Clients werden im UCS-Managementsystem angelegt und konfiguriert (die IP-Adresse kann beispielsweise zentral per DHCP zugewiesen oder die Bildschirm-auflösung zentral vorgegeben werden). Die von den Benutzern verwendeten Terminaldienste werden benutzerbezogen konfiguriert; die Konfiguration erfolgt über die Benutzer-Verwaltung des Univention Directory Managers.

Die Konfiguration der Citrix-Sitzung erfolgt über ICA-Dateien, die im Univention Directory Manager zugewiesen werden können.

4.2.9 Backup

Für die Datensicherung kommt SEP Sesam zum Einsatz. Es bietet ein verteiltes Sicherungskonzept mit verschiedenen Backup-Agenten, die sowohl komplette Systeme als auch Daten sichern können. Für die Sicherung von Datenbanken stehen etwa gesonderte Agenten zur Verfügung. Alle Daten werden von den Standort-Servern in die Zentrale kopiert und dort auf Bandmedien gesichert.

Distributed Replicated Block Device (DRBD) wird für die Spiegelung von Festplatten-Partitionen und anderen Blockgeräten über das Netzwerk zwischen zwei Servern verwendet. Dabei werden alle lokalen Schreibzugriffe zusätzlich über das Netzwerk an den zweiten Server übermittelt. Je nach Konfiguration besteht die Möglichkeiten einen Schreibzugriff auf die Festplatte erst dann als erfolgreich zu erachten, wenn dieser sowohl auf dem lokalen Server, als auch auf dem zweiten Server erfolgreich ausgeführt wurde. Somit besitzen beide Server zu jedem Zeitpunkt eine identische Kopie einer Festplatten-Partition.

4.2.10 Referenzen

- UCS-Handbuch
- UCS Thin Client Services-Handbuch
- Technisches Dokument UCS-Backup
- Technisches Dokument Profilbasierte Installation
- Technisches Dokument Univention Directory Manager Reports
- Technisches Dokument Nagios-Integration
- Technisches Dokument DRBD unter UCS
- Technisches Dokument Erweiterte Administration des Cyrus-Maildienstes
- Technisches Dokument UCS-Active Directory Connector
- http://wiki.univention.de/index.php?title=UVMM_Quickstart

- <http://wiki.univention.de/index.php?title=Passwort-Richtlinien>
- [http://wiki.univention.de/index.php?title=Opsl_\(28open_pc_server_integration\)](http://wiki.univention.de/index.php?title=Opsl_(28open_pc_server_integration))

5 Schulträger

5.1 Ausgangslage

Der Landkreis Rechtwede ist Schulträger für insgesamt acht Grundschulen, Gesamtschulen, Berufsschulen und Gymnasien.

Die Schulen haben in der Regel ein oder zwei Rechnerräume mit 20-30 PCs, an der Berufsfachschule Technik gibt es insgesamt neun PC-Pools mit zusammen 260 Rechnern.

Die Betreuung der PCs - etwa die Installation von Software - wird von interessierten Lehrern und teilweise von Computer-AGs übernommen. Viele Lehrer schrecken vor dem Einsatz von PCs im Unterricht zurück, da viele Schüler in Schulstunden mit Internetzugang abgelenkt sind. Das Verteilen von digitalem Unterrichtsmaterial - etwa ein PDF mit einer Übungsaufgabe - ist kompliziert und überfordert einige Lehrer.

Es gibt einen EDV-Verantwortlichen im Schulamt, der aber zu Wartungsarbeiten anreisen muss und aufgrund der Weiträumigkeit des Landkreises nur sporadisch vor Ort in den Schulen präsent sein kann.

An den meisten PCs - die mit Microsoft Windows XP oder Microsoft Windows 7 betrieben werden - gibt es nur ein gemeinsames Benutzerkonto. Die Rechner werden nicht zentral verwaltet.

Die Schüler verfügen deshalb über keinen persönlichen Speicherplatz auf dem Daten abgelegt werden können und der vor fremden Zugriffen geschützt ist.

Software-Installationsstände weichen oft voneinander ab und auf vielen Rechnern finden sich Viren und Trojaner, da Sicherheitsupdates nicht systematisch installiert werden.

5.2 Umsetzung

Der Schulträger implementiert eine Umgebung auf Basis von UCS@school, einer auf UCS basierenden IT-Komplettlösung mit zahlreichen Zusatzkomponenten für Nutzung, Betrieb und Management der Schul-EDV.

Zum Einsatz kommt eine Infrastruktur bestehend aus einem UCS Domänencontroller Master (DC Master), einem UCS Domänencontroller Backup (DC Backup) und mehreren UCS Domänencontroller Slave (nachfolgend Schul-DC genannt) an den einzelnen Schulen.

Aus Sicherheitsgründen sieht das Konzept von UCS@school vor, dass die Schul-DCs nur eine Teilreplikation des LDAP-Verzeichnisses des Domänencontroller Master vornehmen. In der

Standardeinstellung replizieren sie nur für sie relevante Teile (z.B. Benutzer und Gruppen der jeweiligen Schule) sowie die globalen Strukturen des LDAP-Verzeichnisses.

Der DC Master ist das Kernstück der UCS-Domäne. Auf diesem System wird die zentrale schreibbare LDAP-Kopie vorgehalten.

Der DC Backup stellt weitgehend eine Kopie des DC Master dar. Dadurch sind alle wichtigen Dienste doppelt im Netzwerk vorhanden, die Verfügbarkeit der Dienste wird weiter erhöht und die Last zwischen den UCS-Domänencontrollern verteilt. Sollte der DC Master durch einen Hardwaredefekt ausfallen, kann der DC Backup innerhalb kürzester Zeit zum DC Master umgewandelt werden.

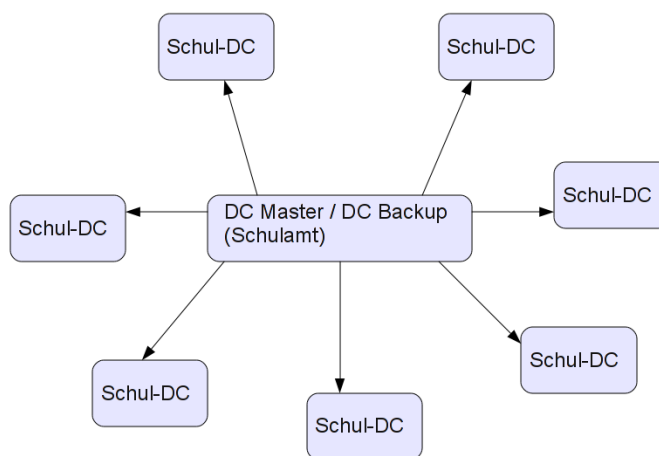


Abbildung 11: Schematischer Aufbau der Schul-Domäne

5.2.1 Verwaltung der Benutzerdaten

Alle Schulanmeldungen, -wechsel und Versetzungen werden durch die Schulverwaltung weiter in der gewohnten Verwaltungssoftware umgesetzt. Zu jedem Schuljahrwechsel erfolgt dann ein Import - im CSV-Format - der Schuldaten in die UCS-Benutzerverwaltung. Nachfolgende Änderungen können über den Univention Directory Manager vorgenommen werden.

In UCS@school existieren vier verschiedene Benutzerrollen:

- **Schüler**

- **Lehrer** verfügen gegenüber Schülern über weitergehende Berechtigungen. Sie können z.B. Passwörter von Schülern zurücksetzen oder den Internetzugang während einer Schulstunde sperren.
- **Schuladministratoren** sind technisch geschulte Lehrer, die weitergehende administrative Schritte übernehmen, z.B. die Verwaltung von Rechnergruppen oder Internetfiltern.
- **Mitarbeiter** sind Benutzer, die nicht direkt an den Schulen eingesetzt werden, also z.B. in der Schulverwaltung.

5.2.2 Dienste auf den Schul-Servern

Auf allen Schul-DCs wird ein lokaler LDAP-Verzeichnisdienst betrieben, auf den alle weiteren Dienste an dem Standort zugreifen. Der Schul-DC repliziert zu diesem Zweck automatisch das LDAP-Verzeichnis des Domänencontroller Master, so dass stets alle notwendigen Daten aktuell und vollständig vorgehalten werden. Der Betrieb des lokalen Verzeichnisdienstes reduziert so die zu übertragenden Datenmengen zum Domänencontroller Master und gewährleistet einen reibungslosen Betrieb, auch wenn die Verbindung zwischen Schul-DC und dem zentralen Domänencontroller Master-System einmal ausfallen sollte.

Auf allen Schul-DCs wird Samba für die Anbindung der Windows-Clients eingesetzt. An der Samba-Installation müssen keine Anpassungen vorgenommen werden, Windows-Clients können direkt der durch UCS bereitgestellten Windows-Domäne beitreten. Der Domänen-Join ist aus Client-Sicht identisch mit dem Beitritt zu einer Windows-basierten Domäne. Die Ablage der Benutzerdaten erfolgt auf einer Heimatverzeichnisfreigabe, die von den Schul-DCs bereitgestellt wird. Schüler und Lehrer haben dabei jeweils ein persönliches Heimatverzeichnis.

Auf den Windows-Clients läuft die Open Source-Softwareverteilung OPSI4UCS. Sie ermöglicht auf den Windows-Clients eine weitgehend automatisierte Verteilung von Sicherheitsupdates und Service Packs, so dass auch ohne dezidierten Administrator alle Systeme auf einem sicheren Stand betrieben werden. Die Konfiguration von OPSI4UCS integriert sich in das UCS-Managementsystem.

Für ein zentrales IP-Management läuft auf jedem Schul-DC ein mit Daten aus dem LDAP-Verzeichnis gepflegter DNS- und DHCP-Server.

Ausserdem läuft dort ein Print-Server, der Druckaufträge an den gewünschten Drucker weiterleitet. Die Printserver werden mit CUPS realisiert, das die verschiedenen Drucker in ein zentrales Spooling einbindet.

5.2.3 Werkzeuge für den pädagogischen EDV-Betrieb

UCS@school bringt verschiedene Werkzeuge für den pädagogischen EDV-Einsatz mit. Sie basieren auf Univention Management Console, einem webbasierten und modularen Frontend.



Abbildung 12: Schulspezifische Anwendungen

Passwort-Änderungen Über einen einfachen Assistenten können Lehrer die Passwörter von Schülern neu setzen. Schuladministratoren können überdies die Passwörter von Lehrern zurücksetzen.

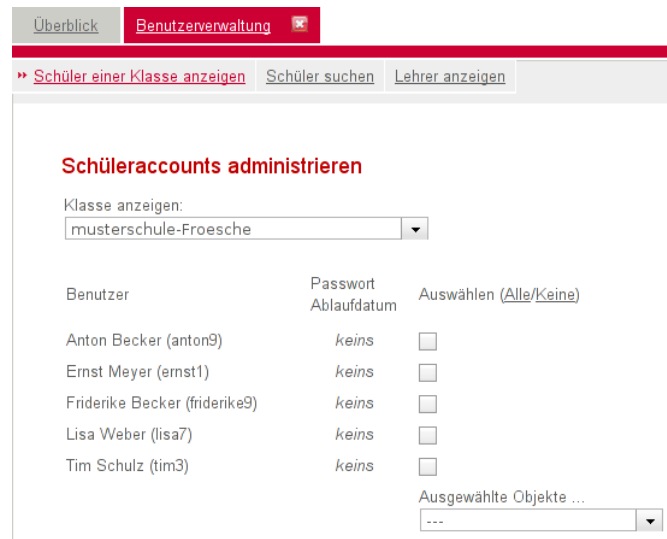


Abbildung 13: Benutzerverwaltung

Gruppenverwaltung Schuladministratoren können zusätzliche Gruppen, wie z.B. eine Informatik-AG, anlegen. Lehrer und Schuladministratoren können dann Schüler in diese zusätzlichen Gruppen hinzufügen oder sie wieder entfernen. Diese Zusatzgruppen sind unabhängig von der zentralen Datenpflege des Schulträgers und können allein von der Schule gepflegt werden.

Verwaltung von Rechnerräumen Mehrere Computer können von Schuladministratoren zu **Rechnerräumen** zusammengefasst werden. Für diese Rechnergruppen kann dann zentral der

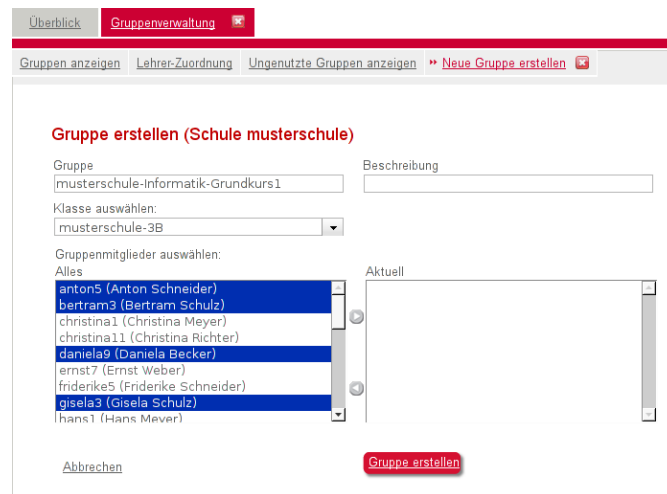


Abbildung 14: Gruppenverwaltung

Internetzugang kontrolliert werden oder die Schüler-Desktops mit iTALC (siehe Kapitel 5.2.5) zentral gesteuert werden.

Materialverteilung Lehrer können Unterrichtsmaterialien (etwa ein PDF-Formular mit einer Übung oder eine Präsentation) in die Heimatverzeichnisse von mehreren oder allen Schülern einer Klasse oder Gruppe verteilen. Die verteilten Dateien können manuell oder automatisch zu einem vorgegebenen Zeitpunkt vom Lehrer wieder eingesammelt und nach Schülern sortiert in seinem Heimatverzeichnis gespeichert werden.

5.2.4 Druckermoderation

Ein Modul ermöglicht Lehrern die Moderation wartender Druckaufträge. Die Druckaufträge können vorab eingesehen und angenommen oder abgelehnt werden. Schüler und Lehrer haben weiterhin die Möglichkeit, die angestoßenen Druckaufträge von einer Dateifreigabe vom Schul-DC zu beziehen, wo sie als PDF-Dokument abgelegt werden.

Unterrichtsvorbereitung Klassenräume können - auch wiederkehrend - reserviert werden. Einstellungen wie der Internetfilter oder zu verteilende Dateien werden dabei hinterlegt und automatisch beim Erreichen des reservierten Zeitraums aktiviert.

Zentrale Kontrolle des Internetzugangs Für Rechnerräume kann der Zugriff auf das Internet anhand von Filtern eingeschränkt werden. So kann etwa in einer Schulstunde, in der recherchiert werden soll, der Zugriff auf die Wikipedia-Domäne beschränkt werden. Lehrer haben außerdem die Möglichkeit den Internetzugriff nur für einen bestimmten Zeitraum freizugeben.

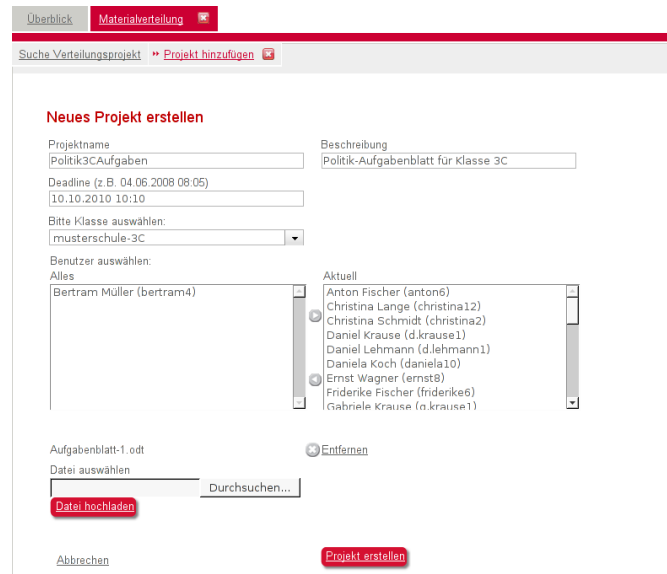


Abbildung 15: Materialverteilung

Helpdesk Über ein integriertes Kontaktformular können Lehrer sich mit einem Helpdesk in Verbindung setzen; in diesem Fall also dem Schulträger.

5.2.5 Management von Schüler-Desktops mit iTALC

iTALC ist eine didaktische Software für den Zugriff auf Schüler-Desktops. iTALC ist Open Source Software und wird auf den Schüler-Desktops installiert (es ist neben Microsoft Windows auch für Linux verfügbar).

Es bietet Lehrern unter anderem folgende Funktionen:

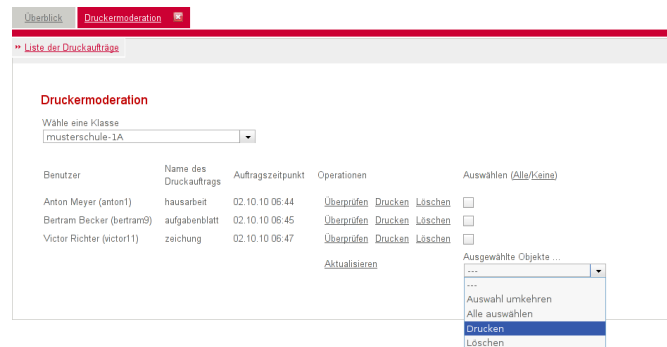


Abbildung 16: Druckermoderation

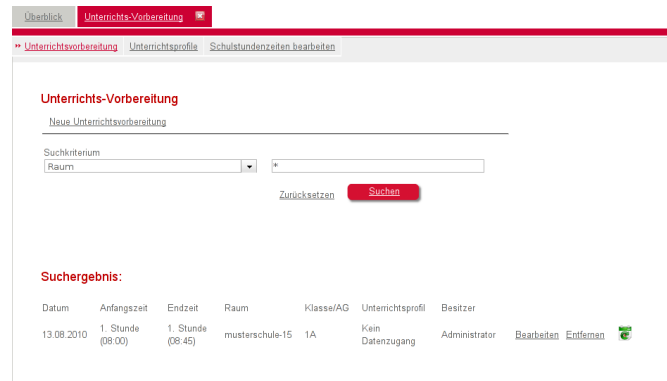


Abbildung 17: Unterrichtsvorbereitung

- Der Desktop eines Schülers kann eingesehen werden und der Lehrer kann ggf. auch unterstützend selbst Änderungen vornehmen.
- Über den Demo-Modus wird der Inhalt des Lehrer-Desktops an alle Schüler-Desktops übertragen. Dabei kann auch der Inhalt eines Schüler-Desktops für den Demo-Modus freigeschaltet werden.
- Um die ungeteilte Aufmerksamkeit der Schüler zu erreichen, können Bildschirme und Eingabegeräte zentral gesperrt werden.
- Rechner können über Wake-on-LAN zentral eingeschaltet und heruntergefahren werden.
- Textnachrichten können an Schüler verschickt werden.

Die iTALC-Einstellungen können pro Computerraum in einem Web-Assistenten konfiguriert werden.

5.2.6 Referenzen

- UCS-Handbuch
- UCS@School-Handbuch für Administratoren
- UCS@School-Handbuch für Lehrer



Überblick Webfilter Einstellungen

Webfilter-Profil » Profile zuordnen

Webfilter-Profil mit Gruppe verknüpfen

Bitte Gruppe auswählen:
musterschule-4B

Bitte Webfilter-Profil auswählen:
Kein_Internet

Setzen

Abbildung 18: Kontrolle des Internetzugangs