univention
be open.

Scenarios for Univention Corporate Server

Release 5.0

Mar 14, 2024

CONTENTS

CHAPTER

ONE

LAWYER'S OFFICE

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 is employed as the client operating system. All the data is 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 through 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.

1.1 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.

1.2 Management of user accounts

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 saved to a LDAP directory server and requested when logging on to the Windows client.

1.3 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 through group policies. From the client point of view, the domain join procedure is identical to joining a Microsoft Windows-based domain.

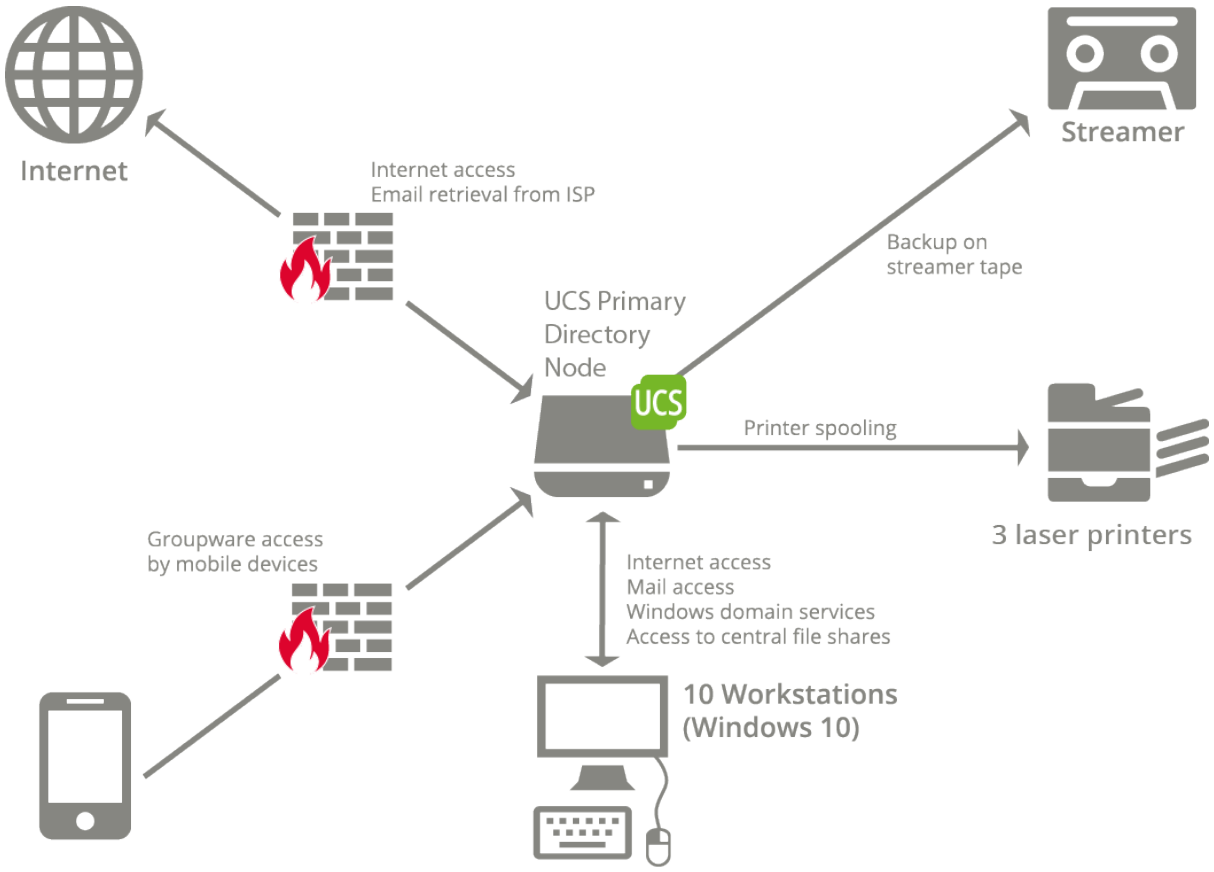

Fig. 1.1: System overview of the lawyer's office Hemmerlein and Sons

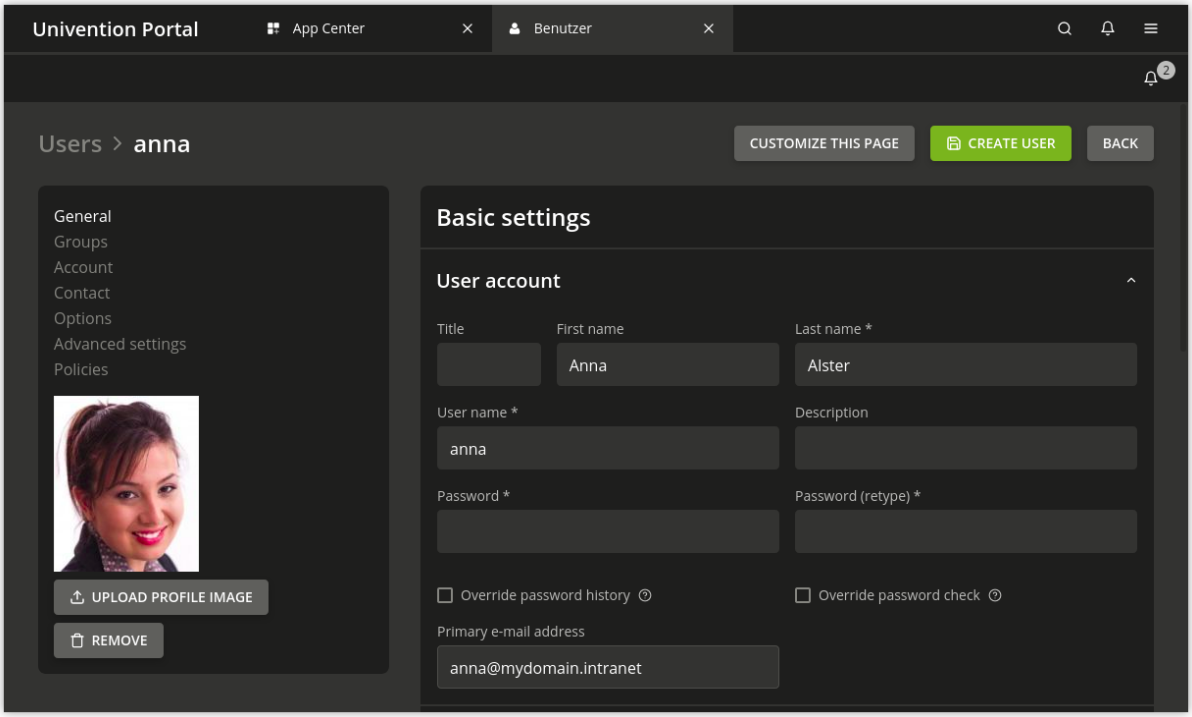

Fig. 1.2: Creating a user in Univention Directory Manager

1.4 Storage management

Samba provides every user with a home directory on the UCS system as a file share through the CIFS protocol. The users thus always receive the same data irrespective of the computer they are 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.

1.5 Single sign-on with a specialist legal application

The chambers connect to 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 users then only need to authenticate themselves in UCS and can use the legal service without renewed authentication. The SAML Identity Provider can be installed through the Univention App Center.

1.6 Printer services

The UCS system provides print services through 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 through 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

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.

1.8 Web proxy and web cache

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 through internet connections can be reduced. Furthermore, the view of internet content can be controlled and managed. For example, it can be defined, which users or user groups view which websites.

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. 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.

1.10 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 is 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

- UCS Manual[1]
- Migrating an Active Directory domain to UCS using Univention AD Takeover[2]
- Bareos Backup Server[3]
- Kopano Core[4]
- Kopano WebApp[5]
- Proxyserver / Webcache (Squid)[6]
- Self Service[7]
- SEP sesam Backup Server[8]

[1] https://docs.software-univention.de/manual/5.0/en/index.html#introduction
[2] https://docs.software-univention.de/manual/5.0/en/windows/ad-takeover.html#windows-ad-takeover
[3] https://www.univention.com/products/univention-app-center/app-catalog/bareos/
[4] https://www.univention.com/products/univention-app-center/app-catalog/kopano-core/
[5] https://www.univention.com/products/univention-app-center/app-catalog/kopano-webapp/
[6] https://www.univention.com/products/univention-app-center/app-catalog/squid/
[7] https://www.univention.com/products/univention-app-center/app-catalog/self-service/
[8] https://www.univention.com/products/univention-app-center/app-catalog/sep-sesam/

CHAPTER

TWO

MEDIUM-SIZED MECHANICAL ENGINEERING COMPANY

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 email 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 needs to 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 is centrally saved on an Storage Area Network device (SAN).

2.1 Implementation

2.2 Directory Nodes / LDAP directory

The company implements an infrastructure composed of a UCS Primary Directory Node, a UCS Backup Directory Node, several UCS Replica Directory Nodes and desktop systems consisting of desktop computers and notebooks. Microsoft Windows and Ubuntu Linux are used on those systems.

The Primary Directory Node is the centerpiece of the UCS domain. The central, writable copy of the LDAP directory service is maintained on this system.

The Backup Directory Node largely represents a copy of the Primary Directory Node. 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 Directory Nodes.

If the Primary Directory Node fails as a result of a hardware defect, the Backup Directory Node can be converted to the Primary Directory Node in a very short time.

The Primary Directory Node and Backup Directory Node 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 Backup Directory Node.

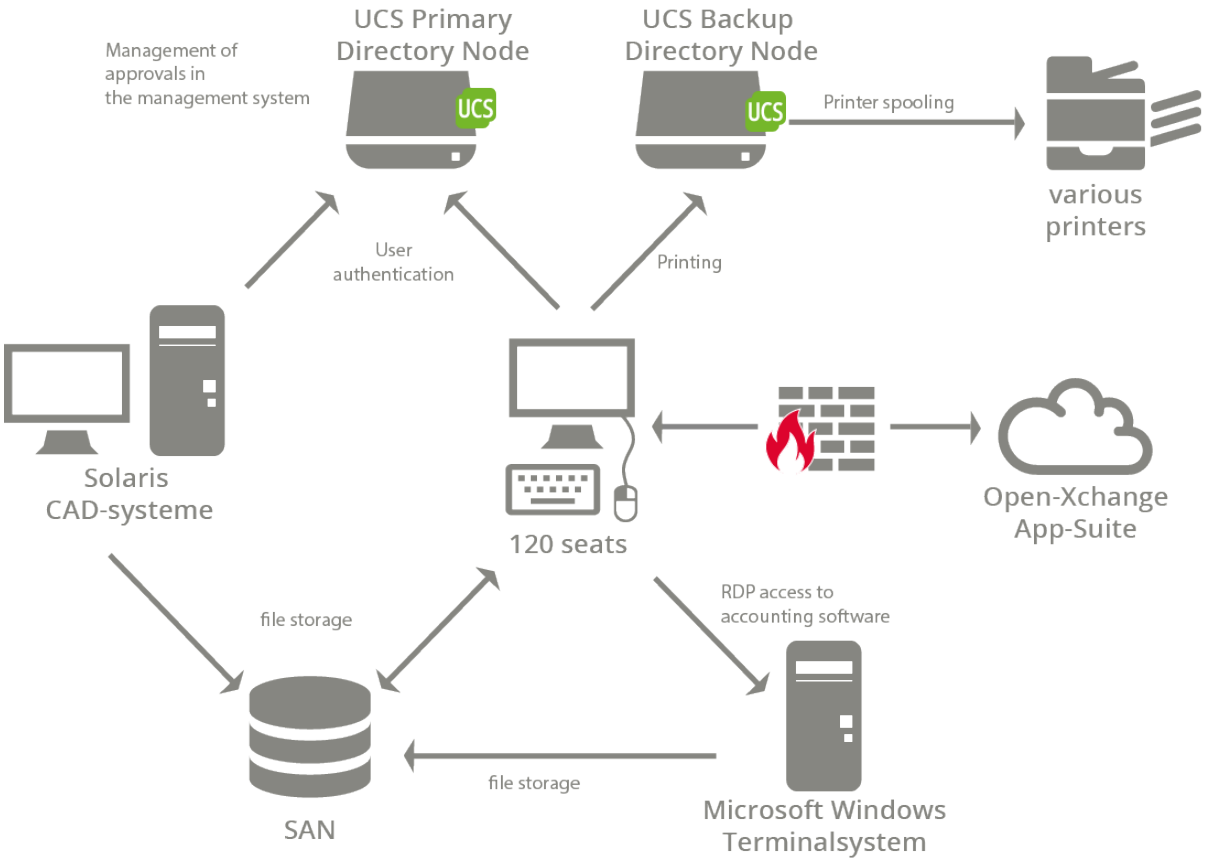

Fig. 2.1: System overview of Ganupa Technologies headquarters (virtualization is not considered)

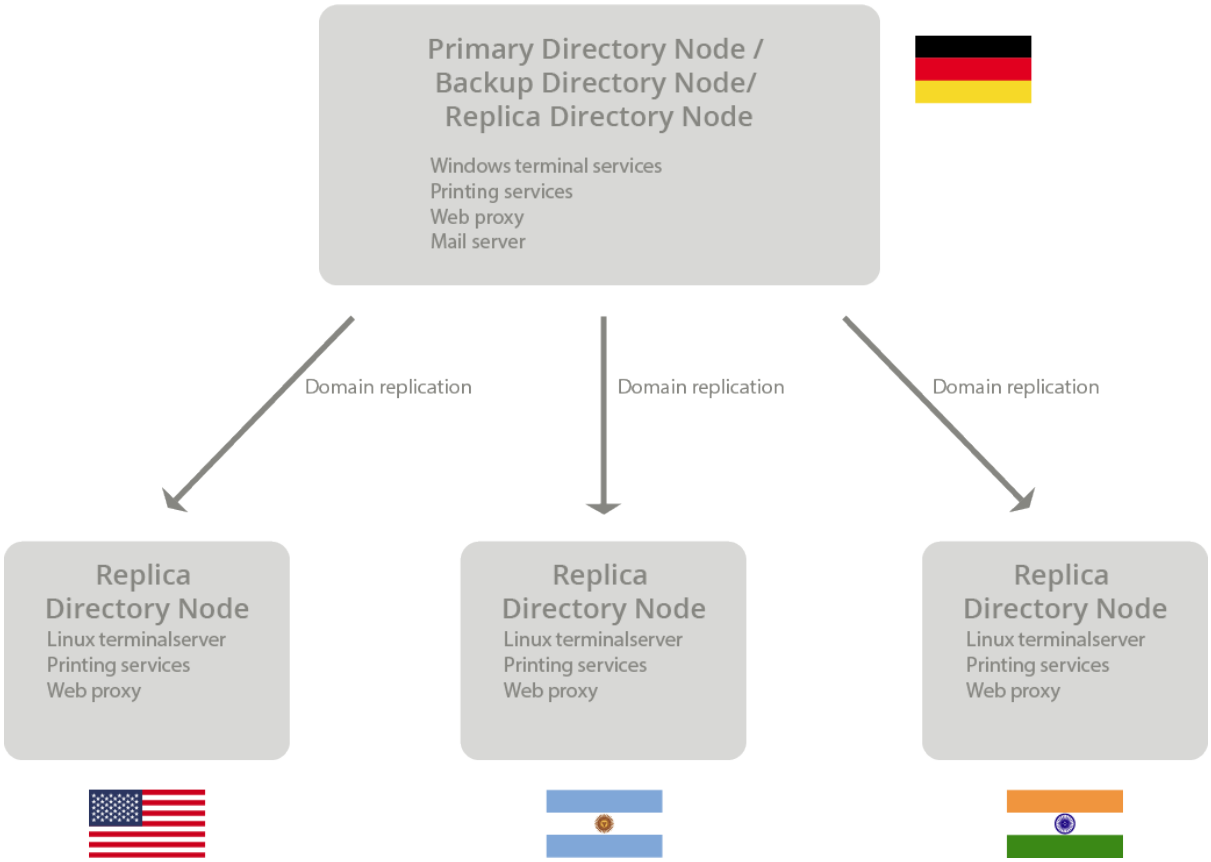

Fig. 2.2: Global organization scheme of Ganupa Technologies

2.3 Print services

Print jobs are forwarded to the requested printer through 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.

2.4 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. Users can sign 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 through DHCP. The files are saved on the UCS file servers through a NFS share.

2.5 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 connect to individual shares through the network file system (NFS), the Windows clients through the CIFS protocol.

2.6 Groupware

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 Replica Directory Node 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 connect to the groupware through the OX App Suite web client and Mozilla Thunderbird.

Mobile devices like smartphones and tablets are integrated through the Microsoft ActiveSync protocol.

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

2.7 Outlook

At a later point in time, the plan is to monitor the internet traffic centrally through 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.

2.8 References

- UCS Manual[9]
- OX App Suite[10]
- Proxy server/ web cache (Squid)[11]

[9] https://docs.software-univention.de/manual/5.0/en/index.html#introduction
[10] https://www.univention.com/products/univention-app-center/app-catalog/oxseforucs/
[11] https://www.univention.com/products/univention-app-center/app-catalog/squid/

CHAPTER

THREE

HETEROGENEOUS ENTERPRISE ENVIRONMENT IN AN INSURANCE COMPANY

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 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 connect to the terminal services with thin clients.

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

All users, computers and services need to be centrally administrable. Critical system status is reported promptly per email and SMS.

All server systems in the headquarters need to 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.

A special application for insurance business runs on a Power7 system with IBM AIX. The users on this system don't need to be maintained twice.

3.1 Implementation

The company implements an infrastructure composed of a UCS Primary Directory Node, a UCS Backup Directory Node, several UCS Replica Directory Nodes and 150 thin clients.

The Primary Directory Node is the centerpiece of the UCS domain. The central, writable LDAP directory is provided on this system.

The Backup Directory Node also largely represents a copy of the Primary Directory Node. 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 Directory Nodes.

If the Primary Directory Node fails as a result of a hardware defect, the Backup Directory Node can be converted to the Primary Directory Node in a very short time.

The Primary Directory Node and Backup Directory Node are both installed at the company headquarters. The locations also contain additional Replica Directory Node systems, which provide Windows domain services, print services and software distribution.

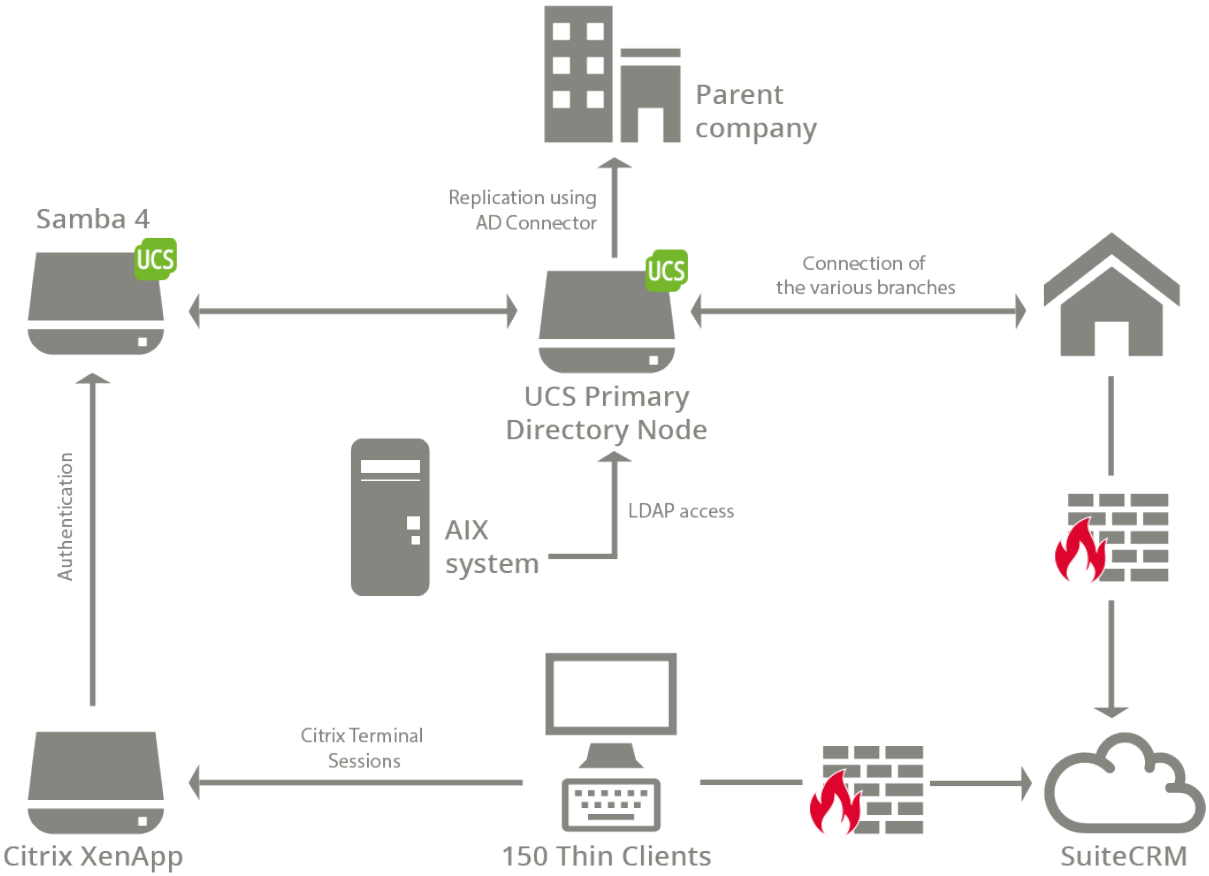

Fig. 3.1: General overview (excluded: storage, DNS, DHCP, print services, virtualization, backup)

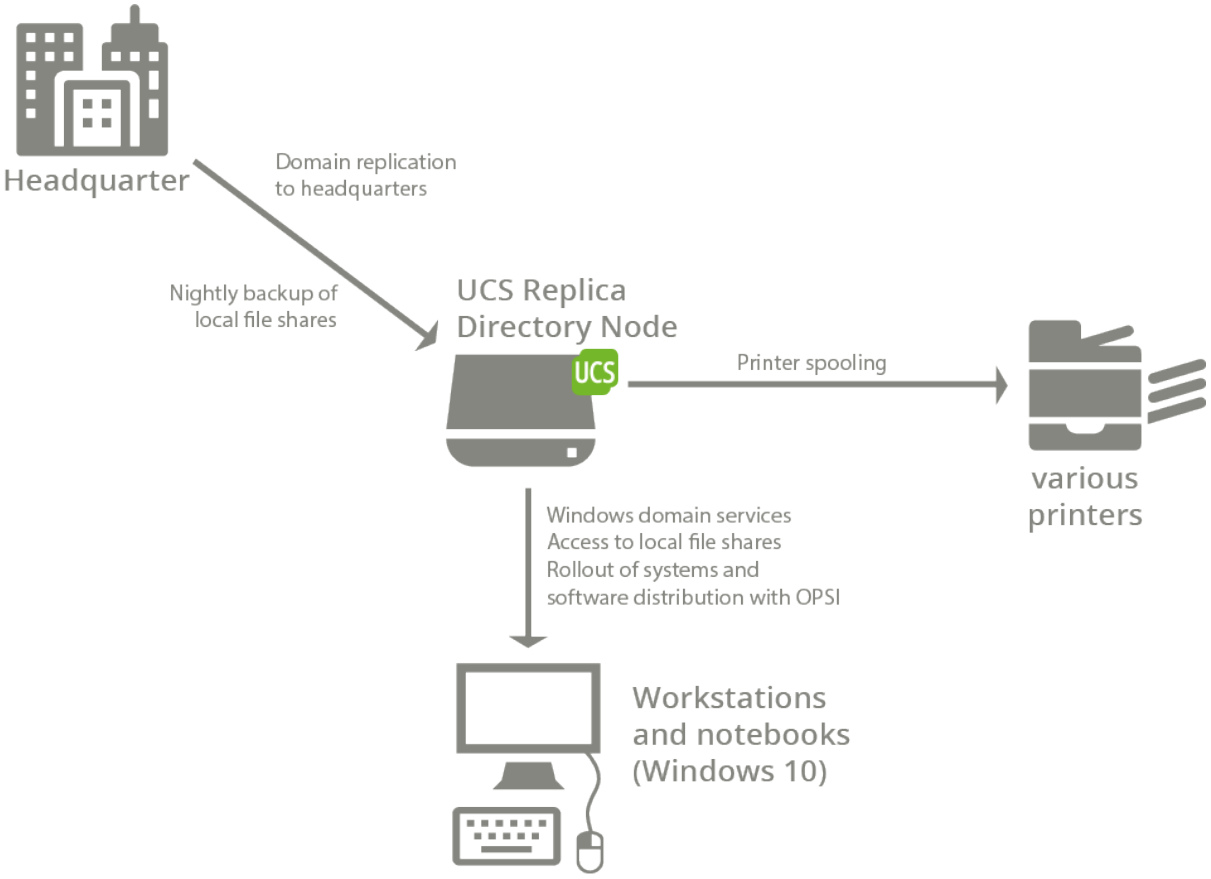

Fig. 3.2: Structure of a location

3.2 Software distribution of UCS systems

Installation profiles have been created for the UCS Directory Nodes. These profiles can be used to roll out additional 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 software packages available for installation 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 or 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.

3.3 Connecting Windows clients and Windows software deployment

Samba/AD is used in the HMV for the integration of Microsoft Windows clients. Samba/AD 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 through 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 to rollout additional Windows systems. These are automatically installed through PXE.

3.4 Active Directory synchronization

The **Univention Active Directory Connector** makes it possible to synchronize directory service objects between a Microsoft Windows 2012/2016/2019 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/AD domain.

3.5 Groupware

The groupware is provided in the form of Exchange Server 2016 by the parent company Vigil Insurances, allowing the users to connect to 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 username / password.

Users can connect to the services of both environments in a transparent way, as the same user settings apply in both domains. For example, a user can sign in both the UCS directory service on their laptop and the Citrix Server in the Microsoft Active Directory with the same username and password.

3.6 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 protocolized 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, for example `secret`.

3.7 System monitoring with Nagios NRPE

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

3.8 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 twice in the local user database of the AIX system. Now only the `secldapclntd` service runs on the AIX system; it performs all the authentication processes against the UCS LDAP directory.

3.9 Citrix terminal services

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/AD domain.

3.10 Integration of SuiteCRM

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 Replica Directory Node system on the Amazon EC2 cloud. This ensures high availability and allows flexible scaling to growing performance and storage requirements.

3.11 References

- UCS Manual[12]
- Audit-proof logging of LDAP changes[13]
- Extended installation documentation[14]
- opsi[15]
- SEP sesam Backup Server[16]
- SuiteCRM[17]

[12] https://docs.software-univention.de/manual/5.0/en/index.html#introduction
[13] https://docs.software-univention.de/manual/5.0/en/domain-ldap/ldap-directory.html#domain-ldap-directory-logger
[14] https://docs.software-univention.de/installation-5.0.html
[15] https://www.univention.com/products/univention-app-center/app-catalog/opsi/
[16] https://www.univention.com/products/univention-app-center/app-catalog/sep-sesam/
[17] https://www.univention.com/products/univention-app-center/app-catalog/digitec-suitecrm/