Odej Kao · Thomas Hildmann (Hrsg.)

Cloudspeicher im Hochschuleinsatz

Proceedings der Tagung „Cloudspeicher im Hochschuleinsatz“
am 05. und 06. Mai 2014 am IT-Service-Center (tubIT) der
Technischen Universität Berlin

Universitätsverlag der TU Berlin

Technische Universität Berlin

Odej Kao | Thomas Hildmann (Hrsg.)
Cloudspeicher im Hochschuleinsatz
Proceedings

Cloudspeicher im Hochschuleinsatz

Proceedings der Tagung „Cloudspeicher im Hochschuleinsatz“
am 05. und 06. Mai 2014 am IT-Service-Center (tubIT) der
Technischen Universität Berlin

Herausgeber:
Odej Kao | Thomas Hildmann

Universitätsverlag der TU Berlin

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de/ abrufbar.

Universitätsverlag der TU Berlin, 2014
http://www.univerlag.tu-berlin.de

Fasanenstr. 88, 10623 Berlin
Tel.: +49 (0)30 314 76131 / Fax: -76133
E-Mail: publikationen@ub.tu-berlin.de

Umschlagfoto:
theaucitron | https://www.flickr.com/photos/theaucitron/5810163712 | CC BY-SA 2.0
https://www.flickr.com/photos/theaucitron/5810163712

Druck: docupoint GmbH
Satz/Layout: J. Bechstein, T. Gebhardt

ISBN 978-3-7983-2697-2 (print)
ISBN 978-3-7983-2698-9 (online)

Zugleich online veröffentlicht auf dem Digitalen Repositorium Technische Universität Berlin:
URL http://opus4.kobv.de/opus4-tuberlin/frontdoor/index/index/docId/5226
URN urn:nbn:de:kobv:83-opus4-52266
[http://nbn-resolving.de/urn:nbn:de:kobv:83-opus4-52266]

Inhalt

Vorwort

Thomas Hildmann

Am 1. Mai 2013 startete die TU Berlin ihren Sync & Share Dienst auf Basis von ownCloud für alle Studierenden (R. Hager, TU Berlin, S. 70). Wenige Tage später wurde der Dienst auch für Mitarbeiterinnen und Mitarbeiter der TU Berlin freigegeben.

Schon während der Betaphasen zum Dienst erreichten uns zahlreiche Anfragen anderer Hochschulen. Von Fragen zu Implementierungsdetails zum Nutzerverhalten, über Fragen zum Datenschutz bis hin zu organisatorischen Fragen reichte die Bandbreite.

Dies veranlasste uns dazu für den 16. August 2013 einen ownCloud Workshop für Hochschulen anzubieten. Auf dieser ersten Veranstaltung besuchten uns bereits 25 Teilnehmende. Der Workshop umfasste Vorträge von ownCloud, dem DFN und der TU Berlin. Auf Tagungen und Workshops im ZKI und DFN zeigte sich, dass das Thema jedoch weit vielfältiger und das Interesse stark genug für eine größere Veranstaltung war. Aus diesem Grund organisierten wir zum 5. und 6. Mai 2014 die Folgeveranstaltung mit 11 Vorträgen und dem hier vorliegendem Tagungsband mit mehr als 50 Teilnehmerinnen und Teilnehmern.

Das Thema Cloudspeicher an Hochschulen ist vergleichsweise neu. Die verschiedenen Hochschulen sind in sehr unterschiedlichen Phasen in Bezug auf die Einführung dieser Dienste. Während einige wenige Hochschulen bereits seit einigen Monaten oder Jahren einen solchen Dienst betreiben, ist man an anderen Hochschulen noch in einer Test- oder Implementierungsphase oder befindet sich noch im Auswahl- oder Ausschreibungsprozess.

Es handelt sich um eine neue Dienstklasse, die eigenen Regeln und Anforderungen folgt und zu der es bislang kaum veröffentlichte Erfahrungen gibt. So stellten wir im Austausch fest, dass von sehr unterschiedlichen Prognosen in Bezug auf Nutzerzahlen und Nutzerverhalten ausgegangen wird. Die Spanne reicht hier von 10–80 % der potentiellen Nutzer. Ausgehend von dieser Unsicherheit im Bereich von 70 % der Benutzer stellt sich dann die Frage nach der Bereitstellung von Hard- und Software in einer geeigneten Skalierung.

Dass das Thema Cloudspeicher kein nationales Phänomen ist zeigt, dass sich auch das SWITCH (J.-C. Fischer, SWITCH, S. 25) mit dem Thema auseinandersetzt. Auch wurde Dr. Vogl (R. Vogl, WWU, S. 5) bereits 2013 zur EUNIS Konferenz nach Riga eingeladen, um über die Vorhaben zur NRW-Cloud zu referieren. Zum Juni wurde ich zu einem Vortrag nach Madrid auf dem DCPerf'14 eingeladen.

Weltweit treiben uns die gleichen Motivationen: Dropbox wurde 2007 gegründet und beendete 2010 offiziell die Betaphase. Der Dienst steht seitdem für alle gängigen Plattformen via Browser und vor allem auch auf mobilen Endgeräten zur Verfügung. Die Synchronisation der Daten über alle Geräte und Geräteklassen hinweg wurde ein Megaerfolg und stellte einen entscheidenden Mosaikstein zum Erfolg der Tablet-PCs dar. Neben Dropbox stehen zahlreiche weitere Dienste wie iCloud, Google Drive, Box, SkyDrive, Wuala, u. s. w. mit unterschiedlichen Ausprägungen, aber ähnlichen Aufgaben zur Verfügung. Es gibt jedoch einige entscheidende Gründe, die Daten im eigenen Haus oder bei einem wohl gewählten Partner zu halten. Dabei ist die Unabhängigkeit in Bezug auf Preisgestaltung und Konditionen nicht zu vernachlässigen. Der meist genannte Grund ist jedoch die Datensicherheit. Begonnen beim Thema Datenschutz, das unabhängig von Anbietern, Produkten etc. adressiert werden muss, über Regelungen zur Verwendung zur Datenablage, Archivierung, Löschung etc. bis hin zu Fragen des Schlüsselmanagements, wenn mit kryptographisch gesicherten Lösungen gearbeitet wird (S. Schwarz, UniBW München, S. 50).

Ein weiterer Grund, von den klassischen Cloudspeicher-Diensten abzuweichen, ist die Integration in die eigene Infrastruktur (P. Fuhrmann, DESY, S. 61), die eigenen Prozesse oder die Verknüpfung mit anderen Daten. Der Integrationsgrad in Bezug auf die Bereitstellung des Dienstes für die Nutzer reicht von einer Shibboleth-Anbindung über eine Registrierung mittels Provisioningsportal bis hin zur vollständigen IDM-Integration, die jedem Mitglied der Einrichtung automatisch Cloudspeicher zur Verfügung stellt.

Datensicherheit und einfache Integration stellt für viele Nutzer aber noch keinen Grund dar, den Universitätsdienst dem kostenlosen Standardanbieter vorzuziehen. Um diese Nutzer zu erreichen, bedarf es geeigneter Mehrwertfunktionen, die z. B. speziell auf ihr Studium oder ihre Tätigkeit abgestimmt sind. Vor diesem Hintergrund bieten gerade OpenSource Projekte besondere Möglichkeiten (A. Khalatyan, AIP, S. 47), um solche speziell auf die Anwendungsfelder zugeschnittenen Mehrwertdienste anzubieten.

Auf die Frage, wie die Hochschule zu einem eigenen Cloudspeicher-Dienst kommt, gibt es viele verschiedene Antworten, die den jeweiligen Anforderungen und Möglichkeiten der Hochschule entspringen. So reicht das Konzept für die Erbringung der Verfügbarkeit des Dienstes von der Entscheidung, schlicht keine Redundanz anzubieten, da bei einem Sync-Dienst die Daten ohnehin an mehreren Stellen zur Verfügung stehen und somit kurze Ausfälle zu keinen Arbeitseinschränkungen führen, über eine simple Active/Passive-Implementierung bis hin zu großen Clusterlösungen mit Loadbalancern oder Konzepten zum automatisierten Roll-Out weiterer Clustermitglieder.

Unsere Beiträge beschreiben Lösungen basierend auf unterschiedlichen Produkten. So sind mindestens die Produkte ownCloud, PowerFolder (N. Schlitter, KIT, S. 40), InSync (D. Rosendahl, RWTH Aachen, S. 33) und TeamDrive (S. Schwarz, UniBW München, S. 50) im Einsatz. Aber auch wer einen Clusterdienst aus verschiedenen Gründen nicht im eigenen Haus betreiben will, hat verschiedene Optionen. So sind Lösungen von Dimension Data (U. Baur, SSP Europe, S. 83) und T-Systems (M. Jürgens, DT, S. 89) hier als Beispiele aufgeführt. Ferner bereitet der DFN über die föderierten Dienste den Weg zur Kooperation von Hochschulen untereinander vor (M. Röder, DFN, S. 20).

Ich möchte an dieser Stelle allen Autoren und Referenten danken, die unsere Veranstaltung „Cloudspeicher im Hochschuleinsatz“ zu einer erfolgreichen Veranstaltung gemacht haben. Mein Dank geht auch an meine Kolleginnen und Kollegen, die mich bei der Durchführung unterstützt haben und die Organisation der Veranstaltung übernommen haben, allen voran Michaela Müller-Klang und Thomas Gebhardt. Ich möchte mich auch noch einmal beim DFN und beim ZKI für die Unterstützung und das Marketing der Veranstaltung bedanken sowie bei T-Systems für die finanzielle Unterstützung. Zuletzt geht mein Dank an alle Teilnehmenden für ihr Interesse, für die spannenden Diskussionen.

Sync & Share NRW – Von einer studentischen Anfrage zum Großprojekt

Raimund Vogl, Holger Angenent, Dominik Rudolph, Christian Schild, Damian Bucher, Stefan Ost

Zentrum für Informationsverarbeitung (ZIV)
Westfälische Wilhelms-Universität Münster (WWU)
Röntgenstraße 7-13, 48149 Münster

Stefan Stieglitz, Christian Meske

Institut für Wirtschaftsinformatik (WI)
Westfälische Wilhelms-Universität Münster (WWU)
Leonardo Campus 11, 48149 Münster

{rvogl|holger.angenent|d.rudolph|schild|bucher|ost|stefan.stieglitz|christian.meske}
@uni-muenster.de

Abstract: Mit der breiten Etablierung öffentlicher Cloud Dienste ist mit dem Bewusstsein für die damit verbundene Datenschutzproblematik auch der Wunsch nach einer von den Hochschulen selbst betriebenen Alternative gewachsen. Im Rahmen des Arbeitskreises der Leiter wissenschaftlicher Rechenzentren in NRW (ARNW) wurde 2012 ein Projekt gestartet, das eine kooperativ betriebene Speicher-Cloud-Lösung für die Hochschulen in NRW zum Ziel hat. Dessen Konsortialführung hat das ZIV (Zentrum für Informationsverarbeitung) der WWU Münster übernommen. Auf Basis einer DFG-Empfehlung für den Förderantrag nach §143c GG und der Finanzierungszusage des Ministeriums für Innovation, Wissenschaft und Forschung NRW (MIWF) wurde nach eingehender Markterhebung eine Systemlösung auf Basis des deutsch-amerikanischen Open-Source Produktes „ownCloud“ ausgewählt. Der Beschaffungsprozess mit dem Ziel eines NRW-weiten Startes für diesen innovativen Dienst zum Wintersemester 2014/15 hat bereits begonnen. Die kooperative Projektstruktur mit einem Betreiberkonsortium aus initial 17 Hochschulen und mit einem „Big Bang“ Einführungsplan ist in der Hochschul-IT-Landschaft beispielhaft und richtungsweisend. Dieses ambitionierte Vorhaben machte Begleitmaßnahmen erforderlich, die so für IT-Projekte im Hochschulbereich bislang wenig etabliert wurden: eine durchgängige wissenschaftliche Begleitung zur empirischen Fundierung der Bedarfsabschätzung, zur bedarfsangepassten Weiterentwicklung des Diensteangebots und zur Evaluation und Dokumentation der Projektergebnisse. Ein juristisches Begleitprojekt diente der umfassenden juristischen Würdigung der komplexen Rechtssituation für hochschulübergreifende IT-Dienste sowie zur Schaffung einer rechtlichen Struktur für das Betreiberkonsortium. Nicht zuletzt ist die Abstimmung der betreibenden Universitätsrechenzentren bezüglich der Zuständigkeiten, Verantwortlichkeiten und gewährleistbaren Dienstequalitäten von höchster Bedeutung.

1 Der Anstoß für und die Formierung von Sync & Share NRW

Gegen Ende des Jahres 2011 hatten öffentliche Cloud-Dienste, insbesondere von US-amerikanischen Anbietern wie Google und Dropbox, bereits eine große Nutzerschaft erreicht – auch im Bereich von Forschung und Lehre. Ein Bewusstsein für die Gefahren für Datensicherheit und geistiges Eigentum, die die Nutzung solcher Dienste mit sich bringt, bestand zwar durchaus, es mangelte jedoch an Alternativen im Einklang mit dem deutschen Datenschutzrecht.

In dieser Situation bat eine studentische Initiative an der WWU Münster über die Informationsverarbeitungs-Kommission (IV-K) das ZIV, einen on-premise Cloud-Speicherdienst als Alternative zu Dropbox für die WWU anzubieten. Dieser Bedarf für einem neuen Dienst wurde auch an den anderen Universitäten in NRW gesehen, so dass der Arbeitskreis der Leiter der wissenschaftlichen Rechenzentren in NRW (ARNW) im Frühjahr 2012 eine Arbeitsgruppe zur Ausarbeitung des Konzepts für einen hochschulübergreifenden, kooperativ erbrachten Cloud-Speicherdienst für die Hochschulen einsetzte.

Im Rahmen dieser Arbeitsgruppe wurden Lösungsarchitekturen und Software-Produkte für Sync & Share geprüft – wegen des zu erwartenden Datenaufkommens. Falls ein solcher Dienst in einem „Big Bang" Szenario gleichzeitig für alle Hochschulen im Land gestartet und auch nachdrücklich beworben würde, bestand Einigkeit, dass eine Systemlösung, die die Verteilung an mehrere Betreiberstandorte erlaubt, unerlässlich war – ein verteilter Betrieb sollte darüber hinaus auch den kooperativen Charakter dieses Projektes verdeutlichen. Das ZIV der WWU wurde als Führer des zu etablierenden Konsortiums für Sync & Share NRW bestimmt, die Universitäten Bonn und Duisburg-Essen fanden sich als Ko-Betreiber.

In einer verbindlichen Bedarfserhebung im Februar 2013 hatten sich 17 Hochschulen (neun Universitäten und acht Fachhochschulen) zur Teilnahme, für Ihre Mitarbeiter und/oder Studierenden, bereit erklärt. Das MIWF NRW hatte die Förderung dieses Referenzprojektes für eine hochschulübergreifende Zusammenarbeit im Rahmen der Großgeräte der Länder nach § 143c GG zugesagt. Dies gab den Anstoß zur Ausarbeitung eines Projektantrags, der im Mai 2013 zur Begutachtung durch die DFG eingereicht und im Januar 2014 empfohlen wurde.

Der kooperative Charakter und die auf eine landesweite Nutzerschaft ausgelegte Skalierung des Projektes stießen schon in der Vorbereitungsphase auf breites Interesse, auch auf europäischer Ebene im Rahmen der European University Information Systems (EUNIS) [Vo13].

Die wissenschaftliche Begleitung, die mit dem Institut für Wirtschaftsinformatik der WWU (Forschungsgruppe Kommunikations- und Kollaborationsmanagement, Prof. Dr. Stefan Stieglitz) initiiert wurde, lieferte wichtigen empirischen Input für die bedarfsangepasste Dimensionierung und funktionale Ausgestaltung des Sync & Share Dienstes und führte zu Beiträgen an Tagungen im Bereich der Information Systems [Me14], wobei sich eine umfassende Ausarbeitung zur Bedarfserhebung anhand einer hochschulübergreifenden Befragung mit über 10.000 Teilnehmern noch im Peer Review-Verfahren einer weiteren Konferenz befindet. Die Verbindungen zur universitären Lehre konnten bereits mit einem Projektseminar zur Entwicklung von ergänzenden mobilen Softwarelösungen zu den ownCloud-Diensten sowie mit einem Information Systems Teaching Case zum Projekt Sync & Share NRW [Wa14] erzielt werden.

Das gemeinsam mit dem Institut für Telekommunikations- und Medienrecht der WWU (Lehrstuhl Hoeren) initiierte juristische Begleitprojekt zur „Ausarbeitung von Vertragsmustern für hochschulübergreifende Kooperationsprojekte im IT-Bereich" wurde vom MIWF NRW finanziell gefördert und lieferte im Frühjahr 2014 die für die Konstituierung des Sync & Share NRW Betreiberkonsortiums notwendige vertragliche Basis.

2 Empirisch fundierte Bedarfsabschätzung und Evaluation des Projekterfolgs

Ein großer Teil aller neu eingeführten technischen Dienste scheitert, im Wesentlichen deshalb, weil für die Nutzer kein substantieller relativer Vorteil zu bestehenden Produkten ersichtlich ist [Ro03]. Deshalb war klar, dass Sync & Share NRW nur dann Erfolg haben kann, wenn der Dienst aus Sicht der potentiellen Nutzer einen vorhandenen Bedarf erfüllt und außerdem eng an den Nutzerwünschen ausgestaltet wird. Zwar waren alle Beteiligten von der Idee eines hochschuleigenen Cloud-Speicherdienstes für Forschung und Lehre überzeugt. Aber aufgrund des hohen Investitionsvolumens und des zu erwartenden Aufwands wäre es leichtfertig gewesen, dies nicht empirisch abzustützen.

Bereits eine im Rahmen der jährlichen Nutzerumfrage des ZIV der WWU durchgeführte Befragung ließ eine sehr hohe Nutzungsbereitschaft für Sync & Share NRW erkennen. Zur weiteren empirischen Prüfung des potentiellen Marktpotentials des Dienstes sowie seiner optimalen Ausgestaltung wurde Ende 2013 gemeinsam mit dem Institut für Wirtschaftsinformatik der WWU (Arbeitsgruppe Stieglitz – Kommunikations- und Kollaborationssysteme) eine großangelegte Online-Befragung an mehreren Teilnehmerhochschulen gestartet. Mit über 10 000 beendeten Fragebögen (7 623 Studenten, 2 744 Mitarbeiter) kann das Ergebnis als repräsentativ angesehen werden. Die Ergebnisse der Studie wurden in verschiedenen Publikationen veröffentlicht [Me14], [Vo13], [Wa14].

Die Studie verfolgte folgende Ziele:

- Ermittlung der potentiellen Nutzerzahl: Gibt es überhaupt einen Bedarf?
- Betrachtung des Marktumfeldes: Welche Konkurrenzprodukte sind bereits im Einsatz?
- Prognose des benötigten Speichervolumens: Wie groß muss die Kapazität bemessen werden?
- Prognose des Diffusionsverlaufs: Wie viel Speicherkapazität muss in welcher Projektphase bereitgestellt werden?
- Ermittlung potentieller relativer Vorteile: Welche Diensteigenschaften sind entscheidend für den Diffusionserfolg und das Marketing?
- Ermittlung potentieller Hemmnisse: Welche Variablen der Dienstequalität schränken die Nutzungsbereitschaft ein? Welche Risiken bestehen?
- Ermittlung der Rolle der Hochschule als Diensteanbieter: Wie sehr wird Hochschulen vertraut, welche Eigenschaften fördern Vertrauen in den Dienst?
- Ermittlung gewünschter Features: Welche Eigenschaften fördern die Akzeptanz des Dienstes?

Die Ergebnisse der Studie zeigen, dass Sync & Share NRW auf ein enormes Interesse innerhalb der Hochschulcommunity stößt (vgl. Abbildung 1): Über 80 % würden den Dienst nutzen, bei den Beschäftigten ist der Anteil dabei sogar noch höher als bei Studierenden.

Dies ist umso bemerkenswerter, da ein sehr großer Prozentsatz bereits Cloud-Speicherdienste nutzt (81 % der Studierenden, 72 % der Beschäftigten), vor allem DropBox. Etwa 75 % aller Befragten legen in ihrem Cloud-Speicherdienst sowohl private als auch studien- bzw. arbeitsbezogene Materialien ab. Ein wichtiger Grund für einen Wechsel zu Sync & Share NRW

mit einem Teil oder sogar mit allen Daten ist das Vertrauen in die Hochschule als Anbieter. 79 % der Studierenden und 72 % der Beschäftigten vertrauen eher der Hochschule statt einem privatwirtschaftlichen Unternehmen als Cloud-Anbieter, da dieses gewinnorientiert ist und ihren Sitz häufig im Ausland hat. Fehlendes Vertrauen in die bisherigen Anbieter in Bezug auf Datensicherheit und Datenschutz ist auch der häufigste Grund für die Personen, die bisher noch keine Cloud-Dienste nutzen. Der Sicherheitsvorteil ist also der entscheidende Schlüsselfaktor für den Erfolg des Dienstes.

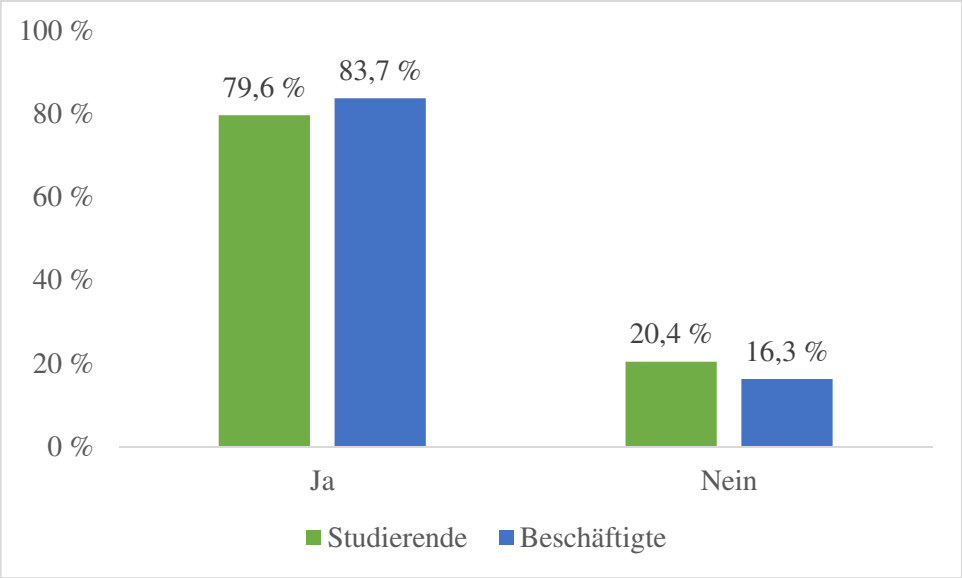


Abbildung 1: Nutzungsabsicht Sync & Share NRW

Daneben konnten in der Studie eine Reihe möglicher Features ermittelt werden, die der Dienst möglichst bieten sollte (vgl. Tabelle 1).

Tabelle 1: Gewünschte Features.

	Studenten (n=7 623)	Beschäftigte (n=2 744)
Dateifreigabe für Andere	6 992 (92 %)	2 485 (91 %)
Gleichzeitige Dokumentenbearbeitung mit Anderen	6 222 (82 %)	2 096 (76 %)
Versionierungsmanagement	6 014 (79 %)	2 228 (81 %)
Volltextsuche	6 455 (85 %)	2 214 (81 %)
Kommentarfunktion	5 025 (66 %)	1 607 (59 %)
Textchat	3 394 (45 %)	405 (15 %)
Synchronisierung von Kalender und Kontakten	517 (51 %)	1 762 (64 %)

Eine der wesentlichen offenen Fragen war die erforderliche Dimensionierung des Speichervolumens. Diese Frage ist von erheblicher Bedeutung für den Finanzierungsbedarf des Projektes und die benötigte Hardware. Die ursprüngliche ad hoc-Schätzung war diesbezüglich zu ungenau. Auf der theoretischen Basis des Diffusionsmodels nach Rogers [Ro03] und den empirischen Ergebnissen der Studie zum derzeitigen Datenvolumen wurde daher eine elaboriertere Prognose erstellt. Da die von Rogers beschriebenen diffusionsfördernden Eigenschaften (hohe Übereinstimmung mit bekannten Produkten, hoher relativer Vorteil, geringe Komplexität, geringes Risiko, gute Erprobbarkeit, gute Kommunizierbarkeit) bei Sync & Share NRW gegeben sind, rechnen wir mit einer sehr schnellen Diffusion des Dienstes, erheblich schneller als DropBox, das zu Beginn der Cloud-Ära als vollkommen neuer Dienst wesentlich schwierigere Bedingungen hatte als ein me-too-Service (vgl. Abbildung 2).

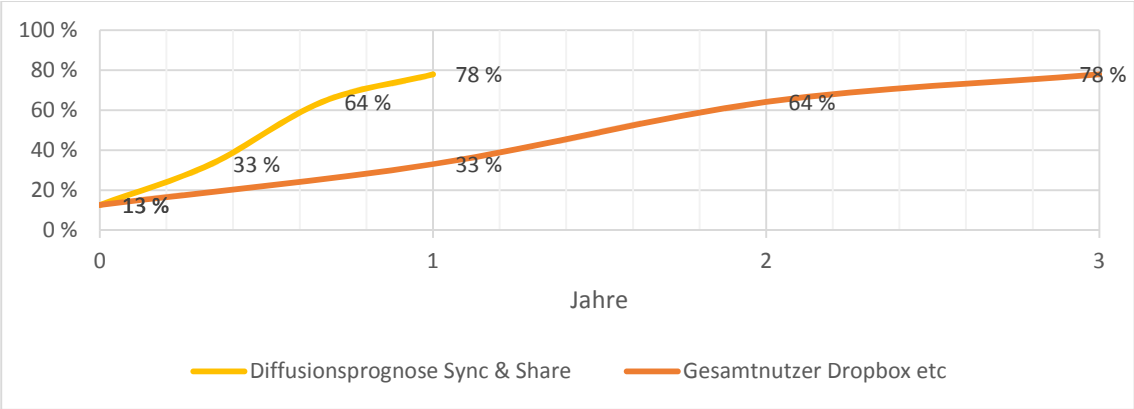


Abbildung 2: Diffusionsprognose Sync & Share NRW

Das Datenvolumen ist sehr schwer zu schätzen, da dazu bislang keine Daten oder Studienergebnisse vorliegen. Auf Basis der Erhebungsdaten schätzen wir, dass etwa 67 % der potentiellen Nutzer den Cloud-Speicherdienst tatsächlich nutzen werden. Nach dem Diffusionsmodell von Rogers verläuft der Diffusionsprozess in fünf Phasen. Dies hängt wesentlich damit zusammen, dass in jeder Stichprobe unterschiedlich innovationsfreudige Individuen versammelt sind, die Rogers in fünf Gruppen einteilt: Innovatoren, Early Adopters, Frühe Mehrheit, Späte Mehrheit sowie Nachzügler. Auf Basis der Daten der Erhebung kennen wir die Geschwindigkeit der DropBox-Diffusion innerhalb unserer Stichprobe. Diese hat den Dienst deutlich früher genutzt als anhand des normalverteilten Modells zu erwarten wäre, so dass es offenbar eine besonders große Gruppe innovationsfreudiger Individuen unter den potentiellen Nutzern gibt. Basierend auf dem von uns zu Grunde gelegten Modell gehen wir davon aus, dass bereits relativ früh relativ viele Personen den Dienst nutzen.

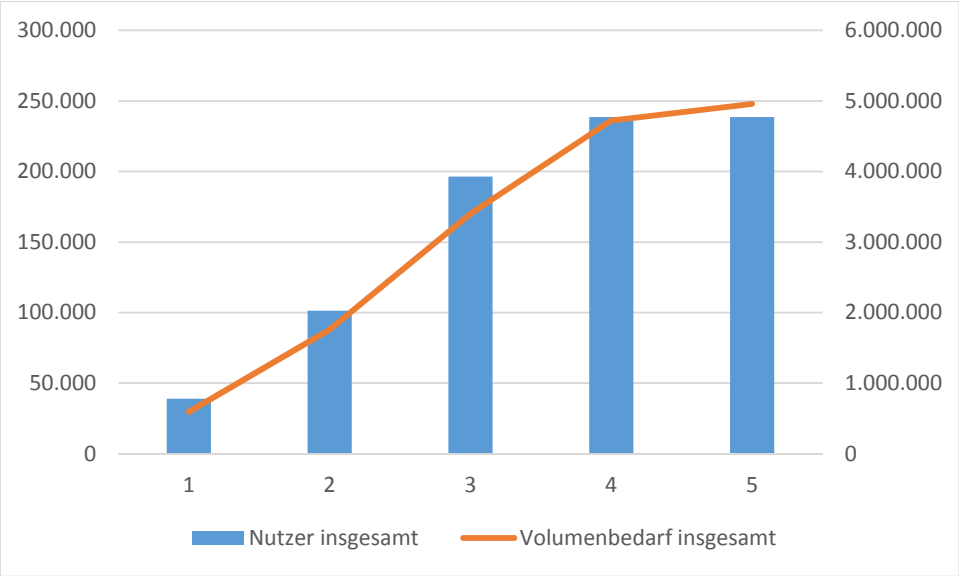


Abbildung 3: Prognose Datenvolumen je Diffusionsphase

Wir gehen weiter davon aus, dass nach einer ersten Grundsynchronisation nach Nutzungsbeginn des jeweiligen Nutzers eine geringere Zusatzmenge an Datenvolumen in den Dienst gegeben wird. Dies haben wir aus der Differenz der derzeitigen Datennutzung und der erwarteten Datennutzung je Nutzer ermittelt (vgl. Abbildung 3). Wir gehen daher von einem Gesamtvolumen von fünf PetaByte am Ende der Diffusion aus. Die Länge der jeweiligen Diffusionsphasen ist allerdings nur schwer schätzbar.

3 Das Sync & Share NRW Konsortium

Die Struktur für das Sync & Share NRW Konsortium sowie der Vertragsrahmen wurden im Zuge eines vom MIWF NRW geförderten Forschungsprojektes zur „Ausarbeitung von Vertragsmustern für hochschulübergreifende Kooperationsprojekte im IT-Bereich“, das vom Institut für Technologie und Medienrecht (ITM, Lehrstuhl Prof. Thomas Hoeren) und dem ZIV betreut wurde, ausgearbeitet. Die daraus entstandenen Musterverträge stehen den Hochschulen in NRW auch für andere, ähnlich geartete kooperative IT-Projekte zur Verfügung. Eine zukünftige Fortschreibung ist angedacht.

Die Grundkonzepte beim rechtlichen Konstrukt für Sync & Share NRW sind die folgenden:

- Es gibt einen *Konsortialführer* (die WWU Münster), die als Antragsteller und Zuwendungsempfänger gegenüber dem MIWF NRW auftritt. Alle am Konsortium beteiligten Hochschulen sind *Teilnehmer*. Die drei am Betrieb beteiligten Hochschulen (die Universitäten Bonn, Duisburg-Essen und Münster) sind darüber hinaus *Betreiber*.

- Alle Rechtsgeschäfte werden durch den Konsortialführer getätigt, als Zuwendungsempfänger ist das System in seinem Eigentum und er ist für die Aufbringung des Finanzierungs-Eigenanteils verantwortlich. Er handelt für das Konsortium bei der Umsetzung des gemeinsamen Großgeräteantrags (insbesondere Beschaffung) und dem Betrieb des Systems. Aus steuer- und zuwendungsrechtlichen Erwägungen wird keine selbständig rechtsfähige Einheit für die Projektumsetzung geschaffen.

- Als rechtlicher Rahmen für die Speicherung von Endnutzerdaten in Sync & Share NRW wird das Instrument der Auftragsdatenverarbeitung gewählt. Entsprechend liegt die Verantwortung für die Einhaltung des Datenschutzgesetzes bei den Teilnehmerhochschulen. Diese stellen den Dienst den berechtigten Endnutzern (Mitarbeiter und/oder Studierende) zur Verfügung. Es besteht keine direkte Rechtsbeziehung zwischen Konsortialführer/Betreibern und den Endnutzern.

Es gibt folglich folgende Verträge:

- *Konsortialvertrag* zwischen der WWU Münster als Konsortialführer und allen Teilnehmern bzw. den Teilnehmern mit der Zusatzrolle als Betreiber (zusätzliche Verpflichtungen). In zwei Anlagen zum Konsortialvertrag werden die Funktion des Systems und die technische Plattform beschrieben.

- *Auftragsdatenverarbeitungsvertrag* zwischen allen Teilnehmern und dem Konsortialführer (die Ko-Betreiber sind dessen Erfüllungsgehilfen).

- *Benutzerordnung für Endnutzer* zwischen der Teilnehmerhochschule und den Endnutzern aus ihrem Bereich. Ein Muster dazu wird den Teilnehmern bereitgestellt.

Abbildung 4 stellt einen schematischen Überblick über das Vertragskonstrukt dar.

Darüber hinaus müssen die Teilnehmer als Auftraggeber der Auftragsdatenverarbeitung ein Verfahrensverzeichnis erstellen und eine Datenschutzvorabkontrolle durchführen.

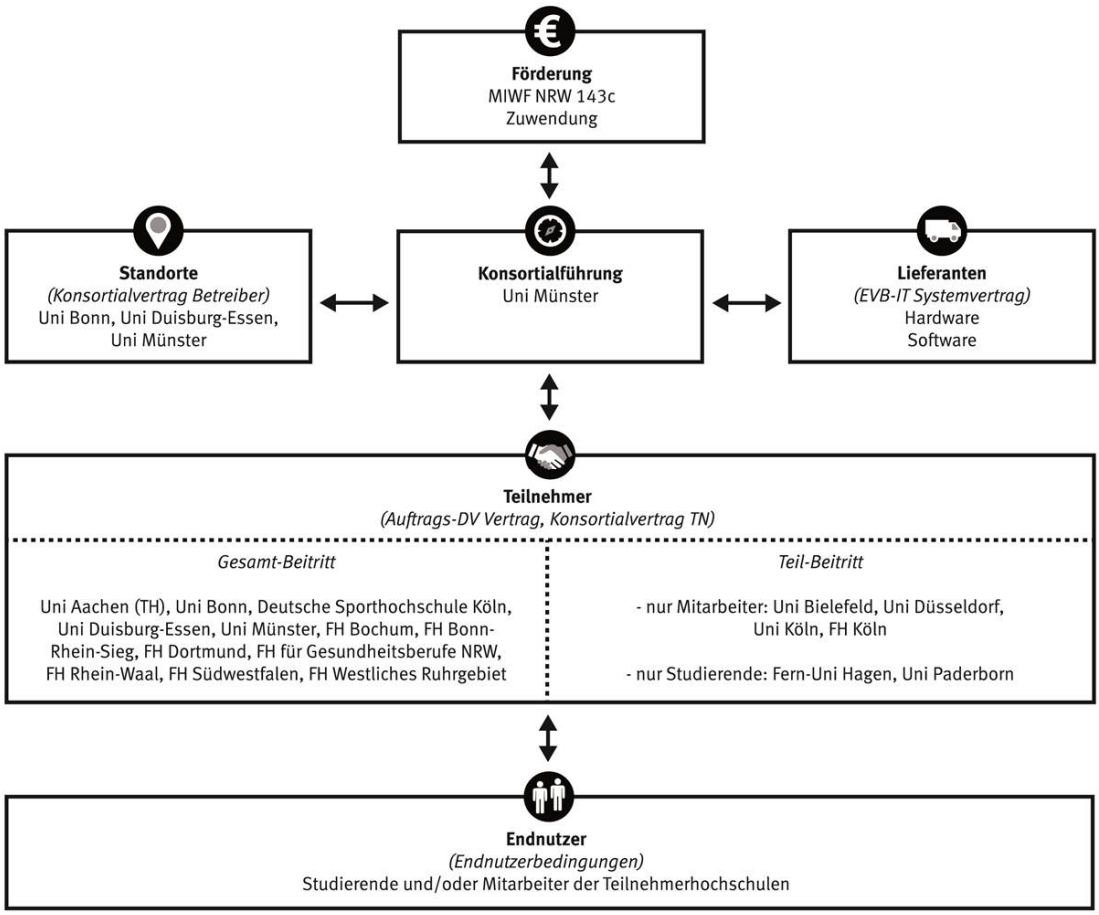


Abbildung 4: Struktur des Sync & Share NRW Konsortiums

Weiterhin verpflichten Sie sich im Konsortialvertrag, eine Schutzbedarfsanalyse für die Eignung bzw. Nicht-Eignung von Datenarten für die Speicherung im Dienst Sync & Share NRW durchzuführen und ihre Endanwender darüber zu informieren.

4 Produktauswahl und Lösungsarchitektur

4.1 Produktevaluation

Bereits im Jahr 2012 wurden verschiedene Produkte hinsichtlich ihrer Eignung für den Betrieb einer Speicher-Cloud untersucht. Zunächst wurden die zum damaligen Zeitpunkt zumindest als Testversion erhältlichen Produkte verglichen, um einen Überblick über die Möglichkeiten zu erhalten und die eigenen Anforderungen besser definieren zu können.

Vom Funktionsumfang her machte bei diesem Vergleich ownCloud den ausgewogensten Eindruck, auch wenn die Reife zu diesem Zeitpunkt noch nicht hinreichend war. Aufgrund einer guten öffentlichen Dokumentation über den Entwicklungsprozess ließ sich jedoch ein hohes Entwicklungstempo erkennen, so dass eine Besserung absehbar war.

In der darauf folgenden Phase wurde eine breitere Palette von Produkten über einen längeren Zeitraum beobachtet und getestet. Dabei wurde insbesondere auf das Zusammenspiel von Hard- und Software Wert gelegt. Eine Situation, in der die Gesamtlösung aus verschiedenen, nicht zusammen getesteten Komponenten besteht, sollte vermieden werden.

Aus diesem Grund wurden die Hersteller aufgefordert, Gesamtpakete aus Hard- und Software zu erstellen und einen entsprechenden Gesamtpreis zu nennen. Auf Grundlage dieser Voraussetzungen haben mehrere Hersteller umfangreiche Informationen geliefert.

Die Produkte wurden im Hinblick auf die Kriterien Skalierbarkeit, Zukunftsaussichten, Nutzererfahrung und Funktionsumfang beurteilt. Eine konkrete Diskussion der einzelnen Produkte soll an dieser Stelle nicht stattfinden, da stellenweise Verschwiegenheitserklärungen unterzeichnet wurden.

Als geeignete Software wurde schließlich auf Grund der oben genannten Faktoren ownCloud ausgewählt. OwnCloud kann mit einem großen Funktionsumfang und einer intuitiven Bedienbarkeit überzeugen. Außerdem wird durch eine hohe Entwicklungsgeschwindigkeit, der Einflussmöglichkeit des Konsortiums als wichtiger Enterprise-Kunde auf die Produktentwicklung, dem Mitwirken der Open Source Community und der Möglichkeit, eigenen Code einzubringen auch in Zukunft eine schnelle Anpassung an entsprechende Erfordernisse sichergestellt.

Ebenfalls entscheidend war die Tatsache, dass es sich um ein Open Source-Produkt handelt. Open Source-Software besitzt in diesem Kontext diverse Vorteile gegenüber anderen, proprietären Produkten.

Das Feld der Cloud Storage-Produkte ist im Vergleich zu anderen Technologien relativ jung und noch in der Entwicklung begriffen. Die Zukunftsaussichten von einzelnen Firmen und deren Produkten sind dadurch zumindest nicht vollständig gewiss. Trotzdem soll das auf fünf Jahre angelegte Projekt mindestens über diesen Zeitraum mit Updates und Weiterentwicklungen versorgt werden. Im Fall einer Nichtweiterentwicklung des eingesetzten Produktes kann bei Open Source-Software auf den bereits veröffentlichten Quellcode zurückgegriffen werden. Dadurch, dass bereits in der Open Source-Community die Entwicklung von ownCloud

unterstützt wird, lässt sich ablesen, dass die Codequalität es erlaubt, auch als externer Entwickler zu partizipieren.

Weiterhin lässt sich ein Open Source-Produkt häufig durch eigene Programmierer anpassen und weiterentwickeln. Gerade im Rahmen von Forschungskooperationen kann dies eine wichtige Rolle spielen. So ist beispielsweise bereits im Rahmen eines Projektseminars auf der Basis der Communityversion von ownCloud eine Windows 8-App entwickelt worden. Dies wurde erst durch das öffentliche API von ownCloud ermöglicht.

Auch für zukünftige Featurewünsche sind Eigenentwicklungen denkbar. Im Vergleich zu Aufträgen an ownCloud könnten diese schneller umgesetzt werden oder besser an die eigenen Bedürfnisse angepasst werden.

Durch das kostenlose Bereitstellen der Community-Version hat sich ownCloud mittlerweile zu einem in vielen Bereichen eingesetzten Produkt entwickelt. Durch Rückmeldungen der zahlreichen Nutzerschaft kann davon ausgegangen werden, dass ownCloud in sehr vielen Hardware- und Nutzungsszenarien getestet wurde.

Auf kommerziellen Support muss trotzdem nicht verzichtet werden. Für die Enterprise-Version von ownCloud werden vollständiger Support und schnelle Reaktionszeiten angeboten.

Im Hinblick auf die Skalierbarkeit für die angepeilte Nutzerzahl von ungefähr 500.000 Nutzern wurde von einer der anbietenden Firmen ein Proof of Concept mit ownCloud durchgeführt. Daraus konnte die benötigte Hardware für eine entsprechende Installation ermittelt werden.

4.2 Lösungsarchitektur für Sync & Share NRW

Die Hardware für Sync & Share NRW soll auf insgesamt drei verschiedene Standorte aufgeteilt werden. Der Hauptgrund dafür besteht in der Entlastung der lokalen Internetanbindungen. Selbst wenn berücksichtigt wird, dass durch dieses Konzept neuer Datenverkehr zwischen den einzelnen Standorten generiert wird, der ansonsten unnötig wäre, muss nur etwa ein Drittel der Gesamtnutzerzahl auf einem Standort arbeiten. Weiterhin wird durch eine frühzeitige Berücksichtigung eines Mehrstandortkonzeptes eine zukünftige Erweiterung des Dienstes erleichtert werden.

Als Standorte wurden die Rechenzentren der Universitäten Münster, Duisburg-Essen und Bonn ausgewählt, da es sich bei diesen um DFN-Kernnetzstandorte handelt und Nordrhein-Westfalen in etwa geografisch gleichmäßig aufteilen. Die Universität Münster koordiniert dabei als Konsortialführer das Vorgehen der einzelnen Standorte. Die einzelnen Installationen durch sollen durch Münsteraner Administratoren durchgeführt werden.

Die Datensicherheit soll ausschließlich durch lokale Mittel gewährleistet werden. Eine Replikation der Daten zwischen den Standorten ist nicht vorgesehen, um die verfügbare Kapazität möglichst effizient auszunutzen. Weiterhin soll auf ein lokales Backup auf Bänder verzichtet werden. Um trotzdem eine hohe Verfügbarkeit zu erreichen, werden die Daten mit einem Trippel-Parity-Verfahren (RAID 8+3 – also 3 Bit Paritätsinformation pro Byte anstelle 2 bei klassischem RAID6) gespeichert. Außerdem wird eine Technik mit sehr kurzen Wiederherstellungszeiten nach dem Ausfall einer Festplatte eingesetzt (declustered RAID).

Die Nutzenden der teilnehmenden Hochschulen sollen den einzelnen Standorte statisch zugeteilt werden. Es wird keine Lastverteilung zwischen den einzelnen Hochschulen durchgeführt, da somit ein Kopieren oder Replizieren der Daten unnötig wird.

Um die drei Standorte für die Nutzenden möglichst einfach darzustellen, soll jede der teilnehmenden Einrichtungen eine eigene, virtuelle Dienstadresse erhalten. Die DNS-Records der Einrichtungen verweisen jeweils auf einen der Standorte. Vorteilhaft dabei ist die Tatsache, dass einem Nutzer nicht bekannt sein muss, zu welcher der zentralen Serverstandorte die eigene Einrichtung zugeordnet ist. Weiterhin kann somit, falls sich in Zukunft herausstellt, dass die initiale Zuordnung korrigiert werden muss, eine Umverteilung der Nutzenden vorgenommen werden, ohne dass diese in den Prozess eingreifen müssten.

An den einzelnen Standorten werden Installationen der Enterprise-Variante von ownCloud durchgeführt. Neben einem Cluster von Webservern ist dabei ein Datenbankbackend nötig, das eine ausreichend hohe Lese- und Schreibperformance aufweist.

Empfohlen wird zu diesem Zweck eine Konfiguration aus Master-Master replizierenden mySQL-Instanzen, die per Galera zu einem Cluster gekoppelt werden. Da eine entsprechende Replikation den Nachteil hat, dass die Schreibperformance nicht gesteigert wird, sollen die einzelnen Server lokal mit leistungsfähigen SSDs ausgestattet werden.

Zur Speicherung der eigentlichen Nutzdaten soll ein leistungsfähiges Dateisystem zum Einsatz kommen. Dieses muss nicht nur mit einer großen Anzahl von Dateien und Ordnern betriebsfähig bleiben, sondern ebenso eine möglichst hohe Betriebsstabilität bieten.

In Abbildung 5 ist schematisch die Aufteilung der Daten und Nutzer zwischen den unterschiedlichen Standorten sowie die generelle Ausstattung mit Hardware skizziert. Der Standort des zentralen Portals syncshare.nrw.de wird sich dabei in Münster befinden.

Technisch wird dies so gehandhabt, dass im Self-Service Verfahren die Nutzer sich per DFN-AAI gegen ihre Heimateinrichtung authentifizieren und darauf in einen zentralen LDAP-Server eingetragen werden. Dieser dient als Quelle der Nutzerkennungen für die ownCloud-Server. Nach jeweils sechs Monaten muss die Anmeldung der Nutzer erneuert werden, ansonsten soll nach einer Kulanzfrist (voraussichtlich ebenfalls sechs Monate) eine Deprovisionierung stattfinden.

Die Vernetzung der Standorte soll auf der Ebene von ownCloud abgebildet werden. Durch eine Erweiterung der Möglichkeit, externe WebDAV-Verzeichnisse einzubinden, wird es ermöglicht, mit Nutzenden anderer Standorte Daten zu teilen. Dabei sind keine zentralen Komponenten notwendig. Somit lässt sich das Konzept bei Bedarf auch auf andere Installationen oder weitere Standorte erweitern.

Der Mechanismus zum Teilen von Daten mit Nutzern anderer Standorte sieht dabei vor, dass, wie auch bei der rein internen Nutzung üblich, nach einem Klick auf „Teilen mit“ in diesem Fall ein Link erzeugt wird, der per Email an den Empfänger gesendet wird, wo dieser in die entsprechende Verzeichnisstruktur gemountet wird. Bei Verwendung eines zentralen LDAP-Servers ist, wie im vorliegenden Fall, eine Autovervollständigung des Nutzernamens, mit dem geteilt wird, möglich. Die Authentifizierung der Server geschieht dabei durch shared-keys. Mithilfe einer Propagation der ETAGS zwischen den Servern kann auch bei diesem Mechanismus eine hohe Performance erreicht werden. Trotzdem müssen keine Daten repliziert werden, so dass kein unnötiger Speicher verwendet wird. Da die Eingriffe auf Administratorseite minimal sind, können über diesen Mechanismus beliebige ownCloud-Server miteinander gekoppelt werden. Einzig die Autovervollständigung benötigt eine zentrale Nutzerverwaltung.

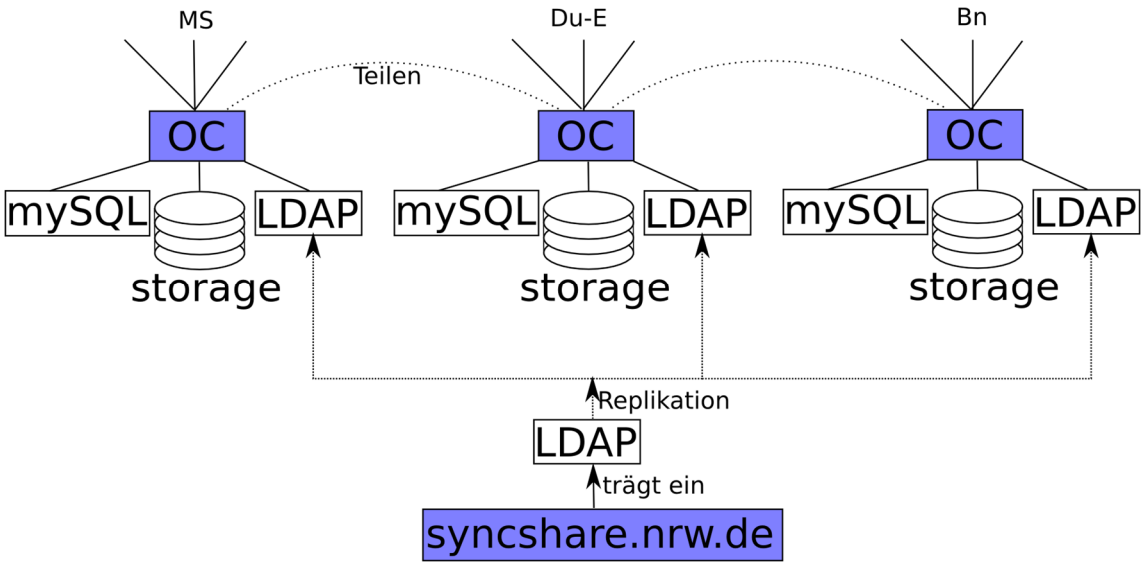


Abbildung 5: Schema des Dreistandortkonzeptes mit lokalen ownCloud Installationen

Die lokalen LDAP-Server erhalten ihre Daten aus einem zentralen Portal, das per DFN-AAI im Self-Service Verfahren befüllt wird. Die einzelnen Standorte Münster, Duisburg-Essen und Bonn sind dabei jeweils über mehrere Dienstadressen erreichbar, um so die verschiedenen teilnehmenden Einrichtungen abzubilden.

In einem nächsten Entwicklungsschritt ist es deswegen denkbar, dies durch ein festes Schema der Nutzernamen zu vereinfachen. Wenn, wie bei Sync & Share-NRW geplant, alle Nutzer eine Kennung nach dem Schema Nutzername@Servername.Domainname besitzen, besteht die Möglichkeit für die Server, per DNS-Abfrage den Heimatserver eines Nutzers zu ermitteln. Somit kann eine Anfrage zum richtigen Server weitergeleitet werden.

4.3 Erläuterungen zum Teilen von Daten mit Hilfe von DNS-Records

Im Folgenden wird eine Möglichkeit beschrieben, die in ownCloud implementiert werden könnte, um das Teilen von Daten zwischen verschiedenen ownCloud-Servern und die Konfiguration der Clients weiter vereinfachen könnte. Sie ist bisher nicht Bestandteil von ownCloud.

Sowohl wenn der Nutzer sich mit seinem Client am Server anmeldet als auch wenn Server mit anderen Servern kommunizieren wollen, muss der richtige Host mit der richtigen Owncloud-Installation gefunden werden.

Es wird nun der Aspekt ausgenutzt, dass die UserID bereits den passenden Domain- bzw. Servernamen enthält. So kann „mustermann@example.com“ bereits eine eindeutige Kennung sein, die mit Hilfe eines richtig konfigurierten DNS alle Informationen enthält um den richtigen Server zu finden. Hierdurch wird die UserID zu einer global eindeutigen GlobalUserID. Dies geschieht durch die Verwendung eines sogenannten Service-Eintrags (SRV) im DNS.

Bei einem SRV handelt es sich um einen vordefinierten „well-known“ Namens-String, der im DNS abgefragt werden kann und der auf den richtigen Host mit dem zugehörigen Owncloud-Server verweist. Etwa auf folgende Weise:

_cloudstorage._tcp.example.com IN SRV owncloudserver.example.com.

Ein Client oder ein Server der nun eine Kommunikation aufbauen will und nur die GlobalUserID kennt, kann diesen well-known SRV Eintrag abfragen und findet so heraus, welchen realen Server er kontaktieren muss. Somit kann ein Client per Autokonfiguration initialisiert werden. Das Server2Server-Protokoll wird erst hierdurch möglich.

Ein entscheidender Nebeneffekt ist, dass die zuständige Owncloud-Instanz auch auf eine andere Domain umgeleitet werden kann. Dies kann entweder bereits im SRV-Eintrag geschehen:

_cloudstorage._tcp.example.com IN SRV owncloudserver.example.org.

Oder besser: der zugehörige A Record zeigt auf eine IP eines Servers einer anderen Domain:

_cloudstorage._tcp.example.com IN SRV owncloudserver.example.com

owncloudserver.example.com IN A 192.0.2.123

123.2.0.192.in-addr.arpa. IN PTR owncloudserver.example.org.

Letzteres Verfahren hat den Vorteil, dass auch im beim Web-Login der reale Owncloud-Servername maskiert wird.

Worauf dieser Service-Eintrag verweisen soll bleibt unter der vollständigen Kontrolle des Domain-Inhabers. Es ist seine Nameservice-Domain und er muss sich willentlich dafür entscheiden, dass jemand anderes für ihn das Owncloud-Hosting übernimmt. Der Remote-Hoster muss ebenso damit einverstanden und informiert sein, denn er muss die entsprechenden GlobalUserIDs anlegen und mitverwalten.

5 Die Rahmenbedingungen für den Dienst Sync & Share NRW

Die Grundidee für Sync & Share NRW war es von Anfang an, dass alle Hochschulen in NRW durch die Teilnahme am Konsortium in die Lage versetzt werden sollen, ihren Endnutzern eine attraktive Alternative zu Speicherdiensten wie DropBox, Google Drive etc. anbieten zu können, folglich müssen folgende zentrale Eigenschaften sichergestellt werden:

- **Gratis:** den Endnutzern (Studierenden und/oder Mitarbeiter (und Projektgruppen) – den Hochschulen steht es frei, ob sie für beide Gruppen oder nur für eine teilnehmen – wird der Dienst kostenlos bereitgestellt. Die Großgerätefinanzierung durch das MIWF NRW ermöglicht dies – die Hochschulen müssen nur den Eigenanteil der Beschaffung sowie die Betriebskosten aufbringen. Sie verpflichten sich dazu auf die voraussichtliche System-Nutzungszeit von fünf Jahren.

- **Großer Speicherplatz:** um die Nutzer der etablierten Gratisangebote für den neuen Dienst gewinnen zu können, muss neben der besseren Datensicherheit auch die Leistung bzgl. Speichervolumen attraktiv sein. Mit 30 GB für jeden Nutzer und der Option, für Projektgruppen gesonderte, nicht-personengebundene Speicher-Folder mit 400 GB (und bei Bedarf mehr) zu erhalten, sollte der Dienst attraktiv genug positioniert sein.

- **Kulanzfrist:** für viele potenzielle Nutzer ist es ein wichtiger Punkt, dass der Zugriff auf Sync & Share NRW nicht sofort mit dem Ende der Zugehörigkeit zur Hochschule endet. Dass die Hochschulzugehörigkeit noch gegeben ist, soll durch eine periodische (alle sechs Monate) Reautorisierung über DFN-AAI sichergestellt werden. Nach dem

Ausbleiben einer Reautorisierung sollen den Endnutzern weitere sechs Monate Kulanzfrist eingeräumt werden, bevor ihre Daten deprovisioniert (d.h. gelöscht) werden.

- **Bequem:** die Software ownCloud ist in ihrer Bedienung sehr ähnlich dem vielen bereits bekannten DropBox und unterstützt auch alle verbreiteten Betriebssystemplattformen. Der Umsteigeaufwand wird minimiert.

Um jedoch einen Dienst mit potenziell 500 000 Nutzern mit den bescheidenen Ressourcen der betreibenden Universitätsrechenzentren realisieren zu können, ist es notwendig, den Aufwand für Endnutzer-Interaktionen zu minimieren:

- Die Nutzer registrieren sich selbst über ein Self-Enrollment Portal.
- Über Online-Informationsangebote zu Systemstatus (NAGIOS), FAQs, ein moderiertes Diskussionsforum und multimedialer Informations-Content soll die Nutzung einer dennoch bereitzustellenden direkten Kontaktmöglichkeit minimiert werden.
- Durch interne technische Maßnahmen zur Hochverfügbarkeit sollen Ausfallszeiten und für den Endnutzer bemerkbare Störungen minimiert werden.
- Wegen des hohen zu erwartenden Datenvolumens ist des den Betreiberhochschulen nicht möglich, nochmals gesonderte Backups auf Magnetband durchzuführen. Auch eine Spiegelung der Daten (z. B. an einen jeweils anderen Standort) verbietet sich aus Gründen des Speicherplatzbedarfs und der konsumierten Netzwerkbandbreite. Die gewählten Speichersysteme mit Tripple-Parity RAID Absicherung sollten jedoch ausreichenden Schutz gegenüber Datenverlust bieten. Die zumindest anfänglich geplante Nutzung von Snapshots sollte auch eine ausreichende Absicherung gegen Software- oder Administrationsfehler bieten.

6 Marketingaktivitäten und Umsetzungszeitplan

Das beste Produkt alleine nützt wenig, wenn die potentiellen Nutzer davon keine oder zu geringe Kenntnis haben. Der Dienst Sync & Share NRW ist für die Nutzer freiwillig, d.h. sie müssen von den Vorteilen überzeugt werden. Die erfolgreiche Diffusion des Dienstes ist daher nur mittels eines professionellen Marketings möglich. Das Marketing steht dabei vor zahlreichen Herausforderungen:

- Starke Konkurrenz durch DropBox mit marktdominierender Stellung als Qualitätsbenchmark
- Heterogene Zielgruppen: Wissenschaftler, Studierende, Verwaltungsmitarbeiter, unterschiedliche Fachbereiche, unterschiedliches technisches Vorwissen
- Hochschulübergreifendes überregionales Marketing
- Kurze Vorlaufzeit
- Geringe Ressourcen

Die Marketingstrategie zielt darauf ab, Sync & Share als hochschulübergreifenden Dienst zu branden. Dies erhöht die Sichtbarkeit und verbessert die Kommunizierbarkeit. Die Marke wird unter einem einheitlichen Logo (vgl. Abbildung 6) und Corporate Design beworben. Ein Namenswettbewerb soll für den Dienst zusätzlich einen geeigneten Namen sowie einen Slogan generieren und Aufmerksamkeit schon vor dem Dienststart erzeugen.

Abbildung 6: Logo von Sync & Share NRW

Zur Ansprache potentieller Nutzer sollen verschiedene Kommunikationskanäle genutzt werden. Besondere Bedeutung hat dabei das zentrale Portal. Die Website syncshare.de stellt die zentrale Informationsquelle insbesondere für neue Nutzer dar, bündelt aber auch alle Informationen für bestehende Nutzer. Hier sollen den potentiellen Nutzern die Vorteile von Sync & Share verdeutlicht und bestehende Vorbehalte zerstreut werden. Die Website ist die Visitenkarte und erste Anlaufstelle. Sie soll daher durch ein zeitgemäßes, intuitives und einladendes Layout Professionalität, technische Kompetenz und Vertrauenswürdigkeit ausstrahlen. Besonders wichtig ist eine einfache, gut verständliche Sprache (Bild und Text), um auch nicht-technikaffine Nutzer zu gewinnen. Durch den Einsatz von Erklärvideos und/oder Demotouren lassen sich die wesentlichen Vorteile auch gegenüber Wettbewerbern wie Dropbox gut verdeutlichen.

Social Media-Plattformen wie Facebook und Twitter eignen sich insbesondere, um bestehende Nutzer an Sync & Share zu binden und die Marke emotional positiv aufzuladen. Sie liefern außerdem eine Plattform, auf der Krisen früh erkannt und eingedämmt werden können, etwa unzufriedene Nutzer oder Gerüchte. Darüber hinaus machen Weiterempfehlungen von Freunden die Marke bekannter (hohe Glaubwürdigkeit).

Direktmailings an alle Angehörigen der Teilnehmerhochschulen sind dank ihrer großen Reichweite ideal zur Aufmerksamkeitsgenerierung und insbesondere zur Bekanntmachung des Dienstes ab Start geeignet. Allerdings haben sie hohe Streuverluste und können nur extrem selten eingesetzt werden.

Durch die große Nutzerzahl, die hohe Landesförderung und die Anknüpfungspunkte an bekannte Themen wie Dropbox oder NSA hat Sync & Share darüber hinaus das Potential für journalistische Berichterstattung. Der Vorteil liegt vor allen in der Bekanntheitssteigerung, positive Presseberichte eignen sich außerdem hervorragend für das Marketing auf der Website, um zögernde Nutzer zu überzeugen. Für die Presse sollen entsprechende Informationstexte zum Download bereitstehen. Auch über die Pressestellen der Teilnehmerhochschulen sollten aktiv Pressemitteilungen zu speziellen Ereignissen verschickt werden (kurz vor Start/Start/100.000 Nutzer). Neben lokalen Medien und technischen Fachzeitschriften können auch spezielle Nischenmedien (mit Zielgruppe Studenten/Forscher) adressiert werden.

Es sollten allerdings auch Krisen-PR-Szenarien berücksichtigt werden, da Risiken für eine negative Berichterstattung vorhanden sind (missbräuchliche Nutzung des Dienstes im großen Stil, nur geringe Nutzung, Datenverlust durch Hacking, Störungen, …).

Nach der Gewinnung von Aufmerksamkeit folgt im Diffusionsprozess die Überzeugungsphase. Hier sind insbesondere die Meinungen von einflussreichen Multiplikatoren entscheidend. Es ist daher wichtig, bereits im Vorfeld solche Personen zu identifizieren und von Sync & Share zu überzeugen und zu Promotoren zu machen. Hier ist beispielsweise an Professoren großer Fachbereiche mit Einführungsvorlesungen zu denken, an IT-Betreuer (IVVen), Fachschaften, ASten oder Mandatsträger (Dekane). Es ist zu überlegen, dieser Zielgruppe bestimmte Vorteile zu geben (z. B. größeres Datenvolumen, Testnutzung vor allen anderen), um eine positive Einstellung zu Sync & Share zu schaffen. Wichtigstes Entscheidungskriterium für zögernde potentielle Nutzer sind positive Erfahrungen und Weiterempfehlungen von Freunden und

Bekannten. Dies kann z. B. auf Facebook stattfinden, wenn im Newsfeed angezeigt wird, dass Freunde Sync & Share liken.

Das Marketing startet mit der Vertragsunterzeichnung (voraussichtlich Ende Mai) und begleitet insbesondere die Einführungsphase im Wintersemester 2014/15, stellt aber auch danach einen wichtigen Faktor da, z. B. bei der Einführung neuer Features oder im Krisenfall. Außerdem liefert es kontinuierlich Daten zur Akzeptanz des Dienstes.

Literaturverzeichnis

[Me14] Meske C., Stieglitz S., Vogl R., Rudolph D., Öksüz A. 2014. 'Cloud Storage Services in Higher Education – Results of a Preliminary Study in the Context of the Sync&Share-Project in Germany.' Contributed to the Proceedings of the 16th Inter-national Conference on Human Computer Interaction (HCI International) 2014, Crete, Greece. [akzeptiert]

[Ro03] Rogers E.: Diffusion of Innovations, Free Press, London, 2003.

[Vo13] Vogl R., Angenent H., Bockholt R., Rudolph D., Stieglitz S., Meske C. 2013. 'Designing a Large Scale Cooperative Sync&Share Cloud Storage Platform for the Academic Community in Northrhine-Westfalia.' In ICT Role for Next Generation Universities - 19th European University Information Systems - EUNIS 2013 Congress Proceedings, edited by Sukovski U, 205-208. Riga: Riga Technical University.

[Wa14] Walter N., Öksüz A., Compeau D., Vogl R., Rudolph D., Distel B., Becker J. 2014. 'Sync&Share North Rhine-Westphalia.'Contributed to the Proceedings of the 22nd European Conference on Information Systems (ECIS 2014), Tel Aviv, Israel. [akzeptiert]

Die organisatorische Aufgabe des DFN-Vereins bei der Erbringung der föderierten Dienste

Michael Röder
DFN-Verein
Alexanderplatz 1
10178 Berlin
roeder@dfn.de

Abstract: Innerhalb des Deutschen Forschungsnetzes mehren sich die Anfragen zur Nutzung gemeinsamer Ressourcen. Ziel ist die Freigabe von sicherheitsrelevanten Daten der Einrichtungen untereinander innerhalb eines sicheren Umfeldes. Eine leistungsfähige Kommunikationsplattform ist mit dem Wissenschaftsnetz vorhanden, die technische Umsetzung innerhalb etablierter Kompetenzzentren ist realisierbar. Die große Herausforderung ist es, ein vertragliches Regelwerk zu schaffen, welches die Nutzung eines Dienstes länderübergreifend gegen ein entsprechendes Entgelt ermöglicht.

Motivation

Aus der abstrahierten Wolke im Zentrum der Strukturskizzen unserer Netzpläne aus der Vergangenheit hat sich mit dem Nutzungskonzept „Cloud-Dienst" in der Landschaft der Informations- und Kommunikationsdienste eine völlig neue Art der Diensterbringung entwickelt. Vor dem Hintergrund einer sicheren Synchronisation und Verteilung von Inhalten unter vertrauenswürdigen Parteien sehen wir uns konfrontiert mit einer Zentralisierung sowohl von Hardware- als auch Softwareressourcen. Die Freigabe der eigenen Infrastruktur wird zum Teil des Dienstes. Selbst die entfernte Verfügbarkeit einer kompletten Entwicklungsumgebung mithilfe einer Webanwendung ist ohne Weiteres realisierbar – zusammengefasst unter dem Begriff der „Platform as a Service". Aber auch das Teilen von Softwarelizenzen ist Teil des Cloudkonzeptes, welches unter dem Stichpunkt „Software as a Service" die temporäre Nutzung einer Softwarelizenz vorsieht. Wenn eine begrenzte Nutzungsdauer absehbar ist, kann eine Lizenz für diesen Zeitraum angemietet werden. Danach verfällt zusammen mit dem Nutzungsrecht auch die langfristige Bindung an die Wartungskosten des Herstellers.

Vielfältige Dienstinhalte vereint auf der Basis gleicher Eigenschaften

Dadurch, dass die Ressourcen auf Nachfrage zur Verfügung stehen, entfällt für die Nutzer neben dem Anschaffungspreis und dem Anschaffungsaufwand auch nahezu der gesamte Administrationsaufwand – diese Grundvoraussetzungen werden auf den Dienstanbieter ausgelagert, der über die technischen Gegebenheiten und die Expertise verfügt. Seinen Grad der Nutzung der geteilten Ressource kann der Teilnehmer dabei innerhalb definierter Grenzen frei skalieren und im Zuge dessen die Leistungseckdaten seiner Dienstnutzung zugunsten einer stärkeren Auslastung oder eines niedrigeren Entgeltes variieren. Vor dem Hintergrund der Nutzung einer örtlich entfernten und nicht selbst betriebenen Infrastruktur muss allerdings in jedem Verhältnis zwischen Anbieter und Teilnehmer auch unmissverständlich die Frage des Umganges mit den personenbezogenen Nutzerdaten geklärt werden.

Benötigt die Wissenschaft eine eigene Cloud?

Das Bedürfnis nach einer Wissenschaftscloud wird durch die Sensibilität der Daten und durch die Notwendigkeit besonderer Umgebungsbedingungen begründet.

Viele kommerzielle Anbieter bieten große Teile der Anforderungen zu günstigen Preisen an, sind aber durch ihre Ausrichtung am Markt auf die Bedürfnisse einer bestimmten Zielgruppe beschränkt. Der Mehraufwand, den es zu betreiben gilt, um sehr spezielle Rahmenbedingungen zu etablieren, kann nicht durch die vergleichsweise geringe Anzahl an Nutzern aus Forschung und Entwicklung vor dem eigenen gewinnorientierten Finanzkonzept gerechtfertigt werden. Intellektuelles Eigentum an Forschungsdaten sorgt beispielsweise für ein gesteigertes Interesse an der verschlüsselten Übertragung der Daten und an der Einhaltung der Urheberrechte.

Die Hoheit über die Diensterbringung innerhalb des Forschungsnetzes zu belassen, bringt darüber hinaus den Vorteil mit sich, dass die Teilnehmer den Speicherort ihrer Daten kennen. Sie können sich sicher sein, dass die Daten innerhalb einer Administrationsdomäne vorgehalten werden, die ihrem eigenen Rechtsraum entspricht; sie werden ihres rechtlichen Handlungsspielraumes nicht dadurch beraubt, dass sich der tatsächliche Speicherort innerhalb anderer Nationen befindet, deren Datenschutzgesetze nicht mit denen der Bundesrepublik Deutschland vereinbar sind.

Weiterhin kann eine Stabilität in der Preisentwicklung gewährleistet werden, wenn an der Diensterbringung ausschließlich Einrichtungen beteiligt sind, die ohne Gewinnansprüche wirtschaften.

Voraussetzungen für einen föderierten Dienst

Wenn sich in der Erbringung der Informations- und Kommunikationsdienste innerhalb des Deutschen Forschungsnetzes hinreichend viele Dienstanbieter etablieren, die die nachgefragten Bedürfnisse vieler Teilnehmer befriedigen können, dann sind wissenschaftliche Cloudanwendungen sichere Alternativen zu den Lösungen kommerzieller Anbieter. Diese Dienstanbieter sind in Form „privater Cloudanbieter“ vorhanden – ihr Wirkungskreis ist jedoch beschränkt auf wenige Einrichtungen, die sich entweder innerhalb einer Organisation oder einer gemeinsamen Administrationsdomäne befinden.

Trennung der Zuständigkeiten

Der DFN-Verein ist zuverlässiger Ansprechpartner für die Erbringung von Informations- und Kommunikationsdiensten im wissenschaftlich-technischen Umfeld der Forschung und Entwicklung. Seine Mitarbeiter verfügen über das nötige Fachwissen, um die administrativen Fragen zu lösen, die gestellt werden, wenn Geldflüsse über die Grenzen einzelner Bildungseinrichtungen hinaus gerechtfertigt werden müssen. Die vertraglichen Regelwerke, mit deren Hilfe die Zusammenarbeit der Anwender des Deutschen Forschungsnetzes untereinander organisiert wird, haben sich bewährt. Gleichzeitig besteht beim DFN-Verein nicht das Interesse, einen eigenen Cloud-Speicher-Dienst zu etablieren.

Um die anbietenden und teilnehmenden Einrichtungen administrativ miteinander zu verbinden und gleichzeitig das Erstellen der Regelwerke nicht in den Einrichtungen selbst geschehen zu lassen, benötigen beide einen vertrauenswürdigen Partner.

Durch die Bereitstellung einer einheitlichen Vertragsstruktur erfüllt der DFN-Verein seine Aufgabe, die Expertise der Anbieter weiter voranzutreiben und die bestehenden Infrastrukturen für alle Anwender am Deutschen Forschungsnetz zur Verfügung zu stellen.

Freiheitsgrade und Allgemeingültigkeit des Regelwerkes ausgewogen gestalten

Um für vielschichtige Forschungsergebnisse zu sorgen, ist ein breit aufgestellter Erprobungsmarkt notwendig – dieser Effekt steigt mit wachsender Anzahl der Anbieter. Die Anzahl der Anbieter ist stark abhängig von der Planungssicherheit, mit deren Hilfe sich anfallende Kosten für die Diensterbringung auch über einen mittelfristigen Zeitraum zuverlässig kalkulieren lassen. Der Anbieter eines Dienstes benötigt Spielraum in der Leistungsbeschreibung bzw. -erbringung, um seine eigene Infrastruktur optimal nutzen zu können. Freiheitsgrade in der Umsetzung stellen aber auch Abgrenzungsmerkmale dar, mit denen sich ein Anbieter von anderen Anbietern unterscheiden und damit unter Umständen an Attraktivität für Interessenten mit besonderen Anforderungen gewinnen kann. Daher liegt es im Interesse aller beteiligten Parteien, die statischen Vorgaben bei der Erstellung der Diensteigenschaften des zu erbringenden Dienstes gering zu halten.

Mit einem einfachen Entgeltschema soll für alle Anbieter und Teilnehmer für klare Rahmenbedingungen gesorgt werden. Dabei ist für eine gemeinsame Basis zu sorgen, auf der das Abrechnungsmodell nachvollziehbar aufbaut. Zusätzlich ist aber zu beachten, dass sich Unterschiede in der Diensterbringung auch in Abweichungen der Entgeltmodelle zueinander abbilden werden. Auf der Grundlage maximaler Gemeinsamkeiten müssen demzufolge auch Freiräume für Spezifika bleiben.

Ein zentral entwickeltes Vertragsmanagement sorgt für gleiche administrative Strukturen unter allen Beteiligten. Sowohl Anbieter als auch Teilnehmer binden sich mithilfe der im Folgenden definierten Regelwerke an den DFN-Verein und bekommen gleichzeitig eine Mustervereinbarung geliefert, die sie in die Lage versetzt, eigene Rahmenbedingungen zu schaffen.

Das Konzept der föderierten Dienste

Jährlich findet gemäß der Satzung des DFN-Vereines mindestens eine Mitgliederversammlung statt. Ziel der Mitgliederversammlung ist es, über den Verlauf aktueller Aufgabenstellungen Bericht zu erstatten und neue Ziele anhand der Bedürfnisse der Teilnehmer am Wissenschaftsnetz zu definieren. Die Ergebnisse der Versammlung werden im Rahmenprogramm für Forschung und Entwicklung festgehalten und durch den DFN-Verein veröffentlicht.

Durch die Aufnahme des Programmschwerpunktes „föderierte Dienste“ hat sich der Fokus bei der Diensterbringung des DFN-Vereins verlagert. Die Planung, Konzeption und Umsetzung zentraler Dienste steht nicht mehr im Mittelpunkt, sondern wird verdrängt durch die Organisation von Diensten, die von Einrichtungen im Deutschen Forschungsnetz für Einrichtungen im Deutschen Forschungsnetz erbracht werden. Daraus ergibt sich das Potential, die Expertise zu bündeln und mit maximaler Effektivität in Form von Dienststrukturen zur Befriedigung der Bedürfnisse anderer Einrichtungen mit nicht-technischer Ausrichtung verfügbar zu machen.

Veranschaulichung der Beziehungen aller beteiligten Parteien zueinander

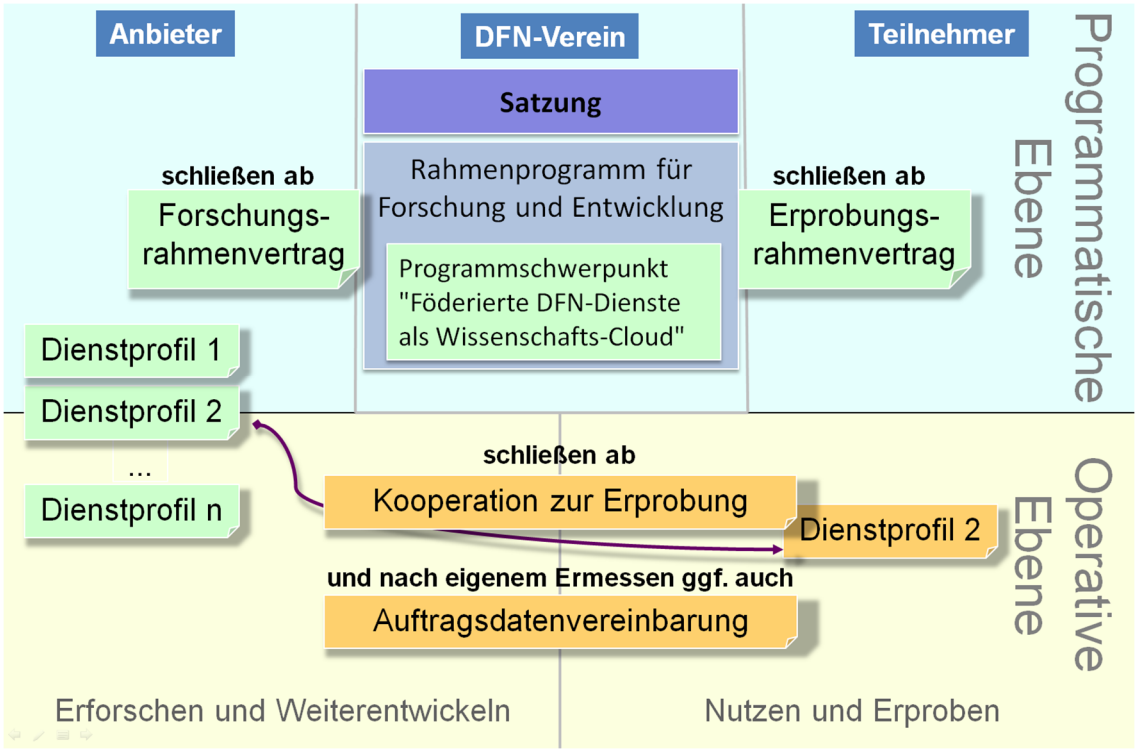


Abbildung 1: Konzept: föderierter Dienst

Eine gemeinsame Basis wird dadurch gebildet, dass sich sowohl Anbieter als auch Teilnehmer am föderierten Dienst mithilfe einer Dienstvereinbarung an den DFN-Verein vertraglich binden. Die Rolle des DFN-Vereines beschränkt sich ausschließlich auf diejenige des Interessenvertreters und Organisators.

Nach Abschluss eines Forschungsrahmenvertrages entwirft der Anbieter für seine eigene Internetpräsenz ein Dienstprofil, welches die Leistung des von ihm angebotenen Dienstes ausschließlich fachlich und technisch beschreibt. Ein föderierter Dienst kann dabei durchaus von verschiedenen Einrichtungen angeboten werden. Alle Dienstprofile werden zentral auf dem Internetauftritt des DFN-Vereines gesammelt und verlinkt. Der DFN-Verein erstattet dem Anbieter ein Entgelt in dem Umfang, in welchem der Dienst von seinen Teilnehmern in Anspruch genommen wird.

Auf der Basis des Dienstprofils, welches sich am besten auf seine Bedürfnisse abbilden lässt, geht der Teilnehmer auf den Anbieter seiner Wahl mit dem Ziel zu, eine Kooperationsvereinbarung abzuschließen. Nach eigenem Ermessen und Ausgangslage ist darüber hinaus der Abschluss einer Datenverarbeitung im Auftrag notwendig. Sowohl für die Erprobungsvereinbarung als auch für die Auftragsdatenvereinbarung liegen beim DFN-Verein Muster bereit.

Aus dem vorgestellten Konzept geht hervor, dass sich der Entwurf über zwei deutlich voneinander getrennte Ebenen erstreckt. Auf der programmatischen Ebene stehen mit Teilnehmer, Anbieter und dem DFN-Verein drei Parteien miteinander in vertraglicher Beziehung, während der DFN-Verein an der eigentlichen Diensterbringung nicht beteiligt ist. Auf operativer Ebene verbleibt das Verhältnis der Nachfrager zu ihren Endnutzern in deren

interner Verantwortung – die Option, den DFN-Verein zur Schlichtung anzurufen bleibt beiden unbenommen.

Alle beschriebenen Vertragsdokumente liegen beim DFN-Verein abrufbereit vor.

Eine Abstraktionsebene über dem Konzept

Die Argumentation bei dem Konzeptentwurf basiert darauf, dass das Deutsche Forschungsnetz nicht nur ein Netzwerk ist, um Forschungseinrichtungen miteinander zu verbinden. Es ist gleichzeitig ein Netz, an dem geforscht wird.

Kommerzielle Anbieter verfügen unter Umständen bereits über ähnliche Angebote. Das Interesse an der Umsetzung sehr spezifischer Insellösungen ist jedoch häufig sehr gering. Dem steht gegenüber, dass ein Dienst, dessen Parameter einzigartig unter den Informations- und Kommunikationsdiensten sind, sehr gut für die Erforschung geeignet ist. So können beispielweise neue Verschlüsselungstechnologien oder eine Anbindung an die DFN-AAI im laufenden Betrieb erprobt und weiter entwickelt werden. Die Grundlage dafür bilden ein ausgeprägtes Vertrauensverhältnis und eine hoch-performante Infrastruktur, die das Wissenschaftsnetz bereitstellt.

SWITCHdrive – automatic deployment of a scalable cloud service infrastructure

Jens-Christian Fischer
Peta Solutions
SWITCH
Werdstrasse 2
CH-8004 Zürich
jens-christian.fischer@switch.ch

Abstract: SWITCHdrive is an ownCloud 6 based file sharing tool that is provided for Swiss academic institutions. We describe how the service is implemented and what tools we use to deploy and maintain a scalable infrastructure. The use of DevOps practices, high degree of automation and continuous deployment make the infrastructure robust and easy to maintain.

In addition, we highlight a number of problematic architectural choices that are present in the ownCloud code base, and how they limit or decrease overall performance of the system.

Situation

SWITCH is the National Research and Education Network of Switzerland and provides a variety of infrastructure services to universities and other tertiary education institutions. This ranges from access to the Internet, federated single sign on, security audits, collaboration software and more. A process called "Innovation Engine" [SW14] allows the institutions to propose new services. One of the often-heard needs from the academic community was for a Switzerland-based file sharing solution, similar to Dropbox.

In 2013, SWITCH ran the BCC (Building Cloud Competency) project to build and operate an OpenStack/Ceph based cloud. The BCC cluster consisted of 10 Intel/AMD servers (Quanta/Delta) with 16 – 24 cores, 128 GB RAM and several COTS 3 TB SATA disks for storage. It ran OpenStack Folsom with Ceph Cuttlefish as a distributed storage system.

SWITCHdrive is not only seen as a valuable service to the community, but also as a validation of a second, upcoming offering from SWITCH: The SWITCH Cloud, an OpenStack based cloud offering that will go productive during 2014.

Pilot Phase

In 2013 SWITCH ran a pilot project with two competing software solutions (ownCloud 5 and PowerFolder). Each software was installed on a virtual machine in our test OpenStack cloud and had around 250 users who shared around 1 TB of data in total. After a test period of two months a survey was sent out to the users. Their feedback showed that there was a need for SWITCH to provide a file sharing service. In addition, the users clearly liked the ownCloud UI better than the one provided by PowerFolder. The word from the engineering team was that the ownCloud installation cost a lot more in terms of problem solving, performance optimizations and general handholding, than the competing PowerFolder installation (which ran without any intervention).

Cloud Infrastructure

Because SWITCHdrive is used to validate the SWITCH cloud offering, and to gain experience with running a moderately complex service on "the cloud", we decided to run the complete system purely virtualized on the hardware that was used to power the test cloud. The currently used OpenStack cluster consists of one controller node, and 8 compute nodes (24 core, 128 GB RAM) and a Ceph cluster (on the same hardware) consisting of 51 3 TB disks for a total of 139 TB raw storage (around 46 TB of real storage, with triple replication of data).

The cluster runs on Ubuntu 13.10 with OpenStack Havana (2013.2.1) and Ceph Dumpling (0.67.7). Besides SWITCHdrive, the cluster hosts a number of other projects (partly from SWITCH, partly from universities) for a total of 91 virtual machines. The Ceph cluster stores around 80 TB of provisioned volumes (which actually only use around 10 TB of real storage), 350 GB of object storage and 1.2 TB of OpenStack related data (images and snapshots). So far, no throttling of resources (especially disk IO) has been implemented, although that is something we are keeping an eye on should we encounter VMs that hog IOPS.

Architecture

ownCloud is a classic single-server LAMP (Linux, Apache, MySQL, PHP) application and can be installed in a couple of minutes on a server with the necessary software installed. While this is great for small installations in small enterprises or workgroups, the general consensus at the time of deployment of our ownCloud infrastructure was that this wouldn't necessarily scale to the number of expected users (50–100 thousand users in Swiss academia). We therefore applied normal scaling techniques for web applications and came up with the following multi-tier architecture of the system.

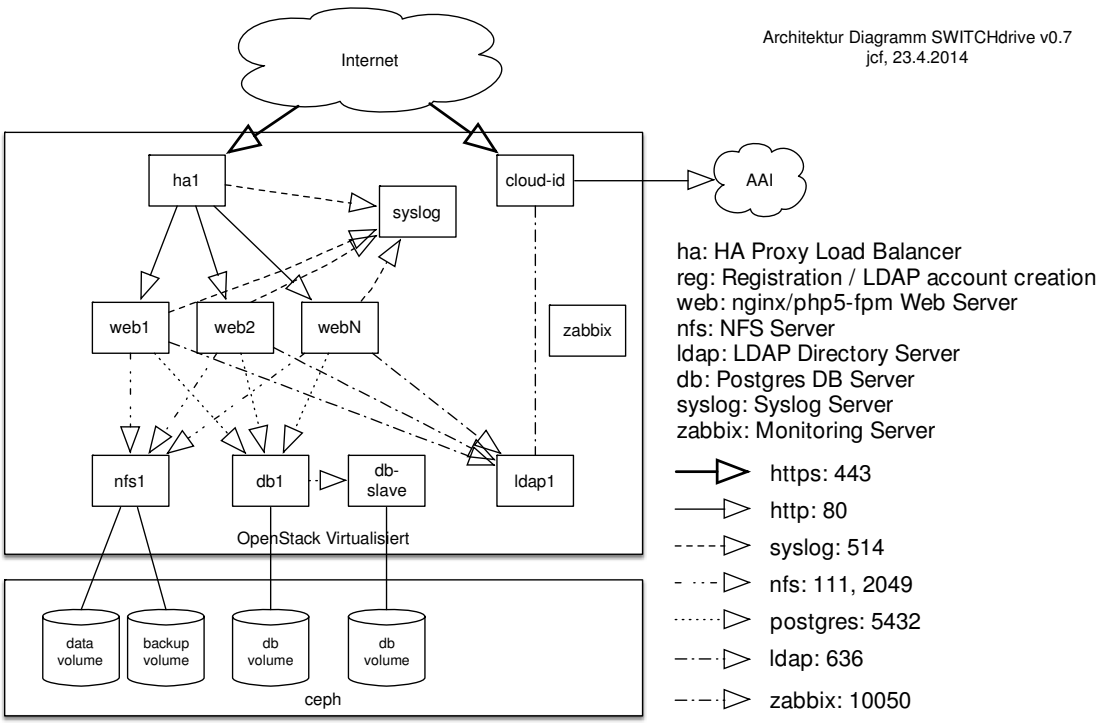


Figure 1: Architecture Overview of the ownCloud installation

The complete stack is running virtualized (contrary to the advice that was given by Hildmann et al [Hi13], where the database servers are run on dedicated hardware). We are closely monitoring the load on the database servers, and will re-evaluate the decision to run virtualized should we measure significant performance issues in the database layer (or indeed, in any other layer of the system).

Starting from the top, all incoming requests are handled by one instance of the HAProxy [Ha14]. HAProxy terminates SSL and distributes incoming requests to a number of web/application servers. SSL termination is made here, in order for the load balancer to be able to manipulate cookies of each request to a) bind one client session to a specific web server and b) to make the cookies from ownCloud "secure". The VM running HAProxy has 2 vCPUs and 4 GB of vRAM. HAProxy uses an evented architecture that runs on 1 CPU, so adding more CPUs will not increase performance.

The requests (now HTTP) go to a number of web servers, which run nginx [Ng14]. We choose nginx over Apache because nginx is a faster and more lightweight webserver, and the only functionality needed is to serve static files and to proxy requests to the PHP backend. For PHP we use PHP5-FPM [Ph11], configured to run between 5 and 20 PHP application processes at any time and dynamically scaling up or down the number of processes according to load. The VMs configured for this task have 8vCPUs and 32 GB of RAM each (which seems to be too much, and we will likely scale them back as we gain more experience with the system). We run ownCloud version 6.0.2 Enterprise Edition, with a minimal set of ownCloud apps enabled (Pictures, LDAP).

The database server is running PostgreSQL 9.3 in a replicating master/slave configuration. The database servers each are configured as 8vCPU, 32 GB RAM machines, with a 100 GB RBD volume for the database. Based on our initial data, this should allow them to scale up to handling at least 5000 users while still serving the complete database from memory and possibly more. The slave server is not in active use yet, it is acting as hot standby and could be used as a read slave if the need arises. We ran initial experiments with load balancing the SQL queries through PGPool II [Pg14] and saw the read load being spread out across the two servers, but the overall DB transaction time almost doubled due to the additional processing and network hops needed. For the time being, we have directed all queries to the DB master and will evaluate the use the load balancer, should we run into performance issues in the future.

Our biggest concern in terms of scalability is the actual storage for files. Each application server needs access to the same file system, which means that we either need a distributed file system or a powerful centralized server. As we use Ceph, we looked at using CephFS, a fully distributed file system as the base of our storage. Unfortunately, CephFS is not considered production ready until the end of 2014, so that option was not viable. Because we hope to use CephFS later, we did not investigate other shared file systems, but opted for a transitional solution, using a NFS servers with a 20 TB sized, RBD backed, volume. The installation is a stock NFS server. We are closely monitoring the load on the virtual machine and the IOPS. Based on our initial data, we see heavy activity (and high IO wait times) when new clients perform their initial upload (or download their data to a new client), and quiet times for regular operations. Based on this usage pattern, we are confident that we can use this solution for several thousand clients, at which time CephFS should be a viable option.

User management is handled via a stock OpenLDAP server. The initial provisioning of LDAP accounts is handled by registration software we have written that logs in users via AAI/Shibboleth, creates an account in LDAP and in addition allows users to change their passwords (or reset forgotten passwords). This software is being extended so that administrators of participating institutions and universities can manage their users directly (terminate accounts, manage quota, etc).

A dedicated Rsyslog server collects the logfiles from HAProxy, nginx and ownCloud so that we have a central, consolidated view on the activity of the system. A Zabbix [ZA14] server collects metrics of all servers and the running applications, giving us an up to date picture of the workings of the whole system.

Installation & Management

Installation and configuration of the complete stack is fully automated via a set of Ansible [An14] "playbooks". This allows us to go from a set of freshly installed servers or virtual machines to a running ownCloud installation with one command in around 30 minutes. The Ansible playbooks specify all commands that need to be run on each server, and all configuration options or configuration files. With this, we have (almost) complete hands-off installation for the complete system, and total hands-off automation for common tasks (like adding or removing a web server from the system or performing basic maintenance on it).

In addition, we can treat almost any part of the system as "throw away". Should a virtual machine become flakey (we have seen one instance of a web server that started to misbehave, for example) we will not try to fix that machine, but throw it away and install a fresh one from scratch instead. This process is done in a couple of minutes.

Configuration changes to the system are also made through Ansible. The changes are defined in the various

Open Sourced

We are working on open sourcing the Ansible playbooks and will release them in May 2014 on https://github.com/switch-ch/owncloud-ansible and https://github.com/switch-ch/cloudservice-owncloud.

They can act as a basis for an individual, large-scale installation of ownCloud.

Problems / Solutions

The process of setting up this ownCloud instance took around 4–5 months. We started with basically the same architecture as described above and spent quite a bit of time monitoring, measuring and tweaking the system. During that time, a number of problems in the ownCloud code were identified and either worked around, patched or reported to the developers.

The general impression of the ownCloud software is mixed. While the UI and the functionality generally are of high quality, the code itself and the architectural decisions made, show that ownCloud wasn't designed for large-scale installations. We spent a lot of time instrumenting the code, profiling and hunting for performance bottlenecks. Below are a few of the findings and remedies we found (everything is based on ownCloud 6 and the various minor releases, and the 1.5 line of the desktop client).

We uses various tools to measure performance – everything from log file analysis down to TCP dumps of the network traffic between clients and servers, and internal server to server communication. To look "into" the PHP code, we employ New Relic RPM on one of the application servers. It gives us a near real time view of what the application server is doing, and shows long running operations and what PHP functions or database calls were being made. This has proven to be invaluable in determining some of the problems described below.

Upload performance

Uploading a number of small files via the desktop client (something we consider a normal use case in an academic environment) is rather slow (less than one file per second). We spent large amounts of time on determining the root cause (ownCloud suggested that our NFS server was the culprit, but we were able to show that this was not the case).

The desktop clients perform a HTTP PUT request (using the WebDAV protocol) to upload files. The 1.5 client does this sequentially, one file after the other. This in itself wastes quite a bit of time, due to the HTTPS connection being setup fresh for every file uploaded. But there are more issues. RPM allows us to drill down into the code of the requests. Fig. 2 shows a pathological slow request (over 15 000 ms) for an upload:

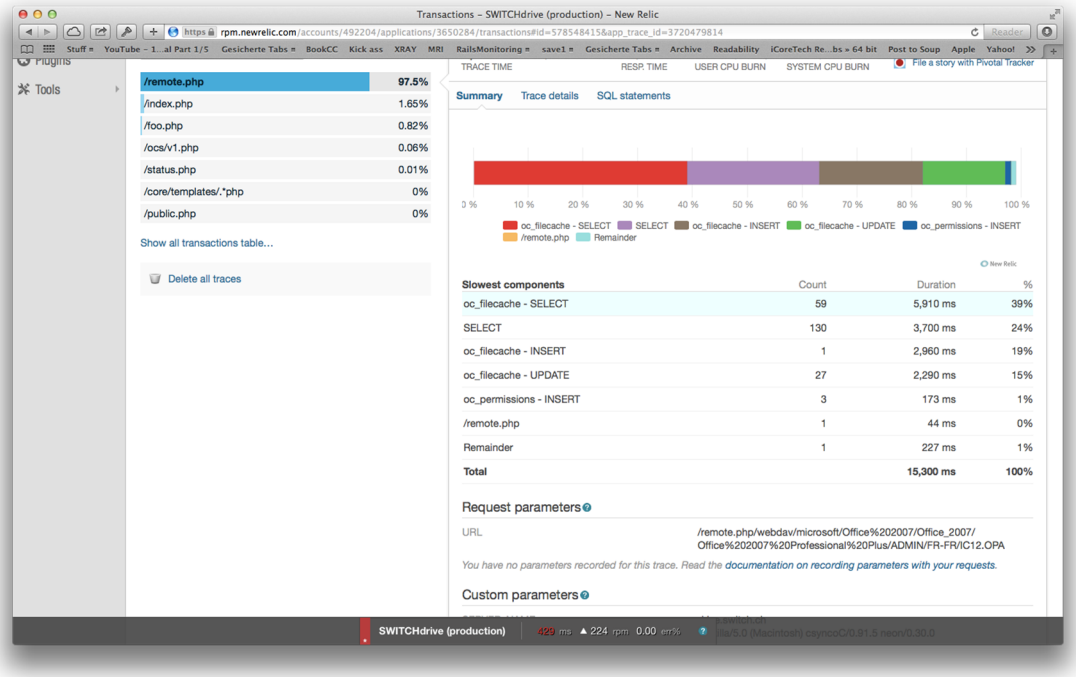


Figure 2: Breakdown of slow upload request

We see several interesting things here: There seems to be a general problem with the database server for this specific request: An INSERT that takes almost 3 seconds is way too slow. But leaving aside the DB performance, we note something else: A single file upload causes around 180 different SELECTs into the database. Even with a response time of 1 ms per request, this takes almost 200 ms per file upload – for a web application, that is a long time. ownCloud engineering has since changed that and reduced the number of database calls being made. This will appear in ownCloud Version 7.

Session locking

Another thing we commonly saw were extreme long times when requests were stalled because they were waiting for the PHP session to be “constructed”. PHP stores session information in a file. On every request, the file is opened and locked until the HTTP request is finished. If there are multiple parallel requests from the same client, all requests are blocked until the first one finishes, after which the next one gets executes, while the remaining requests still are blocked. This causes delays in the Web UI, especially because some requests can take a long time to

complete. The deletion of a folder through the WebUI for example will trigger the deletion immediately, and it is executed in the web request. This can easily block the WebUI for seconds up to 1 or 2 minutes.

Static files via PHP

Another problem is caused by the fact that many static files are sent via PHP instead of the webserver. Again, this blocks the client from issuing more requests. Examples included an error in setting the X-SENDFILE headers correctly when serving files through the WebUI and the storage being an NFS server with user quotas set. (This has been fixed in 6.0.2). Another – as of now still unfixed – case is the SabreDAV library that ownCloud is using for handling WebDAV requests. It does not use the webserver's capabilities to serve files, but sends them from the PHP process – again tying up the server due to the session locking.

JS and CSS files not combined

The WebUI loads a number of JavaScript and CSS files. Contrary to common best practices, these files are not combined into one JavaScript and one CSS files, but are served individually:

/remote.php/core.css
/index.php/apps/files/css/files.css
/index.php/apps/files/css/upload.css
/index.php/core/js/config.js
/remote.php/core.js
/apps/files/js/file-upload.js
/apps/files/js/jquery.iframe-transport.js
/apps/files/js/jquery.fileupload.js
/apps/files/js/jquery-visibility.js
/apps/files/js/filelist.js
/apps/files/js/fileactions.js
/apps/files/js/files.js
/apps/files/js/keyboardshortcuts.js

This is the list of files that is loaded. Those marked bold are served via PHP – the result is immediately visible in the Network timeline of the web browser:

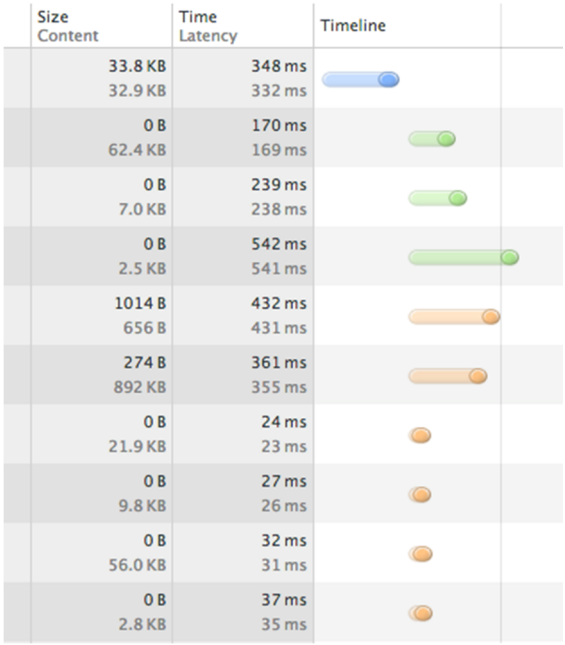


Figure 3: Serialized serving of files

The blue bar shows the load time for the HTML, the next 5 lines are the CSS and JS files requested via HTTP, while the following lines show the JS files that could be served (in parallel) by the web server directly. All in all, this leads to a delay of over 500 ms for every page request through the WebUI. This will be fixed in ownCloud 7.

File system vs. Database view of the world

In the current ownCloud architecture, ownCloud assumes that the files stored in the file system can change without knowledge of the application. This comes from the original design, where ownCloud was installed on a single user's server or NAS and there was a use case that a user manages files directly on the server. In a large multi user environment, this doesn't hold true anymore.

We experienced several issues where this assumption led to slow performance and even data loss. In one case, one of our web servers rebooted (planned) and did not mount the NFS share. The web server saw just the empty mount point. All clients that were landing on this particular server were treated as "new clients", that is the initial folder structure was recreated. All information for that client in the database was deleted. The files were also deleted on the client's computer. We had to restore a database backup to get the information back. When the mount was restored, the clients received the files again.

The ownCloud code also walks the user's directory structure on the server on each request to determine if there were any changes. ownCloud is considering to make that a configurable option.

Conclusion

The current version of ownCloud shows its heritage as a solution for small groups of people, on small servers. Building a scalable infrastructure is a task that takes a couple of months from initial design to a fine-tuned system. The two biggest problems areas are the database and the

shared file system – both are single points of congestion. Approaches like using distributed (No)SQL databases for metadata storage or Object Storage instead of a shared file system would probably alleviate those problems and make for easier scalability.

There is little literature and very little in terms of actual implementation detail for large scale installations. By open sourcing our implementation, we hope to spark collaboration in getting other implementations kickstarted.

We have found it very helpful to investigate the inner workings of ownCloud, both by instrumenting the code and actually looking at system calls and network traces. This has helped to identify a number of bottlenecks in the code.

Literature

[An14] http://www.ansible.com/

[Ha14] http://haproxy.1wt.eu

[Hi13] Hildmann T.; Kao, O.: Deploying and extending on-premise cloud storage based on ownCloud (draft), June 2013

[Ng14] http://nginx.org

[Ph11] http://php-fpm.org

[Pg14] http://www.pgpool.net/

[SW14] SWITCH, Innovation Engine, http://www.switch.ch/uni/innovation/ (Accessed 23.4.2014).

[ZA14] http://www.zabbix.com

Pilotbetrieb einer On Premise Cloud an der RWTH Aachen University

Dörte Rosendahl
IT Center
RWTH Aachen University
Seffenter Weg 23
52074 Aachen
rosendahl@itc.rwth-aachen.de

Abstract: Mit dem vermehrten Aufkommen von mobilen Endgeräten entstand für die Nutzer an der RWTH Aachen University der Bedarf, die Daten auf diesen Endgeräten jederzeit sichern zu können sowie diese Daten auf mehreren Endgeräten, auch auf verschiedenen Plattformen, zur Verfügung zu haben.

Die Nutzung einer Public Cloud wie z. B. Dropbox, Google Drive, iCloud usw. kam aus Datenschutzgründen, wie z. B. wegen der Geheimhaltung von Forschungsergebnissen, für dienstliche Zwecke nicht in Frage.

Das IT Center der RWTH Aachen betreibt seit 2012 eine On Premise Cloud im Pilotbetrieb, eingesetzt wird hierfür die Software inSync der Firma Druva. Der Pilotbetrieb ist mit vorerst 800 Lizenzen gestartet und richtet sich an die Mitarbeiter der RWTH. Neben der Datensicherung und Synchronisation der Endgeräte eines Nutzers ist auch das Sharing von Daten mit anderen Nutzern u.a. auch mit externen Kooperationspartnern möglich.

Die Erfahrungen mit dem Betrieb der sog. RWTH Cloud sind weitgehend positiv und es ist eine steigende Akzeptanz dieses Dienstes an der RWTH Aachen zu beobachten. Einen wichtigen Aspekt für die Zufriedenheit der Nutzer stellt u.a. der Support dar, der seitens des IT Centers für diesen Dienst geleistet wird.

Motivation

„Sowohl im privaten als auch im dienstlichen Bereich gibt es immer mehr Laptops, Smartphones und Tablet-PCs, die sogenannten mobilen Endgeräte, das verändert die Arbeitsweise moderner Unternehmen und stellt IT-Abteilungen vor völlig neue Herausforderungen:

- *Auf Endgeräten befindliche kritische Unternehmensdaten müssen per Backup gesichert werden.*
- *Auf Endgeräten befindliche sensible Unternehmensdaten müssen vor Sicherheitsverletzungen geschützt werden.*
- *Mitarbeiter, die bei der Zusammenarbeit mit internen und externen Beteiligten Dateien gemeinsam nutzen, müssen dies auf sichere Weise tun.“*

[Dr00]

Die oben genannten Ausführungen betreffen gleichermaßen Universitäten und Hochschulen, u.a. auch die hier vorgestellte RWTH Aachen University.

Das IT Center der RWTH Aachen betreibt seit 1997 für Backup und Archiv eine zuverlässige TSM (Tivoli Storage Manager) Infrastruktur, die sich sehr gut für das Sichern von Servern und festen Arbeitsplatzrechnern eignet (zurzeit ca. 4,7 PB Backup/Archivdaten, 2600 Clients).

Der Fokus dieser Lösung liegt darin, den Einrichtungen die Wiederherstellung von gesicherten Daten mit der Client-seitig technisch realisierten Maximalgeschwindigkeit garantieren zu können, um hierdurch Ausfallzeiten durch Datenverluste zu minimieren.

Seit einiger Zeit werden von Mitarbeitern und Professoren wichtige Daten vermehrt auch auf mobilen Endgeräten gespeichert. Diese Endgeräte können sowohl dienstlicher als auch privater Natur sein. Das soll auch so sein, eine Trennung, d. h. zwei Geräte, ist nicht sinnvoll, da gerade bei Wissenschaftlern (Wissenschaft = wesentlicher Lebensinhalt) eine scharfe Unterscheidung kaum möglich ist.

Das TSM Backup kommt für diese Fälle nicht in Betracht, da es für mobile Endgeräte andere Anforderungen an Datensicherung gibt, zu nennen sind unter anderem:

- Automatisches im Hintergrund laufendes regelmäßiges Backup mit minimaler Benutzerintervention
- Unterstützung von Smartphone- bzw. Tablet-Betriebssystemen
- Zugriff auch von externen Netzen ohne VPN, auch aus Mobildatennetzen mit geringer Bandbreite

Darüber hinaus besteht bei den Anwendern der Bedarf, ihre Daten auf verschiedenen eigenen Endgeräten jederzeit zur Verfügung zu haben sowie diese Daten mit Kollegen oder externen Partnern teilen zu können.

Auf dem Consumer Markt existieren für diese Zwecke eine große Anzahl sog. Public Cloudspeicher, deren Nutzung in einem gewissen Maße für Anwender sogar kostenfrei ist. Zu nennen sind hier z.B. Dropbox, iCloud, Google Drive, MS Skydrive etc. Aus Aspekten der Datensicherheit und des Datenschutzes kommt die Nutzung solcher Dienste für viele Anwendungen an der RWTH Aachen nicht in Frage. Man denke z.B. an den Austausch von sensiblen Daten wie z. B. Forschungsergebnissen, Klausurergebnissen etc., die auch strengen rechtlichen Vorschriften unterliegen.

Zudem liegt der Fokus dieser Public Cloud Dienste hauptsächlich auf Sync und Share und nicht auf das Backup und den Restore von Dateien.

Anforderungen an eine RWTH Cloud

Das IT Center der RWTH Aachen begann sich Mitte 2011 mit der Idee einer eigenen On Premise Cloud für Mitarbeiter und Professoren zu befassen. An der RWTH Aachen existieren z.B. folgende Anwendungsszenarien für einen solchen Dienst:

- Ein Mitarbeiter ist auf Dienstreise und speichert Daten auf seinem Smartphone. Diese Daten sollen auch von unterwegs (z. B. vom Mobilfunknetz aus) gesichert werden.
- Ein Mitarbeiter möchte eine Datei, die er auf seinem Arbeitsplatzrechner gesichert hat, auf seinem Laptop wiederherstellen.

- Mehrere Wissenschaftler an unterschiedlichen RWTH Instituten möchten gemeinsam an einem Dokument arbeiten.
- Ein Mitarbeiter möchte einem externen Partner Dokumente zum Download zur Verfügung stellen.
- Ein Professor möchte seine Vorlesungsdateien überall und auf allen seinen Endgeräten im aktuellen Stand zur Verfügung haben, so dass er z. B. zu Hause an den Dateien arbeiten kann und diese dann später für seine Vorlesung auf seinem Dienstlaptop nutzen kann.
- Die für eine Berufungskommission benötigten Dokumente werden den Mitgliedern der Kommission in einem Share-Bereich zur Verfügung gestellt.

Es wurde vom IT Center ein Anforderungskatalog aufgestellt, den eine solche Cloud erfüllen sollte:

- Einfache Benutzerführung
- Verfügbarkeit von Clients für die gängigen Plattformen und zusätzliche Zugriffsmöglichkeit über Web
- Backup- und Restore-Möglichkeiten inkl. Versionierung der Backupdateien
- Plattform übergreifendes Daten-Sharing (verschiedene eigene Geräte/Partner)
- Möglichkeit der Bereitstellung von Dateien über einen Weblink
- Performanter inkrementeller Upload
- Verschlüsselte Datenübertragung und Datenablage
- Weltweite Erreichbarkeit des Cloud-Servers (auch ohne VPN)
- Einfache Installation und Administration der Server Software
- Möglichkeit der Einrichtung von Profilen für unterschiedliche Benutzergruppen
- Dynamische Quota Regelung
- Konfigurierbare Richtlinien für Backups z. B. Anzahl Versionen, Haltezeiten, …
- Möglichkeit der Anbindung an das Active Directory der RWTH Aachen
- Reportingmöglichkeiten

Implementierung der inSync On Premise Cloud an der RWTH Aachen

Nach einer Sondierungsphase entschied sich das IT Center für die Software inSync der Firma Druva. Die oben angegebenen Anforderungskritierien werden von dieser Lösung erfüllt. Für die Einrichtung des Dienstes als Pilotbetrieb für Mitarbeiter und Professoren wurden zunächst 800 Client Lizenzen beschafft. Die inSync Server Software ist zurzeit auf einem IBM Server (Betriebssystem Scientific Linux) mit 5 TB angeschlossenem SAN Storage installiert.

Die für inSync zusätzlich erhältlichen Optionen Geolocation (Auffindbarkeit eines Gerätes) und Data Loss Protection (Löschen der Endgerätedaten bei Verlust bzw. Diebstahl) werden aktuell aus rechtlichen und Datenschutzgründen vom IT Center nicht angeboten. Zurzeit wird mit dem Security Management des IT Centers geklärt, in wieweit diese Funktionen den Nutzern auf Wunsch evtl. doch zur Verfügung gestellt werden können.

Um die Speicherung und Übertragung von Dateien auf ein Minimum zu reduzieren, setzt inSync Deduplizierungstechnologie ein, dabei verwendet es eine globale und anwendungssensible Deduplizierung auf Clientseite. Auf Serverseite nutzt inSync einen Hypercache, um die meist-referenzierten Deduplizierungsindizes in-Memory zu halten. An der RWTH Aachen wird ein Deduplizierungsfaktor von etwa 1:2 erreicht, insgesamt sind zurzeit ca. 2,56 TB Daten auf 1,11 TB Speicherplatz abgebildet. Backups werden inkrementell durchgeführt.

Für die Übertragung von Clientdaten auf den Server verwendet inSync eine 256-bit SSL Verschlüsselung, bei der Ablage der Daten erfolgt eine 256-bit AES Verschlüsselung. Die zugehörigen Admin- und Client-Webschnittstellen nutzen HTTPS-Zugriff, für den Zugriff auf das Active Directory wird SAML verwendet. Die Serverdaten werden vom IT Center täglich ins TSM Backup gesichert. Auf eine Hochverfügbarkeitslösung mit einem 2. Standort wurde für die (noch währende) Pilotphase zunächst verzichtet.

Administration von inSync

Die Administration des inSync Servers erfolgt über eine Admin-Webschnittstelle. Hier stehen für eingetragene Administratoren u.a. folgende Funktionen zur Verfügung:

- Allgemeine Einstellungen:
    - Netzwerk, E-Mail Adresse für Statusmeldungen, Lizenzverwaltung, …
- Benutzerprofil-Verwaltung, d.h. Anlegen und Editieren von Benutzerprofilen, u. a.:
    - Quota, max. Anzahl Geräte pro Benutzer
    - Backupeinstellungen (Zeiten, Häufigkeit, Haltezeiten, Standardordner, ...)
    - Einstellungen für Sharing (Enable/disable, Anzahl Versionen einer Datei, …)
- Benutzerverwaltung:
    - Anlegen, Löschen von Benutzern, Passwort Reset, Profilzuweisung
- Active Directory Mapping
- Übersichten über Geräte, Backups, Storage
- Erstellung von Reports
- Administratoren-Verwaltung (verschiedene Stufen von Rechten möglich)

Abbildung 1: Startseite der inSync Admin-Schnittstelle

Anbindung an das Backup-Portal der RWTH Aachen

Für die TSM Backup Lösung der RWTH Aachen wurde vom IT Center ein sog. Backup-Portal als Webschnittstelle entwickelt, über das die IT Administratoren der RWTH Einrichtungen ihre eigenen Backup-Knoten selbst verwalten können. Der Zugang zu diesem Portal ist über das Identity Management und die Rollenverwaltung der RWTH Aachen geregelt.

Das Backup-Portal wurde für den Betrieb der RWTH Cloud um die Funktionalität zur Verwaltung von inSync-Benutzerkonten erweitert. Der sog. Backup Administrator einer RWTH Einrichtung kann über dieses Portal Benutzerkonten anlegen oder löschen sowie eine Passwort-Rücksetzung veranlassen. Für das Anlegen neuer Konten wurde im inSync ein RWTH-Standardprofil mit einer Quota von 10 GB Speicherplatz konfiguriert.

Mit Hilfe des sog. RWTH-Partner-Verfahrens ist es weiterhin möglich, inSync-Konten für Gäste von externen Einrichtungen anzulegen, so dass die Share-Funktionalität auch für Kooperationen mit externen Partnern nutzbar ist.

Der inSync Server importiert die vom Backup-Portal gelieferten Daten über seine AD Mapping Funktionalität.

inSync Client

Zurzeit gibt es inSync Client-Software für Windows, Mac, Linux, iOS, Android und Windows Phone. Die Software für Windows- bzw. Apple-Laptops oder -Desktops kann auch über Mass Deployment Mechanismen (SCCM bzw. LANdesk) verteilt werden.

Das IT Center der RWTH Aachen stellt seinen Anwendern die Software für Laptops und Desktops über einen internen FTP Server zur Verfügung. Client Apps für mobile Geräte sind über den App-Store des jeweiligen Anbieters kostenlos erhältlich.

Updates für die Client-Software können auch vom inSync Administrator über die Admin-Schnittstelle angestoßen werden.

Über den Client kann der Anwender diverse Einstellungen für das Backup seiner Dateien bzw. Ordner vornehmen. Zusätzlich wird auch das Backup von E-Mails (u.a. Outlook, Thunderbird, Apple Mail) unterstützt. Über die Restore-Funktionalität des Clients können die gesicherten Daten aller eingerichteten Endgeräte ausgewählt und (auch auf einem anderen Endgerät) zurückgeholt werden.

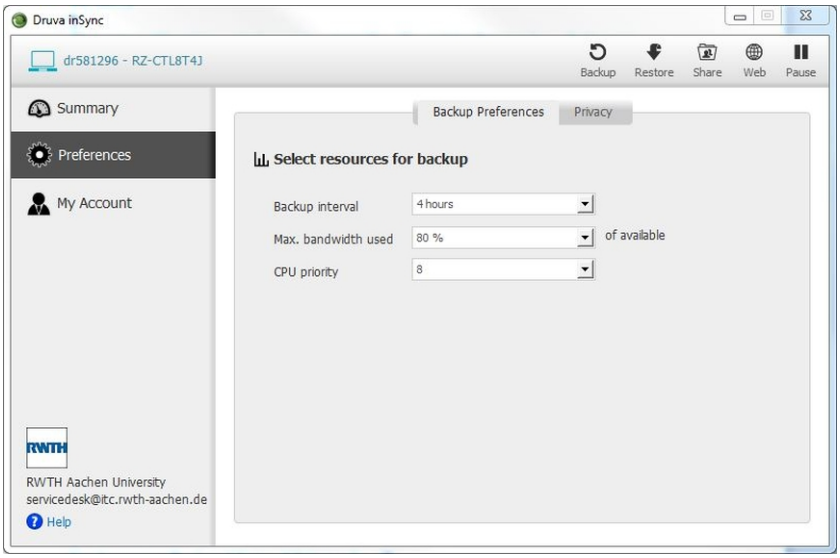


Abbildung 2: inSync Client

Für das Sharing wird auf dem Endgerät automatisch ein inSync Share Ordner angelegt, der, falls gewünscht, mit anderen Endgeräten des Nutzers synchronisiert wird. Die Dateien bzw. Unterordner dieses Ordners können darüber hinaus anderen ausgewählten Nutzern der RWTH Cloud für die Kollaboration freigegeben werden. Weiterhin besteht die Möglichkeit, einen Weblink für Dateien oder Ordner erstellen zu lassen, über den diese für eine befristete Zeit auch Nicht-inSync-Nutzern zum Download bereitgestellt werden können.

Zusätzlich existiert für die Restore- und Share-Funktionalität ein Webclient, welcher über einen Browser auf jedem beliebigen Gerät, auch ohne Installation der Client-Software, genutzt werden kann.

Nutzer-Akquise und Support

Nach einer Testphase mit internen IT Center Nutzern und ausgewählten Ansprechpartnern wurde der Dienst per Anschreiben zunächst den Backup Administratoren der RWTH Aachen

bekanntgemacht. Des Weiteren erfolgte eine Vorstellung des Dienstes bei einem regelmäßigen Treffen der RWTH IT-Administratoren.

Aktuell gibt es 364 eingetragene Benutzer und 515 angemeldete Endgeräte (Stand 16.4.2014). Es stellte sich heraus, dass insbesondere die Share-Funktionalität gefragt ist.

Der 1st Level Support für den inSync Dienst wird vom IT-Servicedesk des IT Centers übernommen, das ggf. Anfragen an das Backup-Team als 2nd Level Support weiterreicht.

Anfragen gibt es hauptsächlich zum Thema Client-Installation, unterstützte OS Versionen, Quota-Erhöhung und zum Löschen von Backups. Probleme, die vom IT Center Personal nicht gelöst werden können, werden in der Regel schnell und kompetent durch den Support der Firma Druva behoben.

Allgemein gibt es von den Nutzern positives Feedback. Gerade in den letzten Monaten bemerkt das IT Center eine steigende Anzahl neuer Benutzerkonten, die auch durch Kollaborationen innerhalb der RWTH Aachen und dadurch bedingtes Kommunizieren des Dienstes an die jeweiligen Kollaborationspartner veranlasst ist.

Die Überlegung, auch Studierende an diesem Dienst teilhaben zu lassen, wurde aus Kostengründen (Lizenzen, Hardwarebedarf, vermehrter personeller Supportaufwand) verworfen, da die Anforderungen der Studierenden im Allgemeinen auch durch Public Cloudspeicher bzw. für Studienzwecke durch andere RWTH Angebote (Campus Office, E-Learning Portal) abgedeckt werden können.

Zukunftsaussichten

Noch ist keine Entscheidung darüber gefallen, ob der inSync Pilotbetrieb in einen regulären Dienst übernommen wird.

Sobald die von der Universität Münster geplante NRW Cloud auch für die Nutzer an der RWTH Aachen bereit steht, ist es denkbar, dass der RWTH Cloud Dienst evtl. in diese NRW-Lösung überführt werden könnte.

Literaturverzeichnis

[Dr00] Druva, inSync Whitepaper „Mehr Power für Endgeräte: Kombination von Datenschutz und Collaboration“, 2012; S. 3

bwSync&Share: A cloud solution for academia in the state of Baden-Württemberg

Nico Schlitter, Alexander Yasnogor
Steinbuch Centre for Computing
Karlsruhe Institute of Technology
76128 Karlsruhe
Nico.Schlitter@kit.edu
Alexander.Yasnogor@kit.edu
Christian Sprajc
PowerFolder
dal33t GmbH
40667 Meerbusch
Sprajc@powerfolder.com

Abstract: Collaboration between scientists is a key factor in answering today's research challenges. Unfortunately, the necessary tools to support such collaboration in a simple and secure manner are not always available in academia. To address this issue, the Karlsruhe Institute of Technology introduced a collaboration service named bwSync&Share in January 2014. The service is a privacy-aware Dropbox alternative for students and scientists in the state of Baden-Württemberg, which allows the synchronization and sharing of documents between multiple devices and users. This paper gives an overview of the service requirements, the software evaluation and the architecture of the bwSync&Share service.

Introduction

Since 2010, the Large Scale Data Facility (LSDF) at the Karlsruhe Institute of Technology addresses the data management and processing requirements of several forthcoming data intensive research experiments. Currently the LSDF is providing storage through common protocols like NFS, CIFS, SFTP and SCP and hosts around 6 PB of storage capacity.

For the last two years, the members of a research project called bwLSDF investigated the advantages and drawbacks of centralized and distributed storage systems and identified the potentials and risks of federal storage usage within the state of Baden-Württemberg. Besides traditional concepts such as Network-Attached Storage (NAS) and Storage-Area-Network (SAN), we were looking into new approaches of flexible storage management. Our objective was the development of a new service which offers storage capacities to all students and scientists studying and working at universities in the state of Baden-Württemberg (Germany).

Since the exchange of documents via USB-drives or email is limited and no longer practical, we introduce a service called bwSync&Share in January 2014. The new service is a privacy-aware alternative to the well-known dropbox and allows documents to be synchronized and shared between different users and devices. The service offers synchronization clients for the most common platforms (Windows, Linux, MacOS, iOS and Android) as well as an intuitive web interface to access and share personal documents. The users benefit from easy-to-use,

collaborative and platform independent workflows which enriches the scientific and academic processes.

Challenges

During the deployment of the bwSync&Share service we faced different challenges. In the following, we briefly address the most pressing issues such as identity management, scalability and high availability of the service as well as federated user support.

Federated Identity Management

The bwSync&Share service is available to about 80 scientific organizations and approximately 450,000 users. Therefore, the most important issue was the secure authentication and authorization of users in a state-wide context. Since centralized identity management systems raise privacy concerns a federated Authentication and Authorization Infrastructure (AAI) is essential.

Scalability of the infrastructure

Facing this huge amount of potential users, we as service provider must be able to react quickly and – in the ideal case – automatically to the changing amount of user requests and the resulting load on the service infrastructure. Therefore, a service architecture that ensures scalability is crucial. Areas of scalability of the service architecture specifically cover web, database, CPU load, network traffic and storage I/O. In all areas the solution needed appropriate answers to handle high service utilization, while reducing the required resources to a minimum on idle. Moreover the service should horizontally scale to reduce maintenance efforts and have a simplified, automated setup of new service resources. This also implies that the service automatically balances the load within the application layer.

Availability of the infrastructure

Besides the highly-scalable architecture, robustness against failure of single infrastructure components (SPOF) is fundamental. The solution should offer redundancy for all components on all layers of the architecture spanning application, web, database and storage layer. Since the service operates on top of shared storage common challenges of HA cluster systems needed to be addressed such as the “split-brain” problem. The service should also support the gradual upgrade of parts of the system, such as nodes within the application and web layer, without noticeable downtime for the end-user.

Federated user support

In many cases, providing a detailed step-by-step user guide is not enough to satisfy the end users. Instead, direct communication via email or phone is necessary to solve user problems. However, the huge number of users of a state-wide service makes it difficult to maintain user support on such a level. Thus, we were looking for possibilities to federate this task, in a way that not only the service provider supports users – but instead each university is responsible to help their users on their own. As a result, KIT offers first-level-support to KIT users only. In addition, we provide second-level-support to the helpdesk teams of the state universities.

Software Evaluation

In 2013, we carried out an extensive software and vendor evaluation to find the software which matches the requirements of the bwSync&Share service best. In order to get a realistic impression of the available software solutions, we built multiple test environments for the sync and share software developed by Druva, OwnCloud, PowerFolder and TeamDrive.

Evaluation Process

We used numerous criteria such as scalability of the software, supported authentication methods and flexibility of the software vendor, to decide which software is most suitable from a provider's perspective. User's perspective was taken into account by opening the test environments to test users from the nine universities in Baden-Württemberg. After the tests, we asked the users to complete an online questionnaire which focused on general usability and feature-completeness.

Our final product decision was based on our experiences during test operation and the feedback of the test users.

Product Decision

After finishing the software tests, we came to the conclusion, that the software provided by PowerFolder is the most suitable solution for the bwSync&Share service.

Since PowerFolder supports federated AAI based on Shibboleth and SAML, the bwSync&Share service is built on top of an AAI which was drafted, designed and implemented within the bwIDM project. This infrastructure is based on a system called Shibboleth which implements the Security Assertion Markup Language (SAML) standard to forward authentication and authorization information of users from an identity provider (IdP) to a service provider (SP). The pre-established trust between IdP and SP enables a federated identity management where the IdP is in charge of providing verified user identities and the service provider accepts the transmitted credentials. This functionality fulfils the bwSync&Share requirements perfectly and was therefore chosen to be used.

The adaptation architecture of the PowerFolder software is highly scalable and allows the dynamic adaption of the infrastructure to the current needs. In addition, the client supports transferring files and deltas directly from device to device (Peer-to-Peer) thus reducing the load on all service endpoints, especially in federated sharing scenarios. This technology also reduces the network traffic at Karlsruhe Institute of Technology and within educational networks in Baden-Württemberg. Furthermore, the software is fully clustered and proved to be robust against partial failure of the infrastructure.

Besides the technological aspects, the vendor of the PowerFolder software proved to be a reliable partner during our evaluation period. Support requests were answered in a prompt and competent fashion and the company was anxious to pursue numerous feature requests.

Finally, long-term experiences at GWDG in Gottingen and myDisk in Luxemburg strengthened our decision to use the PowerFolder software.

The bwSync&Share service

Since January 2014, the bwSync&Share service is available to about 450.000 students and scientist, studying and working in the state of Baden-Württemberg. In addition, external partners from all over the world can be invited to the service. Thus, the service allows users to collaborate within and between scientific organizations in Baden-Württemberg and beyond.

Features

After registering for the service, 10 GB personal storage capacity gets available to each student or scientist in the state of Baden-Württemberg. External users, which can be invited to the service, have no personal storage but can get access to the storage capacities of the invitee.

The provided storage capacities can be used to store research related data. To simplify the data transfer between different users or devices, we provide a synchronization tool for Linux, Windows, MacOS, iOS and Android, which allows an automatic data exchange. In addition, the service offers an easy to use web interface to manage the stored data.

Other than Dropbox, GoogleDrive or SkyDrive, the data of our users is stored on the premises of the Large Scale Data Facility at Karlsruhe Institute of Technology and therefore German privacy laws apply.

The service is funded for a period of three years by the Ministry of Science, Research and the Arts Baden-Württemberg and is therefore free of charge for all users during this period.

User Management

Particular attention was given to user authentication and authorization. The bwSync&Share service supports shibboleth accounts and external accounts. Irrespective of the account type, all users have to complete a registration process to accept the service conditions.

User registration is handled by a self-service portal which was original developed within the bwIDM project. Students and scientists working in the State of Baden-Württemberg can login to the portal and authenticate themselves using the Web-SSO Shibboleth profile. This profile redirects the user to an authentication page provided by its home university. If the user credentials are successfully checked, the user and some user specific information are sent back to our service. The user information contains the user's first name and surname as well as the belonging email addresses and a so called entitlement which specifies if the home university grants the permission to use the bwSync&Share service.

After the successful login to the self-service portal, the user can register for the bwSync&Share service. After the user accepts the service conditions, the portal applies an API call. In addition, the bwSync&Share service in order to create the user account including first name, surname and mail addresses. In addition, the storage capacity that will be available to this user is defined.

After finishing the registration the user has access to the service and can be authenticated using the shibboleth credentials. Of course, the service was designed in a way that shibboleth credentials can never be intercepted by our service. Instead, the service uses either the Web-SSO profile or the Enhanced Client or Proxy profile (ECP) to check the validity of user credentials.

The external accounts are provided for users who are not members of a state university. These accounts are initially created when a shibboleth user shares a folder with a user that does not

exist yet. New users are invited by adding their email address to the access control list of a folder. Subsequently, the invited user receives a welcome message via email which contains some information about the service and its purpose. In addition, the invited user gets informed that its account is deactivated until the registration process including the acceptance of the service conditions is completed. Unfortunately, at the time this message is sent out, the system is not able to decide if the invited user is a shibboleth user or an external user. Therefore the welcome email contains an explanation and two URLs: The first one links to the former mentioned registration portal which can be accessed using shibboleth credentials. The later one links to a special registration process for external users which asks for the first and surname of the user and allows the external user to specify a password for the bwSync&Share service.

Service Architecture

We consider the bwSync&Share project as a big, state-wide cloud service which should be available and scalable for adaptation of current service utilization regardless of time or day. During development, one of the key objectives was the reduction of hardware requirements and costs for operations.

In general, the bwSync&Share service includes two identical but independent systems: the live system for providing the service to our users and a test environment, which allows us to test new features and service configurations. Both systems follow the same architecture, which is shown in Figure 1 and consists of three logical layers: Web Layer, Application Layer and Data Layer. The scalability of the system is maintained by adding or removing of equivalent nodes to each layer of the architecture. Due to well defined internal processes and the usage of a virtual environment based on VMWare ESX cluster technology, the architecture allows the scale out of the service without any service interruptions.

The web layer consists of a hardware load balancer (F5 BIG LTM8400 from F5 Networks Inc.) and several virtual machines providing web server (apache2) and shibboleth service provider functionality (mod_shib). The infrastructure within the web layer serves as a high available proxy component which forwards the incoming user requests to the application layer. The load balancer enables a sticky ip-forwarding to the apache nodes whereas the apache nodes make use of proxy functionality (mod_proxy_ajp) to forward information to the application nodes. In addition, the apache nodes serve as Service Provider (SP) and collect user information from the Identity Provider (IdP) during the user authentication process.

The application layer consists of virtual machines which run the PowerFolder software. The software supports native cluster mode and it is horizontal scalable. If shibboleth authentication is not needed, or after initiating a connection via the web layer, the application layer is able to communicate directly to the clients.

The data layer consists of a storage system called SONAS and a database system based on MySQL. Both systems are independent KIT services and maintained by a different group. The storage system is based on GPFS file systems which are provided via NFS to the bwSync&Share service. The database is a MySQL Galera cluster solution running three active nodes on a VMWare ESX cluster.

For security reasons, we apply a very restrictive firewall policy. The web layer is separated from the internet and reachable via TCP port 80 and 443 only. Another port is user for the direct communication between clients and the node in the application layer. The data layer is fully isolated and not directly reachable from the outside.

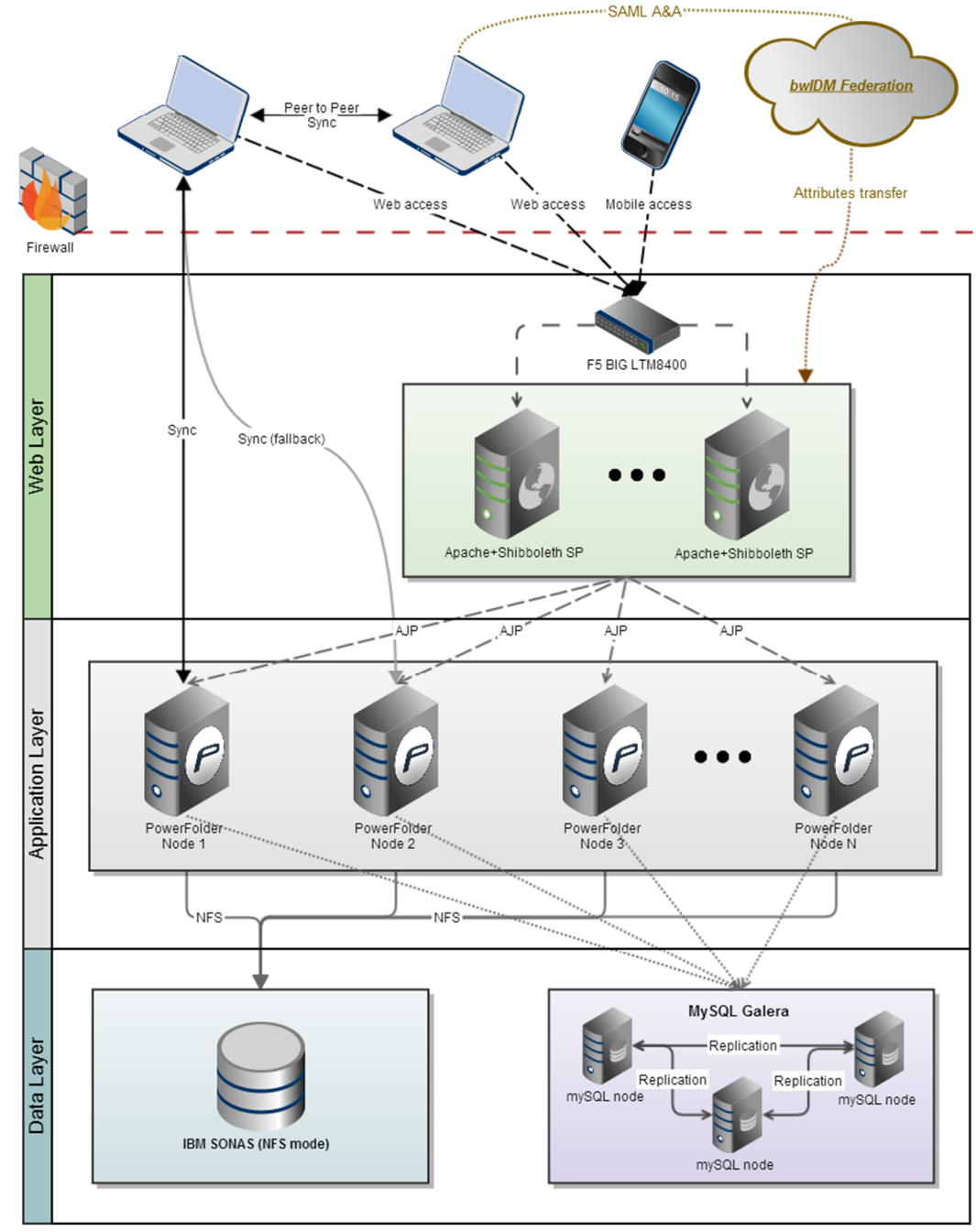


Figure 1: Schematic of the bwSync&Share service

Service Maintenance

Improving service quality and reducing service downtimes are an important and ongoing task, which can be achieved by simplifying the operation of bwSync&Share. Therefore, we

developed software, which is able to manipulate the running virtual machines by native API calls to the VMWare ESX cluster and to adapt the configuration of service components in real time. Thus, we are able to redeploy single components or – in case of an emergency – even the whole system by applying simple commands on a so-called management node. This node carries no core functionality of the service and is non-critical for providing the service. However, it helps us to maintain the system in an efficient manner.

The virtual machines within the web and application layer make use of pre-prepared hard disk images, which are stored in a central repository. These images are distributed to the virtual machines during redeployment of single components. Since these images are under version control, this approach gives us the opportunity to test new software versions or system configurations while maintaining the possibility to roll back easily to a stable version in case of an unexpected system behavior.

Since each change of the live system is tested in advance using our test environment, a rollback of the live system to a former version is rarely necessary. However, not all side effects of this change can be completely investigated within the test environment. Therefore, improving our test procedures is an ongoing task, which will increase the stability of our service furthermore.

Conclusion and Outlook

In this paper, we presented the bwSync&Share service which is free of charge and available to all students and scientists in the state of Baden-Württemberg since January 2014. We sketched our requirements and the software evaluation process. In addition, we presented the challenges which are closely related to the federated nature of the service.

After supplying the nine state universities with bwSync&Share, we are now focusing on providing the service to the remaining academic institutes in Baden-Württemberg. Since we build our service on top of the already existing shibboleth infrastructure for authorization and authentication, the rollout of the service is expected to be simple. Institutes without shibboleth infrastructure can easily outsource this part to the DFN which provides an IdP hosting service.

As a long term perspective, we intend to offer our service to institutes outside of Baden-Württemberg using the DFN as a broker. However, the final conditions of this service (e.g. service level agreements or prices) are still under discussion.

DAS: Data Access Service at AIP

Dr. A.Khalatyan,
eScience-Supercomputing
Leibniz-Institut für Astrophysik Potsdam (AIP)
An der Sternwarte 16,
14482 Potsdam, Germany
akhalatyan@aip.de

Abstract: File sharing between collaborators is one of the main aims of the DAS. The main goal is to keep data at AIP. Besides that, DAS provides many comfortable services to improve productivity of scientific collaboration, such as LaTexEditor/Compiler and MetaData per file apps. Both apps are developed at AIP and publically available at OwnCloud APPs store.

Motivation

From day to day increasing the number of important digital information at home and in business needs to be accessed rapidly from different places and different devices. Particularly the mobile devices and networks are become powerful enough to transfer large amounts of data. In 2011 Cisco Company was reporting that global traffic on mobile devices exceeded 1.5 exabytes per month [CVN14].

The data needs to be protected, easy accessible, in some cases shared between collaborators. The Cloud storage services promise a solution for this problem. Individuals and especially scientific communities hesitate to entrust their data to cloud storage services since the providers have policies intruding seriously on data privacy. The most popular cloud services DropBox, Wuala, SkyDrive, GoogleDrive, iCloud and UbuntuOne are providing limited storage space for free. For more disk space one needs to subscribe to commercial accounts with different payment plans.

Using public cloud services means that private data is provided to a ***"third party"*** with almost full access permissions. Also it is unclear in which geographic area the data will reside.

The public services are providing basic file sharing functionality. In some cases it is not fitting into a scientific workflow. The client and server side software is a closed source and it is open for modifications.

Therefore, at AIP we are providing a solution for file sharing and collaboration based on an Open Source software stack.

The DAS

Facilitating file sharing between collaborators is one of the main aims of the DAS. The data is hosted at AIP. Besides that, DAS provides many comfortable services to improve productivity in scientific collaboration. The user friendly web interface is accessible via SSL secured connection https://cloud.aip.de.

For the software stack we are using the Open Source software (OwnCloud.org) which gives us the freedom to choose, modify and add new features based on users' feedbacks.

Features

DAS provides a Web based interface to quick access the data. The default quota for the standard users is about 10 GB which can be increased on demand. For the most advanced users we are providing almost no quota. The web interface provides several web-embedded viewers: an image, PDF and ODF. For ASCII formatted files web interface provides a text editor with syntax the highlighting.

The maximum size upload data is depending on the method how users are handling uploads. Maximum upload over the web interface is up to 2 GB. Users can share single files or whole folder recursively. The shared URL can be private, public and shared with share time limits. The WebDAVFS interface to service allows users to mount DAS storage as regular network attached storage (NAS). The WebDav protocol is also supported by many data synchronization applications. There is not limitation on maximum file size if upload done over the WebDAV interface.

Life synchronization is also possible. The open source public Sync clients are available from OwnCloud .org.

Hardware and Software solution

DAS is based on software from www.owncloud.org project. We customized it for our needs.

OwnCloud provides an API for plug-in development so called APP's.

At AIP we have developed several apps which are freely available on apps.owncloud.org: **files_metadata:** Short description per file is stored to simplify collaboration between users

files_latexeditor: Embedded Web LaTeX Editor and compiler based on original OC-files text editor. It allows compiling, editing and viewing pdf form latex source files.

Service extension: user management integration with existing AIP IT infrastructure. It allows add, edit, send mass emails to users, manage quotas and account expiretime using cli,XMLRPC or SOAP protocols.(available on demand)

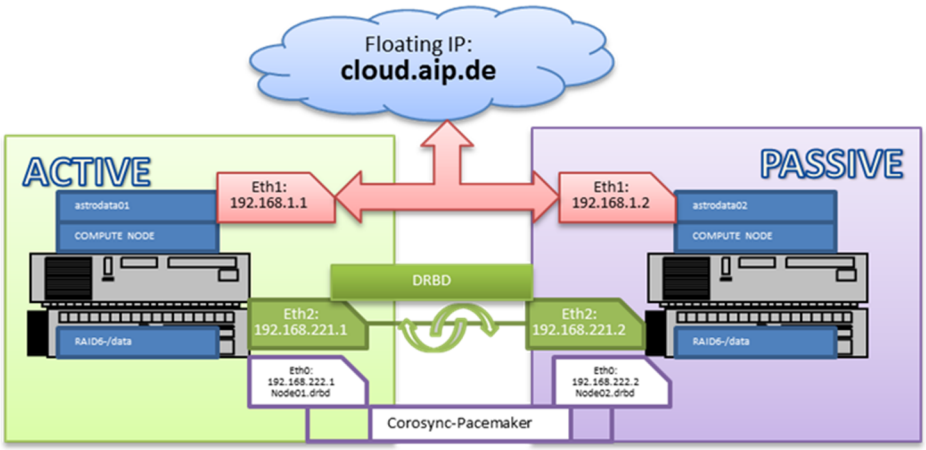


Figure 1: The DAS Active/Passive server hardware configuration

For hosting services we are using setup of an Active/Passive CentOS 6.5 Linux configuration.

The two hardware independent nodes are connected with 3 network interfaces as shown in the Fig 1. If one of the necessary components is failing, all services are migrating to second server. The migration time from one host to another is in the order of few seconds. Thus the hardware and system maintenance can be done without interrupting the DAS service.

The full software stack is based on OpenSource projects: Highly Availability is based on Corosync and Pacemaker, the disk clustering done with DRBD. Apache HTTP web server, PHP and MySQL server are used for the web applications.

Bibliography

[CVN14] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013–2018.

[OC] http://owncloud.org/

Evaluation und Implementierung eines Sync&Share-Dienstes als föderierten Dienst für den universitären Einsatz unter besonderer Berücksichtigung des Datenschutzes

Stefan Schwarz, Christian Voljanskij
Rechenzentrum
Universität der Bundeswehr München
85577 Neubiberg
Stefan.Schwarz@unibw.de
Christian.Voljanskij@unibw.de

Abstract: Bei der Evaluation und Einführung neuer Verfahren wird es auch für Universitäten aufgrund der inzwischen engen Verzahnung zwischen wissenschaftlichen und organisatorischen Bereichen erforderlich, die besonderen Rahmenbedingungen aus den Bereichen IT-Sicherheit und Datenschutz zu berücksichtigen. Dies gilt insbesondere für Verfahren zur Speicherung, automatisierten Verteilung und Austausch von Daten. Durch die zunehmende Beliebtheit in der Nutzung offener Cloud-Dienste aus dem Bereich Sync&Share wird es für die IT-Dienstleister zwingend notwendig, auch geeignete Alternativen für den universitären Bereich anzubieten. Da die Anforderungen der Universitäten im Bereich Sync&Share weitestgehend vergleichbar sind sollte dabei auch das Ziel verfolgt werden, für diesen Dienst entweder bereits bestehende Angebote anderer Universitäten zu nutzen oder bei einer eigenen Implementierungen diesen Dienst auch anderen Universitäten zur Nutzung anzubieten.

Ausgehend von der Analyse des bisherigen Nutzerverhaltens an der Universität der Bundeswehr München (UniBw M) erfolgt die Definition der grundlegenden Anforderungen an einen Sync&Share-Dienst. Nach einer Evaluation bestehender Lösungen durch die Auswertung verfügbarer Studien oder Testimplementierungen am Markt verfügbarer Lösungen wird aufgezeigt, dass derzeit nur sehr wenige der am Markt verfügbaren Lösungen die geforderten Kriterien zumindest annähernd erfüllen.

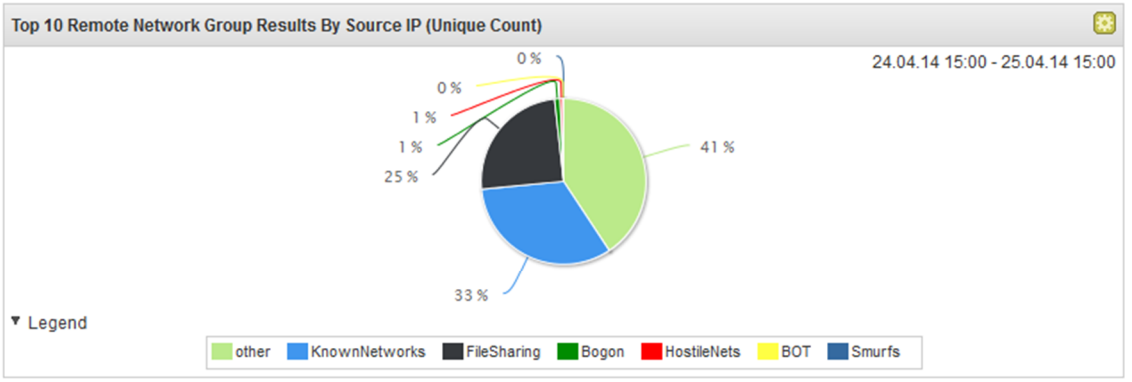
Auf Basis der Lösung TeamDrive des gleichnamigen deutschen Softwareherstellers erfolgt eine umfassende Evaluierung der universitären Einsatzszenarien. Dabei geht es weniger um grundsätzliche aus Nutzersicht erforderliche bzw. wünschenswerte Funktionen sondern vor allem um die Sicherstellung datenschutzkonformer Abläufe sowie deren Bewertung. Es wird aufgezeigt, dass rein organisatorische Regelungen nicht zuverlässig greifen so dass technisch gestützte Lösungen vorzuziehen sind. Dies erfordert aber in vielen Fällen die Bereitschaft des Anbieters, solche Verfahren auch tatsächlich zu implementieren, evtl. auch unter Einschränkung von Komfortfunktionen für den Nutzer.

Abschließend werden anhand der konkreten Implementierung als föderierter Dienst die besonderen datenschutzrelevanten Details zur Integration der DFN-AAI aufgezeigt. Zusätzlich werden notwendige Erweiterungen aus Sicht des Providers dargestellt, um föderierte Aspekte wie Selbstbedienungsfunktionen und Abrechnungssysteme sowohl für den Nutzer als auch den Provider optimal aufeinander abzustimmen.

Cloud-Storage zu Sync&Share an Hochschulen

Bislang liegen zur Nutzung von Sync&Share-Diensten durch Mitarbeiter oder Studenten von Hochschulen keine verwertbaren Erkenntnisse vor. Während klassische Storage-Dienste jetzt auch unter dem Begriff Cloud-Storage firmieren ist es im Umfeld der Sync&Share-Dienste aktuell noch sehr ruhig. Es ist daher davon auszugehen, dass eine Vielzahl der Mitarbeiter sich der freien Sync&Share-Dienste der großen Anbieter bedienen. Dies beruht vor allem auf der Einfachheit in der Bedienung sowie der komfortablen Integration der mobilen Endgeräte, welche inzwischen auch aus dem Umfeld der Hochschulen nicht mehr wegzudenken sind.

Statistische Erfassung der Sync&Share-Nutzung an der Universität der Bundeswehr München (UniBw M)



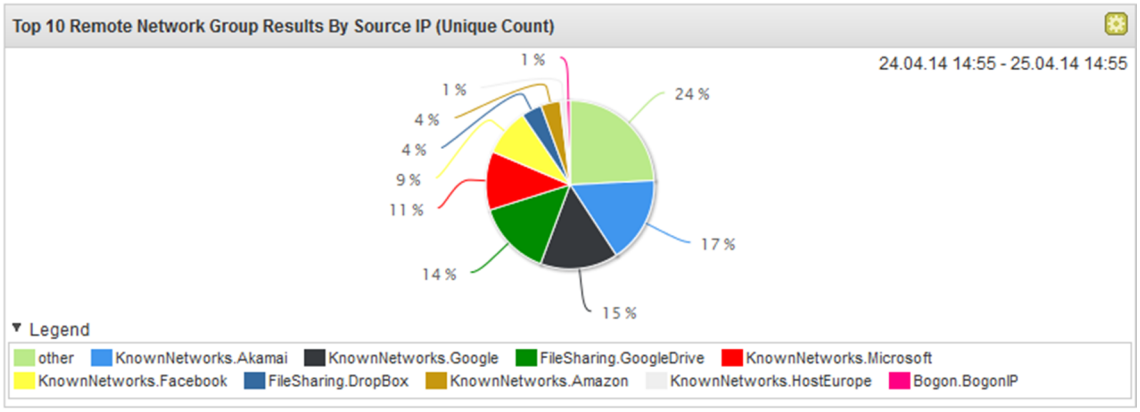
Remote Network Group	Source IP (Unique Count)
other	Multiple (3,848)
KnownNetworks	Multiple (3,108)
FileSharing	Multiple (2,342)

Abbildung 1: Klassifizierung der Providernutzung

Um zumindest einen quantitativen Überblick über die Nutzung von Dateidiensten im Netz zu erhalten erfolgte über einen kurzen Zeitraum eine anonymisierte Auswertung der Verbindungsdaten zu externen Providern mit einer groben Klassifizierung. Abbildung 1 zeigt die Anzahl der beobachteten IP-Adressen im Zeitraum. Dabei zeigt sich, dass ca. 2.300 von insgesamt ca. 3.800 Rechnern Provider zu File-Diensten kontaktierten.

Die Frage nach der konkreten Nutzung von Sync&Share-Diensten kann nur näherungsweise beantwortet werden, da die korrekte Klassifizierung aller Anbieter auf diesem Segment nur sehr schwer gelingt und auch einige Anbieter (Google etc.) keine Unterscheidung im Hinblick auf die verwendeten Provider-IPs zulassen. Dennoch zeigt bereits der grobe Versuch einer Klassifizierung nach Abbildung 2, dass ein typischer Vertreter wie DropBox bereits von etwa 16 % (620 von 3 800) aller beobachteten IPs im Datennetz genutzt wird.

Allerdings lässt sich die Frage nach der Verteilung der Nutzung eines Dienstes wie DropBox innerhalb der Wissenschaft recht gut beantworten, indem das Nutzungsverhalten zwischen Mitarbeitern und Studenten (hier ist natürlich die Einrichtung einer Campus-Universität besonders hilfreich) ausgewertet wird. Dabei zeigt sich recht deutlich, dass die Nutzung von Sync&Share-Diensten keinesfalls eine Domäne der Studentenschaft ist, sondern dass dies auch in Mitarbeiterkreisen inzwischen zum Alltag gehört.

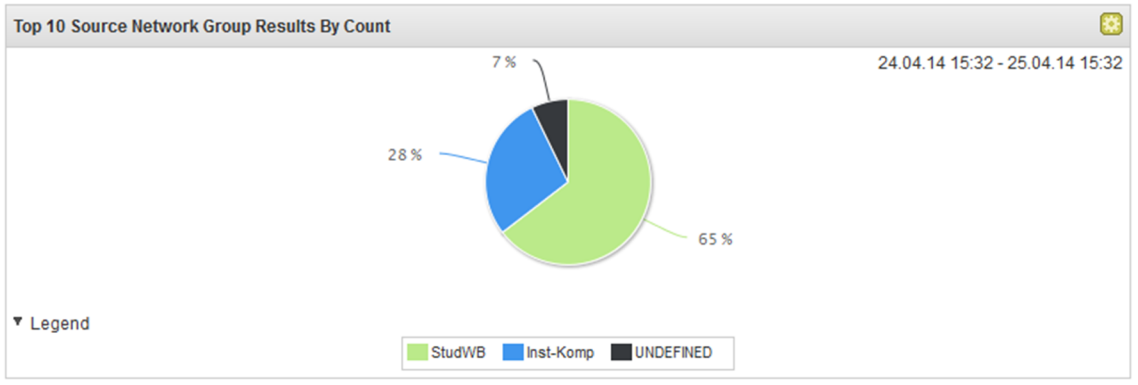


(Hide

Remote Network Group	Source IP (Unique Count)
other	Multiple (3,843)
KnownNetworks.Akamai	Multiple (2,630)
KnownNetworks.Google	Multiple (2,374)
FileSharing.GoogleDrive	Multiple (2,294)
KnownNetworks.Microsoft	Multiple (1,790)
KnownNetworks.Facebook	Multiple (1,438)
FileSharing.DropBox	Multiple (622)

Abbildung 2: Verteilung der Nutzung auf Anbieter von Sync&Share-Diensten

Damit wird deutlich, dass die Nutzung von Sync&Share-Diensten an Hochschulen bereits eine große Bedeutung besitzt und der Bedarf auch gleichmäßig über alle Nutzerkreise besteht. Eine Ausweitung auf alle Nutzerkreise einer Hochschule macht dabei durchaus auch Sinn. Die enge Zusammenarbeit innerhalb einer Hochschule macht unerlässlich, eine Sync&Share-Lösung allen Mitgliedern der Universität anzubieten. Neben der allgemeinen bereichs- oder arbeitsgruppeninternen Kommunikation legen umfangreiche Gremienarbeiten, wissenschaftliche Projekte unter Einbeziehung von studentischen Hilfskräften sowie die erforderliche Kommunikation mit Verwaltungseinrichtungen die flächendeckende Nutzung eines Sync&Share-Dienstes nahe.



(Hide

Source Network Group	Source IP (Unique Count)
StudWB	Multiple (316)
Inst-Komp	Multiple (239)
UNDEFINED	Multiple (54)

Abbildung 3: DropBox-Nutzung im Vergleich zwischen Studenten und Mitarbeitern

Anforderungsprofil für Sync&Share

Zu einer allgemeinen Begriffsbestimmung sowie grundsätzlichen Anwendungsszenarien kann auf [BSI12] verwiesen werden.

Die Definition eines allgemein gültigen Anforderungsprofils für eine hochschulweite Nutzung ist aber dadurch erschwert, dass die aktuellen und künftigen Anforderungen der Nutzer im Gegensatz zu einem weitgehend homogenen Firmenumfeld nicht ausreichend klar spezifiziert werden können. Es wurde bereits gezeigt, dass eine Sync&Share-Lösung möglichst hochschulweit alle Nutzerkreise erfassen sollte. Damit werden natürlich auch die Anwendungsszenarien sehr umfangreich und damit auch die Anforderungen an eine einheitliche Lösung erschwert. Dies gilt insbesondere für eine Campusuniversität wie die Universität der Bundeswehr München, wo für den Großteil der Studierenden gleichzeitig ein militärischer Auftrag zum Studium vorliegt und gleichzeitig militärische Aufgaben zu erfüllen sind in Verbindung mit der Bearbeitung entsprechender Dokumente.

Allerdings haben inzwischen nahezu alle Hochschulen Erfahrungen mit der Bereitstellung von zentralem Datenspeicher in der Form von NAS- oder SAN-Devices zur Nutzung durch ihre Mitglieder. Parallel dazu gibt es vereinzelt auch Dienstanweisungen zum Umgang mit sensiblen, insbesondere personenbezogenen Daten. Davon sind zunehmend auch Daten und Dokumente zu Forschungsarbeiten betroffen, wo beispielsweise mit dem Auftraggeber auch besondere Bestimmungen zum Schutz der Forschungsergebnisse getroffen wurden. Hier ist insbesondere die Notwendigkeit einer sicheren Verschlüsselung von Daten zu nennen. Alle in diesem Umfeld erforderlichen Schutzmechanismen zu den Daten sollten auch in einem Sync&Share-Umfeld vorhanden sein, um eine möglichst umfassende Nutzung zu ermöglichen und damit eine gemeinsame Bearbeitung sowie die Aktualität der Daten auf allen Endgeräten zu gewährleisten.

Der korrekte Umgang mit den Daten, die sichere Übermittlung von Daten sowie die Einhaltung zugesicherter Eigenschaften wie sichere Verschlüsselung und Schlüsselmanagement erfordern ein hohes Maß an Vertrauen in den Betreiber einer Sync&Share-Lösung. Dieses Vertrauen kann dadurch maßgeblich gefördert werden, dass auch der Betreiber aus dem Hochschulumfeld kommt. Daher ist die Möglichkeit, eine Lösung auch im eigenen Rechenzentrum betreiben zu können, ein sehr wichtiges Kriterium. Dieses bietet gleichzeitig die Chance, die eingesetzte Lösung einer intensiven und auch regelmäßigen Kontrolle unabhängig vom Hersteller der Software durchführen zu können.

Aus diesen Gründen können die folgenden spezifischen Anforderungen an eine umfassend nutzbare Sync&Share-Lösung im Hochschulumfeld definiert werden:

- Sichere Verschlüsselung aller Daten im Cloud-Speicher
  Der Anbieter bzw. Administrator des Cloud-Dienstes haben keinen Zugriff auf die Inhalte der Daten. Für den Kunden ergibt sich damit ein maximales Schutzniveau. Dies erfordert ein sicheres Schlüsselmanagement (z. B. verbleiben Schlüssel ausschließlich beim Nutzer)

- Integration in die lokalen Vorschriften zur Datenhaltung
  Damit sind auch lokal vorhandene Verschlüsselungs- und Sicherungskonzepts weiter nutzbar.

- Betrieb der Lösung in eigener Infrastruktur
  Dies ermöglicht letztlich eine bessere Analyse, Überwachung und Bewertung der Dienste.

Marktanalyse

Zur Analyse der aktuell am Markt befindlichen Lösungen wurden die Zusammenstellungen bzw. Auswertungen aus [SIT12] und [DFN12] herangezogen. Die Auswahl aus den darin bewerteten Lösungen fiel sehr leicht, da es zum aktuellen Zeitpunkt (Juni 2012) nur eine Software gab welche den gestellten Anforderungen entsprechen konnte, die Software „TeamDrive“ des gleichnamigen deutschen Anbieters [TD01]. Daher beschränkte sich die weitere Evaluation allein auf dieses Produkt.

Evaluation von TeamDrive

Die Evaluation der grundlegenden Anforderungen für einen Sync&Share-Dienst auch im Vergleich zu konkurrierenden Produkten wie DropBox kann ohne großen Aufwand durch die Nutzung des freien Clients aus [TD01] durchgeführt werden. Wie erwartet können die Anforderungen an eine sichere und zuverlässige Synchronisation und Datenaustausch auch über verschiedene Plattformen gut erfüllt werden. Daher beschränkte sich die weitere Evaluation auf die datenschutzrelevanten Kriterien wie Verschlüsselung und Schlüsselmanagement.

Zu diesen Punkten existiert eine Zertifizierung des „Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein“ (ULD), welches unter [TD02] auch online verfügbar ist. Dieses Gutachten geht aber nur sehr oberflächlich auf die innerhalb der Software ablaufenden Prozesse zur sicheren Verschlüsselung und insbesondere der Schlüsselverwaltung ein, auch die für einen föderierten Dienst erforderliche verteilte Authentifizierung blieb unberücksichtigt. Daher wurde eine detaillierte Untersuchung dieser Prozesse erforderlich.

Durch eigene Auswertungen sowie durch Kontakte mit den Entwicklern erfolgte die Erstellung der wesentlichen Prozessschritte nach Abbildung 4. Die für diesen Beitrag relevanten Prozessschritte werden im Folgenden zusammengefasst.

Registrierung eines neuen Nutzers

2. Der zentrale Registrierungsserver meldet dem Client die tatsächliche Adresse des zuständigen Registrierungsservers der Universität.
7. Der Client authentifiziert sich gegenüber dem Identityprovider
10. Der Client erzeugt ein clientspezifisches asymmetrische Schlüsselpaar (private und public Key). Zusätzlich generiert der Client aus dem durch den Serviceprovider (SP) gelieferten „user_secret“ ein nutzerspezifisches Schlüsselpaar. Dies bedeutet, dass alle Clients innerhalb TeamDrive ein individuelles Schlüsselpaar besitzen, dessen Generierung von außerhalb nicht manipuliert werden kann. Zusätzlich wird ein nutzerspezifisches Schlüsselpaar generiert, welches für den Nutzer, gleich auf welchem Client er arbeitet, identisch ist.
11. Der Client sendet den clientspezifisch generierten public-Key zur Speicherung zum Registrierungsserver. Dieser Key kann damit ab diesem Zeitpunkt für die Verschlüsselung von clientspezifischen Informationen genutzt werden, da die Entschlüsselung dieser Informationen ausschließlich über den private Key möglich ist.

Anlegen eines neuen Space und Einladung eines weiteren Nutzers zur Teilnahme

12. Der Client erzeugt lokal einen Ordner (Space) und den zu diesem Space passenden symmetrischen Schlüssel (Space-Key). Ist der Client so konfiguriert, dass eine zentrale Schlüsselspeicherung auf dem Registrierungsserver gewünscht ist, wird dieser Schlüssel mit dem nutzerspezifischen public-Key (siehe Abbildung 4, Punkt 10) verschlüsselt auf dem Registrierungsserver abgelegt. Damit kann der Nutzer nach der Installation weiterer Clients seine Spaces sofort wieder laden ohne sich dazu selbst noch einmal einzuladen.
13. Im Fall einer Einladung zu einem Space werden alle clientspezifischen public-Key des Einzuladenden vom Registrierungsserver angefordert (d.h. alle Keys der Clients, welcher der einzuladende Nutzer eingerichtet hat). Der lokale Space-Key wird mit diesen public-Keys verschlüsselt. Der jeweilige verschlüsselte Space-Key wird der Einladung des betreffenden Clients hinzugefügt. Diese Einladung wird über den Registrierungsserver zugestellt sobald der Client des Eingeladenen online ist. Hat der Einzuladende noch keine TeamDrive-Installation so ist dieser dem Registrierungsserver nicht bekannt und hat damit auch keinen public-Key hinterlegt. In diesem Fall würde der Space-Key mit dem public-Key des Registrierungsservers verschlüsselt und auf dem Registrierungsserver zwischengespeichert.
14. Da alle eingeladenen Nutzer nun über den gleichen Space-Key verfügen (dieser kann mit dem private-Key des Clients der Einladung entnommen werden), werden alle Daten vor der Übertragung in den Space auf dem Hostserver verschlüsselt. Alle Space-Schlüssel verbleiben auf den Clients.

Aufbewahrung der privaten Schlüssel

Alle privaten Schlüssel verbleiben in unverschlüsseltem Zustand ausschließlich auf den Clients. Um weitere Clients eines Nutzers in einen Space einzuladen werden die clientspezifischen öffentlichen Schlüssel auf dem Registrierungsserver gespeichert. Wird ein Client komplett neu installiert so wird auch ein neues Schlüsselpaar erzeugt. Dies führt unter Umständen dazu, dass einem Nutzer eine größere Anzahl von Clients zugeordnet wird, was aber im aktuellen Betrieb nicht weiter stört.

Sicherung der Space-Schlüssel

Die Daten eines Space werden symmetrisch verschlüsselt, der Verlust des Schlüssels bedeutet einen Verlust der Daten. Auf den Desktop-Clients (Windows, Linux, Mac) wird im Space-Ordner noch ein weiterer Backup-Ordner angelegt. Dort werden alle Schlüssel regelmäßig gesichert und können wieder eingespielt werden. Allerdings sind die Space-Schlüssel auch auf jedem Client des Nutzers (mit eingeladenem Space) identisch vorhanden, so dass selbst bei einem Verlust der Space-Schlüssel auf einem Client dieser nach der Installation von einem weiteren Client des Nutzers wieder eingeladen werden kann.

Schlüsselhinterlegung auf Registrierungsserver

Zusätzlich kann eine Sicherung aller Space-Schlüssel auf dem Registrierungsserver angelegt werden. Diese Option hat der Nutzer in den Desktopclients zur Verfügung und kann diese selbst ein- oder ausschalten. Ist diese Sicherung aktiviert, werden alle Space-Schlüssel mit dem nutzerspezifischen Schlüssel (siehe Abbildung 4, Punkt 10) verschlüsselt auf dem Registrierungsserver abgelegt. Dies ist vor allem eine Komfortfunktion, da damit nach Anlegen

eines neuen Clients (z.B. TeamDrive auf Smartphone) sofort alle existierenden Spaces ohne neue Einladung geladen werden können. Sie ist für ein ordnungsgemäßes Arbeiten mit TeamDrive nicht erforderlich.

Szenarien für Datenverlust oder Schlüsselkompromittierung

Datenverlust durch Schlüsselverlust

Dies wäre dadurch möglich, dass alle Clientinstallationen eines Nutzers vollständig gelöscht werden, keine Datensicherung der Space-Schlüssel existiert und auch keine Schlüsselhinterlegung erfolgte. In diesem Fall liegen die verschlüsselten Daten zwar noch auf dem TeamDrive-Server, können aber nicht mehr entschlüsselt werden. Es gibt keine Nach- oder Zweitschlüssel.

Schlüsselkompromittierung

Da alle clientspezifischen privaten Schlüssel auf den Clients verbleiben kann die Kompromittierung nur durch Zugang zum Space-Schlüssel erfolgen. Dies ist außerhalb des direkten Zugangs zu den Daten über einen installierten Client nur möglich, wenn eine Schlüsselhinterlegung eingerichtet wurde und der nutzerspezifsche Schlüssel bekannt ist. Dies könnte beispielsweise durch eine Kompromittierung des Anmeldevorgangs erfolgen, so dass eine weitere Person ein identisches user_secret erhält. Mit dem daraufhin generierten identischen nutzerspezifischen Schlüssel könnte der hinterlegte Space-Key eines weiteren Benutzers entschlüsselt werden. Dies könnte beispielsweise durch Kompromittierung sowohl des Registrierungsservers als auch des Authentifizierungsservers gelingen. Auf maximale Sicherheit bedachten Nutzern wird daher empfohlen, die Schlüsselhinterlegung auf dem Registrierungsserver zu deaktivieren.

Einladung nicht registrierter Benutzer

In 0 Punkt 13 wurde gezeigt, dass im Falle der Einladung eines nicht registrierten Nutzers der Space-Schlüssel auf dem Server in einer Form hinterlegt wird, dass eine Entschlüsselung auf dem Server durchgeführt werden kann. Dieses Verhalten wurde mit dem Hersteller diskutiert und eine Lösung geschaffen, dass der Server so konfiguriert werden kann dass nur noch vorab registrierte Nutzer eingeladen werden können. Damit ist die Vertraulichkeit der Schlüssel gewährleistet.

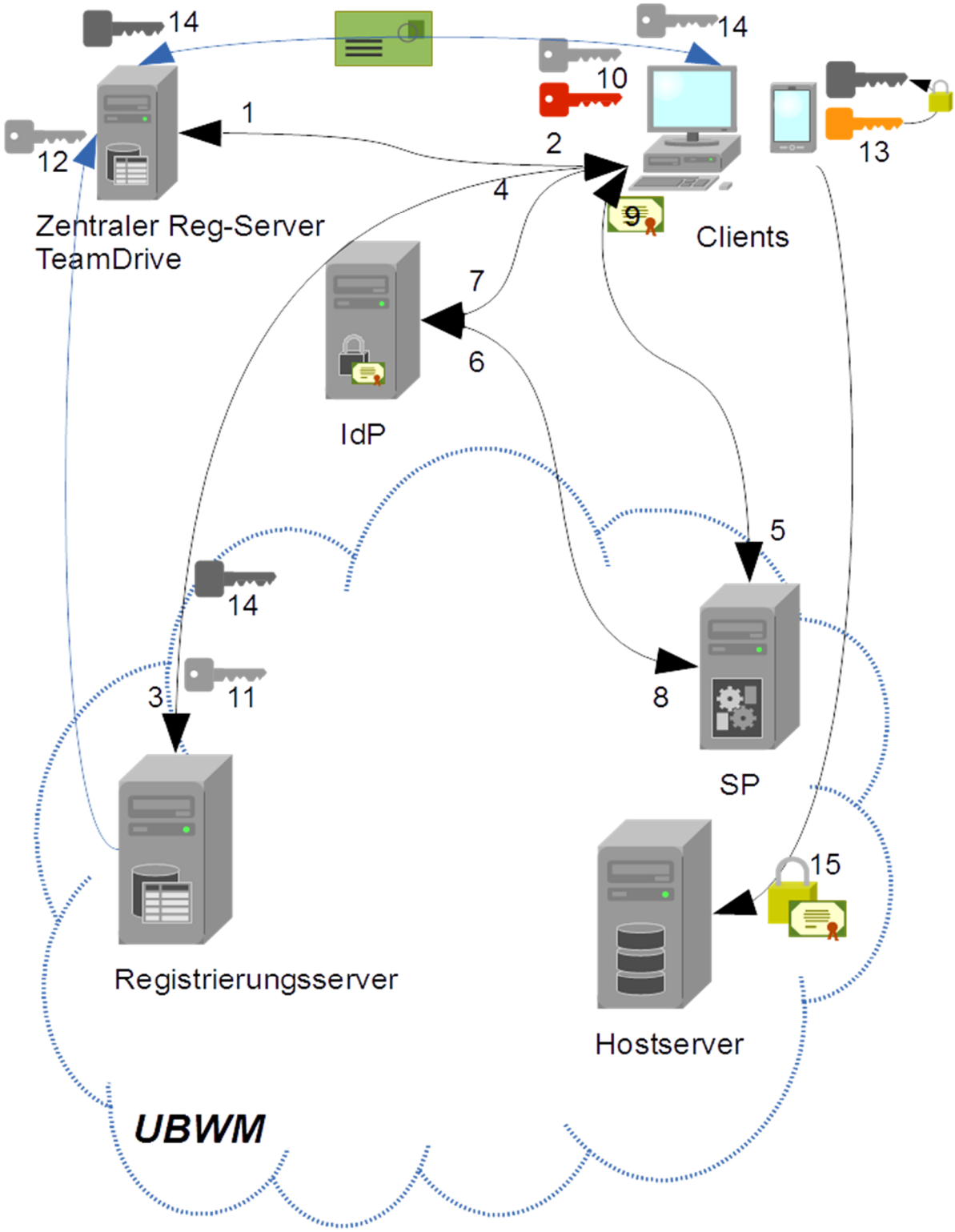


Abbildung 4: Analyse der datenschutzrelevanten Prozesse innerhalb TeamDrive

Administration des Dienstes

Um solch einen föderierten Dienst anbieten zu können, bedarf es Anpassungen und Erweiterungen aus Sicht des Providers (UniBw M), um weitere Teilnehmer (Einrichtungen) möglichst einfach zu integrieren und um einen Überblick über die einzelnen Teilnehmer (z.B. Universität/Einrichtung) zu erhalten. Dafür ist es erforderlich, dass die eingesetzte Software Funktionen über eine API zur Verfügung stellt. Damit wurde eine eigene Administrationsoberfläche entwickelt, die unter anderem die API-Schnittstelle der TeamDrive-Server benutzt.

Integration Shibboleth

TeamDrive bietet die Möglichkeit, eine externe Authentifizierung durchzuführen (siehe auch Abbildung 4). Dies wird über Shibboleth basierend auf der DFN-AAI-Föderation erreicht. Shibboleth ermöglicht es, den eigentlichen Authentifizierungs- und Autorisierungsprozess über die jeweilige Teilnehmereinrichtung durchführen zu lassen. Durch die Integration der DFN-AAI ist die Aufnahme weiterer Teilnehmer ohne Aufwand möglich.

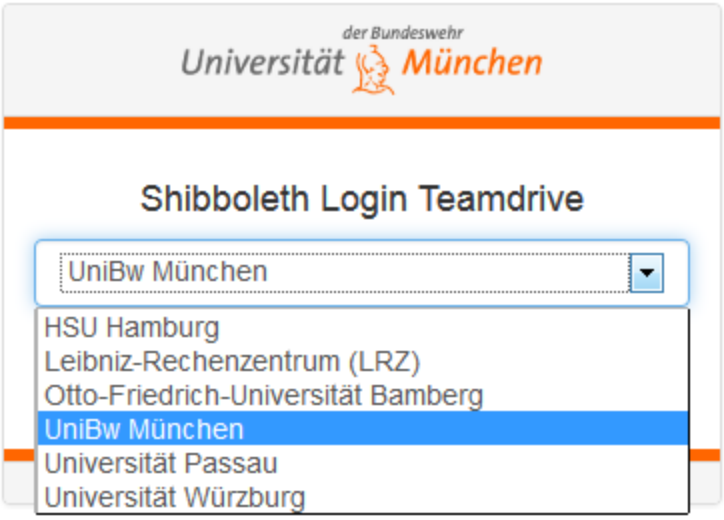


Abbildung 5: Auswahl des Teilnehmers zur Shibbolethauthentifizierung

Folglich bekommt der Service Provider nur die erforderlichen personenbezogenen Daten, die vom Identity Provider für den Dienst TeamDrive explizit freigegeben werden müssen.

Lizenzverwaltung

Die Lizenzierung erfolgt pro Teilnehmer. Bei jedem Teilnehmer wird dann noch nach Nutzergruppe (Affiliation) unterschieden. Somit kann je nach Nutzergruppe eingeteilt werden, welches Lizenz- und Storagemodell angewendet werden soll.

Um eine Lizenz zu beanspruchen, reicht der Login am System aus, sofern der Teilnehmer freigeschaltet ist. Nachdem alle nötigen Attribute an den Server übermittelt wurden, wird eine Lizenz für den eingeloggten Account zugeteilt. Die Lizenz ist dadurch an den Account gebunden.

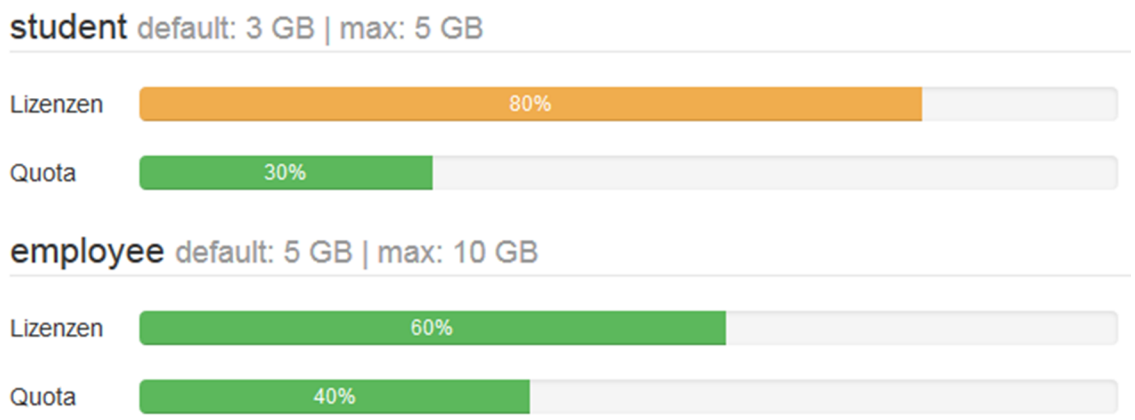


Abbildung 6: Lizenz und Storageübersicht zu zwei Nutzergruppen

Speicherverwaltung

Der Teilnehmer hat die Möglichkeit, der jeweiligen Nutzergruppe unterschiedliche Speicherplatzgrößen zuzuteilen. Hierbei sind zwei Werte möglich, ein Default- und ein Maximalwert. Der Defaultwert wird jedem neuen Nutzer des Teilnehmers zugeteilt. Der Nutzer hat dann die Möglichkeit, seine Quota eigenständig bis zum Maximalwert zu erhöhen. Dadurch ist der Nutzer flexibler und kann den Speicherplatz erhöhen, wenn z.B. für eine bestimmte Zeitspanne mehr Speicherplatz benötigt wird. Sollte der Nutzer aktuell weniger Speicher nutzen als der Defaultwert es vorgibt, so kann auch hier der Speicherplatz auf die optimale Größe verkleinert werden.

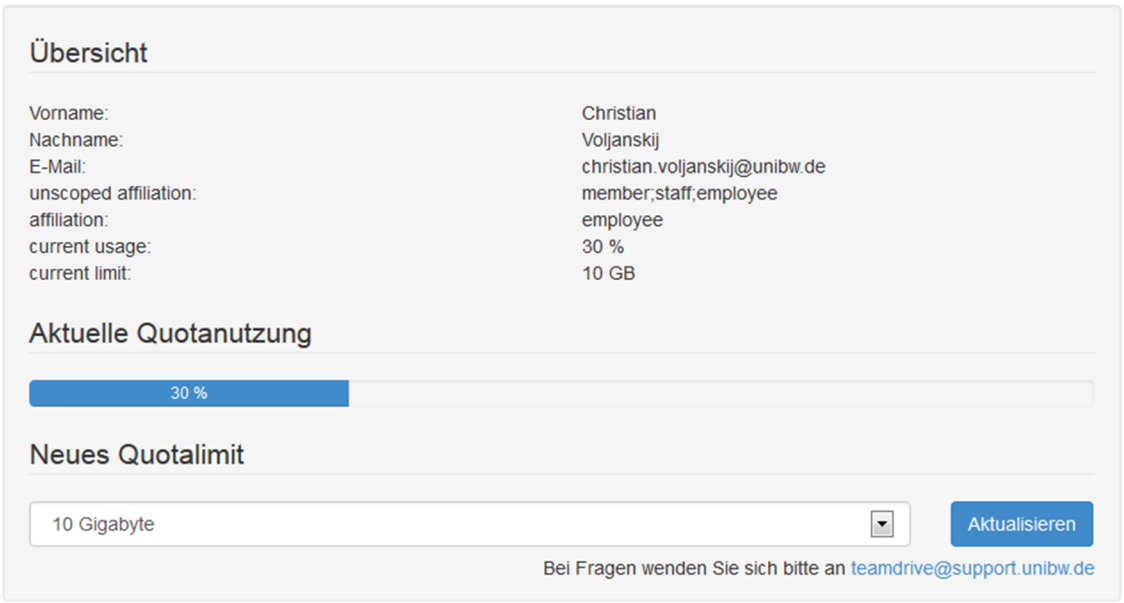


Abbildung 7: Benutzerinterface zur eigenen Quotaanpassung

In besonderen Fällen kann auch der Speicherplatz vom Administrator auf einen bestimmten Wert explizit gesetzt werden, der z.B. nur für einen Benutzer angewendet werden soll. Dies erfolgt aber nur auf Anfrage des Teilnehmers.

Vereinfachtes Abrechnungsverfahren

Bei der Abrechnung eines einzelnen Teilnehmers wird tagesaktuell das eingestellte Quota aller Nutzer verwendet. Damit ergibt sich ein guter Kompromiss für Provider und Teilnehmer, wo der Provider nicht lediglich nur den aktuell genutzten Speicher berechnet und der Teilnehmer bzw. die Nutzer nicht die maximale zulässige Speichergröße finanzieren müssen.

Literaturverzeichnis

[BSI12] Bundesamt für Sicherheit in der Informationstechnik: Überblickspapier Online-Speicher, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Online-Speicher_pdf.pdf?__blob=publicationFile

[DFN12] DFN-Verein: 1. Workshop "Online-Speicher" als föderierter DFN-Dienst, Berlin 07.11.2012

[SIT12] Fraunhofer SIT: On the Security of Cloud Storage Services, Fraunhofer Verlag 03/2012, https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Cloud-Storage-Security_a4.pdf

[TD01] TeamDrive: http://www.teamdrive.de

[TD02] TeamDrive: Gutachten des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, 2005-2013, http://www.teamdrive.com/de/datenschutzguetesiegel.html

The DESY Big Data Cloud Service

Dr. Patrick Fuhrmann, Christian Bernardt, Quirin Buchholz, Tigran Mkrtchyan,
Peter van der Reest, Marvin Schulz, Sven Sternberger

Information Technology
Deutsches Elektronen-Synchrotron, DESY
Notkestrasse 85
22607 Hamburg
Patrick.Fuhrmann@desy.de

Abstract: DESY has a long history in providing huge amounts of reliable high throughput storage space for a variety of scientific communities. However, over the past years, storage requirements for the DESY infrastructure significantly changed in various interesting ways. On the management level, DESY added quite a set of new sciences to its already challenging portfolio, as there are Belle I&II[1], the International Linear Collider[2] (ILC), the Cherenkov Telescope Array[3] (CTR), IceCube[4], the Free Electron Laser[5] (XFEL) as well as the different CFEL[6] groups. In parallel, the global storage world moved forward towards Clouds with its very attractive new semantics. Cloud storage is unlimited and only paid per used. Data in the Cloud can be easily shared with individuals, groups as well as with the general public. Cloud Storage is seamlessly accessible from remote by most common operating systems, browsers, mobile devices and synchronization clients. However, requirements from scientific storage users go much further. Scientific storage users need to access their data through a regular mounted file system, as this is what high-throughput applications expect. For wide area transfers from site to site, by GlobusOnline[7] or FTS[8], data has to be made available by protocols like GridFTP[9] or the Storage Resource Manager[10] (SRM). Moreover, scientists expect to be able to define access latency and retention policies for their data, e.g. how many copies of the data should be held, should the data go to tape for archiving purposes or to a SSD disk for fast analysis? This presentation intends to sketch the way DESY will merge those two worlds by integrating a well-known Cloud software stack (OwnCloud[11]) into an established data management system (dCache[12]), creating a high throughput Big Data Cloud system.

The Scientific Storage Cloud

After the "Cloud Storage" Hype Cycle moved from "Peak of inflated Expectations" to "Plateau of Productivity" [GR05], Universities and Scientific Laboratories found themselves confronted

[1] The Belle Collaboration: belle2.kek.jp
[2] The International Linear Collider: http://www.linearcollider.org/
[3] The Cherenkov Telescope Array: https://www.cta-observatory.org/
[4] The IceCube experiment: https://icecube.wisc.edu/
[5] The Free Electron Laser: http://www.xfel.eu
[6] Center for Free Electron Laser Science: http://www.cfel.de/
[7] Globus Online: https://www.globus.org/
[8] File Transfer Service, CERN Software Product
[9] The GridFTP v2 protocol specification: http://www.ogf.org/documents/GFD.47.pdf
[10] The Storage Resource Manager specification: https://sdm.lbl.gov/srm- wg/doc/SRM.v2.2.html
[11] The OwnCloud Cloud system: http://owncloud.org/
[12] The dCache Technology: http://owncloud.org/

with an increasing pressure to provide Cloud Storage to their employees and associated scientific communities.

As a consequence, beginning of 2014, the DESY IT group decided to provide "Cloud Storage" to its employees and customers. However we found that a more precise definition of "Cloud Storage" obviously depends on the requesting user group or community. We made a quick survey with mostly DESY scientific group leaders and found that one can roughly split the collected requirements into three main categories, which we called "Web 2.0 experience", "Big-Data Management" and requirements "Specific to Science". In the remaining paragraph we'll touch on the main results.

The Web 2.0 experience requirements

This class of requirements focuses on how storage is accessed and manipulated by its users. Within this category we found 3 main requirements.

Web Browser access

There is certainly no doubt that customers need to have access to their data via standard Web Browsers. Basically this is uploading and downloading data, listing directories, deleting data and moving data around within their own namespace. In addition users might appreciate server side data pre-processing, resulting in thumbnail views for pictures, movies and documents or data classification based on MIME type or smart guessing.

Sync Clients and mobile apps

As, even for scientists, mobile devices (e.g. Laptops) replaced the former office-based workstations, users are envisioning to have their disk based devices (Laptops) synchronized with their "Cloud Storage" whenever a network connection can be established. Synchronization should happen both ways, allowing more than one device to be connected to the same section (partition) of the private "Cloud Space". For smaller, hand-held devices, users are expecting Mobile-Apps to be provided, allowing data to be moved between those devices and the "Cloud".

Data Sharing

Similarly important for scientists is to share data with individual colleagues, user groups or the general public. Other than in the past, shared data should appear in the home space of the registered destination user. This differs from the POSIX file system semantics, where Access Control Lists (ACLs) are modified to give access to individual files, while the file itself stays in the private file space of the sharing user. For public sharing, non-traceable URI's should be generated, accessible by non-registered users.

The Big-Data Management requirements

Unlimited

Based on our experience with large storage space vendors, like Amazon©, Google©, the Deutsche Telekom© and others, the concept of storage quotas seem to disappear; at least from the technical perspective. Storage space is unlimited. Customers agree to pay per use, but don't want to hit limits any more.

Indestructible Storage Space (Retention Policies) and high availability

Concerning the durability, customers expect the stored data to be close to indestructible. Here is a quote from the "Amazon S3" storage offering:

"Amazon S3 is designed to provide 99.999999999% durability of objects over a given year. This durability level corresponds to an average annual expected loss of 0.000000001 % of objects. For example, if you store 10,000 objects with Amazon S3, you can on average expect to incur a loss of a single object once every 10,000,000 years."

Quote 1: From FAQ of the Amazon S3 storage offering

So even if there is still a probability to loose data, the likelihood is negligible. Although regular scientific storage space generally doesn't provide that level of durability, sites might consider offering this as an option, e.g. for the purpose of long-term preservation [DP06]. Different levels of durability are generally referred to as "Retention Policy", defined as the quality of the space where files are located. Different "Retention Policies" are naturally associated with different pricing models.

There are similar expectations on the availability of the storage services itself. Quoting Amazon again:

"The service was designed for 99.99% availability, and carries a service level agreement providing service credits if a customer's availability falls below 99.9 %."

Quote 2: From the FAQ of the S3 storage offering.

Access Latencies

Similar to different „Retention Policies" different "Access Latencies" are expected with different pricing models. Again, Amazon is offering fast storage access (regular S3) for significantly higher prices than its high latency „Glassier Storage". So if customers know that certain datasets are less often accessed they expect to get the option to store that data on cheaper media, accepting a higher „Access Latency" but not a reduced „Retention Policy". Different "Access Latencies" vary from fast random access on Solid State Disks, via fast streaming access for regular spinning disks to high latency storage on tape media.

Scientific Data Access Requirements

Some of the collected requirements are obviously arising from specific scientific work of customers at laboratories or universities. It seems that scientists plan to integrate the site local "Cloud Storage" into the data lifecycle of their medium-volume scientific data.

Access Protocols

There are two more scenarios, not covered by regular cloud storage mechanisms.

The first is fast analysis of data in the cloud directly from workernode-clusters or HPC systems. That requires mounting cloud space on those systems with an appropriate low-latency, high-throughput protocol. Using FUSE[13] or similar systems is certainly not performand enough. However parallel NFS (NFSv4.1/pNFS)[14] was especially designed for those purposes.

The second use-case is to transfer bulk data from one site to another, generally from the site where primary or raw data is generated to sites where the data is processed or analysed. There are some systems available for high throughput bulk transfer from which two (FTS and GlobusOnline) require the endpoint to provide the GridFTP[15] protocol.

[13] FUSE, File System in user space: http://fuse.sourceforge.net/
[14] NFSv4.1 RFC: https://tools.ietf.org/html/rfc5661
[15] GridFTPv2 Protocol Specification: http://www.ogf.org/documents/GFD.47.pdf

Authentication Mechanisms

Especially for access protocols discussed in the previous section, username-password authentication is not sufficient. Some protocols need X509 Certificates or Proxies or a Kerberos[16] token to allow non-web base log-in and data access.

Infrastructure imposed requirements.

Finally there are of course requirements imposed by the service provides itself.

Installed systems should seamlessly integrate into the already existing infrastructure, which could be the user/group management, the authentication system or the underlying basic storage technology.

Selecting system components

Taking all the envisioned features into count, it should not come as a surprise that we could not find an affordable technology, providing all of those in once.

However, for most of the non-Web 2.0 features, DESY already had a solution in place: dCache. For more than 10 years, dCache serves the mass storage needs of the DESY and FERMIlab associated for experiments. As DESY is part of the dCache.org collaboration, developing and maintaining dCache, modifications of the dCache code to match the remaining feature requests would have been a possible way to go for us. However, we didn't want to waste time and money implementing functionality into dCache, already available in other products. So we decided to fill the gap in functionality in dCache by intergrating another Open Source technology, which was focusing on web sync and share.

A short survey of installed Cloud solutions at similar institutions finally pointed to ownCloud. ownCloud fulfilled all of the requirements we had concerning the Web 2.0 sync and share feeling. Moreover none of the universities and laboratories we contacted was too unhappy with the product. In particular we took into account the result of the production system at the TU-Berlin [OC02] and the good contacts we have to our colleagues at CERN[17] [OC01], who are evaluating a setup closer to the one we are envisioning, namely running an existing local mass storage system underneath ownCloud.

The following two subsections briefly describe the selected products, with respect to features needed for our hybrid Cloud Storage System.

The dCache storage technology

dCache [DC03,DC04] is a data management technology, in production at more than 70 sites around the world. The total amount of storage managed by dCache exceeds 120 Petabytes in total, with the largest installations holding between 10 and 20 Petabytes of data on disk or tape systems. Although initially designed to solve particle-physics data-lifecycle issues, dCache attracted many other scientific communities, mainly by adopting open standards for data access (e.g. NFS 4.1/pNFS, WebDAV, GridFTP) and data management (e.g. SRM). dCache is an Open Source Software product, provided by dCache.org, an international collaboration composed of

[16] The Kerberos Security System RFC: http://www.ietf.org/rfc/rfc4120.txt
[17] CERN: Organisation Européenne pour la Recherche Nucléaire, Switzerland: www.cern.ch

developers from DESY(Germany), FERMIlab(US) and the Nordic Data Grid Facility, NDGF (Denmark, Sweden, Norway and Finland).

Due to a small set of design decisions, dCache solves most of the data management and scientific data access requirements listed above:

dCache strictly separates data storage from its file namespace, where each namespace entry can point to one or more internal or external copies of the data. This is completely transparent to the user, who only sees the namespace exposed through the supported protocols, like NFS, WebDAV[18] and GridFTP. This allows data to be moved around within dCache and between dCache and external sources without being noticed by users or applications. This design pattern results in the following features:

In vivo system maintenance: Adding or decommissioning hardware can be done while the system is in full operation. When adding hardware, the newly attached storage is immediately available for new requests. Before decommissioning hardware, background processes move data from old hardware to newer storage components before the old hardware is switched off. None of those operations causes system interruptions. This significantly increases the average availability of the system.

User and system defined Retention Policies (Data Durability): As a single name space entry (file name) can point to various internal and external copies of the data, the system or the user can decide to create more copies on disk or tape to increase the retention policy of the file and with that the expected data durability. This allows defining different classes of storage quality to be offered within the same system. As dCache supports media, like Solid State Disks, Spinning disks and tape, different access latencies can be predefined as well.

Scaling and load balancing: dCache was designed to scale out into the 100 Petabytes regime. With installations reaching the 20 Petabytes area, no performance limits were detected yet. However, in large installations, individual storage nodes can be hit by particular high unbalanced load. dCache can be configured to detect those hot spots and to rebalance them by moving files to less loaded storage components.

Another important design pattern is the plug-in framework at various levels of the dCache software stack. Besides other advantages, it allows adding new protocols or new authentication mechanisms without changing the dCache core. As of now dCache supports NFS4.1/pNFS, WebDAV, GridFTP and some proprietary, community specific protocols to access data. For remotely managing data, dCache implements the Storage Resource Manager protocol (SRM[19]). For user authentication, dCache provides username-password based on configuration-files or against Kerberos and X509 Certificates/Proxies for Grid access. dCache supports LDAP for user mapping. Finally, the Cloud Data Management Interface (CDMI[20]) is in preparation, allowing dCache to serve as a data source for OpenStack[21]. All this satisfies the list of features requested by the scientific communities.

The ownCloud cloud system

The ownCloud software is targeting the private storage cloud market. The software is available in an Open Source version as well as a professionally supported commercial version, maintained by the ownCloud Incorporation, with headquarters in the US and Germany.

[18] WebDAV Web Distributed Authoring and Versioning: https://tools.ietf.org/html/rfc4918
[19] The Storage Resource Manager Protocol: https://sdm.lbl.gov/srm-wg/doc/SRM.v2.2.pdf
[20] The Cloud Data Management Interface: http://www.snia.org/cdmi
[21] OpenStack: Open Source Software for building private and public clouds. https://www.openstack.org/

Initially focussed on synching and sharing of small sets of pictures, documents and movies it has been significantly extending its functionality over time, by allowing multiple external storage systems to be attached, providing migration and backup mechanisms and by adding file versioning and group-ware functionality, including shared editing of documents.

For the DESY use-case, only a small set of features and components are of interest:

ownCloud provides “sync clients” for all relevant operating systems. (e. g. Linux, Mac OS and Windows). Those clients bidirectionally synchronize the content of a directory structure on the local computer, where the client is installed and running, with a subset of your private cloud storage within ownCloud.

ownCloud provides Apps for mobile devices to easily upload and download data.

ownCloud allows fine grained sharing of data among its registered users, anonymous users and user groups. Privately shared data is appearing in special ‘Shared’ folders in the destination users home space. Sharing with the public is implemented by generating publicly accessible but non-guessable URLs.

Through additional modules, user authentication and management can be delegated to the local site infrastructure, allowing user and group management to be operated centrally.

Moscicki et al. [OC01], as well as T. Hildmann [OC02] in detail reported on features, deficiencies and performance of ownCloud in a prototype and a production environment.

Component Integration

As a combination of ownCloud and dCache provided essentially everything we needed for the DESY Cloud system, we decided to build a hybrid system. The basic idea is to make a subsection of the dCache home directory of a user available through ownCloud. dCache would provide the different quality of service classes as well as the NFS, GridFTP and WebDAV access and ownCloud would serve parts of the dCache space to sync-clients and would allow sophisticated sharing.

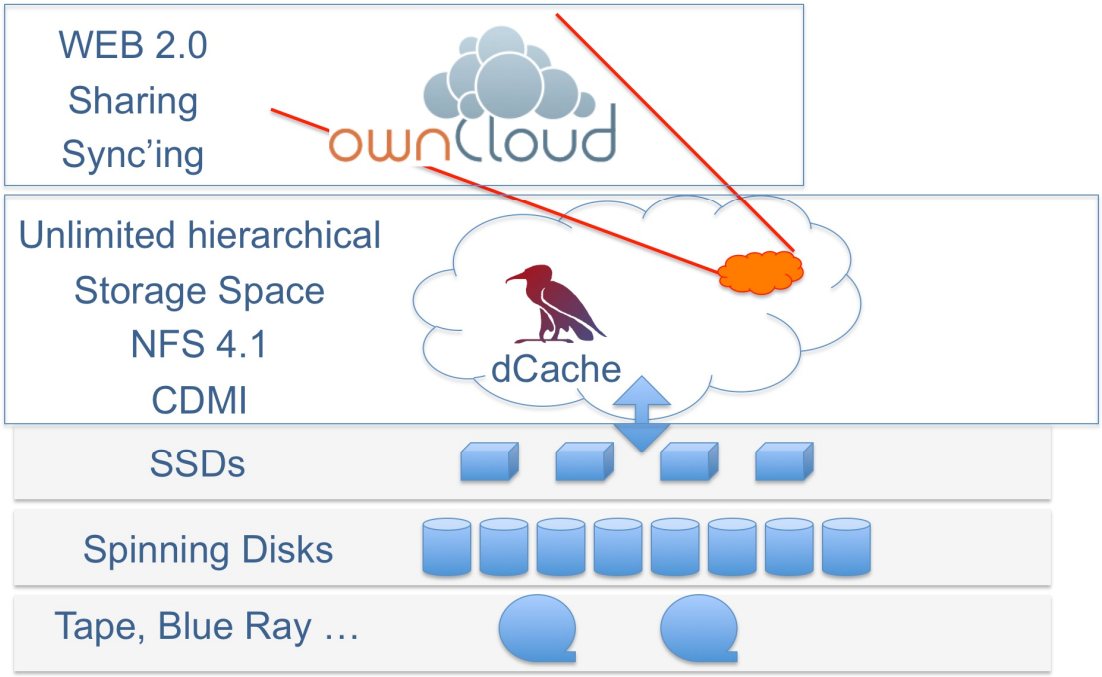


Figure 0-1 The dCache-ownCloud Hybrid System

The first step of that approach (see Figure 0-1) was easy to achieve. ownCloud expects a regular file system for storing its data and dCache provides a regular file system through NFS 4.1/pNFS. The hybrid dCache-ownCloud system was easy to setup and worked as expected. The namespace structure in ownCloud is nicely reflected on the mass storage backend file system in dCache. However, as ownCloud manages its file ownership in an attached database and not with the underlying storage, all files, stored on the backend (dCache) are owned by ownCloud and not by their real owners. This is not an issue as long as data access is exclusively performed though ownCloud. However, as some protocols are only supported by dCache that behaviour needed to be fixed.

The option to modify the ownCloud system to support proper "storage backend ownership" failed, as the file system layer in ownCloud is not sufficiently abstracted. Alternatively we were able to modify dCache to provide the proper ownership in the backend and nevertheless respond to ownCloud requests as the ownCloud system expected.

Prototype, issues and further work

Figure 0-2 drafts the currently deployed prototype where ownCloud is connected to dCache via NFS. The file ownership in ownCloud is maintained within dCache. We keep those synchronized by attaching ownCloud and dCache to the same LDAP server. LDAP path-through to a Kerberos server is used for authentication. This guarantees synchronized authentication of users to ownCloud and dCache with their regular DESY username password pair.

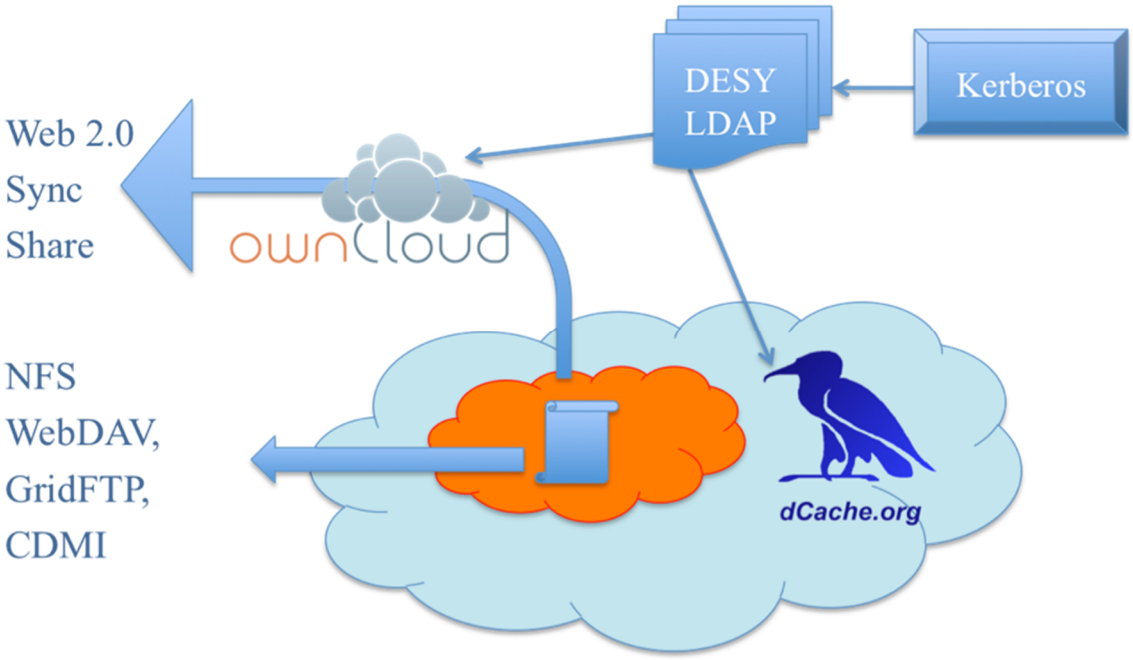


Figure 0-2 Prototype layout and integration into the DESY infrastructure

Issues and future work

File system path layout

In the current version of ownCloud, user home directories are assumed to be subdirectories of a common parent directory. This constrain prohibits us from making only a subdirectory of each dCache home directory available to ownCloud. In our model ownCloud user home directories could be at any arbitrary location in the file system. Our colleagues at CERN modified ownCloud to support that schema. The patch however is not yet fed back upstream to the ownCloud Open Source repository.

Sharing files in ownCloud and dCache.

As described above, the issue of the different file ownerships in ownCloud and dCache is solved. The problem of sharing is not. Access control in ownCloud is managed in its database and is not reflected to the backend storage layer. Consequently files shared in ownCloud are not shared in dCache. In the current version(s) of ownCloud, shared files are appearing in a special folder in the destination user directory, called “Shared“. This folder only “virtually“ exists and is not mapped to a folder in the backend store. Therefore, users accessing their data through dCache directly, won’t have access to that folder and consequently not to the shared data. This problem is extremely difficult to solve. It would require a direct link between the ownCloud virtual file system in the database and the dCache file and access control system.

Using the native dCache WebDAV for file transfers.

Currently, all synchronized data is proxied through the ownCloud front-end servers to the actual storage in dCache. Theoretically this is not necessary, as the ownCloud sync clients essentially are using the WebDAV protocol to communicate with the ownCloud server. dCache however is providing the WebDAV protocol as well. So a redirect from ownCloud to dCache would make data transfers significantly more efficient. Ways to solve this issue are evaluated by dCache.org and the CERN infrastructure team. CERN, similarly to dCache, are planning to operate ownCloud on their home-grown backend storage.

File system abstraction

Some of the issues listed above are the result of the fact that ownCloud assumes a POSIX file system underneath, to store its data. If ownCloud would interact with storage through a published network protocol, exposing file attributes, like owner ship and access permissions, it would be significantly easier to integrate more sophisticated storage back-ends.

Summary

To provide DESY users with a state of the art Big-Data Cloud solution, we evaluated a hybrid system composed of a well-known Cloud product, ownCloud and a Big-Data management system, dCache. The combined feature-set of both systems nicely responds to the requirements collected from our DESY users. The new system provides modern sync and share mechanisms as well as user defined "quality of storage" classes concerning "Access Latency" and "Retention Policy". In addition to "Cloud Protocols" the hybrid system provides protocols essential for the data lifecycle of scientific data, e.g. direct access from computing clusters and wide area bulk transfers. During our evaluation we found non-trivial issues, which we are planning to resolve in collaboration with other interested groups.

Literature

[OC01] Moscicki, J. T. et al.: Prototyping a file sharing and synchronization platform with ownCloud, Chep2013 Proceedings, 2014

[OC02] Hildmann, T.; ownCloud an der Technischen Universität Berlin, Fazit der ersten 6 Monate, ownCloud Hochschulworkshop, 16 Aug 2013

[DC03] Millar, P. et al.: Big Data and HEP, CHEP'13 Proceedings, 2014

[DC04] Fuhrmann, P. et al.: dCache, the agile storage technology, NEC 2013 Proceedings, Varna, Bulgaria.

[GR05] Gardner Report on Research Methodologies
http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp

[DP06] dphep.org: Status Report of the DPHEP Study Group: Towards a Global Effort for Sustainable Data Preservation in High Energy Physics, DPHEP-2012-001 May 2012, http://arxiv.org/pdf/1205.4667.pdf

Ein Jahr mit ownCloud
– von der Planung bis zur Neustrukturierung –

Roland Hager, Thomas Hildmann, Patrick Bittner
tubIT – IT Dienstleistungszentrum
Technische Universität Berlin
Sekr. EN 50, Einsteinufer 17
10587 Berlin
roland.hager@tu-berlin.de
thomas.hildmann@tu-berlin.de
patrick.bittner@tu-berlin.de

Abstract: Die Technische Universität Berlin startete Anfang 2013 als eine der ersten großen Universitäten mit einem Sync&Share Dienst auf Basis von ownCloud. Zu Beginn des Projektes konnte daher auf wenig Erfahrung im Hochschulkontext zurückgegriffen werden. Begonnen von der Motivation zur Einführung eines Sync&Share Dienstes, über die Auswahl der geeigneten Software und die gewählte Startkonfiguration bis hin zu den aktuellen Arbeiten im ownCloud-Kontext wollen wir im vorliegenden Artikel anhand der gesammelten Erfahrungen einen Überblick geben. Die aktuellen Arbeiten umfassen auch die Restrukturierung der Infrastruktur anhand der gewonnenen Kennzahlen. Diese kann auch für andere Einrichtungen als Referenz herangezogen werden. Nach erfolgreicher Einführung des Dienstes liegt unser Hauptfokus heute jedoch mehr auf den Anwendungsfeldern von ownCloud in der Universität die hier auch kurz beleuchtet werden.

Einleitung

Die Bereitstellung von Speicherplatz gehört seit jeher zu den klassischen Aufgaben eines Rechenzentrums. Seit Beginn des Informationszeitalters ist die Datenhoheit von entscheidender strategischer Wichtigkeit.

Angeheizt durch die für Fachkreise wenig überraschenden [Sch01, GK08] Enthüllungen Edward Snowdens [Hol14] im letzten Jahr erlebt die Debatte um „Datensicherheit" eine Renaissance. Ein Hochschulrechenzentrum hat weder die Aufgabe noch die Mittel, Daten so zu sichern, dass sie vor Zugriffen durch Geheimdienste geschützt sind. Wohl aber gehört die Bereitstellung von Datenspeicher in angemessenen Schutzklassen zu den Kernaufgaben.

Outsourcing, Cloud-Computing und Cloud-Storage bleiben auch vor dem Hintergrund von Datenschutzdebatten sinnvolle Chancen, um über Synergien und Bündelungen von Ressourcen und Kompetenzen wirtschaftlich vertretbar den stetig wachsenden Bedürfnissen gerecht zu werden. Entscheidend ist jedoch mit welchen Partnern hierbei zu welchen Konditionen kooperiert werden kann. Vor dem Hintergrund dieser Überlegungen sind Kooperationen zwischen Hochschulen gestützt durch Initiativen wie die des DFN zum Thema Sync&Share als zukunftsweisend zu betrachten. Im globalen Markt werden hier nationale Gesetze und Standards zu entscheidenden Faktoren.

Vor zwei Jahren startete die TU Berlin nicht von Null, als mit dem Projekt „Cloudspeicher" begonnen wurde. Speicherplatz wurde den Nutzern bereits über verschiedene Dienste angeboten. SAN-Speicher kann Servern an der TU durch Unterstellen von Geräten im

Housingbereich oder über Nutzung von virtuellen Servern (Hosting) bereitgestellt werden. Über AFS steht Nutzern seit vielen Jahren eine weltweite Infrastruktur für den Zugriff auf Daten zur Verfügung, die an der Heimatuniversität gespeichert und gesichert werden. Über die WebAFS-Schnittstelle wurde ferner ein Zugriff über Web-Browser auf die Daten ermöglicht. Für die Verwaltung von Source Code oder Dokumenten existiert Subversion. Für die Projektkoordination können Sharepoint-Instanzen bereitgestellt werden.

Mit der Weiterentwicklung der Endgeräte und durch eine neue Konditionierung von Nutzerverhalten u.a. durch Social Media Anwendungen entstehen neue Anforderungen und Erwartungen der Benutzer. Während AFS hervorragend auf Linux-Servern läuft, gibt es auf Windows-PCs häufiger Probleme bei der Nutzung, auf AFS-Daten über das MacBook unterwegs zuzugreifen stellt bereits eine größere Herausforderung dar. Der Zugriff auf die Daten über das Android Tablet und WebAFS kann als nicht mehr zeitgemäß bezeichnet werden.

Warum sollten sich Nutzer mit der fehlenden Nutzerfreundlichkeit der bestehenden Lösungen weiter abmühen, wenn Anbieter wie Dropbox, Microsoft oder Google auf der anderen Seite mittlerweile mehr Speicher kostenlos zur Verfügung stellen? Das Ausmaß der "Datenabwanderung" war im von Dropbox veranstalteten Space Race [Dro12] gut erkennbar.

Der Preis für den kostenlosen Speicher und die gelungene Integration unterschiedlichster Plattformen ist der Verlust der Datenhoheit und Datensicherheit. Neu an den erwähnten Diensten war neben geeigneten Apps für mobile Geräte auch die Möglichkeit der Synchronisation von Daten. Wie bei SVN kann mit einer lokalen Kopie gearbeitet werden, solange der Nutzer offline ist und werden die Daten zurückgeschrieben, sobald eine Netzverbindung bereitsteht. Im Gegensatz zu SVN geschieht dies jedoch für den Nutzer völlig transparent über Verzeichnisstrukturen auf dem jeweiligen PC. Will man die Datenhoheit zurück in die eigene Organisation ziehen, so muss man einen Dienst anbieten, der so einfach ist, wie seine kostenlosen Konkurrenten und möglichst für den Endnutzer erkennbare Mehrwerte bietet, die über die schwer zu greifende Angst vor Datendiebstahl hinaus reichen.

Aus diesen Überlegungen heraus evaluierten wir 2011 einige Sync&Share Lösungen. Unter anderem testeten wir intensiv die Lösungen PowerFolder, Teamdrive und ownCloud. Dabei war ownCloud eigentlich in einer ersten Testrunde bereits als "unreif" ausgeschieden, wurde aber in einer neueren Version am Ende noch einmal neu getestet.

Zum Zeitpunkt unserer Tests waren das intuitivste Userinterface und die Verfügbarkeit von Clients für Linux, Windows, MacOS X, iOS und Android in jeweils nutzbaren Versionen bei unserer Entscheidung für ownCloud ausschlaggebend.

Das Design der Anwendung war klar auf kleinere Benutzergruppen (10–50 Nutzer) ausgelegt aber nicht für potentiell 30–40 Tausend Nutzer. Erste Belastungstests und Hochrechnungen hätten Cluster mit 300–500 Rechner erwarten lassen, um den Zugriffen gerecht zu werden. Uns fehlten belastbare, realistische Werte aus einer großen produktiven Installation. Im Grunde war jedoch klar, dass es sich hier um eine klassische LAMP-Anwendung handeln würde, die wir mit bekannten Techniken skalierbar machen könnten. Also bauten wir zunächst eine kleine Clusterlösung und starteten nach kurzem Test mit wenigen hundert Nutzern in den Flächeneinsatz.

Erste ownCloud Infrastruktur

Basierend auf unseren Erfahrungen mit Diensten wie Typo3 oder unserem Mailcluster starteten wir mit einer Vier-Ebenen-Infrastruktur: Die Basis bildete ein GPFS-Cluster zur Bereitstellung des gemeinsamen Dateisystems und ein MySQL Galera Cluster zur Bereitstellung der

Metadaten. Ein Cluster von Apache-Web-Servern war für die eigentliche Anwendungslogik verantwortlich. Der bereits für viele Dienste erprobte Cisco ACE Load-Balancer war für die Lastenverteilung und zur Sicherstellung der Ausfallsicherheit verantwortlich. Die grundsätzliche Architektur stellte sich im Verlauf als sehr stabil heraus [HK14].

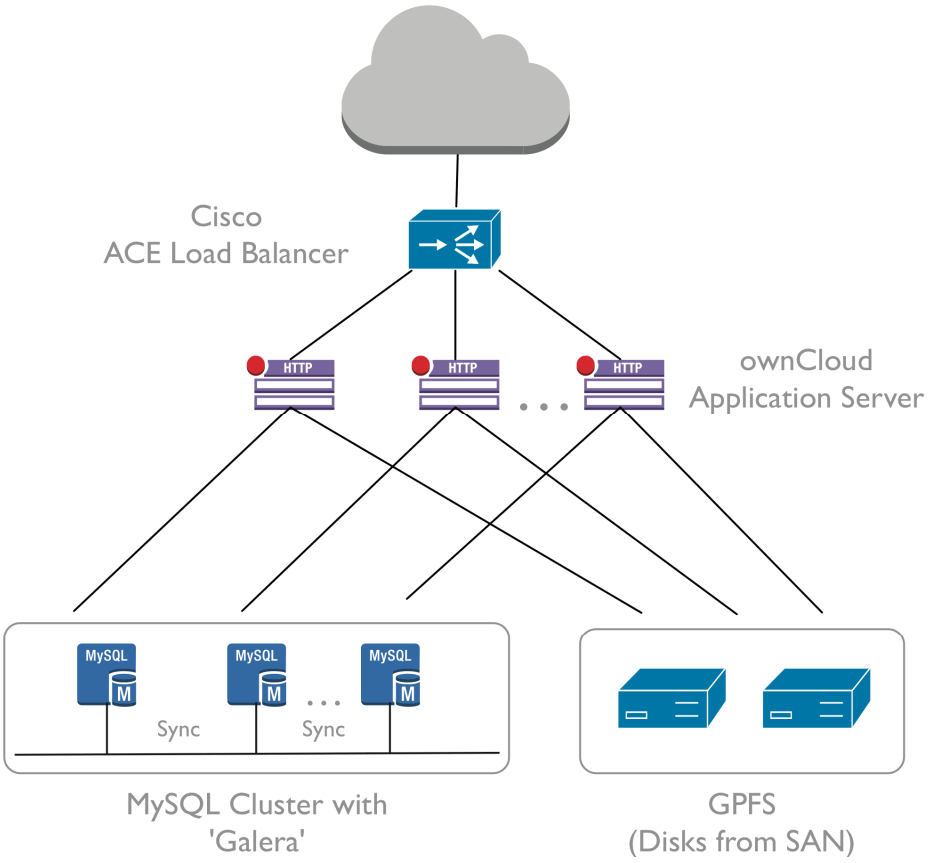


Abbildung 1: Abstrakte Architektur der ownCloud Installation an der TU Berlin

Wie bereits erwähnt lagen uns zu Beginn keine belastbaren Informationen zur Skalierung von Maschinen, Clustergrößen oder zum Nutzerverhalten vor. Wir akquirierten Betatester und beobachteten die Last auf den verschiedenen Systemen.

Die Tests zeigten schnell den Flaschenhals bei den Datenbankanfragen. Eine hohe Auslastung der Datenbanken führte schnell zu einer schlechten Nutzbarkeit. Dabei erkannten wir auch, dass die Probleme weniger bei den Synchronisations-Clients sichtbar werden, als vielmehr beim Webinterface und den mobilen Apps.

Unsere Risikoabschätzungen enthielten begründete Befürchtungen, bei Start für alle Nutzer würde durch das initiale Synchronisieren aller Daten der Dienst lahm gelegt bis hin zur Frage, ob unser SAN der IOPs Anforderung gewachsen sein würde oder unsere Virtualisierungsumgebung durch den Dienst beeinträchtigt würde.

Um eine Beeinträchtigung der existierenden Dienste auszuschließen und bei Bedarf schnell auf Anforderungen reagieren zu können, starteten wir mit einer Mischung aus physikalischen und virtuellen Servern. Der Load-Balancer wurde so konfiguriert, dass er Zugriffe der Sync-Clients und interaktive Zugriffe (Browser, Apps) trennen konnte. Das ermöglichte eine Bearbeitung interaktiver Anfragen mit höherer Priorität.

Die Authentisierung der Nutzer läuft an der TU Berlin gegen ein durch ein zentrales IDM-System gespeistes Active Directory und LDAP mit Kerberos Authentisierung. In unseren Tests sahen wir eine große Last auf dem LDAP-Server und massiven Netzwerkverkehr. Aus diesem Grund entschieden wir uns, auf den Applikationsservern lokale LDAP-Slaves zu installieren und somit den Netzwerkverkehr lokal zu halten bzw. auf die Synchronisation zum LDAP-Master zu beschränken. Um den zahlreichen Authentisierungsanfragen gewachsen zu sein, mussten wir weitere Kerberos-Server bereitstellen, die schlicht über Round-Robin DNS ausbalanciert werden. Auf den Webservern werden die Datenbankabfragen von einem lokalen TCP-Loadbalancer [HAPR] auf das Datenbankcluster verteilt.

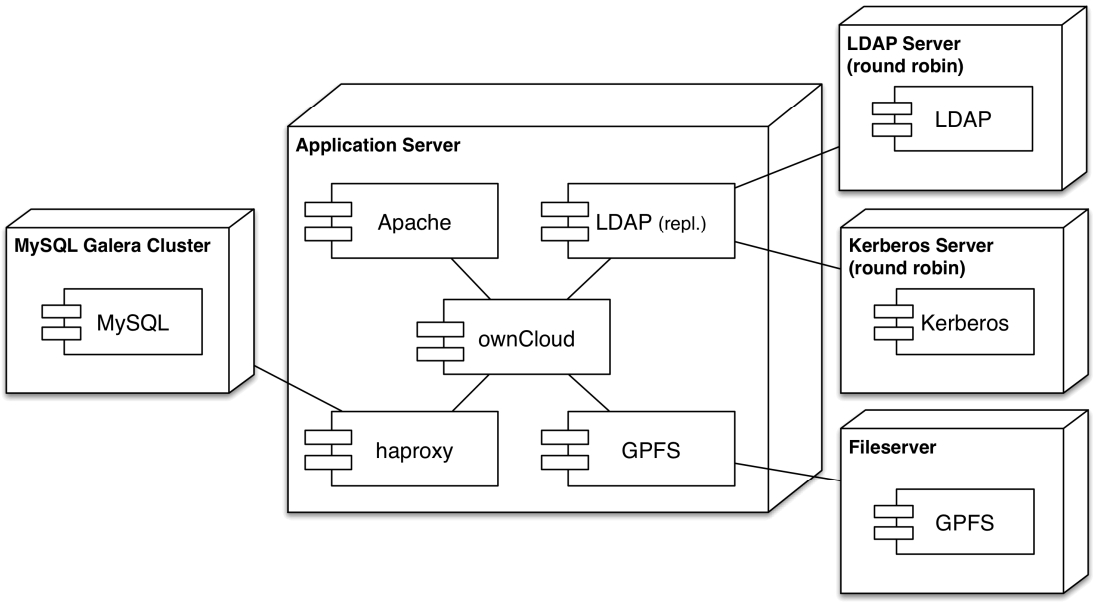


Abbildung 2: Komponenten und Verteilung

Entwicklung der ownCloud Nutzung

Der ownCloud-Dienst wurde am 1.5.2013 offiziell gestartet. Der Feiertag wurde bewusst gewählt, um einen weichen Start zu ermöglichen und bei Performanceengpässen ggf. gegensteuern zu können. Die Einführung des Sync&Share Dienstes wurde allen TUB-Angehörigen via E-Mail bekannt gegeben, auf unseren Webseiten beworben und als Pressemitteilung auf Online-Portalen platziert. Eine dauerhafte Werbekampagne fand jedoch nicht statt. Ausgehend von ca. 300 Nutzern aus den vorangegangenen Testphasen, stieg die Nutzerzahl innerhalb der ersten 14 Tage relativ linear auf ca. 1.600 und nach drei Wochen auf ca. 2.100 Nutzer. Ab diesem Zeitpunkt wuchs die Nutzerzahl kontinuierlich, wenn auch langsamer.

Die erhobenen Daten beziehen sich auf die Version 5 der Community Edition von ownCloud. Während des Betriebs gab es verschiedene Updates, seit Dezember 2013 verwendeten wir die Version 5.0.14. Neben der standardmäßig installierten App „files“, nutzen wir auch die Apps „gallery“ für Bildergalerien und „media“ für die Musikwidergabe. Wir nutzen nicht die Möglichkeit Kalender oder Kontakte mit ownCloud zu synchronisieren.

Um den Grad der Nutzung besser bestimmen zu können, haben wir verschiedene Kennzahlen erhoben bzw. ausgewertet. Im Folgenden sollen die verwendeten Kennzahlen kurz erläutert und voneinander abgegrenzt werden. Die so gewonnenen Daten lassen sich natürlich nicht 1:1 auf

beliebige Umgebungen übertragen, können aber zumindest im universitären Umfeld als Anhaltspunkt für die eigene Planung herangezogen werden.

Nutzer

Ein ownCloud-Nutzer hat sich mindestens ein Mal, egal ob via Webschnittstelle, Desktop- oder Mobil-Client, am Dienst angemeldet. Er kann, muss aber nicht, Dateien synchronisiert haben. Da wir die Benutzer aus unserem zentralen LDAP beziehen, ist die Anzahl der in ownCloud verwalteten Benutzer nicht relevant. In der Tabelle „oc_ldap_user_mapping“ werden die LDAP-Benutzer auf ownCloud-interne Benutzernamen projiziert. Diese Tabelle wird jedoch auch mit Benutzern gefüllt, die beim Teilen von Dateien via auto-complete vorgeschlagen werden. Daher haben wir die Anzahl der Nutzer über die Anzahl der Einträge in der Datenbanktabelle „oc_storages“ definiert, in der jeder Benutzer beim ersten Anmelden einen Eintrag, der auf seinen Speicherbereich im Dateisystem verweist, bekommt. Da wir derzeit keine Einbindung externer oder zusätzlicher Speicher erlauben, existiert in unserer Umgebung tatsächlich nur ein Eintrag pro Benutzer.

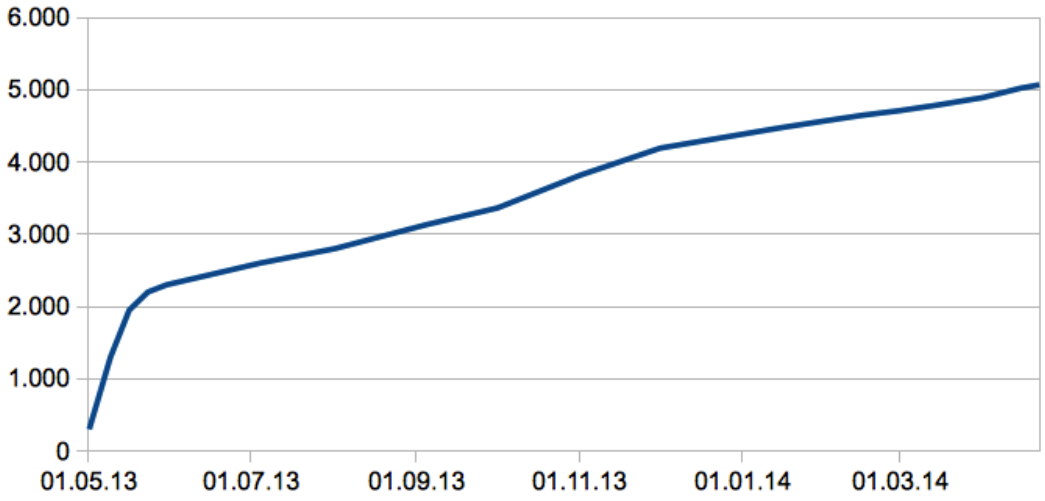


Abbildung 3: Entwicklung der ownCloud-Nutzer

Aktuell zählen wir 5.065 Nutzer. Bei ca. 8.302 MitarbeiterInnen und 31.427 StudentInnen [TUB01] liegt der Anteil der Nutzer somit bei 12,75 %. Seit Jahresbeginn kommen monatlich ca. 182 neue Nutzer hinzu.

Aktive Nutzer

Von aktiven Nutzern sprechen wir, wenn ein Nutzer innerhalb eines definierten Zeitraums innerhalb des eigenen Datenbereichs Dateien oder Ordner geändert, hochgeladen oder gelöscht hat. Hierfür wird in der Datenbanktabelle „oc_filecache“ nach Einträgen gesucht, deren Änderungszeitstempel im jeweiligen Zeitraum liegt. Gelöschte Daten können dabei nur detektiert werden, wenn diese von ownCloud im Papierkorb untergebracht werden. Falls die gelöschten Daten größer als die verfügbare Quota des Nutzers sind und keine älteren Daten aus dem Papierkorb entfernt werden können, ist dies u.U. nicht möglich. Hier besteht die Möglichkeit, dass eigentlich aktive Nutzer nicht korrekt erkannt werden. Nutzer, die ausschließlich Dateien herunterladen oder mit geteilten Daten anderer Nutzer arbeiten, können auf diesem Weg nicht erfasst werden und somit selbst nicht als aktiv gezählt werden. Aber auch

Nutzer ohne jedwede Interaktion mit ownCloud sind nicht zwangsläufig „Karteileichen“. Viele nutzen ihren ownCloud-Speicher als Archiv oder Backup, das nur gelegentlich oder nie aktualisiert wird. Für die Skalierung der Infrastruktur sind die aktiven Nutzer interessant, da diese am meisten Last erzeugen.

Von derzeit 5.065 Nutzern waren 2.121 vom 1.1.2014 bis 22.4.2014 aktiv. Damit haben gut 42 % der Nutzer den Dienst aktiv zur Dateisynchronisation genutzt. Monatlich waren in diesem Zeitraum durchschnittlich 1.179 Nutzer aktiv. Womit fast ein Viertel (23 %) der Nutzer den Dienst mindesten einmal im Monat aktiv nutzte. Die tägliche Nutzung schwankt naturgemäß stark zwischen Werktagen, mit durchschnittlich 287, und Wochenenden bzw. Feiertagen mit durchschnittlich 128 aktiven Nutzern. Insgesamt nutzten seit Jahresanfang durchschnittlich 237 der Nutzer, also ca. 4,68 %, den Dienst täglich aktiv. Die höchste Tagesnutzung lag bei 349 aktiven Nutzern. Die Hauptnutzung liegt Werktags in der Zeit von 10–17 Uhr.

Anzahl der Dateien / Ordner

Da sowohl Dateien als auch ggf. leere Ordner synchronisiert werden müssen – und somit Last erzeugen – unterscheiden wir hier nicht zwischen beiden.

Derzeit (22.4.2014) haben alle 5.065 Nutzer zusammen etwas mehr als 8,77 Mio. Einträge in der Datenbanktabelle „oc_filecache“. Diese Tabelle enthält Metadaten zu den Ordnerstrukturen und Dateien und umfasst auch die vom ownCloud-Core und den ownCloud-Apps angelegten Dateien und Ordner, beispielsweise für den Papierkorb, die Versionierung und den Cache. Seit Jahresbeginn kommen monatlich etwa 450.000 neue Einträge hinzu.

Um nur die Anzahl der von Nutzern selbst angelegten Dateien und Ordner zu ermitteln, betrachten wir lediglich die Einträge der Tabelle, bei denen der Pfad mit „files/“ beginnt, dort liegt der für die Nutzer sichtbare Datenbereich. Hier existieren ca. 7,9 Mio. Einträge. Die Nutzer haben also 7,9 Mio. Dateien und Ordner angelegt und 0,78 Mio. Einträge wurden systemseitig generiert. Das entspricht einem Overhead für Papierkorb, Versionierung und Cache von etwa 10 %.

Die 7,9 Mio. Einträge der Nutzer sind real alles andere als gleich verteilt, wie die folgende Tabelle zeigt.

Anzahl Einträge	Anzahl Nutzer	Einträge insgesamt
1–9	1.270	3.421
10–99	682	26.353
100–999	651	253.272
1.000–9.999	495	1.815.917
10.000+	196	5.805.690
Gesamt:	*3.294*	*7.904.653*

Tabelle 1: Nutzerzahlen gruppiert nach Anzahl der Einträge pro Nutzer

Insgesamt haben also 3.294 Nutzer selbst Daten eingestellt. Davon haben 2.024 Nutzer mindestens 10 Ordner und Dateien erstellt, was in etwa der Anzahl aktiver Nutzer seit Jahresbeginn entspricht. Diese 2.024 Nutzer haben durchschnittlich etwa 3.900 Dateien und

Ordner in ihrem ownCloud-Bereich. Bei 5.065 Nutzern insgesamt haben demnach aber auch 1.771 Nutzer keinerlei eigene Daten gespeichert. Ob diese den Dienst nach einmaliger Anmeldung nicht mehr genutzt haben, oder ob sie ggf. mit den freigegebenen Daten anderer Nutzer arbeiten, ist nicht bekannt, da wir keine Statistiken über das Anmeldeverhalten der Benutzer führen.

Dateigrößen / Quotanutzung

Hier nutzen wir erneut die Tabelle „oc_filecache“ und betrachten nun alle Einträge bei denen der Pfad mit „files/“ beginnt und der mimetype kein Verzeichnis ist. Damit erfassen wir alle Dateien, die von Nutzern hochgeladen wurden. Dabei überwiegen bei weitem kleine Dateien. Gut 88% des Speicherbedarfs entfällt auf Dateien unter 1MB und nur vier Dateien sind größer als 1GB.

Dateigröße	Anteil am Speicherbedarf	Anzahl Dateien
0KB–10KB	49 %	3.460.805
10KB–100KB	24 %	1.700.646
100KB–500KB	11 %	792.435
500 KB–1.000KB	4 %	299.442
1.000KB–10MB	11 %	807.752
10MB–100MB	0,09 %	6.683
100MB–1.000MB	0,0069 %	486
> 1.000MB	0,000006 %	4

Tabelle 2: Anteil am Speicherbedarf und Anzahl nach Dateigröße gruppiert

Von den Nutzern mit Dateien im eigenen Datenbereich verwenden ca. 68% weniger als 1GB ihrer Quota und ca. 25 % nutzen 1 GB bis 10 GB. Mehr als 10 GB verwenden nur ca. 6 % der Nutzer allerdings liegt das Quotalimit für Studierende bei 10 GB.

Web-Anfragen

Hiermit sind Webseitenzugriffe gemeint, die sich aus den Zugriffslogs der Webserver ergeben. Gezählt werden alle Anfragen, nicht nur Seitenanfragen, so dass auch Zugriffe auf CSS-, JavaScript-Dateien und dergleichen erfasst werden. Die Punkte markieren die Anfragen der jeweils kompletten vorangegangenen Woche zwischen Mai 2013 und April 2014.

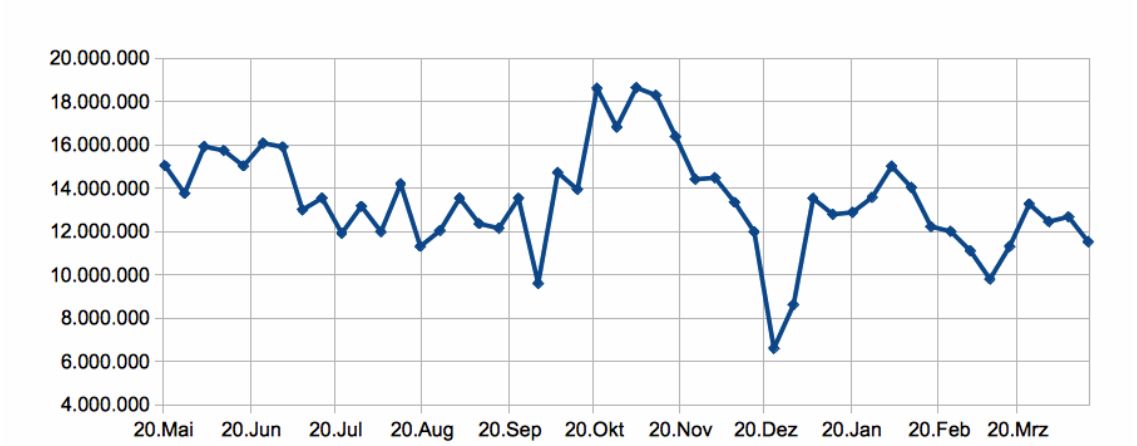


Abbildung 4: Webzugriffe der jeweils letzten Woche

Trotz steigender Nutzerzahlen hat sich die Anzahl der Anfragen auf die Webserver eher verringert, was aber vermutlich auf die verbesserten Sync-Clients zurückzuführen ist, und nicht auf ein geändertes Nutzerverhalten. Ab Version 1.4.x wurde die Art optimiert, wie auf geänderte lokale oder entfernte Daten geprüft wird und so unnötige Serveranfragen und Syncvorgänge vermieden.

Seit Anfang 2014 verzeichnen wir – mit der ownCloud Serverversion 5.0.14 – durchschnittlich ca. 1,78 Mio. Anfragen pro Tag mit Spitzen bis zu 2,6 Mio. Anfragen. Zum Vergleich: Unser zentraler Webauftritt mit Webseiten für ca. 450 Einrichtungen und 280 Teamauftritten verzeichnete seit Jahresbeginn täglich im Schnitt 1,87 Mio. Anfragen mit Spitzen bis zu 3,1 Mio.

Datenbankgröße

Für jede Datei, die in ownCloud gespeichert wird, existiert ein Datenbankeintrag, so dass Metadaten ohne teure Zugriffe auf das Dateisystem ausgewertet werden können. Die Tabelle „oc_filecache“ hat dadurch mit Abstand den größten Platzbedarf. Die weiteren Datenbanktabellen liegen maximal im niedrigen 2- bis 3-stelligem Megabyte-Bereich. Die Datenbankgröße bezieht sich auf den Platzbedarf der owncloud-Datenbank im Dateisystem.

Für die aktuell 5.065 Nutzer fallen insgesamt ca. 5,4 GB Daten an, davon entfallen allein 4,3 GB auf die „oc_filecache“ Tabelle. Seit Jahresbeginn wuchs die Datenbank durchschnittlich um gut 168 MB pro Monat.

Serverskalierung

Für aussagekräftige Zahlen zur Serverauslastung unter realen Bedingungen im Produktivbetrieb, haben wir die Infrastruktur stark reduziert. Für einen vollen Tag wurden alle Anfragen von Sync-Clients auf nur einen realen Websever, anstatt sieben verteilt und alle Browserzugriffe auf zwei virtuelle Webserver anstatt auf drei. Die drei Webserver haben ihre Datenbankanfragen an drei identische reale Server aus dem Galera-Cluster verteilt, anstatt auf sieben.

Am Testtag konnten wir 320 aktive Nutzer verzeichnen, die ca. 2 Mio. Anfragen an den Webserver für Sync-Clients und ca. 46.000 an die beiden Webserver für Browserzugriffe gestellt haben. Die Werte liegen über dem bisherigen Jahresdurchschnitt und sind somit für eine eher großzügige Abschätzung der notwendigen Serverressourcen gut geeignet.

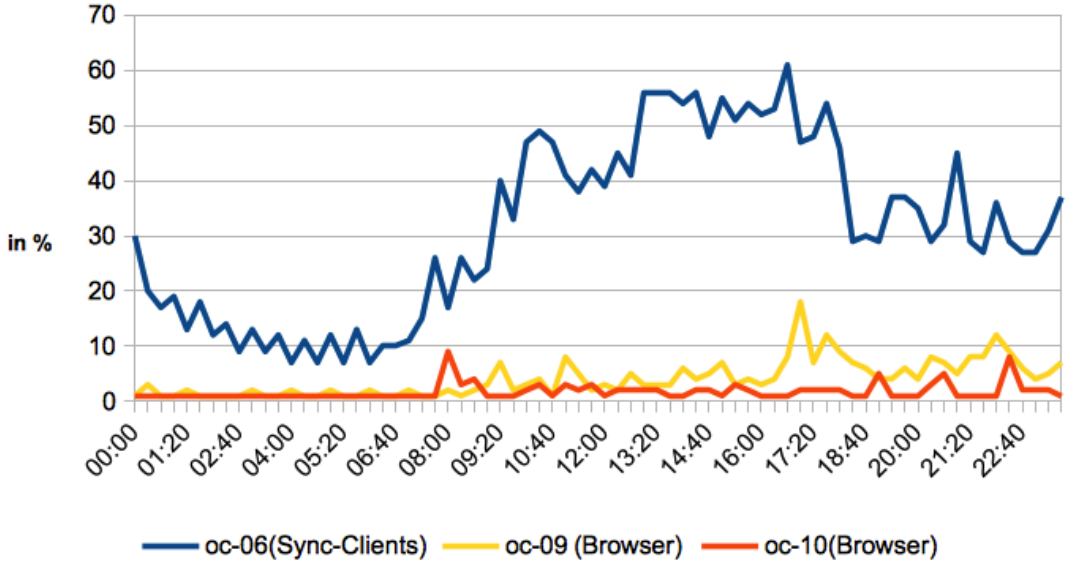


Abbildung 5: CPU-Auslastung der Webserver

Das 95. Perzentil für den Webserver oc-06 lag bei 56 % CPU-Auslastung. Der Arbeitsspeicher war mit ca. 8 GB nahezu konstant zu 50 % belegt. Unter der vereinfachenden Annahme, dass die CPU-Last pro aktivem Nutzer etwa gleich verteilt ist und sich proportional zu diesen entwickelt, könnte der Server rein rechnerisch bis zu 571 aktive Nutzer bedienen. In Spitzenzeiten könnten dann allerdings die freien Webserver-Slots und der verfügbare RAM zum limitierenden Faktor werden. Das wiederum hängt stark von der Konfiguration ab, z.B.wie hoch das „memory limit“ in der php.ini eingestellt ist.

Auf den beiden virtuellen Webservern für die Browser-Zugriffe mussten vergleichsweise wenige Anfragen verarbeitet werden, so dass auch die Auslastung kaum nennenswert ist. Bereits einer dürfte bei ähnlichem Nutzungsverhalten von bis zu 571 aktiven Nutzern mehr als ausreichend dimensioniert sein. Klar wird auch: Die Aufteilung von Sync-Client- und Browser-Zugriffen ist nicht zur gleichmäßigen Lastverteilung geeignet. Sinnvoll ist sie nur für die von uns beabsichtigte Entkopplung von antwortzeitsensitiven interaktiven Zugriffen durch „echte Menschen“ und den Sync-Clients, bei denen eine erhöhte Latenz in den Spitzenzeiten weniger negativ auffällt.

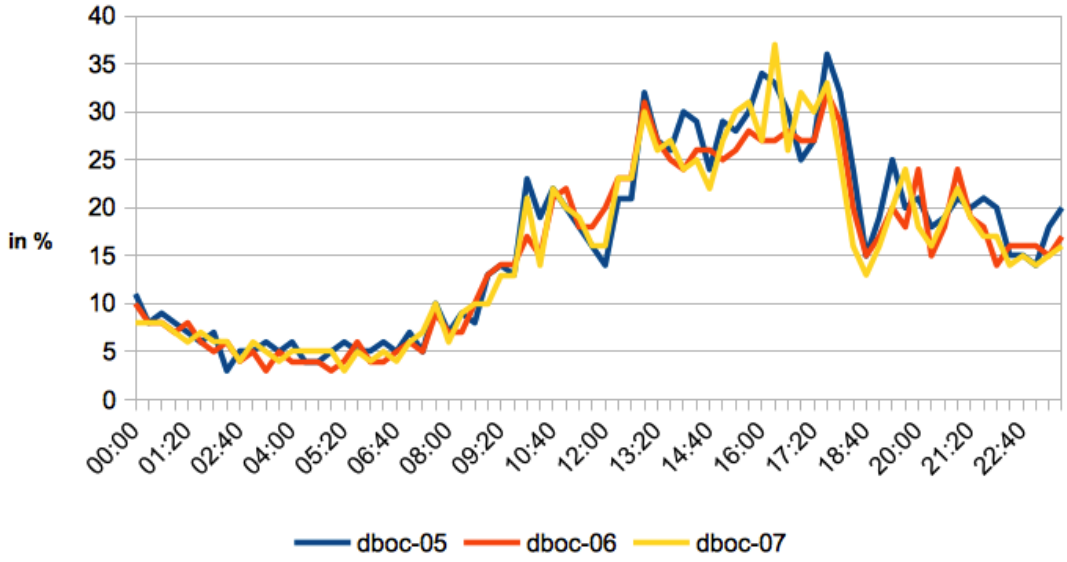


Abbildung 6: CPU-Auslastung der Datenbankserver

Die CPU-Auslastung der drei Datenbankserver ist, auf Grund der gleichmäßigen Verteilung der Anfragen, erwartungsgemäß ebenfalls gleichmäßig verteilt. Die Datenbank füllt den derzeit 10 GB großen InnoDB Buffer Pool zu etwas mehr als 50 %, passt also vollständig in den Arbeitsspeicher. Bei der Skalierung der Datenbankserver sollte unbedingt bedacht werden, dass Schreibzugriffe bei einem Galera-Cluster nur bedingt skalieren. Zwar übernimmt der Server, bei dem die SQL-Anfrage aufläuft, das Query-Parsing, diverse Optimierungsprozesse und dergleichen, das geänderte Schreibset muss jedoch auf allen Datenbankservern nachvollzogen werden. Jeder Schreibzugriff auf einem Server verursacht so auch auf den anderen Servern Last. Ein Galera-Cluster kann somit nicht beliebig in der Breite skalieren. Daher empfiehlt es sich hier eher weniger aber dafür gut ausgestattete Server zu verwenden. Abzuraten ist von der Mischung unterschiedlich performanter Server. Änderungen an der Datenbank erfolgen synchron, so dass ein langsamer Server im Cluster schnell zum Flaschenhals wird.

Nicht betrachtet haben wir die Fileserver. Bereits bei den ersten Untersuchen zur Auslastung der Server einige Wochen nach Dienststart stellten wir fest, dass die verwendeten Fileserver fast keinerlei Auslastung aufwiesen und die anfallenden Daten und Datenänderungen hervorragend bewältigt haben. Natürlich sollte ausreichend freier Speicherplatz vorhanden sein.

Erfahrungen nach dem 1. Jahr

Nach rund einem Jahr Betrieb können wir nicht nur auf gesammelte Monitoringdaten, sondern auch auf zahlreiches Feedback und Supportaktivitäten zurück blicken.

Der Dienst wird gut, wenn auch nicht im erwarteten Umfang angenommen. Die Benutzerzahlen sind stetig steigend. Eine höhere Durchdringung erwarten wir, wenn die ersten Lehrveranstaltungen ownCloud direkt nutzen, sowie nach der Umsetzung der zur Zeit bearbeiteten Erweiterungen (siehe “ownCloud Anwendungsfälle” und “Ausblick”). Kleinere Pannen beim Start des Projektes (z.B. “Out of Inodes" auf dem Fileserver am ersten Wochenende) sind durch die Nutzer schnell verziehen.

Die meisten Nutzer kommen mit dem Dienst gut zurecht. Für einige hundert oder tausend Nutzer ist ownCloud bereits zum alltäglichen Standardwerkzeug geworden. Die Daten der

Projektarbeit und Referenzdaten werden praktisch unbemerkt in die eigene ownCloud synchronisiert und sind von dort aus auch vom Laptop, Smartphone oder sogar vom Webbrowser von unterwegs zugreifbar. Dateien müssen nicht mehr per Mail hin und her geschickt werden, sondern werden geteilt (auch dieses Dokument entstand über ein geteiltes Verzeichnis in ownCloud).

Der Supportaufwand ist trotz steigender Nutzung vergleichsweise niedrig. Ein Großteil der Anfragen wird zur Zeit von einer einzelnen studentischen Hilfskraft (2–3 Anfragen pro Woche) oder bereits im 1st Level Support beantwortet. Nur selten laufen Anfragen ans Backup-Team oder noch seltener beim Web- oder Datenbankteam auf (1–2 Anfragen im Monat).

Oft haben Nutzer versehentlich Dateien gelöscht oder überschrieben und finden diese nicht im Papierkorb oder über die Versionierung wieder. Einige Nutzer berichten von Problemen bei der Synchronisation, häufig verursacht durch "ungeschicktes" Ändern oder Verschieben der Synchronisationsquellen oder -ziele, durch Verwendung unterschiedlicher Clientversionen oder deren Datenbanken, durch Drittsoftware, die mit den Dateien arbeitet usw. Ferner wurden doppelte Dateien, Endlosschleifen bei der Synchronisation oder "unerklärliche" Konfliktdateien oder Löschungen von Dateien oder Verzeichnissen gemeldet. Solche Fälle tauchen jedoch außerordentlich selten auf und lassen sich praktisch in 100 % der Fälle durch Neuaufsetzen der Clientumgebungen (neuester Client, alle Dateien noch einmal neu aus der ownCloud synchronisieren) beseitigen. Alle ownCloud-Daten werden täglich inkrementell auf Bändern gesichert. Ferner werden mehrfach täglich Snapshots vom Dateisystem gemacht. Dies befähigt uns im Falle von besagten Fehlern durch oder bei Nutzern die Dateien wieder herzustellen, sofern das nicht bereits durch die Funktionen in ownCloud vom Nutzer selbst erledigt werden kann.

Auf Grund unserer positiven Erfahrungen haben wir uns entschlossen, das System weiter zu betreiben und auszubauen. Nachdem das System für immer mehr Anwender immer wichtiger wird, haben wir uns entschlossen auf die Enterprise Edition zu wechseln und somit auch professionellen Support für unsere Installation zu besitzen. Längerfristig ist die Enterprise Edition auch mit dem Shibboleth-Modul interessant, wenn in Kooperation auch ownCloud Speicher für andere Hochschulen angeboten werden soll.

Unsere Infrastruktur hat sich als sehr robust erwiesen. Der Einsatz vieler kleiner MySQL-Server hat sich jedoch nicht bewährt. Während lesende Zugriffe hervorragend skalieren, müssen Schreibzugriffe synchron auf allen Servern nachvollzogen werden. Dadurch ist die Skalierbarkeit bei hohen Änderungsraten mit kleineren Servern nur begrenzt möglich. Auf den Fileservern ist kaum Last zu verzeichnen, jedoch machen sich die Zugriffe im nachgelagerten SAN bemerkbar, wo sie mit den Zugriffen anderer Diente konkurrieren und diese mitunter ausbremsen. Darüber hinaus kann der angebundene SAN-Speicher nicht beliebig vergrößert werden.

Umbau der Infrastruktur

Anhand der Erfahrungen haben wir uns entschieden die Infrastruktur im Detail umzubauen, um auch für die nächsten Jahre und bei steigender Nutzerzahl den Dienst stabil betreiben zu können. Dafür haben wir im Bereich der Fileserver ein neues GPFS-Cluster mit zwei GSS24-Servern installiert, also je zwei redundante GSS-Server mit je vier JBODs an zwei Standorten. Das neue GPFS-Cluster bietet insgesamt 322 TB nutzbaren Speicherplatz und entlastet so auch die vorhandene SAN-Infrastruktur, die nun nicht mehr eingebunden wird. Das GPFS-Cluster soll sukzessive auch als shared-storage für andere Webdienste, Fileserver im Bereich der Universitätsverwaltung und für die Heimatverzeichnisse von Benutzern genutzt werden soll.

Der MySQL Galera-Cluster zieht auf drei identische Hardwareserver mit jeweils knapp 380 GB RAM und 1,5 TB redundanten SSD-Festplatten um. Auch hier wird bereits über die Parallele Nutzung der Hardware für andere Dienste nachgedacht.

ownCloud Anwendungsfälle

OwnCloud wird in der TU Berlin inzwischen nicht nur als simples Sync&Share Tool verwendet, sondern wird auch immer stärker in die einzelnen Arbeitsprozesse unterschiedlichster Bereiche integriert.

Dabei ist vor allem der Umstand, dass die Daten direkt in der TU Berlin gehalten werden, und somit als deutlich „sicherer“ angesehen werden, als bei anderen Diensten, für die meisten Anwendungsfälle ausschlaggebend. In Zusammenarbeit mit der Datenschutzbeauftragten wird Umfang und Art der Nutzung genau abgesprochen. Da der Datenschutz in der TU Berlin schon während der Einführungsphase von ownCloud mit dem System und seinem Aufbau vertraut gemacht wurde, ist an dieser Stelle eine adäquate Einschätzung seitens des Datenschutzes ohne weiteres möglich.

Auch das IT-Service-Center der TU Berlin fokussiert die Benutzung von ownCloud, und zwar in mehrfacher Weise:

Zum Einen können Daten, die den Nutzern zur Verfügung gestellt werden sollen, direkt über einen freigegebenen ownCloud Share bereitgestellt werden (eine Möglichkeit, die auch für Lehrveranstaltungen von besonderem Interesse sein kann), zum Anderen setzt auch das an der TU Berlin entwickelte tubIT-LIVE System auf einer ownCloud Nutzung auf:

tubIT-LIVE ist ein speziell auf die Anforderungen der einzelnen Studenten abgestimmtes Betriebssystem-Image, welches den Studierenden der TU Berlin (u.a. über ihren ownCloud Zugang) ab dem Zeitpunkt ihrer Provisionierung zur Verfügung gestellt wird. Dieses System enthält einige Dienste, die schon direkt für die Studenten vorkonfiguriert sind, wie z.B. den Maildienst. Des Weiteren kann, über eine webbasierte Auswahlmaske, die einem Online-Shop nachempfunden wurde, ausgewählt werden, welche Inhalte ein Studierender im System integriert haben möchte. Diese Auswahl initiiert eine Änderung in den onwCloud shares, wodurch den Studierenden die ausgewählten Inhalte direkt in ihren ownCloud Bereichen zur Verfügung gestellt werden.

Die entsprechenden ownCloud Bereiche können im Vorfeld von den Dozenten beantragt und eingerichtet werden. Die Studierenden selbst erhalten dabei einen lesenden Zugriff, welcher ihre eigene Quota nicht weiter beeinflusst, da diese sonst die Anzahl der auswählbaren Inhalte einschränken würde. Dies schließt eine zusätzliche, andersartige Benutzung von ownCloud innerhalb der Lehre nicht aus, sondern stellt lediglich eine von tubIT unterstützte Lehrhilfe dar.

Fazit

Der Aufbau eines Sync&Share Dienstes, der die Daten im Haus hält war notwendig und richtig. Viele Softwarelösungen in diesem Bereich liefern sich zur Zeit einen erbitterten Kampf um Usebility, Stabilität und Funktionsumfang. Dies erklärt, warum andere Hochschulen mit gleicher Fragestellung zu einem anderen Zeitpunkt auch zu einem anderen Auswahlergebnis kamen. Mit unserer aktuellen Wahl von ownCloud sind wir zur Zeit sehr zufrieden.

Sowohl in Bezug auf den eigentlichen Dienst, als auch in Bezug auf Software und Infrastruktur bestand von unterschiedlicher Stelle große Skepsis. Nach nunmehr einem Jahr ohne

nennenswerten Ausfällen und mit vielen positiven Rückmeldungen von Nutzern ist diese Skepsis nunmehr gewichen.

Heute stehen unterschiedliche große Installationen von Sync&Share Diensten. Nicht wenige wurden auf Basis von ownCloud errichtet. Einrichtungen, die heute vor dem Aufbau einer eigenen Installation steht kommt diese Erfahrung zugute.

Der Betrieb von ownCloud ist aus Sicht der Anwender jedoch erst der erste Schritt. Die Universität muss die Installation nun mit Leben füllen, d.h. das ownCloud-Angebot nutzen. Dabei unterstützen wir mit der Integration verschiedener Anwendungen, die mit ownCloud arbeiten oder erst dadurch möglich werden. Die Integration in die Organisationsinfrastruktur und die Nutzung von ownCloud aus anderen Diensten heraus motiviert letztlich auch zur Migration von externen auf die lokalen Speicherdienste. Dies bringt letztlich die Daten wieder nach Hause.

Literaturverzeichnis

[GK08] Gaycken S., Kurz C., 1984.exe – Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien, Transcipt Verlag, Bielefeld 2008

[Sch01] Schneier, B., Secrets & Lies – IT-Sicherheit in einer vernetzen Welt, dpunkt.verlag, Heidelberg 2001

[HK14] Hildmann, T., Kao O., Deploying and extending on-premise cloud storage based on ownCloud, DCPerf'14, Madrid 2014

[Hol14] Holland, M., NSA-Skandal in Europa: Zwischen Fassungslosigkeit, Desinteresse und Resignation, heise online 2014, http://heise.de/-2123804

[Dro12] Dropbox. (2012) Dropbox space race. [Online]. Available: https://www.dropbox.com/spacerace

[TUB01] TU Berlin: Zahlen & Fakten [Online] Stand: 22.04.2014 http://www.tu-berlin.de/menue/ueber_die_tu_berlin/zahlen_fakten/

[RBK14] Ritter, C.; Bittner, P.; Kao, O.: Der Weg von BYOD zum GYSE. Proceedings 7. DFN Forum 2014: Kommunikationstechnologien

[HAPR] HAProxy, The Reliable, High Performance TCP/HTTP Load Balancer http://haproxy.1wt.eu/ [Online] Stand: 22.04.2014

Sicherheit und Collaboration in der Cloud: Die hochsichere Plattform für Datenaustausch und Datenspeicherung im Hochschulumfeld

Ulrich Baur, Alfred Silwester
Manager Cloud Sales, Dimension Data
Business Development, SSP Europe
ulrich.baur@dimensiondata.com
a.silwester@ssp-europe.eu

Abstract: Eine Cloud-Plattform für die Datenspeicherung und den Informationsaustausch zwischen Mitarbeitern, Studierenden sowie externen Einrichtungen bietet viele Vorteile. Allerdings sind es häufig gerade Bedenken hinsichtlich der Informationssicherheit oder der Integrationsfähigkeit, die viele Hochschulen bei der Entscheidung für eine Cloud-Lösung zögern lassen. Die signifikanten Kriterien und unabdingbaren Anforderungen an Management und Rechteverwaltung, Sicherheit, Integration und Handhabung am Beispiel des Secure Data Space der SSP Europe GmbH, auf Grundlage der Managed Cloud Plattform von Dimension Data als Ablaufumgebung, sollen Gegenstand dieser Abhandlung sein.

1 Datensicherheit

Bei der Verschlüsselung sensibler Unternehmensdaten wird häufig der Datensatz in nur einer einzigen Instanz gleichzeitig verschlüsselt und übertragen, liegt dann jedoch unverschlüsselt und für jeden Netzwerkadministrator zugänglich auf den Servern der Cloudservices-Anbieter. Allerdings können Unternehmensdaten nur durch die unmittelbare Verschlüsselung auf dem eigenen Gerät und ohne Zugang des Cloudservice-Anbieters zum Verschlüsselungscode wirklich sicher in der Cloud gespeichert und ausgetauscht werden. Die Datenverschlüsselung des Cloud- und IT Security-Spezialisten SSP Europe wird mit der Triple-Crypt® Technology auf dem Secure Data Space direkt durch die Software auf dem jeweiligen Gerät vorgenommen und anschließend durchgängig weitergeführt.

Dabei wird für jeden Anwender in der Gerätesoftware ein Schlüsselpaar generiert. Indem der öffentliche Schlüssel auf dem Server gespeichert wird, ist es dem Administrator jederzeit möglich, weitere Daten für den Anwender zu codieren. Jedoch können damit keine Daten des Anwenders decodiert werden. Der Anwender kann seinen privaten Schlüssel mit einem persönlichen Kennwort gesichert auf dem Server ablegen, wodurch er ihn von beliebigen Geräten aus abrufen und verwenden kann. Dies gilt sowohl bei der Übertragung über den Web-Client (alle gängigen Browser) als auch bei den nativen Clients (Windows, iOS, Android).

Um die Sicherheit bei der Speicherung von Hochschuldaten so hoch und gleichzeitig so einfach wie möglich zu gestalten, verfolgt SSP Europe einen innovativen Ansatz bei der Anwendung der Triple-Crypt® Technology für den Secure Data Space: Die Verwaltung, Verteilung und Installation von Zertifikaten erfolgt automatisiert und sicher über das integrierte Public-Private-Key-Verfahren, bei dem nur dem Anwender die Zugangsdaten bekannt sind.

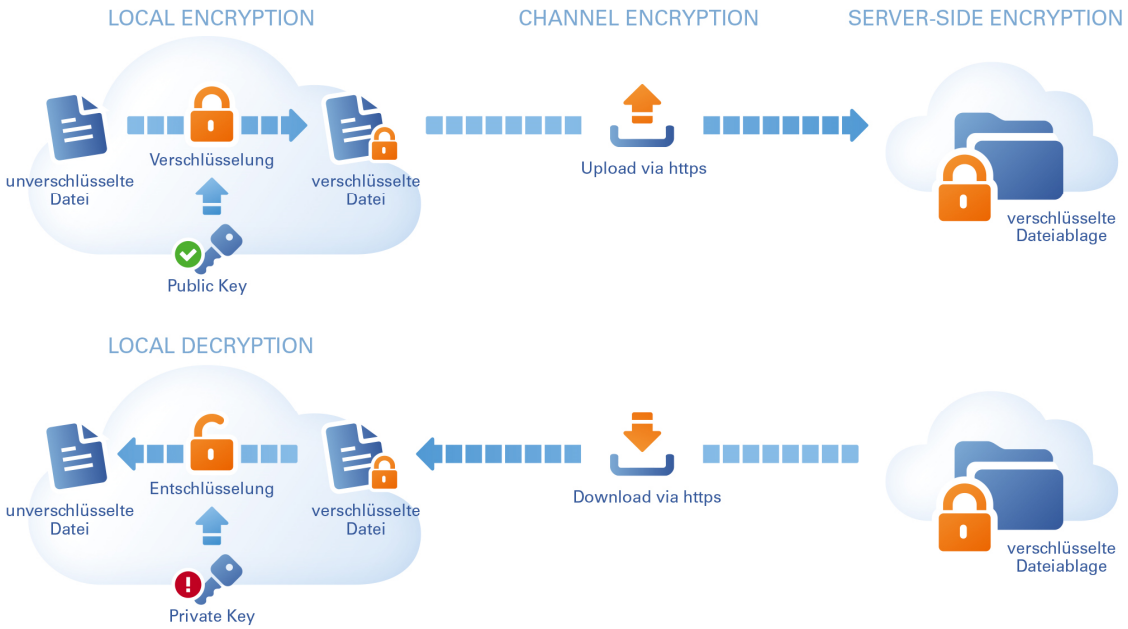


Abbildung 1: 3-way Encryption Secure Data Space

Dabei erfolgt die Kodierung der Daten mittels eines Public-Keys in Kombination mit mathematischen Algorithmen (Asymmetric Encryption). Der Anwender muss diese an seinem Endgerät mit Hilfe eines Private-Keys dekodieren. Da ausschließlich der User seinen Private-Key kennt, ist dieser bestmöglich gegenüber Missbrauch durch Dritte geschützt. Der Public-Key muss dagegen nicht besonders gesichert werden, da er allein keine Funktion für Datenspione hat. Darüber hinaus sind Technologien und Prozesse wie Disaster Recovery, Zugangsbeschränkungen, Intrusion Protection/ Prevention und Firewall-Dienste wichtige Kriterien für einen seriösen Cloudanbieter, wie in diesem Fall der Systemintegrator und Cloud Service Provider Dimension Data, der mit seiner MCP (Managed Cloud Plattform) eine dynamische und hochsichere Cloud-Infrastruktur zur Verfügung stellt: im Rahmen seiner Cloud-Lösungen, die von public über private und hybrid bis hin zu hosted Modellen reichen. An schwankende Bedarfssituationen flexibel anpassbar zu sein, skalierbares Backup und Disaster Recovery, die Erfüllung der relevanten Zertifizierungsstandards sind dabei nur einige Kriterien die die Cloud-Architektur eines Anbieters erfüllen muss. Dimension Data übernimmt und erfüllt für die sichere Datenaustauschlösung Secure Data Space die Anforderungen an ein sicheres Rechenzentrum.

Neben der sicheren Datenverschlüsselung ist aber auch der Ort, an dem die Daten vorgehalten werden, von erheblicher Bedeutung. So votiert beispielsweise eine klare Mehrheit der deutschen Unternehmen für einen Cloudanbieter aus dem Rechtsgebiet der EU, um so den Zugriff außereuropäischer Staaten auf ihre Daten zu unterbinden. Rechenzentren in Deutschland sollten beispielsweise nach der ISO/IEC-Norm 27001 zertifiziert sein, die ein umfassendes Informationssicherheits-Managementsystem gewährleistet.

2 Management und Rechteverwaltung

Idealerweise lassen sich über den Cloudspeicher die Organisationsstrukturen der Hochschule abbilden. Erreicht wird dies über eine mehrstufige Rechteverwaltung für Benutzer und Data Rooms. Hierdurch kann präzise gesteuert und genau festgelegt werden, welche Rechte die jeweiligen Benutzer in den einzelnen Data Rooms besitzen. So lassen sich etwa gestufte

Hierarchien für die Hochschulleitung, die Verwaltungseinrichtungen, das Rechenzentrum, die einzelnen Lehrstühle und Institute sowie die Studierenden einrichten.

Im Rahmen der zentralen Verwaltung kann der verantwortliche Systemadministrator über eine Zwischenrolle (Data-Room-Admins) Rechte zur Selbstverwaltung an die einzelnen Abteilungen und Fachbereiche der Hochschule vergeben, so dass er beispielsweise die Neuanlage von Daten-Räumen delegieren kann und gerade nicht alles in persona durchführen muss. Gleichwohl behält er die erforderliche Kontrolle über das vollständige System und kann regulierend eingreifen.

Mit der Verschlüsselung einzelner Data Rooms für sensible Daten können die Rechte aber so vergeben werden, dass beispielsweise selbst der Data-Room-Admin keine Einsicht in die Dateien hat. Damit bleibt ihm partiell der Zugang zu vertraulichen und besonders geschützten Informationen bzw. Unterlagen verwehrt, die Aufsicht bzw. Kontrolle über alle Nutzungsrechte behält also die Hochschule.

Diese fein differenzierende Regelung ist anwenderfreundlich und trägt den bei einer komplexen Verwaltungseinheit wie einer Hochschule bestehenden Anforderungen an die unterschiedlichen Zuständigkeiten und Verantwortungsbereiche Rechnung.

ROLLEN**KONZEPT**	**DATA SPACE ADMIN** Zentrale Adminfunktion	**DATA ROOM ADMIN** Admin für Data Room	**DATA ROOM USER** Typischer Benutzer	**LINK EMPFÄNGER** Temporärer User
Festlegung globaler Systemeinstellungen	+	–	–	–
Globale Benutzerverwaltung	+	–	–	–
Anlegen von neuen Data Rooms und Zuweisung von Data Room Admins	+	–	–	–
Rechteverwaltung innerhalb der Data Rooms	–	+	–	–
Benutzerverwaltung innderhalb der Data Rooms	–	+	–	–
Verschlüsselung von Data Rooms	–	+	–	–
Hochladen, Löschen und Versenden von Dateien	+	+	+	–
Nutzen von Down- und Uploadlinks	+	+	+	+

Abbildung 2: Rollenkonzept

3 Integration und Handling

Neben der Datensicherheit und dem Management bzw. der Rechteverwaltung sind aber auch die Integration der Cloudspeicher-Lösung in das bestehende System und das Handling im Alltag für die Benutzer von entscheidender Bedeutung.

3.1 Aus Sicht der Administration/IT

Einbindung mehrerer Standorte

Eine hochschulweite Cloudplattform für die Datenspeicherung und den Informationsaustausch unter Hochschulmitarbeitern, Studierenden sowie externen Partnern bietet viele Vorteile. Sie ist eine Alternative zum ungeschützten Datenversand per E-Mail und löst zudem FTP-Server und den häufig vorhandenen Wildwuchs an Einzellösungen ab. Somit ermöglicht sie den Administratoren ein umfassendes Management der Daten sowie deren Sicherheit und erlaubt es,

auch verschiedene Standorte einzubinden. Bei einer Campus-Universität sind etwa die einzelnen Institute, Fakultäten und Serviceeinrichtungen in räumlicher Nähe zueinander untergebracht, sollen aber fachbereichsübergreifend in die Lösung integriert werden. Gleiches gilt für universitäre Einrichtungen, die beispielsweise auf einzelne Gebäude einer Großstadt verteilt sind. Diese Einbindung erfolgt effizient und schnell und belastet die Administratoren nicht zusätzlich.

Active Directory Einbindung

Zudem ist es natürlich möglich, das Active Directory des Microsoft Windows Servers in die Cloudlösung einzubinden. Auf diese Weise kann der Administrator die Benutzerverwaltung wesentlich vereinfachen.

Verschlüsselung

Wie bereits erwähnt liegt die Besonderheit der Collaboration-Lösung Secure Data Space in der einzigartigen Triple-Crypt® Technology. Mit der Triple-Crypt® Technology findet eine dreifache Verschlüsselung sensibler Daten in allen wichtigen Instanzen statt: direkt am Endgerät des Benutzers (Local Encryption), während der Datenübertragung (Channel Encryption) sowie im Cloudspeicher (Server-Side Encryption). Auf diese Weise hat selbst der Dienstleister, der die Daten hostet, keinen Zugriff auf die rundum geschützten Inhalte. Dabei kommt es zu keinen Performanceverlusten, die Arbeit wird also weder verlangsamt noch verkompliziert. Unter dem Schutz dieser komplexen Verschlüsselung behält eine Hochschule die vollständige Kontrolle über ihre Daten und erhält gleichzeitig die Möglichkeit, Teamfunktionen einschließlich Benutzer- und Rechteverwaltung zu nutzen.

Skalierung

Da die Anzahl der Beschäftigen und Studierenden einer Hochschule einem stetigen Wandel unterliegt, sollte sich der Datenspeicher flexibel an die jeweils aktuelle Situation anpassen können. Es ist vorteilhaft, wenn auch der Speicherplatz und die Benutzeranzahl dynamisch mitwachsen können. Idealerweise kann eine Hochschule die erforderlichen Benutzer wie auch das Speichervolumen einfach und rasch hinzu- oder abbuchen. Das bietet den Vorteil, mit einer kleineren Lösung beginnen und das System hinsichtlich der aktuellen Anforderungen exakt skalieren zu können.

Abrechnungssystem/Lizenzierung

Für die verlässliche Budgetplanung einer Hochschule ist ein überschaubares und transparentes Kostenmodell unabdingbar. Der Cloudspeicher-Dienst sollte ein attraktives und variables Lizenzmodell sein, welches monatliche Änderungen bei der Stückzahl und dem Speicherplatz ermöglicht, ohne aber versteckte Kosten für eventuelle zusätzliche Funktionen zu enthalten. So kann eine Hochschule der unvermeidlichen semesterabhängigen Fluktuation von Personal und Studierenden begegnen und zugleich den internen Anforderungen an Kosteneffizienz genügen.

3.2 Aus Sicht der Anwender

Personifizierter Login

Den Anwendern steht beim Einsatz des Cloudspeicher-dienstes ein personifizierter Login zur Verfügung. Damit ist sichergestellt, dass sich keine andere Person auf dem Account einloggen kann und die Kontrolle über die persönlichen Daten ausschließlich beim berechtigten Anwender bleibt.

Zugriff über Browser, Software und App

Der Zugriff auf den Secure Data Space ist auf vielfältige Weise möglich, etwa über den Webbrowser, Software oder Apps. Damit gestaltet sich die Benutzung zeitgemäß und komfortabel. Hochschulmitarbeiter und Studierende können ihre vorhandenen Endgeräte einbringen und mit Notebooks, Tablets oder Smartphones auf die im Cloudspeicher zur Verfügung gestellten Dokumente zugreifen. So bleibt auch genug Raum für die Individualität und Vorlieben der User. Insbesondere aufgrund der zunehmenden Mobilität im Alltag sollte die Option bestehen, auch über Apps für unterschiedliche Betriebssysteme (iOS, Android, etc.) mittels mobiler Endgeräte auf die Daten in der Cloud zugreifen zu können. Die Option für eine Integration mit gängigen E-Mail-Systemen wie MS Outlook ist für den universitären Arbeitsalltag ebenfalls empfehlenswert. So wird die E-Mail Struktur entlastet, der Versand von Dateien wird protokolliert, und der Schutz von Dateianhängen wird durch einen verschlüsselten Austausch gewährleistet.

Daneben liegt ein großer Vorteil des Secure Data Space gerade darin, dass jeder Anwender stets Zugriff auf den aktuellsten Stand der Dokumente erhält. Hierbei kommt es darauf an, die Benutzerrechte flexibel handhaben zu können. Man denke dabei beispielsweise nur an wissenschaftliche Forschungen von Professoren und Habilitanden, Projektarbeiten von Doktoranden oder auch Kooperationen im Rahmen von studentischen Referaten in der Hochschullehre. Doch auch in der Hochschulverwaltung gibt es viele Referate und Teams, die auf eine schnelle und vertrauensvolle Zusammenarbeit angewiesen sind. Für all diese Menschen ist es wichtig, dass die Zugriffsrechte auf die Dokumente in den einzelnen Daten-Räumen variabel sind.

Zudem ist die Kapazität bei der Datenübermittlung auf konventionellen Wegen begrenzt. Oftmals überschreitet das umfangreiche Datenmaterial die Größe der erlaubten Anhänge im Exchange-Server oder kann erst gar nicht versandt werden, weil ein bestimmter Dateityp (z.B.*.exe) blockiert wird. Die bisher genutzten Möglichkeiten von FTP stoßen an die Grenzen der Bedienbarkeit und Sicherheit. Dagegen ist der Cloudspeicher die sinnvolle Lösung für den Datenaustausch, die sowohl effizient verwaltet werden kann als auch den zwingend erforderlichen hohen Sicherheitsanforderungen genügt.

Einbindung als virtuelles Laufwerk auf den Clients

Selbst die Einbindung der Cloudspeicher-Lösung als virtuelles Laufwerk auf den Clients ist vorgesehen. Dies ermöglicht es auch weniger technikaffinen Anwendern, sich ohne Auseinandersetzung mit neuer komplizierter Technik auf einfache Weise zu orientieren und so zu arbeiten, wie sie es bislang vom heimischen PC bzw. Mac aus gewohnt sind. So kommt jeder schnell und problemlos an die hinterlegten Unterlagen, von den Materialien aus Vorlesungen und Seminaren bis hin zu Verwaltungsmitteilungen oder Rundschreiben des Hochschulpräsidenten oder Kanzlers. Dieser Aspekt sollte nicht unterschätzt werden und führt dazu, dass die Integration in bestehende Hochschulprozesse und vorhandenen Clients unkompliziert verläuft.

Web/Client Synchronisation

Die Synchronisation mit dem Web Server über einen Client, der auf dem PC oder Notebook installiert werden kann, ist selbstverständlich auch sichergestellt damit die Daten mit dem Web synchronisiert werden.

Up- und Download-Funktionalitäten

Der Secure Data Space stellt für die Hochschule eine einheitliche, übersichtliche und aktuelle Datenhaltung sicher. In der Praxis wird der hochsichere Dateiaustausch durch Down- und Uploadlinks/Quicklinks gewährleistet, die optional passwortgeschützt und zeitlich limitiert sind.

Das Hochschulmitglied stellt beispielsweise einen Uploadlink bereit und übermittelt diesen automatisiert per E-Mail an den Empfänger. Dieser erhält eine E-Mail und kann die Datei hochladen. Das Passwort wird dem Empfänger je nach Sicherheitslevel über einen Zweitweg, z. B. durch eine weitere E-Mail, am Telefon oder als SMS mitgeteilt. Wenn der Up- bzw. Download von der Zielperson durchgeführt wurde, erhält das Hochschulmitglied umgehend eine Nachricht. So ermöglicht der Secure Data Space eine effiziente Arbeitsweise unter Einhaltung höchster Sicherheitsstandards. Dies ist besonders wichtig bei streng vertraulichen Daten, etwa Forschungsergebnissen oder sensiblen Hochschulinterna, die noch unter Verschluss gehalten werden und nicht Datendieben in die Hände fallen sollen. Auf diese Weise lassen sich beispielsweise Forschungsarbeiten, interdisziplinäre Kooperationen oder auch der Austausch mit anderen Hochschulen sicher gestalten.

Sichere Kollaboration im Konzern und über seine Grenzen hinweg

Matthias Jürgens
Emerging Technologies
Deutsche Telekom / P&I
Andreasstr 10
10243 Berlin
matthias.juergens@telekom.de

Abstract: Der Anspruch an einen modernen Arbeitsplatz ist, effizient Daten mit Mitarbeitern zu teilen, sie gemeinsam zu bearbeiten und deren Ergebnisse im Unternehmen aber auch über seine Grenzen hinweg auszutauschen. Der Austausch soll einfach sein und per se mit jedem Menschen weltweit, aber auch mit jedem Gerät funktionieren, ohne hohe Investitionen zu erfordern.

Nicht zuletzt variiert die Anforderung an den Speicherort der Daten von einem public-cloud Ansatz, bis hin zu einer Installation einer Lösung in einer eigenen Lokation mit spezifischer Hardware.

Der Anspruch an die Sicherheit der Daten eint die Anforderungsprofile. Auf der Suche nach einer umfassenden und zugleich leicht zu bedienenden Lösung, setzt die Deutsche Telekom auf das Produkt Sync & Share.

Die Ausgangslage

Mitarbeitern der Deutschen Telekom stehen verschiedene Datenspeicher an ihrem Arbeitsplatz zur Verfügung. Im Wesentlichen werden die Daten auf konventionellen Fileservern gespeichert.

Die Verzeichnisse sind entweder persönlich zugeordneter Speicher oder es handelt sich um Team oder Projektbezogene Ablagen. Erreichbar sind die Fileserver für Mitarbeiter aus dem VPN heraus.

Mitarbeiter können weder Verzeichnisse Teilen, noch geteilte Verzeichnisse erweitern oder die Anzahl der Mitglieder verringern, ohne den Support zu bemühen.

Kollaboration im Konzern

Um Daten zu teilen werden Dokumente in geteilte Verzeichnisse kopiert, wobei die Datenmenge jeweils um die Dateigröße vermehrt wird.

Ein Zugriff für nicht Telekom Mitarbeiter auf diese Speicher ist ausgeschlossen. Sicherheit wird durch Zugriffsschutz gewährleistet.

Weitere Austauschmöglichkeiten, wie Box® oder Evernote® sind aus Sicherheitsgründen nicht gestattet.

Diese Struktur ermöglicht somit keinerlei Kollaboration mit Partnern oder Kunden. Der De-Facto Kollaborations Standard der Deutschen Telekom heißt „Mail“. Eine echte Kollaboration ist somit ausgeschlossen.

Auch intern wird im Regelfall das Versenden von Dokumenten per Mail und nicht auf Datenspeicherebene vorgenommen.

Die Aufgabe: sichere Kollaboration auf beliebiger Infrastruktur

Die Aufgabenstellung lautete für die Deutsche Telekom, ein Produkt zu finden, welches sich so einfach bedienen lässt, wie Dropbox® und gleichzeitig auf allen Endgeräten, Mobile wie Desktop lauffähig ist. Das Produkt soll es dem User ermöglichen, schnell und flexibel Datenräume für Projektgruppen zum Austausch von Dokumenten einzurichten. Gleichzeitig sollen zentrale Speicher global administriert, Dokumente für alle Mitarbeiter vorhalten, ohne dass diese Dokumente mehrfach abgelegt werden müssen.

Das Produkt muss eine solide Ende zu Ende Verschlüsselung aufweisen, deren Sicherheit von unabhängiger Stelle bestätigt wird. Idealerweise hat sich das Produkt bereits im Markt bewährt und verfügt über Kundenzahlen, die denen der Mitarbeiter der Deutschen Telekom wenigstens entsprechen.

Der Speicher sowie das Backend des Systems soll sowohl auf konventionell aufgesetzten RZ Lokationen mit filebasierten Speichern lauffähig sein, als auch in Clouds mit S3 Speicherprotokollen.

Nicht zuletzt hat die Aufgabenstellung ein Cost-Saving Ziel gegenüber den derzeit eingesetzten Systemen.

Die Lösung

Das evaluierte Produkt trägt den Namen „Sync&Share“ und ist eine Weiterentwicklung der Teamdrive® Lösung. Das Frontend wird gegen eine komplett neu entwickelte GUI ausgetauscht, die dem Nutzer eine Interaktion, ähnlich der Lösung bekannter amerikanischer Produkte ermöglicht.

Sync&Share erfüllt alle oben genannten Anforderungen und reduziert die Kosten signifikant durch den Einsatz kostengünstigerer Hardware Speicher gegenüber der gegenwärtig eingesetzten Produkte. Zudem schafft es ein deutliches Plus an Sicherheit durch das Verdrängen unsicherer Produkte aus dem Konzern. Nicht zuletzt ist auch Mail nicht mehr das notwendige Mittel zum Datenaustausch, was ebenfalls der Sicherheit dient. Der Gewinn an Produktivität ist derzeit noch nicht quantifizierbar, ließ sich aber in ersten Pilotstudien deutlich erkennen.

Online-Ressourcen zur Tagung

Die Vortragsfolien wurden in einem ownCloud-Share abgelegt und sind zu finden unter der URL:

http://www.tubit.tu-berlin.de/cloudevent/menue/slides/

Hierbei handelt es sich um eine Weiterleitung, alternativ können Sie auch die URL des Shares direkt verwenden:

https://owncloud.tu-berlin.de/public.php?service=files&t=f82c4a5c9898af00dcbf41edde109914

Zum Betrachten benötigen Sie den Adobe-Acrobat-Reader, zu finden unter *http://get.adobe.com/de/reader/*.

Eine Mailingliste zur Weiterführung des Informationsaustausches wurde im Anschluss an die Tagung eingerichtet und ist unter *cloud.o.mat@tubit.tu-berlin.de* zu erreichen.

Veranstalter:

Prof. Dr. Odej Kao,
Dr. Thomas Hildmann
Email: *thomas.hildmann@tu-berlin.de*

Organisation:

Michaela Müller-Klang
Tel: +49 30 314 29836
Email: *michaela.mueller-klang@tu-berlin.de*

Thomas Gebhardt
Tel.: +49 30 314 27605
Email: *thomas.gebhardt.1@tu-berlin.de*

Kontakt:
tubIT, IT-Service-Center TU Berlin
Sekr. EN 50
Einsteinufer 17, 10587 Berlin
Tel.: +49 30 – 314 29836
Fax: +49 30 – 314 21060

Universitätsverlag der TU Berlin

Cloudspeicher im Hochschuleinsatz

Proceedings der Tagung „Cloudspeicher im Hochschuleinsatz“ am 05. und 06. Mai 2014 am IT-Service-Center (tubIT) der Technischen Universität Berlin

Die Konzeption und der praktische Einsatz von Cloudspeichersystemen im Hochschulumfeld sind Gegenstand einer hochaktuellen Diskussion mit vielfältigen Aspekten wie z. B. Datensicherheit und Datenschutz, Skalierung oder Föderation. Die verschiedenen Hochschulen sind in sehr unterschiedlichen Phasen in Bezug auf die Einführung dieser Dienste. Während einige wenige Hochschulen bereits seit Monaten oder Jahren einen solchen Dienst betreiben, ist man an anderen Hochschulen noch in einer Test- oder Implementierungsphase oder befindet sich noch im Auswahl- bzw. Ausschreibungsprozess. Dieser Band versammelt die Beiträge der Tagung „Cloudspeicher im Hochschuleinsatz“, die im Mai 2014 an der TU Berlin stattfand.

ISBN 978-3-7983-2697-2 (print)
ISBN 978-3-7983-2698-9 (online)

ISBN 978-3-7983-2697-2

www.univerlag.tu-berlin.de