

## Scenarios for Univention Corporate Server




## Table of Contents

1. Lawyer's office .....	3
1.1. Initial situation .....	3
1.2. Systems and services .....	3
1.3. Management of user accounts .....	4
1.4. Managing the Windows computers .....	5
1.5. Storage management .....	5
1.6. Single sign-on with a specialist legal application .....	5
1.7. Printer services .....	6
1.8. Groupware .....	6
1.9. Web proxy and web cache .....	6
1.10. Backup .....	6
1.11. Outlook .....	6
1.12. References .....	6
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. Print services .....	12
2.6. Integration of Oracle Solaris systems .....	13
2.7. Data management .....	13
2.8. Groupware .....	13
2.9. Outlook .....	13
2.10. References .....	13
3. Heterogeneous enterprise environment in an insurance company .....	15
3.1. Initial situation .....	15
3.2. Implementation .....	15
3.3. Virtualization .....	17
3.4. Software distribution of UCS systems .....	18
3.5. Connecting Windows clients and Windows software deployment .....	19
3.6. Active Directory synchronization .....	19
3.7. Groupware .....	19
3.8. Compliance requirements .....	19
3.9. System monitoring with Nagios .....	20
3.10. Integration of the AIX system .....	20
3.11. Citrix terminal services .....	20
3.12. Backup .....	20
3.13. Integration of SuiteCRM .....	20
3.14. References .....	20

# Chapter 1. Lawyer's office

1.1. Initial situation .....	3
1.2. Systems and services .....	3
1.3. Management of user accounts .....	4
1.4. Managing the Windows computers .....	5
1.5. Storage management .....	5
1.6. Single sign-on with a specialist legal application .....	5
1.7. Printer services .....	6
1.8. Groupware .....	6
1.9. Web proxy and web cache .....	6
1.10. Backup .....	6
1.11. Outlook .....	6
1.12. References .....	6


## 1.1. Initial situation

Feedback 

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 10 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.

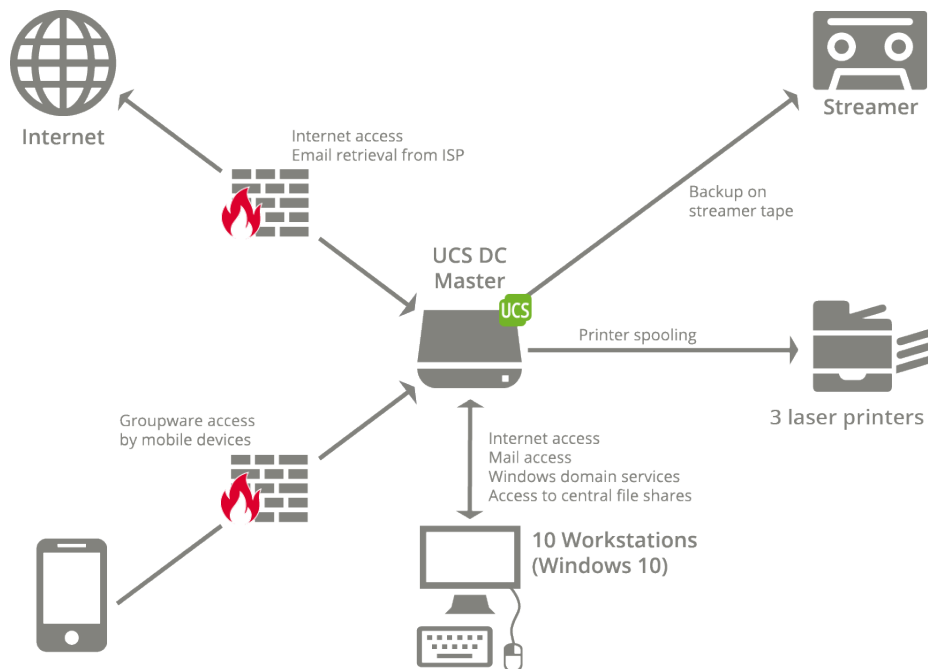
The company has a total of three laser printers (two identical black/white models and one color laser printer), which are all installed in a central office. Large documents with high volumes are printed often.

## 1.2. Systems and services

Feedback 

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

Feedback

User accounts for the ten employees are created in the Univention Management Console web interface. Each employee can set the password with the Self Service App from the App Center. Like all user data the password is save to a LDAP directory server and requested when logging on to the Windows client.

**Figure 1.2. Creating a user in Univention Directory Manager**

## 1.4. Managing the Windows computers

Feedback

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

Feedback

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. Single sign-on with a specialist legal application

Feedback

The chambers access a web-based legal service. This service has its own user administration system. To avoid having to take care of the user identities and password twice, the UCS SAML Identity Provider is used. SAML

(Security Assertion Markup Language) is an XML-based standard for exchanging authentication information, which allows single sign-on across domain boundaries among other things. The legal service is registered with a cryptographic certificate and then trusted by the UCS Identity Provider. The user then only needs to authenticate himself in UCS and can use the legal service without renewed authentication. The SAML Identity Provider can be installed via the Univention App Center.


## 1.7. Printer services

Feedback 

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.


## 1.8. Groupware

Feedback 

On the UCS system the groupware solution *Kopano* is installed as app from the App Center. Kopano accesses the user data of the UCS directory service. The administration integrates seamlessly in the Univention Management Console. The employees use the web-based *Kopano WebApp* for calendaring, also available in the App Center.


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

## 1.9. Web proxy and web cache

Feedback 

A web proxy server and web cache based on Squid is available with the app *proxy server* in UCS. Response times for regular calling the same web pages is reduced. Likewise, the data transfer volume via Internet access can be reduced. Furthermore, the access to Internet content can be controlled and managed. For example, it can be defined, which users or user groups access which websites.

## 1.10. Backup

Feedback 

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. The App Center in UCS offers several solutions like for example Bareos Backup Server and SEP sesam Backup Server that can be used flexibly for different backup and archiving strategies.

## 1.11. Outlook

Feedback 

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.

## 1.12. References

Feedback 

- <https://docs.software-univention.de/manual.html> (UCS manual)

- <https://www.univention.com/appid/kopano-core> (Kopano Core)
- <https://www.univention.com/appid/kopano-webapp> (Kopano WebApp)
- <https://www.univention.com/appid/squid/> (Proxyserver / Webcache (Squid))
- <https://www.univention.com/appid/sep-sesam> (SEP sesam Backup Server)
- <https://www.univention.com/appid/bareos> (Bareos Backup Server)
- <https://docs.software-univention.de/manual.html#windows:adtakeover>

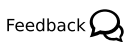




# Chapter 2. Medium-sized mechanical engineering company

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

## 2.1. Initial situation



Ganupa 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.

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.

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

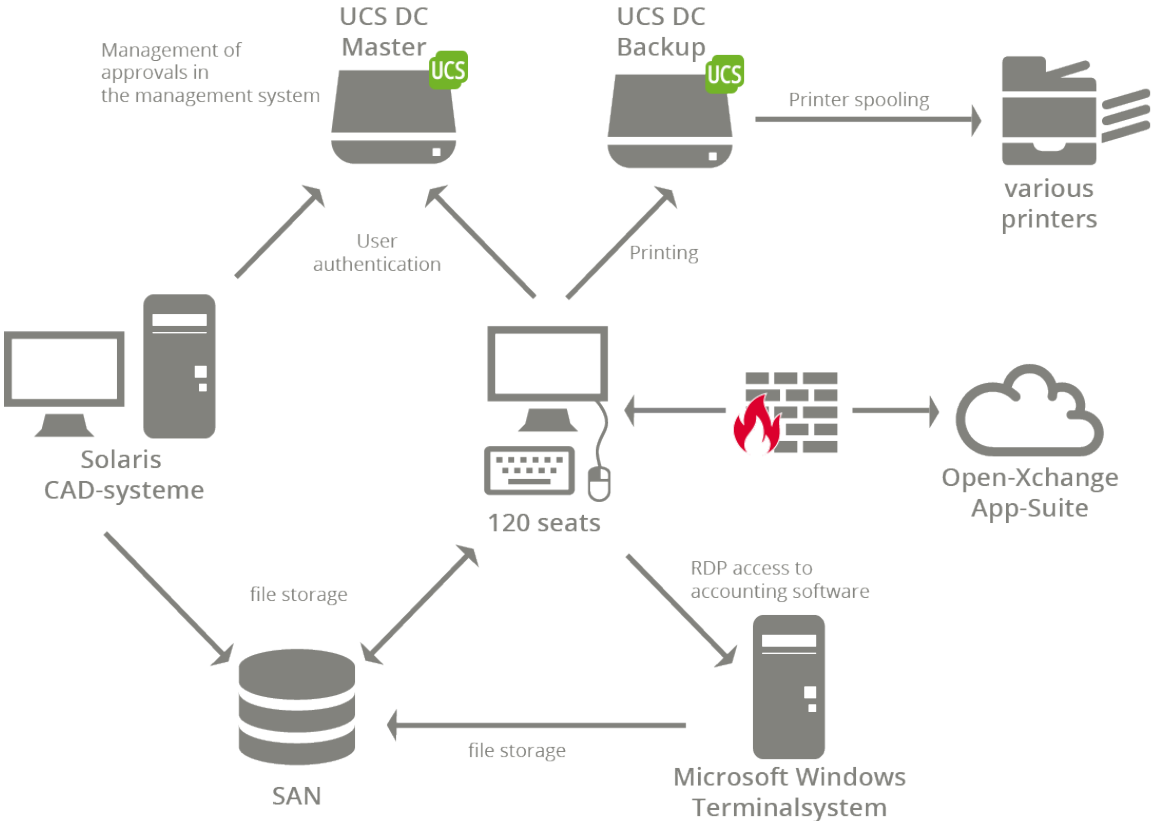
A groupware solution is required for the coordination of the globally distributed work procedures.

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

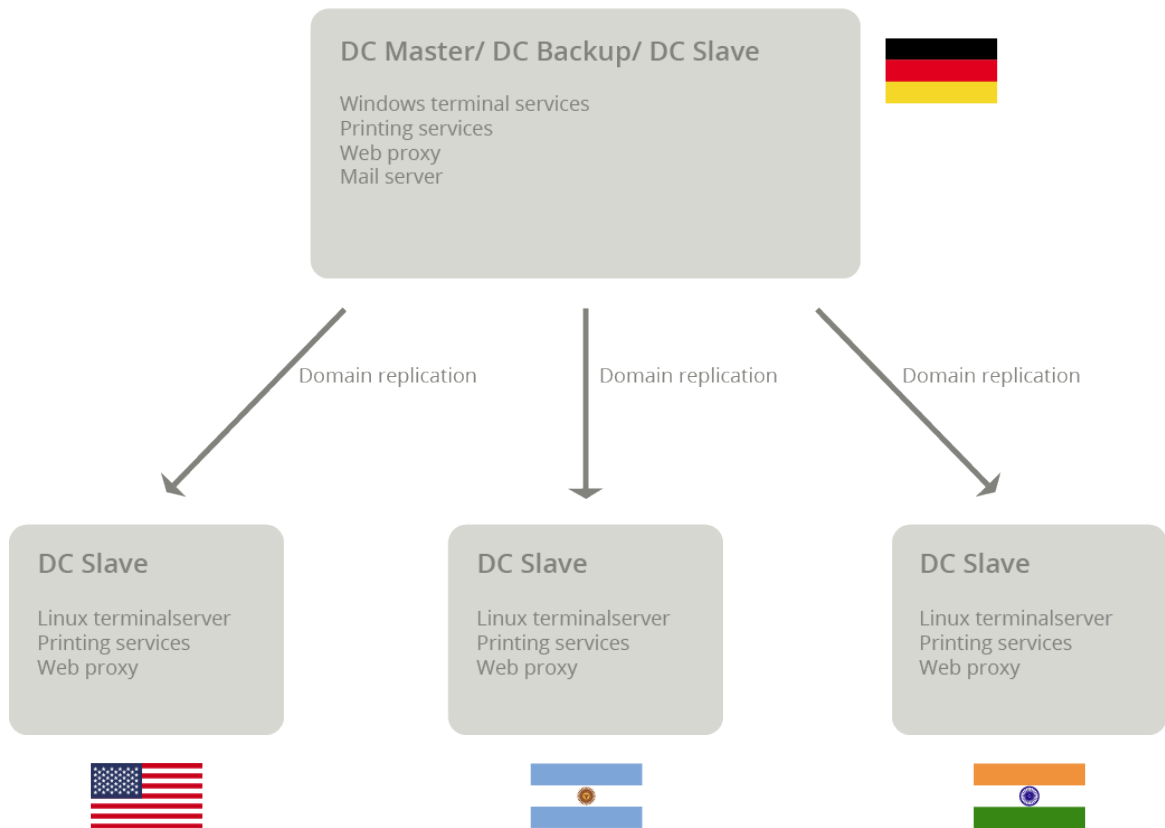
## 2.2. Implementation

Feedback 

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



**Figure 2.2. Global organization scheme of Ganupa Technologies**



## 2.3. Domain controller / LDAP directory

Feedback

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 desktop systems consisting of desktop computers and notebooks. Microsoft Windows and Ubuntu Linux are used on those systems.

The DC master is the centerpiece of the UCS domain. The central, writable 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.

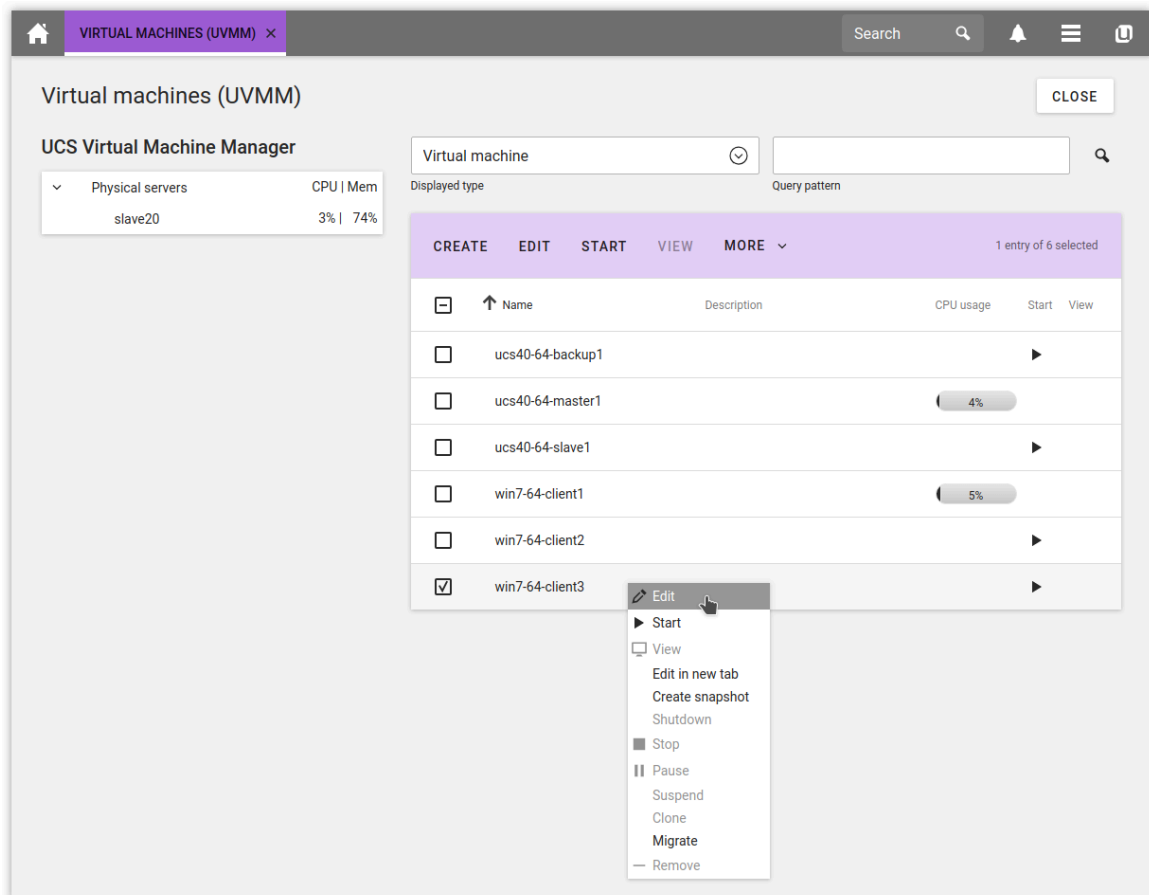
## 2.4. Virtualization

Feedback

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 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.

## 2.5. Print services


Feedback 

Print jobs are forwarded to the requested printer via a print server. The print servers are realized 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 limit the number of pages which can be printed. With the app *Print Server Quota* print quotas can be extended to a usergroup basis.


## 2.6. Integration of Oracle Solaris systems

Feedback 

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.

## 2.7. Data management

Feedback 

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.

## 2.8. Groupware

Feedback 

Ganupa Technologies uses the groupware solution *Open-Xchange App Suite* for arranging meetings and organizing 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 OX App Suite 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.


## 2.9. Outlook

Feedback 

At a later point in time, the plan is to monitor the Internet access centrally via a web proxy. For this purpose, UCS provides the app *Proxy server/ web cache (Squid)*.

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

## 2.10. References

Feedback 


- <https://docs.software-univention.de/manual.html> (UCS manual)
- <https://www.univention.com/appid/oxseforucs/> (OX App Suite)
- <https://www.univention.com/appid/squid/> (Proxy server/ web cache (Squid))



# Chapter 3. Heterogeneous enterprise environment in an insurance company

3.1. Initial situation .....	15
3.2. Implementation .....	15
3.3. Virtualization .....	17
3.4. Software distribution of UCS systems .....	18
3.5. Connecting Windows clients and Windows software deployment .....	19
3.6. Active Directory synchronization .....	19
3.7. Groupware .....	19
3.8. Compliance requirements .....	19
3.9. System monitoring with Nagios .....	20
3.10. Integration of the AIX system .....	20
3.11. Citrix terminal services .....	20
3.12. Backup .....	20
3.13. Integration of SuiteCRM .....	20
3.14. References .....	20

## 3.1. Initial situation

Feedback 

*Hanseatische Marineversicherung* (HMV) is an insurance company with 1800 employees specialized 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 10 is used on all the desktops. Software distribution and the installation of security updates are centralized.

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

Feedback 

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.

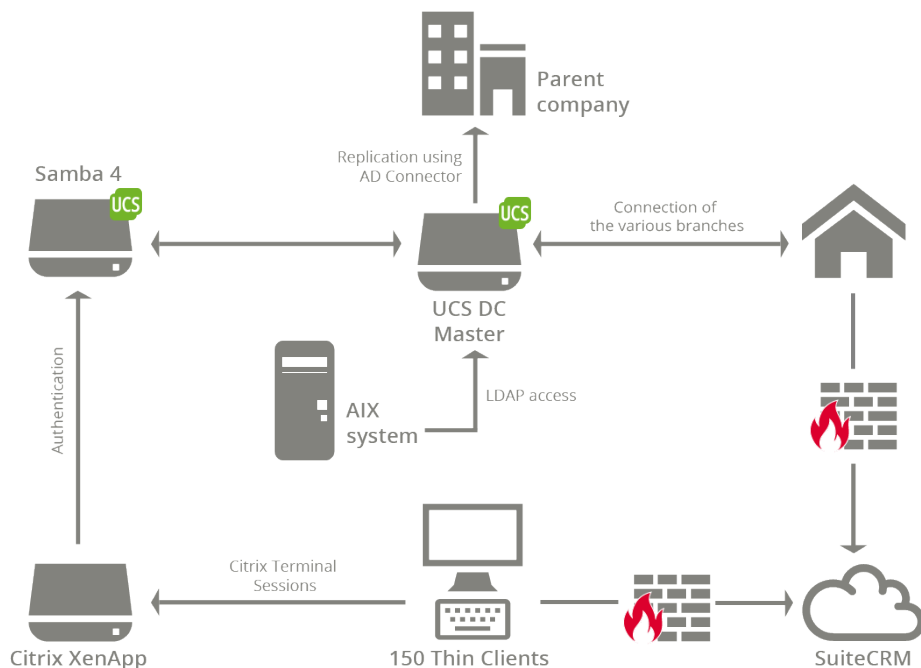
Implementation

The DC master is the centerpiece of the UCS domain. The central, writable 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.

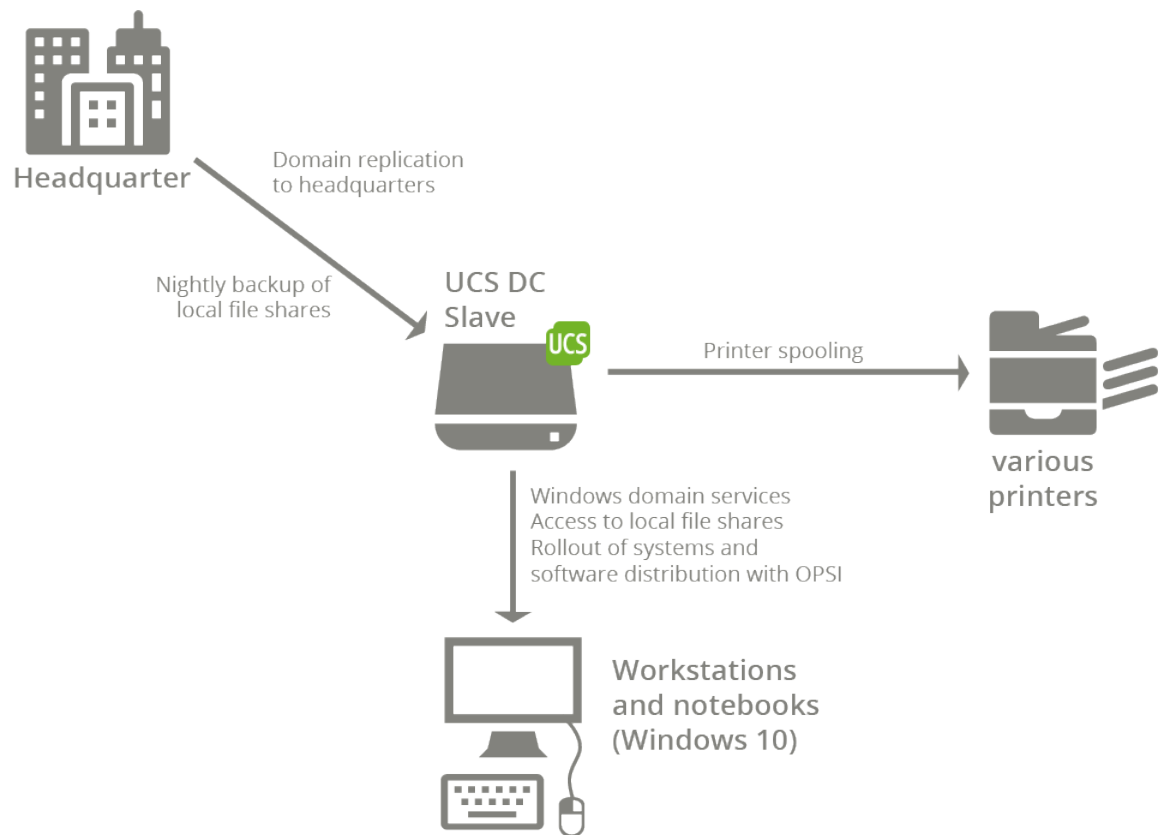
**Figure 3.1. General overview (excluded: storage, DNS, DHCP, print services, virtualization, backup)**




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.



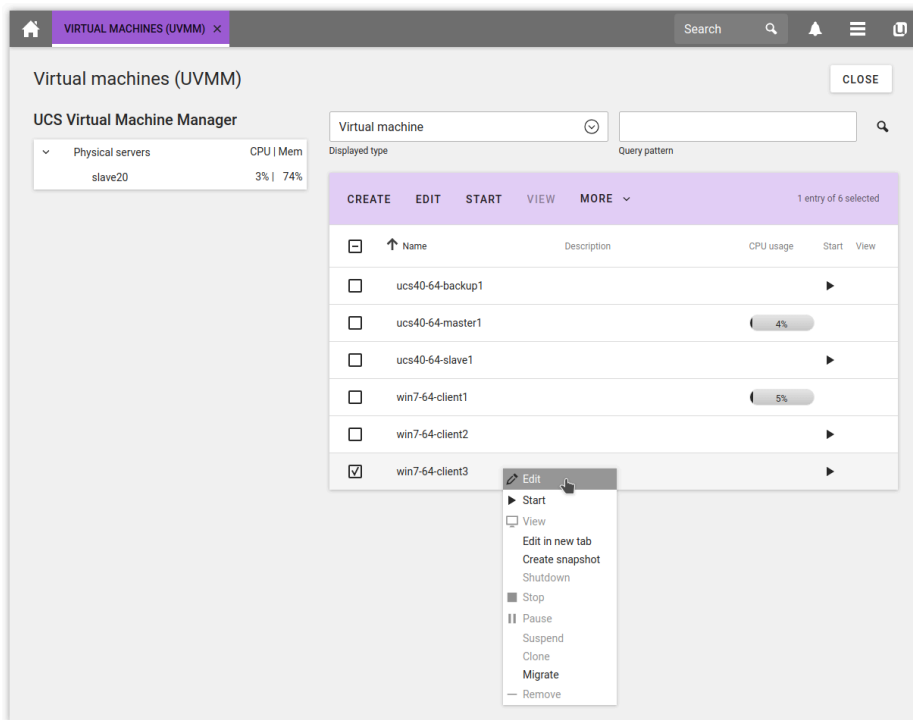
**Figure 3.2. Structure of a location**



### 3.3. Virtualization

Feedback 


All server systems in the HVM 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 KVM 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.

## 3.4. Software distribution of UCS systems

 Feedback 

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 Feedback

Samba 4 is used in the HMV 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.

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

## 3.6. Active Directory synchronization Feedback

The Univention Active Directory connector (AD connector for short) makes it possible to synchronize directory service objects between a Microsoft Windows 2008/2012/2016 server with Microsoft Active Directory (AD) and an Open Source LDAP directory service in Univention Corporate Server.

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

The UCS directory service synchronizes with the Microsoft Active Directory of the parent company. The replication encompasses all the containers, organizational units, users and groups.

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

## 3.7. Groupware Feedback

The groupware is provided in the form of Exchange Server 2016 by the parent company Vigil Insurances, allowing the users to access it using Outlook and Outlook on the web.

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 Feedback

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

Feedback 


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.

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

Feedback 

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 `secdapclntd` service runs on the AIX system; it performs all the authentication processes against the UCS LDAP directory.

## 3.11. Citrix terminal services

Feedback 

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

## 3.12. Backup

Feedback 

*SEP sesam backup server* from the App Center is used for file backup, which can be installed with a few clicks. 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.


## 3.13. Integration of SuiteCRM

Feedback 

*SuiteCRM* is employed as the CRM solution for sales personnel. The administration of the SuiteCRM 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

Feedback 

- <https://docs.software-univention.de/manual.html> (UCS manual)

- <https://docs.software-univention.de/manual.html#domain-ldap:directorylogger> (Audit-proof logging of LDAP changes with Univention Directory Logger)
- <https://docs.software-univention.de/manual.html#uvmm:chapter>
- <https://docs.software-univention.de/installation.html> (Extended installation documentation)
- <https://www.univention.com/appid/opsi/> (opsi)
- <https://www.univention.com/appid/sep-sesam/> (SEP sesam Backup Server)
- <https://www.univention.com/appid/digitec-suitecrm/> (SuiteCRM)

