

Scenarios for Univention Corporate Server

Table of Contents

1. Lawyer's office	5
1.1. Initial situation	5
1.2. Systems and services	5
1.3. Management of user accounts	6
1.4. Managing the Windows computers	7
1.5. Storage management	7
1.6. Printer services	7
1.7. Groupware	7
1.8. Web proxy/web filter	7
1.9. Backup	7
1.10. Outlook	8
1.11. References	8
2. Medium-sized mechanical engineering company	9
2.1. Initial situation	9
2.2. Implementation	10
2.3. Domain controller / LDAP directory	11
2.4. Virtualization	11
2.5. Linux terminal services	12
2.6. Print services	13
2.7. Microsoft Windows terminal services	13
2.8. Integration of Oracle Solaris systems	14
2.9. Data management	14
2.10. Groupware	14
2.11. Outlook	15
2.12. References	15
3. Heterogenous enterprise environment in an insurance company	17
3.1. Initial situation	17
3.2. Implementation	17
3.3. Virtualization	19
3.4. Software distribution of UCS systems	20
3.5. Connecting Windows clients and Windows software deployment	20
3.6. Active Directory synchronisation	20
3.7. Groupware	21
3.8. Compliance requirements	21
3.9. System monitoring with Nagios	21
3.10. Integration of the AIX system	22
3.11. Citrix terminal services	22
3.12. Backup	22
3.13. Integration of SugarCRM	23
3.14. References	23
4. School board	25
4.1. Initial situation	25
4.2. Implementation	25
4.3. Management of user data	26
4.4. Services on the school servers	26
4.5. Tools for using IT-assisted teaching	27
4.6. Management of pupil's desktops using iTALC	30
4.7. Groupware	30
4.8. References	30

Chapter 1. Lawyer's office

1.1. Initial situation	5
1.2. Systems and services	5
1.3. Management of user accounts	6
1.4. Managing the Windows computers	7
1.5. Storage management	7
1.6. Printer services	7
1.7. Groupware	7
1.8. Web proxy/web filter	7
1.9. Backup	7
1.10. Outlook	8
1.11. References	8

1.1. Initial situation

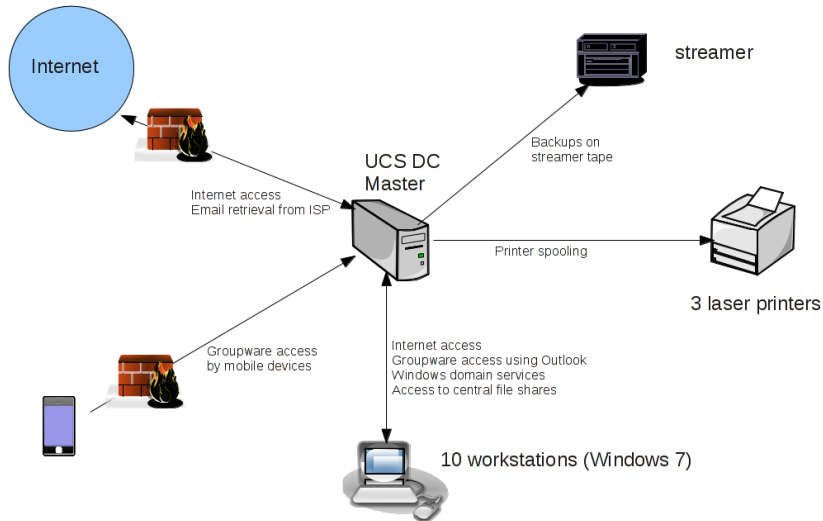
Hemmerlein & Sons lawyer's office has a total of ten employees. The employees work predominantly with office applications and a legal workflow management system, which is only available for Microsoft Windows. Windows 8 is employed as the client operating system. All the data are to be stored centrally on a server and backed up. As there is only limited technical expertise available and it is not viable to finance an in-house administrator team, particular value is placed on simple administration. The administrative duties described below can be configured completely via simple-to-use, web-based interfaces after a successful initial installation.

The company has a total of three laser printers (two identical black/white models and one colour laser printer), which are all installed in a central office. Large documents with high volumes are printed often.

1.2. Systems and services

UCS offers the required services and applications "out of the box" as a complete solution. A single UCS system is used, which provides the logon and file services for the Windows clients, administrates the printers and automates the data backup.

Figure 1.1. System overview of the lawyer's office Hemmerlein and Sons



1.3. Management of user accounts

User accounts for the ten employees are created in the Univention Management Console web interface. Each employee receives a password, which - as all user data - is saved in an LDAP directory service and requested when logging on to the Windows client.

Figure 1.2. Creating a user in Univention Directory Manager

The screenshot shows the Univention Management Console web interface. The top navigation bar includes the Univention logo, a dropdown menu, and user information: Host: sec.qai386.jmm, User: Administrator. The main content area is titled 'Users: hemmerlein' and has tabs for General, Groups, Account, Contact, [Advanced settings], [Options], and [Policies]. The 'General' tab is selected, showing 'Basic settings'.

User account

Title	First name	Last name (*)
	Joseph	Hemmerlein
User name (*)	Description	
hemmerlein		
Password (*)	Password (retype) (*)	
••••••••	••••••••	
<input type="checkbox"/> Override password history <input type="checkbox"/> Override password check		
Primary e-mail address		

Personal information

Display name
Joseph Hemmerlein
Organisation
Hemmerlein & Sons

1.4. Managing the Windows computers

Samba 4 is used on the UCS system for the integration of Microsoft Windows clients. Samba 4 offers domain, directory and authentication services which are compatible with Microsoft Active Directory. These also allow the use of the tools provided by Microsoft for the management of group policies (GPOs).

Microsoft Windows clients can join the Active Directory-compatible domain provided by UCS and can be centrally configured via group policies. From the client point of view, the domain join procedure is identical to joining a Microsoft Windows-based domain.

1.5. Storage management

Samba provides every user with a home directory on the UCS system as a file share via the CIFS protocol. The user thus always receives the same data irrespective of the computer he is logged in to. In addition, the central file storage allows central backups.

Moreover, there is a central share with legal literature, which is mounted on every client.

Similar to users, shares can also be created and managed web-based in the Univention Management Console.

1.6. Printer services

The UCS system provides print services via the CUPS software. Both network-capable printers and printers connected locally to a computer can be centrally administrated. The three printers can be configured conveniently via the Univention Management Console and are directly available to the users on their Microsoft Windows clients.

The two black and white laser printers are grouped together in a printer group: this means that, in addition to the targeted selection of a printer, users also have the opportunity of printing on a pseudo-printer. This is where the print jobs are distributed in turn between the two printers in the printer group. If one printers is busy, the free printer is selected instead, which cuts down waiting times.

1.7. Groupware

Zarafa4UCS, an integration of the groupware *Zarafa Collaboration Platform* in UCS, is installed on the UCS system from the App Center. Zarafa accesses the user data of the UCS directory service. The administration integrates seamlessly in the Univention Management Console. The employees use Microsoft Outlook 2010 as the groupware client.

Virus detection including signature updates and spam filters are integrated at no additional cost.

1.8. Web proxy/web filter

UCS has an integrated web filter based on Squid and Dansguardian, which checks web traffic for viruses using the integrated virus scanner ClamAV. In this way, trojans and viruses on websites are identified and filtered out. Potentially dangerous files such as executable files can also be blocked.

1.9. Backup

All files (both the users' files in the home directory and the legal literature files in the central share) are stored on the UCS system and can thus be centrally saved on a tape drive. For this UCS provides the backup software Bacula, which can be used flexibly for different backup and archiving strategies.

1.10. Outlook

With regard to a planned merger of another office in Munich, it will be simple to install a further UCS system in this branch. All LDAP data are then automatically transferred to the site server allowing the employees to logon at on-site meetings in Munich with their standard user credentials.

The existing Active Directory installation at the Munich office can be migrated to the UCS domain fully automated using Univention AD Takeover.

1.11. References

- <http://docs.univention.de/manual.html> (UCS manual)
- <http://www.univention.de/en/products/ucs/app-catalogue/app/details/zarafa> (Zarafa Collaboration Platform)
- http://wiki.univention.de/index.php?title=UCS_3.1_Univention_AD_Takeover

Chapter 2. Medium-sized mechanical engineering company

2.1. Initial situation	9
2.2. Implementation	10
2.3. Domain controller / LDAP directory	11
2.4. Virtualization	11
2.5. Linux terminal services	12
2.6. Print services	13
2.7. Microsoft Windows terminal services	13
2.8. Integration of Oracle Solaris systems	14
2.9. Data management	14
2.10. Groupware	14
2.11. Outlook	15
2.12. References	15

2.1. Initial situation

Gunapa Technologies is one of the leading manufacturers of rolled steel mills. At the company headquarters in Germany, 260 people are employed in Production, Administration, Design and Sales. In addition, there are also local offices in the USA, Argentina and India, each with 5-10 employees.

Linux is predominantly used on the desktops. The employees from Design and Development are dependent on Linux software and require a freely configurable desktop.

The employees from Administration and Sales will only be offered an office suite, an e-mail client and a web browser. The desktop should not be able to be modified by these users.

An accounting software required by some users is only available for Microsoft Windows. Part of the design process is performed with a CAD software, which is only available for Oracle Solaris.

The administration of the computers should be as central as possible. Whilst there are two IT technicians in the headquarters, there are no technical personnel at the other three branch offices.

To avoid non-productive times caused by malfunctions, the majority of the offered services must be provided redundantly.

To save energy and minimise maintenance costs, the employees in Administration and Sales will be provided with thin clients (computers without hard drives). As no data or configurations are saved locally, a defective thin client can be easily replaced even by non-technical staff.

A proxy server will buffer the network traffic in a cache and provide virus protection.

A groupware solution is required for the coordination of the globally distributed work procedures.

All user data are centrally saved on an Storage Area Network device (SAN).

2.2. Implementation

Figure 2.1. System overview of Ganupa Technologies headquarters (virtualization is not considered)

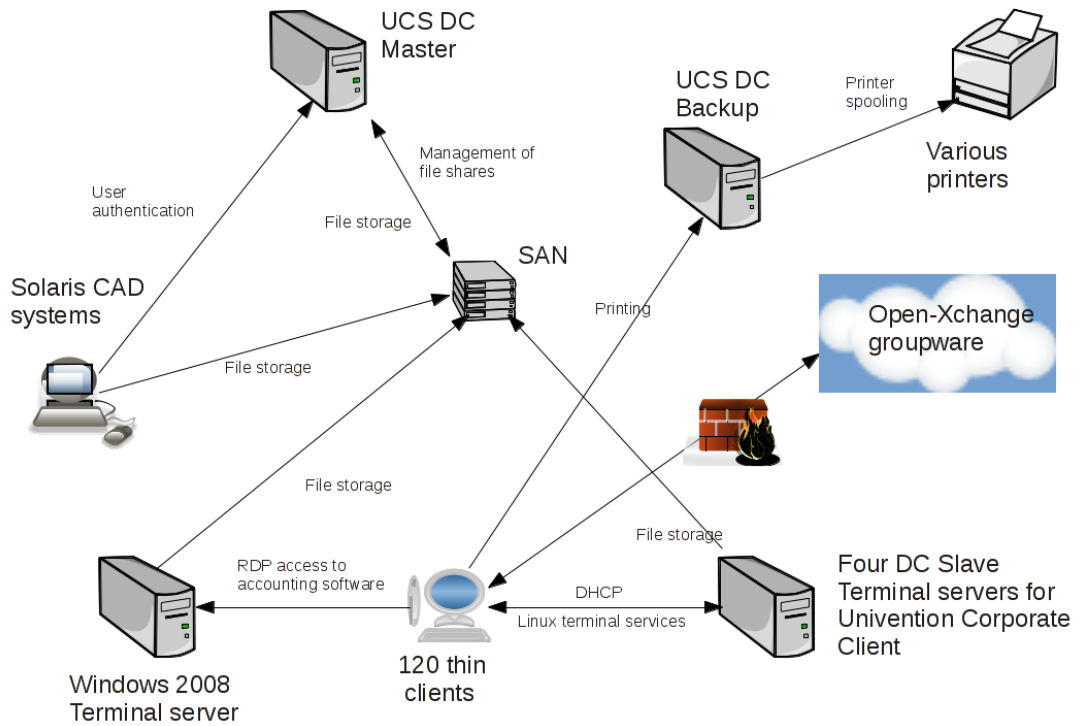
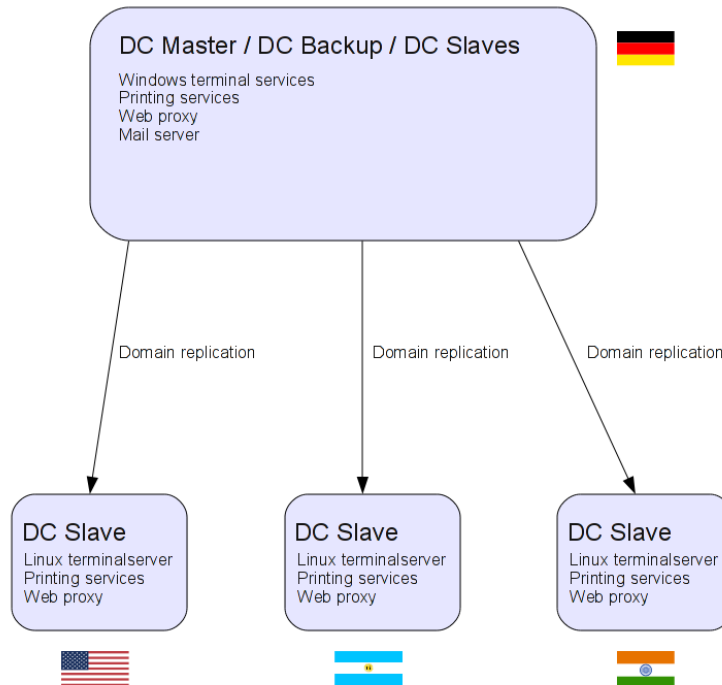


Figure 2.2. Global organisation scheme of Ganupa Technologies

2.3. Domain controller / LDAP directory

The company implements an infrastructure composed of a UCS domain controller master (DC master), a UCS domain controller backup (DC backup), several UCS domain controller slaves (DC slaves) and thin clients.

The DC master is the centrepiece of the UCS domain. The central, writeable copy of the LDAP directory service is maintained on this system.

The DC backup largely represents a copy of the DC master. In this way, the important services are available doubled on the network, the availability of the services is thus further increased and the load is distributed between the UCS domain controllers.

If the DC master fails as a result of a hardware defect, the DC backup can be converted to the DC master in a very short time.

The DC master and DC backup are both installed at the company headquarters. The two UCS systems operate an LDAP server and provide login services for the domains. A DNS and DHCP server maintained with data from the LDAP directory runs on both systems and provides central IP management. A print server is set up on the DC backup.

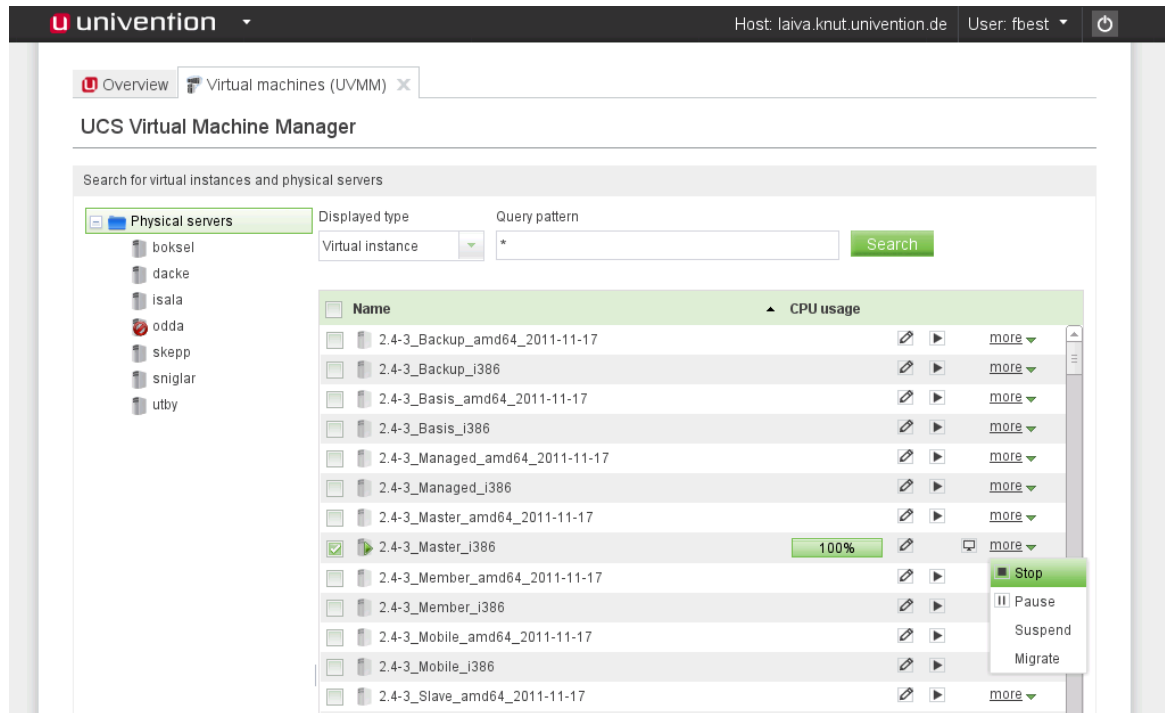
2.4. Virtualization

All server systems of Ganupa Technologies are virtualized with UCS Virtual Machine Manager (UVMM). Only open source software is used.

Virtualization servers based on UCS member servers (UCS servers without a local LDAP server) form the basis for the virtualization. Each of these hosts one or more virtual machines with the KVM virtualization

solution. UCS and Microsoft Windows systems are operated paravirtualized, i.e., the direct access of the virtualized systems to the hosts' resources results in better performance. Paravirtualization drivers for Xen and KVM are provided by Univention as signed MSI installation packages and, as such, can be installed simply.

Figure 2.3. Managing virtual machines with UVMM



All virtual machines can be created and managed conveniently over the web-based UCS Virtual Machine Manager. If maintenance work is necessary on a virtualization server, the virtual machines running on this system can be migrated to another server while still running.

Snapshots allow a simple rollback of updates in the case of error.

The access to the virtual machines is abstracted via a library, so that the virtualization solution Xen can also be used alongside KVM.

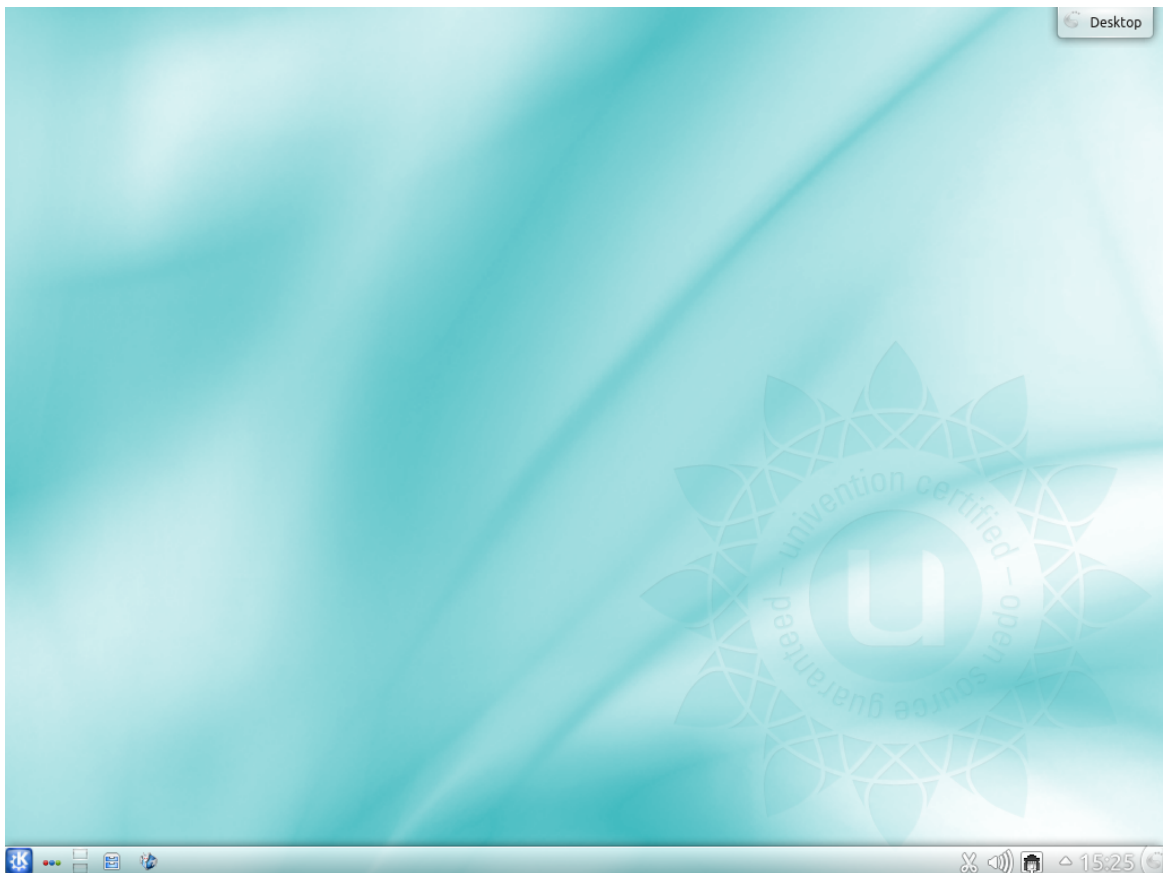
2.5. Linux terminal services

Four domain controller slave systems are installed in the company headquarters. They serve as Linux terminal servers, which can be accessed with thin clients.

The users' applications are run on the terminal servers, while the thin clients merely display the applications and transmit the user inputs to the terminal servers. The screen content is provided by the RDP server xrdp, allowing a low-bandwidth access using the Remote Desktop Protocol (RDP).

The user data are saved on the central SAN. The share used for this is administrated in the Univention Management Console.

The Univention Corporate Client with the KDE 4 desktop is used on the Linux terminal servers. All of the applications required for office duties are supplied as standard (word processing, databases, presentations and spreadsheet analysis with LibreOffice, image processing with Gimp, Mozilla Firefox as web browser, Mozilla Thunderbird as groupware and e-mail client, multimedia applications for playing music and videos and burning DVDs/CDs).

Figure 2.4. Centrally managed Univention Corporate Client

Preconfigured desktops are available for different user groups, in which different applications are preconfigured depending on the duties involved. For example, Administration uses a desktop on which only Mozilla Firefox and LibreOffice are installed, while the technicians have access to a much wider spectrum of applications.

2.6. Print services

Print jobs are forwarded to the requested printer via a print server. The print servers are realised with CUPS, which manages the different printers in a central spooling.

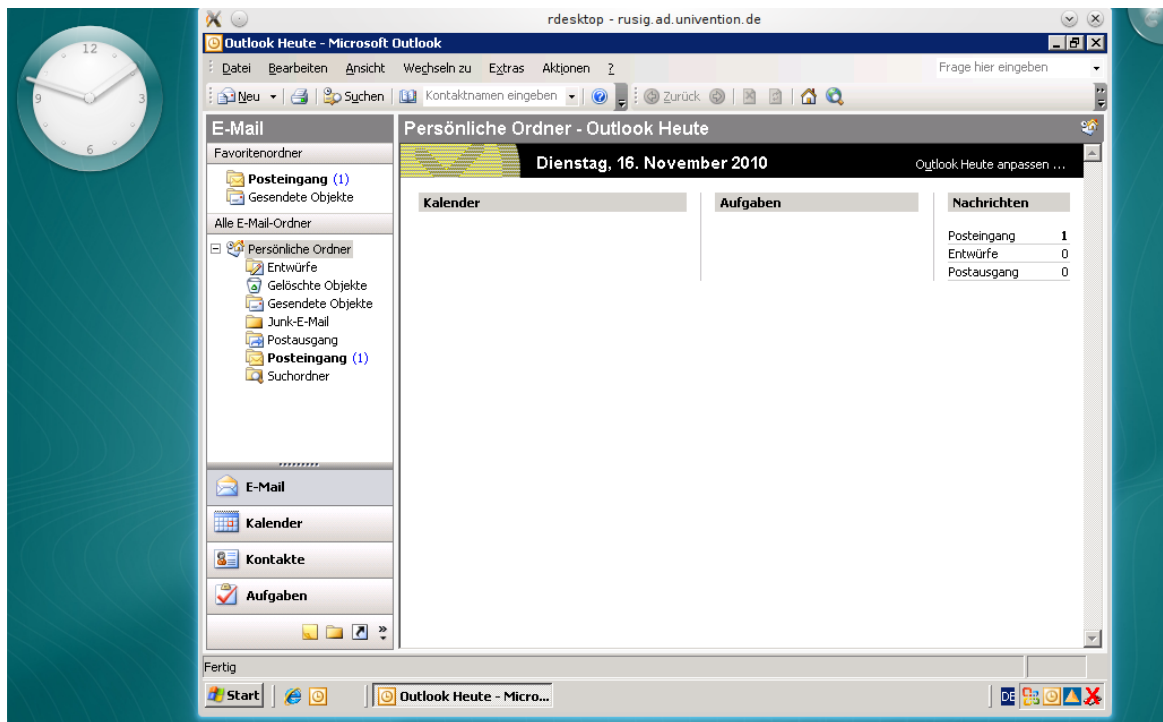
In some larger offices several printers are grouped together into a printer group; the users simply print on this group, whereby the print jobs are equally distributed and the next free printer is used. This saves the users from having to check whether a particular printer is already in use.

In addition, every printer is assigned a page price. This allows Accounting to determine the incurred printing costs per user. This can optionally also be connected to a limit on the number of pages which can be printed.

2.7. Microsoft Windows terminal services

Samba 4 is used to create a Windows domain in which a Microsoft Windows terminal server is joined as a member server. This server is used to run the accounting software, which only functions in Microsoft Windows. The application is displayed seamlessly on Linux desktops via an RDP client.

Figure 2.5. Integrating a Windows application in the Univention desktop client



The Linux and Samba domains use the same user data and users can access their home directories from Linux and Microsoft Windows.

2.8. Integration of Oracle Solaris systems

A specialist application for CAD design is only available for Oracle Solaris. The name services on the Solaris system have been adapted to query the UCS LDAP for authentication, i.e. users can log in to the Solaris system with their domain user identification and password. This negates the need for the additional maintenance of local Solaris user accounts.

The Solaris system is assigned its IP address from the UCS DHCP servers via DHCP. The files are saved on the UCS file servers via a NFS share.

2.9. Data management

All user data is stored on a central Storage Area Network (SAN) system. The different shares are registered and administrated in the Univention Management Console. The Linux and Solaris clients access individual shares via the network file system (NFS), the Windows clients via the CIFS protocol.

2.10. Groupware

Ganupa Technologies uses the groupware solution Open-Xchange Server Edition for arranging meetings and organising contacts and tasks.

The groupware server is operated as a slave domain controller system on the Amazon EC2 cloud. This allows flexible scaling of the groupware system to growing performance and storage requirements. The installation can be performed with a few clicks using the App Center.

The administration of the groupware-related attributes integrates seamlessly in the Univention Management Console. The employees access the groupware via the Open-Xchange web client and Mozilla Thunderbird.

Mobile devices (smartphones and tablets) are integrated via the Microsoft ActiveSync protocol.

Virus detection including signature updates and spam filters are integrated at no additional cost.

2.11. Outlook

At a later point in time, the plan is to monitor the Internet access centrally via a web proxy. For this purpose, UCS provides an integration of the web proxy Squid and the virus scanner ClamAV.

Alternatively, it is also possible to procure a specialised appliance, which can authenticate the users against the UCS-LDAP server.

2.12. References

- <http://docs.univention.de/manual.html> (UCS manual)
- <http://www.univention.de/en/products/ucs/app-catalogue/app/details/oxseforucs> (Open-Xchange Server Edition)

Chapter 3. Heterogenous enterprise environment in an insurance company

3.1. Initial situation	17
3.2. Implementation	17
3.3. Virtualization	19
3.4. Software distribution of UCS systems	20
3.5. Connecting Windows clients and Windows software deployment	20
3.6. Active Directory synchronisation	20
3.7. Groupware	21
3.8. Compliance requirements	21
3.9. System monitoring with Nagios	21
3.10. Integration of the AIX system	22
3.11. Citrix terminal services	22
3.12. Backup	22
3.13. Integration of SugarCRM	23
3.14. References	23

3.1. Initial situation

Hanseatische Marineversicherung (HMV) is an insurance company with 1800 employees specialised in the logistics sector. HMV is a subsidiary of the Vigil Insurances parent company.

The parent company operates an independent directory service based on Microsoft Active Directory, but the user data of the individual subsidiaries is managed internally.

The employees work at a total of 36 locations across the world with the largest being the company headquarter in Bremen with approximately 250 persons. Many of the users work on the move with laptops as salespersons or estimators.

Microsoft Windows 7 is used on all the desktops. Software distribution and the installation of security updates are centralised.

Citrix XenApp needs to be employed in the headquarters because of a superordinate group policy: users should access the terminal services with thin clients.

The groupware Microsoft Exchange is provided centrally by the parent company.

All users, computers and services should be centrally administrable. Critical system status should be reported promptly per e-mail and SMS.

All server systems in the headquarters should be virtualized. The resulting considerable significance of virtualization requires the implementation of an open source solution.

Data backup is performed centrally in Bremen.

Different international compliance requirements from the insurance sector must be satisfied.

3.2. Implementation

The company implements an infrastructure composed of a master domain controller (DC master), a backup domain controller (DC backup), several UCS slave domain controller (DC slaves) and 150 thin clients.

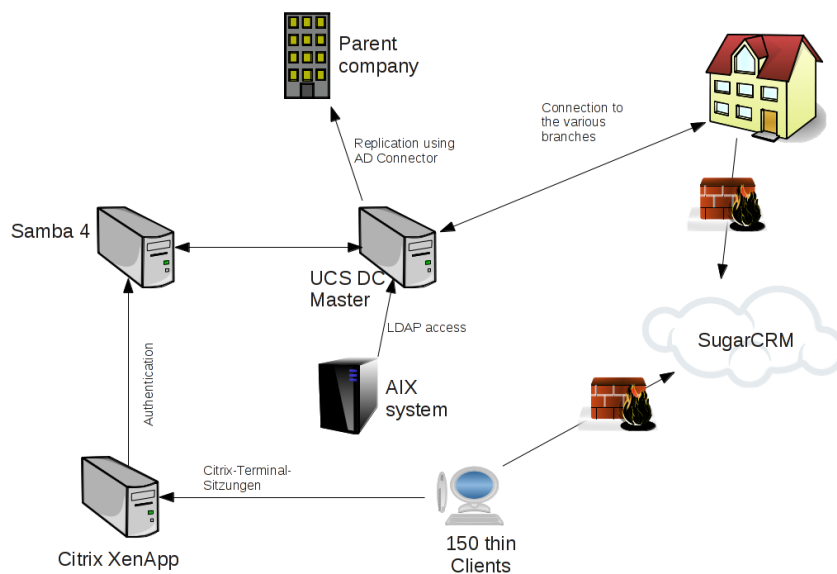
Implementation

The DC master is the centrepiece of the UCS domain. The central, writeable LDAP directory is provided on this system.

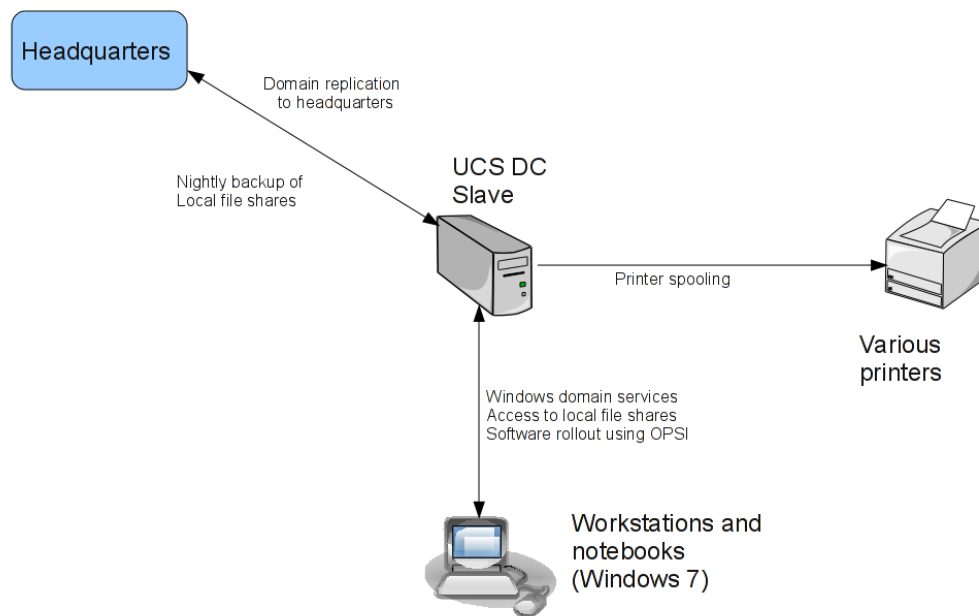
The DC backup also largely represents a copy of the DC master. In this way, the important services are available doubled on the network, the availability of the services is thus further increased and the load is distributed between the domain controllers.

If the DC master fails as a result of a hardware defect, the DC backup can be converted to the DC Master in a very short time.

Figure 3.1. General overview (excluded: storage, DNS, DHCP, print services, virtualization, backup)

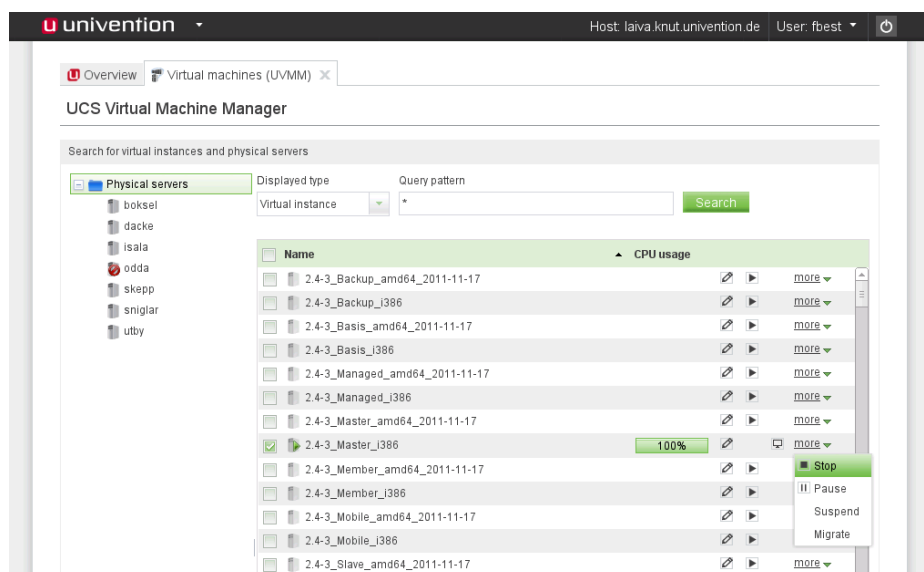


The DC master and DC backup are both installed at the company headquarters. The locations also contain additional slave domain controller systems, which provide Windows domain services, print services and software distribution.

Figure 3.2. Structure of a location

3.3. Virtualization

All server systems in the HMV environment are virtualized with UCS Virtual Machine Manager (UVMM). Only open source software is used.

Figure 3.3. Managing virtual machines with UVMM

Virtualization servers based on UCS member servers (server installations without a local LDAP server) form the basis for the virtualization. Each of these hosts one or more virtual machines with the Xen virtualization solution. UCS and Windows systems are operated paravirtualized, i.e., the direct access of the virtualized systems to the hosts' resources results in better performance.

All virtual machines can be created and managed conveniently over the web-based UCS Virtual Machine Manager. If maintenance work is necessary on a virtualization server, the virtual machines running on this system can be migrated to another server while still running.

The access to the virtual machines is abstracted via a library, so that the virtualization solution KVM can also be used alongside Xen.

3.4. Software distribution of UCS systems

Installation profiles have been created for the UCS domain controllers. These profiles can be used to roll out new systems with the Univention Net Installer using PXE or, as required, to restore systems after hardware failure. The installation concludes without further user interaction.

A central package installation source - the repository - is established on a server in the headquarters for the installation of release updates and the subsequent installation of software packages. All installable software packages and updates are provided there.

Policies in the Univention Management Console can be used to control the software distribution centrally. The updates can be installed or software packages can be subsequently installed at a freely selectable time or when shutting down / starting up the system.

All systems record the installed packages in a central SQL database automatically so that an overview of the software inventory is always available. Security updates for UCS are promptly provided to download and can also be installed automatically.

3.5. Connecting Windows clients and Windows software deployment

Samba 4 is used in the HNV for the integration of Microsoft Windows clients. Samba 4 offers domain, directory and authentication services which are compatible with Microsoft Active Directory. These also allow the use of the tools provided by Microsoft for the management of group policies (GPOs).

Windows clients can join the Active Directory-compatible domains provided by UCS directly and can be centrally configured via group policies. From the client point of view, the domain join procedure is identical to joining a Windows-based domain.

The Open Source software distribution opsi runs on the Windows clients. It allows an extensively automated distribution of security updates and Windows updates as well as the rollout of software packages to the Windows clients. The configuration of opsi integrates itself into the UCS management system with OPSI4UCS.

opsi is also used for the rollout of new Windows systems. These are automatically installed via PXE.

3.6. Active Directory synchronisation

The Univention Active Directory connector (AD connector for short) makes it possible to synchronise directory service objects between a Microsoft Windows 2000/2003/2008/2012 server with Microsoft Active Directory (AD) and an Open Source LDAP directory service in Univention Corporate Server.

The synchronisation settings can be specified individually. The administrator thus has the possibility of controlling the synchronisation precisely and only synchronising selected objects and attributes.

The UCS directory service synchronises with the Microsoft Active Directory of the parent company. The replication encompasses all the containers, organisational units, users and groups. Users have a special position since the password cannot be queried via the LDAP protocol in Microsoft Active Directory. A system service is installed on the Windows server for this purpose, which enables password synchronisation.

The computer accounts are not synchronised, as Windows computers can only be joined in one domain. All Windows clients are joined in the UCS Samba 4 domain.

3.7. Groupware

The groupware is provided in the form of Exchange Server 2010 by the parent company Vigil Insurances, allowing the users to access it using Outlook 2010 and Outlook WebAccess.

The integration of the UCS directory service and the Active Directory of the parent company allows authentication with the same user name / password.

Users can access the services of both environments in a transparent way, as the same user settings apply in both domains. For example, a user can log into both the UCS directory service on his laptop and the Citrix Server in the Microsoft Active Directory with the same user name and password.

3.8. Compliance requirements

HMV must satisfy a range of insurance industry compliance requirements.

- All LDAP write accesses must be verifiable. This is done by means of the Univention Directory Logger. This transcribes each LDAP change in a secure transaction log file, which is protocolled audit-compliantly with checksums.
- The user data must be available immediately for external audit purposes. To do so, Univention Directory Reports can be used to create a PDF document or a CSV file of all or some users and groups from the Univention Management Console.
- Quality standards must be established for passwords. In UCS, for example, one can set a minimum number of lowercase and uppercase characters, symbols or figures for passwords. In addition, passwords can be compared against a list of unsafe passwords (e.g., *secret*).

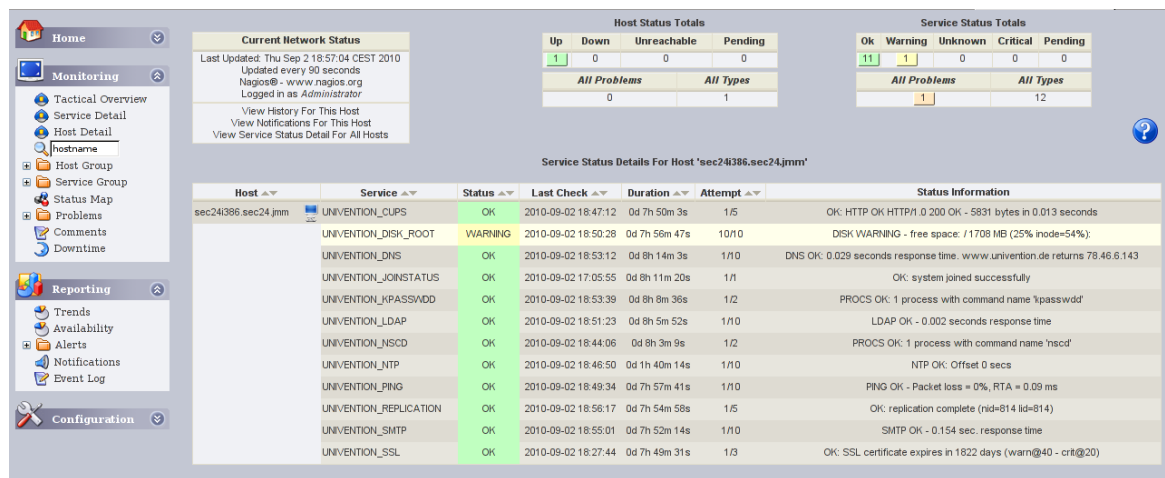
3.9. System monitoring with Nagios

UCS integrates the system monitoring software Nagios, which allows the monitoring of complex IT structures from networks, computers and services. Nagios includes a comprehensive range of monitoring modules, which can also be expanded if necessary.

The Nagios configuration is predominantly performed in the Univention Management Console.

A web-based interface can be used to check the status of the monitored objects. In addition, Nagios is configured in such a way that the administrators receive e-mails when errors occur. SMS messages are sent for serious errors.

Figure 3.4. System monitoring of a server



Nagios checks can be chronologically limited so that non-critical values don't trigger logging messages during the night, for example.

3.10. Integration of the AIX system

The insurance policies are administrated with an application which can only be operated on highly available POWER7 systems using IBM AIX.

In the past, all users working on the system were maintained doubly in the local user database of the AIX system. Now only the secldaplntd service runs on the AIX system; it performs all the authentication processes against the UCS LDAP directory.

3.11. Citrix terminal services

In the headquarters 150 users work with terminal services based on Citrix XenApp 6.0. The XenApp terminal server runs on a Windows member server, which joined the local Samba 4 domain.

Access to the Citrix server is performed via thin clients, which are operated with Univention Corporate Client (UCC): the thin clients are registered and configured in the UCS management system (for example, the IP address can be assigned centrally per DHCP or the monitor resolution can be centrally specified). The terminal services used by the users are configured user-specifically; the configuration is performed via the user administration of the Univention Management Console.

3.12. Backup

SEP sesam is used for file backup. It offers a distributed backup concept with different backup agents, which backup both complete systems and data. Special backup agents are available for the backup of databases. All data are copied from the standard servers in the headquarters and from there saved on tape media. The installation can be performed with a few clicks using the App Center.

Distributed replicated block device (DRBD) is used for the mirroring of hard drive partitions and other block devices via the network between two servers. In doing so, all local write accesses are additionally transferred to the second server via the network. Depending on the configuration you have the possibility to consider the write access to the hard drive as successful only once this has been run successfully on both the local server and the second server. In this way both servers have an identical copy of a hard drive partition at all times.

3.13. Integration of SugarCRM

SugarCRM 6.5 is employed as the CRM solution for sales personnel. The administration of the SugarCRM users and roles integrates directly in the Univention Management Console. The installation can be performed with a few clicks using the Univention App Center.

The installation is operated as a slave domain controller system on the Amazon EC2 cloud. This ensures high availability and allows flexible scaling to growing performance and storage requirements.

3.14. References

- <http://docs.univention.de/manual.html> (UCS manual)
- http://wiki.univention.de/index.php?title=UVMM_Quickstart
- [http://wiki.univention.de/index.php?title=Ops_\(28open_pc_server_integration\)](http://wiki.univention.de/index.php?title=Ops_(28open_pc_server_integration)) (currently only available in German)
- <http://docs.univention.de/ucc-manual-1.0.html> (Univention Corporate Client manual)
- <http://docs.univention.de/installation.html> (Extended installation documentation)
- <http://www.univention.de/en/products/ucs/app-catalogue/app/details/drbd> (DRBD)
- <http://www.univention.de/en/products/ucs/app-catalogue/app/details/sep-sesam> (SEP sesam Backup)
- <http://www.univention.de/en/products/ucs/app-catalogue/app/details/sugarcrm> (SugarCRM)

Chapter 4. School board

4.1. Initial situation	25
4.2. Implementation	25
4.3. Management of user data	26
4.4. Services on the school servers	26
4.5. Tools for using IT-assisted teaching	27
4.6. Management of pupil's desktops using iTALC	30
4.7. Groupware	30
4.8. References	30

4.1. Initial situation

The administrative district Reichtweide is the school body for a total of eight primary schools, comprehensive schools, vocational schools and grammar schools.

The schools generally have one or two computer rooms with 20-30 PCs. The technical vocational school has a total of nine PC pools with 260 computers all together.

These PCs are maintained - for example, the installation of software - by interested teachers and to some extent by school computer clubs. Many teachers shy away from using PCs in the classroom, as many students are distracted by Internet access during lessons. Distributing digital teaching materials - for example, a PDF with an exercise - is complicated and overwhelms some teachers.

There is an IT officer in the local education authority, who has to travel to the schools to perform maintenance work and can only be present in the individual schools sporadically due to the size of the administrative district.

On most PCs - which are operated on Microsoft Windows XP or Microsoft Windows 7 - there is one common user account. The computers are not centrally administrated.

As a result, the pupils do not have personal directories for saving their work which cannot be accessed by others.

Software installation versions are often different on the computers and many computers have viruses and trojans as security updates are not installed systematically.

An additional aim is to introduce a groupware solution for simpler arrangement of meetings between the teaching staff.

4.2. Implementation

The school board is implementing an environment based on UCS@School, a complete IT solution based on UCS with numerous additional components for the use, operation and management of the schools' IT.

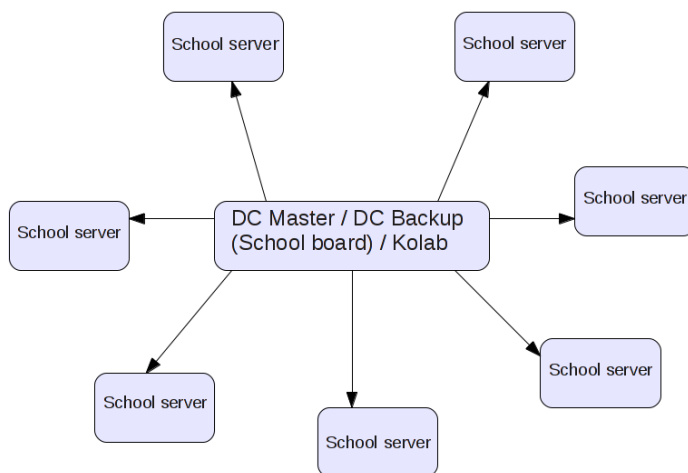
This involves the implementation of an infrastructure composed of a UCS master domain controller (DC master), a backup domain controller (DC backup) and several slave domain controller (hereinafter called school server) in the individual schools.

For security reasons, the UCS@School concept specifies that the school servers only perform a partial replication of the master domain controller's LDAP directory. In the default setting they only replicate the parts relevant for themselves (e.g., users and groups of the respective school) and the global structures of the LDAP directory.

The DC master is the centrepiece of the UCS domain. The central, writeable copy of the LDAP directory service is provided on this system.

The DC backup largely represents a copy of the DC master. In this way, the important services are available doubled on the network, the availability of the services is thus further increased and the load is distributed between the UCS domain controllers. If the DC master fails as a result of a hardware defect, the DC backup can be converted to the DC Master in a very short time.

Figure 4.1. Structure of the school domain



4.3. Management of user data

All school registrations, changes and transfers are managed in the school administration software Magellan by the school administration office. When the school year changes, the school data are imported - in CSV format - into the UCS user administration. Subsequent adjustments can be made via the Univention Management Console.

There are four different user roles in UCS@School:

- *Students*
- *Teachers* have more permissions than pupils. They can, e.g., reset pupil passwords or block Internet access during a lesson.
- *School administrators* are technically trained teachers who take on extensive administrative tasks, e.g., the administration of computer groups or Internet filters.
- *Staff* are users who are not employed directly at the schools, e.g., in the school administration office.

4.4. Services on the school servers

A local LDAP directory is operated on all school servers and can be accessed by all the other computers at the school. For this purpose, the school server automatically replicates the relevant subset of the LDAP directory of the master domain controller so that all the necessary data are available up-to-date and complete.

The operation of the local directory service thus reduces the data volumes to be transferred to the master domain controller and ensures seamless operation, even if the connection between the school server and the central master domain controller system fails.

Samba 4 is used on all the school servers for the integration of Windows clients. Samba 4 offers domain, directory and authentication services which are compatible with Microsoft Active Directory. These also allow the use of the tools provided by Microsoft for the management of group policies (GPOs).

Windows clients can join the Active Directory-compatible domains provided by UCS directly and can be centrally configured via group policies. From the client point of view, the domain join procedure is identical to joining a Windows-based domain.

User data are stored in a home share provided by the school servers. Pupils and teachers alike have their own personal home directory.

The open source software distribution opsi runs on the Windows clients. It allows a largely automated distribution of security updates and service packs to the Windows clients, with the result that all systems can be operated constantly fully protected even without a dedicated administrator. The OPSI4UCS configuration integrates opsi into the UCS management system.

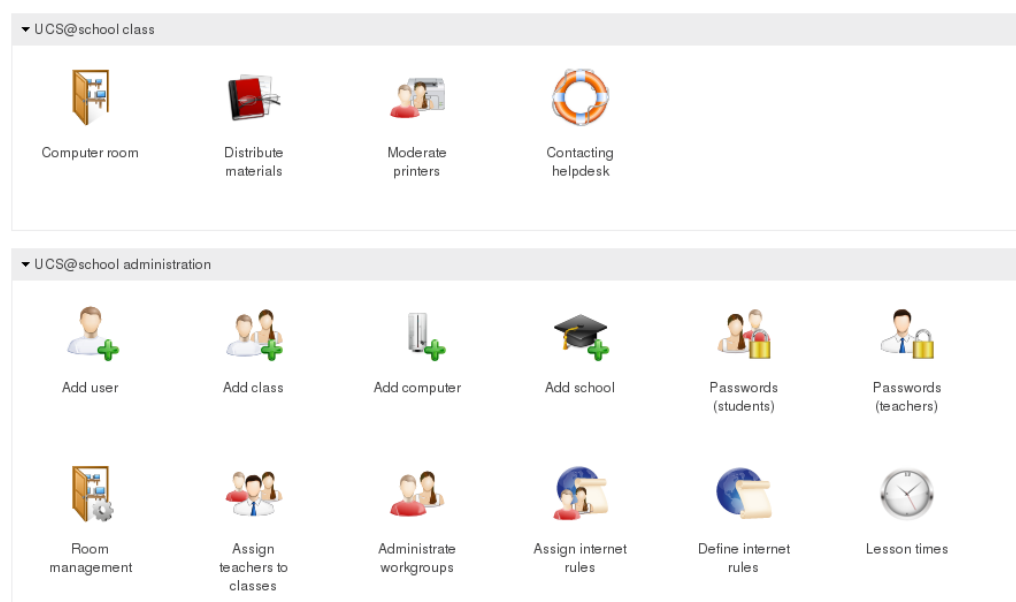
A DNS and DHCP server configured with data from the LDAP directory runs on every school server and provides central IP management.

In addition, there is a print server, which forwards print jobs on to the selected printer. The print servers are realised with CUPS, which integrates the different printers in a central spooling.

4.5. Tools for using IT-assisted teaching

UCS@school offers a range of modules for the Univention Management Console which can be used for IT-supported teaching.

Figure 4.2. Applications related to teaching



Some modules are available to teachers and school administrators, whilst other modules are reserved for school administrators.

Passwords (students) allows teachers to reset pupil passwords. The existing pupil passwords cannot be read in plain text, so if a pupil forgets his password, a new password needs to be entered. This can also be used by school administrators to reset teacher passwords.

Figure 4.3. Password reset

The screenshot shows a web interface for managing student passwords. At the top, there are tabs for 'Overview' and 'Passwords (students)'. Below the tabs is the title 'Reset passwords of student accounts'. A search section includes a dropdown for 'Class or workgroup' (set to 'All classes and workgroups'), a text input for 'Name', and a 'Search' button. Below the search section is a table with three columns: 'Name', 'Password expiration date', and 'Reset password'. The table lists ten students, all with a '-' in the expiration date column and a 'Reset password' button in the third column.

Name	Password expiration date	Reset password
Becker, Anton (anton9)	-	Reset password
Becker, Bertram (bertram9)	-	Reset password
Becker, Christina (christina9)	-	Reset password
Becker, Daniela (daniela9)	-	Reset password
Becker, Ernst (ernst9)	-	Reset password
Becker, Friderike (friderike9)	-	Reset password
Becker, Gisela (gisela9)	-	Reset password
Becker, Hans (hans9)	-	Reset password
Becker, Ines (ines9)	-	Reset password

The **Computer room** module allows the teacher to control the pupil PCs and Internet access during a lesson. Internet access can be blocked or permitted and individual web pages can be white-listed. If a special software (iTALC) is installed on the pupil PCs, these PCs can also be controlled remotely. For example, the screens can be locked so that, for example in a chemistry lesson, the pupils' undivided attention can be focussed on the experiment.

In addition, the contents of the screen of one PC can also be transferred to other systems. This makes it possible for the teacher to hold a presentation without a projector.

Each school is supported by a help desk. The help desk can, for example, be maintained by a support organisation in the education authority or by technically trained teachers in the schools. The **Contacting helpdesk** module allows the teachers and school administrators to send a support request.

Every pupil is a member of a class. In addition, there is also the possibility of using the **Administrate workgroups** module to assign pupils to cross-class workgroups.

The creation of a working group automatically creates a file share on the school server which can be accessed by all the members of the workgroup.

Teachers can add pupils to working groups or remove them, but cannot create any new working groups. This must be done by a school administrator.

Figure 4.4. Group management

Overview **Administrate workgroups** ✕

Add workgroup

This page allows to edit workgroup settings and to administrate which teachers/students belong to the group.

▼ Properties

Workgroup (*)

Description

▼ Members

Members

<input type="checkbox"/>	Becker, Christina (christina9)
<input type="checkbox"/>	Koch, Silke (silke10)
<input type="checkbox"/>	Meyer, Richard (richard1)
<input type="checkbox"/>	Müller, Victor (victor4)
<input type="checkbox"/>	Richter, Bertram (bertram11)

The **Moderate printers** module can also be used to check what the pupils print. The pending print jobs can be checked by the teacher and then either deleted or approved for printing. This can prevent unnecessary or incorrect printing.

The **Distribute materials** module simplifies the distribution and collection of teaching materials from classes and working groups. Optionally, it is also possible to set a period for the distribution and collection. This makes it possible to allocate tasks that need to be done by the end of the lesson. Once this period elapses, the distributed materials are then automatically collected back in again and stored in the teacher's home directory.

Figure 4.5. Distribution of teaching material

Overview **Distribute materials** ✕

Project properties

This page allows to modify properties of an existing or new distribution project.

▼ General

Description (*)

Directory name (*)

▼ Distribution and collection of project files

Distribution of project files

Collection of project files

▼ Members

Assigned classes/workgroups

<input type="checkbox"/>	1A
--------------------------	----

▼ Files

Files

<input type="checkbox"/>	school-history.pdf
--------------------------	--------------------

The **Room management** module is used to assign computers to a computer room in a school. These computer rooms can be centrally managed by the teachers, for example as regards permitting Internet access.

A proxy server is used for the filtering of the Internet access and checks if access to a certain web page is allowed when someone attempts to open that site. If this is not the case, an information page is displayed.

For example, if pupils are supposed to research using Wikipedia during a lesson, a rule list can be defined blocking access to all other Internet sites. This rule list can then be activated by the teacher.

The **Define internet rules** function can be used to administrate the rules.

4.6. Management of pupil's desktops using iTALC

iTALC is a didactic software for accessing pupil desktops. iTALC is open source software and is installed on the pupil desktops (in addition to Microsoft Windows, it is also available for Linux).

It offers teachers the following functions among others:

- The teacher can view a pupil's desktop and make supporting adjustments himself if needs be.
- The demo mode displays the contents of the teacher's desktop on all pupil desktops. In the same way, the content of one pupil desktop can also be approved for the demo mode.
- Screens and input devices can be centrally blocked to gain the full attention of the pupils.
- Computers can be centrally turned on and shut down via wake-on-LAN.
- Text messages can be sent to pupils.

The iTALC settings can be configured in a web assistant for each computer room.

4.7. Groupware

The school board uses the groupware solution Kolab for arranging meetings and organising contacts and tasks among the teachers and school employees. The installation can be performed with a few clicks using the Univention App Center.

The administration of the groupware-relevant attributes integrates seamlessly in the Univention Management Console. The employees access the groupware via the web client Roundcube.

Mobile devices (smartphones) are integrated via the Microsoft ActiveSync protocol.

4.8. References

- <http://docs.univention.de/manual.html> (UCS manual)
- <http://docs.univention.de/ucsschool-manual.html> (UCS@School manuals for administrators (currently only available in German))
- <http://docs.univention.de/ucsschool-teacher-manual.html> (UCS@School manuals for teachers (currently only available in German))
- <http://www.univention.de/en/products/ucs/app-catalogue/app/details/kolab> (Kolab)