univention
be open.

Einsatzszenarien für Univention Corporate Server

univention
be open.

Inhaltsverzeichnis

Kapitel 1. Anwaltskanzlei

1.1. Ausgangslage

Feedback

Die Anwaltskanzlei Hemmerlein & Söhne verfügt über insgesamt zehn Mitarbeiter. Die Mitarbeiter arbeiten im Wesentlichen mit Office-Applikationen und einer juristischen Vorgangsbearbeitung, die nur für Microsoft Windows verfügbar ist. Als Client-Betriebssystem wird Microsoft Windows 10 eingesetzt. Alle Daten sollen zentral auf einem Server gespeichert und gesichert werden. Da nur geringes technisches Know-How verfügbar und eigenes technisches Personal nicht finanzierbar ist, wird Wert auf eine einfache Administration gelegt. Die nachfolgend beschriebenen administrativen Tätigkeiten können nach erfolgter Erstinstallation komplett durch einfach zu bedienende webbasierte Schnittstellen konfiguriert werden.

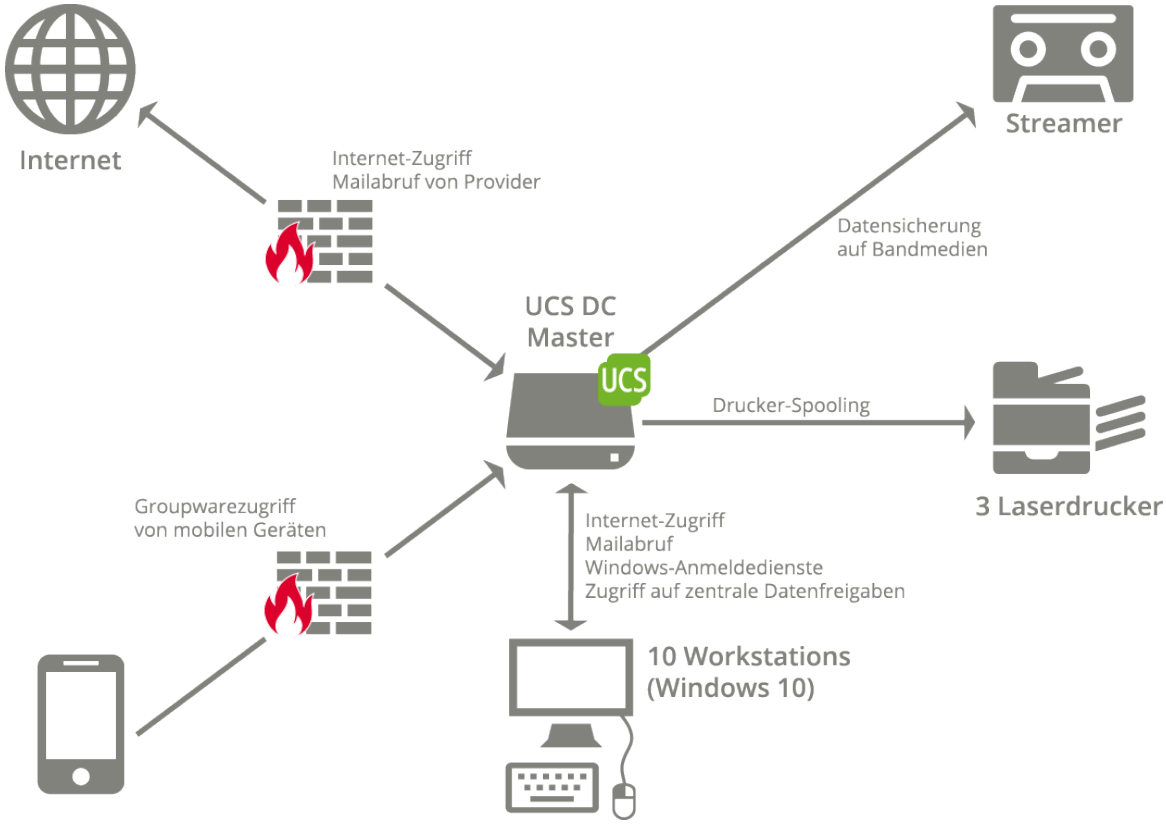
In der Firma existieren insgesamt drei Laserdrucker (zwei baugleiche Schwarz/Weiss-Modelle und ein Farblaserdrucker), die alle in einem zentralen Büro aufgebaut sind. Es werden häufig sehr große Schriftsätze mit hohem Volumen gedruckt.

1.2. Systeme und Dienste

Feedback

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

Abbildung 1.1. Systemübersicht der Kanzlei Hemmerlein und Söhne

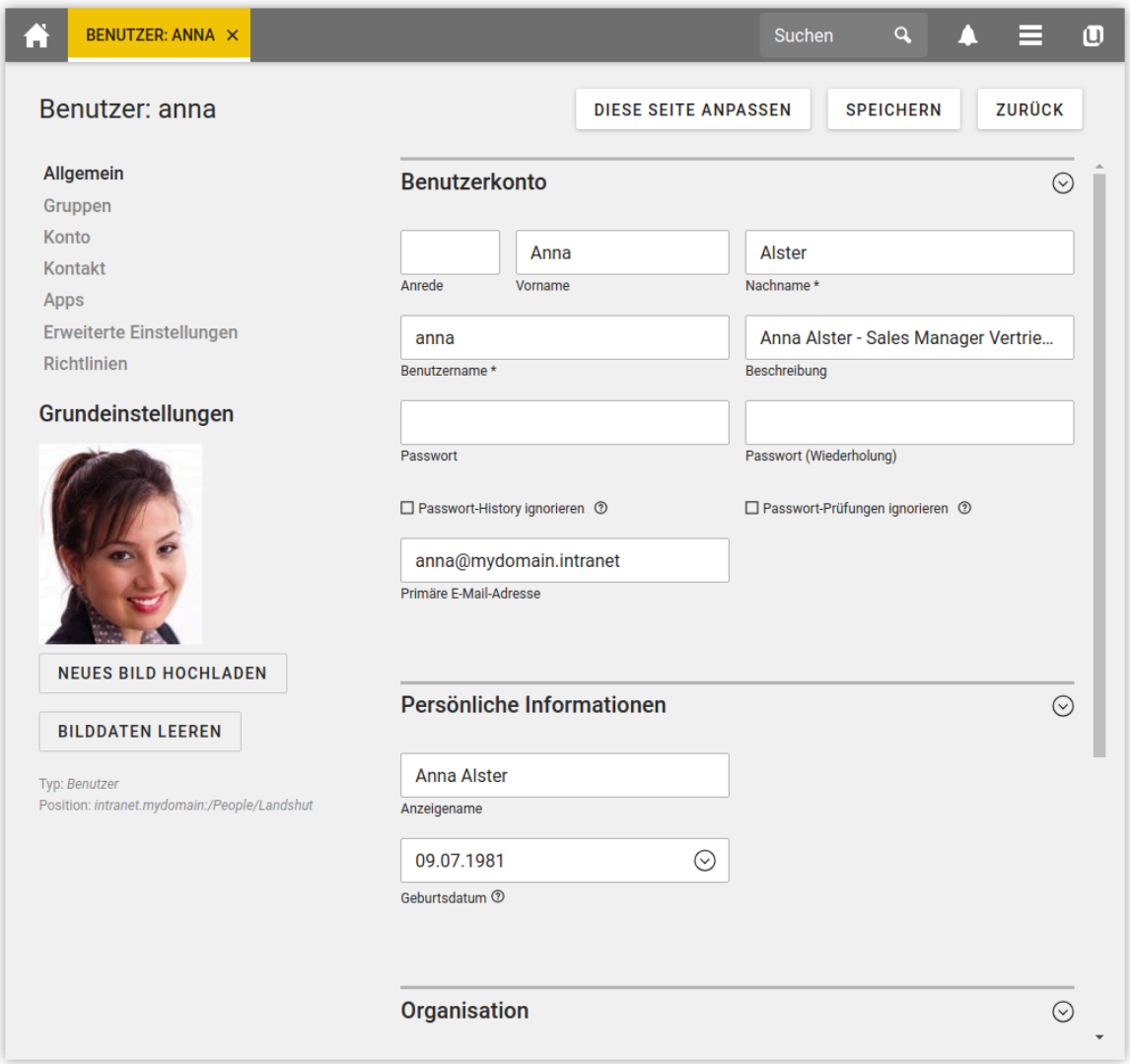


1.3. Verwaltung der Benutzerdaten

Feedback

Für die zehn Mitarbeiter werden im Web-Interface der Univention Management Console Benutzerkonten angelegt. Jeder Mitarbeiter kann sich über die Benutzer *Self-Service* App aus dem App Center sein Passwort selbst setzen, das — wie alle Benutzerdaten — in einem LDAP-Verzeichnisdienst gespeichert und bei der Anmeldung am Windows-Client abgefragt wird.

Abbildung 1.2. Anlegen eines Benutzers in der Univention Management Console



1.4. Verwaltung der Microsoft Windows-Rechner

Feedback

Auf dem UCS-System wird Samba 4 für die Anbindung der Windows-Clients eingesetzt. Samba 4 bietet Domänen-, Verzeichnis- und Authentifizierungsdienste, die kompatibel zu Microsoft Active Directory sind. Diese ermöglichen auch die Verwendung der von Microsoft bereitgestellten Werkzeuge für die Verwaltung von Gruppenrichtlinien (GPOs).

Windows-Clients können direkt der durch UCS bereitgestellten Active-Directory-kompatiblen Domäne beitreten und über Gruppenrichtlinien zentral konfiguriert werden. Der Domänen-Join ist aus Client-Sicht identisch mit dem Beitritt zu einer Windows-basierten Domäne.

1.5. Datenverwaltung

Feedback

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

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

Freigaben können wie Benutzer ebenfalls webbasiert in der Univention Management Console angelegt werden.

1.6. Single-Sign-On mit einer juristischen Fachanwendung

Feedback

Die Kanzlei greift auf einen webbasierten juristischen Fachdienst zu. Dieser benutzt eine eigenständige Benutzerverwaltung. Um zu vermeiden, dass Benutzerkennungen und Passwörter doppelt gepflegt werden müssen, wird der UCS SAML Identity Provider eingebunden. SAML (Security Assertion Markup Language) ist ein XML-basierter Standard zum Austausch von Authentifizierungsinformationen, der u.a. Single-Sign-On über Domänengrenzen hinweg erlaubt. Der juristische Fachdienst wird über ein kryptografisches Zertifikat fest registriert und vertraut dann dem UCS Identity Provider. Der Benutzer authentifiziert sich dann nur noch in UCS und kann den eingebundenen juristischen Dienst ohne erneute Authentifizierung nutzen. Der SAML Identity Provider kann über das Univention App Center installiert werden.

1.7. Druckdienste

Feedback

Das UCS-System stellt über die Software CUPS Druckdienste bereit. Es können sowohl netzwerkfähige Drucker, als auch lokal an einen Rechner angeschlossene Drucker zentral administriert werden. Die drei Drucker können bequem über die Univention Management Console konfiguriert werden und stehen den Benutzern auf ihren Windows-Clients direkt zur Verfügung. Die beiden baugleichen Laserdrucker werden dabei zu einer Druckergruppe zusammengefasst: Das bedeutet, dass die Benutzer neben der gezielten Auswahl eines Druckers auch die Möglichkeit erhalten, auf einem Pseudodrucker zu drucken. Die Druckaufträge werden dabei reihum um die beiden Drucker der Druckergruppe verteilt. Bei belegten Druckern wird auf einen freien Drucker ausgewichen, sodass Wartezeiten vermieden werden.

1.8. Groupware

Feedback

Auf dem UCS-System wird über das App Center *Kopano* installiert, eine Groupware mit Integration in UCS. Kopano greift dabei auf die Benutzerkontoinformationen des UCS-Verzeichnisdienstes zu. Die Verwaltung integriert sich nahtlos in die Univention Management Console. Die Mitarbeiter verwenden die webbasierte *Kopano WebApp* für ihren Kalender, die auch als App im App Center verfügbar ist.

Virenerkennung inkl. Signaturen-Updates und Spamfilterung sind ohne weitere Folgekosten integriert.

1.9. Web Proxy und Webcache

Feedback

Ein Web Proxyserver und Web-Cache auf Basis von Squid steht mit der App *Proxyserver* in UCS zur Verfügung. Antwortzeiten für den regelmäßigen Aufruf gleicher Webseiten werden verringert. Ebenso kann das Daten-Transfervolumen über den Internetzugang reduziert werden. Darüber hinaus wird die Kontrolle und Administration des Zugriffs auf Internetinhalte ermöglicht. So kann beispielsweise festgelegt werden, welche Benutzer oder Benutzergruppen auf welche Webseiten zugreifen.

1.10. Backup

Feedback

Alle Daten (sowohl die Daten der Benutzer im Heimatverzeichnis als auch die Daten auf der zentralen Freigabe für Fachliteratur) liegen auf dem UCS-System und können deshalb zentral auf einen Streamer gesichert werden. Im App Center von UCS gibt es dazu verschiedene Backup-Lösungen wie zum Beispiel Bareos Backup

Server und SEP sesam Backup Server, die flexibel auf verschiedene Sicherungs- und Archivierungsstrategien angewendet werden können.

1.11. Ausblick

Feedback

Für den geplanten Zusammenschluss mit einem weiteren Büro in München kann einfach ein weiteres UCS-System in dieser Filliale installiert werden. Alle LDAP-Daten werden dann automatisch und verschlüsselt an den Standortserver übertragen, sodass Mitarbeiter sich bei Vorort-Terminen am Münchner Standort mit ihren gewohnten Benutzerkennungen anmelden.

Das am Münchner Standort schon bestehende Active Directory kann mit Univention AD Takeover automatisiert in die UCS-Domäne migriert werden.

1.12. Referenzen

Feedback

- https://docs.software-univention.de/handbuch-4.4.html (UCS-Handbuch)
- https://www.univention.de/appid/kopano-core (Kopano Core)
- https://www.univention.de/appid/kopano-webapp (Kopano WebApp)
- https://www.univention.de/appid/bareos (Bareos Backup Server)
- https://www.univention.de/appid/squid/ (Proxyserver / Webcache (Squid))
- https://www.univention.de/appid/self-service/ (Self Service)
- https://www.univention.de/appid/sep-sesam (SEP sesam Backup Server)
- https://docs.software-univention.de/handbuch-4.4.html#windows:adtakeover

Kapitel 2. Mittelständische Maschinenbau-Firma

2.1. Ausgangslage

Ganupa Technologies ist einer der wichtigsten Hersteller für Walzstahlfräsen. Am Firmensitz in Deutschland arbeiten 260 Mitarbeiter in Produktion, Verwaltung, Konstruktion und Vertrieb. Außerdem gibt es in den USA, Argentinien und Indien lokale Standorte mit je 5 bis 10 Mitarbeitern.

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

Für die Mitarbeiter aus der Verwaltung und dem Vertrieb soll nur eine Office-Suite, ein E-Mail-Client und ein Browser angeboten werden.

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

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

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

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

Für die Koordination der weltweit verteilten Arbeitsabläufe wird eine Groupwarelösung benötigt.

Alle Nutzdaten werden zentral auf einem Storage Area Network (SAN) gespeichert.

2.2. Umsetzung

Feedback

Abbildung 2.1. Systemübersicht von Ganupa Technologies am zentralen Standort (die Virtualisierung wird in diesem Schaubild nicht berücksichtigt)

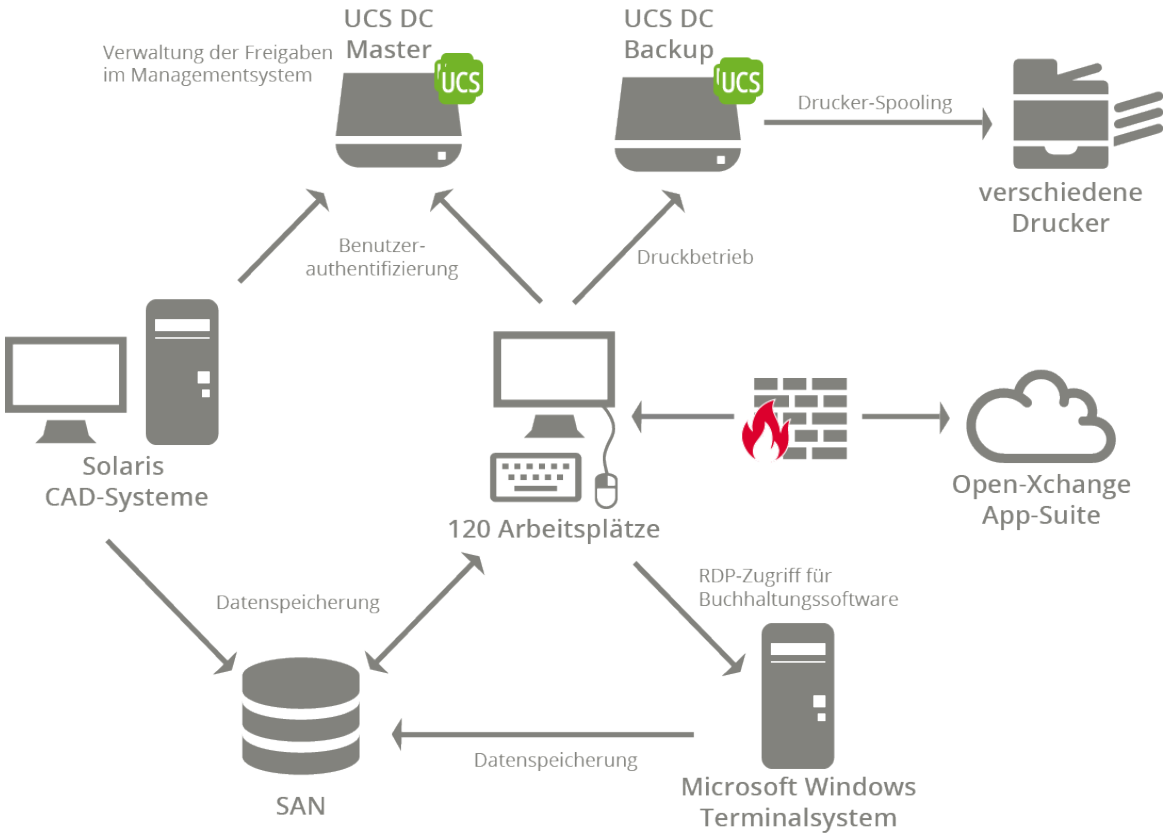
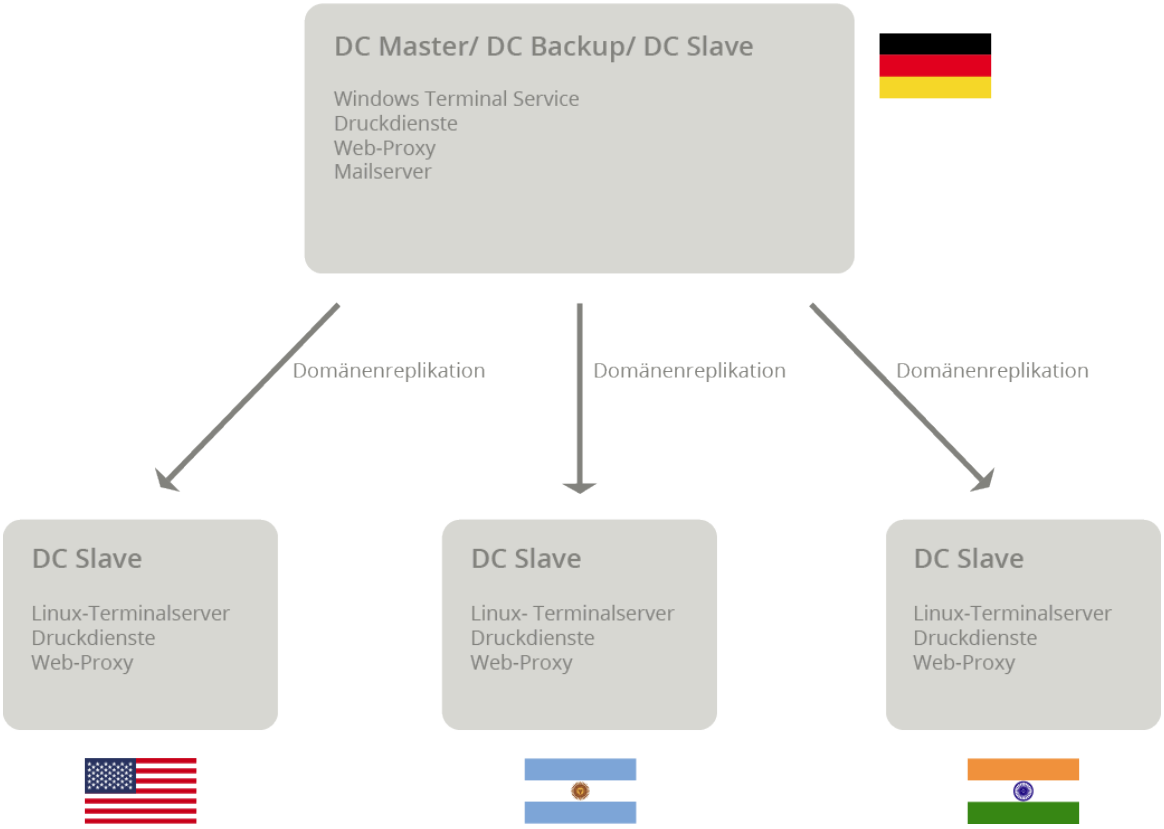


Abbildung 2.2. Globaler Systemaufbau von Ganupa Technologies



2.3. Domänencontroller / LDAP-Verzeichnis

Feedback

Das Unternehmen implementiert eine Infrastruktur bestehend aus einem UCS Domänencontroller Master (DC Master), einem UCS Domänencontroller Backup (DC Backup), mehreren UCS Domänencontroller Slave (DC Slave) und Arbeitsplatzsystemen für Mitarbeiter bestehend aus Desktop-Computern und Notebooks. Zum Einsatz kommen Microsoft Windows und Ubuntu Linux.

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

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

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

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

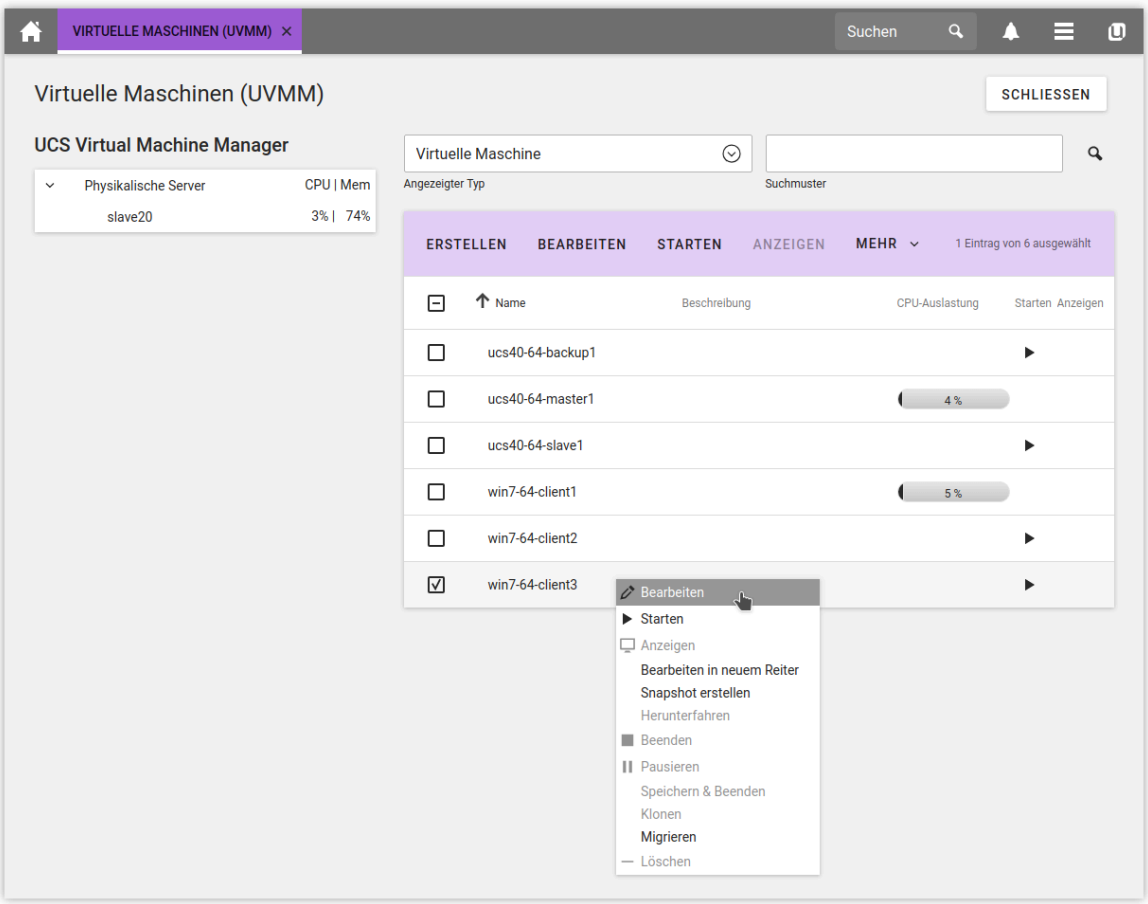
2.4. Virtualisierung

Feedback

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

Als Grundlage der Virtualisierung dienen Virtualisierungsserver auf Memberservern (UCS-Serversysteme ohne lokalen LDAP-Server). Auf diesen laufen jeweils ein bis mehrere virtuelle Maschinen mit der Virtualisierungslösung KVM. UCS- und Windows-Systeme werden paravirtualisiert betrieben, d. h. durch einen Zugriff der virtualisierten Systeme auf die Ressourcen der Wirtsysteme kann ein höherer Durchsatz erzielt werden. Paravirtualisierungstreiber für KVM werden von Univention als signierte MSI-Installationspakete bereitgestellt und können so einfach installiert werden.

Abbildung 2.3. Verwaltung virtueller Maschinen mit UVMM



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

Snapshots ermöglichen einen einfachen Rollback von Updates im Fehlerfall.

2.5. Druckdienste

Feedback

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

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

Außerdem ist jedem Drucker ein Seitenpreis zugeordnet. Dadurch können pro Benutzer die angefallenen Druckkosten ermittelt werden. Dies kann auch mit einer Limitierung von zu druckenden Seiten verbunden werden. Über die App *Print Server Quota* können Druckquotas auch auf Benutzergruppenbasis ausgedehnt werden.

2.6. Einbindung von Oracle-Solaris-Systemen

Feedback

Eine Fachanwendung für CAD-Konstruktionen ist nur für Oracle Solaris verfügbar. Die Namensdienste auf dem Solaris-System wurden auf eine Authentifizierung gegen das UCS-LDAP angepasst, d.h. Benutzer können sich auf dem Solaris-System mit ihrer Domänen-Benutzerkennung und -Passwort anmelden. Die zusätzliche Pflege lokaler Benutzerkonten auf dem Solaris-System entfällt so.

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

2.7. Datenhaltung

Feedback

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

2.8. Groupware

Feedback

Ganupa Technologies verwendet die Groupwarelösung *Open-Xchange App Suite* zur Abstimmung von Terminen, Kontakten und Aufgaben.

Der Groupware-Server wird als Domänencontroller Slave-System in der Amazon EC2-Cloud betrieben. Dies erlaubt eine flexible Skalierung des Groupwaresystems auf wachsende Leistungs- und Speicherplatzanforderungen. Die Installation erfolgt mit wenigen Klicks aus dem App Center.

Die Verwaltung der Groupware-relevanten Attribute integriert sich nahtlos in die Univention Management Console. Die Mitarbeiter greifen auf die Groupware über den Open-Xchange App Suite Web-Client und Mozilla Thunderbird zu.

Mobile Endgeräte (Smartphones und Tablets) werden über das ActiveSync-Protokoll von Microsoft integriert.

Virenerkennung inkl. Signaturen-Updates und Spamfilterung sind ohne weitere Folgekosten integriert.

2.9. Ausblick

Feedback

Zu einem späteren Zeitpunkt soll der Internet-Zugriff zentral über einen Web-Proxy kanalisiert und auf Viren und Malware geprüft werden.

UCS bietet hierfür eine Integration über die App *Proxyserver / Webcache (Squid)*.

Alternativ kann auch die Anschaffung einer spezialisierten Appliance erwogen werden, die die Benutzer dann gegen den UCS-LDAP-Server authentifzieren kann.

2.10. Referenzen

Feedback

- https://docs.software-univention.de/handbuch-4.4.html (UCS-Handbuch)
- https://www.univention.de/appid/oxseforucs/ (OX App Suite)

Referenzen

- https://www.univention.de/appid/squid/(Proxyserver / Webcache (Squid))

Kapitel 3. Heterogene Großumgebung im Konzernverbund

3.1. Ausgangslage

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

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

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

Auf den Desktops kommt durchgehend Microsoft Windows 10 zum Einsatz. Die Softwareverteilung und Installation von Sicherheitsupdates erfolgt zentralisiert.

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

Die Groupware wird durch Microsoft Exchange zentral von der Konzernmutter bereitgestellt.

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

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

Die Datensicherung erfolgt zentral in Bremen.

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

Eine Spezialapplikation für die Versicherungswirtschaft wird auf einem POWER7-System mit IBM AIX betrieben. Die Benutzer auf diesem System sollen nicht doppelt gepflegt werden.

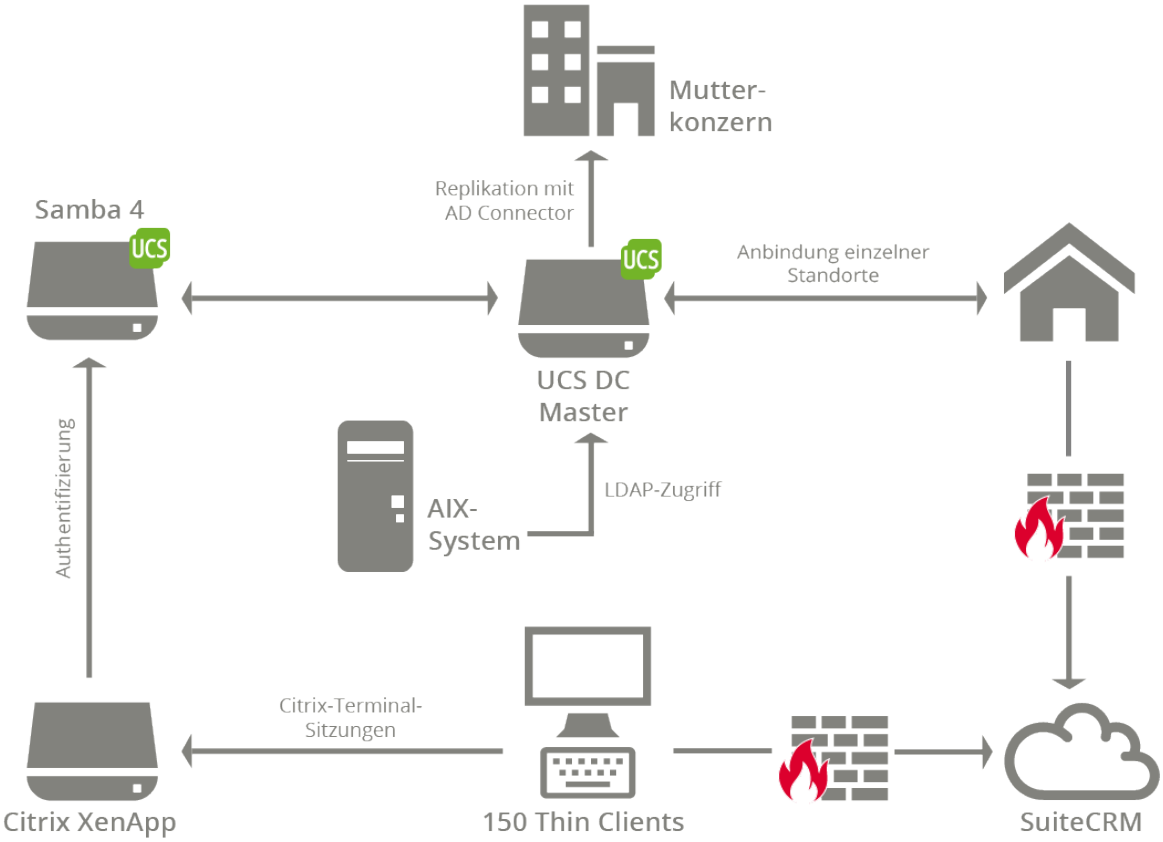
3.2. Umsetzung

Feedback

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

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

Abbildung 3.1. Gesamtüberblick (nicht im Bild: Storage, DNS, DHCP, Druckdienste, Virtualisierung, Backup)

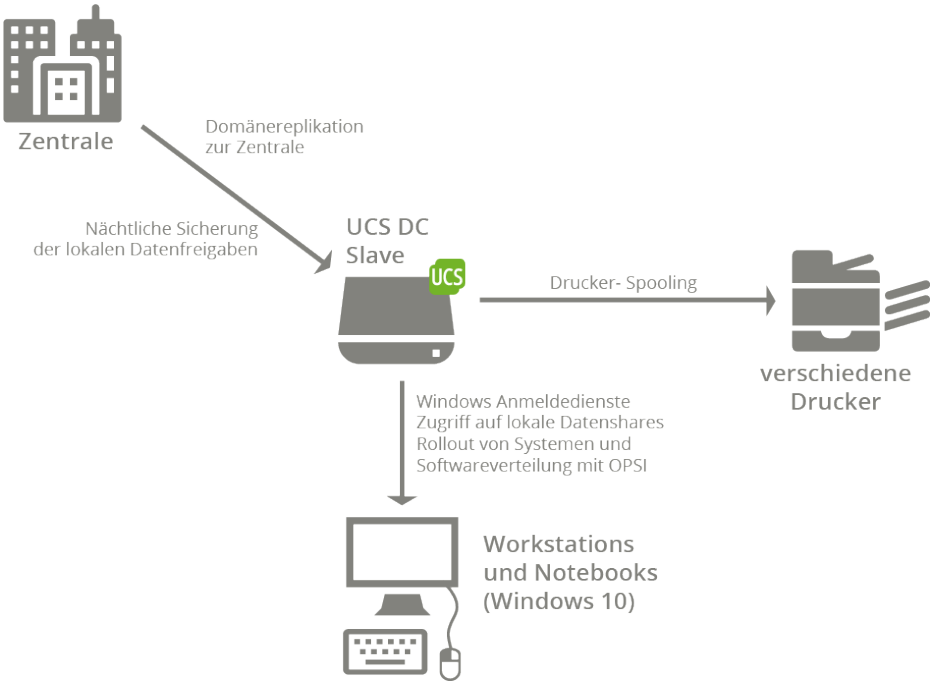


Der DC Backup stellt weitgehend eine Kopie des DC Master dar. Dadurch sind alle wichtigen Dienste doppelt im Netzwerk vorhanden, die Verfügbarkeit der Dienste wird also weiter erhöht und die Last zwischen den Domänencontrollern verteilt.

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

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

Abbildung 3.2. Aufbau eines Standort-Servers

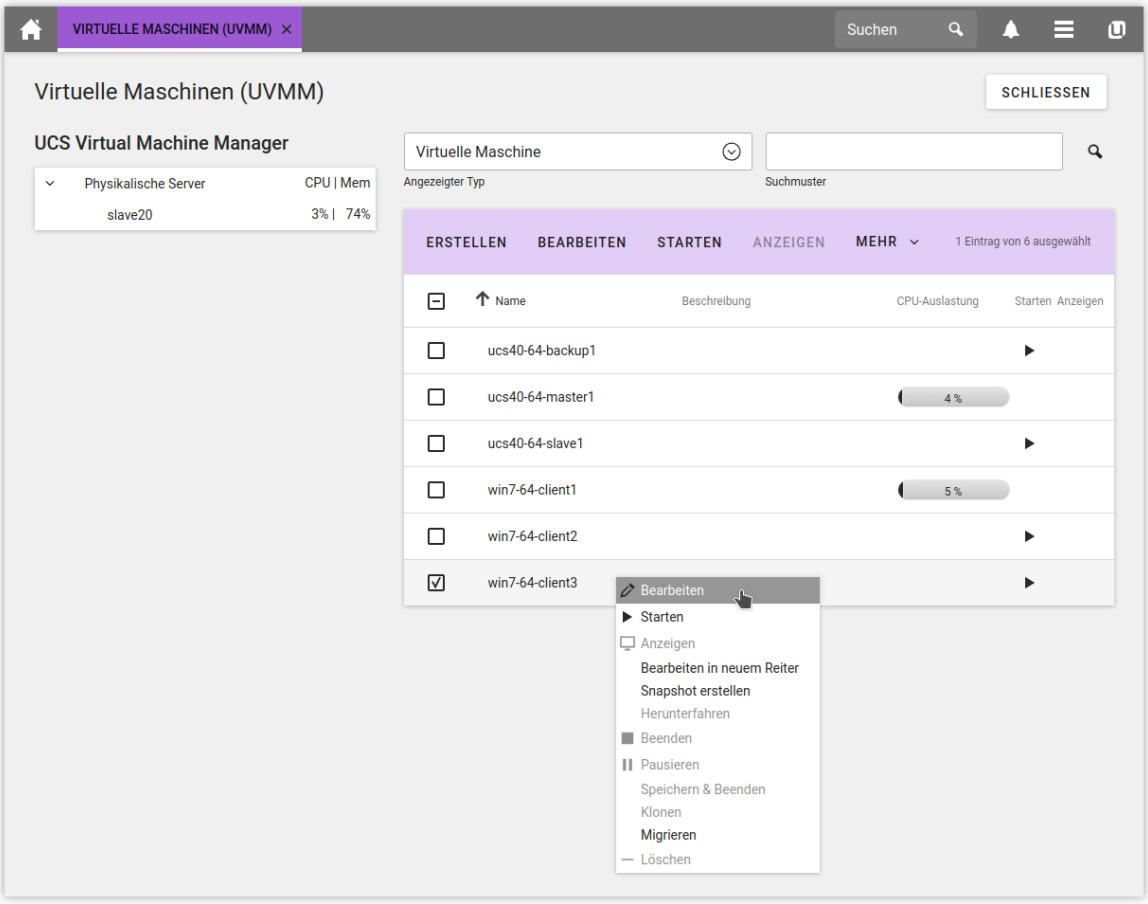


3.3. Virtualisierung

Feedback

Alle Serversysteme in der Umgebung der HMV sind mit UCS Virtual Machine Manager (UVMM) virtualisiert. Zum Einsatz kommt dabei ausschließlich Open-Source-Software.

Abbildung 3.3. Verwaltung virtueller Maschinen mit UVMM



Als Grundlage der Virtualisierung dienen Virtualisierungsserver auf UCS-Memberservern (Serversysteme ohne lokalen Verzeichnisdienst). Auf diesen laufen jeweils ein bis mehrere virtuelle Maschinen mit der Virtualisierungslösung KVM. UCS- und Windows-Systeme werden paravirtualisiert betrieben, d.h. durch einen Zugriff der virtualisierten Systeme auf die Ressourcen der Wirtsysteme kann ein höherer Durchsatz erzielt werden.

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

3.4. Software-Verteilung der UCS-Systeme

Feedback

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

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

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

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

3.5. Anbindung von Windows-Clients und Software-Verteilung

Feedback

In der HMV wird Samba 4 für die Anbindung der Windows-Clients eingesetzt. Samba 4 bietet Domänen-, Verzeichnis- und Authentifizierungsdienste, die kompatibel zu Microsoft Active Directory sind. Diese ermöglichen auch die Verwendung der von Microsoft bereitgestellten Werkzeuge für die Verwaltung von Gruppenrichtlinien (GPOs).

Windows-Clients können direkt der durch UCS bereitgestellten Active Directory-kompatiblen Domäne beitreten und über Gruppenrichtlinien zentral konfiguriert werden. Der Domänen-Join ist aus Client-Sicht identisch mit dem Beitritt zu einer Windows-basierten Domäne.

Auf den Windows-Clients läuft die Open Source-Softwareverteilung opsi. Sie ermöglicht auf den Windows-Clients eine weitgehend automatisierte Verteilung von Sicherheitsupdates und Windows-Updates sowie den Rollout von Software-Paketen.

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

3.6. Active Directory-Anbindung

Feedback

Der UCS Active Directory Connector (kurz AD Connector) ermöglicht eine Synchronisation von Verzeichnisdienstobjekten zwischen einem Microsoft Windows 2008/2012/2016 Server mit Microsoft Active Directory (AD) und dem OpenLDAP-Verzeichnisdienst in Univention Corporate Server.

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

Der UCS-Verzeichnisdienst synchronisiert sich mit dem Microsoft Active Directory-Verzeichnis des Mutterkonzerns. Die Replikation umfasst alle Container, Organisationseinheiten, Benutzer und Gruppen.

Die Rechnerkonten werden nicht synchronisiert, da Windows-Rechner nur in eine Domäne eingebunden sein können. Alle Windows-Clients sind in die UCS-Samba-4-Domäne gejoint.

3.7. Groupware

Feedback

Die Groupware wird in Form von Exchange Server 2016 komplett durch die Konzernmutter Vigil Insurances bereitgestellt, auf das die Benutzer mit Outlook und Outlook-on-the-web zugreifen.

Durch die Anbindung des UCS-Verzeichnisdienstes an das Active Directory der Konzernmutter erfolgt die Authentifizierung mit der gleichen Benutzernamen/Passwort-Kombination.

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

3.8. Compliance-Anforderungen

Feedback

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

- Alle LDAP-Schreibzugriffe müssen verifizierbar sein. Hierzu wird der Univention Directory Logger eingesetzt. Dieser schreibt jede LDAP-Änderung in eine gesicherte Transaktionslogdatei, die über Prüfsummen revisionssicher protokolliert wird.
- Die Benutzerdaten müssen zeitnah für eine Betriebsprüfung abrufbar sein. Hierfür kann über Univention Directory Reports aus der Univention Management Console heraus ein PDF-Dokument oder eine CSV-Datei über alle oder einige Benutzer und Gruppen erstellt werden.
- Es müssen Qualitätsstandards für Passwörter etabliert werden. In UCS kann für Passwörter beispielsweise eine Mindestanzahl von Klein- und Großbuchstaben, Sonderzeichen oder Ziffern konfiguriert werden. Außerdem können Passwörter gegen Listen unsicherer Passwörter (z.B. *secret*) abgeglichen werden.

3.9. System-Monitoring mit Nagios

Feedback

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

Die Konfiguration von Nagios erfolgt weitestgehend in der Univention Management Console.

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

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

3.10. Integration des AIX-Systems

Feedback

Die Versicherungspolicen werden mit einer Applikation verwaltet, die nur auf hochverfügbaren POWER7-Systemen mit IBM AIX betrieben werden kann.

In der Vergangenheit wurden alle Benutzer, die auf dem System arbeiten, doppelt in der lokalen Benutzerdatenbank des AIX-Systems gepflegt. Auf dem AIX-System läuft nun der `secldapclntd`-Dienst, der sämtliche Authentifizierungsvorgänge gegen das UCS-LDAP-Verzeichnis durchführt.

3.11. Citrix Terminal Services

Feedback

In der Zentrale arbeiten 150 Benutzer mit Terminaldiensten auf Basis von Citrix XenApp. Der XenApp-Terminalserver läuft auf einem Microsoft Windows Memberserver, der in die Samba 4-Domäne gejoint ist.

3.12. Backup

Feedback

Für die Datensicherung kommt *SEP sesam Backup Server* aus dem App Center zum Einsatz, das mit wenigen Klicks installiert ist. Es bietet ein verteiltes Sicherungskonzept mit verschiedenen Backup-Agenten, die sowohl komplette Systeme als auch Daten sichern können. Für die Sicherung von Datenbanken stehen etwa gesonderte Agenten zur Verfügung. Alle Daten werden von den Standort-Servern in die Zentrale kopiert und dort auf Bandmedien gesichert. Die Installation erfolgt mit wenigen Klicks aus dem App Center.

3.13. Integration von SuiteCRM

Feedback

Als CRM-Lösung für Vertriebsmitarbeiter wird *SuiteCRM* eingesetzt. Die Verwaltung der SuiteCRM Benutzer- und -rollen integriert sich direkt in die Univention Management Console. Die Installation erfolgt mit wenigen Klicks aus dem App Center.

Die Installation wird als Domänencontroller Slave-System in der Amazon EC2-Cloud betrieben. Dies stellt eine hohe Erreichbarkeit sicher und erlaubt eine flexible Skalierung auf wachsende Leistungs- und Speicherplatzanforderungen.

3.14. Referenzen

Feedback

- https://docs.software-univention.de/handbuch-4.4.html (UCS-Handbuch)
- https://docs.software-univention.de/handbuch-4.4.html#domain-ldap:directorylogger (Revisionssichere LDAP-Protokollierung mit Univention Directory Logger)
- https://docs.software-univention.de/handbuch-4.4.html#uvmm:chapter
- https://docs.software-univention.de/installation-4.4.html (Erweiterte Installations-Dokumentation)
- https://www.univention.de/appid/opsi/ (opsi)
- https://www.univention.de/appid/sep-sesam/ (SEP sesam Backup)
- https://www.univention.de/appid/digitec-suitecrm/ (SuiteCRM)