

Inhalt

Teil 1	3
Aufgabenstellung.....	3
ANFORDERUNGEN.....	3
Ausgangslage	3
Evaluation	3
Abnahme der Evaluation	3
Use Case	3
Usability	3
Performance	4
Datensicherheit	4
Betrieb und Nachhaltigkeit.....	4
Quantitative Anforderungen	4
Server	4
Versionsverwaltung.....	4
Userdokumentation	4
Vorkenntnisse.....	5
Vorarbeiten	5
Firmenstandards.....	5
Projektorganisation	6
Zeitplan.....	7
Arbeitsjournal.....	8
Teil 2	18
Management Summary.....	18
Ausgangssituation	18
Umsetzung.....	18
Erwartetes Ergebnis	18
Analysieren	19
Evaluation	19
Eigene Empfehlung.....	21
Ausgewählte Software	21
Planen	22
Konzept.....	22
Meilenstein 1.....	23

Realisieren	24
Installation	24
Konfigurieren	29
Meilenstein 2	40
Benutzerdokumentation	41
Testen	44
Funktionen	44
Performance	46
Fazit	47
Meilenstein 3	47
Abgabe	48
Meilenstein 4	48
Schlusswort	48
Abkürzungen / Fachbegriffe	49
Anhang	50
E-Mail Text	50
Konfigurationsfiles	51
Filesender	51
SimpleSAMLphp	74
PHP5	96
Apache2	138

Teil 1

Aufgabenstellung

ANFORDERUNGEN

Aufgabe der IPA ist es das Pflichtenheft des Auftraggebers (Gruppenleiter IT-Betrieb) welches mit der folgenden Aufgabenstellung kompatibel ist, zu erfüllen.

Der neue Web-Dienst soll am Ende der IPA unseren Kunden zur Verfügung stehen und unser Dienstleistungsportfolio erweitern.

Ausgangslage

Die Zürcher Hochschule der Künste (ZHdK) mit rund 2500 Studierenden und 1300 Mitarbeitenden vereint unter ihrem Dach ein einmaliges Studienangebot in den Bereichen Design, Film, Kunst, Medien, Musik, Tanz, Theater und Vermittlung der Künste.

Das IT-Zentrum betreut die ganze Institution und besteht aus Entwicklern, Systemadministratoren (Mac, Windows, Linux) und Supporten.

Gewünscht wird ein neuer Dienst der es Mitglieder der ZHdK ermöglicht, grosse Dateien anhand eines webbasierten Tools mit Internen und Externen Personen austauschen.

Dabei verbleiben die auszutauschenden Inhalte in einem Firmen-internen Datenspeicher und werden nach einer gewissen Zeitdauer automatisch gelöscht. Die beiden wichtigsten Qualitätskriterien dieses Dienstes sind eine hohe Benutzerfreundlichkeit und das vergleichsweise zügige Verschieben der Daten. Das Verschieben der auszutauschenden Daten darf nicht durch die Applikation an sich, sondern nur durch das Netzwerk an sich beschränkt werden (Bandbreite, Netzanbindung, ...).

Evaluation

Eine kurze, aussagekräftige Evaluation macht klar, aus welchem Grund genau dieses Produkt gewählt wurde. Das heisst, Wahl des Tools muss begründet werden. Der Gruppenleiter muss vor der Umsetzung die Wahl absegnen.

Abnahme der Evaluation

Die Evaluation wird dem Auftraggeber (Gruppenleiter) präsentiert. Das Produkt wird festgelegt.

Use Case

Die Applikation soll das Austauschen von grossen Dateien ermöglichen: Ein Mitglied der ZHdK möchte eine grosse Datei einer oder mehreren Personen für eine gewisse Zeit an einem geheimen Ort bereitlegen. Die beziehenden Personen erfahren nach dem Bereitstellen, wie und wie lange sie auf die Datei zugreifen können. Nach Ablauf der zeitlichen Frist steht die Datei nicht mehr zur Verfügung. Die Nutzung der Applikation muss beidseitig möglich sein: Ein Mitglied der ZHdK kann einer Person ausserhalb der ZHdK eine Einladung zum Bereitstellen einer Datei senden. Die "externe" Person lädt dann die auszutauschende Datei hoch, woraufhin die anderen beteiligten Personen informiert werden, wie sie die Datei beziehen können.

Usability

Die Applikation muss über die aufgeführten Webbrowser (Safari ab V.6, Firefox ab V. 17 ESR, Internet Explorer ab V. 9) zugänglich sein und ohne Silverlight, Flash und Java auskommen. Die Nutzung der Funktionalitäten muss dabei so einfach oder selbsterklärend sein, dass weder eine Schulung noch umfassende Anleitungen für die Nutzung benötigt werden. Bei der Beurteilung der Usability kann von einer typischen Person des administrativen Lehrbereiches ausgegangen werden

(Sekretariatsmitarbeitende). Der nötige Informationsaustausch mit den Beteiligten sollte über die gängigen Kommunikationskanäle der ZHdK laufen (E-Mail). Dem Zugriff auf die Datei sollen möglichst keine Barrieren im Weg stehen (möglichst keine oder wenige Authentifizierung, möglichst wenige Klicks). Die Authentifizierung für interne User soll mit dem normalen Mail-login erfolgen (mit oder ohne "@login.itz suffix"). Das bedeutet eine Anbindung an unser Active-Directory, Authentication-Gateway oder AAI. Interne User können externe dazu berechtigen eine Datei hochzuladen.

Performance

Das Verschieben der auszutauschenden Datei darf nicht durch die Applikation an sich, sondern nur durch das Netzwerk an sich beschränkt werden (Bandbreite, Netzanbindung). Falls das Laden der Datei lange Zeit in Anspruch nimmt, soll der Prozess auch "im Hintergrund" weiterlaufen können.

Datensicherheit

Die auszutauschenden Daten sollen auf unseren eigenen Storage-Systemen zu liegen kommen.

Betrieb und Nachhaltigkeit

Die Applikation sollte auf freier Software basieren oder mindestens auf offene Standards zurückgreifen. Weiter muss die Software in der IT-Infrastruktur der ZHdK betrieben werden und auf bestehende Systeme (Storage, Server, Netzwerk) zurückgreifen. Der Betrieb und die Wartung der Applikation sollten möglichst klein sein und kein seltenes Spezialwissen erfordern. Für einen zuverlässigen Betrieb sollte die Applikation in ein automatisiertes Überwachungssystem (Nagios) eingebunden werden können.

Quantitative Anforderungen

- Grösse einer Datei: maximal 10 Gigabyte
- Vorhaltezeit der Datei: mindestens 2, maximal 28 Tage.
- Messgrösse für Usability: Der typische Arbeitsplatz zur Nutzung des Dienstes ist über Kabelverbindung mit 100 Megabit am Netzwerk angeschlossen.

Server

Die Software muss auf einem Firmen-internen Webserver mit Storage- und Active-Directory-Anbindung aufgesetzt werden.

Die Verbindung vom Server zum Active-Directory muss verschlüsselt erfolgen.

Die Verbindung vom Client zum Server muss verschlüsselt und mit gültigem Zertifikat erfolgen.

Aus den detaillierten Log-Dateien können Verbindungsfehler und Authentisierungsfehler zeitgenau identifiziert werden.

Versionsverwaltung

Alle bearbeiteten Konfigurations-Dateien werden in einem Firmen-internen Git-Repository verwaltet.

Alle für die IPA relevanten Dokumente und Dokumentationen werden in einem Firmen-internen Git-Repository verwaltet.

Userdokumentation

Es soll eine vollständige step-by-step Benutzerdokumentation erstellt werden.

Vorkenntnisse

Apache2 = In der Schule kurz angeschaut und schon produktiv eingesetzt aber nicht allzu oft

Postfix = Grundkenntnisse aus der Schule

PHP5 = Noch nie richtig eingesetzt

SimpleSAMLphp = keine Vorkenntnisse

FileSender = keine Vorkenntnisse

PostgreSQL = Keine Vorkenntnisse, dafür MySQL

Linux = Betreut 2 Linux Server

Vorarbeiten

Damit ich während der IPA nicht auf bestellte Dienste etc. warten muss, habe ich schon einige Sachen bei mir im Unternehmen vorbestellt.

Debian Linux Server	Transporter
IP-Reservierungen	195.176.254.107 10.10.10.107
DNS-Reservation	transporter.zhdk.ch
QuoVadis Server Zertifikat	
NFS-Storage	[filer2 (10.10.10.201)] /vol/transporter/transporter
Firewall Gruppe	Webserver

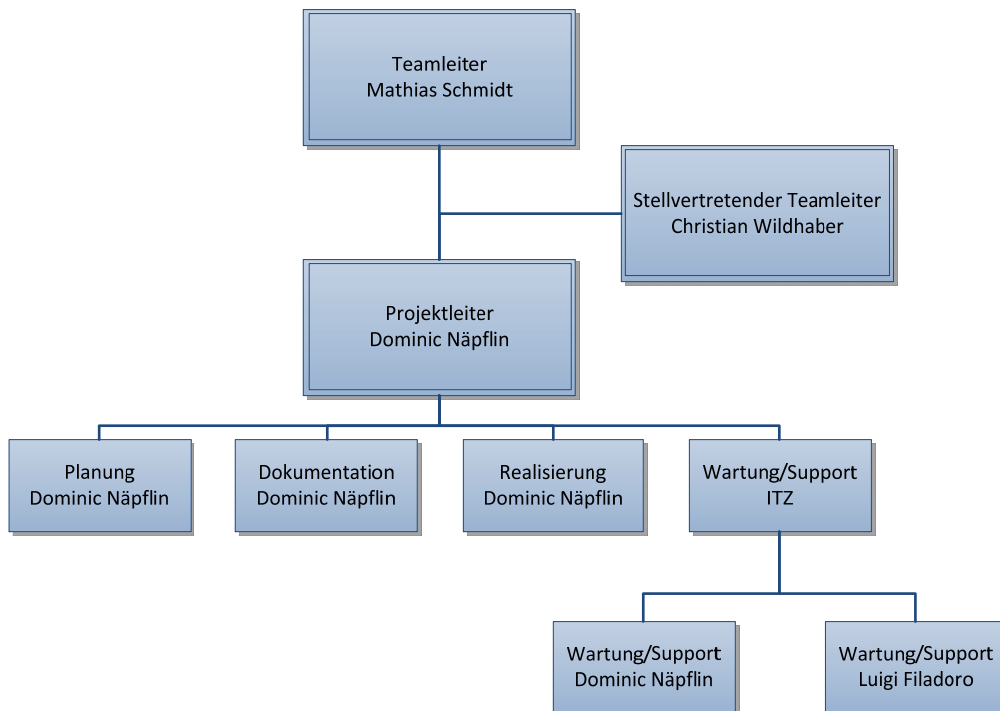
Firmenstandards

Die Zürcher Hochschule der Künste hat keine richtigen Firmenstandards.

Die Firmenstandards sind auf Linux Seite „The Debian Way“, was eine andere Bezeichnung für Common Practices ist. Das beinhaltet Daten und Software im richtigen Verzeichnis zu speichern, den Server „sauber“ zu halten und Software wenn möglich mit dem Installer apt-get zu installieren.

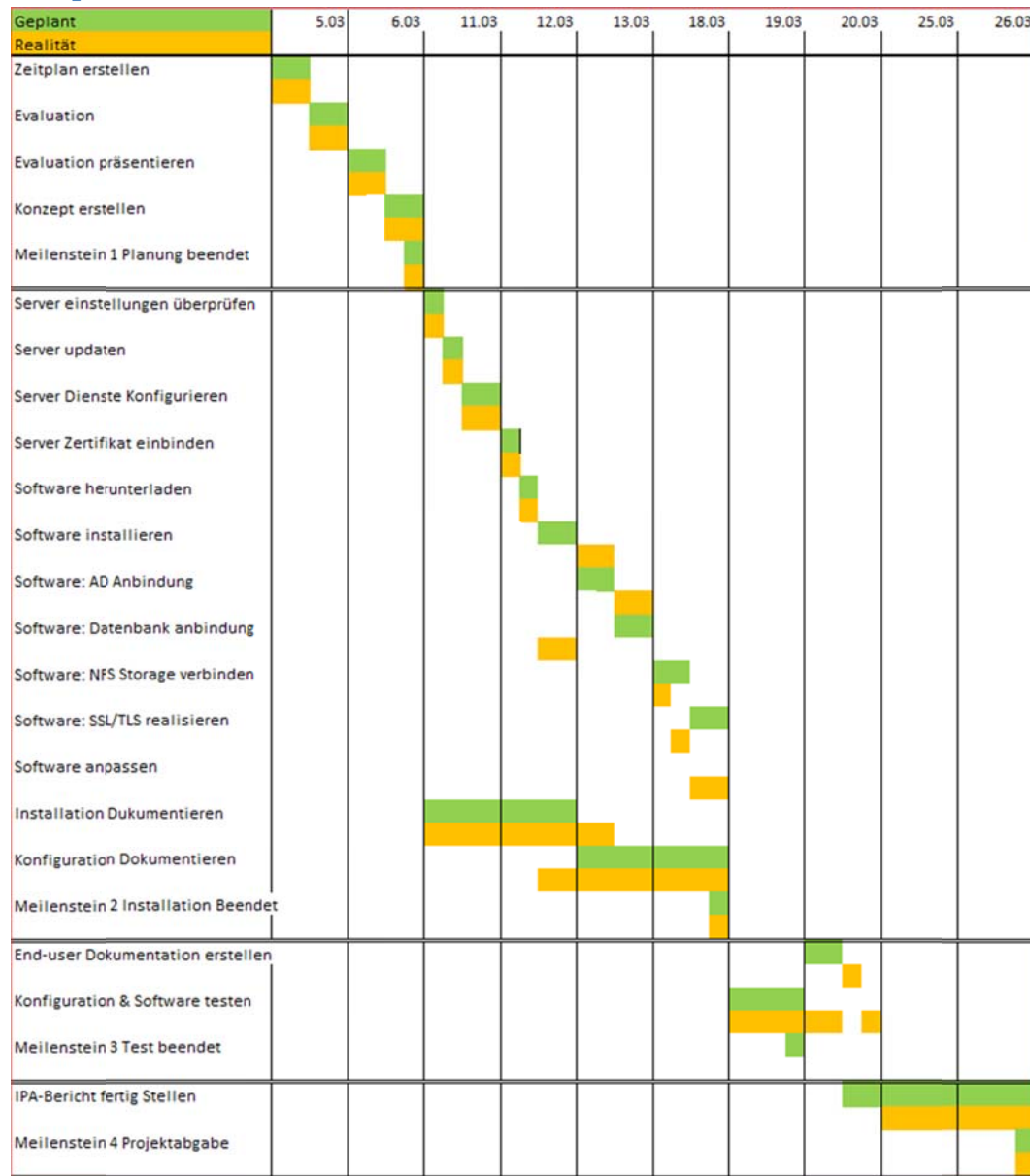
Die Dokumente werden mit dem Microsoft Office Paket erstellt und geführt.

Projektorganisation



Das Projekt wird vom Lehrenden Dominic Näpflin der Zürcher Hochschule der Künste geleitet und ausgeführt. Der Auftraggeber ist der Teamleiter des ITZ (Informationstechnologie-Zentrum) und in seiner Abwesenheit sein Stellvertreter. Als Projektmanagementmethode wird ein angepasstes Wasserfallmodell verwendet, mit den Phasen Analyse, Planen, Realisieren, Testen und Abgabe.

Zeitplan



Arbeitsjournal

Arbeitstag 1, 05.03.12

Tagesplanung

Tagesziele:

Zeitplan erstellen
Evaluation beginnen und beenden

Erreicht:

Zeitplan erstellt
Evaluationsunterlagen erarbeitet

Arbeitsjournal

Realisierung

Zeit:

08:30-12:00
12:30-17:00
17:00-17:30

Arbeitsschritte/Teilschritte

Zeitplan erstellen
Evaluation erstellen
Arbeitsjournal erstellen & nachtragen

Soll-Termin:

05.03 12:00
05.03 17:00
05.03 17:30

Reflexion

Allgemeine Zusammenfassung: Am ersten Tag lief alles wie geplant, ich konnte genug Zeit in den Zeitplan und die Evaluation stecken, damit ich einen guten Zeitplan und richtige Argumente für die Auswahl der Software habe.
Verlauf: Alles verlief wie geplant.
Probleme: Probleme Traten heute keine auf.
Lösungen:

Planung für den nächsten Tag

Morgen werde ich mein Ergebnis der Evaluation dem Teamleiter Präsentieren und mit ihm entscheiden, welche Software eingesetzt wird.

Arbeitstag 2, 06.03.12

Tagesplanung

Tagesziele:

Gespräch mit dem Experten
Evaluation präsentieren
Konzept erarbeiten

Erreicht:

Gespräch gehalten
Evaluation präsentiert
Evaluation besprochen
Konzept erstellt

Arbeitsjournal

Realisierung

Zeit:

07:30-08:00	Auf Expertengespräch vorbereitet
08:00-08:45	Gespräch mit Expert
08:45-09:10	Vorbereitung auf Evaluationspräsentation
09:10-09:50	Evaluationspräsentation
09:50-12:00	Evaluation Nachbesprechung
12:30-16:30	Konzept erstellen

Soll-Termin:

08:00-09:00
09:00-10:00
10:00-12:00
12:30-16:30

Reflexion

Allgemeine Zusammenfassung: Heute musste ich viel schreiben, was mir eigentlich nicht sehr liegt. Aber ich bin trotzdem gut vorangekommen und konnte alle gesetzten Ziele erreichen. Auch das Evaluationsgespräch war sehr hilfreich, da wir dort nochmal die Ziele festlegten die nicht so genau definiert waren.

Verlauf: Das Gespräch mit dem Experten und das Evaluationsgespräch verliefen meiner Meinung nach sehr gut und waren auch informativ. Der restliche Tag verlief ziemlich so wie ich es geplant hatte.

Planung für die Schultage und das Wochenende

Ich werde diese Woche noch nicht neben der normalen Arbeitszeit arbeiten, da ich sehr gut im Zeitplan liege.

Arbeitstag 3, 11.03.12

Tagesplanung

Tagesziele:

Servereinstellungen überprüfen
 Server Updaten
 Serverdienste Installieren/konfigurieren (PHP5, Apache2, SimpleSAMLphp, postfix)
 Installation dokumentieren

Erreicht:

Servereinstellungen überprüft
 Server war auf dem neusten Stand
 Serverdienste installiert & konfiguriert
 Installation dokumentiert

Arbeitsjournal

Realisierung

Zeit:

09:00-10:00
 10:00-12:50
 13:20-17:30
 09:00-17:30

Arbeitsschritte/Teilschritte

Server Einstellungen überprüfen
 Serverdienste installieren
 Serverdienste konfigurieren
 Installation/Konfiguration dokumentieren

Soll-Termin:

09:00-11:00
 12:00-17:30
 12:00-17:30
 09:00-17:30

Reflexion

Allgemeine Zusammenfassung: Die Servereinstellungen waren alle korrekt und Updates waren keine nötig. So konnte ich viel Zeit sparen und diese in die Installation und Konfiguration der Dienste einsetzen. Dokumentiert habe ich, aber noch nicht so ausführlich wie es am Schluss sein soll.

Verlauf: Die Einstellungen des Server zu kontrollieren ging viel schneller als erwartet und die Updates auch, da der Server ja schon auf dem aktuellsten Stand ist.

Probleme: Ich hatte einige Probleme mit den Apache Konfigurationsfiles, es wollte einfach nicht funktionieren, denn ich war mir nicht mehr ganz sicher wie ich das SSL einstellen muss damit es auch funktioniert.

Lösungen: Ich suchte im Internet nach einer Lösung und fand eine die für meine Einstellungen funktioniert hat, dieser Link ist in den Quellen unter apache2 zu finden.

Planung für den nächsten Tag

Morgen werde ich die Server Zertifikate installieren und den apache2 so konfigurieren, dass er sie akzeptiert. Ausserdem werde ich die Software Filesender herunterladen und installieren.

Arbeitstag 4, 12.03.12

Tagesplanung

Tagesziele:

Serverzertifikat einbinden
 PostgreSQL installiert und konfiguriert
 FileSender Herunterladen
 Installation dokumentieren

Erreicht:

Serverzertifikat eingebunden
 PostgreSQL installiert & konfiguriert
 FileSender heruntergeladen
 Installation dokumentiert

Arbeitsjournal

Realisierung

Zeit:

08:30-11:30
 11:30-13:00
 13:30-17:30
 08:30-17:30

Arbeitsschritte/Teilschritte

Serverzertifikat einbinden
 Filesender Herunterladen
 PostgreSQL installieren und konfiguriert
 Installationsdokumentation nachtragen

Soll-Termin:

08:30-10:30
 10:30-13:00
 13:30-17:30
 08:30-17:30

Reflexion

Allgemeine Zusammenfassung: Heute hatte ich einige Probleme mit dem Zertifikat, ich konnte aber alle Probleme lösen und bin danach gut vorangekommen.

Verlauf: Weil ich für das Zertifikat länger hatte als geplant, musste ich mich ein bisschen ranhalten. Mir ist ausserdem aufgefallen, dass ich PostgreSQL vor dem Filesender installieren muss, damit ich mehr Kontrolle über die Datenbank habe, als wenn ich es während der Installation des FileSenders mache.

Probleme: Ich konnte das Zertifikat und den Schlüssel nicht einbinden. Als erstes wurde das Zertifikat nicht gefunden und danach der Schlüssel nicht akzeptiert.

Lösungen: Das Zertifikat war unter einem falschen Namen in der Apache Konfiguration gespeichert und wurde deswegen nicht gefunden, der Schlüssel war nicht korrekt auf unserem Server gespeichert. Die Formatierung in dem Key-File war nicht korrekt, nach Änderungen funktionierte es ohne Probleme.

Planung für den nächsten Tag

Morgen werde ich die Installation des Filesenders die ich heute nicht machen konnte nachholen und den Filesender mit unserer AD verbinden.

Arbeitstag 5, 13.03.12

Tagesplanung

Tagesziele:

FileSender installieren
AD Anbindung realisieren

Erreicht:

FileSender ist installiert
AD Anbindung funktioniert

Arbeitsjournal

Realisierung

Zeit:

08:30-13:00
13:30-17:30
08:30-17:30

Arbeitsschritte/Teilschritte

FileSender installiert
AD Anbindung realisiert
Installations- und Konfigurationsdokumentation nachtragen

Soll-Termin:

08:30-13:00
13:30-17:30
08:30-17:30

Reflexion

Allgemeine Zusammenfassung: Die Installation des Filesenders ging recht gut voran, es traten keine grossen Fehler und Ungereimtheiten auf. Leider konnte ich den FileSendern nicht über apt-get installieren, da ich ein extra Repository hätte einbinden müssen auf dem der FileSender noch in der Alten Version gespeichert ist.

Verlauf:

Probleme: Ich musste mich erst in das simpleSAMLphp einlesen, da die AD Anbindung über dieses Tool geregelt ist. Ich hatte einige Zeit bis ich endlich aus dem Tool schlau wurde und die Konfiguration in Angriff nehmen konnte.

Lösungen: Nach einigem Lesen im Internet, ist mir klar geworden, wie ich die Konfiguration verändern musste. Auch dieser Link ist in den Quellen vermerkt.

Planung für den nächsten Tag

Morgen steht auf dem Zeitplan, NFS-Storage und SSL einrichten.

Arbeitstag 6, 18.03.12

Tagesplanung

Tagesziele:

NFS-Storage einbinden
SSL/TLS einrichten
Installation und Konfiguration dokumentieren

Erreicht:

NFS-Storage eingerichtet
SSL eingerichtet
Installation dokumentiert
Website & E-Mail angepasst

Arbeitsjournal

Realisierung

Zeit:

08:30-09:30 NFS-Storage einbinden
09:30-11:30 SSL/TLS einrichten
11:30-13:00 Website & E-Mails anpassen
13:00-17:30 Website & E-Mails anpassen
08:30-17:30 Dokumentiert

Arbeitsschritte/Teilschritte

Soll-Termin:

08:30-12:30
13:00-17:30
-
-
08:30-17:30

Reflexion

Allgemeine Zusammenfassung: Die Zeit die ich für das integrieren des NFS Storage eingeplant hatte war bei weitem zu viel. Auch das SSL einrichten ging um einiges schneller, obwohl nicht alles auf Anhieb funktionierte. Ausserdem ist mir während des Konfigurierens noch aufgefallen, dass die Texte auf der Seite und in den E-Mails und das Logo auf der Seite verändert werden kann. Dies teilte ich gleich meinem Teamleiter mit und bat ihn um die Texte und das Logo. Verlauf: Es lief alles schneller als geplant, deswegen konnte ich noch weitere Konfigurationen vornehmen. Auch die Texte bekam ich sehr schnell und konnte sie eintragen. Probleme: Ich bekam lange Zeit nicht die richtige SSL Konfiguration hin, das bedeutet, dass ich Probleme mit dem DocumentRoot hatte. Lösungen: Ich habe die Konfigurationsdatei default-ssl Komplet neu angefangen und sie mit den Bausteinen „ausgefüllt“ die ich kannte und wusste wie sie funktionieren, bis alles funktionierte.

Planung für den nächsten Tag

Morgen werde ich das System auf "Herz und Nieren" Prüfen.

Arbeitstag 7, 19.03.12**Tagesplanung****Tagesziele:**

Konfiguration & Software Testen
Gegebenen falls Anpassungen

Erreicht:

Tests erstellt und durchgeführt
Anpassungen vorgenommen

Arbeitsjournal**Realisierung****Zeit:**

08:30-13:00

13:30-17:30

Arbeitsschritte/Teilschritte

Funktionen getestet

Performance getestet

Soll-Termin:

08:30-13:00

13:30-17:30

Reflexion

Allgemeine Zusammenfassung: Das testen der Funktionen verlief grössten Teils erfolgreich. Ich musste aber einige Einstellungen noch verändern, damit alles so funktionierte wie es vorgesehen war. Bis auf den Internet Explorer V9 der kein HTML5 anzeigen kann. Der Performance Test war hingegen recht komplex und es stellte sich heraus, dass er recht langsam Dateien uploadet. Verlauf: Als ich die Tests festgelegt hatte, verlief alles wie geplant.

Probleme: Ich hatte ein Problem mit dem cronjob, eigentlich musste ich nur ein Befehl ausführen, der alles einrichtet, leider funktionierte das bei mir nicht.

Lösungen: Nach langem betrachten und der Hilfe von Herr Filadoro bemerkte ich, dass ich erstens den Befehl nicht ganz abgeschrieben hatte und zweitens noch ein Schreibfehler drin hatte. Herr Filadoro hat mir den Befehl erklärt und was er genau macht, so dass ich den cronjob setzen konnte.

Planung für den nächsten Tag

Morgen kommt der Experte zum zweiten Gespräch. Zusätzlich muss ich morgen die Tests zu Ende bringen und die Benutzerdokumentation schreiben. Ich werde mich an die Linux Webserver Spezialisten bei uns im Unternehmen wenden, um zu überprüfen, ob der Server nicht noch beschleunigt werden kann.

Arbeitstag 8, 20.03.12

Tagesplanung

Tagesziele:

2. Expertengespräch
Benutzerdokumentation
FileSender Test fertig stellen

Erreicht:

Gespräch hat stattgefunden
Benutzerdokumentation ist erstellt
Tests sind abgeschlossen

Arbeitsjournal

Realisierung

Zeit:

08:15-09:00
09:00-12:00
12:30-14:00
14:00-17:30

Arbeitsschritte/Teilschritte

2. Expertengespräch
FileSender Testen
Benutzerdokumentation schreiben
FileSender Testen

Soll-Termin:

08:15-09:00
-
09:00-13:00
-

Reflexion

Allgemeine Zusammenfassung: Heute wollte ich eigentlich die Benutzerdokumentation erstellen und mit dem Fertigstellen des IPA-Berichts beginnen. Leider wurde das Testen der Performance des FileSenders aufwändiger als gedacht. Deswegen habe ich heute noch einige Stunden mit zwei Experten das Problem angeschaut und versucht es zu lösen.

Verlauf: Das Erstellen der Benutzerdokumentation war sehr einfach, da der FileSender selber schon selbsterklärend ist. Das Testen der Performance war anspruchsvoll zog sich sehr in die Länge.

Probleme: Der FileSender empfängt nur sehr langsam die Dateien und es ist nicht klar ersichtlich an was es liegt.

Lösungen: Weil alle Websites die wir betreiben einen so geringen Upload-Speed haben, setzen sich die verantwortlichen Personen an das Upload-Problem.

Planung für den nächsten Tag

In den noch verbleibenden zwei Tagen werde ich den IPA-Bericht fertig stellen.

Arbeitstag 9, 25.03.12**Tagesplanung****Tagesziele:**

IPA-Bericht fertig stellen

Erreicht:

An IPA-Bericht gearbeitet

Arbeitsjournal**Realisierung****Zeit:**

08:00-13:00

13:30-17:30

Arbeitsschritte/Teilschritte

IPA-Bericht bearbeitet

IPA-Bericht bearbeitet

Soll-Termin:

08:00-

17:30

Reflexion

Allgemeine Zusammenfassung: Heute habe ich mein Schlusswort und andere wichtige Teile des Berichts verfasst.

Verlauf: Der Tag verlief sehr ruhig, da ich nur mit dem Dokument beschäftigt war.

Probleme: Ich war mir nicht mehr ganz sicher, ob ich alle meine Konfigurationsdateien in den Anhang nehmen kann, denn sie sind zum Teil sehr lang.

Lösungen: Ich fragte meinen Fachvorgesetzten, ob diese Seiten nicht mitzählen. Er hat mir geantwortet, dass der Anhang nicht zu den 100 Seiten gehört.

Planung für den nächsten Tag

Morgen stelle ich den IPA-Bericht fertig und lade ihn auf die pkorg.ch Seite hoch.

Arbeitstag 10, 26.03.12

Tagesplanung

Tagesziele:

IPA-Bericht fertig stellen
 IPA-Bericht drucken lassen
 IPA-Bericht (gedruckte Form) versenden
 IPA-Bericht hochladen

Erreicht:

IPA-Bericht fertiggestellt
 IPA-Bericht gedruckt
 IPA-Bericht hochgeladen
 IPA-Bericht versand

Arbeitsjournal

Realisierung

Zeit:

08:30-

Arbeitsschritte/Teilschritte

IPA-Bericht fertig stellen
 IPA-Bericht drucken lassen
 IPA-Bericht hochladen
 17:30 IPA-Bericht versenden

Soll-Termin:

08:30-

17:30

Reflexion

Allgemeine Zusammenfassung: Ich habe den IPA-Bericht fertig gestellt und werde jetzt noch heute den Ausdruck machen und ihn absenden.

Verlauf: Ich habe den Bericht fertig gestellt und nach einem Geschäft geschaut, das den Bericht binden kann.

Probleme: Ich bin morgen an einer Beerdigung und kann deswegen den Bericht morgen nicht absenden.

Lösungen: Ich sende den IPA-Bericht heute ab.

Teil 2

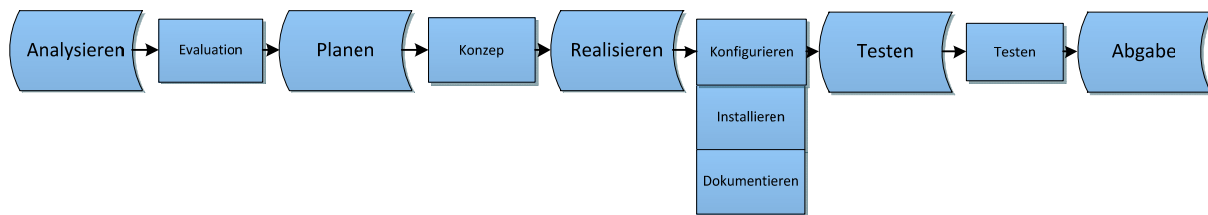
Management Summary

Ausgangssituation

Wir, die Zürcher Hochschule der Künste, brauchen ein Tool, das unseren Mitarbeitenden erlaubt, grosse Dateien zu versenden. Dies funktioniert im Moment nur mit grossem Aufwand und ist deshalb nicht sehr beliebt bei den Mitarbeitenden.

Umsetzung

Das Projekt wird in fünf Phasen aufgeteilt und durchgeführt:



Wasserfallmodell Planung 1

Es wird als erstes eine Evaluation gemacht, um die richtige Software zu finden.

Wenn klar ist, welche Software eingesetzt wird, muss das Konzept so angepasst werden, dass die Anforderungen auch erfüllt werden können. Die Änderungen werden durch den Teamleiter abgesegnet und danach wird mit der Implementierung des Tools begonnen.

Am Ende werden noch die Funktionen getestet und eine Benutzer-Dokumentation erstellt.

Erwartetes Ergebnis

Ein Tool soll installiert und konfiguriert werden, mit dem unsere Mitarbeitenden grosse Dateien versenden können, ohne grossen Aufwand zu betreiben. Das Tool soll einfach zu bedienen sein, damit keine grossen Anleitungen von den Mitarbeitenden gelesen werden müssen. Es soll auch möglich sein Dateien, die eine gewisse Zeit gespeichert bleiben, an externe Benutzer, die nicht der ZHdK angehören, zu senden. Ausserdem soll es auch möglich sein, externen Benutzern das Recht zu geben, eine Datei über das Tool zu senden.

Analysieren

Der Abschnitt Analyse behandelt die Evaluation der Software. Es werden verschiedene Möglichkeiten durchgegangen und wird mit dem Teamleiter entschieden, welche eingesetzt wird.

Evaluation

Weil keine Software explizit genannt wurde, wird eine Evaluation gemacht, die bestimmen soll, welche Software genutzt werden soll. Die Kriterien, welche die Software einhalten muss, werden der Aufgabenstellung entnommen.

Nach der Evaluation wird das Ergebnis dem Teamleiter präsentiert und mit ihm zusammen entscheiden, welche Software eingesetzt wird.

Es stehen fünf verschiedene Softwarelösungen zur Evaluation bereit: Filesender, Dropbox, Teamdrive, OwnCloud und Google Apps.

Folgende Kriterien wurden dem Text entnommen:

User Case

Dateien Bis zu 10 GB versenden
AD-Anbindung
Ablaufdatum der Dateien
Dateien an externe Kunden Senden
Externe können Dateien hochladen

Usability

Webbrowser kompatibel
benötigt keine Plug-Ins
ist Selbsterklärend
Kommunikation über Email

Performance

Applikation ist schnell
Hochladen soll im Hintergrund möglich sein

Datensicherheit

Dateien werden auf internen Ablage gespeichert
Dateien werden Verschlüsselt übertragen und gespeichert

Betrieb & Nachhaltigkeit

Freie Software
Offene Standards
Läuft im ITZ mit bereits vorhandenen Servern

Geringe Wartung
Kein Extrawissen notwendig
Überwachung möglich

Von den obigen genannten Kriterien sind folgende die **K.O. Kriterien**:

AD-Anbindung
Externe können Dateien hochladen
Läuft im ITZ mit bereits vorhandenen Servern
Dateien an externe Kunden Senden

Damit eine gute Einschätzung der Software gemacht werden kann, wird eine Präferenzmatrix erstellt, mit der die Gewichtung der verschiedenen Kriterien besser eingeschätzt werden kann.

Die Präferenzmatrix wird erstellt, indem man die Anforderungen in einer Liste einträgt. Danach werden immer die zwei Anforderungen die untereinander stehen miteinander verglichen und die wichtigere Anforderung wird eine Spalte weiter geschoben. So erhält man eine gute Gewichtung, die nachvollziehbar ist.

Präferenzmatrix				Projektbezeichnung	
für das Projekt					
Gewicht	Rangfolge	Anzahl	Kriterien		
		Noten			
1.169590643	8	2	a Daten Bis zu 10 GB versenden		
0	15	0	b Applikation ist schnell		
0.584795322	10	1	c Ablaufdatum der Daten		
36.84210526	1	63	d Daten an externe Kunden Senden		
0	15	0	e Geringe Wartung		
0.584795322	10	1	f Webbrowser Kompatibel		
15.20467836	3	26	g Läuft im ITZ mit vorhandenen Servern		
0	15	0	h Selbsterklärend		
0.584795322	10	1	i Kommunikation über Email		
2.923976608	5	5	j Offene Standards		
0	15	0	k Hochladen soll im Hintergrund möglich sein		
9.356725146	4	16	l Daten liegen bei uns		
2.923976608	5	5	m Verschlüsselt übertragen oder gespeichert		
0.584795322	10	1	n Freie Software		
25.73099415	2	44	o AD Anbindung		
0	10	1	p kommt ohne Plug-Ins aus		
0	15	0	q Kein Extrawissen notwendig		
1.169590643	8	2	r Überwachung möglich		
1.754385965	7	3	s Externe kann Daten hochladen		
99.41520468		171			

Beim Betrachten der Präferenzmatrix scheint es einige sehr wichtige Punkte zu geben und andere, die nicht so wichtig sind. Dieser Eindruck entsteht, weil die Präferenzmatrix sehr strikt ist und so wichtige Kriterien schon am Anfang ausscheiden können. Das passiert, wenn ein noch wichtigeres Kriterium daneben steht.

Deswegen wird die Präferenzmatrix benutzt, aber in der Präsentation und dem Gespräch mit dem Teamleiter so definiert, dass auch allen wichtigen Kriterien genug Sorge getragen wird.

Mit Hilfe der Präferenzmatrix kann eine Evaluationstabelle erstellt werden, in der die verschiedenen Anforderungen mit der Gewichtung dargestellt werden. So entsteht eine aussagekräftige Tabelle, die hilft, die richtige Software für unsere Anforderungen zu finden.

	Gewichtung	Filesender	OwnCloud	Dropbox	Teamdrive	Google Apps
User Case						
Daten Bis zu 10 GB versenden	1.169590643				unbekannt	unbekannt
AD Anbindung	25.73099415					
Ablaufdatum der Daten	0.584795322				unbekannt	unbekannt
Daten an externe Kunden Senden	36.84210526					
Externe kann Daten hochladen	1.754385965		umwege			
Usability						
Webbrowser Kompatibel	0.584795322					
kommt ohne Plug-Ins aus	0					
Selbsterklärend	0		fast	fast	unbekannt	unbekannt
Kommunikation über Email	0.584795322			Link		Link
Performance						
Applikation ist schnell	0	unbekannt	unbekannt		unbekannt	
Hochladen soll im Hintergrund möglich sein	0	In einem Tab	Ordner Sync	Ordner Sync	Ordner Sync	
Datensicherheit						
Daten liegen bei uns	9.356725146					
Verschlüsselt übertragen oder gespeichert	2.923976608					
Betrieb & Nachhaltigkeit						
Freie Software	0.584795322					
Offene Standards	2.923976608					
Läuft im ITZ mit vorhandenen Servern	15.20467836					
Geringe Wartung	0	SimpleSAMLphp	unbekannt		unbekannt	
Kein Extrawissen notwendig	0	SimpleSAMLphp			unbekannt	
Überwachung möglich	1.169590643					
Gewichtung Total		99.41520468	98.5380117	38.8888889	95.90643275	67.25146199

Das Ergebnis der Evaluationstabelle zeigt klar, dass drei der fünf Software-Lösungen in Frage kommen: Filesender 99,4, OwnCloud 98.5 und Teamdrive 95.9. Aber jede hat Vor- und Nachteile, die für den Entscheid mit dem Teamleiter besprochen werden müssen um abzuklären.

Vor- und Nachteile

FileSender kann Dateien mit einem Link einfach an interne, aber auch externe User/Email-Adressen versenden. Ausserdem ist es möglich, externen Usern einen temporären Account zu erstellen, mit dem Sie Dateien an ein ZHdK-Mitglied senden können.

Der Nachteil dieser Software ist, dass SimpleSAMLphp eingesetzt wird. Dies ist ein Tool, das keiner unserer Systemadministratoren kennt.

OwnCloud ist ein sehr grosses Programm und erinnert stark an Dropbox. Mit diesem Programm lassen sich Dateien in der Cloud gut verwalten. Auch bei dieser Software ist es möglich, Dateien an externe Benutzer zu senden. Leider kann OwnCloud aber keine temporären User erstellen und ist für unseren Zweck überdimensioniert.

Teamdrive ist ähnlich wie OwnCloud, aber kostenpflichtig. Dies bedeutet, man zahlt für die Software und deren Benutzung pro Monat einen Betrag an die Entwicklerfirma. Der Vorteil von Teamdrive ist, dass ein guter Support geboten wird und dass eine starke Verschlüsselung der Dateien möglich ist.

Eigene Empfehlung

Ich empfehle nach der Evaluation, die Software Filesender, da sie genau das macht, was wir wollen. Dies zeigt auch die Evaluationstabelle mit der fast perfekten Gewichtung von 99.4 und das alle K.O. Kriterien eingehalten wurden..

Das einzige Problem ist, dass niemand sich mit SimpleSAMLphp auskennt. Dies ist eine Software, die es ermöglicht, einen Single Sign On Punkt zu erstellen. Weil wir das aber nicht benutzen und brauchen, ist die zusätzliche Komplexität nicht ideal. Dazu kommt noch, dass bei grossen Änderungen ein grösserer Aufwand entstehen könnte, als bei anderen Lösungen, die den Systemadministratoren bekannt sind.

Trotzdem denke ich, dass diese Software die richtige ist.

Ausgewählte Software

Wir haben uns für die Software Filesender entschieden, weil nur diese Software alle K.O.-Kriterien erfüllt hat.

Der Hauptgrund für den Entscheid gab das Kriterium „Externe können Dateien hochladen“ und dass die Software genau das kann, was wir wollen. Es kann nicht zu einem weiteren Ablageplatz für Dateien werden, die nie gelöscht werden.

Wir haben beschlossen, dass einige Änderungen in den Anforderungen gemacht werden müssen. Diese werden im Konzept erläutert

Planen

In dieser Phase wird ein Konzept mit detaillierten Angaben für den Transporter-Dienst erstellt.

Konzept

Das Konzept aus dem Pflichtenheft wird fast 1 zu 1 übernommen. Es müssen nur einige Veränderungen an der Aufgabenstellung gemacht werden, damit es mit der ausgewählten Software auch umsetzbar ist.

Anforderungen der Zielgruppe

Es soll mit der Software Filesender, eine Webseite aufgebaut werden, mit der ZHdK-Kunden (ZHdK-Login) Dateien an externe und interne Benutzer senden können. Die Dateien müssen auf unseren internen Server gespeichert und der Link zu den Dateien muss mittels E-Mail versendet werden können.

Zu erstellende Dokumente

Neben der funktionierenden Software muss auch eine detaillierte Installations- und Konfigurationsdokumentation erstellt werden, damit jeder Systemadministrator der ZHdK die Installation und Konfiguration durchführen kann. Diese Anleitungen werden in der internen Wikipedia gespeichert und zusätzlich dem IPA-Bericht beigelegt.

Auch eine Step-by-Step Anleitung für die Benutzer soll erstellt werden, die dann in das Services-Portal des ITZ zugänglich gemacht wird.

Geänderte Anforderungen

Weil einige Anforderungen nicht oder nur in abgewandelter Form von FileSender unterstützt werden, mussten die Anforderungen umgeschrieben und klarer definiert werden.

Die Software muss nicht mehr selbsterklärend sein, da diese Formulierung nicht klar definierbar ist und von Person zu Person unterschiedlich ist. Die neue Formulierung ist wie folgt:

Eine Person, die Erfahrung hat, mit einem Web-Browser im Internet zu navigieren, kann mit Hilfe der Step-by-Step-Anleitung alle Funktionen des Dienstes nutzen.

Auch die Angaben über das Authentifizieren und Klicken mussten ein wenig angepasst werden, da nicht klar definiert ist, was „wenig Klicks“ sind und was mit einer einfachen Authentifizierung gemeint ist.

Die Anzahl der erlaubten Klicks für Einloggen, Datei hochladen und Versenden ist auf 10 gesetzt und das Authentifizieren soll beim hochladen der Datei nur einmal erforderlich sein.

Weil sich Filesender klar als Sieger platzieren konnte und diese eine spezielle Software zum Einloggen benutzt, die niemand an der ZHdK kennt, mussten wir die Angabe „keine Spezialwissen notwendig“ auf „sehr gute Installations- und Konfigurationsdokumentation“ ändern.

Um die Effizienz der Software zu testen, wird die Geschwindigkeit des Hoch- und Herunterladen mit unserem FTP-Server und mit der VPN-Verbindung verglichen. Genauere Angaben zum Test der Performance werden im Abschnitt Testen angegeben.

Das Hoch- und Herunterladen von Dateien soll in einem separaten Tab funktionieren.

Backup

Für diesen Webdienst wird kein Backup eingerichtet. Die Dateien liegen auf dem NFS-Storage und werden dort nicht noch zusätzlich gesichert, da es nur ein Tool zum Übertragen von Dateien ist und somit diese Dateien noch irgendwo anders gespeichert sind.

Die Konfiguration hingegen liegt lokal auf dem virtuellen Server und wird automatisch mit den anderen virtuellen Servern gesichert.

Vorgehen

Auf dem vorbereiteten Linux-Debian-Server werden die Software FileSender und weitere benötigten Applikationen installiert und konfiguriert, damit es produktiv einsetzbar ist.

Als erstes wird der Server so vorbereitet, dass mit der Installation der Software und den nötigen Konfigurationen begonnen werden kann.

Dazu zählen:

- QuoVadis Root Zertifikat einbinden

Linux OS updaten/upgraden falls nötig

Nach den Vorbereitungen wird mit der Installation der Software begonnen. Dazu werden Anleitungen aus dem Internet für unseren eigenen Zweck umgeschrieben.

Die Anbindung von FileSender an unsere Active-Directory wird über das Tool SimpleSAMLphp realisiert.

Als Datenbank wird PostgreSQL verwendet, da dieser Datenbanktyp der Standard von FileSender ist. Weil wir kein PostgreSQL-Server haben, wird die Datenbank lokal auf dem Transporter installiert und betrieben.

Als Webdienst wird Apache2 mit PHP-Modulen verwendet und so eingestellt, dass der Dienst nur über HTTPS erreichbar ist. Dazu wird ein Zertifikat der Zertifizierungsstelle QuoVadis verwendet.

Den NFS-Container wird so eingebunden, dass nur die Dateien, die hochgeladen werden, im NFS-Speicher abgelegt werden.

Meilenstein 1

Als erster Meilenstein ist die Beendigung der Evaluation und des Konzepts, sowie die Präsentation der Ergebnisse.

Die Evaluation und das Konzept sind erstellt und mit dem Teamleiter besprochen und abgesegnet worden. Jetzt muss in der Realisierung die Anforderungen umgesetzt werden.

Das nächste Mal würde ich eine klarere Trennung von Soll und Muss Kriterien vornehmen.

Realisieren

In diesem Abschnitt wird das umgesetzt, was in den vorherigen Phasen geplant wurde.

Installation

Als erstes bei der Realisierung, werden die notwendigen Pakete heruntergeladen und installiert, aber noch nicht konfiguriert.

System-Beschreibung

Alle Einstellungen und Konfigurationen, die in dieser Installationsdokumentation gemacht werden, sind auf dem Server transporter.zhdk.ch durchzuführen. Es ist ein Linux Debian 6.0 Server, der im ZHDK-Cluster steht. Der Server hat einen Intel(R) Xeon(R) CPU L5640 @ 2.27GHz Prozessor, 6 GB RAM und 15 GB interner Speicher.

Aus Platzgründen werden hier nur die Teile aus den Konfigurationsdateien aufgelistet, die ich selber verändert habe und relevant sind. Die gesamten Konfigurationsdateien befinden sich im Anhang.

Updates

Zuerst muss überprüft werden, ob das Debian Betriebssystem auf dem aktuellen Stand ist. Dies funktioniert mit folgenden Befehlen:

- `apt-get update`
- `apt-get upgrade`

Root Zertifikat

Als zweiter Schritt muss das QuoVadis Root Zertifikat auf dem Debian Server installiert werden. Da QuoVadis den Zeitpunkt verpasst hat, bei den Debian Entwicklern ihr Root Zertifikat rechtzeitig einzureichen, ist es in der Version 6.0 nicht standardmässig installiert.

Das Root Zertifikat kann von einem produktiven Server (hier wiki.zhdk.ch) bei dem es schon installiert ist, kopiert werden. Der Befehl kopiert das Zertifikat und speichert es auf dem Transporter in das Verzeichnis `/etc/ssl/certs/`.

- `scp dominic@wiki.zhdk.ch:/etc/ssl/certs/QuoVadis_Global_SSL_ICA.pem /etc/ssl/certs/`

Nun muss das Zertifikat in die Datei `/etc/ldap/ldap.conf` eingetragen werden

```
# Hier wird das QuoVadis Root Zertifikat im ldap eingebunden
TLS_CACERT /etc/ssl/certs/QuoVadis_Global_SSL_ICA.pem
```

Um zu testen, ob das Root-Zertifikat korrekt eingebunden wurde, kann mit dem Befehl `ldapsearch` versucht werden, mit dem Server zu verbinden. Zuerst muss aber noch das Paket `ldap-utils` installiert werden.

- `apt-get install ldap-utils`
- `ldapsearch -Z -H "ldap://172.30.10.12" -x -D 'CN=ldapsearch,OU=Service Accounts,OU=Accounts,OU=_ZHdK manuell,DC=vera,DC=hgka,DC=ch' -w '<Passwort>' -b 'dc=vera,dc=hgka,dc=ch' '(msNPAllowDialin=FALSE)'`

Apache2

Als nächstes muss der Webdienst installiert werden. Wir haben uns für Apache2 entschieden, da alle unsere internen Webserver mit Apache2 laufen.

```
apt-get install apache2
```

Da die Verbindung zum Webserver verschlüsselt sein soll, muss das apache2 SSL-Modul und die SSL-Seite aktiviert werden.

- `a2enmod ssl`
- `a2ensite default-ssl`
- `/etc/init.d/apache2 restart`

PHP5

Nun muss noch PHP5, ein Apache2 PHP-Modul und das PHP-LDAP-Modul installiert werden.

- `apt-get install php5 libapache2-mod-php5 php5-ldap`

PostgreSQL

Die PostgreSQL Datenbank wird mit folgendem Befehl erstellt:

- `apt-get install postgresql php5-pgsql`

Damit vom localhost auf die PostgreSQL-Datenbank eingeloggt werden, kann muss noch die Konfigurationsdatei `/etc/postgresql/8.4/main/pg_hba.conf` angepasst werden:

```
# Database administrative login by UNIX sockets
local          all          postgres          ident
# TYPE          DATABASE    USER  CIDR-ADDRESS    METHOD
# "local" is for Unix domain socket connections only
local          all          all              ident
# IPv4 local connections:
host           all          all    127.0.0.1/32     md5
# IPv6 local connections:
host           all          all    ::1/128          md5
```

Nach den Änderungen an der Konfigurationsdatei muss der Dienst neu gestartet werden.

- `/etc/init.d/postgresql restart`

SimpleSAMLphp

Eigentlich könnte dieses Paket über den Befehl „apt-get install“ installiert werden. Aber diese Version ist leider nicht die aktuelle Version, die von den FileSender-Programmierer verwendet wird. Daher wird das Paket von der site googlecode.com heruntergeladen und von Hand installiert.

Zuerst wird in den `/tmp` Ordner gewechselt und danach kann mit dem `wget`-Befehl das Paket heruntergeladen werden:

- `cd /tmp`
- `wget http://simplesamlphp.googlecode.com/files/simplesamlphp-1.10.0.tar.gz`

Nach dem Herunterladen muss überprüft werden, ob das Packet richtig und vollständig gespeichert wurde. Dies funktioniert mit dem Befehl sha1sum.

- `sha1sum -b simplesamlphp-1.10.0.tar.gz`

Wenn die SHA1 Checksum gleich ist, wie die auf der Download-Page

(<http://code.google.com/p/simplesamlphp/downloads/detail?name=simplesamlphp-1.10.0.tar.gz&can=2&q=>), kann das Packet entpackt werden.

Zuerst muss aber für alle FileSender-relevanten Dateien das Verzeichnis(/usr/local/filesender/) erstellt werden.

- `mkdir /usr/local/filesender`
- `cd /usr/local/filesender`
- `tar -xvf simplesamlphp-1.10.0.tar.gz`

Damit der SimpleSAMLphp-Dienst einfach angesprochen werden kann, wird noch ein Symlink erstellt.

- `ln -s simplesamlphp-1.10.0/ simplesaml`

Filesender

Als letztes wird nun FileSender installiert. Dieses Paket wird wie das SimpleSAMLphp-Paket mit dem wget-Befehl heruntergeladen und installiert. Dies muss gemacht werden, weil das Filesender-Paket nicht von den Debian-Repositories heruntergeladen werden kann.

- `cd /tmp/`
- `wget --no-check-certificate http://download.filesender.org/filesender-1.5.tar.gz`

Um zu überprüfen, ob das Packet richtig und vollständig heruntergeladen wurde, muss wieder die SHA1 Checksum überprüft werden. Die SHA1 Checksum findet sich unter folgendem Link:
https://www.assembla.com/wiki/show/file_sender/Release_1-5

- `sha1sum -b filesender-1.5.tar.gz`

Jetzt muss das Packet noch entpackt und an den richtigen Ort verschoben werden.

- `mv filesender-1.5.tar.gz /usr/local/filesender/`
- `cd /usr/local/filesender`
- `tar -xvzf filesender-1.5.tar.gz`
- `mv filesender-1.5/* /usr/local/filesender/`

Nun muss noch die Konfigurationsdatei erstellt werden. Dies wird mit der existierenden .dist Konfiguration gemacht.

- `cp config/config-dist.php config/config.php`

GitHub

Als Versionisierungstool wird GitHub verwendet, für den IPA-Bericht, aber auch für die Konfigurationsdateien auf dem Linux Server. Dazu wird nach jedem Schritt die Datei gespeichert und auf den Git-Sever hochgeladen.

Linux

Die Installation auf Linux kann mit apt-get installiert werden.

- apt-get install git

Als nächster Schritt sollte man in das Verzeichnis wechseln, in dem man das Repository platzieren möchte.

- cd /home/admin/

Damit Git weiss, wie der Benutzer und die dazugehörige E-Mail Adresse heissen, müssen folgende Befehle ausgeführt werden. Der Benutzername und E-Mail Adresse müssen mit einem bestehenden Git-Benutzer übereinstimmen.

- git config --global user.name "DomCom"
- git config --global user.email "dominic.naepflin@zhdk.ch"

Nun muss noch das Transporter Repository mit folgendem Befehl eingebunden werden.

- git clone <http://DomCom@github.com/DomCom/Transporter.git>

Weiter muss dann noch für jedes Paket ein Verzeichnis angelegt werden, damit es eine Ordnung im Verzeichnis hat.

- mkdir Tansporter/FileSender Tansporter/FileSender/config
Tansporter/FileSender/language Tansporter/FileSender/cron
- mkdir Tansporter/simpleSAMLphp Tansporter/simpleSAMLphp/conf
- mkdir Tansporter/PHP5 Tansporter/PHP5/apache2 Tansporter/PHP5/conf.d
- mkdir Tansporter/Apache2 Tansporter/Apache2/ sites-available

Danach müssen noch die verschiedenen wichtigen Konfigurationsdateien mit einem Hard-Link in den entsprechenden Ordner verlinkt werden.

- ln /usr/local/filesender/filesender/config/config.php FileSender/config/
- ln /usr/local/filesender/filesender/config/banner.png FileSender/config/
- ln /usr/local/filesender/filesender/language/de_DE.php FileSender/language/
- ln /usr/local/filesender/filesender/cron/cron.php FileSender/cron/
- ln /usr/local/filesender/simplesaml/config/authsources.php
simpleSAMLphp/config/
- ln /usr/local/filesender/simplesaml/config/config.php simpleSAMLphp/config/
- ln /etc/apache2/sites-available/default Apache2/sites-available/
- ln /etc/apache2/sites-available/default-ssl Apache2/sites-available/
- ln /etc/apache2/ports.conf Apache2/
- ln /etc/php5/apache2/php.ini PHP5/apache2/

- In /etc/php5/conf.d/suhosin.ini PHP5/conf.d/

Ab diesem Moment an können die Dateien mit dem Repository synchronisiert werden.

Dies funktioniert mit folgenden Befehlen:

- `git add Transporter/*`
- `git commit -m „Nachricht“`
- `git push`

Das Konfigurationsdatei-Repository ist unter <https://github.com/DomCom/Transporter> zu erreichen.

Windows

Auf Windowsseite ist das einbinden eines Git-Repositorys nicht so Aufwendig wie unter Linux.

Als erstes muss man auf die Windows Seite von Git: <http://windows.github.com/>. Dort kann man das Windows-Tool kostenfrei herunterladen.

Die Installation ist selbsterklärend und ist mit wenigen Klicks gemacht. Wenn die Installation fertig ist, kann man sich mit seinem Account anmelden. Nach der Anmeldung gibt es zwei Orte wo Repositorys liegen können. Entweder kann man Lokal ein neues erstellen, oder man sucht unter „github“ -> Benutzername nach schon existierenden, auf dem Profil.

Erstellt man ein neues, wird ein neues Verzeichnis angelegt und alle Dateien die in diesem Verzeichnis sind werden in das Repository aufgenommen.

Um die Daten zu synchronisieren, muss das Programm GitHub geöffnet werden und das entsprechende Repository mit einem Doppelklick ausgewählt werden. Nun erscheint ein neues Fenster, mit den ganzen neuen Dateien die in dem Ordner sind. Um die Dateien zu synchronisieren muss eine „Commit Message“ eingegeben werden und mit dem Klicken auf „Commit“ bestätigt werden. Damit die Dateien auch synchronisiert werden muss der Commit noch mit das klicken auf sync bestätigt werden.

Das Windows Repository mit den IPA Dokumenten ist unter <https://github.com/DomCom/IPA-Dokumente> zu erreichen.

Konfigurieren

Jetzt sind alle notwendigen Pakete installiert, und es kann mit der Konfiguration begonnen werden.

NFS-Storage

Weil die Dateien, die mit dem Transporter versendet werden, auf einem NFS-Storage liegen sollen, muss dieser nun entsprechend so eingerichtet werden. Die Files des Filesenders werden im Verzeichnis `/usr/local/filesender/filesender/files` gespeichert. Somit kann man den NFS-Storage auf diesen Ordner mounten und alle Dateien werden automatisch auf den NFS-Storage gespeichert.

Diese Einstellung wird in der Datei `/etc/fstab` mit folgendem Eintrag vorgenommen:

```
10.10.10.201:/vol/transporter/transporter
/usr/local/filesender/filesender/files nfs
rsize=64512, wsize=64512, intr, noacl, nolock, ac, async, tcp, auto
0 0
```

Danach muss der Mount-Befehl durchgeführt werden.

- `mount -a`

Postfix

Weil Postfix schon standardmässig auf den Debian Server installiert ist, muss nur noch eine kleine Einstellung vorgenommen werden. Postfix soll über den SMTP der ZHdK Mails versenden, denn ohne den SMTP würden die meisten Mails wohl in einem Spam-Ordner landen.

Dazu müssen in der Postfix-Konfigurationsdatei einige Einstellungen geändert werden:

`/etc/postfix/main.cf`

```
# Hier wird die Domain angegeben
mydomain = zhdk.ch
#myhostname = transporter.zhdk.ch
# Hier wird angegeben, von welchen Quellen Postfix Mails
annehmen soll
mydestination = $myhostname, localhost, localhost.localdomain,
localhost
# Hier wird der SMTP angegeben der verwendet werden soll
relayhost = SMTP.zhdk.ch
```

Filesender

Beim Filesender muss als erstes die Rechtevergabe geregelt werden, denn einige Konfigurationsdateien und Verzeichnisse müssen lesbar sein, andere hingegen nicht.

Die Verzeichnisse `Files/`, `log/` und `tmp/` müssen dem Benutzer und der Gruppe `www-data` gehören.

- `chown www-data:www-data tmp files log`
- `chown o-rwx tmp files log`
- `chgrp www-data config/config.php`
- `chmod o-rwx tmp/ files/ log/`
- `chmod g-w tmp/ files/ log/`

Die Konfigurationsdatei `/usr/local/filesender/filesender/config/config.php` muss noch der Gruppe `www-data` zugewiesen werden.

- `chown root:www-data config/config.php`

Die Rechte der Verzeichnisse und Dateien müssen wie auf dem folgenden Screenshot aussehen.

```

root@transporter:/home/dominic# ls -lah /usr/local/filesender/filesender/config/
total 44K
drwxr-xr-x  2 root    root    4.0K 2013-03-20 10:48 .
drwxr-xr-x 13 root    root    4.0K 2013-03-12 10:23 ..
-rw-r--r--  2 dominic dominic 2.5K 2013-03-13 16:18 banner.png
-rw-r-----  1 root    root    15K 2012-10-28 19:45 config-dist.php
-rw-r-----  2 root    www-data 16K 2013-03-25 10:51 config.php
root@transporter:/home/dominic# ls -lah /usr/local/filesender/filesender/
total 84K
drwxr-xr-x 13 root    root    4.0K 2013-03-12 10:23 .
drwxr-sr-x  4 root    staff    4.0K 2013-03-12 11:56 ..
-rw-r--r--  1 root    root    19K 2013-03-03 13:01 CHANGELOG.txt
drwxr-xr-x  2 root    root    4.0K 2013-03-03 20:24 classes
drwxr-xr-x  2 root    root    4.0K 2013-03-20 10:48 config
drwxr-xr-x  2 root    root    4.0K 2013-03-03 20:24 config-templates
drwxr-xr-x  2 root    root    4.0K 2013-03-03 20:24 cron
drwxr-x---  4 www-data www-data 4.0K 2013-03-26 05:54 files
drwxr-xr-x  2 root    root    4.0K 2013-03-03 20:24 includes
-rw-r--r--  1 root    root    4.0K 2013-03-01 12:09 INSTALL.txt
drwxr-xr-x  2 root    root    4.0K 2013-03-03 20:24 language
-rw-r--r--  1 root    root    1.7K 2013-03-02 20:06 LICENCE.txt
drwxr-x---  2 www-data www-data 4.0K 2013-03-26 05:54 log
drwxr-xr-x  2 root    root    4.0K 2013-03-03 20:24 pages
-rw-r--r--  1 root    root    2.4K 2013-03-01 12:07 README.txt
drwxr-xr-x  2 root    root    4.0K 2013-03-03 20:24 scripts
drwxr-xr-x  7 root    www-data 4.0K 2013-03-13 16:21 www

```

Rechte 1

Weil die temporären Dateien auch sehr gross werden können, wird der Ordner tmp/ in den Ordner files verschoben, damit alle Dateien, die beim Hochladen entstehen, auf dem NFS-Storage liegen.

- `mv /usr/local/filesender/filesender/tmp /usr/local/filesender/filesender/files/`

Die maximale Upload-Grösse muss auch noch in der Datei
/usr/local/filesender/filesender/config/config.php geändert werden.

```

$config['max flash upload size'] = '10737418240'; // Hier wird
angegeben, das mit Scripts bis zu 10 GB grosse Files
hochgeladen werden können
$config['max html5 upload size'] = '10737418240'; // Hier wird
angegeben, das mit HTML5 bis zu 10 GB grosse Files hochgeladen
werden koennen
$config["upload chunk size"]  = '2000000';//Wenn die Daten mit
HTML5 hochgeladen werden, wird ein chunk verwendet, wenn
dieser vergrössert wird, kann die Überuebertagungsrate
verbessern.

```

Weitere Einstellungen müssen auch noch in der Konfigurations-Datei config.php gemacht werden.

```

$config['admin'] = ''; // UID's (from
$config['saml uid attribute']) that have Administrator
permissions
$config['adminEmail'] = 'service.itz@zhdk.ch'; // Email
Adresse an die Meldungen gesendet werden
$config['Default TimeZone'] = 'Europe/Berlin'; //Welche
Zeitzone wird die Seite verwenden
$config['site defaultlanguage'] = 'de DE'; // Welche Sprache

```

```
wird als Standard verwendet
$config['site_name'] = 'Transporter.zhdk.ch'; // Wie sich der
Dienst selber bezeichnet
```

Da es nachvollziehbar sein soll, wer was Hoch- und Runtergeladen hat, muss folgende Option auf true geändert werden, denn so wird jeder Client protokolliert. Diese Logfiles befinden sich im Verzeichnis /usr/local/filesender/filesender/log.

```
$config["client_specific_logging"] = true; // sollen Client
geloggt werden (true/false)
```

Einstellungen für die Authentifizierung werden im Abschnitt saml settings gemacht.

```
$config['saml_email_attribute'] = 'mail'; // Attribut, welches
die E-Mailadresse angibt
$config['saml_name_attribute'] = 'cn'; // Attribut, welches
den Namen des Benutzers angibt
$config['saml_uid_attribute'] = 'SAMAccountName'; // Attribut,
welches den Benutzer identifiziert
```

Unter dem Abschnitt Server settings, kann eingestellt werden wie viele Tage ein File gespeichert werden soll, welche Suffixe nicht erlaubt sind und wieviele E-Mails pro Datei versendet werden kann.

```
$config['default_daysvalid'] = 20; // Gibt die maximale Zeit
an, die ein File gespeichert wird.
$config['ban_extension'] = 'exe,bat'; // Gibt an welche
Dateiendungen blockiert werden.
$config["max_email_recipients"] = 100; // Gibt die maximale
Anzahl gleichzeitig versendbarer E-Mails an, 0 ist
unlimitiert.
```

Damit nur auf unseren Active-Directory Server verbunden werden kann, muss bei der folgenden Option das selbst erstellte LDAP-Profil stehen.

```
$config['site_authenticationSource'] = "zhdk-ldap"; //Gibt den
verwendeten SimplaSAMLphp Authentisierungspunkt an
```

Damit der FileSender nur SSL akzeptiert, muss folgende Einstellung noch bearbeitet werden.

```
$config['forceSSL'] = true; // Soll nur SSL zugelassen werden
(true/false)
```

Bei den folgenden Optionen wird angegeben, wo welche Dateien gespeichert werden sollen.

```
$config['site_filestore'] =
'/usr/local/filesender/filesender/files/'; //Gibt den
absoluten Pfad zu dem Ordner files
$config['site_temp_filestore'] =
'/usr/local/filesender/filesender/files/tmp/'; //Gibt den
absoluten Pfad zu dem Ordner der temp Dateien
$config['site_simplesamllocation'] =
'/usr/local/filesender/simplesaml/'; //Gibt den absoluten Pfad
zum Simplesamle Verzeichniss an
$config['log_location'] =
'/usr/local/filesender/filesender/log/'; //Gibt den absoluten
Pfad zu den Logs an
```

Die folgenden Einstellungen beziehen sich auf die verwendete Datenbank.

```
$config["db_type"] = "pgsql";// pgsql or mysql, welche
Datenbank wird verwendet
$config['db_host'] = 'localhost'; //Gibt an auf welchem Host
die Datenbank i t
$config['db_database'] = 'filesender'; //Gibt den Namen der
Datenbank an
$config['db_port'] = '5432'; //Gibt den Verwendeten Port an
// database username and password
$config['db_username'] = 'filesender'; //Gibt den
Benutzernamen des Besitzers der Datenbank an
$config['db_password'] = '<Passwort>'; //Gibt das Passwort des
Benutzers an
```

Jetzt muss noch das Konfigurationsfile des Moduls Sanity Check an den richtigen Ort speichert werden, denn ohne dieses File kann der Funktionstest des FileSenders nicht durchgeführt werden:

- `cp simplesaml/modules/sanitycheck/config-templates/config-sanitycheck.php
simplesaml/config/config-sanitycheck.php`

Es ist auch möglich; den Banner, der auf der Seite angezeigt wird, zu ändern. Dazu braucht es ein Bild im Format 800x60 Pixel.

Weil die Zürcher Hochschule der Künste ein Corporate Design hat, ist das Erstellen eines solchen Logos nicht einfach. Die Logos müssen von der Grafik & Design-Abteilung der Zürcher Hochschule der Künste kommen. Es gibt aber eine Website mit Anleitungen und Downloads.

Leider war es nicht möglich, das normale Logo der Zürcher Hochschule der Künste zu verwenden, da es nur in 100%-Grösse abgebildet werden darf, das würde 5.6cm x 2.2cm bedeuten. Deswegen wird das Logo Minimalform verwendet, denn dieses darf verkleinert werden.

Das Bild wird in einem Bildbearbeitungsprogramm geöffnet, dann wird das Logo Minimalform auf eine Höhe von 60 Pixel verkleinert. Danach wird das Bild auf 800x60 Pixel vergrössert und muss als Banner.png abgespeichert werden.

Als nächstes muss dieses Bild auf den Server Transfer kopiert werden:

- scp banner.png dominic@transporter.zhdk.ch:
/usr/local/filesender/filesender/config/banner.png

Jetzt liegt das Bild am richtigen Ort, ist richtig Formatiert und wird automatisch als Banner verwendet.

Vorher



Filesender 1

Nachher



Filesender 2

Nun müssen noch die Texte des FileSender angepasst werden. Dazu gehören die Nutzungsbedingungen, das E-Mail um Dateien herunterzuladen und das E-Mail welches den temporären Benutzern gesendet wird. Damit die Formulierungen korrekt und vom Teamleiter abgesegnet sind, habe ich den Teamleiter angefragt den Willkommenstext und die E-Mails zu verfassen.

Der Willkommens Text und die Nutzungsbedingungen, werden in folgender Datei konfiguriert:

/usr/local/filesender/filesender/language/de_DE.php

```
// Login Willkommens Text
$lang["_SITE_SPLASHHEAD"] = "Willkommen bei ".
htmlspecialchars($config['site_name']);
$lang["_SITE_SPLASHTEXT"] = "Der ".
htmlspecialchars($config['site_name']) ." ist eine
Dienstleistung des ITZ und eine sichere Methode, an der ZHdK
grosse Dateien zu teilen. Mit dem Transporter kann man Daten
auch mit Personen austauschen, die nicht zur ZHdK gehören.
Melden Sie sich an um grosse Dateien über den Transporter zu
versenden oder um jemanden aufzufordern, Ihnen eine grosse
Datei über den Transporter zur Verfügung zu stellen.";
// Hier kann der Text für die Nutzungsbedingungen eingegeben
werden.
$lang["_AUPTERMS"] = " Auch bei der Nutzung des Transporters
gelten die IT-Nutzungsbedingungen der ZHdK. ";
```

Die E-Mails werden in der Haupt-Konfigurationsdatei festgelegt. Weil es sehr lange Einträge sind, werde ich nur das wichtige angeben und die komplette Konfigurationsdatei ist im Anhang.

/usr/local/filesender/filesender/config/config.php

\$config['filedownloadedemailbody']

```
<BODY>
<P>Guten Tag</P>
<P>Die unten stehende Datei wurde von der Seite {siteName} von
{filefrom} heruntergeladen.</P>
```

\$config['fileuploadedemailbody']

```
<BODY>
<P>Guten Tag</P>
<P>Die weiter unten in diesem Mail verlinkte Datei wurde auf
den {siteName} hochgeladen. {filefrom} gewährt Ihnen über den
folgenden Link Zugriff auf die Datei. Bitte laden Sie sich die
Datei herunter. Der Transporter dient nur zum Austausch von
Dateien. Die verlinkte Datei wird am {fileexpirydate}
gelöscht.</P>
```

\$config['voucherissuedemailbody']

```
<BODY>
<P>Guten Tag</P>
<P>Sie wurden von {filefrom} eingeladen, eine Datei über den
{siteName} mit jemandem zu teilen. Bitte verwenden Sie den
folgenden Link um einmalig eine Datei auf den Transporter zu
laden. Sie können dann auch festlegen, wem Zugriff zur
hochgeladenen Datei gewährt wird. Der Transporter dient nur
zum Austausch von Dateien. Die von Ihnen hochgeladene Datei
wird spätestens nach 20 Tagen wieder gelöscht.</P>
```

\$config['defaultvouchercancelled']

```
<BODY>
Guten Tag<BR><BR>Ein voucher von {filefrom} wurde
gelöscht.<BR><BR>
    <P>Freundliche Grüße</P>
```

\$config['defaultfilecancelled']

```
<BODY>
Guten Tag<BR><BR>Die Datei '{htmlfileoriginalname}' von
{filefrom} wurde gelöscht und ist nicht mehr zum Downloaden
verfügbar.<BR><BR>
    <P>Best regards,</P>
```

Als letztes muss beim Filesender noch der Cron-Job eingerichtet werden, der alle abgelaufenen Dateien und temporäre Benutzer löscht. Dieser Crone-Job ist im FileSender gespeichert und muss nun noch in die Täglichen Crons eingetragen werden.

- ```
echo "#!/bin/sh >
php -q /usr/local/filesender/filesender/cron/cron.php >
/etc/cron.daily/filesender
```

Damit er auch ausgeführt wird, muss noch die richtigen Berechtigungen auf den Crone-Job angewandt werden.

- ```
chmod 755 /etc/cron.daily/filesender
```

PostgreSQL

Damit PostgreSQL für den Filesender verwendet werden kann, muss als erstes ein Benutzer erstellt werden. Der Benutzer wird einfachheitshalber filesender genannt und das Passwort wird in einer KeePass-Datenbank gespeichert, das wiederum auf dem Filer2 abgelegt wird.

- `sudo -u postgres createuser -S -D -R -P filesender`

Jetzt muss die Datenbank noch erstellt werden; auch die Datenbank wird filesender genannt.

- `sudo -u postgres createdb -E UTF8 -O filesender filesender`

Wenn die Datenbank steht, muss noch der Inhalt erstellt werden. Dazu hat FileSender ein Skript:

- `psql -h localhost filesender filesender <
/usr/local/filesender/filesender/scripts/filesender_db.sql`

PHP5

Damit grosse Dateien versendet werden können, müssen in dem Konfigurationsfile `/etc/php5/apache2/php.ini` einige kleine Änderungen vorgenommen werden.

```
;Die Inputtime wird auf unlimitiert gesetzt, damit auch
langsamen Leitungen grosse Dateien versendet werden können.
max_input_time = -1
;Den max-Upload wird auf 10240M (10 GB) gesetzt, damit auch
grosse Daten versendet werden können.
upload_max_filesize = 10240M
;Hier wird die maximale Grösse für den Post-Upload angegeben.
Das ist der max-Upload + POST-Zusätze. Deswegen ist auch etwas
grösser als der upload_max_filesize.
post_max_size = 10500M
;Hier kann das temporäre Upload-Verzeichnis angegeben werden.
Das Verzeichnis muss genug Platz für die temporären Upload-
Daten haben.
upload_tmp_dir = /usr/local/filesender/files/tmp/
;Hier wird angegeben, dass das Error-Log eingeschalten ist.
log_errors = On
;Hier wird angegeben, in welches Logfile die Error Meldungen
geschrieben werden
error_log = php_errors.log
;Gibt an, ob das Cookie nur über das HTTP-Protokoll zugänglich
ist oder nicht
session.cookie_httponly = On
```

Nun muss noch im Suhosin – den Security Patch für PHP – die maximale Länge geändert werden.

```
; Hier wird die Länge der maximal zugelassenen value geändert
suhosin.get.max_value_length = 2048
```

Um die ganzen Einstellungen zu aktivieren, muss Apache2 neu gestartet werden.

- `/etc/init.d/apache2 restart`

Apache2

In den Apache2-Einstellungen geht es hauptsächlich um die HTTPS-Anbindung und um Umleitung von HTTP auf HTTPS.

Diese Einstellungen werden in den Dateien im Verzeichnis `/etc/apache2/sites-available/` vorgenommen

Als erstes wird die Umleitung von HTTP auf HTTPS eingestellt. Dies wird in der Datei `/etc/apache2/sites-available/default` gemacht. Dazu wird die Datei auf `old.default` umbenannt und eine neue mit Namen `default` erstellt, damit die Standard-Konfiguration nicht verloren geht.

- `mv /etc/apache2/sites-available/default /etc/apache2/sites-available/old.default`

`nano /etc/apache2/sites-available/default`

```
VirtualHost *:80>
#Mit folgendem eintrag wird die ganze verbindung auf die HTTPS
Seite umgeleitet
Redirect permanent / https://transporter.zhdk.ch
</VirtualHost>
```

Nun muss `default-ssl` auch umbenannt werden, damit die Datei `filesender-ssl` auf `default-ssl` umbenannt werden kann. So kann man sich einige Zeit sparen, da nur wenige Korrekturen vorgenommen werden müssen und der Rest schon in der Datei steht.

- `mv /etc/apache2/sites-available/default-ssl /etc/apache2/sites-available/old.default-ssl`
- `mv /etc/apache2/sites-available/filesender-ssl /etc/apache2/sites-available/default-ssl`

Zertifikate

Als nächstes muss noch das Server-Zertifikat und der Schlüssel auf den Transporter kopiert werden. Die Zertifikate liegen auf einem unserer Storage-Server.

[\\filer\Services\SER_SUP_ITZ\2_Betrieb\22_Infrastruktur\223_Server\Certificates\transporter](#)

Die Zertifikate werden auf den Transporter gespeichert, indem der Inhalt der Zertifikate per Copy & Paste in neu generierte Files, im richtigen Verzeichnis gespeichert werden.

- `nano /etc/ssl/private/transporter.key`
- `nano /etc/ssl/certs/transporter.crt.pem`

SSL Einstellungen

Nun muss noch die HTTPS-Seite Konfiguriert werden. Dies kann man entweder tun, indem man eine eigene Konfigurationsdatei erstellt und diese in den Ordner `/etc/apache2/sites-available/` speichert oder man nimmt die vorhandene Datei `default-ssl/filesender-ssl` und bearbeitet diese.

/etc/apache2/sites-available/default-ssl

```
<IfModule mod_ssl.c>
<VirtualHost _default_:443>
    #Gibt den Namen des Servers an
    ServerName transporter.zhdk.ch
    #Gibt an wer der Admin des Servers ist
    ServerAdmin webmaster@localhost
    #Gibt an wo das Hauptverzeichnis liegt
    DocumentRoot /usr/local/filesender/filesender/www
    <Directory />
        Options FollowSymLinks
        AllowOverride None
    </Directory>
    Alias /filesender /usr/local/filesender/filesender/www
    <Directory "/usr/local/filesender/filesender/">
        Options FollowSymLinks MultiViews
        DirectoryIndex index.php
        AllowOverride None
        Order deny,allow
        Allow from all
    </Directory>
    Alias /simplesaml /usr/local/filesender/simplesaml/www
    <Directory "/usr/local/filesender/simplesaml/www">
        AllowOverride None
        Options FollowSymLinks MultiViews
        Order deny,allow
        Allow from all
    </Directory>
    #Gibt an, wo das Errorlog gespeichert werden soll
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/ssl_access.log combined
    #Gibt an wie geloggt werden soll
    LogLevel warn
    SSLEngine on
    #Gibt an wo das verwendete Zertifikat und der
    Schlüssel liegen
    SSLCertificateFile
    /etc/ssl/certs/transporter.zhdk.ch.crt.pem
    SSLCertificateKeyFile /etc/ssl/private/transporter.key
</VirtualHost>
</IfModule>
```

Wenn die Datei fertig konfiguriert ist, muss sie noch aktiviert werden, falls nicht default-ssl verwendet wurde, denn diese wurde weiter oben schon aktiviert.

Damit die Konfiguration angewendet wird, muss noch der Apache2 neu gestartet werden.

- /etc/init.d/apache2 restart

SimpleSAMLphp

Als letztes muss noch die Anbindung an das Active-Directory erfolgen. Dies wird mit dem Tool SimpleSAMLphp realisiert.

Als erstes braucht SimpleSAMLphp einen Salt, um - wenn nötig - einen geheimen Hash zu erstellen. Ein Salt kann mit folgendem Befehl erstellt werden:

- `tr -c -d '0123456789abcdefghijklmnopqrstuvwxyz' </dev/urandom | dd bs=32 count=1 2>/dev/null;echo`

Die Einstellungen des SimpleSAMLphp sind in verschiedenen Dateien gespeichert. Die grundlegenden Einstellungen sind in der Datei config.php gespeichert.

simplesaml/config/config.php

```
//Hier wird der Salt eingetragen
'secretsalt' => 'ut71eaqblv291djmp9mcd723ctjauxuc',
//Bei dieser Option wird das Passwort des Admins bestimmt
'auth.adminpassword' => '5iMp13:P4s5',
//Hier wird festgelegt, wer bei technischen Problemen
kontaktiert werden soll
'technicalcontact_name' => 'Dominic Naepflin',
'technicalcontact_email' => 'webmaster@zhdk.ch',
```

Die ganzen LDAP-Einstellungen werden nicht in der Datei config.php gespeichert, sondern in einer separaten Authentisierung-Konfigurationsdatei.

simplesaml/config/authsources.php

```
//Gibt den Namen der LDAP-Konfiguration an
'zhdk-ldap'=>array(
    'ldap:LDAP',
//Gibt an, auf welchen LDAP-Server verbunden werden soll.
    'hostname'=>'ldap.zhdk.ch',
//Gibt an, ob TLS/SSL verwendet werden soll
    'enable_tls' => TRUE,
//Der Pfad zu den Benutzern. Ist deaktiviert, da nicht
benötigt, wenn die Suche aktiv ist.
    //'dnpattern' =>
'sAMAccountName=%username%,dc=vera,dc=hgka,dc=ch',
//Anstelle eines Pfades zu den Benutzern, ist hier die
Möglichkeit die Benutzer zu suchen.
    'search.enable' => TRUE,
//Gibt die Suchbasis an
    'search.base' => 'dc=vera,dc=hgka,dc=ch',
//Welche Attribute sind mit dem Username identisch und sollen
bei der Suche benutzt werden.
    'search.attributes' => array('sAMAccountName',
'mail'),
//Gibt den Benutzer und das Passwort für den Suchvorgang an
    'search.username' => 'ldapsearch',
    'search.password' => '<Passwort>',
...
)
```

Meilenstein 2

Das installieren und die Konfiguration des Transporters ist beendet. Das Installieren würde sicher schneller gehen, wenn man die verschiedenen Programme wie PHP, SimpleSAMLphp etc. schon kennt und nicht erst die Einstellungen suchen muss. Deswegen wäre eine genauere Planung von Vorteil gewesen, da dort schon sich herausgestellt hätte, welche Programme genutzt werden und man hätte sich darauf vorbereiten können.

Benutzerdokumentation

Wozu können sie diese Seite nutzen?

Die Seite Transporter.zhdk.ch ist dazu gedacht kleine und grosse Dateien an externe oder interne Benutzer zu senden. Es ist auch möglich, externen Benutzern einen temporären Benutzer zu erstellen, mit dem sie Dateien hochladen und versenden können.

Max. Upload Grösse einer Datei: 10GB

Max. Ablaufzeit für Dateien: 20 Tage

Max. E-Mail Empfänger: 100

Wie funktioniert sie?

Als erstes müssen Sie sich auf die Seite <https://transporter.zhdk.ch> mit dem Firefox oder Safari verbinden(Internet Explorer unterstützt nicht die vollständigen Funktionalität). Auf der Seite müssen Sie auf den Button „Einloggen“ drücken um auf die Seite zu gelangen auf der Sie sich einloggen können.

Auf dieser Seite müssen Sie ihr Benutzername(ohne @login.itz) und Passwort eingeben und mit „Anmelden“ bestätigen.

Dann werden Sie auf eine Seite weitergeleitet, auf der Sie auswählen können, was Sie machen wollen.

Welche Möglichkeiten haben Sie?

Datei senden: Mit dem Transporter können sie Daten versenden, die Sie auf der Transporter Seite hochgeladen haben.

The screenshot shows the 'Datei senden' (Send File) interface of the Transporter.zhdk.ch website. At the top, there is a navigation bar with the 'zhdk' logo and buttons for 'Datei senden', 'Gast einladen', 'Meine Dateien', 'Hilfe', 'Impressum', and 'Abmelden'. Below the navigation bar, a 'Willkommen' (Welcome) message is displayed on the left, and 'HTML 5' with a green checkmark is on the right. The main content area is titled 'Datei senden' and includes a sub-header 'Vorname Nachname - Benutzername'. The form contains several input fields: 'An:' (recipient email), 'Von:' (sender email, pre-filled with 'Vorname.nachname@zhdk.ch'), 'Betreff: (optional)' (subject), and 'Nachricht: (optional)' (message). To the right of these fields is a numbered list of steps: 1. 'Geben Sie die E-Mail Adressen der Empfänger ein', 2. 'Setzen Sie das Ablaufdatum', 3. 'Suchen Sie Ihre Datei', and 4. 'Senden klicken'. Below the message field is the 'Ablaufdatum:' (expiration date) set to '07.04.2013'. The 'Datei wählen:' (select file) section includes a file selection button and a 'Durchsuchen...' (browse) button. At the bottom, there is a checkbox labeled 'Ich bin mit den Nutzungsbedingungen einverstanden. [Anzeigen/Verstecken]' (I agree with the terms of use. [Show/Hide]).

Filesender 3

Der Aufbau der Benutzeroberfläche ist ähnlich wie ein E-Mail Formular, da es ein E-Mail versendet, das den Link zur hochgeladenen Datei enthält.

Halten Sie sich an die vier Punkte, sie beschreiben genau was gemacht werden muss um eine Datei hochzuladen und ein Link zur Datei zu versenden.

Gast einladen: Sie können einer externen Person ein temporäres Konto erstellen, mit dem er/sie Dateien hochladen und versenden kann. Der FileSender verwendet den Begriff „Voucher“ anstelle von Gast, oder temporärer Benutzer.

Gast einladen

Ein Voucher erlaubt es einem Anderen, Ihnen eine Datei zu schicken.
Um einen Voucher zu erstellen, geben Sie seine Email Adresse ein und klicken sie auf 'Voucher senden'.
Dem Empfänger wird eine E-Mail mit einem Link zum Voucher erhalten.

Voucher senden an:

Ablaufdatum: 07.04.2013

Voucher senden

An	Erstellt	Ablaufdatum	
beispiel@gmail.com	18.03.2013	19.03.2013	

Filesender 4

Um einer externen Person ein temporären Benutzer zu erstellen, müssen Sie im Feld „Voucher senden an“ seine E-Mail-Adresse eingeben. Dazu kann noch ein Ablaufdatum des temporären Benutzers angegeben werden. Wenn kein Ablaufdatum bestimmt wird, ist es automatisch 20 Tag nach dem hochladen der Datei.

In der Liste am unteren Ende der Website werden die von Ihnen erstellten temporären Benutzer, mit Erstellungs- und Ablaufdatum aufgeführt. Löschen kann man den Benutzer indem man auf das blaue Viereck mit dem roten Kreis klickt.

Meine Medien: Auf dieser Unterseite werden ihre Dateien angezeigt, welche Sie auf den Server gespeichert haben.



The screenshot shows the Filesender 5 web interface. At the top, there is a large 'Z' logo and the text 'hdk'. Below this, there are several buttons: 'Datei senden', 'Gast einladen', 'Meine Dateien', 'Hilfe', 'Impressum', and 'Abmelden'. A 'Willkommen' message is displayed on the left, and 'HTML5' with a green checkmark is on the right. The main section is titled 'Meine Dateien' and contains a table with the following data:

	An	Von	Dateiname	Größe	Betreff	Nachricht	Erstellt	Ablaufdatum	
	 beispiel @beispiel.com	Mir	beispiel.bt	3.32 GB	test18		18.03.2013	07.04.2013	

Filesender 5

Die von Ihnen hochgeladene Dateien werden wie auf dem Bild (Filesender 5) mit allen Attributen angezeigt. Hier können sie wie bei den Voucher ganz rechts die Datei löschen, indem Sie auf das blaue Viereck mit dem roten Kreis klicken.

Testen

Der Transporter läuft und alle Konfigurationen wurden vorgenommen, jetzt muss nur noch überprüft werden, ob alles so funktioniert, wie wir uns das vorstellen. Dazu werden einige Tests durchgeführt und dazu Testprotokolle erstellt.

Die Tests werden vom Arbeitsgerät von Dominic Näpflin aus gemacht und dokumentiert. Es ist ein PC mit 8 GB RAM, Intel Core2 Quad Q9650@3,00GHz, Windows 7 64 Bit und einem 100MBit/s Netzwerkadapter.

Funktionen

Testfall	Ereignisse	Ergebnis
Ist die Seite transporter.zhdk.ch nur unter HTTPS erreichbar	Wenn man im Webbrowser transporter.zhdk.ch eingibt, wird man automatisch auf https://transporter.zhdk.ch weitergeleitet. Wenn der Redirect nicht aktiv ist und man nicht weitergeleitet wird, verweigert der FileSender die Session.	Funktioniert
Kann ein ZHdK-Benutzer eine Datei hochgeladen und an einen ZHdK-Benutzer Versenden?	Der ZHdK Benutzer kann ohne Probleme einloggen und das versandene E-Mail kommt nach kurzer Zeit im E-Mail-Konto des Empfängers an.	Funktioniert
Kann ein ZHdK-Mitarbeiter einem externen Benutzer einen temporären Benutzer erstellen?	Das Einloggen funktionierte ohne Probleme und ich konnte einem Google-Mail Konto einen temporären Benutzer erstellen. Das E-Mail kam auch nach kurzer Zeit an. Auch das Einloggen mit dem temporären Benutzer funktioniert.	Funktioniert
Kann ein externer Benutzer (mit Gast Benutzer) eine Datei hochladen und versenden?	Mit dem temporären Benutzer des Google-Mail Kontos konnte ohne Probleme eine Datei hochgeladen und versandt werden. Das Mail des FileSenders ist auch im Namen des Google-Mail angekommen.	Funktioniert
Kann ein ZHdK-Benutzer eine Datei an einen externen Benutzer senden?	Das Hochladen funktioniert ohne Probleme, auch das E-Mail mit dem Link kam an. Mit dem Link konnte man auch ohne Probleme die Datei herunterladen. Der Versender der Datei erhält sogar eine Erinnerung, wer die Datei heruntergeladen hat.	Funktioniert
Wird die Willkommens Nachricht richtig angezeigt?	Es wird auf der Startseite der richtige Text „Willkommen bei Transporter.zhdk.ch“ angezeigt. Der Transporter.zhdk.ch ist eine Dienstleistung des ITZ und eine sichere Methode, an der ZHdK grosse Dateien zu teilen. Mit dem Transporter kann man Dateien auch mit Personen austauschen, die nicht zur ZHdK gehören. Melden Sie sich an um grosse Dateien über den Transporter zu versenden oder um jemanden aufzufordern, Ihnen eine grosse Datei über den Transporter zur Verfügung zu stellen.“	Funktioniert

Wird der richtige E-Mail-Text angezeigt in den verschiedenen E-Mails?	Die E-Mails werden im Anhang abgelegt. Datei zum Runterladen: Richtiger Text Datei gelöscht: Richtiger Text Temporärer Benutzer: Richtiger Text Temporärer Benutzer gelöscht: Richtiger Text E-Mails sind im Anhang aufgelistet.	Funktioniert
Können Dateien nur bis 10GB hochgeladen werden?	Dateien die grösser als 10GB sind werden von dem FileSender nicht angenommen. Es erscheint eine rote Schrift unter dem Datei Wählen Feld: Datei darf nicht grösser sei als 10 GB. Bitte wählen Sie eine andere Datei“.	Funktioniert
Kann ein Downloadmanager verwendet werden?	Es sind zwei Downloadmanager für diesen Test verwendet worden jDownloader und Free Download Manager. Der jDownloader konnte mit dem Link nichts anfangen, der Free Download Manager hingegen bekommt den Download, wenn das Firefox Plug-In aktiv ist.	Funktioniert nicht
Werden die Dateien nach der Ablaufzeit gelöscht?	Die Dateien wurden nicht gelöscht. Ein Fehler im Cronjob, mit der Einbindung, verhinderte das. Nach einer Besprechung mit Herr Filadoro kamen wir auf die Fehlerquelle und behoben diese. Erneuter Test verlief erfolgreich.	Funktioniert
Werden die Benutzer nach dem ablaufen das Ablaufdatum gelöscht?	Benutzer wurden nicht gelöscht, nach genauerem nachlesen und Besprechung mit Herr Filadoro stellte sich heraus, das in der Konfiguration des Cronjobs Fehler unterlaufen sind. Der Fehler wurde behoben und der Test erneut durchgeführt. Alle Benutzer mit einem abgelaufenen Ablaufdatum wurden gelöscht.	Funktioniert
Können die Browser Safari ab V.6, Firefox ab V. 17 ESR, Internet Explorer ab V. 9 die Seite richtig anzeigen?	Safari: HTML5 funktioniert und alles wird richtig angezeigt. Firefox: HTML5 funktioniert und alles wird richtig angezeigt. Internet Explorer: In Version 9 kann der Internet Explorer kein HTML5 anzeigen. Somit kann er nur über das Flash hochladen(ingeschränkte Möglichkeiten).	Funktioniert teilweise
Kann eine Datei Versand werden, mit weniger als 10 Klicks?	Es reichen 4 Klicks um eine Datei zu versenden, solange nur die Buttons gezählt werden.	Funktioniert
Das Automatische Loggen funktioniert.	Die einzelnen Benutzer werden in einem für jeden Benutzer eigenes Logfile geloggt. Das Logfile ist nicht sehr übersichtlich, aber die wichtigsten Angaben sind nach suche im Logfile zu finden. Ausserdem loggt apache jede Anmeldung an der AD.	Teilweise

Performance

Der Test, ob der Transporter die Dateien gleichschnell wie der FTP verschieben kann wird aufwändig. Denn ich werde als erstes messen, wie lange es dauert von innerhalb des ZHdK-Netzwerkes eine Datei auf den FTP-Server zu verschieben. Das gleiche wird auch noch von ausserhalb des ZHdK-Netzwerkes getestet. Danach werde ich das gleiche über den Filesender testen.

Die 100 MB, 1 GB und 5 GB Files erstelle ich mithilfe des Programms dd auf einer Linux Maschine.

- `dd if=/dev/urandom of=/tmp/test-100mb.txt count=204800`
- `dd if=/dev/urandom of=/tmp/test-1gb.txt count=2048000`
- `dd if=/dev/urandom of=/tmp/test-5gb.txt count=10240000`

Übertragungsart	FTP	Transporter/FileSender
Intern 100MB	9 Sekunden	1 Minute 10 Sekunden
Extern 100MB		
Intern 1GB	1 Minute 28 Sekunden	11 Minuten 58 Sekunden
Extern 1GB		
Intern 5GB	7 Minuten 22 Sekunden	
Extern 5GB		

Nach den ersten Tests aus dem internen Netzwerk war klar, dass entweder der FileSender langsam im Übertragen von Dateien ist, oder einige Einstellungen nicht optimal eingerichtet wurde. Deswegen habe ich den Test abgebrochen und bat die zwei Linux und Webserver Experten Herr Roman Haefeli und Herr Luigi Filadoro das Problem mit mir anzugehen und zu testen.

Der Test wurde ein bisschen verändert und zwar wird der FileSender mit dem Tool Rsync verglichen, da man mit diesem Tool Dateien ohne Probleme auf den Transporter kopieren kann. Das Ergebnis war eindeutig, während der FileSender immer stark schwankte und maximal auf 20 Mbps kam, konnte der Rsync die ganze Leitung des Computers ausnutzen und kam auf 99Mbps.

Als erstes haben wir die php Erweiterung Suhosin deinstalliert. Suhosin ist ein Sicherheitstool welches unter Umständen die geringe Geschwindigkeit erklären könnte.

- `apt-get remove php5-suhosin --purge`
- `/etc/init.d/apache2 restart`

Das Ausschalten des Suhosin erhöhte die Upload-Rate auf 30Mbps. Diese Übertragungsrate war immer noch zu gering, deswegen erhöhten wir in der php.ini das Limit für das verwendete RAM auf 1GB.

```
; Das Memory Limit wird erhöht um das Übertragen zu verbessern
memory_limit = 1024M
```

Das Erhöhen des verwendeten RAM brachte nicht eine grosse Veränderung in der Übertragungsrate. Deswegen schauten wir uns auch noch die Apache2 Konfiguration an. Wir entschieden uns die unnötigen Module auszuschalten, da diese den Apache2 auch verlangsamen können. Leider brachte das keine Verbesserung in der Übertragungsrate.

Weil wir keine weiteren Einstellungsmöglichkeiten gefunden haben, machten wir eine kleine Pause und danach ein Brainstorming, was diese schlechte Übertragungsrate verursachen könnte. Eine Idee war der NFS, denn nicht nur der Speicher für die Dateien sind auf einem NFS-Storage, sondern auch das System durch das Virtualisieren.

Deswegen kopierten wir den Server auf das Development-System, das auf lokalen Festplatten gespeichert ist. Diese Veränderung erhöhte die Datenrate auf ca. 50 Mbps, als wir den NFS-Storage(files/) auch abgehängt erhöhte sich die Datenrate sogar auf ca. 90 Mbps.

Nach Angaben von Roman Haefeli, entsteht das Problem wahrscheinlich, weil PHP relativ häufig auf Dateien zugreift, auch wenn es nur darum geht zu überprüfen, wann eine Datei das letzte Mal verändert wurde. Weil NFS ein verteiltes Datensystem ist, werden Dateien nicht im RAM gecached und dies führt dazu, dass jeder noch so triviale Dateizugriff zu einer Abfrage auf dem Server führt. Das kann einige Anwendungen verlangsamen, wie bei uns der FileSender.

Als möglicher Lösung schlägt er vor, dass der Server als eigene Image-Datei, die auf einem NFS liegt betrieben werden könnte. Denn so wird dem System vorgaukelt das es ein Ext4-Dateisystem hat und so die Dateien gecached werden. Dies könnte den FileSender schneller machen, da nicht mehr so viele Dateizugriffe stattfinden.

Fazit

Der FileSender läuft und erfüllt fast alle getesteten Vorgaben, nur die Übertragungsrate ist nicht so hoch wie erwünscht. Leider haben wir nicht genügend Zeit und Ressourcen den Vorschlag von Roman Haefeli umzusetzen. Deswegen wird der FileSender so betrieben wie er installiert wurde.

Meilenstein 3

Die Testphase konnte einigermaßen erfolgreich beendet werden. Leider konnte nicht alle Anforderungen erreicht werden, was zum Teil an der Software und dem verwendeten Protokoll liegt, oder am nicht optimal geplanten vorgehen und Infrastruktur, wie der NFS-Storage der alles verlangsamt.

Bei einem nächsten Mal, würde ich mich im Vorfeld schlau machen, ob solche Probleme auftreten können. Denn dann kann man Vorbereitungen treffen, die solche Probleme vorbeugen.

Abgabe

In der Abgabe muss die Installations- und Konfigurationsdokumentation auf die ITZ interne Wikipedia kopiert werden, damit jeder Administrator ohne Probleme auf die Dokumentation zugreifen kann. Auch die Benutzerdokumentation muss auf das ITZ Service-Portal geladen werden, damit die Benutzer auch darauf zugreifen können.

Ausserdem muss das Programm noch dem Teamleiter vorgeführt werden.

Meilenstein 4

Das Projekt ist beendet und das Produkt Transporter.zhdk.ch steht und ist zum gebrauchen freigegeben.

Schlusswort

Das Projekt ist nun fertig und ich kann ein Resümee ziehen.

Das Projekt fand ich persönlich eine sehr gute Auswahl für die IPA, denn so konnte ich auch mal in die „Cloud“ schauen und verstehen was damit gemeint ist. Auch der Lehreffekt war vorhanden, denn ich kannte einige Programme die verwendet wurden gar nicht oder nur flüchtig und jetzt verstehe ich sie, bis zu einem gewissen Punkt.

Ich würde, wenn ich noch einmal ein solches Projekt leiten würde einiges anders machen. Unter anderem würde ich während der Evaluation überprüfen, ob das Programm überhaupt die von uns gewünschte Leistung bringen kann, mit den verwendeten Protokollen etc. Ausserdem würde ich bei spezifischen Problemen, zum Beispiel bei der Performance schneller mit den Experten in Verbindung setzen.

Es gab aber auch einige Dinge die sehr gut funktioniert haben, wie ich sie geplant habe, zum Beispiel würde ich die Versionierung, von Konfigurationsdateien und Dokumenten wieder mit GitHub machen, denn es ist einfach einzusetzen, von überall zugänglich und es kann nachvollzogen werden, was gemacht wurde. Oder das Teilen der Installation und der Konfiguration fand ich sehr praktisch, denn so kann man die Installation bei installierten Paketen verkürzen und nur die Konfiguration durch machen.

Mit dem Endprodukt bin ich sehr zufrieden, vor allem dass ich es ohne grössere Probleme aufsetzen konnte. Aber nicht nur wegen dem, sondern auch weil fast alle Anforderungen erfüllt werden konnten und ich nicht so viel Hilfe brauchte wie erwartet.

Abkürzungen / Fachbegriffe

ITZ = Das Informationstechnologie-Zentrum ist die Informatik Abteilung der ZHdK

Salt = Ist eine Bezeichnung einer zufällig gewählten Zeichenfolge, die dazu verwendet wird Passwörter oder Andere Dateien verschlüsselt zu übertragen.

Saml=Die Security Assertion Markup Language ist ein XML-Framework das von dem OASIS-Konsortium entwickelt wird, mit Fokus auf Single Sign-on, Verteilte Transaktionen und Autorisierungsdienste.

ZHdK = Zürcher Hochschule der Künste

Quellen

Konzept

<http://www.indoit.com/de/services/technische-dokumentation-software-erstellen.htm>
<http://anleitung-tipps.anleiter.de/wie-kann-man-ein-konzept-schreiben-vorlage>
<http://www.access-im-unternehmen.de/index1.php?id=300&BeitragID=263>
<http://moodle.bzu.ch>

Installations- & Konfigurationsdokumentation

Filesender

https://www.assembla.com/spaces/file_sender/wiki/Installation_-_Linux_Source
https://www.assembla.com/wiki/show/file_sender/Administrator_reference_manual

Apache2

<http://httpd.apache.org/docs/2.2/mod/core.html#>
http://www.linode.com/wiki/index.php/Apache2_SSL_in_Ubuntu

SimpleSAMLphp

<http://simplesamlphp.org/docs/1.8/ldap:ldap>
<http://www.worldgoneweb.com/2013/installing-simplesamlphp-and-use-it-as-sp-and-idp-for-development-env-only/>

PHP5

<http://www.isp-star.at/index.asp?file=php-upload-files.asp>
http://www.hardened-php.net/suhosin/configuration.html#suhosin.post.max_value_length

Abkürzungen/Fachbegriffe

http://de.wikipedia.org/wiki/Security_Assertion_Markup_Language