Identitätsmanagement für Hybrid-Cloud-Umgebungen an Hochschulen – Erfahrungen im Münchner Wissenschaftsnetz

Silvia Knittl
Technische Universität München
knittl@tum.de

Wolfgang Hommel
Leibniz-Rechenzentrum
hommel@lrz.de

Abstract: Hybrid-Cloud ist die aktuell gängige Bezeichnung für den Mischbetrieb von lokalen und externen IT-Diensten, die auf Basis einer Kombination aus physischer und virtueller Hardware erbracht werden. Die aktuellen Entwicklungen im Cloud-Computing bringen eine Reihe interessanter Management- und Administrationswerkzeuge hervor, deren Einsatz auch für Hochschulen und deren Rechenzentren attraktiv ist, selbst wenn dort nicht jeder neue Hype mit offenen Armen empfangen wird. Die neuen Formen der Diensterbringung, die sich dank der neuen Werkzeuge inzwischen auch effizient in die Praxis umsetzen lassen, bringen aber auch eine Vielzahl neuer Herausforderungen mit sich, die sich wiederum auf die bereits vorhandene IT-Infrastruktur auswirken. In diesem Beitrag beleuchten wir das Zusammenspiel zwischen Hybrid-Cloud-Umgebungen und dem Identity & Access Management, also einer der tragenden Säulen des organisationsweiten Sicherheitsmanagements, im Hochschulumfeld auf Basis unserer praktischen Erfahrungen im Münchner Wissenschaftsnetz.

1 Motivation

Wie in privatwirtschaftlichen Unternehmen hat der Betrieb von IT-Systemen auch in Hochschulumgebungen – von Forschungsvorhaben zunächst abgesehen – keinen Selbstzweck, sondern dient der gezielten Unterstützung der Geschäfts- bzw. Hochschulprozesse. Heute könnte keine Hochschule ihren Aufgaben in einer für Mitarbeiter und Studierende attraktiven Weise mehr nachkommen, ohne Anwendungen, wie etwa Personal- und Studentenverwaltungssoftware, E-Mail, Web- und Fileserver, einzusetzen. Anders als in den meisten Unternehmen erfolgt der IT-Betrieb bislang aber nicht stark organisationsintern zentralisiert bzw. mit einer zentralisierten Koordination möglicher Outsourcing-Bereiche. Vielmehr stellt eine Verteilung der IT-Ressourcen, beispielsweise zwar mit einem Schwerpunkt im Hochschulrechenzentrum, aber mit deutlich erkennbaren Mengen ergänzender Systeme in der Hochschulverwaltung und den einzelnen Fakultäten und Fachbereichen, ein nach wie vor gängiges Bild vieler deutscher Hochschulen dar.

Ein Wandel dieser Form des IT-Betriebs wird dabei einerseits durch Rezentralisierungsbemühungen angestrebt, der den in den 1990er Jahren vorherrschenden IT-Dezentralisierungsdrang eindämmen, Wildwuchs verhindern, Kompetenzen bündeln und die Gesamtkosten beim Betrieb der Hochschul-IT-Infrastruktur reduzieren soll, aber aufgrund

befürchteter resultierender Einschränkungen für Forschung und Lehre oft auch auf Widerstand stößt. Andererseits ändern sich durch die natürliche Fluktuation an Hochschulen und die massiv zunehmende Anzahl so genannter *Digital Natives* auch die Anforderungen an die IT-Dienste an einer Hochschule, da Personen, die mit IT-Systemen und IT-Diensten aufgewachsen sind und sich auch privat intensiv damit auseinandersetzen, ein offenkundig meist grundlegend anderes Verständnis von IT mitbringen als beispielsweise die Angehörigen geisteswissenschaftlicher Fachrichtungen vor 20 Jahren. Gerade diese Zielgruppe, die im weitesten Sinne als Cloud-Services bezeichenbare IT-Dienste aus ihrem privaten Umfeld kennt, wünscht sich auch an der Hochschule vergleichbare Dienstleistungen und stellt dabei die klassische Prämisse, möglichst viel Hardware im eigenen Bürotrakt unterzubringen, in den Hintergrund [BDNP10].

Die Beurteilung von Cloud-Computing an deutschen Hochschulen gestaltet sich schwierig: Während sich insbesondere Informatik und Wirtschaftswissenschaften durchaus überwiegend euphorisch mit dem neuen Forschungsgebiet auseinandersetzen und beispielsweise seine ökonomischen, betrieblichen und sicherheitsspezifischen Aspekte durchleuchten, sehen andere darin alten Wein in neuen Schläuchen oder einen durch die Marketingabteilungen von Herstellern hochgehaltenen Hype und fragen sich, wo der Unterschied zum in der Wissenschaft längst etablierten Grid Computing oder konkrete Anwendungsfälle an Hochschulen liegen sollen (vgl. [FZRL09]). Allen Begriffsunklarheiten und Definitionsversuchen, die das Cloud-Computing immer noch prägen, zum Trotz zeigen sich jedoch zwei Eigenschaften, die auch für Hochschulen interessant sind: Zum einen kommt dem Einsatz von System- und Netzvirtualisierungstechniken eine tragende Rolle zu, die unabhängig vom Cloud-Hype verstärkt in den letzten 3–5 Jahren auch in Hochschulrechenzentren Einzug gehalten haben. Zum anderen bietet Cloud-Computing mit der Kategorisierung in Infrastructure, Platform und Software as a Service (IaaS, PaaS und SaaS) eine auch auf klassische Hochschul-IT-Dienste anwendbare Strukturierung, deren praktische Bedeutung mit der zunehmenden Verfügbarkeit entsprechender Management- und Administrationswerkzeuge zunimmt.

In diesem Beitrag betrachten wir das Cloud-Computing weder direkt noch in seinem vollen Umfang. Vielmehr konzentrieren wir uns nach einem kurzen Überblick über eine ausgewählte, sich im Produktivbetrieb befindende „Hochschul-Cloud“ auf so genannte *hybrid clouds*. Eine Hybrid-Cloud liegt nach aktueller allgemeiner Auffassung dann vor, wenn eine Kombination verschiedener Cloud-Modelle (public, private, community; häufig auf virtueller Hardware basierend) mit einer traditionellen IT-Umgebung (auf physischer Hardware basierend) vorliegt. Die Begriffe *public*, *private* und *community* beziehen sich hierbei auf die Betreibermodelle bzw. Eigentumsverhältnisse (siehe [MG09]). Durch eine geeignete Kombination sollen a) die Vorteile aller Varianten entsprechend zum Tragen kommen, b) mit zusätzlichen Cloud-Ressourcen Lastspitzen (z. B. zu Semesterbeginn) abgefedert werden und c) sanfte Migrationen bzw. schnelle Integrationsmöglichkeiten geboten werden (vgl. [KP10]). Neue technische Möglichkeiten bringen im Allgemeinen aber auch neue Risiken mit sich, und eine Hybrid-Cloud bildet in dieser Hinsicht leider keine Ausnahme (vgl. [ENI09]). Von den vielen, bislang meist noch nicht ausreichend erforschten und nur unzureichend praktisch gelösten IT-Security-Problemen, die mit dem Cloud-Computing einhergehen, konzentrieren wir uns bei den Hybrid-Clouds im Sinne eines den Daten-

schutz betonenden *Privacy-by-Design*-Ansatzes (vgl. [Cav10]) auf das Identity & Access Management (I&AM), wie es sich typischerweise zur Benutzer- und Berechtigungsverwaltung, beispielsweise mit LDAP-Servern und Konnektoren zu den Quellsystemen im Campus Management implementiert, an Hochschulen findet.

Als Beispiel ziehen wir dafür die Zusammenarbeit zwischen der Technischen Universität München (TUM) und dem Leibniz-Rechenzentrum (LRZ) im Münchner Wissenschaftsnetz (MWN) heran. Das LRZ ist der zentrale IT-Dienstleister aller Münchner Wissenschaftseinrichtungen (siehe [LRZ10]) und hat sein I&AM-System eng mit den entsprechenden Systemen insbesondere der Ludwig-Maximilians-Universität (LMU) und der TUM gekoppelt, um den Hochschulangehörigen einen möglichst benutzerfreundlichen Zugang zu den von ihnen benötigten IT-Diensten zu ermöglichen. Die im Rahmen des 2009 abgeschlossenen, DFG-geförderten Projekts IntegraTUM mit dem Ziel der Übertragbarkeit ihrer Bestandteile auf andere Hochschulen entwickelte I&AM-Infrastruktur [BEH+10] wird TUM-weit genutzt, regelt die Nutzung von LRZ-Diensten durch TUM-Angehörige und dient auch maßgeblich der Integration innerhalb der TUM neu aufgebauter IT-Dienste. Abbildung 1 zeigt einen vereinfachten Ausschnitt der IT-Dienstleistungslandschaft der TUM mit eigenen IT-Ressourcen in Kombination mit Diensten von public Cloud-Providern (Wikispaces in der Abbildung) und dem LRZ als IT-Dienstleister, wobei die einzelnen IT-Dienste den drei Kategorien IaaS, PaaS und SaaS zugeordnet sind. Die Motivation für und die Details dieser Zuordnung finden sich in unserer früheren Arbeit [KL10]; Ansätze zum hochschulspezifischen IT-Risikomanagement haben wir im Kontext des MWN in [KH10] vorgestellt.

Im nächsten Abschnitt erörtern wir anhand dieses Beispiels die Auswirkungen von Hybrid-Clouds auf Hochschul-I&AM-Systeme und schließen mit einer Zusammenfassung der Ergebnisse in Abschnitt 3.

2 Hochschul-Identity-Management und der Betrieb von Hybrid-Clouds

I&AM-Systeme lassen sich auch bei ihrem Einsatz an Hochschulen bezüglich ihrer Gesamtarchitektur in drei Bereiche untergliedern, die auch in Abbildung 2 am Beispiel von TUM und LRZ dargestellt sind:

- Autoritative Quellsysteme sind eng mit den Geschäftsprozessen verknüpft und liefern dem Kern des I&AM-Systems möglichst alle zu berücksichtigenden Benutzer. An Hochschulen stellen traditionell die Personal- und Studierendenverwaltungssysteme die wichtigsten Datenquellen dar und werden z. B. durch Gästeverwaltungsmechanismen (für Konferenzteilnehmer, Angebote für Schüler u. ähnl.) ergänzt. Die Betrachtung einzelner Datenquellen ist in den vergangenen Jahren dem Paradigma der Campus-Management-Systeme (CaMS) gewichen, die beispielsweise auch sicherstellen, dass ein Studierender, der gleichzeitig auch Mitarbeiter ist (z. B. als Hilfskraft oder im Rahmen eines Promotionsstudiengangs), nur einmal und nicht mehrfach als digitale Identität erfasst wird.

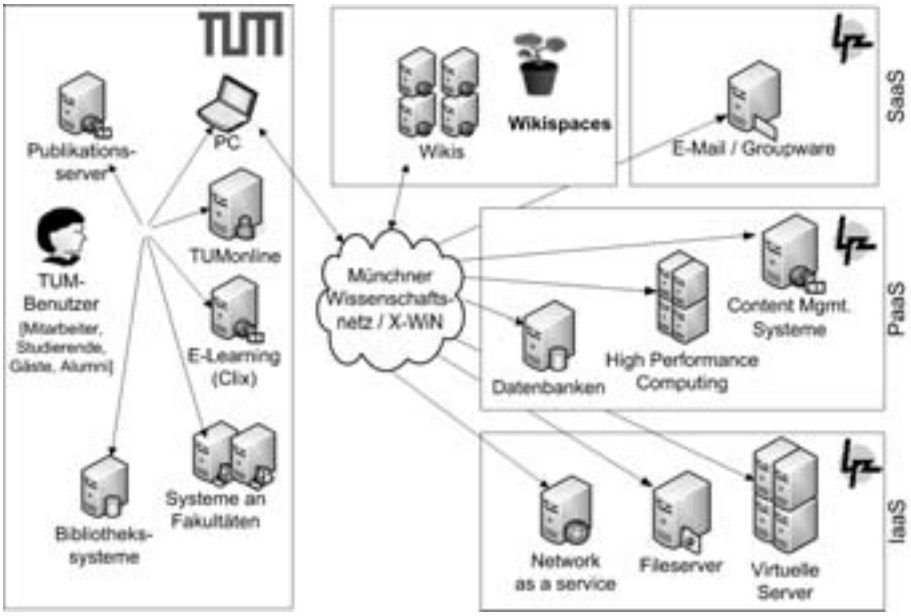

Abbildung 1: Die IT-Dienstlandschaft der TUM im Zusammenspiel mit dem LRZ

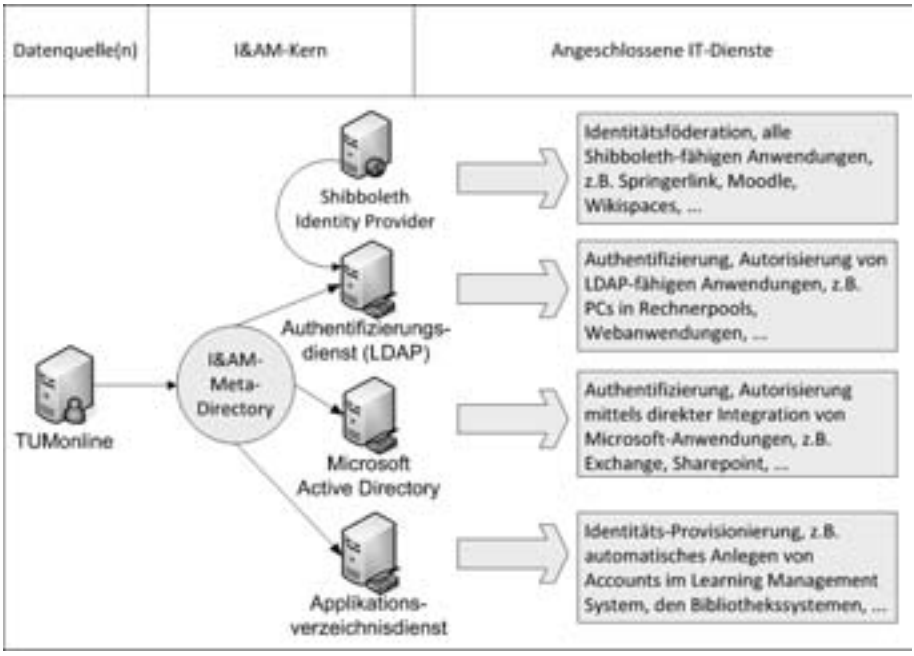

Abbildung 2: Die drei Bereiche Quellen, Kern und Dienste in I&AM-Architekturen

- Der Kern des I&AM-Systems besteht aus einem zentralen Datenbestand, der meist in Form von LDAP-Servern bereitgestellt wird, und auf diesem aufbauenden Funktionen, so dass beispielsweise aus der organisatorischen Zugehörigkeit eines Benutzers automatisch Default-Berechtigungen abgeleitet werden können. Die Grenzen zwischen den von CaMS und den von I&AM-Self-Service-Portalen erbrachten Möglichkeiten zur manuellen Steuerung individueller Berechtigungen sind derzeit fließend: Während beispielsweise das Ändern von Passwörtern durch Benutzer klassisch dem I&AM-System zuzuordnen ist, fungieren CaMS zunehmend als zentrale, webbasierte Schnittstelle auch zu den einzelnen Benutzern und reichen entsprechende Datenänderungen an das I&AM-System durch.
- Die einzelnen IT-Dienste und IT-Systeme nutzen das I&AM-System als technische Komponente zur Authentifizierung und Autorisierung ihrer Benutzer. Während LDAP-fähige IT-Dienste auf einen lokalen Benutzerdatenbestand ganz verzichten oder lediglich ergänzende Informationen lokal vorhalten müssen, werden die anderen IT-Dienste vom I&AM-System über so genannte Konnektoren mit allen relevanten Benutzerdaten versorgt; der entsprechende Vorgang wird als (User) Provisioning bezeichnet.

Für rein hochschulintern genutzte IT-Dienste ist das Thema Benutzerverwaltung mit einer Anbindung an das I&AM-System erledigt: Die Integration möglichst vieler Hochschul-IT-Dienste und der dafür pro IT-Dienst erforderliche Aufwand sind weit verbreitete (aber nicht die einzigen) Beurteilungskriterien für I&AM-Systeme. Sollen darüber hinaus auch Externe auf die IT-Dienste Zugriff erhalten, werden Mechanismen des Federated Identity Management angewandt, beispielsweise durch eine Integration in die Authentifizierungs- und Autorisierungsinfrastruktur des DFN-Vereins (DFN-AAI); in diesen Fällen steht, beispielsweise durch den Einsatz der Software Shibboleth, nicht mehr nur der lokale LDAP-Server zur Benutzerverwaltung zur Verfügung, sondern es können beispielsweise auch ausgewählte Daten externer Studierender von deren jeweiliger Heimathochschule abgefragt werden. Eine praktische Anwendung erfolgt beispielsweise bei Learning Management Systemen über das DFN-AAI E-Learning-Profil [DGH+08]: Studierende einer Hochschule können E-Learning-Kurse an anderen Hochschulen belegen und erhalten dafür auch Leistungsnachweise; dieser Prozess ist beispielsweise an der Virtuellen Hochschule Bayern (vhb) seit längerem in Betrieb und wird derzeit nach und nach in die DFN-AAI integriert.

Das Identity-Management an Hochschulen dient aber in den meisten Fällen vorrangig der Bewältigung eines Massenproblems: Viele Benutzer und zahlreiche angeschlossene Systeme müssen möglichst weitgehend automatisiert samt ihren Berechtigungen verwaltet werden. Während das I&AM-System also durchaus dem E-Mail-System gegenüber als autoritative Datenquelle bezüglich der E-Mail-Adressen der eigenen Benutzer fungiert und dem Learning Management System anhand von Informationen über den vom Studierenden belegten Studiengang liefert, um den Zugang zu ausgewählten Kursen freizuschalten, wurden systemadministrative Berechtigungen – beispielsweise, wer auf welchen Linux-Servern priviligierten Zugriff hat – bislang nur unzureichend in der Kette CaMS–I&AM–Dienst betrachtet. So genannte Privileged Account Management Systeme, die sich auf die Verwaltung solcher Kennungen mit weitrechenden Befugnissen und Maßnahmen gegen ihren

Missbrauch befassen, haben zwar längst einen festen Platz beispielsweise im militärischen Bereich und im Bankenwesen, dringen unter dem Einfluss internationaler gesetzlicher Auflagen u. a. in multinationale börsennotierte Unternehmen vor, spielten an Hochschulen aber bislang keine große Rolle, da die Anzahl der Administratoren überschaubar und der mutwillige Missbrauch damit einhergehender Berechtigungen selten war.

Mit dem Betrieb von Hybrid-Clouds geht nun jedoch einher, dass durch das einfache Bereitstellen virtueller Maschinen nicht nur die Gesamtzahl zu verwaltender Systeme insgesamt zunimmt, sondern sich auch die Anzahl mit erweiterten Berechtigungen auszustattender Benutzer erhöht. In Kombination mit der in der Praxis leidlich hohen Dynamik, die das einfache Hinzuschalten und Wegnehmen virtueller Maschinen ermöglicht, ist eine wie bislang übliche, manuelle Verwaltung von Administrator-Accounts nicht mehr sinnvoll. Beispielsweise plant das LRZ derzeit die Inbetriebnahme eines als VM-Shop bezeichneten Webportals, mit dem von Lehrstuhlinhabern berechtigte Hochschulmitarbeiter virtuelle Maschinen in einem vorab vereinbarten Maximalumfang online konfigurieren und weitestgehend automatisiert in Betrieb nehmen können. Mit der Abwicklung der Bestellung ist verbunden, dass der Anwender eine Reihe zusätzlicher Berechtigungen erhält: Neben den systemadministrativen Berechtigungen auf der neuen virtuellen Maschine muss er beispielsweise für die Nutzung der VMware-Managementwerkzeuge, die für das Ein- und Ausschalten der virtuellen Maschine benötigt werden und weitere Funktionen wie Snapshots zur Verfügung stellen, freigeschaltet werden, was aufgrund der Integration der VMware-Umgebung in die Microsoft-Windows-Umgebung entsprechende Berechtigungen im Active Directory voraussetzt (vgl. Abbildung 3). Somit ergeben sich bereits für relativ einfache Anwendungsfälle komplexe Abhängigkeiten, die das I&AM-System aufgrund der hohen Dynamik vollständig automatisieren muss, und deren Umsetzung mangels einfacher manueller Kontrollmethoden auch konsequent automatisch auf Konsistenz und mögliche Fehler (wie fälschlicherweise nicht wieder entzogene Berechtigungen) geprüft werden muss.

Die rein anwendungsfallgetriebene Erweiterung von Hochschul-I&AM-Systemen wie im Beispiel für die Bereitstellung kundenspezifischer virtueller Maschinen würde langfristig aber nicht skalieren, da für jeden neuen Typ von Cloud-Dienst, der angeboten werden soll, spezifische Erweiterungsarbeiten erforderlich wären. Auch im Hinblick auf die hochschulrechenzentrums-interne Umsetzung des Hybrid-Cloud-Ansatzes bietet sich deshalb eine Orientierung an den von der Cloud Security Alliance (CSA) im April 2010 veröffentlichten Leitlinien für das I&AM [Clo10] an. Dementsprechend sind vier funktionale Bereiche zu betrachen:

1. Provisioning und Deprovisioning digitaler Identitäten: Das bislang übliche reine Anlegen und Löschen neuer digitaler Identitäten in einem System, zu dessen Benutzung der Anwender berechtigt wurde bzw. dem die Berechtigung entzogen wurde, alleine reicht nicht mehr aus. Vielmehr untergliedert sich die Umsetzung einer Berechtigungsänderung in einzelne Schritte (von der CSA als *multi-stage setup* bezeichnet), mit denen auch Einträge und Zuordnungen z. B. in den Managementsystemen vorgenommen werden. Dabei muss ggf. auch auf die richtige Reihenfolge geachtet werden, was bei vielen Implementierungen, die Provisioning-Aktivitäten hochgradig parallelisieren, zur Erforderlichkeit tiefer Eingriffe führen kann.

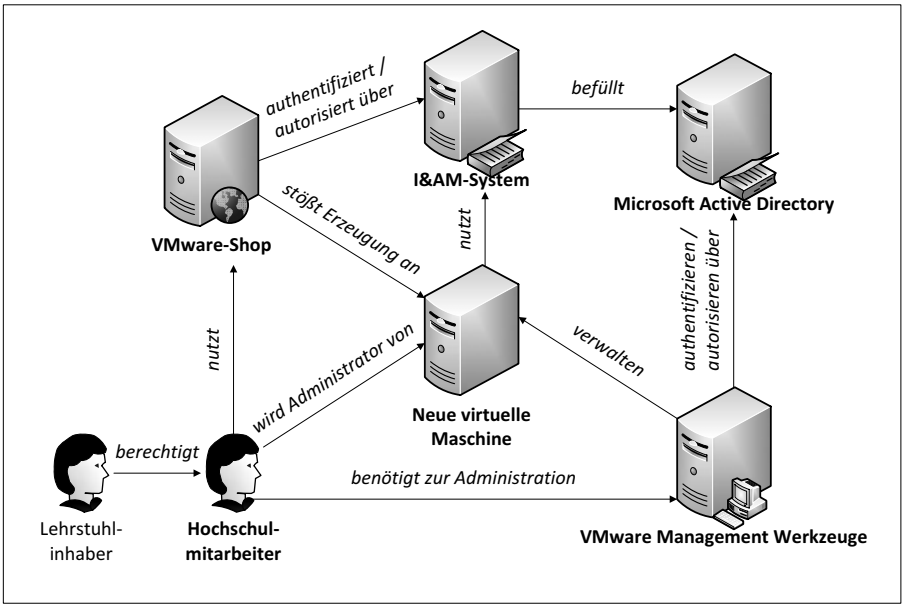

Abbildung 3: Abhängigkeiten bei der Bereitstellung virtueller Maschinen im MWN

2. Authentifizierung, Single Sign-On und Föderation: Für bereitgestellte Cloud-Services muss z. B. das Thema Passwort-Management überdacht werden; beispielsweise sollte vermieden werden, dass neue virtuelle Maschinen entweder alle dasselbe Startpasswort für den root-Account verwenden oder dass das benutzerspezifische Passwort daran gekoppelt wird (wie es bei vielen anderen Diensten üblich ist, damit der Benutzer ein gemeinsames Passwort für alle seine persönlichen Hochschul-IT-Dienste hat). Die dynamisch bereitgestellten Dienste sollten zudem bezüglich ihrer Benutzerverwaltung so vorkonfiguriert werden, dass sie vorhandene I&AM-Systeme bzw. Föderationsschnittstellen nutzen können, ohne dass ein lokaler Benutzerdatenbestand aufgebaut werden muss.

3. Zugriffskontrolle und Benutzerprofilmanagement: Mit dem Provisioning wird auch die Zugriffsüberwachung auf die Cloud-Ressourcen komplexer. Beispielsweise müssen auch Monitoringsysteme an die Managementwerkzeuge für virtuelle Maschinen gekoppelt werden, um entscheiden zu können, ob eine virtuelle Maschine ausgefallen ist oder vom Benutzer bewusst abgeschaltet wurde. Analog dazu können die Anwender von Cloud-Diensten anderen Anwendern selektiv Zugriff gewähren, um beispielsweise Mashups implementieren zu können, was über das I&AM-System und die Benutzerprofile geeignet abgebildet werden muss. Ebenso müssen Protokolle und Audit-Logs nicht mehr nur intern ausgewertet, sondern auch den entsprechenden Anwendern für ihren jeweiligen Bereich zur Verfügung gestellt werden.

4. Compliance: Gesetzliche Auflagen spielen nicht nur dann eine Rolle, wenn externe

Anbieter mit der Bereitstellung von Cloud-Ressourcen beauftragt werden, worauf wir hier nicht näher eingehen. Vielmehr müssen beispielsweise adäquate Maßnahmen zum Datenschutz auch und gerade dann umgesetzt werden, wenn neue Dienste dynamisch im Auftrag eines Benutzers instanziiert werden. Hierzu gehört einerseits, die unnötig breite Streuung personenbezogener Daten auf viele Systeme zu vermeiden, und zum anderen die Implementierung von Mechanismen, um anfallende personenbezogene Daten wie Zugriffsprotokolle und detaillierte Accountinginformationen innerhalb eines angemessenen Zeitraums auch wieder zu löschen.

Für die in Hochschul-I&AM-Systemen typischerweise enthaltenen Komponenten ergeben sich somit folgende Auswirkungen:

- Konnektoren und Verzeichnisdienste mit dienstspezifischen Datenschemata: Die gezielte Versorgung einzelner IT-Dienste mit Benutzerdaten im von ihnen benötigten Format erfordert aufwendige Implementierungsarbeiten, z. B. zur Datentransformation zwischen dem I&AM-Format und anwendungsspezifischen Benutzerprofilformaten. Die Anbindung über Konnektoren eignet sich auch unabhängig von diesem Bereitstellungsaufwand nur für längerfristig betriebene, einzelne IT-Dienste. Für die Integration einer Vielzahl dynamisch bereitgestellter Dienste muss auf eine der anderen Varianten ausgewichen werden.

- LDAP-basierte Authentifizierungs- und Autorisierungsdienste: Durch ihre im allgemeinen hohe Performance bzw. Skalierbarkeit und die clientseitig einfache Konfiguration sind LDAP-Server auch für die Anbindung der dynamisch über Cloud-Methoden eingerichteten Dienste attraktiv. Sie eignen sich insbesondere für IT-Dienste, bei denen sich der an der Hochschule registrierte Benutzer explizit authentifizieren soll. Falls hingegen Eigenschaften wie Single Sign-On oder die Unterstützung externer Benutzer über Föderationen benötigt werden, sollte auf eine der beiden nachfolgenden Varianten gesetzt werden.

- Active-Directory-Integration: Zum zentralen Management von Windows-Servern und Desktop-PCs bzw. Notebooks mit Microsoft-Betriebssystem kommt an sehr vielen Hochschulen bereits ein Microsoft Active Directory zum Einsatz; es ist wie oben erläutert auch eine Voraussetzung für den Betrieb einer VMware-basierten Virtualisierungsinfrastruktur und bildet die Basis für diverse weitere Microsoft- und Windowsdienste wie Exchange und Sharepoint. Durch seine LDAP-Schnittstelle kann es jedoch auch für die Anbindung von Linux-Maschinen genutzt werden. Mit dem Einsatz von Active Directory ist u. a. mittels seiner Kerberos-Funktionalität die Möglichkeit zum Single Sign-On, also die Nutzung aller ins Active Directory integrierten Dienste ohne pro Dienst zu wiederholende Passworteingabe, gegeben. Sie bietet sich deshalb insbesondere zur nahtlosen Integration der mit den Cloud-Diensten assoziierten Managementwerkzeuge an.

- Shibboleth (oder andere Software zur Teilnahme an hochschulübergreifenden Föderationen): Die Anpassung noch nicht föderationsfähiger Software an Shibboleth ist nach wie vor mit einem nicht zu vernachlässigenden Einarbeitungsaufwand für

die Entwickler bzw. Administratoren verbunden. Allerdings steigt die Anzahl der auch im Hochschulumfeld populären Webanwendungen, die an Shibboleth angepasst wurden, weiterhin stetig an. Neben dem Single Sign-On wird mit dieser Variante auch die selektive und aus Anwendungssicht transparente Benutzung durch externe Anwender unterstützt. Da I&AM-seitig keine Anpassungen erforderlich werden, skaliert dieser Lösungsansatz auch, wenn eine Vielzahl neuer Dienste dynamisch mittels Cloud-Ressourcen aufgebaut wird.

Die sich für den Betrieb Cloud-basierter Dienste abzeichnende Abkehr von konnektorenbasiertem Provisioning und die verstärkte Integration in Active-Directory-Infrastrukturen erfordert somit ein partielles Umdenken und tiefere Eingriffe in die bereits implementierten I&AM-Systeme.

3 Zusammenfassung

In diesem Beitrag haben wir zunächst motiviert, dass es im Umfeld des Cloud-Computing durchaus Entwicklungen gibt, die auch für Hochschulen und deren Rechenzentren interessant sind. Hybrid-Clouds, die eigene IT-Dienste mit Cloud-Services gezielt miteinander kombinieren, eignen sich unter anderem dazu, die Vorteile beider Betriebsformen zu kombinieren, Lastspitzen abzufedern und Migrationsszenarien umzusetzen. Die Bereitstellung virtueller Maschinen, eine der grundlegenden Technologien des Cloud-Computings, ist für viele *Digital Natives* darüber hinaus schon zum Normalfall im privaten Umfeld geworden, so dass entsprechende Anforderungen auch an Hochschul-IT-Infrastrukturen laut werden.

Die neue Technologie hat aber auch Auswirkungen auf schon vorhandene Konzepte und Architekturen, beispielsweise auf das Identity & Access Management. Am Beispiel des Münchner Wissenschaftsnetzes haben wir aufgezeigt, mit welchen Zielsetzungen und Realisierungsoptionen I&AM-Systeme an Hochschulen in den letzten Jahren aufgebaut wurden und welche Änderungen erforderlich werden, um die Anforderungen, die sich aus dem Einsatz von Cloud-Technologien ergeben, erfüllen zu können. Dabei haben wir uns am I&AM-Leitfaden der Cloud Security Alliance orientiert und seine Konzepte auf die Hochschul-I&AM-Landschaft übertragen.

Diese Untersuchungen haben gezeigt, dass bei I&AM-Integrationskonzepten und den technischen Infrastrukturen zu ihrer Umsetzung tiefere Eingriffe erforderlich sind, um beispielsweise ein Privileged Account Management und gegenseitige Abhängigkeiten zwischen Berechtigungen adäquat berücksichtigen zu können. Während sich bereits an vielen Hochschulen begonnene Aktivitäten zur Anpassung von Diensten an Shibboleth auch im Kontext von Cloud-Diensten bezahlt machen, stoßen traditionelle I&AM-Konzepte wie der Einsatz von Konnektoren zum Provisioning bei der Cloud-Dynamik an ihre Grenzen.

Die Umsetzung der neuen Konzepte wird im Münchner Wissenschaftsnetz derzeit mit dem Aufbau eines VM-Shops erprobt, der autorisierten Hochschulmitarbeitern u. a. der LMU und TUM ermöglichen soll, schnell und weitestgehend automatisiert neue virtuelle Maschinen bereitzustellen, um auf dieser Basis eigene Hochschul-IT-Dienste anzubieten, die

nahtlos in die vorhandene I&AM-Infrastruktur und die Nutzung der DFN-AAI-Föderation integriert werden können.

Danksagung:
Die Autoren danken den Mitgliedern des Munich Network Management Teams (MNM-Team) für wertvolle Kommentare und Anregungen zu früheren Versionen dieses Beitrags. Das MNM-Team ist eine Forschungsgruppe der Ludwig-Maximilians-Universität, der Technischen Universität München, der Universität der Bundeswehr München und des Leibniz-Rechenzentrums der Bayerischen Akademie der Wissenschaften unter der Leitung von Prof. Dr. Dieter Kranzlmüller und Prof. Dr. Heinz-Gerd Hegering. Siehe `http://www.mnm-team.org/`.

Literatur

[BDNP10] Rob Bristow, Ted Dodds, Richard Northam und Leo Plugge. Cloud Computing and the Power to Choose. *EDUCAUSE Review*, 45(3), Mai/Juni 2010. Verfügbar online unter `http://net.educause.edu/ir/library/pdf/ERM1030.pdf`.

[BEH+10] Latifa Boursas, Ralf Ebner, Wolfgang Hommel, Silvia Knittl und Daniel Pluta. IntegraTUM Teilprojekt Verzeichnisdienst: Identity & Access Management als technisches Rückgrat der Hochschul-IuK-Infrastruktur. In Arndt Bode und Rolf Borgeest, Herausgeber, *Informationsmanagement in Hochschulen*. Springer Berlin Heidelberg, 2010.

[Cav10] Ann Cavoukian. Modelling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach. Verfügbar online unter `http://www.ipc.on.ca/images/Resources/pbd-NEC-cloud.pdf`, Mai 2010.

[Clo10] Cloud Security Alliance. Domain 12: Guidance for Identity & Access Management - V2.1. Verfügbar online, April 2010.

[DGH+08] Jörg Deutschmann, Peter Gietz, Wolfgang Hommel, Renate Schroeder, Jens Schwendel und Tobias Thelen. DFN-AAI E-Learning-Profil: Technische und organisatorische Voraussetzungen, Attribute für den Bereich E-Learning. `http://www.aai.dfn.de/der-dienst/attribute/`, 2008.

[ENI09] European Network and Information Security Agency ENISA. Cloud Computing - Benefits, risks and recommendations for information security. Verfügbar online unter http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment , Zugriff am 12.01.2010, November 2009.

[FZRL09] I. Foster, Y. Zhao, I. Raicu und S. Lu. Cloud Computing and Grid Computing 360-Degree Compared. *ArXiv e-prints*, 901, December 2009.

[KH10] Silvia Knittl und Wolfgang Hommel. Umgang mit Risiken für IT-Dienste im Hochschulumfeld am Beispiel des Münchner Wissenschaftsnetzes. In *INFORMATIK 2010, Band 2*, 2010.

[KL10] Silvia Knittl und Albert Lauchner. Hybrid-Cloud an der Technischen Universität München – Auswirkungen auf das IT-Management. In *INFORMATIK 2010, Band 1*, 2010.

[KP10] Silvia Knittl und Hans Pongratz. Application Integration Methods For Learning Managment Systems. In IADIS, Herausgeber, *International Conference e-Learning 2010*, Freiburg, Deutschland, Juli 2010.

[LRZ10] LRZ. Dienstleistungskatalog. Verfügbar online unter `http://www.lrz.de/wir/regelwerk/dienstleistungskatalog.pdf`, September 2010.

[MG09] Peter Mell und Tim Grance. The NIST Definition of Cloud Computing. Technical report, National Institute of Standards and Technology, Information Technology Laboratory, Juli 2009.