Projektdokumentation

XEN ADEX Version 1.0

Person	Beschreibung
Ulrich Ritter	Projektleiter XEN ADEX
Alexander Walter	Teilprojektleiter ADEX
Janos Lehnhardt	Teilprojektleiter ADEX

Inhaltsverzeichnis

1. Projekt

1.1 Projektumfeld

Im Zuge der Microsoft-Strategie der Firma sidion betreuen die Studenten Alexander Walter und Janos Lehnhardt das Teilprojekt ADEX im Rahmen ihrer studentischen Projektarbeit.

Hierbei handelt es sich um eine Kooperation der Hochschule der Medien, Studiengang Medieninformatik, und der Firma sidion software- und ingenieurdienstleistungen.

Sie erhalten präzise Anforderungen und Projektziele und sind verantwortlich für die Projektplanung, Projektdurchführung, Umsetzung der Anforderungen und Erreichen der Projektziele.

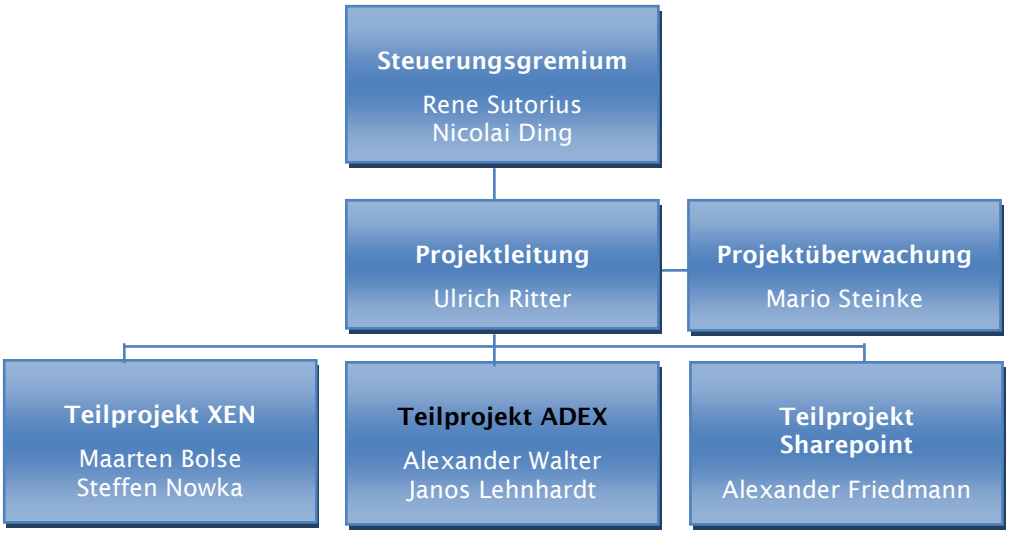
Der Umfang der studentischen Projektarbeit beträgt je 8 ECTS und somit pro Person maximal 240 Stunden. Außerdem haben sie die Möglichkeit auf weitere Personalressourcen zurückzugreifen.

Das Projekt wird durch Prof. Dr.-Ing. Oliver Kretzschmar von der Hochschule der Medien betreut und findet in den Büroräumen der Firma sidion in Stuttgart-Vaihingen statt, die Studenten sind in diesem Zeitraum als studentische Mitarbeiter/Werkstudenten angestellt.

Alle Projektinhalte dürfen in der Projektpräsentation vorgeführt werden, Änderungen werden aus Datenschutz- und Sicherheitsaspekten vorbehalten.

1.2 Projektbeteiligte

Das Projekt XEN ADEX gliedert sich in mehrere Teilprojekte, wie in nachfolgendem Organigramm ersichtlich ist. Das studentische Projekt befasst sich mit dem Teilprojekt ADEX, weshalb der Projektteil XEN in dieser Dokumentation ausgeklammert ist.



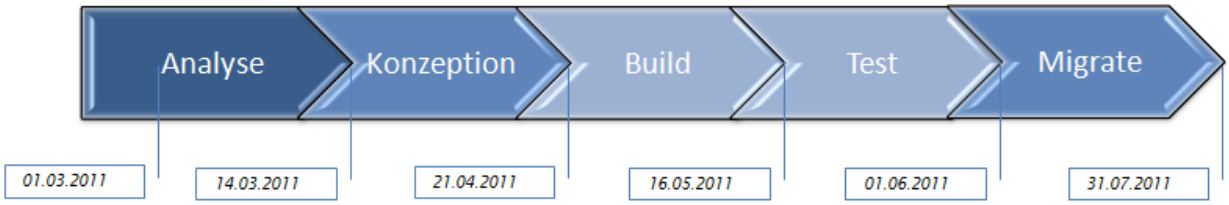
Die Teilprojektleitung übernehmen Alexander Walter und Janos Lehnhardt, als betreuende Ressource stehen zudem die Mitarbeiter Alexander Friedman und Kay Urbach zur Verfügung.

Die Leitung des Projektes wird von Ulrich Ritter übernommen, der auch für die Festlegung der Anforderungen zuständig ist, die Projektüberwachung erfolgt durch Mario Steinke.

Dieses Dokument wurde ausschließlich von Alexander Walter und Janos Lehnhardt erstellt, da sie als Prüfungsleistung eingereicht wird.

1.3 Projektplanung

Das Teilprojekt ADEX ist in mehrere Phasen untergliedert, die jeweils einen klar definierten Start- und Endzeitpunkt zugewiesen haben.



Das Projekt beginnt mit einer Analysephase, in welcher die Anforderungen detailliert analysiert und auf Machbarkeit geprüft werden. Darauf folgt die Analyse der Ausgangssituation sowie Einarbeitung in die bisherige Infrastruktur, um anschließend anhand der Anforderungen die Zielsituation zu konzipieren. Diese Phase beginnt zeitgleich mit dem Semesteranfang am 01.03.2011.

Am 14.03.2011 folgt die Konzeption, in der die gegebene Zielsituation detailliert und konkret geplant wird. Dies umfasst nicht nur die reine Konzeption, sondern auch den Wissensaufbau und Machbarkeitstests, was notwendig ist um eine realitätsnahe Konzeption und Rollout-Planung zu ermöglichen. In dieser Phase findet zudem eine detaillierte Arbeitspaketplanung/Vorgehensplanung für die Konzeptionsphase, aber auch für die Phasen Build, Test und Migrate statt.

Nach Abschluss der Konzeption findet der Build statt, in dem Hardware, Software und Systeme gemäß der Konzeption installiert bzw. konfiguriert werden, außerdem findet hier der Projektrollout gemäß des zuvor konzeptionierten Rolloutplans statt.

Die Testphase zeigt, in wie weit die Planungen aus der Konzeption umgesetzt und funktionsfähig sind, was über Funktionstests erreicht wird. Zu diesem Zeitpunkt sind alle Systeme aktiv im Einsatz und nutzbar, werden aber noch im Parallelbetrieb durch Administratoren und ausgewählte Nutzer getestet.

Nach erfolgreichem Test findet das Projekt seinen Abschluss in der Phase Migrate, bei der alle Nutzdaten von den Alt-Systemen in die Neu-Systeme migriert werden und die Neu-Systeme komplett in der sidion Infrastruktur integriert sind. Die Migration stellt das Herzstück des Projektes dar und ist aus Firmensicht besonders kritisch, aus diesem Grund bedarf es einer gründlichen Planung der Migrations- und Rolloutphase. Es werden verschiedene Lösungsstrategien ausgearbeitet und evaluiert. Detaillierte Informationen finden Sie unter dem Punkt 3.7 Migration und 3.8 Rollout.

Das Projekt wird an der MediaNight der Hochschule der Medien am 30.06.2011 in Stuttgart-Vaihingen präsentiert.

1.4 Zeitplanung

Die Studenten Alexander Walter und Janos Lehnhardt arbeiten vom 01. März 2011 bis einschließlich 31. Juli 2011 an diesem Projekt, jeweils ganztags donnerstags (8 Stunden) und halbtags freitags (4 Stunden), also 12 Stunden pro Woche.

Über die komplette Projektzeit von 21 Kalenderwochen leistet somit jeder Student einen Arbeitsaufwand von 252 Stunden ab.

Zusätzlich arbeiten einige Festangestellte sidion Mitarbeiter an diesem Projekt, speziell bei der Implementierung und beim Rollout.

2. Analyse

2.1 Anforderungen

Im Fachkonzept des Gesamtprojekts existiert ein umfangreiches Anforderungsregister, welches sowohl grobe als auch detaillierte Anforderungen umfasst.

Die Anforderungen wurden im Detail betrachtet und sind vollständig in die Konzeptionierung eingeflossen, um diese Projektdokumentation nicht unnötig zu vergrößern, folgen nur die wichtigsten Anforderungen.

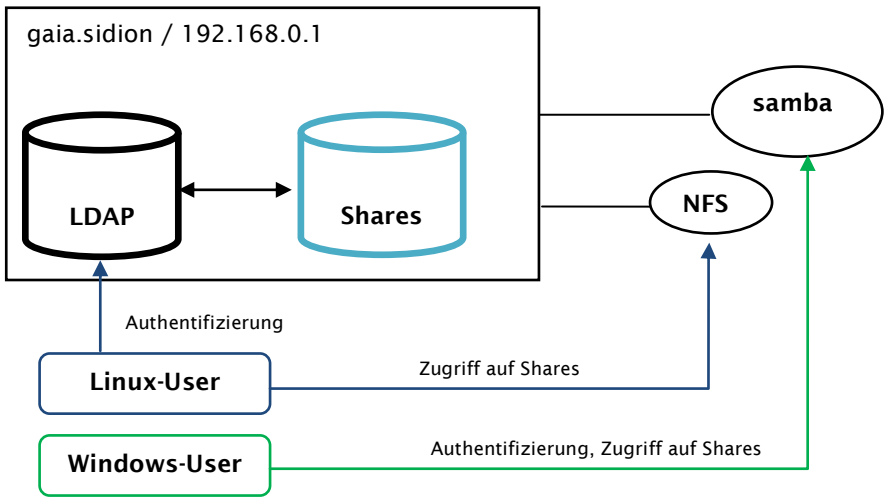
- Ablösung Lotus Notes durch einen inhouse gehosteten MS Exchange 2010 E-Mail Server
- Vollständige Migration aller E-Mails, Postfächer, Kalender, Termine, Ressourcen
- Integration einer Windows Domäne unter Verwendung eines Active Directory
- Ablösung des LDAP-Verzeichnisses durch den Active Directory (Benutzer und Profilverwaltung)
- Integration des Active Directory in die bestehende Single Sign On Lösung
- Vollständige Migration der bestehenden Benutzerdaten und Benutzerprofile in die neue Domäne
- E-Mail Zugriff über Webschnittstelle (Https) sowie POP3, IMAP

2.2 Ausgangssituation

2.2.1 SIDION Domäne

Die heterogene Clientlandschaft im sidion Netzwerk besteht aus Windows und Linux Clients, es existiert eine Domäne SIDION zur zentralen Benutzerverwaltung auf den Clients und globalen Verwaltung und Verwendung von serverseitig gespeicherten Benutzerprofilen.

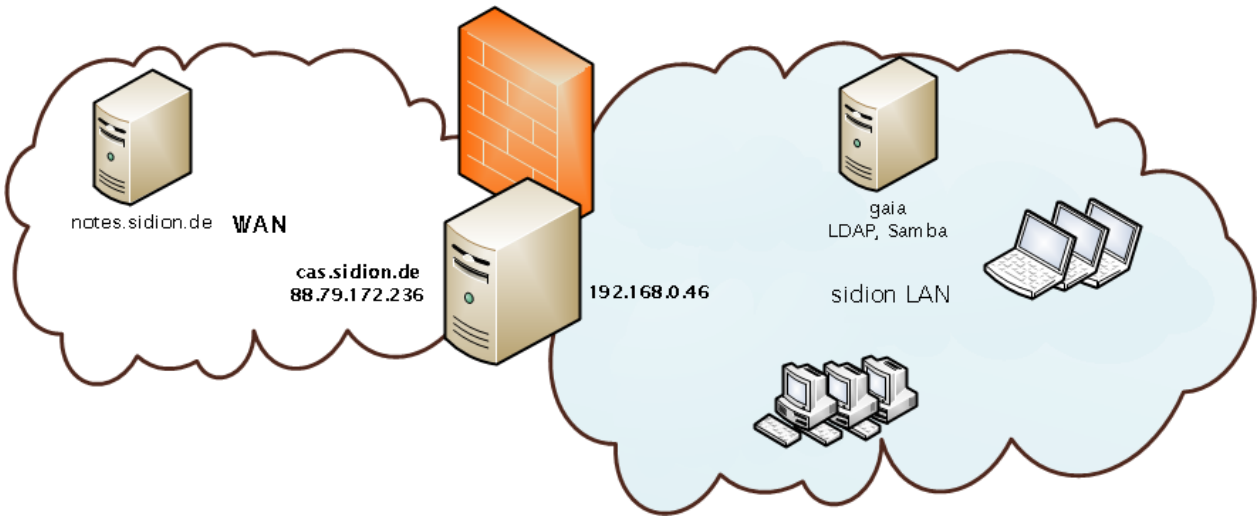
Alle Windows Clients sind über den Samba Dienst, der eine Windows Domäne im Netz simuliert, mit der Domäne verbunden. Der Samba Dienst synchronisiert die Benutzerdaten mit dem LDAP-Verzeichnis. Alle Linux Clients greifen direkt über LDAP auf die Domäne zu.



Die Benutzerprofile sind zentral auf einem Server (gaia.sidion) gespeichert und werden bei jeder An- und Abmeldung abgerufen bzw. synchronisiert. Die Dateifreigabe zur Bereitstellung der Benutzerprofile und gemeinsam genutzten Netzlaufwerke (Shares) findet für Linux Clients über NFS statt, Windows-Clients greifen über den Samba-Dienst zu.

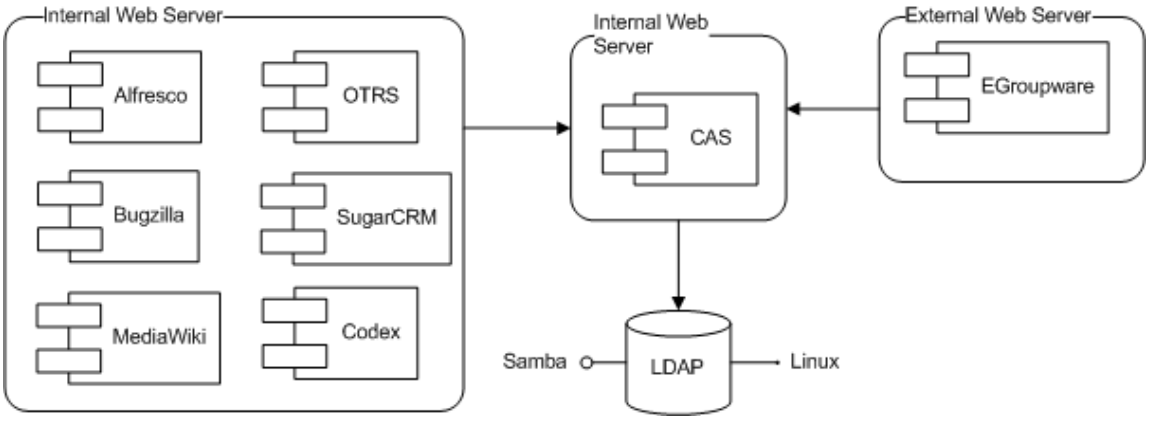
2.2.2 Webservice Single Sign On

Die Authentifizierung von Usern im sidion Intranet (Webservices) wird über einen sogenannten CAS-Server (Central Authentication Server) realisiert, der intern im sidion LAN gehostet ist und sowohl vom sidion LAN als auch über das Internet über die Adresse cas.sidion.de erreichbar ist. Dadurch wird ein Single Sign On (SSO) innerhalb des sidion Netzes erreicht, das bedeutet eine einmalige Authentifizierung reicht aus, um sich anschließend nahtlos zwischen den verschiedenen Webservices zu bewegen.



Bei der Anmeldung erhält dabei jeder Client ein Ticket, welches von jedem einzelnen Webservice im Trust-Verbund verifiziert wird.

Die Authentifizierungsdaten sind zentral auf einem LDAP Server gespeichert, der ebenfalls auf dem Server gaia gehostet ist, die Rechteverwaltung wird jedoch lokal in den Webservices gehalten.



Das Aktivitätsdiagramm im Anhang stellt den Standard-Ablauf bei der CAS-Anmeldung dar. Der Active Directory Server ist in diesem Fall das LDAP-Verzeichnis.

Damit Benutzer ihre Passwörter selbstständig ändern können, wurde ein PHP-Skript entwickelt, welches eine Passwortänderung direkt an den LDAP-Server weiterreicht.

Eine Ausnahme stellt die Authentifizierung via Indevis-VPN und Lotus Notes (E-Mail) dar, die jeweils eine separate Benutzerverwaltung verwenden.

2.2.3 Beteiligte Server

Für die Realisierung der heterogenen Domäne und des Single Sign On sind die in 2.1 erwähnten Server gaia und cas von hoher Bedeutung, daher zeigt die folgende Tabelle die grundlegende Hard- und Softwarespezifikation der Server.

Host	**IP-Adresse**	**Subnetmaske**	**Beschreibung**
gaia	192.168.0.2	255.255.255.0, /24	Bare Metal Dell PowerEdge R710 CPU: 1x Intel XEON E5502 1.86 GHz Dualcore RAM: 3x 2GB Dual Rank 667 MHz DDR2 HDD: 5x 1TB SAS RAID: 1 NIC: 3x Broadcom NETXTREME || 5708 GBit Warranty: 25.01.2013 Support: DELL
DNS-Record(s)		**Betriebssystem**	**Software / Dienste**
gaia.sidion ldap.sidion swat.sidion		Ubuntu 9.10	Bacula Backup (Serverseitiges Backup aller Server) LDAP-Verzeichnisdienst NFS-Server (Bereitstellung Netzwerkshares) Samba-Server (Simulation Windows Domäne)
Host	**IP-Adresse**	**Subnetmaske**	**Beschreibung**
cas	192.168.0.46 88.79.172.236	255.255.255.0, /24	Virtual Machine (Xen basiert) CPU: 2 Virtuelle Prozessoren RAM: 1024 GB Explizit HDD: 250 GB NIC: 2 Virtuelle LAN Karten
DNS-Record(s)		**Betriebssystem**	**Software / Dienste**
cas.sidion.de		Ubuntu 9.10	CAS Server inkl. Tomcat, Apache2 Passwort Ändern Seite

2.2.4 Authentifizierung an der Domäne

Jeder Mitarbeiter besitzt einen einzigartigen Benutzerzugang, der zur Anmeldung (Authentifizierung) an Windows- und Linux-Maschinen sowie Netzwerkdiensten dient. Anhand dieser Benutzerzugänge findet die Rechteverwaltung statt. Laptops haben in der Regel eine lokale Anmeldung. Die Authentifizierung auf interne Systeme und Lotus Notes muss manuell erfolgen.

Im LDAP ist es außerdem möglich Benutzergruppen zu definieren, diese werden für die Rechtevergabe auf den Services SugarCRM und Codex verwendet.

2.2.5 Benutzerprofile

Für alle Windows- und Linux-Clients werden serverseitig gespeicherte Benutzerprofile verwendet. Diese befinden sich im NFS-Share des Storage-Servers gaia unter

Linux: **\\gaia\AlleHomes\Max.Mustermann**
Windows: **\\gaia\AlleHomes\samba\profiles**

Außerdem legt der Domänencontroller für jedes Betriebssystem einen separaten Ordner nach folgender Struktur an.

Windows XP: **\\gaia\AlleHomes\samba\profiles\Max.Mustermann**
Windows Vista: **\\gaia\AlleHomes\samba\profiles\Max.Mustermann.V2**
Windows 7: **\\gaia\AlleHomes\samba\profiles\Max.Mustermann.V3**

Zusätzlich besitzt jeder Mitarbeiter ein "Home-Verzeichnis", welches als sichere Dateiablage dient und täglich inkrementell gesichert wird.

Darüber hinaus existiert eine Reihe von Netzfreigaben, die alle auf den Storage-Server gaia verweisen.

\\gaia\CAE
\\gaia\Gruppenordner

Die Rechteverwaltung wird über LDAP Gruppen und Benutzer gesteuert.

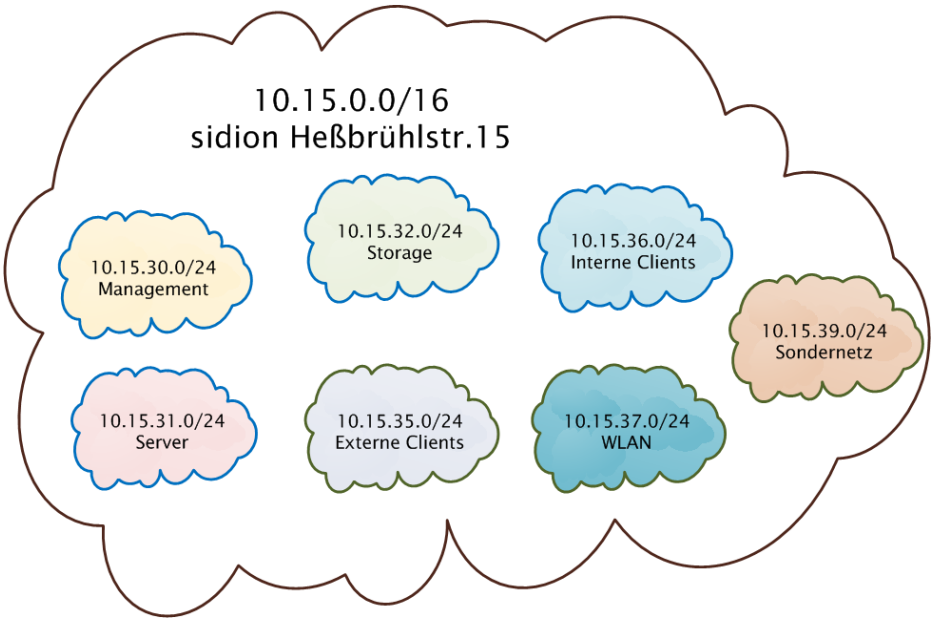
2.2.6 DNS & DHCP

Als DNS-Server wird der OpenSource Server bind9 verwendet, als DHCP-Server dient der Debian dhcpd-Service.

Das sidion Netzwerk verwendet eine private Class B Adresse mit 65536 möglichen Adressen, mithilfe von Subnettierung wurde es in 7 weitere Subnetze segmentiert, die je 256 mögliche Adressen beinhalten.

Hauptnetz:	10.15.0.0/16
Management:	10.15.30.0/24
Server:	10.15.31.0/24
Storage:	10.15.32.0/24
Externe Clients:	10.15.35.0/24
Interne Clients:	10.15.36.0/24
WLAN:	10.15.37.0/24
Sondernetz:	10.15.39.0/24

Die in der Abbildung blau markierten Netze werden komplett über DHCP verwaltet, hierbei ist es möglich feste IPs über eine MAC-Adressen Zuordnung zu vergeben.



2.2.7 E-Mail-Funktionalität Generell

Die Anwendung und die Mailboxen werden extern von Fa. SystAG betreut und administriert. Die Einrichtung neuer Benutzer erfolgt im Rahmen eines kostenpflichtigen Zusatzauftrages. SystAG stellt die Verfügbarkeit, Vertraulichkeit und die Vollständigkeit des Emailssystems sicher.

Der Zugang erfolgt standardmäßig über einen Lotus Notes Client oder über einen direkten Lotus Notes Webzugang. In Einzelfällen ist der Zugriff per Smartphone eingerichtet.

Es besteht ein Helpdesk zur Störungsmeldung. Alle administrativen Aufgaben des Lotus Notes Systems (Monitoring, Backup, Patching, etc) erfolgen durch SystAG.

Die Authentifizierung findet unabhängig des CAS-Servers mit einem separaten Benutzer-, Rollen- und Rechtekonzept.

2.2.8 Postfächer

E-Mail-Funktion wird allen internen und externen festangestellten Mitarbeitern zur Verfügung gestellt. In Ausnahmefällen erhalten auch freie Mitarbeiter einen Emailaccount. Zugriff auf die Mailboxen erfolgt vom LAN, über eine VPN-Verbindung oder über Lotus Notes Web-Access.

Die Postfächer erhalten standartmäßig 500 MB Kapazität, es ist möglich die Kapazität gegen Aufpreis zu erhöhen, das derzeit größte Postfach beläuft sich auf 2500 MB.

Die Bruttogesamtkapazität aller Postfächer liegt am Projektbeginn 50 GB, die Nettogesamtkapazität bei rund 25 GB. Große Schwankungen sind während des Projektes nicht zu erwarten.

2.2.9 Gruppen / Verteiler

Die sidion Administratoren können mit Lotus Notes E-Mail-Verteiler kostenlos erstellen, die auf beliebige E-Mail-Adressen weiterleiten können. Der Anteil aktiver Verteiler liegt am Projektbeginn bei 25 Verteilern.

Darüber hinaus ist es möglich Lotus Notes Benutzer zu gruppieren um Gruppenfunktionalitäten (Gruppentermine, Gruppenkalender) gemeinsam zu nutzen. Die Anzahl der Gruppen beläuft sich auf 3.

2.2.10 Ressourcen

Über Lotus Notes ist es möglich Ressourcen zu definieren und diese für Termine zu reservieren. Derzeit gibt es folgende Ressourcen:

- AIS Team Laptop
- Digi Cam
- sidion Beamer
- sidion Besprechungsraum
- Siemens Handy Ladegerät für Autos

2.2.11 Aufgaben, Termine, Kalender

Lotus Notes erlaubt eine detaillierte Termin- und Kalenderverwaltung. Über Rechtevergabe ist es möglich, den Zugriff auf Kalender und Termine feingranular zu gewährleisten. Termine sind in folgende Kategorien unterteilbar:

- Feiertag
- Urlaub
- Projekte
- Kunden
- Anrufe
- Unterwegs
- Benutzerdefinierte Kategorien

Zusätzlich gibt es folgende Features:

- Führen von Gruppenkalender
- Terminvorschläge
- Besprechungsanfragen
- Führen von individuellen Aufgaben und Wiedervorlage von Aufgabe

2.2.12 Globales Adressen-Verzeichnis

Es existiert ein globales sidion Verzeichnis in dem alle Benutzer mit benutzerdefinierten Angaben wie Adresse und Telefonnummer aufgelistet sind. Zusätzlich werden alle vorhandenen Gruppen und Non-Personal-Accounts dargestellt.

Weiterer Funktionsumfang

- Senden / Empfangen / Weiterleiten / Wiedervorlage von E-Mails
- Archivierung von Mails auf lokalen Datenbanken
- Abwesenheitsagent
- Vertretungsregelung und Zugriffsrechteverwaltung
- Abruf von E-Mails/Terminen und Aktivitäten auch über Smartphones
- Offline Zugriff auf die eigene Notes-Datenbank

2.2.13 Security

Der Lotus Notes Mailserver wird von der SystAG vor Spam und Malware geschützt. Für den Schutz der Windows- und Linux-Clients wird bisher das Softwareprodukt AntiVir Professional verwendet. Es existieren 100 Lizenzen für die Anwender, die Software ist lokal auf den Clients installiert und wird direkt von den Clients verwaltet, konfiguriert und aktualisiert.

2.3 Zielsituation

In Anbetracht der Unternehmensentwicklung ist es notwendig, die IT-Services mit höherer Zuverlässigkeit zur Verfügung zu stellen. Dabei sind sowohl Sicherheitsthemen als auch optimale Bereitstellung der IT-Services relevant. Diese Ziele werden erreicht durch technische und organisatorische Anpassungen der aktuellen IT Landschaft.

Es gibt im Wesentlichen 2 Projekt-Oberziele:

- Ablösung Lotus Notes durch Microsoft Exchange
- Single Sign On durch den Einsatz einer Microsoft Active Directory

Diese Ziele werden untermauert bzw. detailliert durch zahlreiche inhaltliche und qualitative Anforderungen. Im Rahmen der Umsetzung sind folgende Ziele definiert:

- Externe Lotus Notes Dienstleistung sollte möglichst zum regulären Vertragsende am 31.Juli 2011 enden.

Allerdings unter der Prämisse von:

- Qualitative hochwertige Installation und Migration zu MS Exchange
- Minimale Migrations-Auswirkungen auf die Endbenutzer

Die konkurrierenden Projektbeziehungen Budget-Time-Qualität werden zugunsten der Qualität gesetzt und haben ggf. Auswirkungen auf die Projektdauer. Wird im Rahmen der Meilensteinplanung erläutert.

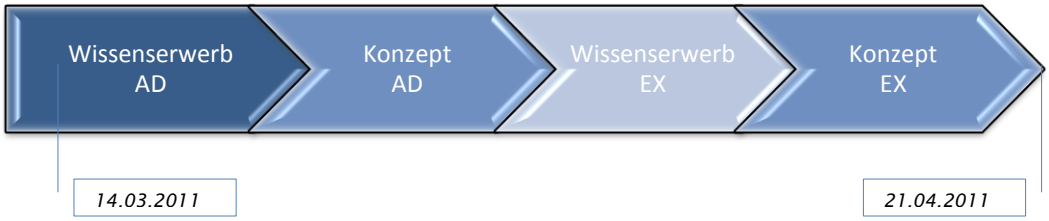
Daraus lassen sich allgemeinere Projektziele ableiten.

- Mit der Einführung und dem Betrieb der Microsoft Produkte soll die Kompetenz der internen IT Mitarbeiter erhöht werden, um dadurch externe Beratungsaufträge professionell umsetzen zu können.
- Der Funktionsumfang wird durch die Einführung von Exchange gegenüber Lotus Notes verbessert.
- Integration von Drittsystemen wird erst durch die geänderte Plattform möglich.
- Voraussetzung für Exchange ist eine Domäne mit einer Active Directory Struktur. Diese soll genutzt werden als primäre Anmeldedomäne und steuert alle nachgelagerten Systemzugriffe (Single-Sign-On).
- Mit Exchange ist eine gesetzeskonforme Archivierung von Emails möglich

3. Konzeption

3.1 Planung

Eine möglichst realistische Planung und zielgenaue Konzeption benötigt Erfahrung und das nötige Fachwissen. Da dieses Projekt für alle Projektbeteiligten gleichzeitig den Einstieg in die Microsoft Welt bedeutete, mussten diese Faktoren zunächst aufgebaut werden.



Die beiden Phasen Wissenserwerb AD/EX beinhalten neben Lektüre vor allem das experimentelle Anwenden der später zur Verwendung kommenden Softwareprodukte, um effizient Erfahrung und Fachwissen aufzubauen.

Aus diesem Grund wurden jeweils realitätsnahe Testumgebungen virtualisiert aufgebaut und alle für die spätere Projektumsetzung notwendigen Situationen im Kleinformat unter dem Begriff Wissenserwerb AD/EX getestet. Getestet wurde in einem separaten Testnetz.

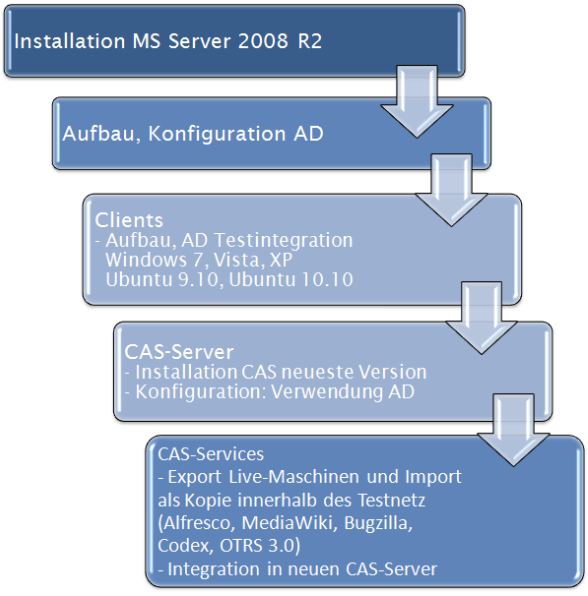
Anschließend wurde anhand der Testergebnisse das Konzept des Active Directory (AD) und Exchange Servers (EX) und die Planung des Rollouts und der Migration (Phase Migrate) erstellt.

Außerdem wurde die Phase Migrate bereits durch die Erstellung von Checklisten vorbereitet.

3.2 Wissenserwerb AD

Zu Testzwecken und zur Wissensaneignung wurde eine „AD-Spielwiese“ eingerichtet. Anhand der Ergebnisse wurden anschließend erste, unvollständige Anleitungen erstellt sowie die Konzeption begonnen. Neben der Installation eines Windows-Server und Konfiguration eines Active Directory, sowie Integration aller im sidion-Netz verfügbarer Betriebssystemen, wurde auch der CAS-Server in die Testumgebung integriert und getestet. Dabei stellte sich heraus, das die bisher verwendete, veraltete, Version des CAS-Servers nicht in der Lage ist sich gegen einen Microsoft Active Directory zu authentifizieren.

Aus diesem Grund musste der CAS-Server aktualisiert werden – da sich dieser Aufwand allerdings mit der Neuinstallation und Neukonfiguration eines CAS-Servers auf neuester Version gleichzusetzen ist, fiel die Wahl auf einen kompletten Neuaufbau des CAS-Servers. Hierbei wurden folgende Szenarien aufgebaut und spielend getestet.

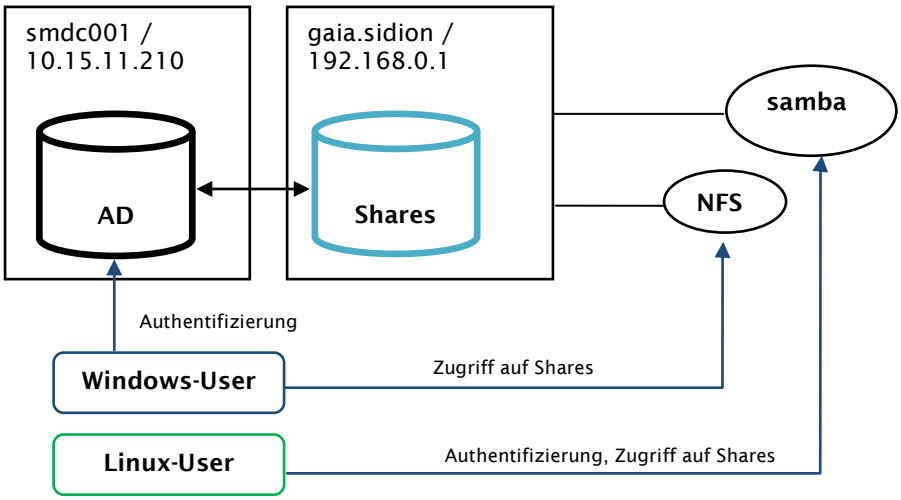


3.3 Zielarchitektur Active Directory

Windows Domäne

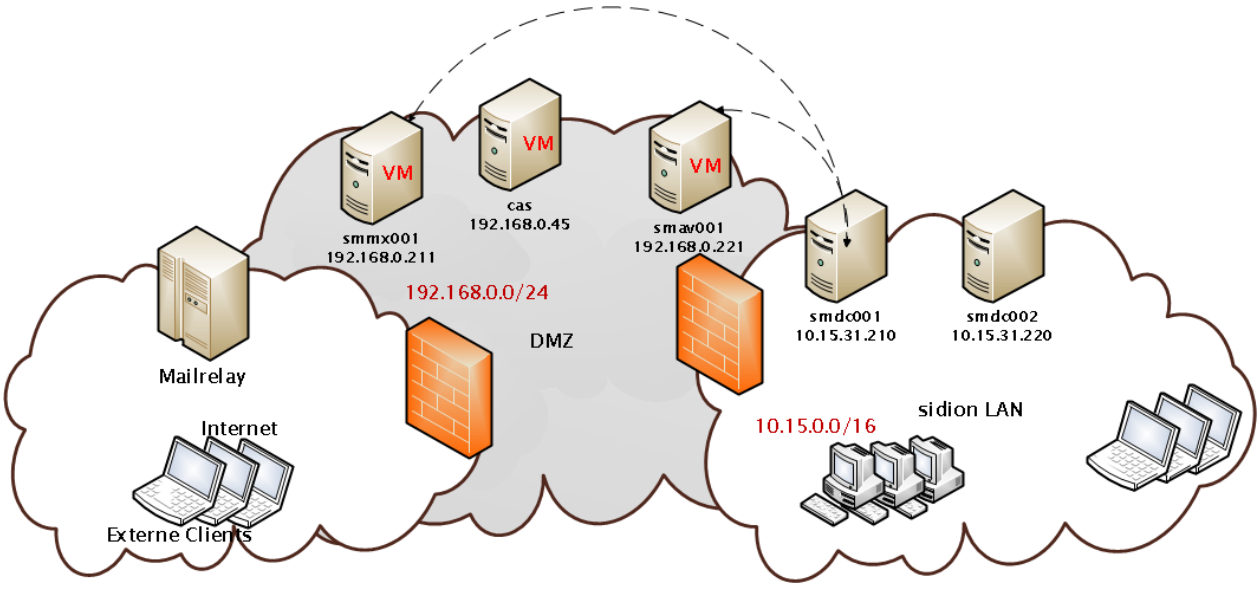
Die Samba-/LDAP-Domäne wird durch ein Microsoft Active Directory ersetzt. Alle Windows-Clients authentifizieren sich direkt über die Windows-Domäne, die Linux-Clients verwenden einen Samba-Client. Die Shares befinden sich unverändert auf dem Fileserver gaia und werden über NFS- und Samba-Freigaben bereitgestellt.

Der Fileserver läuft unter Debian und verwendet ebenfalls einen Samba-Client, um auf sich mit der Domäne zu verbinden. Dadurch wird eine Authentifizierung am NFS-Server mit den Daten des Active Directory ermöglicht.



Serverlayout & Hochverfügbarkeit

Der Domain Controller (DC) wird auf zwei physischen Servern mit Windows Server 2008 RC2 installiert. Die beiden Server, smdc001 und smdc002 genannt, sind intern im sidion LAN gehostet. Zum Realisierungszeitpunkt wurde das sidion Netzwerk um eine DMZ* (Abbildung: Graue Wolke) erweitert, in der alle extern verfügbaren Dienste platziert sind. Auf beiden Servern wird außerdem die Microsoft Virtualisierungslösung Hyper-V installiert, mit deren Hilfe eine virtuelle Maschine smmx001 instaliert wird. Dieser logische Server beinhaltet den Microsoft Exchange-Server, welcher in der DMZ gehostet ist und somit sowohl im sidion LAN als auch im WAN erreichbar ist.

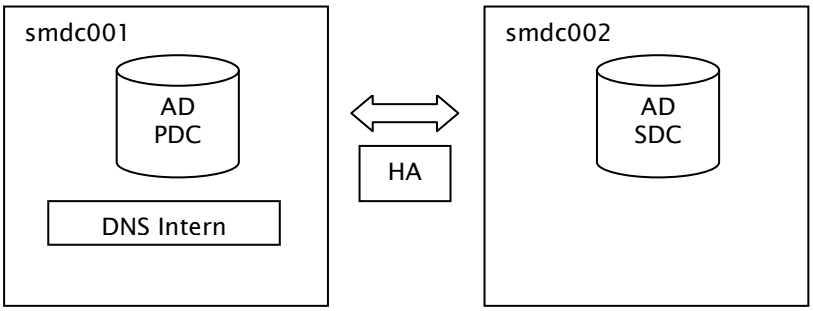


Die Domäne stellt einen kritischen Service des sidion LAN dar und muss somit hochverfügbar sein. Um einen Single Point of Failure (SPOF) zu vermeiden, dient der erste Server smdc001 als primärer

Domänencontroller (PDC), auf dem neben der AD die Services DNS und DHCP betrieben werden. Der zweite Server smdc002 wird als sekundärer Domänencontroller (SDC) redundant betrieben.

Das im Windows Server 2008 R2 Enterprise enthaltene High Availability Feature ermöglicht eine permanente Synchronisierung der Datenbestände (AD, DNS, DHCP) und einen problemlosen Client-Übergang (Reassociation) vom PDC zum SDC.

* Die neu einzuführende DMZ wird außerhalb des Projektes von den sidion Netzwerktechnikern realisiert und wird somit im nicht mehr weiter betrachtet.



Beteiligte Server

Das Softwarepaket des CAS-Servers muss komplett aktualisiert werden. Da über den bisherigen CAS-Server keine ausreichend gute Dokumentation vorhanden ist, wurde der strategische Entschluss getroffen, den CAS-Server auf einer separaten virtuellen Maschine neu zu installieren und alle benötigten Anwendungen zu konfigurieren. Nachdem der CAS-Server vollständig getestet wurde, wird dieser parallel zum bisherigen CAS-Server betrieben und erst zum Zeitpunkt des AD-Livegangs in die Systemlandschaft integriert, sodass der alte CAS-Server ersetzt wird.

Diese vollständige Neuinstallation wird detailliert dokumentiert und ist im Installationshandbuch nachzulesen.

Der neue CAS-Server erhält nachfolgende Spezifikationen.

Host	**IP-Adresse**	**Subnetmaske**	**Beschreibung**
cas	192.168.0.46	255.255.255.0, /24	Virtual Machine (Xen basiert) CPU: 2 Virtuelle Prozessoren RAM: 2046 MB Explizit HDD: 250 GB NIC: 2 Virtuelle LAN Karten
DNS-Record(s)		**Betriebssystem**	**Software / Dienste**
cas.sidion.de		Debian	CAS Server 3.4.6 Tomcat Server Apache 2 Webserver Passwort Ändern Seite PHP5
Host	**IP-Adresse**	**Subnetmaske**	**Beschreibung**
smdc001	10.15.31.210	255.255.255.0, /24	Bare Metal Dell PowerEdge 1950 CPU: 2x Quad-Core XEON E5410 2.33 GHz RAM: 8x 2GB Dual Rank 667 MHz DDR2 HDD: 4x 500GB SATA 7.200 NIC: 3x Broadcom NETXTREME || 5708 GBit Warranty: 16.08.2011 Support: DELL
DNS-Record(s)		**Betriebssystem**	**Software / Dienste**
smdc001		Microsoft Windows 2008 Enterprise R2	Windows Active Directory Hypervisor „Microsoft Hyper-V“

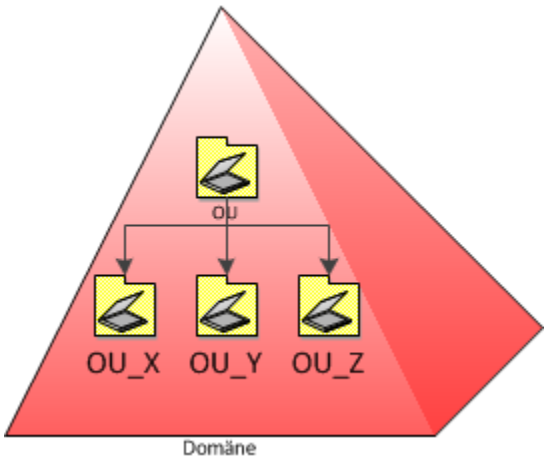
Host	IP-Adresse	Subnetmaske	Beschreibung
smdc002	10.15.31.210	255.255.255.0, /24	Bare Metal Dell PowerEdge 1950 CPU: 2x Quad-Core XEON E5410 2.33 GHz RAM: 8x 2GB Dual Rank 667 MHz DDR2 HDD: 4x 500GB SATA 7.200 NIC: 3x Broadcom NETXTREME || 5708 GBit Warranty: 16.08.2011 Support: DELL
DNS-Record(s)		**Betriebssystem**	**Software / Dienste**
smdc002		Microsoft Windows 2008 Enterprise R2	Windows Active Directory Hypervisor „Microsoft Hyper-V“

3.4 Domänen Konzept

Beim Aufbau einer Active Directory (AD) ergibt sich die Möglichkeit, die Struktur dieser nach verschiedenen Konzeptionsmodellen aufzubauen. Im Folgenden wird auf drei Konzeptionsmodelle eingegangen und die beste Variante für das Projekt ADEX gewählt.

3.4.1 Domänen Modelle

Es existiert eine einzige Domäne für das gesamte Unternehmen, die mit einer OU-Struktur kombiniert wird und sich an den geografischen Verhältnissen orientiert.



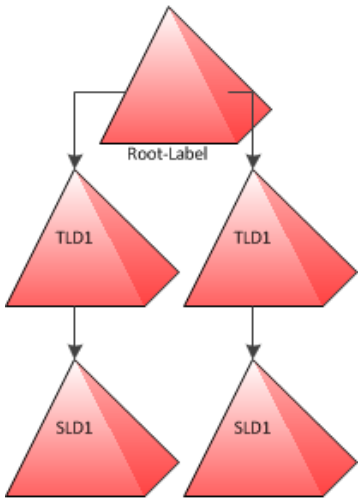
Vorteile	Nachteile
Zentrale Administration der Sicherheitsrichtlinien (Policies)	Eine große Domain deshalb entsprechend hohe Hardware Anforderungen an die Domaincontroller
Sehr Flexibles Modell für Reorganisation, Hinzufügen neuer OU	Hohe Auslastung der WAN-Verbindung bei Sync. mit Sekundären-DC (im Falle, dass der sekundäre DC im nicht im LAN ist)
Einfaches Verschieben von Objekten innerhalb der Struktur. (User/Gruppen/Folder)	
Jeder Domaincontroller bekommt alle Objekte Replizier	

3.4.2 Tree Modell

Das Tree-Modell besteht aus mehreren Domänen die in einer Baum-Struktur angeordnet sind. Dabei wird der Namensraum je nach Strukturtiefe erweitert.

Bsp: „SLD.TLD.RL“

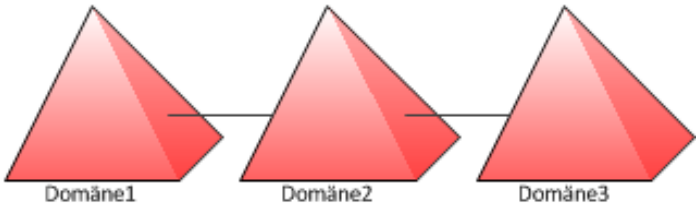
SLD: 2nd-Level-Domain
TLD: Top-level-Domain
RL: Root-Label



Vorteile	Nachteile
Der Namensraum repräsentiert die Struktur des Unternehmens	Reorganisation ist mit immensem Aufwand verbunden
Unternehmensbereiche haben komplette Verfügungsgewalt über ihre Domäne	Verschieben von Objekten (User/Ressourcen) zwischen den Domänen ist komplex
	Keine zentrale Administration möglich

3.4.3 Forrest Modell

Dieses Modell ist eine weitere Variante des Tree-Modells bei der jedoch der Namensraum nicht fortlaufend ist. Das Domain-Modell lässt sich in diese Struktur erweitern. Dabei sind die einzelnen Domänen sind auf einer Ebene angeordnet.



Vorteile	Nachteile
Domänen können bei Erweiterung ihren bisherigen Namensraum weiter benutzen	Verschieben von Objekten (User/Ressourcen) zwischen den Domänen ist komplex
Domänen haben komplette Verfügungsgewalt	Keine zentrale Administration möglich
	Um umfassende LDAP-Abfragen zu gewährleisten, müssen diese an einen übergeordneten Global Catalog Server gerichtet werden

3.4.4 Entscheidung

Die Eigenschaften des Domain-Modells sind für die Firma sidion und das Projekt ADEX optimal. Die Flexibilität der Struktur, die Möglichkeit die Objekte innerhalb der Struktur unkompliziert neu zu Organisieren und die Struktur ohne großen Reorganisationsaufwand zu erweitern sind die Hauptkriterien warum wir uns für dieses Konzept entschieden haben.

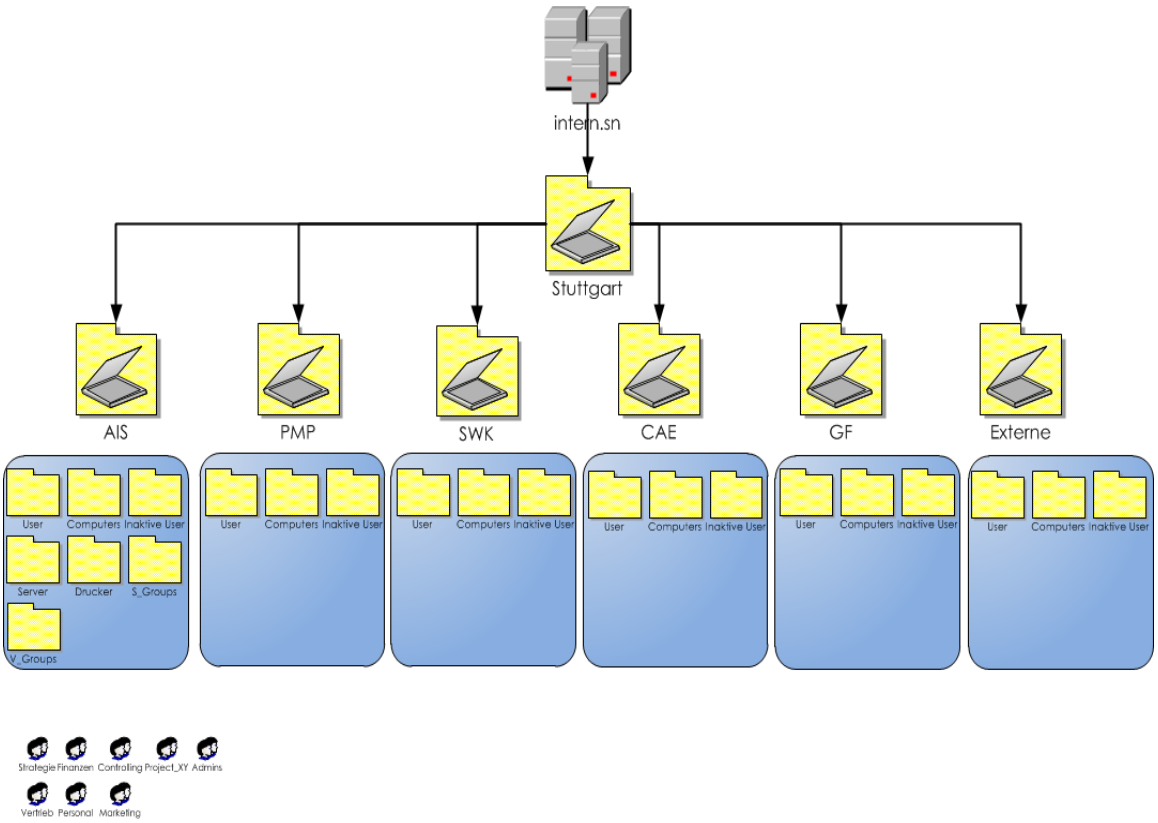
3.4.5 Domänen Konzept im Detail

Die Konzeption der Organisationseinheiten beruht auf der Firmenstruktur und bildet die einzelnen Abteilungen AIS (IT-Architektur und Infrastruktur), PMP (Projektmanagement und Prozesse), SWK (Softwareentwicklung und Konzeption), CAE (Computer Aided Engineering) und GF (Geschäftsführung) ab. Die einzelnen Organisationseinheiten beinhalten Container mit den Benutzern, die in dieser Abteilung angestellt sind. Die Infrastruktur OU hat als einzige eine Ausnahme, in dieser befinden sich weitere Container mit Druckern und Servern. Zusätzlich gibt es die Möglichkeit vorübergehend inaktive Mitarbeiter in den Container „inaktive User“ zu verschieben, sodass die zugehörigen Benutzeraccounts deaktiviert, aber nicht gelöscht werden.

Neben den Abteilungen existiert eine Organisationseinheit „Externe“, in der alle extern eingesetzen Mitarbeiter zu finden sind.

Um die Domänenstruktur möglichst flexibel und skalierbar zu gestalten, wurde eine übergeordnete Organisationseinheit mit dem Namen des jeweiligen Standorts, in diesem Fall Stuttgart, angelegt.

Die Domäne selbst heißt intern.sn.



3.4.6 Benutzerprofile

Bisher wurden serverseitig gespeicherte Profile verwendet, dies barg folgende Vor- und Nachteile.

Vorteile	Nachteile
Benutzerkomfort	Sehr langsame An- und Abmeldezyklen
Zentrale Ablage, die komplett gesichert wird	Hohe Netzlast
	Versionierungsprobleme bei Verwendung verschiedener Betriebssysteme
	Backup Datenoverhead durch nicht-geschäftsrelevante Dateien

Aufgrund dieser Nachteile fiel die Entscheidung zur Änderung der bisherigen Strategie.

Unter der neuen Windows Domäne werden alle Benutzerprofile lokal gespeichert und jedem Mitarbeiter ein Netzlaufwerk zur Sicherung seiner Daten zur Verfügung gestellt.

Dadurch erhöht sich die Performance, da nicht mit jeder An- und Abmeldung alle Daten komplett über das Netzwerk synchronisiert werden müssen.

Vorteile	Nachteile
Schnelle An- und Abmeldezyklen	Umstellung für Benutzer
Verringerter Datenoverhead beim Backup	Verlust lokaler Benutzereinstellungen bei Festplattencrash (Client)
Geringere Netzlast	Versionierungsprobleme bei Verwendung verschiedener Betriebssysteme
Übersichtliche und gleiche Dateistruktur auf jedem Betriebssystem	

Das Risiko „Verlust lokaler Benutzereinstellungen durch einen clientseitigen Festplattencrash“ ist statistisch gesehen eher gering, der letzte Komplett-Crash einer Festplatte im sidion Netzwerk ist auf das Jahr 2009 zu beziffern.

Außerdem wird jeder Mitarbeiter angehalten sensible, geschäftsrelevante und wichtige Daten grundsätzlich auf dem permanent bereitgestellten Netzlaufwerk zu sichern, sodass ein Festplattenausfall lediglich den Verlust der lokalen Benutzereinstellungen bedeuten würde.

Das neu bereitgestellte Netzlaufwerk verweist auf ein neu einzurichtendes Share auf dem Storage-Server gaia, auf das ausschließlich der Benutzer Vollzugriff besitzt und weitere Rechte granular anhand der Active Directory Nutzer und Gruppen vergeben kann.

Unter Windows erhält das Netzlaufwerk den einheitlichen Namen **P:**, unter Linux **sidionHome**, in beiden Fällen verweist es auf **\\gaia\daten\users\$USER .**

Um den Benutzern den Übergang zu erleichtern und eine schnelle Datenmigration zwischen den alten Benutzerprofilen und dem neuen Netzlaufwerk zu ermöglichen, werden alle alten Profilordner innerhalb des Linux-Profilordners in separaten Unterordnern zusammengefasst, wobei der Linux-Pfad als Netzlaufwerk eingebunden wird.

Hierfür wird für jedes verwendete Benutzerprofil ein Unterordner unterhalb des Linux-Home-Ordners wie folgt angelegt.

Von Windows XP Benutzerprofil **\\gaia\daten\home\samba\profiles\Max.Mustermann**
Nach Linux Unterordner **\\gaia\daten\users\$USER\WindowsXP**

Von Windows Vista Benutzerprofil **\\gaia\daten\home\samba\profiles\Max.Mustermann.V2**
Nach Linux Unterordner **\\gaia\daten\users\$USER\WindowsVista**

Von Windows 7 Benutzerprofil **\\gaia\daten\home\samba\profiles\Max.Mustermann.V3**
Nach Linux Unterordner **\\gaia\daten\users\$USER\Windows7**

Von Windows 7 Benutzerprofil **\\gaia\daten\home\Max.Mustermann**
Nach Linux Unterordner **\\gaia\daten\users\$USER\Linux**

Jeder Client ist, nach erfolgreicher AD-Integration, angehalten seine Daten zwischen altem Benutzerprofil und neuem Netzlaufwerk zu migrieren und zu pflegen, da diese nach maximal 45 Tagen deaktiviert und die Daten nach einem initialen Vollbackup gelöscht werden.

3.4.7 Domänen Beitritt

Durch die Umstellung auf einen Microsoft Active Directory ändert sich auch die Client-Einbindung in die AD. Im heterogenen sidion Netzwerk werden sowohl Windows (XP, Vista, 7) als auch Linux (Ubuntu 9.x, 10.x) Betriebssysteme verwendet.

Windows Clients werden standartmäßig in die Windows-Domäne eingebunden, es ist keine extra Software für den Domänenzutritt notwendig.

Linux Clients werden zukünftig über einen Samba-Client eingebunden, hierfür ist initial auf jedem Linux Client zusätzlicher Installations- und Konfigurationsaufwand zu betreiben. Für diesen Zweck wurde eine Anleitung im Systemhandbuch erstellt.

3.4.8 Rollen

Es existieren folgende Standard-Rollen:

Benutzer

Ist ein Standardbenutzer der keine Administrativen Rechte in der Domäne hat und keine Systemkritischen Einstellungen verändern kann.

Externe Benutzer (Laptop)

Die Externen Benutzer haben eine eigene Rolle mit eingeschränkten Rechten in der Domäne, desweiteren werden diese in eine Eigenständige Organisationseinheit ausgelagert.

Privilegierter Benutzer

Ist ein Benutzer mit erweiterten Rechten in der Domäne kann keine Systemkritischen Einstellungen ändern, dennoch hat er das Recht z.B. Software zu installieren bzw. deinstallieren

Administrator

Administratoren haben keinerlei Einschränkungen und können Systemkritische Einstellungen sowie alle Einstellungen an den Domänenrechnern vornehmen.

3.4.9 Gruppenrichtlinien

Gruppenrichtlinien sind Sammlungen von Benutzer- und Computerkonfigurationseinstellungen die mit den vorhandenen Organisationseinheiten (OU`s) der Active Directory verknüpft werden und die Benutzer bzw. Computerkonfiguration übernehmen.

Im konkreten werden die Systemeinstellungen für Benutzer deaktiviert, sowie die Netzlaufwerke beim Anmelden an die Domäne verbunden und eine entsprechende Verknüpfung auf dem Desktop angelegt.

Externe Benutzer haben eine eigene Organisationseinheit somit können diese in Bezug auf Rechte separat behandelt werden.

Es werden Gruppenrichtlinienvorlagen für die einzelnen Rollen der Active Directory angelegt und den entsprechenden Organisationseinheiten zugeteilt, alle Benutzer dieses Containers erhalten die Richtlinie nach der entsprechenden Vorlage.

Desweiteren werden initial bei der ersten Anmeldung an der Domäne die Standarddesktopverknüpfungen wie z.B. der Firefox, Alfresco Share Folder, Skype und die sidion Homepage auf dem Desktop angelegt. Zusätzlich wird der Internet Explorer mit sidion Firmeneinstellungen konfiguriert und der Desktop im Bezug auf Hintergrundbild und klassischer Ansicht angepasst.

3.4.10 Passwort Policy

Um eine hohe Sicherheit zu garantieren wurden zwei Kennwortrichtlinien erstellt, für Benutzer und privilegierte Benutzer mit administrativen Rechten.

Beide Kennwortrichtlinien haben folgende Gemeinsamkeiten.

Jedes Kennwort muss Zeichen aus drei der folgenden Kategorien enthalten.

- Großbuchstaben (A bis Z)
- Kleinbuchstaben (a bis z)
- Zahlen bis Basis 10 (0-9)
- Nicht alphabetische Zeichen aus dem ASCII Satz (z.B. !, $, #, %)
- Minimale Kennwortlänge: 10 Zeichen
- Maximale Kennwortlänge: unbeschränkt
- Kennwörter in umkehrbarer Verschlüsselung speichern: deaktiviert

Unterschiede finden sich im Kennwortalter wieder.

- Minimales Kennwortalter: Benutzer 0, Administratoren 0
- Maximales Kennwortalter: Benutzer 18 Monate, Administratoren 1 Monat
- Kennwortchronik: Benutzer 10, Administratoren 14

Aus Sicherheitsgründen wird ein Benutzerzugang bei fünf fehlerhaften Anmeldeversuchen gesperrt und muss vom Administrator wieder aktiviert werden, sodass ein Bruteforce-Angriff nicht möglich ist.

3.4.11 Benutzer Namenskonzept

Variante 1

Alle Benutzernamen im CAS-Umfeld setzen sich bisher aus **vorname.nachname** zusammen.
Hierbei ergeben sich folgende Vor- und Nachteile.

Vorteile	Nachteile
Benutzerkomfort	Transparenz als Sicherheitsrisiko Benutzername -> E-Mail-Adresse -> Profilordner
Klare Zuordnung	Probleme bei Namensänderungen
Einfache Administration	Probleme bei redundanten Namen

Variante 2

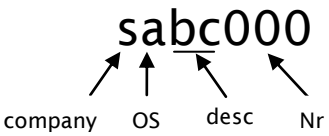
Eine praktikable Alternative stellt die Entkopplung des Benutzernamens vom eigentlichen Namen dar. Um trotzdem eine klare Zuordnung zu ermöglichen ist es notwendig ein einzigartiges, persönliches Merkmal in den Benutzernamen einfließen zu lassen. Besonders geeignet erscheint hier die Kombination mit der eindeutigen Personalnummer.

Der Benutzername setzt sich dann aus zwei zufällig gewählten Buchstaben sowie der Personalnummer zusammen, z.B. **pq9251**

Vorteile	Nachteile
Sicherheit	Benutzerkomfort leidet
Lösung des Problems der Namensänderung	Noch nicht abgeschätzter Zusatzaufwand
Lösung des Problems der redundanten Namen	Erschwerte Administration
	Automatisierte E-Mail-Adressvergabe nicht ohne weiteres möglich

3.4.12 Server Namenskonzept

Es wurde folgendes Server-Namenskonzept ausgearbeitet und verabschiedet. Anhand diesem Konzepts werden alle neuen Server benannt, die bestehenden Server werden nicht umbenannt.



Beispiele hierfür sind.

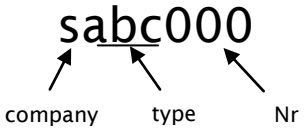
Servername	Beschreibung
smdc001	sidion Microsoft Domain Controller (Primary)
slwr001	sidion Linux Webserver (Primary)
mwdc001	Mercedes Domain Controller (Primary)

Daraus ergeben sich folgende Servernamen.

Servername	Beschreibung
smdc001	sidion Microsoft Domain Controller (Primary)
smdc002	sidion Microsoft Domain Controller (Secondary)
smmx001	sidion Microsoft Mail Exchange (Primary)
smow001	sidion Microsoft Online Web Access (OWA)
smav001	sidion Microsoft AntiVir (Security Server)

3.4.13 Client Namenskonzept

Das Client-Namenskonzept orientiert sich stark am Server-Namenskonzept und innerhalb des Projektes umgesetzt.



Im Rahmen des Projekts müssen alle Desktops und Notebooks erfasst und neu benannt werden.

Beispiele hierfür sind.

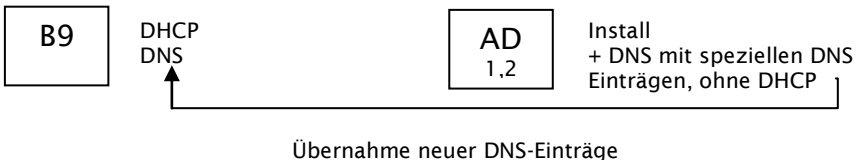
Servername	Beschreibung
sdsk001	sidion Desktop
snb001	sidion Laptop

3.4.14 Komponenten: DNS, DHCP

Der DNS und DHCP Service bleibt auf den bestehenden Servern, es ist lediglich notwendig auf dem Domain Controller alle Windows relevanten DNS-Einträge vorzunehmen, sodass die Namensauflösung gegeben ist.

Diese DNS Einträge werden anschließend in den bestehenden DNS Server übernommen.

Das Vorgehen wird in folgender Abbildung nochmals grafisch dargestellt, der bestehende Diensteserver wurde als B9 gekennzeichnet.



Folgende DNS-IP-Zuordnungen sind notwendig,

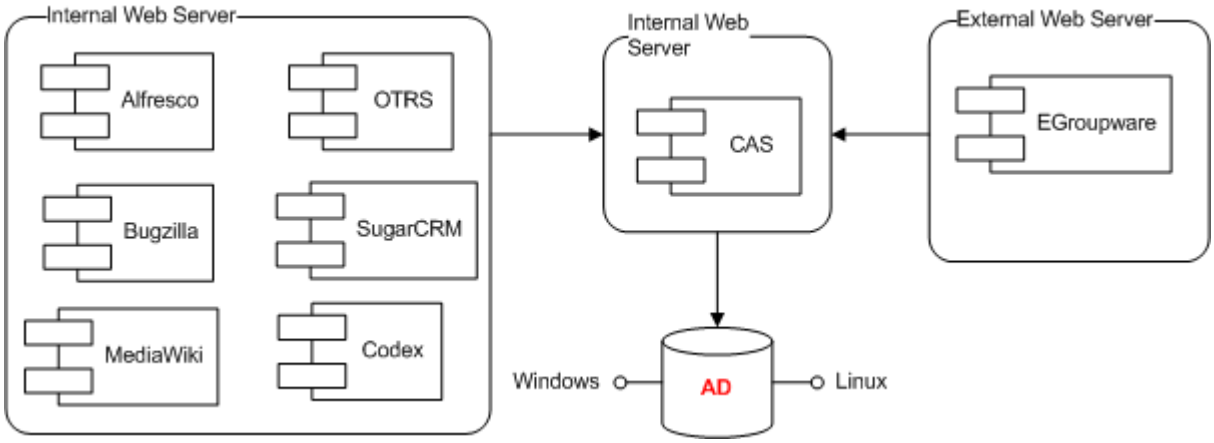
DNS Eintrag	IP-Adresse
smdc001	10.15.31.210
smdc002	10.15.31.220
smmx001	192.168.0.211
smav001	192.168.0.221

3.4.15 Single Sign On Integration: CAS Server

Um die bestehende Single Sign On Lösung weiterhin zu nutzen, muss der CAS-Server geändert werden, sodass dieser zukünftig die Windows AD anstelle des LDAP-Verzeichnisses nutzt. Alle „CASified Services“, die sich direkt über den CAS-Server authentifizieren, müssen daraufhin nicht angepasst werden, sondern funktionieren übergangslos über die Windows AD.

Der CAS-Server muss hierfür auf die Version 3.4.6 aktualisiert werden, wie aus einem Test hervorgegangen ist, ist der für das Upgrade benötigte Aufwand gleichzusetzen mit einer Neuinstallation und Neukonfiguration des CAS-Servers.

Aus diesem Grund wird in diesem Projekt ein neuer CAS-Server installiert und konfiguriert, eine detaillierte Installationsanleitung finden Sie im Dokument

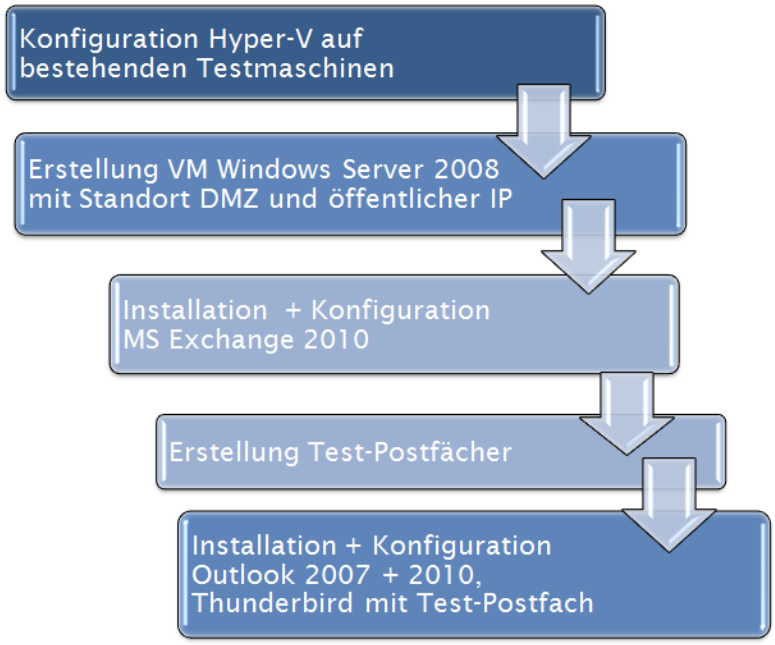


3.5 Wissenserwerb Microsoft Exchange

Analog zur AD-Spielwiese wurde auch eine EX-Spielwiese eingerichtet, um Wissen und Erfahrung anzueignen und zu erproben. Hierbei stellte die Konfiguration der Microsoft Virtualisierungslösung Hyper-V die größte Hürde dar, da dieser Hypervisor im Gegensatz zu gängigen Produkten wie VMWare oder XEN noch wenig verbreitet ist und das Wissen erst aufgebaut werden musste.

Im Anschluss wurde eine virtuelle Windows Maschine aufgesetzt und auf dieser der MS Exchange Server 2010 installiert und konfiguriert. Es folgte die Erstellung von Test-Postfächern und der Test mit den E-Mail-Clients MS Outlook 2007 und MS Outlook 2010.

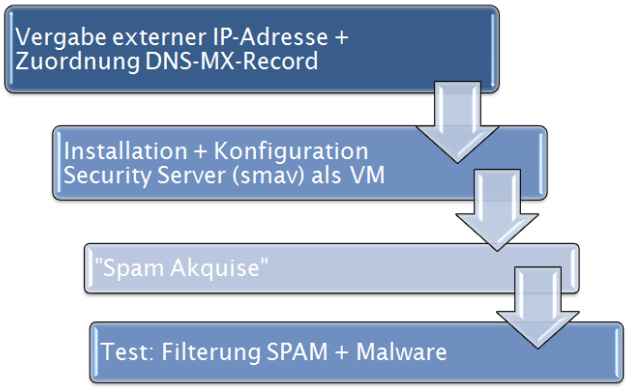
Anhand dieser Erkenntnisse wurden bereits erste Anleitungen geschrieben, die im Anwenderhandbuch zu finden sind.



Im Anschluss wurde die Konzeption des Microsoft Exchange Servers vorgenommen und das Produkt zur Gewährleistung der E-Mail-Sicherheit gewählt, näheres finden Sie im Abschnitt 3.6.5 .

Es folgte ein Security-Test, um das Avira Business Bundle zum Schutz vor SPAM und Malware zu testen. Hierbei wurde der Test-Server mit einer externen IP-Adresse und Domäne konfiguriert und SPAM Akquise betrieben, also die eingerichteten Postfächer im Internet bekannt gegeben, sodass eine Masse von SPAM und Malware eintritt. Der Test wurde insgesamt 2 Woche ausgeführt.

Zuvor wurde der Avira Business Bundle Server, genannt smav001, mit Schutz für den Exchange Server auf einer separaten VM installiert und entsprechend konfiguriert, das erlangte Wissen floss in das Installationshandbuch ein. Bei diesem Test wurden nahezu 100% der unerwünschten Mails gefiltert, sodass die gewählte Sicherheitslösung als sicher gelten kann und unseren Anforderungen in Sachen E-Mail- und Client-Schutz als erfüllt angesehen werden.



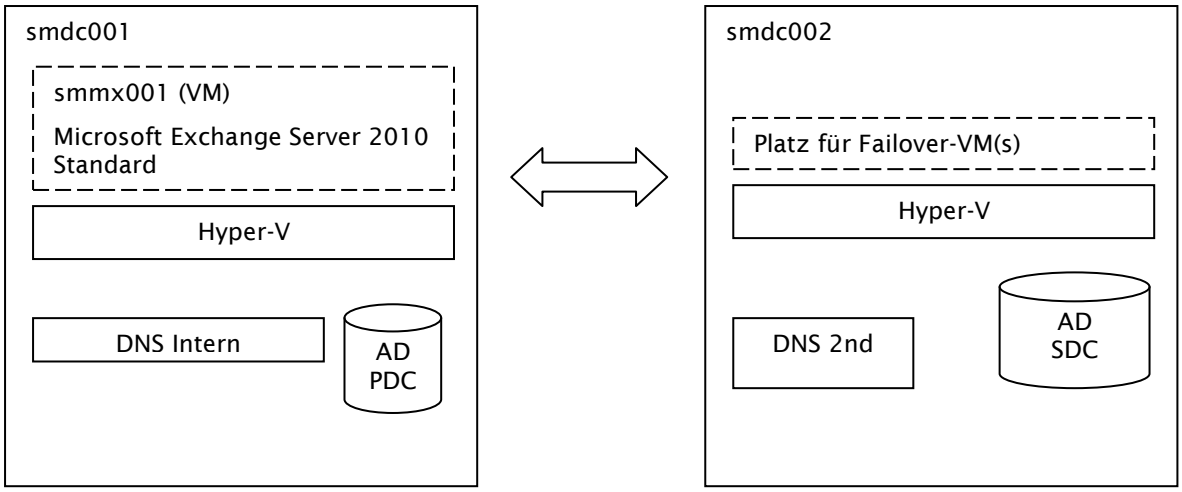
3.6 Konzeption Microsoft Exchange

Nach erfolgreichem Abschluss des Teilprojekts AD existieren zwei physische Server, genannt smdc001 und smdc002. Beide Server sind physisch im sidion LAN beheimatet. Unter Verwendung der Virtualisierungslösung Hyper-V wird auf einem der beiden Server ein logischer Server (VM) virtualisiert, genannt smmx001.

Als Betriebssystem dient Windows 2008 Server, außerdem befindet sich auf diesem Server der Microsoft Exchange Server, welcher den zentralen Mailserver darstellt.

Dieser VM wird ein festes Ethernet-Interface zugeordnet, welches über VLAN in die DMZ gepatched ist. Somit befindet sich der smmx001 Server innerhalb der DMZ und ist dadurch sowohl intern als auch extern erreichbar.

Da beide Server Hyper-V beherrschen ist es möglich den Exchange Server, genannt smmx001, zwischen den beiden Servern zu verschieben (Hochverfügbarkeit). Außerdem existiert über ein Mailrelay über einen externen Internetprovider, welches bei Ausfall der DMZ alle ankommenden E-Mails zwischenspeichert (Caching) und diese zu einem späteren Zeitpunkt zustellt.



Die notwendigen Konfigurationsparameter sowie Softwarepakete sind in nachfolgender Tabelle festgehalten.

Host	**IP-Addresse**	**Subnetmaske**	**Beschreibung**
smmx	192.168.0.211	255.255.255.0, /24	Virtual Machine (Xen basiert) CPU: 2 Virtuelle Prozessoren RAM: 4096 MB Explizit HDD: 1000 GB NIC: 2 Virtuelle LAN Karten
DNS-Record(s)		**Betriebssystem**	**Software / Dienste**
smmx		Microsoft Server 2008	Microsoft Exchange Server 2010
Host	**IP-Addresse**	**Subnetmaske**	**Beschreibung**
smav	192.168.0.221	255.255.255.0, /24	Virtual Machine (Xen basiert) CPU: 4 Virtuelle Prozessoren RAM: 8192 MB Explizit HDD: 250 GB NIC: 2 Virtuelle LAN Karten
DNS-Record(s)		**Betriebssystem**	**Software / Dienste**
smav		Microsoft Server 2008	Avira Business Bundle

3.6.1 Mails und Mailboxen

Jeder Mitarbeiter erhält einen User-Account im Active Directory und jeder Active Directory User eine Mailbox und Vollzugriff auf diese. Die Mailboxgrößte ist auf 1 GB limitiert und jeder Mitarbeiter ist angehalten, seine E-Mails regelmäßig zu Archivieren und an einem dafür vorgesehenen Speicherplatz auf dem Fileserver abzulegen.

Die E-Mail-Versandgröße ist auf 100MB reglementiert worden. Alle vorhandenen Daten, wie in der Ausgangslage beschrieben, werden migriert.

Genauere Informationen zur Migration finden Sie im Abschnitt Migration.

3.6.2 Ressourcen

Die Ressourcen werden migriert und sind für alle Exchange Benutzer verwendbar, eine detaillierte Anleitung findet sich im Anwenderhandbuch im Anhang.

3.6.3 Password Policy

Ein E-Mail-Postfach ist nur in Verbindung mit einem Active Directory User-Account verfügbar, somit gilt die AD Passwort Policy aus Kapitel 3.4.10.

3.6.4 Clients

Es existieren etwa 100 Postfächer, wobei rund 75 Postfächer als echte E-Mail-Clients zu berücksichtigen sind. Die restlichen sind Sammelpostfächer, wie etwa bewerbung@sidion.de.

Die E-Mail-Adressen werden komplett migriert und es gilt das AD Namenskonzept, die nachfolgenden E-Mail-Clients werden unterstützt.

Windows Desktop

Jeder Mitarbeiter besitzt ein Microsoft Office 2007/2010 Paket, in dem der Microsoft Outlook Client 2007/2010 vorhanden ist, weitere Lizenzen müssen daher nicht bestellt werden.

Mit diesem Client wird die bestmögliche Funktionalität in Verbindung mit dem Exchange Server erreicht, er gilt daher als Standard E-Mail-Client für Microsoft-Benutzer.

Für das Anwenderhandbuch wurden umfangreiche Anleitungen zum Umgang mit dem Microsoft Outlook Client zu folgenden Themen erstellt, um den Mitarbeitern einen leichten Einstieg zu ermöglichen.

- Client Einrichtung
- Signaturen
- (Gruppen)-Kalender
- Archivierung
- Ressourcen
- Offline Zugriff

Linux Desktop

Im sidion Netzwerk existieren 5 Linux-Clients, diese können mit dem Outlook Web Access, kurz OWA, arbeiten. Für den einfachen E-Mail-Abruf und Versand wird der Freeware E-Mail-Client Mozilla Thunderbird neuester Version installiert. Eine Anleitung findet sich im Anwenderhandbuch.

iPhone OS Smartphone

Der hausinterne Exchange Server wird über die im iPhone integrierte ActiveSync Komponente angebunden. Das Postfach, die Kontakte sowie die Kalendar Funktionen sind mobil erreichbar. Weitere Informationen zur Einrichtung des ActiveSync Accounts auf dem iPhone befinden sich im Anwenderhandbuch.

Android OS Smartphone

Die Verbindung mit dem Exchange Server lässt sich mit dem Andriod 2.2 Betriebssystem ohne zusatzliche App einrichten. Es sind alle Exchange Grundfunktionen Mail, Kalendar und Kontakte mobil erreichbar. Informationen zur Einrichtung der Exchange Verbindung befinden sich im Anwenderhandbuch.

Symbian OS Smartphone

Smartphones mit dem Betriebssystem Symbian OS können über die kostenlose Nokia-Anwendung Mail for Exchange E-Mails abrufen, schreiben sowie Besprechungen koordinieren. Eine Synchronisierung zwischen Exchange Kalender und Smartphone ist möglich.

Es existiert eine Anleitung im Anwenderhandbuch.

Webzugang

Microsoft Exchange Server bietet mit Outlook Web Access (OWA) eine komfortable Webschnittstelle, um mit dem Internet Explorer auf die komplette E-Mail-Funktionalität zugreifen zu können.

Hierfür eignet sich jeder gängige Browser, das volle Funktionsspektrum ist jedoch nur mit dem Internet Explorer verfügbar.

3.6.5 Spam, Malware

Aus dem Fachkonzept lassen sich folgende Anforderungen für den Schutz vor Spam und Malware definieren.

- Sicherer Schutz vor Spam, Malware auf dem Exchange-Server („Ex Protect“)
- Sicherer Schutz vor Malware auf den Clients („Client Protect“)
- Zentrale Verwaltung

Zur Erfüllung der Anforderungen wurden mehrere Lösungsstrategien evaluiert und miteinander verglichen, anhand einer Entscheidungsmatrix wurde anschließend eine Lösungsstrategie gewählt.

Lösungsstrategie 1: Microsoft Forefront Security

Verwendung der Microsoft Bordmittel und der zusätzlichen Sicherheitsanwendung Microsoft Forefront. Dieses Produkt ist relativ günstig, dafür aber noch wenig verbreitet und es gibt wenige Informations- und Referenzquellen.

Anforderung	Produkt	Kosten für 100 User/p.a
Ex Protect	MS Forefront Protection 2010 for Exchange	€: 1075,00 / $: 1500,00
Client Protect	MS Forefront Endpoint Protection 2010	€: 733,00 / $: 1020,00
Gesamt		€: 1808,00

Lösungsstrategie 2: Barracuda Virtual Appliance + Avira oder Endpoint Protection 2010

Barracuda Networks bietet eine Spam & Virus Firewall Lösung als Virtual Appliance (Vx), relevant wäre hier das Produkt BSF 300Vx, welches Schutz für bis zu 1000 aktive E-Mail-Nutzer bietet.

Das Lizenzierungsmodell richtet sich nicht nach der Anzahl der User, sondern stellt einen einmaligen Festpreis dar. Diese Lösung bietet keinen lokalen Virenschutz auf den Windows Servern und ist nur langfristig rentabel

Anforderung	Produkt	Kosten für 100 User
Ex Protect	Barracuda Spam & Virus Firewall 300	€: 2149,00 Einmalig €: 749,00 Jährliche Updates €: 499,00 24/7 Support+Service
Client Protect	MS Forefront Endpoint Protection 2010	€: 733,00 / $: 1020,00
Gesamt Barracuda		€: 3397,00 im 1.Jahr €: 1248,00 Jedes weitere

Lösungsstrategie 3: Avira SmallBusiness Suite

Die Avira SmallBusiness Suite bietet für kleine bis mittelständische Unternehmen mit bis zu **100** Rechnern eine Komplettlösung der Anforderungen. Die SmallBusiness Suite enthält:

- AntiVir Professional (Windows)
- AntiVir Server
- AntiVir Exchange + AntiSpam
- Security Management Center für Windows Server (zentrale Verwaltung)

Anforderung	Produkt	Kosten für 100 User
Ex Protect Client Protect	Avira SmallBusiness Suite	€: 3810,00
Gesamt Avira SmallBusiness Suite		€: 3810,00

Lösungsstrategie 4: Avira Business Bundle

Das Avira Business Bundle stellt die Erweiterung der Small Business Suite dar und deckt denselben Funktionsumfang, allerdings für mehr als 100 Rechner, ab.

Anforderung	Produkt	Kosten für 100 User
Ex Protect Client Protect	Avira Business Bundle	€:3810,00
Gesamt Avira Business Bundle		€:3810,00

Entscheidungsmatrix

Lösungsstrategie	Vorteile	Nachteile
1 – MS Forefront	▪ Hohe Kompatibilität ▪ Kosten	- Keine Erfahrung - Lizenzmodell mit CALs etc. - Postfach CALs
2 – Barracuda + AV Extra	▪ out of the box Lösung	- separate Client Protection - Kosten erst langfristig rentable - kein deutscher Support?
3 – Avira SmallBusiness	▪ Komplettlösung ▪ Wenig Umstellungsaufwand Clients ▪ Skalierbarkeit ▪ Einfache Umstellung auf Business Bundle ab 100 Clients+ 30% Produktersparnis Clients	- Kosten Wobei: Aktuelle Lösung kostet 1970,00€ ohne zentrale Verwaltung
4 – Avira Business Bundle	▪ Wie Small Business, aber keine Obergrenze	

Trotz höherer Kosten entscheiden wir uns aufgrund der Skalierbarkeit und des breiten Funktionsspektrum für das Avira Business Bundle, also Lösungsstrategie 4.

3.7 Migration

Als Migrationstool wird die von Microsoft empfohlene Transport Suite eingesetzt. Diese hat allerdings die Einschränkung, dass es nur von Lotus Notes Domino Server auf Microsoft Exchange 2007 migrieren kann, da allerdings Microsoft Exchange 2010 in der Produktivumgebung eingesetzt werden soll, muss die Migration in zwei Schritten erfolgen.

Erster Migrationsschritt:

Ein Microsoft Exchange Server 2007 wird temporär als eine virtuelle Maschine auf dem Hyper-V Hypervisor installiert. Als Grundlage muss zwingend ein Microsoft 2008 Server ohne R2 verwendet werden.

Vor der Installation des Exchange Servers 2007 sind einige Punkte zu beachten:

- IIS Serverfunktionalität muss nachträglich installiert werden, dazu noch
- ASP.NET
- ISAPI Extensions
- ISAPI Filters
- Server Side Includes
- .NET Extensibility
- Basic Authentication
- Windows Authentication
- Digest Authentication
- Dynamic Content Compression
- IIS 6 Management Compatibility
- IIS 6 Metabase Compatibility
- IIS 6 WMI Compatibility
- IIS 6 Scripting Tools
- IIS 6 Management Console

Es sollte geprüft werden, ob der Service Pack 2 für Exchange 2007 Server installiert ist, wenn dies nicht der Fall ist wird von Microsoft empfohlen dieses nachträglich zu installieren, bevor man die Daten migriert.

Die Transport Suite erfordert des Weiteren die neueste Version von .NET sowie Powershell und Lotus Notes Software (empfohlen: Einzelplatzinstallation) auf dem Client bzw. Server der zur Migration verwendet wird.

Die Migration läuft mit den vorhandenen Daten (ca. 12GB) 12-14 Stunden und kann somit über Nacht bzw. am Wochenende durchlaufen.

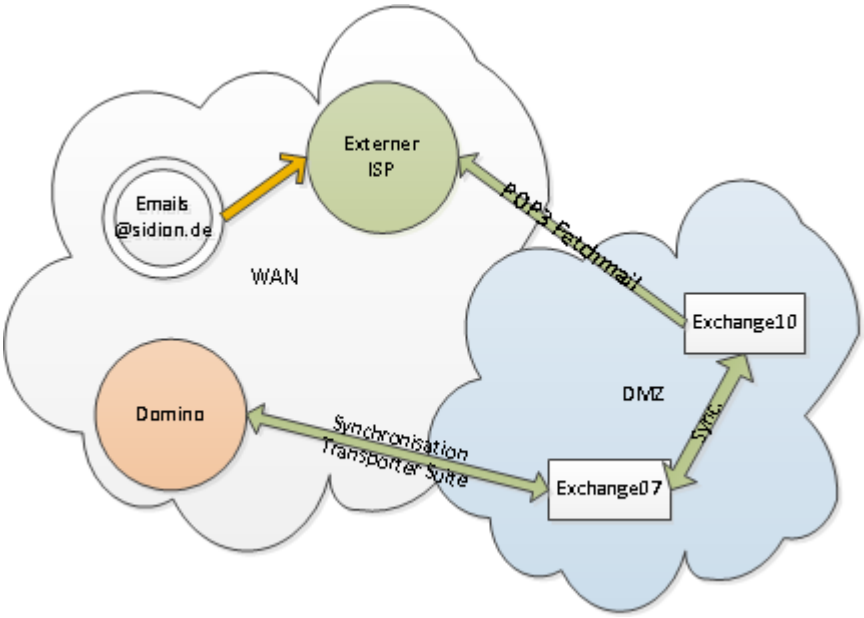
Zweiter Migrationsschritt:

Die Daten sind nun in die Exchange Organisation migriert und müssen vom Exchange 2007 zu Exchange 2010 migriert werden. Dazu wird der Exchange Server 2010 installiert und in die gleiche Exchange Organisation wie der Exchange Server 2007 aufgenommen.

Die Postfach- und Benutzerdaten sind nun auch vom Exchange Server 2010 einzusehen. Da diese allerdings nach wie vor auf dem Exchange Server 2007 liegen müssen folgende Schritte durchgeführt werden:

- Verschieben des Exchange 2010 Datenbankpfads
- Verschieben der Öffentliche Ordner-Datenbank
- Hinzufügen des Exchange 2010 Sendeconnectors
- Anlegen eines neuen Empfangconnectors
- Replikat des Öffentlichen Ordners erstellen und hinzufügen
- Pfad für neuen Öffentlichen-Ordner-Speicher auf postfach-Datebank von Exchange 2010 ändern
- Verschieben des Offline-Adressbuchs
- Verschieben der Postfächer mit „online-mailbox-move“

Die Serverumgebung sieht nun wie folgt aus:

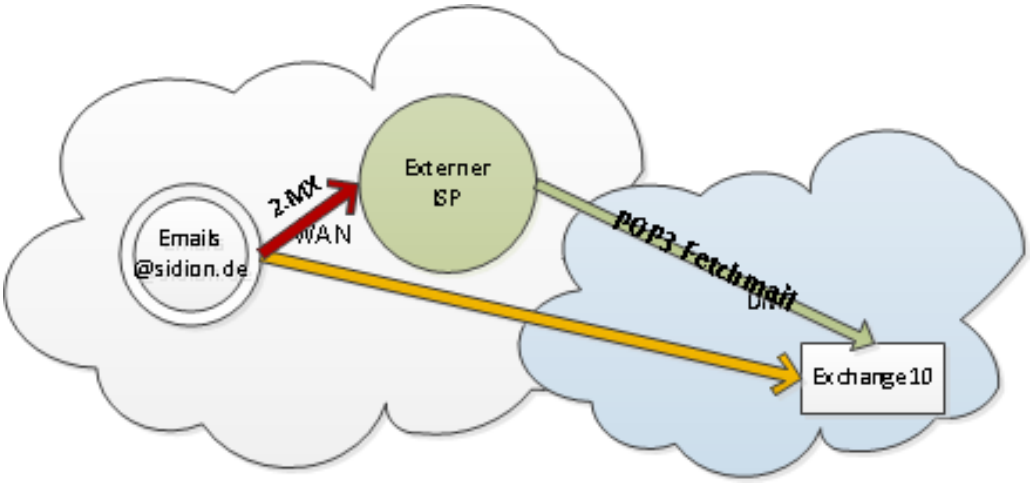


Cleanup:

Zum Abschluss ist es notwendig die Exchange Organisation zu bereinigen. Dafür geht man wie folgt vor.

- Webseite des alten Servers für die Offline-Adressbuch Verteilung entfernen
- Entfernen des alten Exchange 2007 Sendeconnectors
- Replikate der alten Datenbank aus den öffentlichen Ordnern entfernen
- Deinstallation Exchange Server 2007

Nach dem Cleanup ist die Serverstruktur in Ihrem Produktivzustand, dieser sieht wie folgt aus:

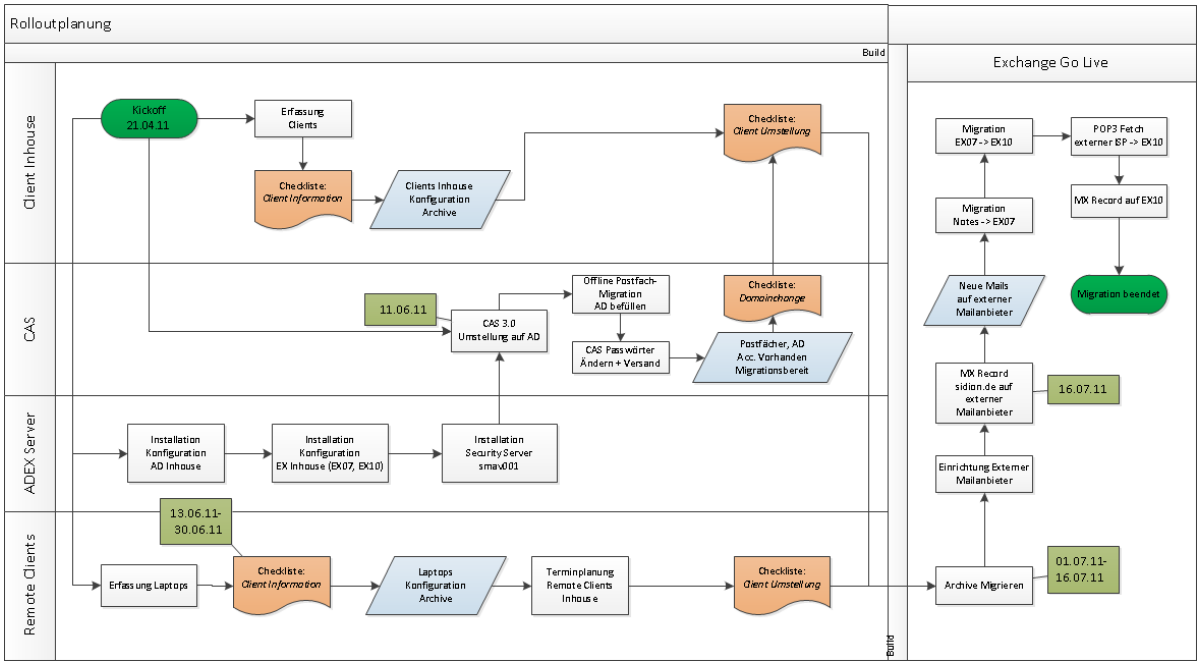


E-Mails, die an @sidion.de gehen, werden durch den primären MX-Record auf den hausinternen Exchange Server 2010 weitergeleitet. Ist dieser aus Störungsgründen nicht erreichbar, wird als Backuplösung ein externer ISP als Ausfalllösung verwendet. Dabei zeigt der sekundäre MX-Record auf den Externen ISP, der im Störungsfall die eingehenden Emails empfängt und zwischenspeichert, bis die Störung behoben ist. Danach werden die eingegangenen E-Mails vom hauseigenen Exchange Server 2010 per Fetchmail abgeholt.

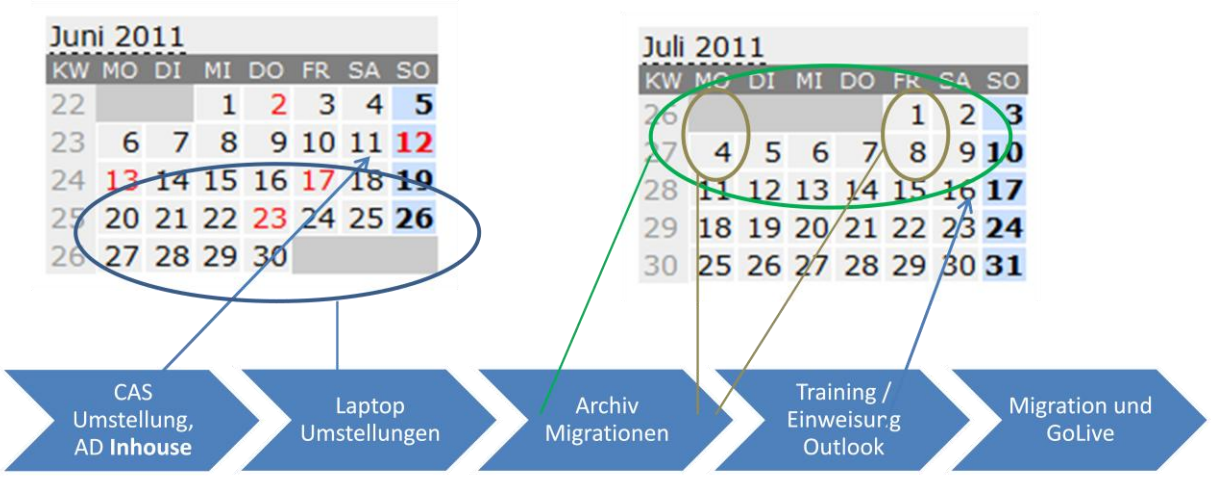
3.8 Rollout

Neben einem sehr detaillierten Implementierungsplan wurde eine detaillierte Rolloutplanung erstellt. Den Implementierungsplan finden Sie im Anhang unter XEN ADEX_Implementierungsplan.mpp.

Die Rolloutplanung berücksichtigt die für den gezielten Rollout notwendigen Arbeitspakete und findet sich in nachfolgender Abbildung.



Die dargestellt Rolloutstrategie wurde in nachfolgender Abbildung nochmals visuell und termingetreu visualisiert. Wie in der Rolloutplanung wurden auch hier Verweise auf zuvor erstellte Checklisten gesetzt. An den einzelnen Tagen werden die darunter aufgeführten Arbeitspakete sowie Checklisten abgearbeitet, um eine problemlose und vollständige Migration zu gewährleisten.



11.6.2011
1. Inhouse PCs vorberei.
2. Checkliste
   - *Client Information*
3. AD befüllen
4. CAS-Server Upgrade
5. AD + CAS LIVE
6. Inh. PCs Aufnahme
7. .Checklisten
   - *Client Umstellung*
   - *Domainchange für Server* (CAS,AD, Drittsyst.)
8. CAS PWs Versand

13.-30.6.2011
1. Laptops vorbereiten
2. Checkliste
   - *Client Information*
3. Laptops reinholen mit Terminvereinb.
4. Laptop AD Aufn.
5. Checkliste
   - *Client Umstellung*

1.-16.7.2011:
1. Archive migrieren
2. Stopp der Notes Archivierung

27.6 – 8.7
1. Einladungen zur User-Schulung
2. 4 Schulungstage a 2 Stunden, siehe Doku

16.7.2011
1. Migration Notes-Daten
2. Umstellung MX-Record
3. Checkliste
   - *Migrationsplan*
4. Info an SystAG „Abschalten!“

3.9 Backup & Restore

Als Backuplösung wird eine Erweiterung für die bereits vor Projektbeginn bestehende und firmenintern etablierte Software bacula eingesetzt. Diese Erweiterung erlaubt ein inkrementelles und automatisiertes Online-Backup, das täglich um 1:00 Uhr nachts ausgeführt wird.

Zur zusätzlichen Sicherung der Exchange Datenbanken wird ein Backup über den von Exchange Version 2010 vorhandene Dienst VSS (Volume Shadow Service) vorgenommen. Dieser Dienst legt eine Schattenkopie des Laufwerks an auf dem sich die Exchange Database befindet. Aus diesem Grund ist es empfehlenswert ein eigenes Volume für die Exchange Maildatabase und die Transaktionslogs anzulegen.

Die Schattenkopie lässt sich mit einem Snapshot oder Image eines Volumes zu einem bestimmten Zeitpunkt vergleichen.

Diese Schattenkopien liegen Lokal auf dem Storage des Exchange Servers und sind somit im Falle von Mailverlust von Usern oder anderen Inkonsistenz der Exchange Datenbank schnell erreichbar und können durch den Administrator wiederhergestellt werden.

Der Backup- und Restore-Prozess wurde umfangreich getestet, näheres hierzu finden Sie im angehängten Testplan (Verweis siehe 4.1 Testing), dort im Reiter Exchange Tests ab Zeile 70 folgend.

3.10 Drittsysteme

Durch die Änderung der Domäne und der Domänenstruktur müssen Änderungen an bestehenden Drittsystemen vorgenommen werden.

Die vorzunehmenden Änderungen werden in die Bereiche **config** und **content** eingeordnet und im Dokument **sidion_AIS_XENADEX_Rollout_Planung** detailliert erklärt.

4. Dokumentation

4.1 Testing

Ein detailliertes Testingkonzept wurde vor Projektbeginn von Ulrich Ritter erstellt. Es wurde für *alle* funktionalen und nicht-funktionalen Anforderungen ein Test-Case geschrieben, der nach Abschluss der jeweiligen Systembausteine durchgeführt wurde.

Die Testergebnisse finden Sie im Dokument XENADEX_Testplan.xlsx.

4.2 Installationshandbuch

Das Installationshandbuch umfasst die komplette Dokumentation der Installation. Es beschreibt Schritt-für-Schritt, wie die Systeme anhand der Konzeption installiert und konfiguriert wurden.

Sie finden es im Dokument XENADEX_Installationshandbuch.docx.

4.3 Anwenderhandbuch

Um den Anwendern eine einfache Eingewöhnung in die neue E-Mail-Lösung zu ermöglichen, wurde eine Reihe von Standard-Funktionen detailliert in Form des Anwenderbuchs erklärt.

Sie finden es im Dokument XENADEX_Anwenderhandbuch.docx.

4.4 Administrationshandbuch

Neben dem Installationshandbuch wurden die wichtigsten Funktionen im Umgang mit der neuen Systemlandschaft für die sidion Administratoren dokumentiert.

Sie finden es im Dokument XENADEX_Administrationshandbuch.docx.

5. Anhang

5.1 User Training

Um den Benutzern einen leichten Einstieg in die neue E-Mail-Architektur zu ermöglichen, wird ein firmeninterner Workshop an 4 Terminen angeboten.

Grober Termin: Montag, Freitag in KW 26 und KW 27
Geplante Dauer: ~ 1,5 Stunden

Es wird folgender grober Umfang behandelt.

Look & Feel Microsoft Outlook 2007 und 2010

- E-Mails: Versenden, Versenden an Verteileradresse, Zurückziehen
- Kontakte: Lokale Kontakte pflegen, Globale Kontakte verwenden
- Kalender: Termine planen, Personen zu Terminen einladen, Termine absagen
- Ressourcen: Reservieren, Absagen
- Signaturen: Anlegen und Ändern
- Archivierung: Archiv erstellen und im Netzlaufwerk ablegen

Das User Training wird von Ulrich Ritter und Kay Urbach geleitet, hierbei werden abwechselnd über einen Beamer Funktionen präsentiert und die Schulungsteilnehmer können selbst an Schulungsrechnern/Laptops erste Erfahrungen sammeln.

Für die Schulung werden folgende Ressourcen benötigt:

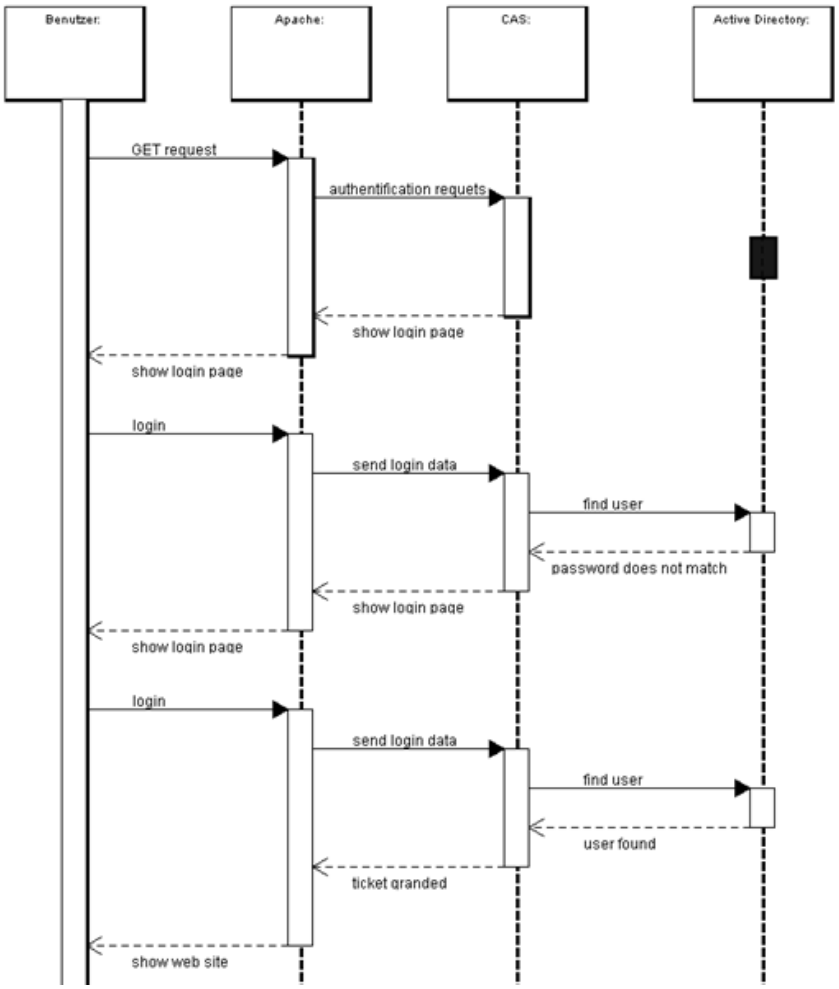
- Raum für mind. 10 Teilnehmer
- 5 Trainingsrechner: Windows XP/Vista/7, Outlook 2007, Outlook 2010, jeweils mit komplett konfigurierten Schulungspostfächern
- Beamer
- Präsentationslaptop: Windows, Outlook 2007, Outlook 2010

Außerdem soll jeder User nochmal den Hinweis erhalten, dass ein Anwenderhandbuch bereitgestellt wurde, welches im sidion Wiki zu finden ist.

Für eine genaue Ausgestaltung des User Trainings sind die Leiter zuständig.

5.2 Abbildungen

5.2.1 Sequenzdiagramm CAS-Anmeldung



5.3 Quellenverzeichnis

Umfangreiche Anleitungen finden Sie unter http://www.msxfaq.de/.

5.4 Glossar

Begriff	Bedeutung	Erklärung
.NET		Entwicklungsplattform für Microsoft-nahe Programmiersprachen wie C# oder ASP
AD	Active Directory	Verzeichnisdienst zur Benutzerkontenverwaltung
ASP	Active Server Pages	Internetbasierte Programmiersprache
B9	Bind9	Opensource DNS-Service
CAS	Central Authentification Service	SSO-Produkt
Codex		Buchverwaltungssoftware, bei sidion entwickelt
DHCP	Dynamic Host Configuration Protocol	Protokoll/Dienst zur automatischen IP-Vergabe
DMZ	Demilitarisierte Zone	Netzwerkbereich als "Pufferzone", spätestens hier werden Gefahren gefiltert
DNS	Domain Name Server	Protokoll/Dienst zur Zuordnung von IP-Adressen zu Domain-Namen
ECTS	European Credit Transfer System	*Versuch* einen europäisch einheitlichen Leistungsvergleich unter Studenten zu ermöglichen
HTTP	Hypertext Transfer Protocol	Gängiges Protokoll zur Anzeige von Internetseiten
HTTPS	Hypertext Transfer Protocol Secure	Mit SSL gesichertes http-Protokoll
HyperV		Virtualisierungslösung von Microsoft
IIS	Internet Information Service	Webserver von Microsoft, ähnlich Apache
IMAP	Internet Message-Access Protocol	Eingangsprotokoll für E-Mail-Empfang
ISAPI	Internet Server Application Programming Interface	Werkzeug zur Veröffentlichung von Webseiten auf dem IIS-Webserver
ISP	Internet Service Provider	Internetanbieter
LDAP	Lightweight Directory Access Protocol	Verzeichnisdienst für Windows und Linux Infrastrukturen
MS	Microsoft	Eine kleine Firma in den USA
MX-Record		Mailexchange DNS-Eintrag
OTRS	Open Ticket Request System	Quelloffenes TroubleTicketSystem
OWA	Online Web Access	Per Webbrowser erreichbarer E-Mail-Dienst
PHP	Personal Homepage	Internetbasierte Programmiersprache
POP3	Post Office Protocol	Eingangsprotokoll für den E-Mail-Empfang
SSO	Single Sign On	Ermöglicht nach einmaliger Anmeldung die Nutzung aller im Trusted Verbund befindlicher Anwendungen, ohne zusätzliche Anwendung
SugarCRM		Costumer Relationship Management Softwareprodukt, d.h. Software zur Verwaltung von Kunden
VSS	Volume Shadow Service	Dienst für Schattenkopien im Microsoft Exchange Server
WMI	Windows Management Instrumentation	Programm zur Verwaltung von Microsoft Computern
XEN		Virtualisierungslösung