Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Bachelorarbeit

Martin Slowikowski

Analyse von Cloudstack-Lösungen auf Grundlage der Definition des NIST

Fakultät Technik und Informatik
Studiendepartment Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Martin Slowikowski

Analyse von Cloudstack-Lösungen auf Grundlage der Definition des NIST

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung

im Studiengang Bachelor of Science Technische Informatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr. Bernd Kahlbrandt
Zweitgutachter: Prof. Dr. Olaf Zukunft

Eingereicht am: 20. August 2013

Martin Slowikowski

Thema der Arbeit
Analyse von Cloudstack-Lösungen auf Grundlage der Definition des NIST

Stichworte
Cloud-Computing, Cloudstack, NIST, Citrix, VMware, IaaS, PaaS, SaaS, Private Cloud, Public Cloud, Community Cloud, Hybrid Cloud, Virtualisierung

Kurzzusammenfassung
Diese Arbeit vermittelt zunächst Grundlagen des Begriffs Cloud-Computing. Anschließend folgt eine Vorstellung konkreter Cloudstack-Produkte der Hersteller Citrix und VMware. Cloudstack bezeichnet hierbei integrierte Produkte zum Aufbau und Betrieb einer Cloud-Infrastruktur. Ein Teilaspekt der Grundlagen ist die Vorstellung der NIST-Definition für Cloud-Computing. Die Interpretation dieser Definition durch den Autor dient als Bewertungsgrundlage für die vorgestellten Produkte.

Abschließend erfolgt eine kritische Würdigung, inwieweit sich die Produkte der genannten Hersteller in die NIST-Definition einordnen lassen und inwieweit sich die Definition nach NIST als Bewertungsgrundlage nutzen lässt.

Martin Slowikowski

Title of the paper
Analysis of cloudstack solutions based on the definition of NIST

Keywords
Cloud computing, cloudstack, NIST, Citrix, VMware, IaaS, PaaS, SaaS, private cloud, public cloud, community cloud, hybrid cloud, virtualization

Abstract
First, this thesis provides fundamentals of the term cloud computing, followed by a presentation of concrete cloudstack products by the manufacturers Citrix and VMware. In doing so cloudstack is defined as integrated products for construction and operation of a cloud infrastructure. One aspect of the fundamentals is the presentation of the NIST definition of cloud computing. The author's interpretation of this definition serves as the basis of assessment for the featured products.

In conclusion, there is a critical appreciation about what extent the products of the manufacturers can be classified within the NIST definition. Furthermore how far this NIST definition can be used as basis of evaluation is also discussed.

Danksagungen

Ich möchte mich an dieser Stelle bei meinen Freunden bedanken, die mich während der Bearbeitungszeit dieser Bachelorarbeit unterstützt und motiviert haben. Ein großer Dank gilt dabei meinen unermüdlichen Korrekturlesern Tell Müller-Pettenpohl, Jan-Tristan Rudat und Familie König für ihr bemerkenswertes Engagement. Insbesondere auch bei Thassilo Nowacka möchte ich mich hier für die aufmunternden Gespräche und anregenden Diskussionen zu meinem Thema bedanken. Diese waren mir eine erhebliche Hilfe!

Ganz besonders bedanken möchte ich mich bei Prof. Dr. Bernd Kahlbrandt für die erstklassige Betreuung dieser Arbeit, seine Motivation und Unterstützung haben mir sehr geholfen, diese Arbeit erfolgreich zu gestalten. Prof. Dr. Olaf Zukunft danke ich für seine Bereitschaft, das Zweitgutachten zu erstellen.

Ein weiterer Dank geht an die Firma Silpion IT-Solutions GmbH für die Bereitstellung der Mittel und an Dr. Fred Hantelmann von der Firma Silpion IT-Solutions GmbH für die Hilfe bei der Themenwahl und Betreuung während der Bearbeitung.

Schließlich möchte ich meiner Familie meinen ergebenen Dank aussprechen, sie war nicht nur während dieser Bachelorarbeit, sondern im Laufe des gesamten Studiums stets für mich da und gab mir die nötige Zeit und emotionale Unterstützung, dieses Studium erfolgreich abzuschließen.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einführung

1.1 Motivation

Virtualisierung und Cloud-Computing sind heutzutage ein fester Bestandteil moderner IT-Infrastrukturen. Cloud-Computing besteht dabei aber weniger aus neuen Technologien, sondern ist vielmehr die Kombination und konsequente Weiterentwicklung bestehender Technologien. Auf diese Weise lassen sich neue IT-Services und Geschäftsmodelle ermöglichen, auf deren Basis Anbieter komplexe Leistungen aus Soft- und Hardware in Form eines abstrakten Dienstes bereitstellen. Bei solchen Diensten entzieht sich demnach der Aufbau und die genaue Funktionsweise der Ansicht des Anwenders. Dieser nutzt die angebotenen Dienste lediglich. Software, Datenspeicher, Rechenzeit oder auch daraus zusammengesetzte, komplexere Dienste lassen sich über definierte Schnittstellen abfordern. Dabei spielt es keine Rolle, auf welcher Zielhardware diese letztendlich ausgeführt werden.

Zur IDC[1]-Studie "*Cloud-Computing in Deutschland 2012 - Evolution der Revolution*" wurden 284 deutsche Unternehmen mit mehr als 100 Mitarbeitern bezüglich ihrer Einstellung und Aktivitäten in Bezug auf Cloud-Computing befragt. 83 Prozent der Unternehmen haben ihre Strategien in Richtung Cloud skizziert. 23 Prozent davon planen Cloud-Dienste in so vielen Bereichen wie möglich einzusetzen. 38 Prozent wollen in einigen Segmenten der hauseigenen IT Cloud-Dienste nutzen. Cloud-Computing durchdringt Unternehmen zunehmend stärker und ist in den Beschaffungsstrategien der Unternehmen ein wesentlicher Bestandteil. Laut IDC wird eine Mischung aus herkömmlicher IT-Infrastruktur in Kombination mit Public und Private Clouds die IT-Landschaften in Unternehmen bestimmen. [vgl. KZ12]

Der "*Cloud Monitor*" ist eine Studie des BITKOM[2] und der Wirtschaftsprüfungs- und Beratungsgesellschaft KPMG[3]. Diese Studie wird im Zeitraum von 2011 bis 2014 jährlich durchgeführt. Für das Jahr 2012 wurden insgesamt 436 Unternehmen in Deutschland mit mehr als 20 Mitarbeitern befragt. Ergeben hat die Studie, dass gut 37 Prozent der Unternehmen Cloud-Computing eingesetzt haben. Im Vergleich zur Studie im Jahr 2011 entspricht das einem

[1] IDC Deutschland: http://www.idc.de
[2] Branchenverband der deutschen Informations- und Telekommunikationsbranche: http://www.bitkom.org
[3] KPMG International Cooperative: http://www.kpmg.com

Wachstum von neun Prozent. Weitere 29 Prozent planten den Einsatz konkret oder diskutierten darüber. Für ein Drittel der Befragten kam Cloud-Computing nicht in Frage. Bei 65 Prozent der großen Unternehmen mit mehr als 2000 Mitarbeitern wurde Cloud-Computing bereits eingesetzt. Im Mittelstand mit 100 bis 1999 Mitarbeitern setzten Unternehmen zu 45 Prozent auf Cloud-Computing. Bei kleinen Unternehmen mit 20 bis 99 Angestellten wagten nur 25 Prozent den Schritt. Die Studie hat ergeben, dass immer mehr Unternehmen dem Thema Cloud-Computing aufgeschlossen gegenüber stehen, allerdings wächst die Anzahl der Skeptiker gleichermaßen. Der Fokus der Nutzung liegt dabei hauptsächlich auf Private-Cloud-Lösungen. Markttreibend sind dabei Eigenschaften wie schnelle Skalierbarkeit von IT-Leistungen, verringerter administrativer Aufwand und der einfache Zugriff auf geografisch verteilte Ressourcen. Größte Hemmnisse sind die Angst vor Datenverlust, Schwierigkeiten bei der Integration und Unsicherheiten im Hinblick auf rechtliche Bestimmungen. [vgl. BK13]

Diese Bachelorarbeit wurde im Hause der Firma Silpion IT-Solutions GmbH[4] in Hamburg angefertigt, wo der Autor dieser Arbeit in der Infrastrukturabteilung tätig ist. Informationen zum Firmenprofil finden sich im folgenden Abschnitt 1.2. Die Beweggründe für die Themenstellung dieser Arbeit finden sich daher im beruflichen Umfeld des Autors. Die wesentlichen Aufgabenfelder in der Infrastrukturabteilung, wie beispielsweise Virtualisierung, Netzwerke, Speicherlösungen, Cloud-Computing und Cloud-Applikationen, sind hier von besonderem persönlichen Interesse.

1.2 Firmenprofil der Silpion IT-Solutions GmbH

Die Silpion IT-Solutions GmbH hat sich auf zwei Geschäftsfelder spezialisiert: Softwareentwicklung und Infrastrukturmanagement. Für Lösungen kommen, je nach Bedarf und Eignung, kommerzielle Produkte, Open-Source-Produkte oder Eigenentwicklungen zum Einsatz. Zur Zeit beschäftigt Silpion 105 Festangestellte und ca. 35 Freelancer.

Die Softwareentwicklung umfasst sowohl gehobene Enterprise-Java-Anwendungen als auch die Erstellung von Content-Management-Systemen, Community-Plattformen oder E-Commerce-Systemen. Eine besondere Expertise ist im schnell wachsenden Bereich der mobilen Anwendungen (Apps für iPhones, Android-Smartphones oder auf Windows Mobile basierende Handys) erarbeitet worden. Die Softwareabteilung zeichnet aus, dass agile Methoden in der Softwareentwicklung (Scrum), sofern möglich und sinnvoll, zum Einsatz kommen. Weiterhin wird Kunden auch inhouse Scrum-Coaching angeboten.

Die IT-Infrastruktur ist das zweite Standbein der Firma Silpion. Entstanden aus dem Wunsch heraus, die Softwareentwicklung zu unterstützen und zu beschleunigen, sind diese beiden Bereiche eng miteinander verzahnt. Die Ausrichtung an den Kundenwünschen hat mit der

[4] Silpion IT-Solutions GmbH: http://www.silpion.de

Zeit zur Erweiterung des Leistungskataloges geführt. IT-Konzeption und Operations für Webanwendungen bilden bis heute allerdings den Schwerpunkt der Arbeit. Die Expertise reicht vom Storage über Virtualisierung von Ressourcen jeglicher Art bis hin zu Betriebssystemen, Netzwerken, Middleware, Web-Applikationen und Intranets. Die Infrastrukturabteilung arbeitet herstellerübergreifend und partnerschaftlich mit technologieführenden Unternehmen wie Microsoft, VMware, EMC, Cisco, Citrix und HP zusammen. [vgl. IS12a, IS12b]

1.3 Zielsetzung

Ziel dieser Arbeit ist die Prüfung, inwieweit sich Cloudstack-Produkte von Herstellern in die Definition für Cloud-Computing des National Institute of Standards and Technology (NIST)[5] einordnen lassen. In diesem Zusammenhang soll eine Untersuchung derzeit am Markt befindlicher Cloudstack-Produkte der Hersteller Citrix und VMware erfolgen. Die Wahl fällt auf diese beiden Hersteller wegen ihrer Positonierung am Markt für Cloud-Computing. Außerdem ist die Firma Silpion an diesen Herstellern besonders interessiert.

1.4 Aufbau der Arbeit

- **Kapitel** 1 beschreibt Motivation und Zielsetzung dieser Arbeit und enthält weiterhin das Firmenprofil der Silpion IT-Solutions GmbH.
- **Kapitel** 2 definiert zunächst allgemein den Begriff Cloud-Computing, anschließend folgt die Definition des NIST. Weiterhin vermittelt dieses Kapitel Basiswissen zum Thema Cloud-Computing, unter anderem die verschiedenen Cloud- und Servicemodelle sowie verschiedene weitere Aspekte des Cloud-Computings.
- **Kapitel** 3 stellt konkrete Cloudstack-Produkte der Hersteller Citrix und VMware vor.
- **Kapitel** 4 beinhaltet die Analyse und Ergebnisdarstellung zu den in Kapitel 3 vorgestellten Cloudstack-Produkten auf Grundlage der Interpretation der NIST-Definition durch den Autor.
- **Kapitel** 5 enthält eine kritische Würdigung der erzielten Ergebnisse sowie die Darstellung der noch offenen Punkte.

[5] National Institute of Standards and Technology: http://www.nist.gov

2 Grundlagen des Cloud-Computings

2.1 Allgemeine Definition von Cloud-Computing

Cloud-Computing bezieht sich auf die Bereitstellung von Anwendungen und Diensten über ein Netzwerk auf Basis virtualisierter Ressourcen. Es kann sich dabei um IT-Infrastruktur, Plattformen oder Anwendungen jedweder Art handeln. Darauf zugegriffen wird über gängige Internetprotokolle und Netzwerkstandards.

Cloud-Computing zeichnet sich durch die Idee aus, dass Ressourcen virtuell und geradezu unbegrenzt zur Verfügung stehen. Weiterhin bleiben die Details der physischen Systeme, auf denen die Anwendungen und Dienste laufen, vor dem Anwender verborgen. Dieser hat kein Wissen und keine Kontrolle über die Technologien, die sich hinter den konkreten Cloud-Lösungen verbergen.

Cloud-Computing umfasst einerseits die Anwendungen, welche als Dienst über das Internet angeboten werden, andererseits die erforderliche Hard- und Software, die in Rechenzentren zur Bereitstellung der Dienste notwendig ist. [vgl. Sos10, S. 3]

Angebote aus der Cloud sind nicht auf bestimmte Anwendungen beschränkt. Prinzipiell lässt sich jede Anwendung in einer Cloud-Umgebung ausführen oder mit einem Cloud-Dienst kombinieren. Die Einsatzgebiete für Cloud-Computing sind daher weit gefächert. Sie reichen von einmaligen und zeitlich begrenzten Bedürfnissen über das Bewerkstelligen von extremen Lastsituationen bis hin zum Management saisonaler Nachfrage-Effekte. Im Allgemeinen fällt darunter ebenfalls das Outsourcing von Funktionalitäten und Diensten an Dritte. Cloud-Computing kann dabei sowohl für Testzwecke als auch für produktive Umgebungen sinnvoll zum Einsatz kommen. [vgl. BKNT11, S. 117]

Cloud-Computing stellt einen echten Paradigmenwechsel in der Art und Weise dar, wie sich Systeme einsetzen lassen. Das große Ausmaß an Cloud-Computing-Systemen wurde unter anderem durch das Wachstum des Internets ermöglicht. Ebenfalls dazu beigetragen haben die wachsende Rechenleistung von Computern und eine großflächige Verfügbarkeit von hohen Bandbreiten. Cloud-Computing erfüllt den lang ersehnten Traum des Utility Computing

mit Pay-per-Usage-Konzept, hoher Skalierung sowie Elastizität und universell verfügbaren Systemen.

Unter Utility Computing versteht man Techniken und Geschäftsmodelle, bei denen ein Anbieter seinen Nutzern Ressourcen zur Verfügung stellt und diese nach Verbrauch abrechnet. Solche Ressourcen können beispielsweise Rechenleistung, Speicherkapazität oder Applikationen sein.

Beim Cloud-Computing können Anwender also mit wenigen Ressourcen beginnen und diese in kurzer Zeit rapide ausweiten. Aus diesem Grund ist Cloud-Computing revolutionär, selbst dann, wenn die zugrunde liegende Technologie nur evolutionär ist. [vgl. Sos10, S. 3, BIT09, S. 22]

Die Verwendung des Wortes "Wolke" nimmt Bezug auf die beiden wesentlichen Konzepte:

- **Abstraktion**: Cloud-Computing abstrahiert die Details der Implementierung des Systems von Anwendern und Entwicklern. Anwendungen laufen auf nicht näher spezifizierten physischen Systemen. Daten werden an Orten gespeichert, ohne genau zu wissen wo. Die Administration von Systemen wird an Dritte ausgelagert und der Zugriff durch Benutzer kann von überall erfolgen.

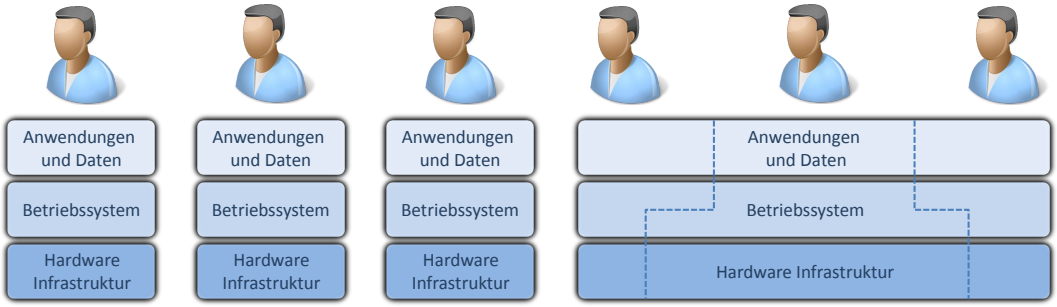
- **Virtualisierung**: Virtualisierung macht Cloud-Computing erst möglich. Dienstangebote sind unabhängig von der physischen Infrastruktur. Cloud-Computing virtualisiert Systeme durch Pooling und Aufteilen von Ressourcen. Rechenleistung und Speicherkapazität werden bei Bedarf von einer zentralisierten Infrastruktur bereitgestellt, die Kosten dafür nach tatsächlichem Verbrauch bemessen.

  Die Infrastruktur ist mandantenfähig (Multi-Tenant-Architektur) und Ressourcen sind, je nach Bedarf, in unterschiedlichem, veränderbarem Umfang anpassungsfähig. Abbildung 2.1.1 zeigt in (a) die Single-Tenant-Architektur, wo für jeden Anwender eine dedizierte Infrastruktur bereitgestellt wird. Bei der in (b) dargestellten Multi-Tenant-Architektur teilen sich verschiedene Anwender separiert voneinander eine gemeinsame Infrastruktur. [vgl. Sos10, S. 4]

Eine kurze, zusammenfassende Definition des Begriffs Cloud-Computing nach [BKNT11, S. 4]:

> *"Unter Ausnutzung virtualisierter Rechen- und Speicherressourcen und moderner Web-Technologien stellt Cloud-Computing skalierbare, netzwerk-zentrierte, abstrahierte IT-Infrastrukturen, Plattformen und Anwendungen als on-demand Dienste zur Verfügung. Die Abrechnung dieser Dienste erfolgt nutzungsabhängig."*

Um Cloud-Computing besser verstehen zu können, folgt eine Beschreibung der verschiedenen Bereitstellungs- und Servicemodelle in der Cloud. Bereitstellungsmodelle beschreiben,



(a) Single-Tenant-Architektur (b) Multi-Tenant-Architektur

Abbildung 2.1.1: Single- und Multi-Tenant-Architektur im Vergleich

wo sich die Cloud befindet und zu welchem Zweck. Die Unterscheidung liegt weniger in der technischen Umsetzung, als vielmehr in der Zugangsform und Einbettung in eine vorhandene Infrastruktur, z.B. in einem Unternehmen. Zu den Bereitstellungsmodellen zählen Public, Private, Hybrid und Community Clouds.

- **Public Cloud**: Sind Cloud-Dienste für jedermann öffentlich über das Internet zugänglich, spricht man von einer Public Cloud.
- **Private Cloud**: Stehen die Dienste nur einem ausgewählten Nutzerkreis zur Verfügung, z.B. nur Mitarbeitern eines bestimmten Unternehmens, handelt es sich um eine Private Cloud.
- **Hybrid Cloud**: Hybrid Clouds sind Kombinationen aus beiden vorhergehenden Ansätzen. Es werden verschiedene, eigenständige Cloud-Infrastrukturen über standardisierte Schnittstellen gemeinsam genutzt. Dabei lassen sich für bestimmte Funktionen zusätzlich öffentliche Dienste beziehen.
- **Community Cloud**: Bei Community Clouds wird die Infrastruktur von mehreren Einrichtungen gemeinsam genutzt. Betreiber ist einer dieser Einrichtungen oder ein Dritter.

Eine detaillierte Beschreibung dieser Cloudmodelle findet sich in Abschnitt 2.3.

Die Servicemodelle beschreiben die Art der Dienste, welche ein Dienstanbieter zur Verfügung stellt. Die bekanntesten Servicemodelle sind Software as a Service (SaaS), Platform as a Service (PaaS) und Infrastructure as a Service (IaaS), auch als das SPI-Modell des Cloud-Computings bezeichnet (siehe Abbildung 2.4.1). Die Servicemodelle bauen aufeinander auf

und definieren, was der Anbieter verwalten muss und welche Verantwortlichkeiten in den Bereich des Anwenders fallen.

- **Infrastructure as a Service**: IaaS bietet dem Anwender Infrastrukturdienste an, welche dieser über das Internet bezieht. Dies sind typische Ressourcen, wie z.B. Rechenleistung (in Form von virtuellen Maschinen (VMs)) und Speicherkapazität.
- **Platform as a Service**: Ein Anbieter stellt Anwendern eine Plattform mit standardisierten Schnittstellen zur Verfügung, die der Kunde nutzen kann. Der Anwender kann auf der Plattform eigene Anwendungen betreiben, ohne sich dabei um die zugrunde liegende Infrastruktur kümmern zu müssen. PaaS-Dienste bieten also die Möglichkeit, online Anwendungen zu entwickeln und diese beim Anbieter ausführen zu lassen.
- **Software as a Service**: Hierbei kommen Programme nicht mehr lokal auf dem eigenen Rechner zur Ausführung, sondern auf einem Server im Rechenzentrum des Anbieters. Der Nutzer greift dann beispielsweise über einen Webbrowser auf die Anwendung zu.

Neben diesen drei Hauptausprägungen existieren noch weitere Ausprägungen, die im Sinne des Everything as a Service (XaaS) entstanden sind. Dazu zählen beispielsweise Desktop as a Service und IT as a Service. Eine tiefergehende Beschreibung der Begriffe IaaS, PaaS sowie SaaS folgt im Abschnitt 2.4.

Aber nicht alle Anwendungen profitieren vom Einsatz in der Cloud. Probleme mit Latenzzeit, Transaktionskontrolle und vor allem Sicherheit und Verhaltensmaßregeln sind von besonderer Bedeutung. [vgl. Sos10, S. 3ff.]

2.2 Abgrenzung zu anderen Begrifflichkeiten

2.2.1 Klassisches IT-Outsourcing

Beim Outsourcing handelt es sich um die Auslagerung von Arbeits-, Produktions- oder Geschäftsprozessen eines Unternehmens zu einem externen Dienstleister. Beim IT-Outsourcing wird der Betrieb von Teilen oder gar der gesamten IT-Infrastruktur ausgelagert, meist über einen definierten Zeitraum. Oftmals wird die komplette gemietete Infrastruktur nur exklusiv durch einen Kunden genutzt (Single-Tenant-Architektur), selbst dann, wenn der Dienstleister eine Vielzahl an Kunden hat.

Zwei Modelle der Bereitstellung lassen sich unterscheiden: Zum einen kann sich die ausgelagerte Infrastruktur und Software beim Kunden befinden, zum anderen beim Dienstleister selbst. In beiden Fällen verbleibt die Verantwortung jedoch beim Dienstleister.

Motivationsgründe für IT-Outsourcing sind oftmals die Konzentration auf das Kerngeschäft, die Nutzung der Kompetenzen des Dienstleisters und vordergründig das Sparpotenzial bei den laufenden Kosten für Betrieb, Wartung und Administraion der Infrastruktur.

Klassisches Outsourcing gleicht in vielen Gesichtspunkten der Nutzung von Cloud-Diensten. Einige Unterschiede gilt es jedoch zu berücksichtigen:

- Aus Gründen der Wirtschaftlichkeit teilen sich beim Cloud-Computing mehrere Anwender eine gemeinsame Infrastruktur (mandantenfähige Architektur).
- Cloud-Computing stellt skalierbare und anpassungsfähige Dienste zur Verfügung. Die kurzfristige Anpassung an den tatsächlichen Bedarf kann - im Gegensatz zum IT-Outsourcing, bei dem Langzeitverträge den Regelfall bilden - sehr viel schneller geschehen. Es lassen sich sowohl zusätzliche Kapazitäten abfordern als auch ungenutzte Kapazitäten wieder freigeben.
- Die Administration der genutzten Cloud-Dienste erfolgt im Regelfall über ein Webinterface durch den Anwender selbst. Er kann so die genutzten Dienste seinen Bedürfnissen anpassen.
- Durch die im Cloud-Computing eingesetzten Techniken lässt sich eine Verteilung der IT-Leistung über geographisch weit verstreute Standorte (Inland wie Ausland) erreichen. Der Anwender kann so die genutzten Dienste und Ressourcen von unterschiedlichen Orten aus abrufen, ist also nicht auf einen Standort beschränkt.
- Anwender können Dienste und Ressourcen einfach und mit wenig Interaktion seitens des Providers über Webinterfaces oder geeignete Schnittstellen selbst administrieren. [vgl. BSI]

2.2.2 Grid-Computing

Beim Grid-Computing handelt es sich um eine Form des verteilten Rechnens, bei der die Rechenleistung aus einem Verbund lose gekoppelter Systeme erzeugt wird. Grid-Computing kommt zur Lösung von rechenintensiven Problemen zum Einsatz, findet aber ebenfalls in weiteren Bereichen Anwendung. Es ist vorwiegend in der Forschung und Wissenschaft anzutreffen, kommt aber auch kommerziell, z.B. in der Pharmaforschung und den Wirtschaftswissenschaften, zum Einsatz.

Grid-Computing ähnelt in den verwendeten Basistechnologien sehr dem Cloud-Computing, dennoch gibt es klare Unterschiede. Ein Grid stellt ein hochperformantes verteiltes System

dar, das verteilte Ressourcen zur entfernten Ausführung von speziellen Anwendungen und Lösungen von Problemstellungen - beispielsweise komplexe mathematische Berechnungen - zur Verfügung stellt.

Beim Cloud-Computing stehen benutzerspezifische Funktionalitäten im Mittelpunkt, um eine individuelle IT-Umgebung zu schaffen und zu betreiben. Weiterhin ist die Anwenderzahl hier weitaus größer, wodurch die Anwendungsfälle viel allgemeiner ausfallen.

Beim Grid-Computing handelt es sich immer um ein verteiltes System, die Infrastruktur ist dabei dezentral organisiert. Jeder Knoten ist autonom, das Management unterliegt nicht einer zentralen Kontrollinstanz. Weiterhin besteht ein Grid aus heterogenen Ressourcen. Diese können sich in Konfiguration, Schnittstellen und Administration unterscheiden. Dabei werden häufig standardisierte Programmbibliotheken und Middleware eingesetzt.

Cloud-Computing lässt sich ebenfalls verteilt betreiben, allerdings kann ein Anbieter eine Cloud auch mit einem einzelnen leistungsstarken Server aufsetzen. Beim Cloud-Computing mangelt es an standardisierten Protokollen und Schnittstellen, wodurch die Infrastruktur meist homogen durch den jeweiligen Anbieter zur Verfügung gestellt wird. Das Management der Cloud erfolgt zentral im Rechenzentrum des Anbieters.

Zu guter Letzt bleibt zu erwähnen, dass es beim Grid-Computing zumeist schwer fällt, eine klare Garantie für den verfügbaren Service abzugeben. Cloud-Computing stellt klare Richtlinien für die Dienstgüte (Quality of Service) auf und ermöglicht einen einfachen Zugriff auf dynamische und bedarfsgerechte Ressourcen. [vgl. BKNT11, S. 5, MH11, S. 19f.]

Tabelle 2.2.1 bietet nochmals einen tabellarischen Vergleich von IT-Outsourcing, Cloud- und Grid-Computing.

2.3 Bereitstellungsmodelle im Cloud-Computing

Ein Unterscheidungsmerkmal beim Cloud-Computing ist die Offenheit der Plattform. Es werden Private, Public, Hybrid und Community Clouds unterschieden. Dabei geht es im Prinzip um den Zugriff auf die einzelnen Plattformen.

2.3.1 Public Cloud

Das einfachste und am häufigsten gebräuchlichste Bereitstellungsmodell ist die Public Cloud. Dabei stellt ein unabhängiger Anbieter seine Dienste mehreren Kunden öffentlich zur Verfügung. Dies können sowohl Anwender als auch Unternehmen sein. Die Kunden sind bei diesem Modell weder Eigentümer der Infrastruktur noch der genutzten Softwarelösungen. Die Cloud wird allein vom Anbieter verwaltet und in dessen Rechenzentren betrieben. Kunden

	IT-Outsourcing	Cloud-Computing	Grid-Computing
Anwendungsform	Typischerweise ein Server pro Aufgabe	Virtualisierung von Servern; ein Server berechnet verschiedene Aufgaben gleichzeitig	Mehrere Server rechnen parallel an einer Aufgabe
Art der Ressourcen	Physisch	Virtuell	virtueller Supercomputer aus lose gekoppelten Systemen
Ressourcenverwaltung	Zentral	Zentral	Dezentral
Ressourcenbereitstellung	Lokal, Online	Online	Online
Anpassbarkeit von Ressourcen	Schwierig	Einfach möglich	Möglich
Preismodell	Langzeitverträge	Pay-per-use	Pay-per-use
Investition	Gegeben	Gering	Gering
Anwendungsfälle	Allgemein	Allgemein	Speziell

Tabelle 2.2.1: Outsourcing, Cloud- und Grid-Computing im Vergleich [vgl. Lip11, S. 14]

haben kein Mitbestimmungsrecht über Prozessabläufe in der Cloud und die Ressourcen werden mit mehreren Kunden geteilt. Das bedeutet hier, dass Datenspeicher oder Rechenzeit durch denselben physischen Server bereitgestellt werden. In Abbildung 2.3.1 stellen “Anbieter 1“ und “Anbieter 2“ jeweils einen eigenständigen Anbieter von Public-Cloud-Diensten dar.

Vorteilhaft für die Kunden ist die größere Flexibilität durch die Vermeidung des Betriebs einer eigenen Infrastruktur und die niedrigeren Kosten aufgrund der größeren Anzahl an Nutzern. Auf der anderen Seite spielt die Datensicherheit durch die gemeinsame Nutzung der Ressourcen durch mehrere Kunden eine zentrale Rolle, da der Kunde keine Kontrolle über Art und Ort der Speicherung seiner Daten hat (siehe dazu ebenfalls Abschnitt 2.6.2).

Die Abrechnung der verbrauchten Ressourcen geschieht in der Regel monatlich. Für den Selfservice ist das Angebot eines Web-Portals der Regelfall. Darüber können die Anwender den gewünschten Leistungsumfang selbst bestimmen.

Zu den bekanntesten Anbietern von öffentlichen Cloud-Diensten zählen beispielsweise Amazon[6], Google[7], Microsoft[8] sowie Salesforce[9]. [vgl. MH11, S. 21f., Lip11, S. 21f.]

[6] Amazon Web Services: http://aws.amazon.com
[7] Google Cloud Platform: https://cloud.google.com
[8] Microsoft Windows Azure: http://www.windowsazure.com
[9] Salesforce: http://www.salesforce.com

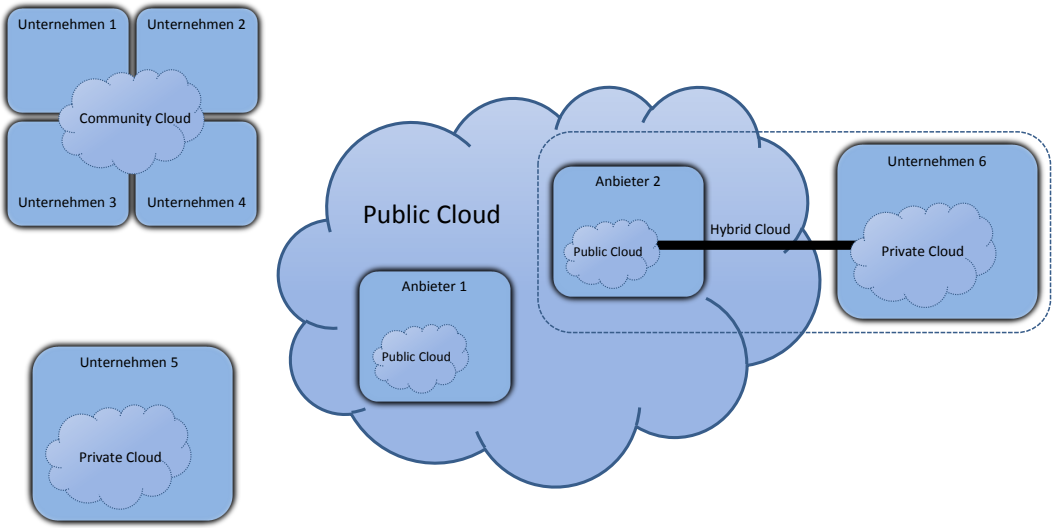


Abbildung 2.3.1: Cloud-Bereitstellungsmodelle im Überblick [vgl. BKNT11, S. 28]

2.3.2 Private Cloud

Bei einer Private Cloud handelt es sich um eine selbst betriebene Cloud eines Unternehmens. Bei diesem Modell gehören Anbieter und Nutzer derselben Institution an. Zu den Akteuren innerhalb der Private Cloud zählen die Mitarbeiter des Unternehmens sowie ggf. Kunden oder Lieferanten, die Zugriff auf Teilbereiche oder Tools zur Kooperation mit dem Unternehmen erhalten.

Bei einer Private Cloud wird die Infrastruktur nur für ein Unternehmen betrieben. Dabei erfolgen Organisation und Betrieb der Cloud-Infrastruktur durch das Unternehmen selbst oder durch einen Dritten. Die Infrastruktur kann im unternehmenseigenen Rechenzentrum oder in einer fremden Institution lokalisiert sein. In Abbildung 2.3.1 sind die beiden Unternehmen 5 und 6 jeweils Betreiber einer eigenständigen Private Cloud.

Als Hauptargument für den Einsatz von Private Clouds werden meist Sicherheitsaspekte genannt. Da das Unternehmen selbst der Cloud-Betreiber ist, verbleibt die Kontrolle über sensible Daten im Unternehmen und Datensicherheit, Datenspeicherort und Privatsphäre lassen sich einfacher kontrollieren.

Nachteilig an Private Clouds ist, dass sich das Unternehmen selbst um die Bereitstellung von Infrastruktur und Softwarelösungen bemühen muss. Weiterhin fallen höhere Personalkosten an, da die Cloud-Infrastruktur gewartet und betrieben werden muss. Damit sich der Einsatz einer eigenen Private Cloud rentiert, muss das Unternehmen also eine entsprechende Größe haben. Für kleinere Unternehmen bietet sich dieses Modell also weniger an. [vgl. Lip11, S. 23f., BKNT11, S. 28f.]

2.3.3 Hybrid Cloud

Hybrid Clouds sind Kombinationen aus Public, Private oder Community Clouds. Bei diesem Modell wird die eigene Private oder Community Cloud mit skalierbaren Diensten einer Public Cloud kombiniert. Unternehmen und Anwender können im Regelbetrieb ihre eigenen Ressourcen und Anwendungen nutzen. Bei Lastspitzen lassen sich jederzeit Rechenleistung oder weitere Ressourcen aus der Public Cloud beziehen, ohne die eigene Infrastruktur aufrüsten zu müssen. Zur Erhöhung der Ausfallsicherheit der eigenen Infrastruktur lassen sich Dienste aus der Public Cloud hier ebenfalls einsetzen. In Abbildung 2.3.1 ist die Verbindung der Private Cloud von "Unternehmen 6" mit der Public Cloud von "Anbieter 2" zu einer Hybrid Cloud dargestellt.

Hybrid Clouds bieten damit ein hohes Maß an Flexibilität. In Bezug auf Datensicherheit und Privatsphäre bleibt abzuwägen, dass nur unkritische Funktionalitäten und Daten ausgelagert werden dürfen. Auf diese Weise lassen sich dann bestimmte Dienste bei öffentlichen Anbietern über das Internet abwickeln, während datenschutzkritische Anwendungen und Daten unternehmensintern verbleiben. [vgl. BKNT11, S. 29, MRV11, S. 19f.]

2.3.4 Community Cloud

Wie in Abschnitt 2.3.2 bereits erwähnt, bietet sich die Private Cloud nur für große Unternehmen an. Aber auch kleinere und mittelständische Unternehmen wollen von der Cloud-Architektur und den Vorteilen einer Private Cloud profitieren. Bei der Community Cloud handelt es sich um ein Modell, bei dem sich mehrere Unternehmen mit ähnlichen Anforderungen und Interessen gemeinsam eine Infrastruktur teilen. Abbildung 2.3.1 zeigt für die Unternehmen 1 bis 4 den Zusammenschluss zu einer gemeinsamen Community Cloud.

Betrieben wird eine solche Cloud durch eines oder mehrere der beteiligten Unternehmen oder durch einen Dritten. Im Regelfall ist eine Community Cloud nicht öffentlich, sondern ausschließlich der Gemeinschaft der teilnehmenden Unternehmen zugänglich. Es besteht die Möglichkeit, maßgeschneiderte, individuelle Dienste für die spezielle Gemeinschaft bereitzustellen. Auch wenn sich bei diesem Modell die Kosten auf wenige Nutzer verteilen, lassen sich durch eine gemeinsame Nutzung der Ressourcen finanzielle Vorteile erwirtschaften. [vgl. Lip11, S. 24, MRV11, S. 19]

2.4 Servicemodelle im Cloud-Computing

Die verschiedenen Servicemodelle des Cloud-Computings werden auch als Ebenen bezeichnet. Diese sind nach ihrem Abstraktionsgrad angeordnet. Die höheren und abstrakteren Ebenen können die Dienste der tieferen und konkreteren Ebenen zu ihrer eigenen Dienstrealisierung nutzen. Höhere Ebenen können die Dienste aller unterliegenden Schichten nutzen und nicht nur die der nächst tieferen Schicht.

Die unterste Ebene bildet IaaS. Hier stellt der Anbieter lediglich die Infrastruktur zur Verfügung. Darauf aufbauend folgt PaaS, wo der Anbieter bereits eine gänzlich verwaltete Umgebung (Entwicklungs- und Laufzeitumgebung) bereit stellt. Der Nutzer muss sich hier lediglich selbstständig um den Entwurf einer Software kümmern. Den höchsten Grad an Abstraktion kann der Anwender bei SaaS erreichen. Das Angebot umfasst vollständige Anwendungen und Anwendungsdienste zum sofortigen Einsatz.

Abbildung 2.4.1 zeigt die Anordnung der drei Ebenen und die jeweils zugehörigen Bestandteile, auf die in den nachfolgenden Abschnitten zu IaaS, PaaS und SaaS eingegangen wird. [vgl. BKNT11, S. 30f]

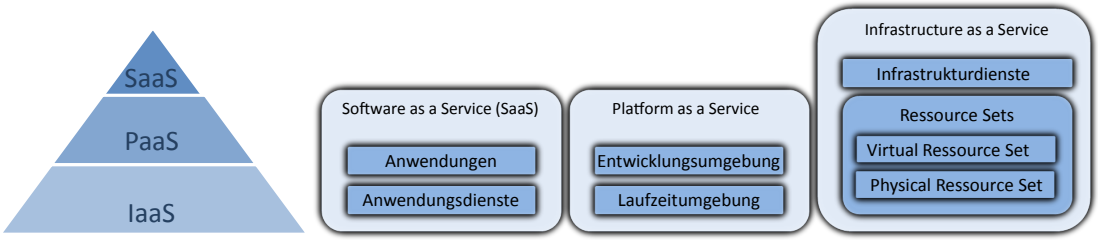


Abbildung 2.4.1: Cloud-Servicemodelle im Überblick [vgl. BKNT11, S. 30]

2.4.1 Infrastructure as a Service (IaaS)

Bei IaaS handelt es sich um die Bereitstellung virtualisierter Infrastruktur durch den Cloud-Computing-Anbieter. Der Anwender bezieht dabei Server, Datenspeicher, Netzwerkkomponenten und weitere Infrastruktur als abstrakten und virtualisierten Dienst über das Internet. Die Anwender sehen diesen Service als ein privates, virtuelles Rechenzentrum. Um die zugrunde liegende physische Hardware müssen sie sich dabei nicht kümmern. Nutzer dieses Dienstes haben hier unter anderem die Möglichkeit, eigene virtuelle Serverinstanzen anzulegen, zu starten und zu beenden. Weiterhin können sie eigene Netzwerktopologien anlegen und beliebige Software auf dieser Infrastruktur installieren. Dabei haben sie vollen administrativen Zugriff

auf alle virtuellen Ressourcen. Ermöglicht wird dieses durch eine Virtualisierungsschicht. Diese abstrahiert und isoliert die Kundenumgebungen vollständig von der zugrunde liegenden Hardware.

Genutzte Ressourcen lassen sich in zwei verschiedene Kategorien unterteilen:

- **Virtual Resource Set (VRS)**: Physische Hardware wird komplett abstrahiert, es kommen vollständig virtualisierte Ressourcen zum Einsatz. Diese Variante entspricht der Idee des Cloud-Computings und ist daher am häufigsten anzutreffen.
- **Physical Resource Set (PRS)**: Diese basieren auf proprietärer physischer Hardware, bei der auf die Virtualisierungsebene verzichtet wird. Die Verwaltung geschieht, wie bei VRS, über komfortable Schnittstellen. Gründe für den Einsatz sind Stabilität, Performanz oder spezielle Anforderungen an die genutzte Hardware seitens des Anwenders.

Für den Einsatz der Infrastruktur ergeben sich vielfältige Alternativen. Mögliche Einsatzgebiete sind Web- und Mailserver, Domänencontroller oder Datenbankserver. Möchte man beispielsweise eine Webanwendung erstellen, so muss sich der Nutzer selbstständig um die Installation und Einrichtung der notwendigen Laufzeitumgebungen, wie z.B. PHP, Java oder .NET, kümmern. Verwaltung und Wartung der virtuellen Infrastruktur obliegt dabei allein dem Nutzer. Die Verwaltung erfolgt über Benutzerschnittstellen. Hierüber können die allokierten Ressourcen flexibel nach oben und unten skaliert werden.

Die Abrechnung der genutzten Ressourcen erfolgt typischerweise nutzungsabhängig. Grundlage dafür bilden im Datenspeicherbereich der belegte Datenspeicher sowie das zugehörige Datentransfervolumen. Im Rechenbereich dient als Abrechnungsgrundlage der Verbrauch von CPU-Zeit und Arbeitsspeicher pro Zeiteinheit und ebenfalls das externe Datentransfervolumen.

Aufgrund der Tatsache, dass der Nutzer selbst die gesamte Software, Laufzeitumgebung, Anwenderdaten usw. bereitstellen muss, ist der administrative Aufwand gegenüber PaaS und SaaS demnach höher. IaaS bietet dafür ein Höchstmaß an Flexibilität, denn weitere Cloud-Computing-Dienste können auf diese Plattform aufsetzen. [vgl. BKNT11, S. 31f., MH11, S. 24f., BIT09, S. 24f.]

2.4.2 Platform as a Service (PaaS)

Die mittlere Abstraktionsebene bildet PaaS. Die Dienste dieses Modells richten sich in erster Linie an Anwendungsentwickler und nicht an Endanwender. Die Cloud-Computing-Anbieter stellen bei PaaS eine bereits verwaltete Umgebung zur Verfügung. Auf dieser lassen sich eigene Anwendungen entwickeln und bereitstellen. Die dazu benötigten technischen Frameworks

(Laufzeitumgebung, Datenbanken, Middleware usw.) stellt der Anbieter bereit. Der Zugriff auf die genutzten Dienste erfolgt über standardisierte Internet-Technologien [vgl. Lip11, S. 11].

Entwickler können auf PaaS-Plattformen beispielsweise Anwendungen entwickeln, die sich danach als SaaS-Anwendungen nutzen lassen. Mit der technischen Umsetzung dieser Dienste muss sich der Entwickler nicht befassen. Auch um die Beschaffung der zugrunde liegenden Hardware oder Software muss er sich nicht kümmern. Systemadministration und Infrastrukturwartung entfallen ebenfalls.

Anwender erwarten eingebaute Monitoring- und Reporting-Funktionen, womit sich das Laufzeitverhalten der entwickelten Anwendungen überwachen lässt. Dies ermöglicht es dem Entwickler, sich ganz auf die Anwendungsentwicklung zu konzentrieren.

Der administrative Aufwand ist im Vergleich zu IaaS wesentlich geringer, dafür bieten PaaS-Lösungen aber keinen Zugriff mehr auf das zugrunde liegende Betriebs- und Dateisystem. Es können lediglich bereitgestellte Application Programming Interfaces (APIs) der Plattform genutzt werden. Ein wichtiger Punkt bei PaaS ist die Verwendung von interoperablen Schnittstellen. Nur auf diese Weise lassen sich verschiedene Plattformen anbinden.

PaaS bietet typischerweise Dienste für Zugriffskontrolle, Prozesssteuerung, Datenhaltung und Synchronisierung. Durch die Vorgaben und Einschränkungen seitens des Anbieters verringert sich die Flexibilität im Hinblick auf die Konfiguration der genutzten Plattform und die Portierbarkeit zu anderen Cloud-Anbietern. Bei unterschiedlichen Anbietern umfasst das Angebot ggf. andere Frameworks und Programmiersprachen (Vendor-Lock-in) [vgl. MH11, S. 26ff.].

Die Abrechnung der Dienste erfolgt wieder in Abhängigkeit der Nutzung, so dass die entstehenden Kosten damit in direktem Zusammenhang mit dem Bedarf und den verwendeten Ressourcen stehen. [vgl. BIT09, S. 26]

2.4.3 Software as a Service (SaaS)

Die Ebene mit dem höchsten Grad an Abstraktion ist die SaaS-Ebene. Diese richtet sich an Endanwender. Der Nutzer bezieht hier Anwendungen als Dienst direkt über das Internet.

Der Vorteil bei SaaS ist, dass Software nicht mehr lokal auf jedem Endgerät installiert und konfiguriert werden muss. Weiterhin entfällt die Bereitstellung von nötigen Ressourcen für den Betrieb. Die Anwendungen sind sofort über einen Browser nutzbar, unabhängig vom Ort der Ausführung. Für den Anwender ist es unerheblich, ob die Anwendung verteilt über verschiedene Clouds ausgeführt wird. Wichtig ist nur, dass der Anwender ein einheitliches grafisches Benutzerinterface (Graphical User Interface (GUI)) geboten bekommt. Der Anwender

hat dabei keine Kenntnis und keinen Zugriff sowohl auf die zugrunde liegende Infrastruktur oder das Betriebssystem als auch auf die PaaS-Ebene, auf der die Anwendung aufsetzt.

Oftmals findet sich die Bezeichnung "Mietsoftware" für SaaS-Angebote. Diese Bezeichnung ist unzureichend, denn aufgrund der Art und Weise, wie die Dienstleistung erbracht wird, mietet der Anwender keine Software. Er bezieht vielmehr einen Anwendungsservice mit Abnahme nach Bedarf, leichter Erweiterbarkeit und Bezahlung nach Abnahmemenge.

Bei SaaS-Diensten sind bereits alle für die Nutzung erforderlichen Komponenten enthalten. Dazu zählen Hard- und Software, Wartung sowie Betrieb. Alle Anwender nutzen dieselbe Anwendung und Infrastruktur. Vorteil dieser 1:n-Lösung ist, dass Updates, Änderungen und Erweiterungen, die alle Anwender betreffen, nur einmal zentral beim Anbieter erfolgen müssen. Dieses hohe Maß an Standardisierung führt allerdings dazu, dass SaaS-Angebote in den Möglichkeiten zur Individualisierung durch den Anwender stark eingeschränkt sind. Individuelle Anpassungen sind ohne weitere Cloud-Computing-Ebenen (IaaS, PaaS) oftmals nicht möglich. Die Anwendungen werden vom Anbieter als fertige Lösung angeboten, die einen bestimmten Problembereich abdecken. Weiterhin ist der Anwender zur Nutzung der SaaS-Dienste abhängig von einer Internetanbindung. [vgl. BIT09, S. 27f., MH11, S. 28ff.]

Tabelle 2.4.1 fasst die Unterschiede der drei Servicemodelle nochmals tabellarisch zusammen.

2.4.4 Everything as a Service (XaaS)

Neben den durch das NIST definierten Servicemodellen haben sich bereits weitere Modelle etabliert. Zusammenfassen lassen sich diese unter dem Namen XaaS. Dieser Ansatz beschreibt, dass sich quasi alles als Dienst auslagern lässt. Cloud-Anbieter verfolgen dabei ebenfalls ein dienstleistungsbasiertes Geschäftsmodell. Anwender zahlen nur für das, was sie tatsächlich nutzen.

Oftmals ist der Einstieg für viele Unternehmen ins Cloud-Computing Communication as a Service und Collaboration as a Service. Ersteres umfasst die Auslagerung von Telefonie- und Kommunikationsanwendungen an einen Cloud-Anbieter, der diese wiederum als Dienst bereitstellt. Zweiteres ist die Weiterentwicklung von Communication as a Service; hier steht der gemeinsame Zugriff auf Dokumente im Vordergrund. Zu den Bestandteilen einer Collaboration-as-a-Service-Lösung gehören beispielsweise Unified Messaging (Integration von Sprache, Fax, SMS und E-Mail), Web- und Videokonferenzen, Instant Messaging, Blogs und Wikis, Kalender usw. [vgl. BIT09, S. 28]

Über diese beiden Beispiele hinaus gibt es noch eine Vielzahl an weiteren XaaS-Diensten, wie Storage as a Service, Backup as a Service, Network as a Service, Desktop as a Service und Human as a Service, nur um einige wenige zu nennen. Eine tiefergehende Betrachtung dieser

Servicemodelle findet aufgrund der Zielsetzung in dieser Arbeit nicht statt. Von Interesse sind die drei wichtigsten Servicemodelle, IaaS, PaaS und SaaS, die auch das NIST listet.

	IaaS	**PaaS**	**SaaS**
Abstraktionsgrad	Niedrig	Mittel	Hoch
Verwaltungsaufwand	Hoch	Mittel	Niedrig
Anpassbarkeit	Hoch	Mittel	Niedrig
Zielgruppe	Systemhäuser, IT-Dienstleister, IT-Abteilungen, Softwareentwickler	Softwareentwickler	Endanwender
Preismodell	Pay-per-use	Pay-per-use	Pay-per-use

Tabelle 2.4.1: Unterschiede der Servicemodelle [MH11, S. 30]

2.5 Definition der Cloud nach NIST

Es existieren viele unterschiedliche Definitionen des Begriffs Cloud-Computing, aber bisher konnte sich keine Definition als allgemeingültig durchsetzen. Die Definition des NIST bietet mit den zugehörigen Kriterien, Service- und Bereitstellungsmodellen einen sinnvollen Abgrenzungsrahmen und findet in Fachkreisen oftmals Anwendung, beispielsweise in der für diese Arbeit verwendeten Lektüre Sos10 und BKNT11 oder bei der European Network and Information Security Agency (ENISA)[10] und dem Bundesamt für Sicherheit in der Informationstechnik (BSI).

Grundlage für diese Arbeit bildet die NIST-Definition von Cloud-Computing [NIS11], die weiterhin aus fünf Eigenschaften, drei Service- und vier Bereitstellungsmodellen besteht (im Folgenden aus dem Englischen übersetzt):

> *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*[NIS11, S. 2]

> *Cloud-Computing ist ein Modell, das Anwendern bei Bedarf, jederzeit und überall komfortabel Zugriff auf einen geteilten Pool von konfigurierbaren Rechnerressourcen*

[10] Europäische Agentur für Netz- und Informationssicherheit: http://www.enisa.europa.eu

(z.B. Netzwerke, Server, Datenspeicher, Anwendungen und Dienste) über ein Netzwerk bietet. Diese Ressourcen können schnell und mit minimalem Managementaufwand oder Eingreifen seitens des Serviceproviders zur Verfügung gestellt werden.

Folgende fünf Eigenschaften charakterisieren laut NIST eine echte Cloud-Lösung:

- **On-demand Selfservice** (Diensterbringung auf Anforderung):
  Die Provisionierung der Ressourcen (z.B. Rechenleistung, Speicherkapazität) erfolgt nach Bedarf durch den Nutzer und läuft automatisch ohne menschliche Interaktion mit dem Anbieter ab.

- **Broad Network Access** (Umfassender Netzwerkzugriff):
  Die Ressourcen und Dienste sind über Standardnetzwerktechnologien, z.B. über das Internet, verfügbar und unterstützen beliebige Endgeräte (z.B. Smartphones, Tablets, Laptops etc.).

- **Resource Pooling** (Ressourcen Pooling):
  Die Ressourcen des Anbieters sind in Pools zusammengefasst, aus denen sich viele Anwender gleichzeitig nach Bedarf bedienen können (mandantenfähige Architektur). Dabei teilen sich mehrere Anwender z.B. Speicherkapazität, Rechenleistung und Netzwerkbandbreite. Die Anwender selbst wissen dabei nicht, wo die Ressourcen lokalisiert sind. Sie haben aber ggf. die Möglichkeit, vertraglich den Speicherort (beispielsweise Region, Land oder Rechenzentrum) festzulegen.

- **Rapid Elasticity** (Schnelle Elastizität):
  Ressourcen können schnell und elastisch bei Bedarf skaliert werden, in manchen Fällen sogar automatisch. Für die Anwender hat es den Anschein, als ließen sich unendlich viele Ressourcen zu jedem Zeitpunkt bereitstellen.

- **Measured Services** (Messbare Dienstqualität):
  Die Ressourcennutzung lässt sich auf der jeweiligen Nutzungsebene messen und überwachen. Üblicherweise geschieht das auf Basis eines Pay-per-Use-Modells. Dies schafft zum einen Transparenz und Vertrauen beim Kunden, zum anderen bildet es die Grundlage für eine nutzungsbedingte Abrechnung seitens des Anbieters.

Das NIST listet folgende drei Servicemodelle (Service Models):

- **Infrastructure as a Service** (IaaS):
  Der Anwender hat die Möglichkeit, grundlegende Rechenressourcen, wie Rechenkapazität, Datenspeicher und Netzwerke, zu provisionieren, auf denen er beliebige Software installieren und betreiben kann (beispielsweise das Betriebssystem und weitere Anwendungen). Der Anwender steuert oder verwaltet nicht die zugrunde liegende Cloud-Infrastruktur, hat aber die Kontrolle über Betriebssystem, Datenspeicher und installierte Anwendungen. Er hat ggf. limitierten Zugriff auf Netzwerkkomponenten, wie beispielsweise Hardware-Firewalls.

- **Platform as a Service** (PaaS):
  Der Anwender hat die Möglichkeit, eigens erstellte oder erworbene Anwendungen auf der Cloud-Infrastruktur zu installieren, die mit anbieterseitig unterstützten Programmiersprachen, Bibliotheken, Diensten und Programmen erstellt wurden. Der Anwender steuert oder verwaltet nicht die zugrunde liegende Cloud-Infrastruktur. Dazu zählen Netzwerk, Server, Betriebssysteme oder Datenspeicher. Aber er hat die Kontrolle über seine installierten Anwendungen und ggf. über Einstellungen der Umgebung, auf der die Anwendungen betrieben werden.

- **Software as a Service** (SaaS):
  Der Anwender hat die Möglichkeit, die vom Dienstanbieter bereitgestellten Anwendungen, die auf der Cloud-Infrastruktur laufen, zu nutzen. Die Anwendungen sind von verschiedenen Endgeräten aus über entweder eine schlanke Schnittstelle (z.B. ein Webbrowser) oder eine Programmschnittstelle nutzbar. Dabei steuert oder verwaltet der Anwender nicht die zugrunde liegende Cloud-Infrastruktur, wie Netzwerk, Server, Betriebssysteme, Datenspeicher oder gar individuelle Leistungsmerkmale der Anwendungen. Mögliche Ausnahme sind limitierte anwenderspezifische Anwendungseinstellungen.

Schließlich unterscheidet das NIST folgende vier Bereitstellungsmodelle (Deployment Models):

- **Public Cloud**:
  Die Cloud-Infrastruktur wird für die Nutzung durch die breite Öffentlichkeit bereitgestellt. Die Cloud-Infrastruktur kann einem Geschäfts- oder Wissenschaftsbetrieb, einer staatlichen Stelle oder einer Kombination aus beiden gehören und wird betrieben durch einen Geschäfts- oder Wissenschaftsbetrieb, eine staatlichen Stelle oder eine Kombination aus diesen. Die Cloud-Infrastruktur wird in den Räumlichkeiten des jeweiligen Anbieters betrieben.

- **Private Cloud**:
  Die Cloud-Infrastruktur wird exklusiv für eine Organisation, bestehend aus mehreren Anwendern (z.B. Abteilungen), bereitgestellt. Die Cloud-Infrastruktur kann der Organisation, einem Dritten oder einer Kombination aus diesen gehören und wird betrieben durch die Organisation, einen Dritten oder eine Kombination aus beiden. Die Cloud-Infrastruktur kann dabei innerhalb der Räumlichkeiten der Organisation oder extern betrieben werden.

- **Hybrid Cloud**:
  Die Cloud-Infrastruktur ist eine Mischung aus mindestens zwei eigenständigen Cloud-Infrastrukturen (Private, Community oder Public), die jeweils für sich eigene Einheiten bleiben, aber über standardisierte oder proprietäre Technologie verbunden sind. Über diese Kopplung ist die Portabilität von Daten und Anwendungen möglich, beispielsweise für die Behandlung von Lastspitzen.

- **Community Cloud**:
  Die Cloud-Infrastruktur wird exklusiv für einen speziellen Nutzerkreis von Organisationen bereitgestellt, die beispielsweise ein gemeinsames Interesse hinsichtlich des Aufgabengebiets, der Sicherheitsanforderungen oder diverser Grundsätze aufweisen. Die Cloud-Infrastruktur kann einer oder mehreren Organisationen der Gemeinschaft, einem Dritten oder einer Kombination aus diesen gehören und wird betrieben durch eine oder mehrere Organisationen der Gemeinschaft, einen Dritten oder eine Kombination aus beiden. Die Cloud-Infrastruktur kann dabei in den Räumlichkeiten der Organisationen oder extern betrieben werden.

Abbildung 2.5.1 zeigt die genannten Modelle und Eigenschaften des Cloud-Computings im Zusammenhang. [vgl. NIS11, S. 2f.]

2.6 Aspekte des Cloud-Computings

Der folgende Abschnitt beschäftigt sich mit den wichtigsten Vor- und Nachteilen von Cloud-Computing hinsichtlich technischer, sicherheitskritischer, rechtlicher und wirtschaftlicher Aspekte.

2.6.1 Technische Aspekte

Cloud-Computing ist deshalb attraktiv, weil es die Komplexität der Informationstechnologie vor Nutzern und Entwicklern verbirgt. Man muss nicht im Einzelnen wissen, wie ein Dienst

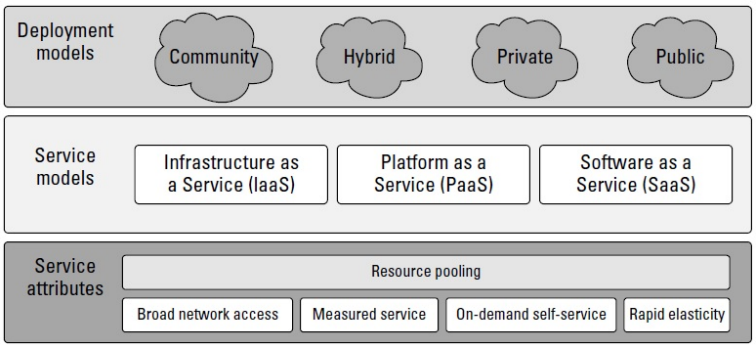


Abbildung 2.5.1: Modelle und Eigenschaften des Cloud-Computings [Sos10, S. 6]

generiert wird. Es ist die Aufgabe des Dienstleisters, eine entsprechende Abstraktionsschicht bereitzustellen. Dieser Abschnitt gibt einen Überblick über Technologien, auf denen Cloud-Computing basiert. Dabei handelt es sich um Virtualisierung, Serviceorientierte Architektur (SOA) und Webservices. [vgl. BKNT11, S. 9ff.]

2.6.1.1 Virtualisierung

Die Virtualisierung von Ressourcen ist eine der wichtigsten Grundlagen des Cloud-Computings. Virtualisierung ermöglicht einen abstrakten, logischen Blick auf physische Ressourcen. Dazu zählen neben Servern, Datenspeicher und Netzwerken auch Software. Für die Realisierung wird eine Abstraktionsebene zwischen Anwendungen und der physischen Hardware eingefügt. Dadurch greifen Anwendungen nicht mehr direkt auf Ressourcen zu, sondern auf die Virtualisierungsschicht.

Die Idee der Virtualisierung basiert darauf, dass sich physische Ressourcen logisch in Pools zusammenfassen und gemeinsam verwalten lassen. Aus diesen Pools erfolgt dann nach Bedarf die Erfüllung der Anforderungen. Durch die Virtualisierung ergeben sich sowohl auf Betreiberseite als auch auf Nutzerseite Vorteile:

- **Ressourcen Auslastung**: Physische Server sind oftmals nicht optimal ausgelastet, denn es müssen Reservekapazitäten für die Abdeckung von Lastspitzen vorgehalten werden. Bei VMs lassen sich solche Lastspitzen durch den Ressourcen-Pool bedienen.
- **Management**: Die Verwaltung der in den Pools enthaltenen Ressourcen kann automatisiert erfolgen, neue VMs lassen sich bei Bedarf automatisch erzeugen und konfigurieren.

- **Konsolidierung**: Systeme, Datenbestände und Anwendungen werden vereinheitlicht und zusammengeführt, die Anzahl an benötigten physischen Komponenten sinkt. Die Infrastruktur wird vereinfacht und die Effizienz gesteigert.
- **Energieverbrauch**: Energiekosten für den Betrieb eines Servers übersteigen oftmals - gemessen an der Lebensdauer - die Beschaffungskosten. Durch die Konsolidierung vermindert sich die Anzahl an physischen Komponenten. Hierdurch sinken zudem die Energiekosten.
- **Platzersparnis**: Stellfläche in Rechenzentren ist knapp und teuer. Durch die Konsolidierung lässt sich dieselbe Leistung auf weniger Stellfläche erbringen.
- **Notfallplanung**: VMs können verschiedenen Ressourcen-Pools angehören. Die Verfügbarkeit von Diensten wird erhöht und die Einhaltung von Service Level Agreements (SLAs) wird vereinfacht. Durch Hardware bedingte Wartungsfenster können gänzlich entfallen.
- **Dynamik**: Anforderungen lassen sich bedarfsgerecht und jederzeit erfüllen, bei Lastspitzen stehen einer VM zusätzliche Ressourcen (CPU, Speicher, I/O-Leistung usw.) zur Verfügung.
- **Verfügbarkeit**: Dienste sind hochverfügbar und stehen jederzeit zur Nutzung bereit. Bei Ausfallzeiten (Wartung, Ausfall) erfolgt die Migration der Anwendungen während des Betriebs auf ein anderes System.
- **Zugriff**: Die Virtualisierungsschicht bietet eine Isolation der einzelnen VMs, sowohl zu anderen VMs als auch zur physischen Infrastruktur. Die Systeme sind mandantenfähig (Multi-Tenant-Architektur) und bieten den Anwendern Managementfunktionalitäten, so dass diese ihre Leistungen durch Selfservice erwerben können.

Betriebssystemvirtualisierung Dieses ist die Variante mit dem niedrigsten Virtualisierungsgrad. Sie wird auch als Partitionierung bezeichnet. Bei dieser Art laufen unter einem Betriebssystemkern mehrere voneinander abgetrennte Laufzeitumgebungen, die nach außen wie ein eigenständiges System auftreten. Sie werden als Jails oder Container bezeichnet.

Alle laufenden Anwendungen teilen sich den gleichen Betriebssystemkern und die gleichen Laufzeitbibliotheken, laufen aber isoliert in ihrem Container und haben dabei keine Kenntnis von anderen Containern oder deren Ressourcen und Prozessen. Abbildung 2.6.1 zeigt die voneinander isolierten Container zusammen auf dem gemeinsamen Betriebssystem.

Durch den geringen Overhead bei der Virtualisierung ist dieses Verfahren sehr performant und es lassen sich vergleichsweise viele gleichartige Instanzen auf einer Hardwareplattform betreiben. Jedoch geht dies zu Lasten der Flexibilität, denn es lassen sich nur unabhängige Instanzen desselben Betriebssystems nutzen. Internet Service Provider (ISP) setzen diese Form der Virtualisierung oftmals bei virtuellen Mietservern (Root-Server) ein. [vgl. MWRS11, S. 17f., BKNT11, S. 13f.]

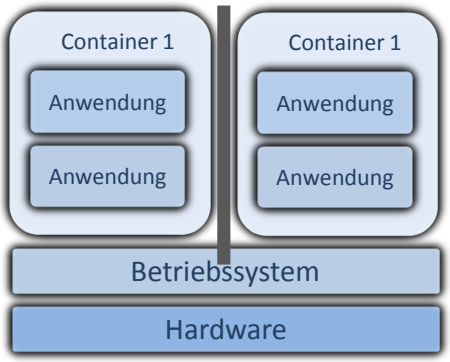
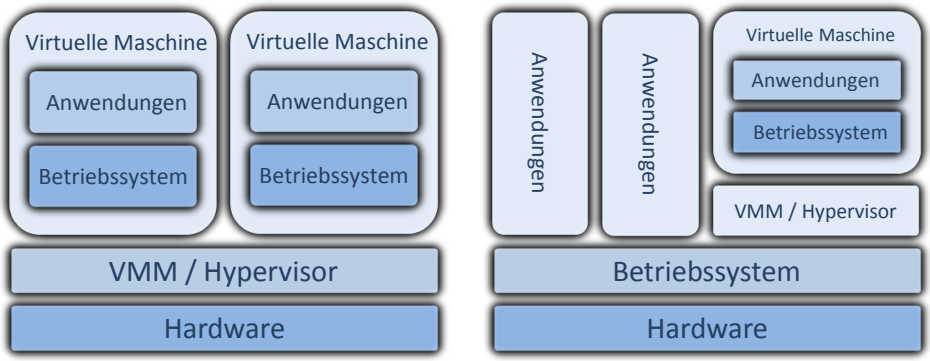


Abbildung 2.6.1: Betriebssystemvirtualisierung [vgl. BKNT11, S. 13]

Plattformvirtualisierung Diese Form erlaubt die Ausführung beliebiger Betriebssysteme und Anwendungen innerhalb virtueller Umgebungen. Die zwei wichtigsten Varianten sind die vollständige Virtualisierung und die Paravirtualisierung. Die Erklärung dieser beiden Formen erfolgt in diesem Abschnitt.

Grundlage zum Betrieb von VMs auf physischer Hardware ist ein Virtual Machine Monitor (VMM) bzw. Hypervisor. Dieser stellt die Virtualisierungsschicht dar, welche die gleichzeitige Ausführung und Steuerung mehrerer VMs ermöglicht. Der Hypervisor koordiniert die VMs und regelt deren Zugriffe auf die unterliegende physische Hardware. Unterscheiden lassen sich zwei Arten: ein Typ-1 Hypervisor (Bare Metal) setzt direkt ohne zusätzliches Betriebssystem auf die physische Hardware auf. Das macht ihn performanter, da die Ressourcenteilung durch ein zusätzliches Betriebssystem entfällt. Abbildung 2.6.2 zeigt in (a) den Hypervisor als eigene Schicht oberhalb der Hardware und unterhalb der VMs.

Ein Typ-2 (Hosted, bzw. VMM) Hypervisor setzt als Applikation auf ein vorhandenes Betriebssystem auf. Das erhöht zwar die Flexibilität, aber der Nachteil äußert sich in der zusätzlichen Schicht zwischen Gastsystem und Hardware. In Abbildung 2.6.2 läuft der Hypervisor bzw. VMM in (b) als Anwendung auf dem vorhandenen Betriebssystem.



(a) Bare Metal Hypervisor (Typ-1) (b) Hosted Hypervisor (Typ-2)

Abbildung 2.6.2: Bare Metal und Hosted Hypervisor bzw. VMM [vgl. MWRS11, S. 14]

Bei der x86-Architektur ist der Speicher in sogenannte Ringe unterteilt. Prozesse können nicht auf Speicherbereiche zugreifen, deren Ringnummer kleiner ist als ihre eigene. Ring 0 (Kernel Space) verfügt über die höchsten Berechtigungen, also Vollzugriff auf den gesamten Speicher. In diesem Ring läuft der Betriebssystemkern. In Ring 3 (User Space) laufen die Anwendungen. Hier gibt es die wenigsten Berechtigungen.

Bei der vollständigen Virtualisierung arbeitet der Hypervisor in Ring 0. Für jede VM wird ein kompletter virtueller Rechner mit virtuellen Ressourcen (CPU, RAM, Laufwerke, Netzwerkkarten usw.) und eigenem BIOS bereitgestellt. Am Gastbetriebssystem müssen keine Anpassungen erfolgen, daher lässt sich eine Vielzahl verschiedener Systeme virtualisieren.

Der Gastbetriebssystemkern arbeitet in Ring 1, daher müssen alle Zugriffe auf die Ressourcen durch den Hypervisor durchgereicht werden, bevor sie in Ring 0 ausgeführt werden können. Die Verarbeitungsgeschwindigkeit der Gastbetriebssysteme gleicht fast der Geschwindigkeit, die sich ohne Virtualisierung erzielen ließe. Für mehr Effizienz sorgen die von AMD[11] und Intel[12] entwickelten Befehlssatzerweiterungen für hardwarebasierte Virtualisierung für die x86-Architektur (AMD-V bzw. Intel VT). Diese bieten eine höhere Geschwindigkeit gegenüber Softwarelösungen.

Bei der Paravirtualisierung läuft das Gastbetriebssystem direkt im Ring 0 neben einem Hypervisor. Es steht keine emulierte Hardwareebene zur Verfügung, nur eine Anwendungsschnittstelle. Der Kernel des Gastbetriebssystems muss so modifiziert werden, dass alle direkten Hardwarezugriffe, welche der Kernel nicht direkt ausführen kann, an den Hypervisor weiter-

[11] Advanced Micro Devices, Inc.: http://www.amd.com
[12] Intel Corporation: http://www.intel.com

gereicht werden (Hypercall). Der Hypervisor führt den zugehörigen Systemaufruf (Systemcall) durch und bedient die aufrufende VM. Diese Art der Virtualisierung arbeitet nahe an der Hardware, so dass diese Form oftmals schneller als die Vollvirtualisierung ist. Die zwingend nötigen Anpassungen am Gastbetriebssystem schränken wiederum die Auswahl an möglichen Betriebssystemen ein. [vgl. MWRS11, S. 13ff., BKNT11, S. 14f.]

Speichervirtualisierung Bei dieser Variante wird eine zentral verwaltete Virtualisierungsschicht über sämtliche Speicherressourcen gelegt und diese in Pools zusammengefasst. Für Anwender präsentiert sich das System als eine große Einheit. Die Pools sind für Anwender in einer logischen Form verfügbar, so dass Anwendungen und Anwender dynamisch ihre Anforderungen daraus bedienen können. Die Datentransfers laufen dabei über ein spezielles Speichernetzwerk (Storage Area Network (SAN)) oder ein Firmennetzwerk (Local Area Network (LAN)).

Speichervirtualisierung erhöht die Flexibilität der Speicherverteilung. Der Anwender ist nicht an physische Grenzen gebunden. Die Ressourcen lassen sich somit effizient nutzen. Eine höhere Verfügbarkeit entsteht, Wartung und Management werden zentralisiert und vereinfacht.

Über die Virtualisierungsschicht lassen sich weiterhin neue Funktionen, welche die ursprünglichen Speichersystemen nicht bieten, realisieren. Dazu zählen beispielsweise Snapshots, Deduplikation und Thin Provisioning. Speichervirtualisierung eröffnet zudem die Möglichkeit, Speicher verschiedener Kategorien in Hierarchien zu organisieren, was wiederum als Grundlage für Information Life Cycle Management (ILM) dient. [vgl. BKNT11, S. 16, BIT12b, S. 6ff.]

Netzwerkvirtualisierung Es existieren unterschiedliche Ansätze sowohl auf Software- als auch Hardwareebene, um die Netzwerkinfrastruktur in logische Einheiten aufzuteilen. Dabei bildet ein physisches Netzwerk die Basis für mehrere voneinander unabhängige logische Netzwerke. Netzwerkvirtualisierung bietet hohe Flexibilität, Skalierbarkeit, Sicherheit und vereinfachtes Management.

Zentrale Schnittstelle der Netzwerkvirtualisierung in virtuellen Umgebungen sind virtuelle Switches im Hypervisor. Diese abstrahieren die physischen am Server anliegenden Netzwerverbindungen und stellen sie den VMs zur Verfügung. Komplexe Netzwerkinfrastrukturen lassen sich so bereits auf dem Virtualisierungs-Host abbilden. Das ermöglicht mandantenfähige Architekturen auf dem Hypervisor, wie sie beispielsweise das BSI oder die International Organization for Standardization (ISO) fordern. Virtuelle Switches stehen hinsichtlich ihres Funktionsumfangs den klassischen Switches in nichts nach. Sie bieten sogar meist mehr Unter-

stützung für zukünftige Anforderungen, z.B. IPv6, Virtual Extensible LAN (VXLAN), Shortest Path Bridging (SPB) usw.

Virtual Local Area Networks (VLANs) unterteilen ein Netzwerk in voneinander abgeschirmte Segmente. Dabei werden Ports am Switch zu logischen Gruppen zusammengefasst. Alle Geräte in einem solchen isolierten virtuellen Netzwerk können nur mit Geräten aus demselben Segment kommunizieren. Ein physisches Netzwerk verhält sich also wie mehrere, nicht miteinander verbundene LANs.

Ein weiteres Beispiel für Netzwerkvirtualisierung liefern Virtual Private Networks (VPNs). Sie stellen ein Netzwerk dar, das zum Transport von (meist privaten) Daten ein öffentliches Netzwerk verwendet. Dabei tauschen die Anwender Daten wie in einem internen Netzwerk, obwohl sich beide nicht im selben Netzwerk befinden. Ermöglicht wird dieses durch die Nutzung spezieller Kommunikationsprotokolle. [vgl. Mey12]

Anwendungsvirtualisierung Diese Form wird auch als Applikationsvirtualisierung bezeichnet. Anwendungen lassen sich zentral verwalten und dem Anwender über ein Netzwerk anbieten, so dass die clientseitige Installation entfällt. Die Anwendung und alle zur Ausführung nötigen Komponenten und Dateien sind in einem Container untergebracht, von wo aus auch der Aufruf erfolgt. So lassen sich Konflikte mit anderen Programmen oder dem Betriebssystem vermeiden und die Softwareverteilung vereinfachen. Abbildung 2.6.3 stellt unter (a) beispielhaft zwei solcher Anwendungscontainer auf einem gemeinsamen Betriebssystem dar.

Anwendungen lassen sich durch einfaches Löschen des Containers entfernen. Der Start unterschiedlicher Versionen oder Instanzen einer Software ist auf diese Weise ebenfalls parallel möglich. Der Anwender erhält in der Regel einen Link auf den zentralen Speicherplatz (Application Streaming Server) der Anwendung. Aktiviert er diesen, wird die Anwendung geladen (Streaming) und ausgeführt. Dabei kann die Anwendung im Cache verbleiben, so dass keine dauerhafte Netzverbindung bestehen muss.

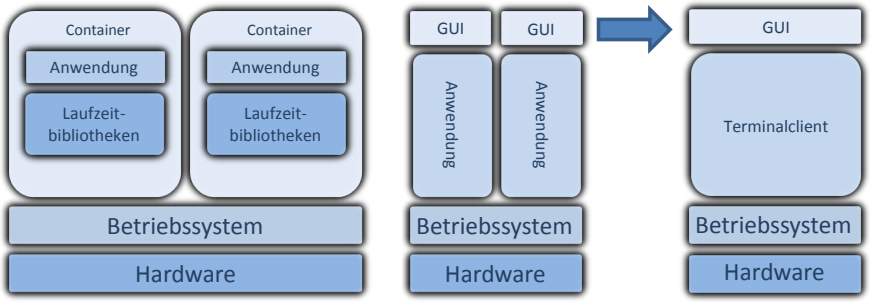
Vorteile bietet die Anwendungsvirtualisierung durch einfache und zentrale Verwaltung, automatisches Update- und Patchmanagement, Lizenzverwaltung und globale Verfügbarkeit. Durch die Bereitstellung über ein Netzwerk, beispielsweise das Internet, ist der Anwender allerdings zum Starten der Anwendung abhängig von einer zuverlässigen Netzanbindung. [vgl. MWRS11, S. 24f.]

Präsentationsvirtualisierung Bei dieser Form der Virtualisierung erfolgt die Trennung von der Anzeige und der eigentlichen Ausführung der Anwendung. In einer virtuellen Benutzersitzung (Session) werden sowohl einzelne Anwendungen als auch ein Desktop eines

entfernten Rechners (Terminalserver) wiedergegeben. Beim Anwender erfolgt über geeignete Übertragungsfunktionen auf seinen verschiedenen Endgeräten nur noch die grafische Ausgabe. Die Abbildung 2.6.3 zeigt unter (b) einen beispielhaften Aufbau. Auf der Infrastruktur der linken Seite kommt eine Anwendung zur Ausführung. Der Client auf der rechten Seite dient nur für die grafische Ausgabe dieser Anwendung.

Die Verwaltung und Pflege erfolgt serverseitig. Am Client erfolgt lediglich die Einrichtung einer Verbindung zum jeweiligen Server. Bei dieser Form entfällt, wie bei der Anwendungsvirtualisierung, die Softwareverteilung.

Ein großer Vorteil ist, dass (sensible) Daten nicht mehr für ggf. Dritte erreichbar auf dem lokalen Arbeitsplatz gespeichert sind. Die Datenhaltung und Sicherung geschieht serverseitig, wodurch sich Sicherheit und Verfügbarkeit erhöhen lassen. Nachteilig ist, dass im Gegensatz zur Anwendungsvirtualisierung eine dauerhafte Netzverbindung zum Server bestehen muss. [vgl. MWRS11, S. 22f.]



(a) Anwendungsvirtualisierung (b) Präsentationsvirtualisierung

Abbildung 2.6.3: Anwendungs- und Präsentationsvirtualisierung [vgl. MWRS11, S. 11]

Desktopvirtualisierung Diese Form wird als Virtual Desktop Infrastructure (VDI) bezeichnet. Statt mehrere Benutzersitzungen auf einem Terminalserver zu hosten, erfolgt der Betrieb einer individuellen VM für jeden Anwender auf dem Server. Der Anwender greift über das Remote Desktop Protocol (RDP) von einem beliebigen Arbeitsplatz darauf zu und erhält nur noch die Bildschirmausgaben. Anders als bei der Präsentationsvirtualisierung, wo sich mehrere Anwender die Ressourcen eines Terminalservers teilen, bekommt der Anwender also eine vollständige Systemumgebung und einen eigenen Desktop zugewiesen.

Weiterhin bietet sich die Möglichkeit der zentralen Wartung und Pflege. Als Arbeitsplatzrechner können energiesparende Thin Clients zum Einsatz kommen. [vgl. BIT12a, S. 8]

2.6.1.2 Webservices

Eine weitere Grundvorraussetzung für Cloud-Dienste sind Webservices, da das Dienstangebot über Netzwerke auf Basis standardisierter Protokolle und APIs erfolgt. Webservices dienen dabei der Schaffung einer verteilten Softwarearchitektur. Eine Anwendung wird in einzelne Komponenten zerlegt, die sich an unterschiedlichen Orten befinden können. Diese sind nur lose über Verbindungen und Protokolle gekoppelt. Als Standard für die Formatierung von Nachrichten haben sich die Implementierungen SOAP/Web Services Description Language (WSDL) und Representational State Transfer (REST) durchgesetzt.

SOAP ist ein Nachrichtenprotokoll und WSDL die zugehörige Schnittstellenbeschreibungssprache. Zur Repräsentation der Daten wird Extensible Markup Language (XML) verwendet. Zum Senden von Nachrichten kann SOAP beliebige Transportprotokolle nutzen, beispielsweise Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP).

REST bezeichnet einen Architekturstil, der auf HTTP aufsetzt und die zugehörigen Methoden (GET, POST, PUT, DELETE usw.) verwendet. Neben XML können zur Repräsentation der Daten auch die Formate Hypertext Markup Language (HTML) und JSON verwendet werden. [vgl. BKNT11, S. 22ff.]

2.6.1.3 Serviceorientierte Architekturen

SOAs sind Strukturmuster, um Dienste in einem IT-System zu strukturieren und diese entkoppelt anbieten und nutzen zu können. Dabei sollen die Abhängigkeiten zwischen den Elementen eines verteilten Softwaresystems reduziert werden. Die einzelnen Dienste, meist Webservices, sind voneinander unabhängig.

Konkrete Dienstimplementierungen orientieren sich an Geschäftsprozessen. Ein Anwender legt Aufrufe und Datenaustausch verschiedener Dienste in einer bestimmten Reihenfolge fest. Die Zusammensetzung verschiedener Dienste zu einer Komposition beschreibt einen ausführbaren Geschäftsprozess (Orchestrierung). Auf diese Weise lassen sich flexibel weitere Dienste erstellen.

Die verfügbaren Dienste trägt der jeweilige Dienstanbieter in ein Dienstverzeichnis ein und veröffentlicht diese. Ein Dienstnutzer kann dann eine Suchanfrage mit seiner Anforderungsspezifikation an das Dienstverzeichnis senden und erhält als Rückmeldung die Adresse, unter der er auf den Dienst zugreifen kann. Es ist somit eine lose Kopplung zur Laufzeit möglich. Abbildung 2.6.4 zeigt nochmals die Teilnehmer und Aktionen innerhalb einer SOA. [vgl. Gö12]

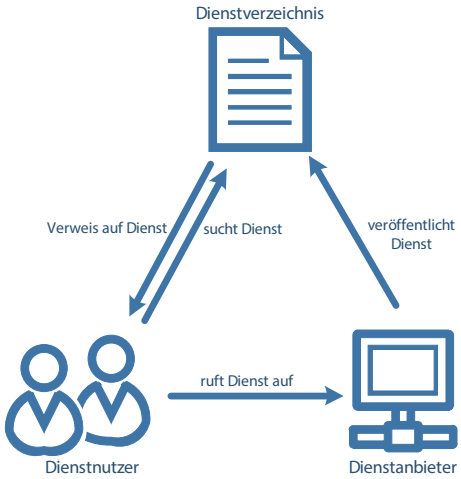


Abbildung 2.6.4: Teilnehmer und Aktionen einer SOA [vgl. BKNT11, S. 20]

2.6.2 Sicherheitsaspekte

Die Cloud bietet Anwendern und Unternehmen eine komplette IT-Infrastruktur oder Teile davon als Dienstleistung. Die Nutzung dieser Dienste beinhaltet natürlich den Transfer von Daten zum externen Dienstleister über das Internet. Davon sind auch vertrauliche Daten, wie beispielsweise personenbezogene Daten, Betriebsgeheimnisse oder die Buchhaltung, betroffen. Bevor diese Daten außerhalb des Unternehmens gespeichert werden, muss geklärt sein, wie die jeweiligen Anbieter die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit der Daten sowie die Verbindlichkeit durchgeführter Handlungen gewährleisten.

Vertraulichkeit ist der Schutz der Daten vor unautorisierter Einsicht (Geheimhaltung). Dies fordert die Festlegung von Berechtigungen und Kontrollen, so dass sichergestellt ist, dass keine nicht autorisierten Subjekte Zugriff auf gespeicherte Daten oder solche, die über ein Netzwerk übertragen werden, erlangen (Zugriffskontrolle). Berechtigungen zur Verarbeitung von Daten müssen vergeben und entzogen werden können, weiterhin muss die Einhaltung der Rechte kontrolliert werden. Zur Einhaltung der Vertraulichkeit kommen kryptografische Verfahren zur verschlüsselten Übertragung und Speicherung von Daten und Zugangskontrollen, die auf starker Authentifikation basieren, zum Einsatz.

Integrität meint den Schutz der Daten vor unautorisierter und unbemerkter Veränderung oder Löschung. Die Integrität von Daten bezeichnet deren Unverfälschtheit bzw. Vertrauenswürdigkeit. Die Veränderung von Daten bei einer Datenübertragung lässt sich nicht verhindern, daher zielen Verfahren zur Wahrung der Integrität auf das Erkennen von korrupten Daten ab.

Zum Einsatz kommen dabei kryptografische Verfahren, wie Signaturen, Hash-Funktionen und Message Authentication Codes (MACs).

Die Verfügbarkeit eines Systems ist die Wahrscheinlichkeit, dieses System zu einem bestimmten Zeitpunkt in einem funktionsfähigen Zustand anzutreffen. Sie bezeichnet den Schutz des Systems vor beabsichtigten oder unbeabsichtigten Störungen. Ein Cloud-Computing-System soll stets den vereinbarten Zugriff auf die genutzten Ressourcen bieten. IT-Systeme, die unternehmenskritische Prozesse unterstützen, müssen zuverlässig und hochverfügbar sein. Dabei darf die Verfügbarkeit nicht durch unautorisierte Aktionen oder Angriffe von intern oder extern beeinträchtigt werden, beispielsweise durch Überlastungsangriffe (Denial of Service (DoS)). Realisiert wird die Verfügbarkeit z.B. durch redundant ausgelegte Hardware und die verteilte Speicherung oder Replikation der Datenbestände in verschiedene Rechenzentren.

Verbindlichkeit oder auch Nichtabstreitbarkeit meint, dass sich durchgeführte Handlungen eindeutig zurechnen lassen und damit kein nachträgliches Abstreiten mehr möglich ist. Erreichbar ist dies beispielsweise durch den Einsatz elektronischer Signaturen.

Die Erfüllung dieser Schutzziele muss der Anwender mit dem jeweiligen Dienstanbieter in SLAs aushandeln. [vgl. TV11, S. 78ff.]

Da beim Cloud-Computing mit Virtualisierungstechniken gearbeitet wird, muss der Anbieter in der Lage sein, sowohl die physische als auch die virtuelle Infrastruktur zu schützen. Besonders bei mandantenfähigen Architekturen, wo die Infrastruktur der gemeinsamen Nutzung von verschiedenen Prozessen, Anwendungen und Unternehmen unterliegt, spielt die Isolation virtueller Instanzen eine wichtige Rolle. [vgl. MWRS11, S. 41]

Bei den Servicemodellen im Cloud-Computing gelten aufgrund der Offenheit der verschiedenen Ansätze unterschiedliche Verantwortlichkeiten. Bei IaaS hat man den Vorteil der größtmöglichen Flexibilität, muss sich jedoch um den Sicherheitsaspekt weitestgehend selbst kümmern. Der Anbieter ist nur für die physische Sicherheit verantwortlich. Bei den höheren Ebenen verschiebt sich diese Verantwortung allerdings zu Gunsten des Anwenders. Bei PaaS hat man mittlere Flexibilität, aber die Verantwortung für Sicherheit liegt gleichermaßen auf beiden Seiten. SaaS bietet am wenigstens Flexibilität, dafür liegt die Verantwortung für Sicherheit nahezu ausschließlich auf der Seite des Anbieters. Man legt damit allerdings zunehmend mehr Verantwortung in die Hände des Cloud-Computing-Anbieters. [vgl. BKNT11, S. 85]

Cloud-Computing-Umgebungen lassen sich genauso sicher gestalten wie IT-Umgebungen innerhalb eines Unternemens. Dabei kann Cloud-Computing sogar sicherer sein als der Betrieb eigener Infrastruktur im Unternehmen. Die Betreiber großer Rechenzentren investieren viel in die Sicherheit und beschäftigen teilweise ganze Abteilungen, die sich ausschließlich um die Aktualisierung und Verbesserung der Sicherheit kümmern. Betreiber verfügen über viel

Erfahrung und gute technische Ausstattung, um Daten und Systeme vor potenziellen Gefahren zu schützen. Wichtig sind hier Standards und Zertifizierungen nach ISO/IEC[13] 2700x, BSI IT-Grundschutz und IT Infrastructure Library (ITIL). Besonders kleine und mittelständische Unternehmen (KMU) profitieren in diesem Fall vom Cloud-Computing. Die Sicherheitsstandards sind auf Großkunden ausgelegt, aber auch für KMUs verfügbar. Die Ablage von verschlüsselten Daten in der Cloud kann somit sicherer sein, als die unverschlüsselte Speicherung lokal im Unternehmen. [vgl. RM10, S. 74, TV11, S. 75]

Die Sicherheit im Cloud-Computing hängt aber nicht nur von den technischen Gegebenheiten ab. Oftmals veröffentlichen die Anbieter zwar ihre Sicherheitsrichtlinien, schließen aber die Möglichkeit eines Besuches vor Ort, wo sich der Kunde persönlich von der Gewährleistung der Informationssicherheit überzeugen könnte, aus. Somit ist Cloud-Computing eine Frage des Vertrauens. Selbst wenn man davon ausgehen kann, dass der Anbieter in der Lage ist die Schutzziele einzuhalten, muss der Kunde darauf vertrauen können, dass die Daten nicht durch den Anbieter für z.B. eigene Zwecke missbraucht werden. [vgl. MWRS11, S. 41f.]

2.6.3 Rechtliche Aspekte

Neben dem Interesse von Unternehmen, die eigenen Daten zu schützen, gibt es bei bestimmten Datenbeständen zusätzlich gesetzliche Vorschriften und Branchenstandards, wie diese zu behandeln und zu speichern sind. Aufgrund dieser eindeutigen und messbaren Sicherheitsbestimmungen müssen Unternehmen nachweisen, wie sie Daten verarbeiten und speichern. Die Einhaltung von Verhaltensmaßregeln, Gesetzen und Richtlinien im IT-Bereich wird als IT-Compliance bezeichnet. Die Erhebung, Verarbeitung und Nutzung von beispielsweise personenbezogenen Daten regelt in Deutschland insbesondere das Bundesdatenschutzgesetz (BDSG). Ergänzt wird das BDSG durch das Landesdatenschutzgesetz (LDSG), Telemediengesetz (TMG), Telekommunikationsgesetz (TKG) und Sozialgesetzbuch (SGB). [vgl. BKNT11, S. 88]

Aufgrund ihrer Verfügbarkeit und lastabhängigen Verteilung sind Clouds oftmals grenzüberschreitend. Häufig ist daher der genaue Ort der Speicherung und Verarbeitung von Daten nicht bekannt. Dies führt zu neuen Herausforderungen bezüglich der Einhaltung von Gesetzen und Richtlinien. Die Datenschutzrichtlinien innerhalb der EU sind allerdings weitestgehend vereinheitlicht. Daher gelten innerhalb der EU-Grenzen keine Besonderheiten gegenüber der rein innerdeutschen Speicherung. Anders sieht es aus, wenn Daten in Ländern außerhalb der EU gespeichert oder verarbeitet werden. Sie unterliegen hier mit hoher Wahrscheinlichkeit länderspezifischen und damit anderen Datenschutzbestimmungen. Als Beispiel sei hier der USA PATRIOT Act genannt. Sobald ein Cloud-Anbieter seinen Firmensitz in den USA hat,

[13] ISO/IEC Information Centre: http://www.standardsinfo.net

haben dortige Ermittlungsbehörden jederzeit die Möglichkeit, auf Daten innerhalb dessen Cloud zuzugreifen. Dabei ist es unerheblich, ob die zugehörigen Server in den USA oder z.B. in Europa stehen. [vgl. MWRS11, S. 42, iX12]

Nach dem BDSG bleibt der Cloud-Anwender gesetzlich verantwortlich für die Verarbeitung der von ihm in die Cloud übertragenen Daten. Dieser muss selbstständig prüfen, ob technische und organisatorische Vorkehrungen des jeweiligen Anbieters ausreichend sind, um die Anforderungen an die IT-Compliance zu gewährleisten. Aus diesem Grund offerieren einige Cloud-Anbieter, ihre Dienste auf bestimmte Regionen zu begrenzen. Amazon bietet bei seinen Cloud-Diensten beispielsweise die Regionen USA, Europa und Asien an, so dass sich durch geeignete Wahl der Rechtsraum für Dienste festlegen lässt.

Viele Cloud-Anbieter schließen aber die Gewährleistung der Sicherheit aus, die über die Überprüfung des Sicherheitspersonals und die Sicherheit beim Übergang zwischen dem Anbieternetz und dem Internet hinaus geht. [vgl. BKNT11, S. 88f., MWRS11, S. 42]

2.6.4 Wirtschaftliche Aspekte

Die Frage, ob Cloud-Computing grundsätzlich Einsparpotenzial für ein Unternehmen mit sich bringt, kann nicht allgemein beantwortet werden, da sich viele verschiedene Faktoren auf die Wirtschaftlichkeit auswirken. Daher müssen Unternehmen in jedem speziellen Fall den Einsatz von Cloud-Computing individuell abwägen. Prinzipiell bietet Cloud-Computing aber viele Vorteile gegenüber herkömmlichen Lösungen und kann sehr wohl ein Erfolgsfaktor sein und erhebliche Kostenvorteile einbringen.

Durch mandantenfähige Architekturen können sowohl Anbieter einer Cloud als auch deren Nutzer profitieren, da die Ressourcennutzung effizienter erfolgt. Auf Anbieterseite besteht die Möglichkeit, durch Konsolidierung von Ressourcen die Betriebskosten für z.B. Hardware, Software, Sicherheit und Wartung zu senken. Die Nutzer profitieren von Skaleneffekten (Economies of Scale), da die anfallenden Nutzungskosten mehrere Kunden gleichzeitig tragen. [vgl. MRV11, S. 62]

Cloud-Computing bietet den Nutzern Skalierbarkeit und Flexibilität bei der Nutzung von Ressourcen. Anwender können zusätzlich benötigte Ressourcen jederzeit abfordern oder überflüssige abstoßen. Dabei kann diese Anpassung sehr feingranular und unverzüglich erfolgen, es vergehen dabei meist nur Minuten und nicht Wochen oder Monate. Für den Nutzer minimiert sich durch diese Elastizität das Risiko, hohe Ressourcen für seltene Lastspitzen vorhalten zu müssen (overprovisioning), die nicht effizient ausgelastet sind (underutilization) bzw. über zu wenig Ressourcen zu verfügen (underprovisioning) und anstehende Lastspitzen nicht abdecken zu können (saturation). [vgl. BKNT11, S. 118]

Der IT-Bereich ist durch kurze Innovationszyklen geprägt und komplexe Softwarelösungen erfordern leistungsfähige Hardware. Durch die schnelle Nutzbarkeit und die Möglichkeit zur Anpassung an die eigenen Anforderungen verkürzen Cloud-Dienste die Amortisierungszeit für den Nutzer. Längerfristige Beschaffungs- und Verteilungsprozesse entfallen. Die implementierten Dienste können so schneller einen Mehrwert generieren. Insbesondere KMUs profitieren so von der Möglichkeit, Zugang zu neuen Technologien zu erhalten, die andernfalls nur durch hohe Investitionen für große Unternehmen zugänglich waren.

Das Pay-as-you-go-Modell bietet den Unternehmen eine dynamische Anpassung von Ressourcen und die anschließende nutzungsabhängige Abrechnung. Dadurch lassen sich Fixkosten reduzieren und in operative Kosten (Betriebskosten) umwandeln. Dieses Modell basiert auf der zeitverteilten, tatsächlichen Nutzung von Ressourcen. In der Abrechnung für einen Cloud-Dienst sind in der Regel sämtliche Kosten enthalten, beispielsweise für Hardware, Nutzungsentgelte für Anwendungen (Lizenzkosten), Updates und Support.

Demgegenüber steht das Anschaffungs- oder Leasingmodell. Hier werden Ressourcen auf Dauer gekauft oder über einen definierten, meist längerfristigen, Zeitraum angemietet und abgerechnet. Die Abrechnung geschieht dabei unabhängig von der tatsächlichen Nutzung. Ein Unternehmen muss also zunächst in Hard- und Software investieren, bevor sich neue Technologien erschließen lassen. Beim Cloud-Computing hingegen entstehen keine Investitions- oder Leasingkosten, lediglich Betriebskosten. Durch Cloud-Computing lässt sich eine geringere Kapitalbindung in IT-Ressourcen erzielen und damit einhergehend eine Variabilisierung der langfristigen Fixkosten. [vgl. Lip11, S. 15, MRV11, S. 64f.]

Als nachteilig und problematisch für den Nutzer gelten oft fehlende standardisierte Schnittstellen. Dadurch erschwert sich das einfache Wechseln von Anbietern und verursacht unter Umständen hohe Wechselkosten (Vendor-Lock-in). Die Abhängigkeit eines Nutzers vom Cloud-Anbieter wächst dabei mit der Menge an Daten, die bereits dorthin transferiert wurden. Ändert beispielsweise ein Anbieter seine Preispolitik, kann der Nutzer nicht ohne Weiteres den Anbieter wechseln. Der Wechsel ist zum einen mit hohen Kosten für die Übertragung der Daten verbunden, da in der Regel nach Übertragungsvolumen abgerechnet wird, und zum anderen verfügen Anbieter meist über eigene proprietäre Schnittstellen. Für bestehende Anwendungen und Dienste muss also erst eine Anpassung an die APIs des neuen Anbieters erfolgen. [vgl. Lip11, S. 16, MWRS11, S. 41]

3 Vorstellung der Cloudstack-Produkte

Im folgenden Kapitel bietet der Verfasser einen Überblick über die Produkte der Hersteller Citrix und VMware zur Realisierung von Cloud-Umgebungen. Die benötigten Produkte bzw. Produktgruppen zum Aufbau von IaaS-Cloud-Umgebungen sind bei den hier betrachteten Herstellern deutlich erkennbar als solche am Markt positioniert. Für den Aufbau einer PaaS- oder SaaS-Cloud-Umgebung fehlt teilweise eine klare Abgrenzung der benötigten Produkte seitens der Hersteller. Weiterhin positionieren sich die Hersteller aber nicht oder nicht eindeutig in allen Bereichen des Cloud-Computings. Schwerpunkt der vorgestellten Produkte ist daher der gemeinsame und damit vergleichbare Bereich IaaS. Der Fokus liegt dabei auf den Kernkomponenten für die Realisierung einer IaaS-Cloud-Umgebung.

3.1 Citrix

3.1.1 XenServer 6.1

XenServer ist die kommerzielle Virtualisierungsplattform von Citrix und basiert auf dem Open-Source-Hypervisor Xen[14]. Zusätzlich zu einer freien Version bietet Citrix weitere kostenpflichtige Versionen an, die den Funktionsumfang und Service erweitern.

XenServer ist ein Typ-1 (Bare Metal) Hypervisor und läuft direkt auf der Hardware. Nach dem Start des Hypervisors startet in der ersten VMs, auch Control Domain (dom0) genannt, i.d.R. ein angepasstes Linux mit speziellen Privilegien für den Zugriff auf die physische Hardware. In dieser Ebene laufen die Gerätetreiber, weiter sind zwei APIs implementiert: Xen Management API (XAPI) als Managementschnittstellen für VMs und Ressourcen sowie Storage Manager API (SMAPI) für die Anbindung von Datenspeicher. XenServer bietet die Möglichkeit zur vollständigen Virtualisierung, z.B. für Windows Betriebssysteme, und Paravirtualisierung, wodurch angepasste Gastsysteme dann nahezu native Performanz bieten. [vgl. Xen13]

Für die Konfiguration und Verwaltung von Hosts mit XenServer kommt die Verwaltungsanwendung XenCenter unter Windows zum Einsatz. Damit lassen sich neben Hosts auch VMs überwachen und verwalten. Über das XenCenter lassen sich zusätzliche Funktionen,

[14]Xen Open-Source-Projekt: http://www.xenproject.org

wie Hochverfügbarkeit und Disaster Recovery, nutzen. Anders als beim vCenter Server von VMware werden die Konfigurationsdaten nicht in einer zentralisierten Datenbank gehalten, sondern über alle XenServer Hosts in einem Ressourcenpool verteilt gespeichert, um einen Single Point of Failure zu vermeiden. Tatsächlich ist XenCenter damit nur ein Client. [vgl. Cru12]

3.1.2 CloudPlatform 3.0.6

CloudPlatform dient laut Citrix für die Bereitstellung und Verwaltung von Public-, Private- und Hybrid-IaaS-Clouds und basiert auf dem Open-Source-Projekt Apache CloudStack[15]. Es ist die von Citrix kommerziell unterstützte Version, basierend auf dem Apache CloudStack, die Unterstützung seitens des Herstellers Citrix sowie das Nutzungsrecht für XenServer Advanced mitbringt.

Eine CloudPlatform Installation besteht aus dem Management Server und der zugrunde liegenden Infrastruktur. Ressourcen, wie z.B. Hosts, Datenspeichergeräte oder IP-Adressbereiche, fügt man dem Management Server hinzu, der diese dann verwaltet. CloudPlatform fasst Rechenressourcen in Pools zusammen und dient der zentralen Verwaltung dieser Ressourcen. CloudPlatform ist dabei mandantenfähig, unterstützt diverse Hypervisoren für den Einsatz in Umgebungen mit heterogenen Systemen, bietet Möglichkeiten für den Selfservice und weitere Schnittstellen, beispielsweise zur Ermittlung detaillierter Daten für eine verbrauchsabhängige Kostenerfassung und Dokumentation der genutzten Ressourcen. Laut Citrix lassen sich Cloud-Computing-Umgebungen erstellen und über eine einzige Plattform verwalten. CloudPlatform bildet dabei die Grundlage für weitere Dienste, wie Desktop as a Service oder PaaS. [vgl. Cit13a, Cit13b, S. 3ff.]

3.1.3 CloudPortal Business Manager 2.0

CloudPortal Business Manager erweitert bestehende IaaS-Clouds auf der Basis von CloudPlatform um ein eigenes Selfservice-Portal zur Betriebsunterstützung, Verwaltung und Dienstbereitstellung. Mit CloudPortal Business Manager erfolgt dann die Nutzerverwaltung von Anwendern samt Ticketsystem und weiteren CRM-Funktionen. Dienste werden samt Preismodell in Katalogen gruppiert und veröffentlicht. Laut Citrix lassen sich Arbeitsflüsse für das operative Geschäft oder bei der Dienstbereitstellung automatisieren und orchestrieren, so dass Anwender ohne Unterstützung durch Dritte selbstständig Dienste auswählen, buchen und nutzen können. Sie sind in der Lage, in Eigenregie ihr Benutzerkonto, Ressourcen und Dienste zu

[15] Apache CloudStack: http://cloudstack.apache.org

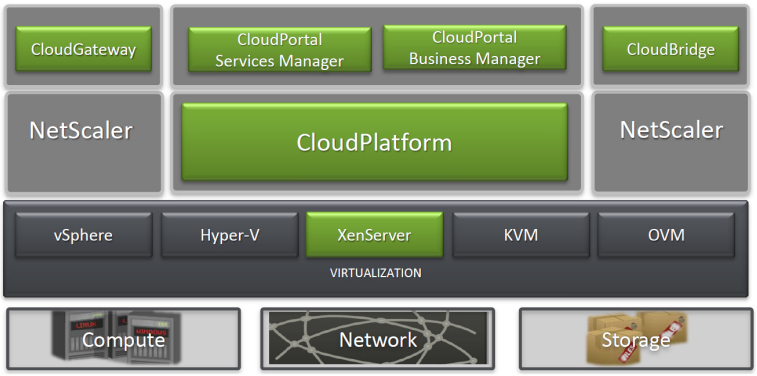


Abbildung 3.1.1: Citrix Cloud-Übersicht [vgl. Fer12]

verwalten. Weiterhin erhalten Administratoren und Anwender einen umfassenden Überblick über die Cloud bzw. ihre genutzten Dienste. Die verbrauchsabhängige Kostenerfassung und das anschließende Rechnungswesen erfolgt ebenfalls über den CloudPortal Business Manager. Über das zugehörige Software Development Kit (SDK) und die CloudPlatform API können Dienste über IaaS hinaus erstellt und in bestehende oder externe Unternehmenssysteme angebunden werden. [vgl. Cit13d, Cit13c]

3.1.4 NetScaler 10

NetScaler optimiert die Bereitstellung von Anwendungen und Web-Applikationen über das Internet oder private Netzwerke und bietet weitere Optimierungen, Sicherheit auf Anwendungsebene und Verwaltung des Netzwerkverkehrs. Sämtliche Verbindungen der betreffenden Server werden durch NetScaler geleitet. Die aktivierten Eigenschaften und festgelegten Richtlinien wendet NetScaler dann auf den ein- und ausgehenden Datenverkehr an. Zu den Funktionen von NetScaler zählen unter anderem Routing, Load Balancing, Content Switching, Application Layer Firewall mit Content Filter und Schutz vor DoS-Angriffen. [vgl. Cit12b]

3.1.5 CloudBridge 2.0

CloudBridge verbindet unternehmenseigene Rechenzentren mit externen Rechenzentren oder den Amazon Web Services (AWS) und erweitert so das Unternehmensnetzwerk über einen gesicherten Tunnel. Auf diese Weise kann CloudBridge laut Citrix das Unternehmensnetzwerk um Angebote aus der Public Cloud erweitern oder eine bestehende Private Cloud mit entsprechenden Angeboten zu einer Hybrid Cloud erweitern. Das Produkt ist als eigenständige physische Appliance, virtuelle Appliance oder integriert in NetScaler Platinum verfügbar. [vgl. Cit12a]

3.2 VMware

3.2.1 vCloud Suite 5.1

Laut Hersteller vereint die vCloud Suite alle Komponenten, die Anwender benötigen, um Cloud-Infrastrukturen aufzubauen, zu betreiben und zu verwalten. Dieses Produkt baut auf der Grundlage der Virtualisierung von VMware auf und weitet das Konzept auf das gesamte Rechenzentrum aus. VMware spricht dabei vom Software Defined Data Center. Dienste aus den Bereichen Speicher, Netzwerk, Sicherheit und Verfügbarkeit werden abstrahiert und in Pools zusammengefasst. So sollen sich sehr einfach virtuelle und flexible Rechenzentren erstellen lassen. [vgl. VMw13c, Hal12, S. 1]

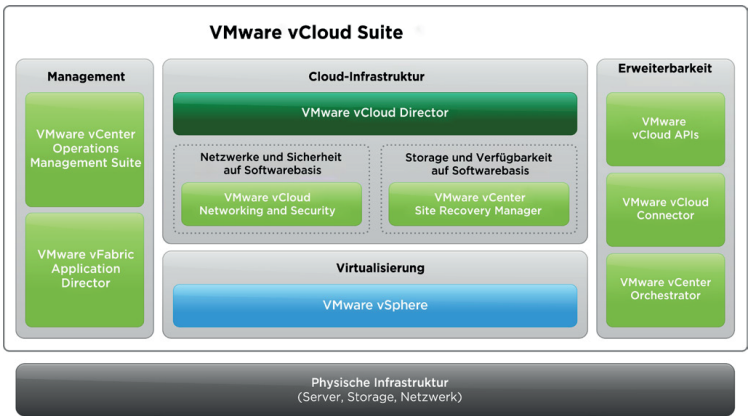


Abbildung 3.2.1: VMware vCloud Suite [VMw13c]

3.2.1.1 vSphere 5.1

VMware vSphere ist die Virtualisierungsplattform für x86-basierte Computersysteme und dient gleichzeitig als Grundlage für den Aufbau von VMware Cloud-Infrastrukturen. Zentrales Element ist der vSphere ESXi Hypervisor, der seit vSphere 5 als einziger Hypervisor verfügbar ist. Dabei handelt es sich um einen Bare Metal Hypervisor. Offiziell wird vSphere ESXi generell nur auf zertifizierter Hardware unterstützt. Der Hypervisor ist in zwei Varianten verfügbar: als vSphere Hypervisor (kostenlos) und als vSphere (kostenpflichtig). Der Unterschied liegt dabei im Funktionsumfang. Über eine SOAP API bietet der Hypervisor die Möglichkeit zur Administration, z.B. mit Hilfe des kostenlosen vSphere-Clients oder dem vSphere-Webclient. [vgl. Low11]

Zu den wichtigsten Funktionen von vSphere zählen:

- **vSphere vMotion und Storage vMotion**: Ermöglicht die Migration von VMs bzw. deren Laufwerken zwischen Hosts bzw. Datenspeichern im Betrieb und ohne Ausfallzeiten.
- **vSphere Distributed Resources Scheduler (DRS) und Storage DRS**: Automatischer Lastenausgleich zwischen Host und Storage.
- **vSphere High Availability und Fault Tolerance**: Erhöht die Verfügbarkeit von Anwendungen, Infrastruktur und Management. Beim Ausfall eines physischen Servers startet High Availability die betroffenen VMs auf einem anderen Host des Clusters automatisch neu. Fault Tolerance bietet eine unterbrechungsfreie Verfügbarkeit durch eine Schatteninstanz der zu schützenden VM auf einem anderen Host im Cluster. Bei einem physischen Ausfall erfolgt ein automatischer Failover ohne Ausfallzeit.
- **vShield Zones und Endpoint**: Dieses Produkt bietet Firewallfunktionen und die Auslagerung von Virenschutzfunktionen auf eine zusätzliche VM. [vgl. ZWS+12, S. 44ff.]

vCenter Server Mit einer einzigen Konsole bildet der vCenter Server die zentrale Management-Schnittstelle für vSphere-Umgebungen. Über den vCenter Server lassen sich weitere Produkte (z.B. vCenter Site Recovery Manager, vCenter Operations Manager) und Funktionen (z.B. vMotion, High Availability, DRS) aktivieren. Der vCenter Server ist allerdings kein Bestandteil der vCloud Suite und muss gesondert erworben werden. [vgl. ZWS+12, S. 56]

3.2.1.2 vCloud Director 5.1.1

VMware vCloud Director ist ein zentraler Bestandteil einer VMware Cloud und dient hier zur Automatisierung und Verwaltung. Der vCloud Director setzt auf der Virtualisierungsplattform vSphere auf. Als weitere Abstraktionsschicht fasst dieser die vorhandenen virtuellen Infrastruktur-Ressourcen in virtuellen Rechenzentren zusammen. Ein virtuelles Rechenzentrum besteht dabei aus Rechen-, Netzwerk- und Datenspeicherressourcen. Weiterhin ist der vCloud Director mandantenfähig und die einzelnen virtuellen Rechenzentren können so direkt Nutzern zugeordnet werden. Auf diese Weise können verschiedene Organisationen, Geschäftsbereiche, Abteilungen usw. dieselbe Infrastruktur isoliert voneinander nutzen. [vgl. VMw13j, VMw12b, S. 11ff]

3.2.1.3 vCloud Connector 2.0

Laut VMware dient der vCloud Connector zum Betreiben und Verwalten von Hybrid Clouds, die auf VMware vSphere und vCloud Director basieren. VMware Private Clouds kann der vCloud Connector mit Public Clouds, betrieben durch zertifizierte vCloud-Anbieter, zu einer Hybrid Cloud verbinden. VMs, vApps und virtualisierte Anwendungen können zwischen den einzelnen Clouds migriert werden. Für das Management sorgt ein zentrales Interface, entweder über den vSphere-Client oder einen Webbrowser (`vcloud.vmware.com`). [vgl. Hal12, S. 2, VMw13e]

3.2.1.4 vCloud Networking & Security 5.1.2

vCloud Networking & Security ist laut VMware ein softwaredefiniertes Netzwerk- und Sicherheitsprodukt, das es Anwendern ermöglicht, logische Netzwerke zu erstellen, zu verwalten und zu überwachen. Ähnlich dem Pooling von Rechenressourcen bei vSphere, abstrahiert und fasst vCloud Networking & Security Netzwerke und Sicherheitsfunktionen in Ressourcenpools zusammen. Mit Diensten wie VXLAN, VPN, Firewall, Isolation von Netzwerken und Load Balancing ist vCloud Networking & Security eine Schlüsselkomponente für mandantenfähige Umgebungen. [vgl. VMw13f]

Zu den wichtigsten Merkmalen von vCloud Networking & Security zählen:

- **Edge**: Bietet portbasierte Firewall-Funktionen und Gateway-Dienste, wie Load Balancing, VPN, NAT und DHCP zur Absicherung des virtuellen Rechenzentrums (Perimeterschutz).
- **App Firewall**: Firewall für VMs und Anwendungen, segmentiert und isoliert diese voneinander.
- **VXLAN**: Technologie für Netzwerkvirtualisierung und -abstraktion, Elastizität und Skalierung im gesamten Rechenzentrum. [vgl. VMw12a, S. 7ff, VMw13b]

Genutzt wird vCloud Networking & Security mit virtuellen Appliances. Durch diese wird der Netzwerkverkehr geleitet und Dienste wie Firewall und Load Balancing werden angewendet. Weiterhin lassen sich über RESTful APIs weitere Netzwerk- und Sicherheitsprodukte von Drittanbietern einbinden, die dann ebenfalls über diese Appliances Zugang zum Netzwerkverkehr haben. [vgl. VMw13k]

3.2.1.5 vCloud Automation Center 5.1

Das vCloud Automation Center dient der automatischen Bereitstellung von Diensten auf verschiedenen Virtualisierungsplattformen. Dabei soll es Anwender unterstützen, die Bereit-

stellung und das Lifecycle-Management von Diensten oder VMs automatisiert zu steuern. Für die Verwaltung bietet es ein Selfservice-Portal und integriert sich zudem in den vCloud Director und den vCenter Orchestrator.

Das vCloud Automation Center erlaubt eine auf Richtlinien basierende Bereitstellung von Diensten für VMware basierte Private Clouds und Public Clouds, physische Infrastrukturen (DELL[16], HP[17], Cisco[18]), zusätzliche Hypervisoren und AWS (Elastic Compute Cloud (EC2)). Dieses Produkt stammt aus der Übernahme der Firma DynamicOps durch VMware im Juli 2012[19]. [vgl. VMw12d, Som12]

3.2.1.6 vFabric Application Director 5.0

Der vFabric Application Director soll die Konfiguration und Bereitstellung von VMs für mehrstufige Anwendungen (vApps) über eine einfache Oberfläche ermöglichen. Anwender wählen alle für die Anwendung erforderlichen Komponenten wie Betriebssystem, Middleware und Datenbanken aus und haben die Möglichkeit, diese Konfiguration für den späteren Gebrauch zu speichern. Auf dieser Basis lassen sich dann weitere Instanzen der Anwendungen erzeugen. Die erstellten Anwendungen eignen sich für den Betrieb in verschiedenen Public-Cloud- bzw. Private-Cloud-Umgebungen, z.B. AWS. [vgl. Som12, Har12]

3.2.1.7 vCenter Site Recovery Manager 5.1.0.1

Der Site Recovery Manager erweitert den vCenter Server um automatisches Disaster Recovery für eine VMware Infrastruktur. Benötigt werden dafür zwei physisch getrennte Rechenzentren, die jeweils auf vSphere basieren und mit vCenter Server verwaltet werden. Der Site Recovery Manager integriert sich in die Oberfläche des vCenter Servers. Dort wählt man aus, welche VMs im Ernstfall im Notfallrechenzentrum gestartet werden sollen und in welcher Reihenfolge. Der Site Recovery Manager bietet keine Hochverfügbarkeitsfunktionen, sondern Replikation der VMs und Datenspeicher. Im Notfall werden die selektierten VMs im Notfallrechenzentrum in definierter Reihenfolge gestartet und der Normalbetrieb fortgeführt. Weiterhin lassen sich Notfallszenarien im Vorwege simulieren, um den Ernstfall zu proben. [vgl. ZWS+12, S. 1091f.]

[16] Dell: http://www.dell.com
[17] Hewlett-Packard Company: http://www.hp.com
[18] Cisco Systems, Inc.: http://www.cisco.com
[19] Übernahme von DynamicOps durch VMware: http://www.vmware.com/de/company/acquisitions/dynamicops.html

3.2.2 vCenter Operations Management Suite 5.7

Die vCenter Operations Management Suite erweitert das vCenter um Funktionen zur Planung und Überwachung virtueller sowie Cloud-Infrastrukturen. Die wichtigsten Aufgaben umfassen die Leistungsüberwachung und das Kapazitätsmanagement, die Sicherstellung der Einhaltung von Richtlinien und definierten Konfigurationen und das Auffinden von Leistungsengpässen. Die vCenter Operations Management Suite ist Bestandteil der vCloud Suite. [vgl. VMw13i]

3.2.2.1 vCenter Chargeback Manager 2.5

Der vCenter Chargeback Manager ermöglicht eine verbrauchsabhängige Kostenerfassung samt Analyse und Dokumentation für genutzte Ressourcen. Damit bietet dieser einen Einblick in die tatsächlich anfallenden Kosten für die benötigte virtuelle Infrastruktur. [vgl. ZWS+12, S. 1084]

3.2.2.2 vCenter Operations Manager 5.7

Der vCenter Operations Manager sammelt und analysiert Daten auf jeder Ebene der virtuellen Infrastruktur, unter anderem vom Hypervisor, vCenter Server und vCenter Configuration Manager. Diese Daten dienen dem Performanz-, Kapazitäts- und Konfigurationsmanagement zur Sicherstellung der SLAs. So lassen sich in Echtzeit Informationen über den Status oder mögliche Problemquellen der virtuellen Umgebung abrufen. Über die Daten der Ressourcenauslastung erhält man Hinweise zur Anpassung der Ressourcen von VMs. Der vCenter Operations Manager kann weiter potentielle Probleme, z.B. durch Konfigurationsänderungen, erkennen und entsprechende Abhilfemaßnahmen vorschlagen. [vgl. VMw13a, VMw12c]

3.2.2.3 vCenter Configuration Manager 5.6

Der vCenter Configuration Manager dient der Automatisierung des Konfigurationsmanagements für virtuelle und physische Maschinen. Dieses Softwaremodul ist eine Configuration Management Database (CMDB), in der neben den Konfigurationen für die Virtualisierungshosts auch die Konfigurationen der Gastsysteme in den VMs erfasst werden. Über diese gespeicherten Daten und zusätzlich definierten Regelwerke lassen sich Compliance-Anforderungen bei Konfigurationsänderungen an den Systemen überwachen und automatisch korrigieren. In dem Rahmen verteilt der vCenter Configuration Manager unter anderem auch Patches, Updates und Anwendungen. Der vCenter Configuration Manager ist in der Lage, fehlende Software in einer VM zu erkennen, beispielsweise einen Virenscanner, und kann diesen automatisch nachinstallieren. Weiterhin können auf der Basis der Regelwerke Vorlagen für neue Systeme bereitgestellt werden. [vgl. VMw13g]

3.2.2.4 vCenter Infrastructure Navigator 2.0

Der Infrastructure Navigator erkennt automatisch Abhängigkeiten zwischen den Anwendungen und der Infrastruktur. Diese Abhängigkeiten von Ressourcen der virtuellen Infrastruktur stellt er grafisch dar. So erhält man einen Überblick über die auf der virtuellen Infrastruktur ausgeführten Anwendungsdienste samt Abhängigkeiten. Dazu zählen beispielsweise alle beteiligten VMs einer mehrstufigen Anwendung (siehe dazu Abschnitt 3.2.1.6), vApps, die Visualisierung der Kommunikationspfade oder Informationen über genutzte Datenspeicher. [vgl. VMw13h]

3.2.2.5 vFabric Hyperic 5.0

vFabric Hyperic ist die Monitoringkomponente der Cloud-Anwendungsplattform VMware vFabric und dient der Performanz- und Verfügbarkeitsüberwachung von Webanwendungen in physischen, virtuellen und Cloud-Umgebungen. Es eignet sich dabei für das Management einer Vielzahl an Produkten, z.B. Anwendungsserver, Webserver, Datenbanken, Betriebssysteme, Hypervisoren, Messaging- und Verzeichnisserver usw. [vgl. VMw13d]

4 Analyse der vorgestellten Produkte

Die in Kapitel 3 vorgestellten Produkte fokussieren den Bereich IaaS. Der Schwerpunkt dieses Kapitels liegt daher in der Überprüfung, inwieweit sich IaaS-Cloud-Umgebungen mit den Produkten der Hersteller realisieren lassen. Dabei wird geprüft, ob und wie die Produkte die in Abschnitt 2.5 definierten Kriterien für Cloud-Computing nach NIST erfüllen und welche Bereitstellungsmodelle sich realisieren lassen.

4.1 Informationsgrundlage

Für die Analyse der Möglichkeit zum Aufbau einer IaaS-Cloud-Umgebung mit Produkten von VMware aus der vCloud Suite kann auf die Infrastruktur im Hause der Firma Silpion zurückgegriffen werden. Die hier bereits vorhandene vSphere-Umgebung lässt sich nutzen, um Teile der vCloud Suite direkt zu testen. Die Testumgebung besteht aus einem vCenter-Server-Cluster mit vSphere 5.1 ESXi Hosts. Folgende Produkte lassen sich, zum Teil mit Demo-Lizenzen, direkt analysieren:

- vSphere ESXi 5.1 (bereits bei Silpion im Betrieb, Vollversion)
- vCloud Director 5.1.1 (virtuelle Appliance, Testlizenz mit vollem Funktionsumfang)
- vCloud Connector 2.0 (virtuelle Appliance, Testlizenz mit vollem Funktionsumfang)
- vCloud Networking & Security 5.1.2 (virtuelle Appliance, Testlizenz mit vollem Funktionsumfang)

Zusätzliche Informationen zu den einzelnen Produkten stammen aus den jeweiligen Handbüchern des Herstellers und aus direktem Gespräch mit dem Hersteller. Insbesondere die Informationen zu den folgenden Produkten basieren auf den jeweiligen Handbüchern und Gesprächen mit VMware:

- vCenter Chargeback Manager 2.5
- vCloud Automation Center 5.1

- vFabric Application Director 5.0

Um zusätzlich zum eigenen Testaufbau die Möglichkeiten für den Aufbau einer Hybrid Cloud zu testen, lässt sich nach Rücksprache mit der Firma StratoGen[20] ein vCloud-Director-Zugang aus der Public Cloud in die Analyse einbinden.

Für die Analyse der Möglichkeit zum Aufbau einer IaaS-Cloud-Umgebung mit Produkten von Citrix werden folgende Produkte direkt analysiert:

- XenServer 6.1 (Testlizenz mit vollem Funktionsumfang)
- CloudPlatform 3.0.6 (Testlizenz mit eingeschränkter Hypervisorunterstützung)

Der Testaufbau besteht aus einem einfachen Netzwerk mit drei Computern. Zwei Computer dienen als Host mit XenServer und der dritte Computer mit dem Betriebssystem CentOS 6.4[21] als Management-Server mit der CloudPlatform-Installation. Zum Einsatz kommen Demo-Lizenzen, welche die sonst möglichen Hypervisoren auf XenServer und Kernel-based Virtual Machine (KVM)[22] begrenzen. Gespräche mit dem Hersteller und die verfügbaren Handbücher dienen zusätzlich als Informationsgrundlage. Insbesondere gilt dies für die Informationen hinsichtlich des CloudPortal Business Managers. Ein ähnliches Angebot für Demo-Zugänge zu CloudPlatform oder CloudPortal Business Manager aus der Public Cloud oder von Citrix waren während der Bearbeitung nicht verfügbar.

4.2 Bewertungsschema

Die in Abschnitt 2.5 beschriebene Definition von Cloud-Computing durch das NIST bietet einen guten Abgrenzungsrahmen, aber ebenfalls Spielraum für Interpretation. Das nachfolgende Bewertungsschema spiegelt die Interpretation und das Verständnis der NIST-Definition durch den Autor wider. Die vom NIST definierten Kriterien für Cloud-Computing, das IaaS-Servicemodell und die verschiedenen Bereitstellungsmodelle sind, sofern nötig, unterteilt in Subkriterien. Kriterien sind klassifiziert in Muss-Kriterien (M) und Kann-Kriterien (K). Ein Hauptkriterium ist dann erfüllt, wenn alle Muss-Subkriterien erfüllt sind.

[20] StratoGen VMware Hosting: http://www.stratogen.net
[21] CentOS Betriebssystem: http://www.centos.org
[22] KVM Hypervisor: http://www.linux-kvm.org

4.2.1 NIST-Kriterien für Cloud-Computing

- On-demand Selfservice (Diensterbringung auf Anforderung)
  - **(M)** Ressourcenprovisionierung nach Bedarf
  - **(M)** Provisionierung ohne direkte menschliche Interaktion mit Betreiber
  - **(M)** Mindestens ein Zugriffsmodell vorhanden
    (z.B. Web-Portal oder APIs)
- Broad Network Access (Umfassender Netzwerkzugriff)
  - **(M)** Verfügbarkeit über Standardnetzwerktechnologie
    (z.B. HTTP, Transmission Control Protocol/Internet Protocol (TCP/IP), RESTful APIs)
  - **(M)** Unterstützung beliebiger Endgeräte
- Ressource Pooling (Ressourcen Pooling)
  - **(M)** Mandantenfähigkeit auf Benutzer- und Netzwerkebene
  - **(M)** Bildung von Ressourcenpools
  - **(M)** Dynamische Ressourcenzuweisung an Anwender
  - **(M)** Keine Übersicht über Standort genutzter Ressourcen
  - **(K)** Wahl des Ressourcenstandorts auf höherer Ebene
    (Einflussnahme beispielsweise durch Wahl eines speziellen Rechenzentrums)
- Rapid Elasticity (Schnelle Elastizität)
  - **(M)** Elastische Anpassung von Ressourcen (Anwender)
    (Anwender können quasi unendlich viele Ressourcen anfordern oder wieder freigeben)
  - **(K)** Automatisierte Anpassung von Ressourcen (Anwender)
    (Bezieht sich auf Programmfunktionen der Produkte, nicht auf die Nutzung möglicher APIs)
  - **(M)** Skalierbarkeit der Produkte (Betreiber)
  - **(K)** Automatische Skalierbarkeit der Produkte (Betreiber)

- Measured Services (Messbare Dienstqualität)
  - **(M)** Automatische Überwachung des Ressourcenverbrauchs
  - **(M)** Übersicht über genutzte und verbrauchte Ressourcen
  - **(M)** Transparente Kostendarstellung

4.2.2 NIST-Kriterien für IaaS-Servicemodell

- IaaS
  - **(M)** Provisionierung von Rechenressourcen
    (Rechenkapazität, Arbeitsspeicher, Datenspeicher, Netzwerke usw.)
  - **(M)** Möglichkeit zur Installation eigener Betriebssysteme oder Anwendungen
  - **(M)** Keine Einsicht und Kontrolle der zugrunde liegenden Cloud-Infrastruktur

4.2.3 NIST-Kriterien für IaaS-Bereitstellungsmodelle

- Public Cloud
  - **(M)** Erfüllung der NIST-Kriterien für Cloud-Computing und IaaS
  - **(M)** Nutzung durch die breite Öffentlichkeit
- Private Cloud
  - **(M)** Erfüllung der NIST-Kriterien für Cloud-Computing und IaaS
  - **(M)** Interne, externe oder gemeinsame Bereitstellung
- Community Cloud
  - **(M)** Erfüllung der NIST-Kriterien für Cloud-Computing und IaaS
  - **(M)** Interne, externe oder gemeinsame Bereitstellung
  - **(M)** Nutzung durch mindestens zwei Organisationen mit gemeinsamen Interesse
- Hybrid Cloud
  - **(M)** Erfüllung der NIST-Kriterien für Cloud-Computing und IaaS
  - **(M)** Kombination aus mindestens zwei eigenständigen Bereitstellungsmodellen
  - **(M)** Standardisierte oder proprietäre Verbindungstechnologie
  - **(M)** Portabilität von Daten und Anwendungen
  - **(K)** Zentrales Management der hybriden Umgebung

4.3 Untersuchung der Cloudstack-Produkte

Im Laufe der Untersuchung wird die vCloud Suite von VMware als eine gesamte Einheit betrachtet, wie sie sich auch bei VMware im Angebot befindet. Die jeweils beteiligten Produkte für die Umsetzung der Kriterien sind einzeln im Text benannt.

Bei Citrix bildet CloudPlatform die Basis der Betrachtung. Eine zusätzliche Betrachtung weiterer Produkte erfolgt an Punkten, wo diese ergänzend zum Einsatz kommen können. Im Anschluss an die Untersuchung folgt eine tabellarische Ergebnisdarstellung.

4.3.1 Untersuchung nach Kriterien für Cloud-Computing

4.3.1.1 On-demand Selfservice

Citrix Der Selfservice bei Citrix erfolgt über CloudPlatform. Mittels des zugehörige Web-Portals oder der API verwalten Anwender alle Ressourcen und Dienste, die auf CloudPlatform basieren. Über Vorlagen haben Anwender Zugriff auf einen Katalog an vorkonfigurierten VMs und ISO-Abbildern. Der Anwender kann aber ebenfalls eigene ISO-Abbilder hochladen und eigene Vorlagen aus vorhandenen VMs und Snapshots erstellen. Zusätzlich lassen sich Vorlagen für die unterstützten Hypervisoren im jeweils zugehörigen Format hochladen.

Anwender können eigenständig neue VMs anlegen und verwalten. Bei der Erstellung hat der Anwender die Möglichkeit, den zu nutzenden Hypervisor selbst zu wählen. Die Leistungsdaten, wie Anzahl der CPUs, MHz, RAM oder Netzwerkbandbreite, wählt der Anwender zusammenhängend aus vom Betreiber vordefinierten Konfigurationen. Diese werden innerhalb von CloudPlatform als Compute Offerings bezeichnet, gleiches gilt für den Datenspeicher. Die Netzwerkkarten und die zugehörige Konfiguration werden beim Anlegen einer neuen VM erstellt. Die Leistungsdaten von VMs kann der Anwender nachträglich nur über einen Wechsel des Compute Offerings erzielen, den Datenspeicher kann er durch das Erstellen oder Löschen von virtuellen Festplatten erweitern oder verringern.

Zur Verwaltung von VMs gehört weiterhin beispielsweise die Möglichkeit zur Erstellung von Snapshots, das Ein- und Ausschalten, der Zugriff auf die Konsole und das Zurücksetzen des Passworts oder der kompletten VM. Der Anwender ist in der Lage, zusätzliche Netzwerke anzulegen und Dienste wie Network Address Translation (NAT), Dynamic Host Configuration Protocol (DHCP), VPN, Domain Name System (DNS), Firewalls, Port Forwarding und Load Balancing zu konfigurieren.

Weiterhin bietet CloudPlatform Unterstützung für die AWS EC2 API. Dabei übersetzt CloudPlatform EC2-API-Aufrufe in CloudPlatform-API-Aufrufe. Auf diese Weise können Anwender

ihre ggf. vorhandenen und AWS-kompatiblen Anwendungen in Zusammenarbeit mit CloudPlatform weiterhin nutzen.

Eine Cloudumgebung auf Basis von CloudPlatform lässt sich durch die ergänzende Nutzung von CloudPortal Business Manager erweitern. Für den Selfservice nutzt der Anwender dann allein das Web-Portal des CloudPortal Business Managers. Eine eigene API stellt dieser nicht bereit, die CloudPlatform API sowie die Unterstützung für die AWS EC2 API kann der Anwender aber weiterhin nutzen.

Alle zuvor beschriebenen Optionen des Selfservice im Web-Portal von CloudPlatform eröffnen sich dem Anwender ebenfalls im Web-Portal von CloudPortal Business Manager. Zusätzlich findet er hier die Bepreisung und Abrechnung der einzelnen Ressourcen und Dienste vor und kann die durch CloudPortal Business Manager bereitgestellten Funktionen für die Kundenpflege (Customer Relationship Management (CRM)) nutzen. Über CloudPortal Business Manager bietet sich ihm weiterhin die Möglichkeit, weitere angebotene Dienste neben IaaS zu buchen. Die Verwaltung dieser Dienste erfolgt nicht über CloudPortal Business Manager.

VMware Für den Selfservice bei VMwares vCloud Suite kommt vCloud Director zum Einsatz. Über das Web-Portal und die API des vCloud Director können Anwender nur Ressourcen auf Basis von vSphere verwalten.

VMs werden in vCloud Director als vApps bezeichnet. Diese Container enthalten eine oder mehrere VMs und unter anderem noch die zugehörige Netzwerkkonfiguration. Über Kataloge können Anwender auf Vorlagen für vApps oder Mediendateien zugreifen. Selbst erstellte Vorlagen für vApps lassen sich aber auch im Open Virtualization Format (OVF) hochladen.

Der Anwender kann selbstständig neue VMs anlegen, die Leistungsdaten dabei frei wählen und VMs verwalten. Dazu gehört beispielsweise das Ein- und Ausschalten, der Zugriff auf die Konsole der VMs, die Erstellung von Snapshots von einzelnen VMs oder kompletten vApps und die Anpassung von CPU, RAM und Datenspeicher. Weiterhin kann der Anwender zusätzliche Netzwerkkarten zu VMs hinzufügen, zusätzliche Netzwerke erstellen und verwalten sowie Dienste wie NAT, DHCP, VPN und Firewalls konfigurieren.

4.3.1.2 Broad Network Access

Citrix Je nach Bereitstellungsumgebung muss der Betreiber für eine stabile und ausreichend dimensionierte Netzwerkanbindung, z.B. an das Internet, sorgen. Handelt es sich beispielsweise um eine Public Cloud, ist eine Anbindung an das Internet unumgänglich. Die Dimensionierung der Anbindung hängt wiederum von der Anzahl der Anwender und den angebotenen Diensten ab. Gleiches gilt für das Netzwerk der zugrunde liegenden Cloud-Infrastruktur. Bei einer Private

Cloud ist eine breitbandige Internetanbindung ggf. nicht gleichermaßen von Bedeutung wie die innerbetriebliche Netzwerkanbindung der Cloud-Infrastruktur.

Der Anwender kann über das Web-Portal (HTTP) von CloudPlatform bzw. CloudPortal Business Manager oder über die CloudPlatform API (REST) auf seine Ressourcen zugreifen und diese verwalten. Bei Nutzung des Web-Portals kann der Zugriff von beliebigen Endgeräten erfolgen, sofern auf diesen ein Browser vorhanden ist.

Erzeugen viele Anwender gleichzeitig eine hohe Anfragedichte, können diese auf einen Cluster von Management-Servern für CloudPlatform bzw. CloudPortal Business Manager mit Hilfe von Lastverteilung (Load Balancing) durch z.B. NetScaler aufgeteilt werden.

VMware Je nach Bereitstellungsumgebung muss der Betreiber für eine stabile und ausreichend dimensionierte Netzwerkanbindung, z.B. an das Internet, sorgen (siehe dazu vorherigen Abschnitt zu Citrix). Der Anwender kann dann über das Web-Portal (HTTP) oder die vCloud API (REST) von vCloud Director auf seine Ressourcen zugreifen und diese verwalten. Bei Nutzung des Web-Portals kann der Zugriff von beliebigen Endgeräten aus erfolgen, sofern auf diesen ein Browser vorhanden ist.

Erzeugen viele Anwender gleichzeitig eine hohe Anfragedichte, können diese auf mehrere vCloud Director Instanzen, sogenannte vCloud Director Cells, mit Hilfe von Lastverteilung (Load Balancing) durch vCloud Networking & Security aufgeteilt werden.

4.3.1.3 Ressource Pooling

Citrix Das Pooling von Ressourcen findet bereits auf den einzelnen Hosts durch den Hypervisor statt. Dort werden Ressourcen wie beispielsweise Rechenkapazität, Arbeitsspeicher und Datenspeicher in Pools zusammengefasst. Diese Kapazitäten können je nach verwendetem Hypervisor wiederum durch die Gruppierung der einzelnen Hosts zu Clustern in einem großen Ressourcenpool zusammengefasst werden.

Eine CloudPlatform-Installation besteht aus Zonen, Pods und Clustern. Eine Zone repräsentiert dabei typischerweise einen physischen Standort bzw. ein Rechenzentrum. Eine Zone besteht aus einem oder mehreren Pods und Secondary Storage (sekundärer Datenspeicher). Dieser Speicher beinhaltet die Vorlagen, ISO-Abbilder und Snapshots. Ein Pod repräsentiert ein Hardware-Rack und beinhaltet ein oder meherere Cluster. Ein Cluster besteht aus mindestens einem Host und Primary Storage (primärer Datenspeicher). Auf diesem Speicher befinden sich alle virtuellen Festplatten der VMs, die auf Hosts des zugehörigen Clusters laufen. Für die

einzelnen Hosts unterstützt CloudPlatform die Hypervisoren XenServer, vSphere ESXi, Oracle VM[23] und KVM.

Die Ressourcen der einzelnen Hosts und Datenspeicher fasst CloudPlatform in einem großen Pool zusammen und stellt den Anwendern so Rechenkapazität, Arbeitsspeicher, Datenspeicher und Netzwerkdienste für den Betrieb von VMs bereit. Anwender können beim Erstellen von VMs aber wählen, in welcher Zone die neue VM erstellt wird. Auf diese Weise haben diese bei Bedarf die Möglichkeit, über den Standort der genutzten Ressourcen zu entscheiden. Dieser Aufbau einer Zone innerhalb von CloudPlatform ist zur Verdeutlichung nochmals in Abbildung 4.3.1 dargestellt.

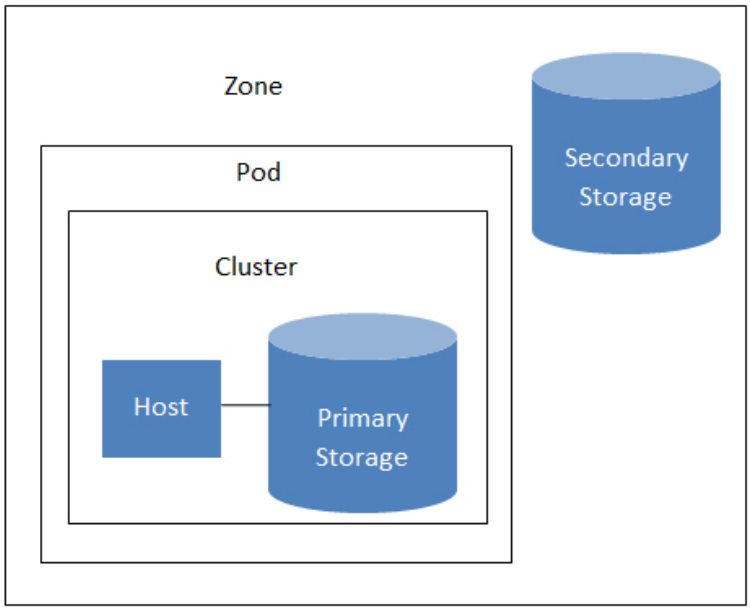


Abbildung 4.3.1: Aufbau von Citrix CloudPlatform [Cit13b, S. 6]

Anwender sind innerhalb von CloudPlatform in Domains, Accounts und User strukturiert. Domains repräsentieren beispielsweise eine Organisation oder einen Dienstanbieter. Jede Domain besteht aus Accounts, die z.B. einzelne Abteilungen oder Kunden darstellen. Somit können zu jedem Account wiederum weitere User gehören, welche die eigentlichen Anwender darstellen. Anwender desselben Accounts haben Zugriff auf alle Ressourcen dieses Accounts. Alle Anwender beziehen ihre Ressourcen aus dem gleichen, oben bezeichneten großen Pool, den CloudPlatform bereitstellt.

[23] OVM Hypervisor: http://www.oracle.com/technetwork/server-storage/vm/overview/index.html

Die Struktur der Benutzerverwaltung bildet die Basis für einen mandantenfähigen Betrieb. Die Isolation der Accounts und User auf Netzwerkebene gilt pro Zone. Der Netzwerktyp einer Zone kann entweder Basic oder Advanced sein. Unterschiede gibt es bei der Isolation des Netzwerkverkehrs, dem Angebot an möglichen Netzwerkdiensten und den unterstützten Hypervisoren.

In einer Basic-Zone erfolgt die Trennung durch Security Groups, in einer Advanced-Zone kommen VLANs zum Einsatz. Die optionale Integration von NetScaler erweitert das Angebot an Netzwerkdiensten durch spezifische Funktionen von Citrix NetScaler.

VMware Das Pooling von Ressourcen findet bereits auf den einzelnen Hosts durch den Hypervisor statt. Dort werden Ressourcen, wie beispielsweise Rechenkapazität, Arbeitsspeicher und Datenspeicher, in Pools zusammengefasst. Diese Kapazitäten können wiederum durch die Gruppierung der einzelnen Hosts in vCenter-Server-Clustern zu einem großen Ressourcenpool zusammengefasst werden.

vCloud Director stellt Rechenkapazität, Arbeitsspeicher, Datenspeicher und Netzwerkdienste für den Betrieb von VMs auf Grundlage von vSphere-Ressourcen bereit. Die benötigten Ressourcenpools können vCloud Director durch Anfügen von vCenter-Servern verfügbar gemacht werden. Für die Bereitstellung von Netzwerkdiensten benötigt vCloud Director den vShield Manager aus vCloud Networking & Security.

Nach dem Anfügen können die Ressourcenpools, Datenspeicher und Netzwerke virtuellen Provider-Datencentern zugeordnet werden. Virtuelle Provider-Datencenter fassen die Ressourcen in Pools zusammen und dienen damit als Quelle für virtuelle Organisations-Datencenter. Jede Organisation in vCloud Director ist eine abgetrennte Verwaltungseinheit mit eigenen Benutzern und Ressourcen. Eine Organisation kann hierbei z.B. für ein Unternehmen, eine Abteilung oder einen einfachen Anwender stehen. Organisationen bekommen Ressourcen aus diesen Pools für ihre zugehörigen virtuellen Organisations-Datencenter zugewiesen. Die Ressourcen von geografisch getrennten Rechenzentren können in verschiedenen virtuellen Provider-Datencentern gruppiert werden. So haben Organisationen dann die Möglichkeit, bei Bedarf über den Standort der genutzten Ressourcen zu entscheiden. Dieser Aufbau von vCloud Director ist zusätzlich grafisch in Abbildung 4.3.2 dargestellt.

Das Konzept von Organisationen und virtuellen Datencentern mit isolierten Ressourcen bildet die Grundlage für einen mandantenfähigen Betrieb. Für die Trennung der einzelnen Organisationen auf Netzwerkebene kommt vCloud Networking & Security zum Einsatz. Die enthaltene VXLAN-Technologie abstrahiert physische Netzwerkinfrastrukturen und erlaubt die

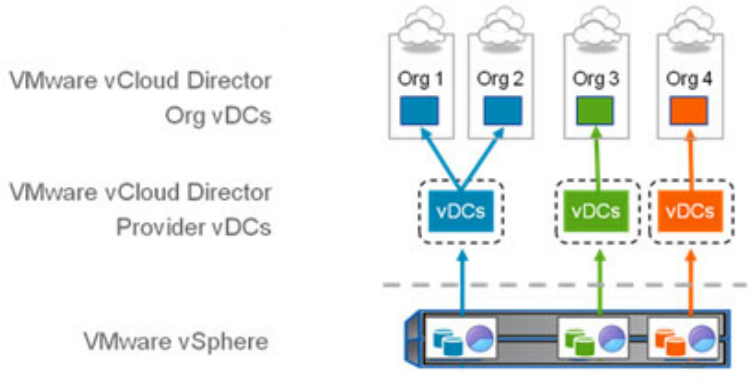


Abbildung 4.3.2: VMware vCloud Director Aufbau [vgl. JY12]

einfache Erstellung von logischen und voneinander isolierten Netzwerken auf dem zugrunde liegenden Netzwerk.

4.3.1.4 Rapid Elasticity

Citrix Über die Benutzerverwaltung kann der Administrator konfigurieren, welche und in welcher Anzahl Anwender oder Domains Ressourcen belegen können. Weiterhin lässt sich einstellen, ob Ressourcen überbelegt werden sollen und innerhalb welcher Grenzen dies geschieht. Ressourcen, die ein Anwender über CloudPlatform bzw. CloudPortal Business Manager bucht, werden ihm erst im Anschluss entsprechend der Parameter zur Überbelegung garantiert. Bei entsprechender Konfiguration kann ein Anwender quasi unbegrenzt zusätzliche Ressourcen belegen oder auch wieder freigeben. Über die CloudPlatform API hat der Anwender die Möglichkeit, Ressourcen durch externe Anwendungen automatisiert zu provisionieren oder zu löschen.

Der Betreiber sollte entsprechende Infrastruktur vorhalten. Eine automatische Erweiterung der Cloud-Infrastruktur zentral über CloudPlatform ist nicht möglich. Es lassen sich aber entsprechende Funktionen seitens der unterstützten und eingesetzten Hypervisoren unabhängig von CloudPlatform konfigurieren und nutzen. XenServer bietet für Cluster beispielsweise die Funktionen XenMotion und Workload Balancing. Diese passen die Ressourcenauslastung dem aktuellen Bedarf an, indem sie Lasten automatisch auf die Hosts und Datenspeicher verteilen und Hosts während geringer Auslastungsphasen abschalten bzw. bei Lastspitzen wieder aktivieren. Gleiches bieten die vSphere-Funktionen DRS, Storage DRS und Distributed Power Management (DPM). Zusätzlich bietet vSphere die Funktion Auto Deploy, mit der sich neue

Hosts automatisch installieren, konfigurieren und in vorhandene Cluster einfügen lassen, um die Kapazitäten zu erweitern.

Eine CloudPlatform-Installation ist von Citrix bis zu einem Maximum von 30.000 Hosts bei vier Manangement-Servern zertifiziert. Für die maximal mögliche Anzahl an VMs gibt es keine offizielle Angabe, weiterhin hängt diese Zahl von den jeweils genutzten Hypervisoren ab.

Die Verwendung von Security Groups in einer Basic-Zone bietet eine hohe Skalierbarkeit für die Isolation von Anwendern auf Netzwerkebene. Der Einsatz von Security Groups ist nur bei den Hypervisoren XenServer und KVM möglich und beschränkt somit die Auswahl der möglichen Hypervisoren. Kommt beispielsweise vSphere ESXi als Hypervisor zum Einsatz, muss eine Advanced-Zone eingerichtet werden, in der die Netzwerkisolation auf Basis von VLANs geschieht. Die Skalierbarkeit ist hier durch die physische Grenze von maximal 4094 möglichen VLANs limitiert.

Eine weitere Option ist die Nutzung von Public-Cloud-Diensten oder die Anbindung der eigenen Infrastruktur. So lässt sich die eigene Cloud schnell erweitern. Dieser Hybrid-Cloud-Ansatz wird in Abschnitt 4.4 noch näher untersucht.

VMware In vCloud Director existieren verschiedene Modelle für die Reservierung und Nutzung von Ressourcen. Für jede Organisation lässt sich festlegen, welche Ressourcen garantiert sind und innerhalb welcher Grenzen Ressourcen überbelegt werden können. Mit dem Modell Pay-as-you-go kann der Anwender quasi unbegrenzt zusätzliche Ressourcen belegen oder auch wieder freigeben.

Leases für Rechen- und Speicherressourcen bieten dem Anwender die Möglichkeit der automatischen Löschung von vApps oder Speicherobjekten nach einem bestimmten Zeitraum. So lassen sich Ressourcen automatisch freigeben, wenn sie nicht mehr benötigt werden (Lifecycle-Management). Zusätzlich bietet die vCloud Director API dem Anwender die Möglichkeit, Ressourcen durch externe Anwendungen automatisiert zu provisionieren oder zu löschen. Auch das vCloud Automation Center bietet in Zusammenarbeit mit dem vCloud Director Möglichkeiten für eine automatisierte Provisionierung und das Lifecycle-Management von VMs.

Der Betreiber sollte entsprechende Infrastruktur vorhalten. Unter Zuhilfenahme von vSphere Auto Deploy lassen sich beispielsweise neue Hosts automatisch installieren, konfigurieren und in vorhandene Cluster einbinden, um die Kapazitäten zu erweitern. Die vSphere-Funktionen DRS, Storage DRS und DPM können die Ressourcenauslastung dem aktuellen Bedarf anpassen, indem sie Lasten automatisch auf die Hosts und Datenspeicher verteilen und Hosts während geringer Auslastungsphasen ausschalten oder bei Lastspitzen wieder einschalten.

Eine vCloud-Director-Installation ist von VMware für ein Maximum von 2.000 vSphere-Hosts bei zehn vCloud Director Cells und 30.000 VMs zertifiziert. Die Verwendung des VXLAN-Protokolls durch vCloud Networking & Security für die Erstellung logischer Netze zur Isolation der Anwender auf Netzwerkebene bietet eine hohe Skalierbarkeit.

Eine weitere Möglichkeit ist die Anbindung bereits vorhandener vSphere-Umgebungen oder die Nutzung von Public-Cloud-Diensten, die auf vCloud basieren. So lässt sich die eigene Cloud schnell erweitern. Dieser Hybrid-Cloud-Ansatz wird in Abschnitt 4.4 noch näher untersucht.

4.3.1.5 Measured Services

Citrix CloudPlatform speichert Daten bezüglich des Ressourcenverbrauchs der einzelnen Anwender. Innerhalb von CloudPlatform haben Anwender aber keine detaillierte Einsicht in genutzte Ressourcen, sie haben nur eine Anzeige des durchschnittlichen Verbrauchs von CPU und Netzwerkbandbreite. Für den Zugriff auf detaillierte Informationen kann der Administrator die CloudPlatform API verwenden, um Nutzungsdaten beispielsweise in ein externes Programm für die Erstellung von Kostenreports und zur Abrechnung zu importieren. Alternativ lässt sich CloudPlatform zusammen mit CloudPortal Business Manager einsetzen.

CloudPortal Business Manager integriert sich mit CloudPlatform und stellt dem Anwender im Web-Portal eine Zusammenfassung der genutzten und verbrauchten Ressourcen zur Verfügung, beispielsweise VMs, Datenspeicher, Netzwerkdienste und -bandbreite sowie die bereits angefallenen Kosten zur Verfügung.

Über den CloudPortal Business Manager bucht der Anwender Ressourcen, die auf den angebotenen Ressourcen und Diensten von CloudPlatform basieren. Im CloudPortal Business Manager werden diese in Form von Produkten geführt. Hier werden die Preismodelle für die einzelnen Ressourcen festgelegt. Beispielsweise kann dem Nutzer CPU-Geschwindigkeit, Anzahl der CPU-Kerne, Netzwerkbandbreite und Anzahl Netzwerke, Arbeitsspeicher, Datenspeicher uvm. individuell angepasst berechnet werden. Darüber hinaus lassen sich zusätzliche Einmalkosten, wie z.B. Einrichtungsgebühren oder Lizenzkosten, berechnen. Diese Produkte fasst CloudPortal Business Manager zu sogenannten Produkt-Bundles zusammen, die der Anwender dann über Kataloge buchen kann. Für verschiedene Anwender oder Benutzergruppen können Kataloge mit unterschiedlichen Produkt-Bundles und Preisen existieren.

Für die Abrechnung kann der Administrator bei Erstellung von Produkt-Bundles unter anderem das Pay-as-you-go-Modell wählen. Bei Buchung zahlt der Anwender dann nur für die tatsächlich verbrauchten Ressourcen. Die Zahlung kann direkt mittels Kreditkarte erfolgen. Alternativ lassen sich die Nutzungs- und Rechnungsdaten für den Import in externe Zahlungssysteme exportieren.

CloudPlatform bietet keine eigenen Funktionen zur Optimierung der Ressourcennutzung. Hier kann nur auf Funktionen der jeweils unterstützten Hypervisoren zurückgegriffen werden. Wie bereits zuvor im Abschnitt 4.3.1.4 für Citrix erwähnt, zählen zu diesen Funktionen beispielsweise XenMotion oder Workload Balancing bei Nutzung von XenServer.

VMware Innerhalb von vCloud Director hat der Anwender eine Zusammenfassung der aktuell genutzten Ressourcen. Die bedarfsgerechte Abrechnung der verbrauchten Ressourcen erfolgt über den vCenter Chargeback Manager. Der Chargeback Manager interagiert mit der virtuellen vSphere-Umgebung, vCloud Director und dem vShield Manager aus vCloud Networking & Security, um Daten zu den genutzten Ressourcen, wie VMs, Datenspeicher, Netzwerkdienste und -bandbreite, zu ermitteln.

Für die Administration und zur Erstellung von Kostenreports steht ein eigenes Web-Portal und eine API zur Verfügung. Für jede Organisation innerhalb von vCloud Director wird eine eigene Chargeback-Hierachie angelegt, die alle genutzten Ressourcen enthält. Hier werden die Preismodelle für die einzelnen Ressourcen festgelegt. Beispielsweise kann dem Nutzer CPU-Geschwindigkeit, Anzahl der CPU-Kerne, Datenspeichertransfers, Netzwerkbandbreite und Anzahl Netzwerke, Arbeitsspeicher, Datenspeicher uvm. individuell angepasst berechnet werden. Weiterhin lassen sich zusätzliche Dienstmerkmale, wie vSphere High Availability oder Fault Tolerance (siehe dazu auch Abschnitt 3.2.1.1), berechnen. Dies gilt ebenfalls für einmalige, nicht in Verbindung mit vSphere-Ressourcen stehende Kosten. Darunter fallen beispielsweise Einrichtungsgebühren oder Lizenzkosten. Die Abrechnung erfolgt dann entsprechend dem genutzten Zuweisungsmodell in vCloud Director. Beim Pay-as-you-go-Modell werden nur die tatsächlich verbrauchten Ressourcen berechnet.

Reports zu den verbrauchten Ressourcen generiert der Betreiber über das zugehörige Web-Portal, für das ebenfalls Anwender einen Zugang erhalten können, so dass diese selbstständig Reports für ihre Organisation generieren und einsehen können. Über die API des vCenter Chargeback Managers lassen sich Nutzungsdaten für den Import in ggf. vorhandene Zahlungssysteme exportieren.

Wie bereits zuvor im Abschnitt 4.3.1.4 für VMware erwähnt, lässt sich mit den vSphere-Funktionen DRS, Storage DRS und DPM die Ressourcennutzung optimieren. Zusätzlich kann der Betreiber vCenter Operations Manager zur Kapazitätsplanung und somit zur Optimierung der Ressourcennutzung und deren Zuweisung an die virtuellen Systeme nutzen.

4.3.2 Untersuchung nach Kriterien für IaaS-Bereitstellungsmodell

Citrix Anwendern stehen nach Bedarf grundlegende Ressourcen, wie Rechenkapazität, Arbeitsspeicher, Datenspeicher und Netzwerkdienste, auf Basis von CloudPlatform zur Verfügung. Der Anwender hat dabei keine Kontrolle oder Einsicht in die eigentliche Cloud-Infrastruktur und somit kein Wissen über den genauen Standort seiner genutzen Ressourcen. Bei der Erstellung neuer VMs hat der Anwender die Möglichkeit, dass einzusetzende Betriebssystem oder beliebige andere Software selbstständig zu installieren.

VMware Dem Anwender stehen nach Bedarf grundlegende Ressourcen, wie Rechenkapazität, Arbeitsspeicher, Datenspeicher und Netzwerkdienste, auf Basis von vSphere-Ressourcen und vCloud Networking & Security zur Verfügung. Dabei haben die Anwender einer zugehörigen Organisation innerhalb von vCloud Director keine Kontrolle oder Einsicht in die zugrunde liegende Cloud-Infrastruktur und somit kein Wissen über die genaue Lokalisation ihrer genutzen Ressourcen. Anwender können selbstständig neue VMs anlegen und beliebige Betriebssysteme oder andere Software installieren.

4.3.3 Ergebnisdarstellung der Untersuchung

Zur übersichtlichen Darstellung der Ergebnisse folgen die Tabellen 4.3.1 und 4.3.2 auf der Grundlage der vorhergehenden Untersuchung. Die vCloud Suite von VMware wird weiterhin als eine Einheit betrachtet. Für Citrix findet sich in den Tabellen eine gesonderte Betrachtung von CloudPlatform sowie der Kombination aus CloudPlatform und CloudPortal Business Manager. Beide Produkte lassen sich voneinander unabhängig oder in Kombination erwerben und betreiben. Citrix führt aber beide Produkte unter der Kategorie Cloud-Infrastruktur. Diese Unterteilung bietet eine differenzierte Übersicht.

Die Kennzeichnung von Muss- und Kann-Kriterien innerhalb der tabellarischen Darstellung erfolgt analog zu dem in Abschnitt 4.2 definierten Bewertungsschema. CloudPortal Business Manager wird innerhalb der folgenden Tabelle mit CPBM abgekürzt.

		Citrix		VMware
NIST-Kriterien für Cloud-Computing		CloudPlatform	CloudPlatform + CPBM	vCloud Suite
On-Demand Selfservice		X	X	X
Ressourcenprovisionierung nach Bedarf	M	X	X	X
Provisionierung ohne direkte menschliche Interaktion mit Betreiber	M	X	X	X
Mindestens ein Zugriffsmodell vorhanden	M	X	X	X
Broad Network Access		X	X	X
Verfügbarkeit über Standardnetzwerktechnologie	M	X	X	X
Unterstützung beliebiger Endgeräte	M	X	X	X
Ressource Pooling		X	X	X
Mandantenfähigkeit auf Benutzer- und Netzwerkebene	M	X	X	X
Bildung von Ressourcenpools	M	X	X	X
Dynamische Ressourcenzuweisung an Anwender	M	X	X	X
Keine Übersicht über Standort genutzter Ressourcen	M	X	X	X
Wahl des Ressourcenstandorts auf höherer Ebene	K	X	X	X
Rapid Elasticity		X	X	X
Elastische Anpassung von Ressourcen (Anwender)	M	X	X	X
Automatisierte Anpassung von Ressourcen (Anwender)	K	-	-	X
Skalierbarkeit der Produkte (Betreiber)	M	X	X	X
Automatische Skalierbarkeit der Produkte (Betreiber)	K	-	-	X
Measured Services		-	X	X
Automatische Überwachung des Ressourcenverbrauchs	M	X	X	X
Übersicht über genutzte und verbrauchte Ressourcen	M	-	X	X
Transparente Kostendarstellung	M	-	X	X

Tabelle 4.3.1: Ergebnisdarstellung nach Kriterien für Cloud-Computing

		Citrix		VMware
NIST-Kriterien für IaaS-Servicemodell		CloudPlatform	CloudPlatform + CPBM	vCloud Suite
IaaS		X	X	X
Provisionierung von Rechenressourcen	M	X	X	X
Möglichkeit zur Installation eigener Betriebssysteme oder Anwendungen	M	X	X	X
Keine Einsicht und Kontrolle der zugrunde liegenden Cloud-Infrastruktur	M	X	X	X

Tabelle 4.3.2: Ergebnisdarstellung nach Kriterien für IaaS-Servicemodell

4.4 Prüfung möglicher IaaS-Bereitstellungsmodelle

Es folgt die Prüfung, welche Bereitstellungsmodelle sich im Bereich IaaS mit den untersuchten Produkten realisieren lassen. Für diese Untersuchung sind insbesondere die Ergebnisse der vorhergehenden Untersuchung aus Abschnitt 4.3.3 von Bedeutung. Eine tabellarische Ergebnisdarstellung findet sich direkt im Anschluss in Tabelle 4.4.1.

Citrix CloudPlatform für das Infrastrukturmanagement der Cloud und CloudPortal Business Manager als primäres Web-Portal erfüllen nur gemeinsam in Kombination die erforderlichen Kriterien des Cloud-Computings für IaaS nach NIST. Die Produkte lassen sich innerhalb eines Unternehmens auf eigener Infrastruktur oder extern betreiben, auch ein kombinierter Betrieb ist möglich. Es lassen sich auf diese Weise Private oder Community Clouds realisieren.

Durch die in Abschnitt 4.3.1.3 beschriebene Mandantenfähigkeit der Produkte erfolgt die Separierung der einzelnen Anwender auf Benutzer- und Netzwerkebene. Der Aufbau von Public Clouds zur Nutzung durch die breite Öffentlichkeit ist somit ebenfalls durchführbar.

Für die Erstellung einer Hybrid Cloud bietet CloudPlatform Nutzern die Erstellung von VPN-Tunneln, um sich mit beliebigen anderen Clouds oder der firmeneigenen Infrastruktur zu verbinden.

Das Produkt CloudBridge eröffnet die Möglichkeit, verschiedene Infrastrukturen über einen transparenten Netzwerktunnel zu verbinden, um beispielsweise Firmeninfrastrukturen zu verbinden oder diese um Cloud-Angebote, wie AWS, zu erweitern. Der Einsatz von CloudBridge zielt daher eher auf Private oder Community Clouds ab.

Diese beiden Ansätze erlauben zwar eine Kopplung von verschiedenen Infrastrukturen und somit eine Erweiterung der eigenen Cloud, aber in beiden Fällen fehlt das zentrale Management oder die Portabilität der VMs zwischen den verschiedenen Infrastrukturen. Insbesondere die fehlende Portabilität führt dazu, dass sich mit CloudPlatform und CloudPortal Business Manager keine Hybrid Cloud im Sinne des NIST aufbauen lässt.

VMware Die vCloud Suite erfüllt im Hinblick auf IaaS alle erforderlichen Kriterien für Cloud-Computing des NIST. Die Produkte lassen sich innerhalb eines Unternehmens auf eigener Infrastruktur oder extern betreiben, ein kombinierter Betrieb ist ebenfalls möglich. Es lassen sich mit der vCloud Suite Private und Community Clouds realisieren.

Sofern eine Separierung der einzelnen Anwender auf Benutzer- und Netzwerkebene erwünscht ist, lässt sich dies aufgrund der in Abschnitt 4.3.1.3 beschriebenen Mandantenfähigkeit von vCloud Director ebenfalls durchführen. Mittels der gegebenen Mandantenfähigkeit be-

steht weiterhin die Möglichkeit, Public Clouds zur Nutzung durch die breite Öffentlichkeit zu erstellen.

Um eine Hybrid Cloud zu realisieren, bringt die vCloud Suite primär den vCloud Connector mit. Mit dem vCloud Connector lassen sich verschiedene vCloud-Director-Zugänge, sowohl aus dem Private- als auch Public-Cloud-Bereich und ggf. beim Anwender vorhandene vSphere-Umgebungen verbinden. Über das vCloud-Web-Portal[24] oder den vSphere-Client erfolgt dann die zentrale Verwaltung. Auf diese Weise lassen sich zentral VMs und Kataloge erstellen und verwalten. Weiterhin können Anwender VMs zwischen den verschiedenen Infrastrukturen verschieben. Durch die Nutzung von vCloud Networking & Security lassen sich die einzelnen Infrastrukturen auch dahin gehend auf Netzwerkbasis durch ein Site-to-Site-VPN verbinden, dass Netzwerkkonnektivität zwischen den VMs der verschiedenen Infrastrukturen besteht. Hybrid Clouds im Sinne des NIST lassen sich auf diese Weise erfolgreich mit dem vCloud Connector realisieren.

Zu einer Alternative zum vCloud Connector könnte sich das vCloud Automation Center entwickeln. Anwendern dient es für die zentrale Verwaltung von internen sowie externen Ressourcen. Es unterstützt dabei nicht nur vSphere und vCloud Director, sondern auch weitere Hypervisoren und physische Infrastrukturen sowie AWS. Über das eigene Web-Portal bietet das vCloud Automation Center einen großen Funktionsumfang für Verwaltung, Provisionierung und Automatisierung rund um VMs und Anwendungen in heterogenen Infrastrukturen und Public sowie Private Clouds.

Eine Hybrid Cloud im Sinne des NIST kann mit dem Produkt aber derzeit noch nicht erstellt werden, da es keine Möglichkeit bietet, Workloads zwischen den verschiedenen Infrastrukturen zu verschieben. Der Funktionsumfang sowie die Integration in die VMware-Produktpalette soll sich in Zukunft allerdings noch weiter verbessern.

[24] vCloud: http://vcloud.vmware.com

		Citrix		VMware
NIST-Kriterien für IaaS-Bereitstellungsmodelle		CloudPlatform	CloudPlatform + CPBM	vCloud Suite
Public Cloud		-	X	X
Erfüllung der NIST-Kriterien für Cloud-Computing und IaaS	M	-	X	X
Nutzung durch die breite Öffentlichkeit	M	X	X	X
Private Cloud		-	X	X
Erfüllung der NIST-Kriterien für Cloud-Computing und IaaS	M	-	X	X
Interne, externe oder gemeinsame Bereitstellung	M	X	X	X
Community Cloud		-	X	X
Erfüllung der NIST-Kriterien für Cloud-Computing und IaaS	M	-	X	X
Interne, externe oder gemeinsame Bereitstellung	M	X	X	X
Nutzung durch mindestens zwei Organisationen mit gemeinsamen Interesse	M	X	X	X
Hybrid Cloud		-	-	X
Erfüllung der NIST-Kriterien für Cloud-Computing und IaaS	M	-	X	X
Kombination aus mindestens zwei eigenständigen Bereitstellungs-modellen	M	X	X	X
Standardisierte oder proprietäre Verbindungstechnologie	M	X	X	X
Portabilität von Daten und Anwendungen	M	-	-	X
Zentrales Management der hybriden Umgebung	K	-	-	X

Tabelle 4.4.1: Ergebnisdarstellung nach Kriterien für IaaS-Bereitstellungsmodelle

5 Schlussbetrachtung

5.1 Kritische Würdigung der Ergebnisse

Da sich für den Begriff Cloud-Computing bislang noch kein Standard etablieren konnte, findet dieser Begriff für eine Vielzahl von Diensten und Nutzungsszenarien Anwendung. Oftmals wird das Schlagwort Cloud-Computing auch leichtfertig für Marketingzwecke genutzt, was durch die unklare Definition des Begriffs und die unterschiedlichen zugrunde liegenden Technologien begünstigt wird. Dieser Umstand erschwert einen Vergleich unterschiedlicher Produkte und Hersteller für Cloud-Computing. Die Definition für Cloud-Computing nach NIST trifft hierbei auf weitgehende Akzeptanz. Diese beschreibt die wichtigsten Eigenschaften, die Servicemodelle und Bereitstellungsmodelle von Cloud-Computing. Damit bietet sie einen guten Abgrenzungsrahmen, aber auch Spielraum für Interpretation.

Nicht alle Kriterien, die das NIST formuliert, sind in jedem Fall erstrebenswert für die Umsetzung einer Cloud-Strategie. Bei einer Private Cloud ist beispielsweise der ubiquitäre Zugriff über das Internet oder die verbrauchsabhängige Erfassung der Ressourcen, anders als in der Public Cloud, nicht zwangsläufig erforderlich. Ebenso kann es weitere Punkte im speziellen Einzelfall geben, die für den jeweils speziellen Anwendungsfall notwendig oder unerlässlich sind. Als mögliche Beispiele solcher zusätzlichen Punkte bzw. Kriterien seien hier Sicherheit, Usability, Automation, Nutzung standardisierter Schnittstellen für Zugriff und Verwaltung der Cloud und Nutzung standardisierter Datenformate genannt. Zu diesen Punkten trifft die Definition des NIST bisher keine oder keine konkrete Aussage.

Ziel dieser Arbeit war die Prüfung, inwieweit sich Produkte der Hersteller Citrix und VMware in die NIST-Definition für Cloud-Computing einordnen lassen. Dafür erfolgte zunächst die Einführung in die Grundlagen des Cloud-Computings und die Definition der Cloud nach NIST. Auf die Vorstellung von Produkten der Hersteller Citrix und VMware aus dem Bereich IaaS folgte im Anschluss die Analyse dieser im Hinblick auf das NIST.

Wie sich zum Ende dieser Arbeit gezeigt hat, bietet die NIST-Definition eine gute Grundlage für die Einordnung von Produkten verschiedener Hersteller auf einer gemeinsamen Basis. Auf diese Weise lassen sich Produkte unterschiedlicher Hersteller oder Anbieter vergleichbar

machen. Wie auch in [NIS11, S. 1] erwähnt, ist der Begriff des Cloud-Computings ein sich stetig weiterentwickelndes Paradigma . Der Markt für Cloud-Computing ist ständig in Bewegung. Daher sollte die Definition auch nicht zu dogmatisch angesehen werden. Es ist ein Versuch, eine allgemein anerkannte Definition des Begriffs Cloud-Computing zu etablieren.

Das in Abschnitt 4.2 erarbeitete Bewertungsschema auf der Grundlage der Interpretation der NIST-Definition durch den Autor ließ sich gut auf die Produkte bzw. Produktgruppen der Hersteller Citrix und VMware für den Bereich IaaS anwenden. Die Unterteilung in Sub-Kriterien ermöglichte eine klare Identifikation von Funktionen bzw. Eigenschaften, die zur Erfüllung der Kriterien nötig waren.

VMware Bei der Untersuchung der vCloud Suite von VMware hat sich gezeigt, dass die Kriterien des NIST für Cloud-Computing und IaaS erfüllt sind. Die anschließende Prüfung der zusätzlichen Kriterien für die vier Bereitstellungsmodelle Public, Private, Community und Hybrid Cloud ergab, dass sich diese vier Modelle mit der vCloud Suite realisieren lassen. Insbesondere für die Hybrid Cloud fiel auf, dass VMware neben der geforderten Portabilität von Daten und Anwendungen auch die zentrale Verwaltung der gekoppelten Cloud-Modelle oder virtualisierten Infrastrukturen ermöglicht. Allerdings ist man bei der vCloud Suite auf die Nutzung von vSphere und vCloud-basierten Diensten begrenzt.

Citrix Die Betrachtung von Citrix CloudPlatform ergab, dass die Protokollierung von Informationen zur Ressourcennutzung zwar in einer Datenbank stattfindet und auch ein Export erfolgen kann, jedoch keine Anzeige der Daten für Betreiber oder Anwender innerhalb von CloudPlatform möglich ist. Damit ist ein wesentliches Kriterium für Cloud-Computing nach NIST nicht erfüllt, nämlich die verbrauchsabhängige Ressourcennutzung und Abrechnung (Measured Services) (siehe Tabelle 4.3.1). Obwohl die übrigen Kriterien und die zusätzlichen Kriterien für den Bereich IaaS erfüllt sind, lassen sich so die vier Bereitstellungsmodelle im Sinne des NIST nicht umsetzen (siehe Tabelle 4.4.1).

Der kombinierte Einsatz von CloudPlatform zusammen mit CloudPortal Business Manager schließt diese Lücke. Bei den Bereitstellungsmodellen sind Private, Community und Public Clouds möglich. Für die Realisierung von Hybrid Clouds bietet CloudPlatform die Anbindung beliebiger Cloud-Modelle über VPN. Eine zentrale Verwaltung oder Portabilität, wie in der NIST-Definition beschrieben, ist jedoch nicht vorgesehen, weshalb der Aufbau einer Hybrid Cloud im Sinne des NIST mit CloudPlatform und CloudPortal Business Manager nicht realisierbar ist. Von Vorteil bei CloudPlatform ist jedoch die Unterstützung von verschiedenen Hypervisoren.

Dies bietet Flexibilität, insbesondere bei heterogenen Infrastrukturen, da der Anwender nicht auf die Nutzung von Produkten nur eines Herstellers begrenzt ist.

PaaS- und SaaS-Umgebungen Für die Bereiche PaaS sowie SaaS scheint das Angebot für Dienste aus der Public Cloud wesentlich breiter etabliert zu sein, im Gegensatz zu Produkten für die Realisierung solcher Umgebungen im eigenen Rechenzentrum. Für den Aufbau einer PaaS- oder SaaS-Cloud-Umgebung fehlt teilweise eine klare Abgrenzung der benötigten Produkte seitens der Hersteller Citrix und VMware. Weiterhin positionieren sich beide Hersteller aber auch nicht - oder nicht eindeutig - in allen Bereichen des Cloud-Computings. Die Fragestellung, inwieweit sich nun PaaS- und SaaS-Umgebungen mit Produkten der Hersteller unter Zuhilfenahme der NIST-Definition realisieren lassen, ist abschließend noch offen. Diese Fragestellung samt möglichen Ansätzen für eine Umsetzung für die beiden betrachteten Hersteller findet sich nachfolgend in Abschnitt 5.2.

5.2 Offene Punkte

Aufgrund der zu Beginn von Kapitel 3 beschriebenen Einschränkungen behandelt diese Arbeit nur den Bereich IaaS. Infolgedessen ist eine detaillierte Analyse der Fragestellung, inwieweit sich PaaS- und SaaS-Cloud-Umgebungen nach den Kriterien und der Definition des NIST durch Produkte der Hersteller Citrix und VMware aufbauen lassen, noch offen. Nachfolgend finden sich für Citrix und VMware mögliche Ansätze für eine solche Umsetzung. Ein weiteres Schwergewicht im Virtualisierungs- und Cloud-Computing-Markt ist Microsoft. Für Microsoft folgt ein kurzer Einblick in die Cloud-Produkte. Diese Ansätze bieten eine Grundlage für mögliche weitere Arbeiten zu diesem Themengebiet.

5.2.1 Platform as a Service

Citrix Für die Erstellung einer PaaS-Umgebung hat Citrix keine eigenen Produkte im Portfolio. Drittanbieter oder Citrix-Partner, wie beispielsweise Cumulogic[25], bieten für diesen Bereich Produkte zur Nutzung mit CloudPlatform an. Über Konnektoren lassen sich externe Produkte so in CloudPortal Business Manager integrieren, dass Anwender die gebotenen Dienste über das Web-Portal von CloudPortal Business Manager buchen können. Auch die Abrechnung kann über CloudPortal Business Manager erfolgen. Die Nutzung und Verwaltung erfolgt hingegen nicht über CloudPortal Business Manager, sondern über die Oberfläche des jeweiligen Produkts.

[25] Cumulogic: http://www.cumulogic.com

VMware PaaS liegt nicht im Fokus der vCloud Suite, weshalb sich entsprechende Umgebungen mit dieser Suite nicht erstellen lassen. Der enthaltene vFabric Application Director lässt sich nutzen, um Anwendungen in Form von VMs zu erstellen. Vorlagen für vorkonfigurierte Systeme heißen Blueprints. Über das Web-Portal des vFabric Application Director lassen sich Anwendungen dann fertig konfiguriert in Form von vApps in den eigenen vCloud-Director-Zugang bereitstellen. Der Anwender hat dabei aber die Kontrolle und Verantwortung für die der Anwendung zugrunde liegenden Systeme in Form von VMs und den darauf installierten Betriebssystemen. Dies widerspricht dem Ansatz von PaaS nach der Definition des NIST.

Für die Erstellung einer PaaS-Umgebung bieten sich möglicherweise die Produkte von VMwares vFabric Suite[26] an. VMware selbst spricht bei den vFabric-Produkten allerdings nicht von PaaS, sondern von Anwendungsplattform. Enthalten sind Produkte für die Bereitstellung von Laufzeitumgebungen, Datenhaltung und Verwaltung. Eine weitere Möglichkeit für den Aufbau einer PaaS-Umgebung, unter anderem auch auf der Basis von vSphere, bietet das Open-Source-PaaS-Projekt Cloud Foundry[27].

5.2.2 Software as a Service

Citrix Das Citrix Produkt CloudPortal Services Manager kann SaaS-Dienste, wie beispielsweise Exchange[28] Mailboxen, Lync[29]- oder Sharepoint[30]-Zugriff und Anwendungen auf Basis von Citrix XenApp[31], bereitstellen. Diese Dienste lassen sich über Konnektoren in CloudPortal Business Manager einbinden. So können Anwender sie über das Web-Portal des CloudPortal Business Managers buchen. Für die Abrechnung der Dienste meldet der CloudPortal Services Manager die jeweils relevanten Nutzungsdaten zurück an CloudPortal Business Manager. Diese Konnektoren befinden sich zum Zeitpunkt dieser Arbeit allerdings noch in der Entwicklungsphase.

VMware Auch SaaS-Cloud-Umgebungen liegen nicht im Fokus der vCloud Suite. Für die Erstellung von SaaS-Angeboten gibt es bei VMware in der Horizon Suite[32] das unter anderem enthaltene Produkt Horizon Workspace. Dieses Produkt stellt Anwendern ein Web-Portal

[26] VMware vFabric Suite: http://www.vmware.com/products/application-platform/vfabric/overview.html
[27] Cloud Foundry: http://www.cloudfoundry.com
[28] Microsoft Exchange: http://office.microsoft.com/en-us/exchange/
[29] Microsoft Lync: http://office.microsoft.com/de-de/lync/
[30] Microsoft Sharepoint: http://office.microsoft.com/de-de/sharepoint/
[31] Citrix XenApp: http://www.citrix.de/products/xenapp/overview.html
[32] VMware Horizon Suite: www.vmware.com/go/horizonsuite

zur Verfügung, über das sie beispielsweise browserbasierte Anwendungen oder mit Hilfe von VMware ThinApp[33] virtualisierte Anwendungen nutzen können.

5.2.3 Microsoft

Mit Microsofts Virtualisierungsplattform Hyper-V 3.0[34] in Verbindung mit System Center 2012 SP1[35] lassen sich laut Microsoft Cloud-Infrastrukturen realisieren. Innerhalb der Betriebssysteme Windows Server 2008, 2008 R2 und 2012 ist Hyper-V als Serverrolle verfügbar. Weiterhin lässt sich Hyper-V separat als Hyper-V Server 2012 installieren.

System Center 2012 SP1 umfasst Werkzeuge zur Überwachung und Verwaltung von physischen sowie virtuellen und Cloud-Infrastrukturen, Anwendungen und Produkten verschiedener Drittanbieter. Weiterhin dient es unter anderem zur Softwareverteilung, Inventarisierung, Patch- und Updatemanagement, Überwachung, Datensicherung, Servicemanagement und Prozessautomatisierung. Dabei unterstützt es nicht nur Betriebssysteme und Hypervisoren von Microsoft, sondern beispielsweise auch Linux/Unix, VMware vSphere und Citrix XenServer. [vgl. FLLF13, S. 11ff., FVLF12, S. 13ff.]

Primär dienen Windows Server 2012 und System Center 2012 SP1 der Realisierung und Verwaltung von Private-Cloud-Umgebungen innerhalb von Unternehmen, insbesondere für den Bereich IaaS. Über den im System Center 2012 enthaltenen Configuration Manager lassen sich Applikationen für die Nutzung durch Anwender bereitstellen, was den Bereich SaaS bedienen könnte. Dabei ist ggf. noch der Einsatz weiterer Komponenten der System-Center-Familie notwendig. Zusätzlich lassen sich Angebote aus Microsofts Public-Cloud-Plattform Windows Azure einbinden, so dass eine Hybrid Cloud entsteht.

Für Dienstanbieter ist die Erweiterung Service Provider Foundation seit System Center 2012 SP1 enthalten. Damit sollen sich mandantenfähige Selfservice-Portale erstellen lassen, womit Dienstanbieter auch Public Clouds zur öffentlichen Nutzung aufbauen können.

Mit dem neuen Produkt Windows Azure Pack[36] für den Windows Server möchte Microsoft Windows Azure Technologie frei verfügbar machen. Mit dieser Technologie werden Unternehmen und Dienstanbieter in die Lage versetzt, Cloud-Umgebungen nach dem Vorbild von Windows Azure eigenständig zu realisieren und zu verwalten. Insbesondere betrifft dies die Bereiche IaaS und PaaS. Das Windows Azure Pack ersetzt damit den Vorgänger Windows Azure Services for Windows Servers. [vgl. Mic13a, S. 6ff., Mic13b, S. 1]

[33] VMware ThinApp: http://www.vmware.com/de/products/desktop_virtualization/thinapp/overview
[34] Microsoft Hyper-V: http://www.microsoft.com/de-de/server/windows-server/server-virtualisierung/default.aspx
[35] Microsoft System Center: http://www.microsoft.com/de-de/server/system-center/2012.aspx
[36] Microsoft Windows Azure Pack: http://www.microsoft.com/en-us/server-cloud/windows-azure-pack.aspx

Glossar

Appliance Ein kombiniertes System aus Hardware und speziell auf diese Hardware optimierter Software wird als Appliance bezeichnet. Im Wesentlichen dient eine Appliance einer oder wenigen Anwendungen. 36, 39, 43

Application Layer Firewall Eine Application Layer Firewall betrachtet zusätzlich zu den reinen Verkehrsdaten wie Quelle, Ziel und Dienst zusätzlich den Inhalt der Netzwerkpakete. 36

BIOS Das BIOS (Basic Input/Output System) ist quasi die Systemfirmware eines Computers. Es beinhaltet die grundlegende Konfiguration der Hardware und startet weiterhin das Betriebssyystem. 24

Configuration Management Database Eine CMDB ist eine Datenbank für Zugriff und Verwaltung von Configuration Items. Als Configuration Item können alle Betriebsmittel aus dem IT-Bereich bezeichnet werden. 41, 72

Content Filter Der Content Filter ist Teil einer Application Layer Firewall und kann die Nutzdaten einer Verbindung analysieren, um beispielsweise Schadsoftware herauszufiltern. 36

Content Switching Content Switching ist eine Form von Load Balancing, bei der Router oder Switches die Verteilung der Anfragen abhängig vom Dateninhalt steuern. 36

Deduplikation Datenbestände enthalten je nach Anwendung redundante Informationen, was zu einer Vielzahl gleicher Datensegmente führt. Mit Deduplikation werden Segmente mit gleichem Inhalt nur einmalig vorgehalten, was den Speicherbedarf erheblich verringern kann. 25

Disaster Recovery Disaster Recovery in der Informationstechnik, im Deutschen auch Notfallwiederherstellung, bezeichnet Maßnahmen nach einem Katastrophenfall. Dazu zählen

die Wiederherstellung der Datenbestände sowie die kurzfristige Wiederaufnahme der Geschäftstätigkeit. 35, 40

Failover Ein Failover ist bei einem fehlertoleranten System die Funktion einer Komponente, die im Fehlerfall von einer redundaten Komponente übernommen wird. 38

Framework Auch Rahmenwerk oder Grundstruktur. Wird gleichermaßen in der Softwareentwicklung, Organisation und dem Vertragswesen verwendet. 15

Host Als Virtualisierungs-Host oder einfach Host wird das Wirtsystem bezeichnet, welches den Hypervisor für den Betrieb von Gastsystemen beherbergt. 34, 35, 38, 43, 44, 49–54

Information Life Cycle Management Umfasst Strategien, Methoden und Anwendungen, um Informationen automatisiert entsprechend ihrem Wert und ihrer Nutzung optimal auf dem jeweils kostengünstigsten Speichermedium bereitzustellen, zu erschließen und langfristig sicher aufzubewahren. 25, 73

ISO-Abbild Ein ISO-Abbild oder ISO-Image bezeichnet eine Datei, die ein Speicherabbild des Inhalts einer CD oder DVD, die im Format ISO 9660 strukturiert ist, beinhaltet. 47, 49

IT Infrastructure Library Die ITIL ist eine Sammlung von Erfolgsmethoden in einer Reihe von Publikationen zur Umsetzung eines IT-Service-Managements und gilt international als Industriestandard. Das Regel- und Definitionswerk beschreibt die für den Betrieb einer IT-Infrastruktur notwendigen Prozesse, Aufbauorganisationen und Werkzeuge. 31, 73

JavaScript Object Notation kurz JSON, ein kompaktes Datenformat in für Mensch und Maschine einfach lesbarer Textform zum Zweck des Datenaustauschs zwischen Anwendungen. 73

Lifecycle-Management Bei virtuellen Maschinen bedeutet Lifecycle-Management das Verwalten und Nachverfolgen von virtuellen Maschinen von der Bereitstellung bis zur Löschung. Es verhindert Wildwuchs in der virtualisierten Infrastruktur und die unnötige Belegung von teuren Ressourcen. 40, 53

Load Balancing Mittels Load Balancing (Lastverteilung) wird eine große Anzahl von gleichzeitigen Anfragen auf mehrere parallel arbeitende Systeme verteilt. 36, 39, 47, 49

Mandantenfähigkeit Verschiedene Anwender können auf demselben Server oder System arbeiten, ohne dass sie gegenseitigen Einblick in ihre Daten, Benutzerverwaltung usw. haben. 5, 8, 18, 22, 25, 30, 32, 35, 38, 39, 45, 51, 59, 66

Middleware Bezeichnet in der Informatik anwendungsneutrale Programme, die auf eine Weise zwischen Anwendungen vermitteln, so dass die Komplexität dieser Anwendungen und ihre eigentliche Infrastruktur dem Anwender verborgen bleiben. 9, 15, 40

Perimeter In der Informationstechnik bezeichnet ein Perimeter ein Netzwerksegment, das an der Schnittstelle von zwei Netzwerken steht. Oftmals ist dies der Übergang vom Intranet zum Internet. 39

Port Forwarding Port Forwarding (Portweiterleitung) bezeichnet das Weiterleiten einer Verbindung, die über ein Netzwerk auf einem bestimmten Port eingeht, zu einem anderen Computer. 47

Quality of Service Auch Dienstgüte genannt, beschreibt alle Verfahren, die den Datenfluss in Netzwerken so beeinflussen, dass der Dienst mit einer festgelegten Qualität beim Empfänger ankommt. 9

Scrum Scrum ist ein Rahmenwerk, um Projekte auf Basis der Grundsätze der agilen Softwareentwicklung durchzuführen. 2

Security Group Security Groups sind eine Technik zur Kontrolle und Isolation von Netzwerkverkehr bei virtuellen Maschinen. Eine Security Group verhält sich wie eine Firewall, die den ein- und ausgehenden Datenverkehr von zugehörigen virtuellen Maschinen anhand von Regeln überwacht. Sie arbeiten auf Schicht 3 des OSI-Schichtenmodells. Virtuelle Maschinen können zu einer oder mehreren Security Groups gehören. 51, 53

Selfservice Nutzer (Kunden) werden durch interaktive Medien (z.B. Internet) dazu befähigt, selbstständig eine Dienstleistung in Anspruch zu nehmen. Dies stellt also eine Schnittstelle zwischen ihnen und dem Dienstleister (Unternehmen) dar. 10, 18, 22, 35, 40, 47, 48, 66

Service Level Agreement Auch Dienstgütevereinbarung genannt. Bezeichnet eine Vereinbarung zwischen Kunde und Dienstleister für wiederkehrende Dienstleistungen. Zugesicherte Leistungseigenschaften wie Leistungsumfang, Reaktionszeit und Schnelligkeit der Bearbeitung sollen genau definiert und für den Kunden kontrollierbar sowie transparent

sein. Wichtiger Bestandteil ist dabei die Dienstgüte (Servicelevel), welche die vereinbarte Leistungsqualität beschreibt. 22, 74

Single Point of Failure Bei einem Single Point of Failure führt der Ausfall eines Bestandteils eines technischen Systems zum Ausfall des gesamten Systems. 35

Skaleneffekten Von Skaleneffekten spricht man, wenn bei steigender Ausbringungsmenge die variablen Stückkosten sinken. Dies wird auch als Economies of Scale bezeichnet. 32

Snapshot Beim Snapshot wird ein Abbild des Dateisystems und Arbeitsspeichers einer virtuellen Maschine zu einem bestimmten Zeitpunkt erstellt. Zu einem späteren Zeitpunkt kann man so zu diesem Stand zurückkehren. 25, 47–49

SOAP Standardisiertes Nachrichtenprotokoll über das Kommunikation zwischen verteilten Anwendungen ermöglicht wird. 28

Storage Area Network Beschreibt dedizierte Speichernetze, welche Server und Speichersysteme über Breitbandnetze, wie Fibre Channel, miteinander verbinden und gegenseitig entkoppeln. 25, 74

Thin Client Bezeichnet einen Computer als Endgerät (Terminal) eines Netzwerks, dessen Ausstattung auf die Ein- und Ausgabe beschränkt ist und nicht für die lokale Verarbeitung der Daten zuständig ist. 27

Thin Provisioning Physischer Speicher wird erst dann zugeteilt, wenn die Anwendung diesen benötigt. Das setzt voraus, dass die Speicher nicht vollständig verplant sind und nicht belegte Speicherbereiche verschoben werden können. Thin Provisioning reduziert dadurch den tatsächlichen Speicherbedarf. 25

USA PATRIOT Act Ein Gesetz in den USA, welches die Ermittlungen der Bundesbehörden im Fall einer terroristischen Bedrohung vereinfachen soll. Hierzu werden bestimmte, auch die Grundrechte betreffende, Gesetze eingeschränkt und durch weitere Regelungen ergänzt oder ersetzt. 31

vApp Unter anderem virtuelle Maschinen werden in VMwares vCloud Director als vApps bezeichnet. vApps sind Container, die eine oder mehrere virtuelle Maschinen und unter anderem die zugehörige Netzwerkkonfiguration enthalten. 39, 40, 42, 48, 53

Vendor-Lock-in Verbraucher werden durch finanzielle Investitionen in bestimmte Technologien (Betriebssystem bzw. Laufzeitumgebung) an einen Anbieter gebunden (Herstellerabhängigkeit) 15, 33

VXLAN Virtual Extensible LAN erstellt logische Layer-2-Netzwerke, die in Layer-3-IP-Paketen gekapselt werden. Die logischen VXLAN-Netzwerke unterscheiden sich durch eine Segment-ID in jedem Frame voneinander, sodass keine VLAN-Tags erforderlich sind. Dies ermöglicht die parallele Verwendung einer großen Anzahl von isolierten Layer-2-VXLAN-Netzwerken in einer gemeinsamen Layer-3-Infrastruktur bei vollständiger Isolation voneinander und vom zugrunde liegenden Netzwerk. 26, 74

Web Services Description Language Beschreibungssprache für Webservices zum Austausch von Nachrichten auf Basis von XML. WSDL wird häufig in Verbindung mit SOAP und dem XML-Schema verwendet, um Webservices zu erstellen. 28, 74

Abkürzungsverzeichnis

API Application Programming Interface 15, 28, 33, 34, 36, 37, 39, 45, 47–49, 52–55

AWS Amazon Web Services 36, 40, 47, 48, 59, 60

BDSG Bundesdatenschutzgesetz 31, 32

BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. 1

BSI Bundesamt für Sicherheit in der Informationstechnik 17, 25, 31

CMDB Configuration Management Database 41

CPBM CloudPortal Business Manager 56

CRM Customer Relationship Management 35, 48

DHCP Dynamic Host Configuration Protocol 39, 47, 48

DNS Domain Name System 47

DoS Denial of Service 30, 36

DPM Distributed Power Management 52, 53, 55

DRS Distributed Resources Scheduler 38, 52, 53, 55

EC2 Elastic Compute Cloud 40, 47, 48

ENISA European Network and Information Security Agency 17

FTP File Transfer Protocol 28

GUI Graphical User Interface 16

HTML Hypertext Markup Language 28

HTTP Hypertext Transfer Protocol 28, 45, 49

IaaS Infrastructure as a Service 6, 7, 13–17, 19, 30, 34–36, 43, 44, 46, 48, 59, 62–64, 66

IEC International Electrotechnical Commission 31

ILM Information Life Cycle Management 25

ISO International Organization for Standardization 25, 31

ISP Internet Service Provider 23

ITIL IT Infrastructure Library 31

JSON JavaScript Object Notation 28

KMU kleine und mittelständische Unternehmen 31, 33

KVM Kernel-based Virtual Machine 44, 50, 53

LAN Local Area Network 25, 26

LDSG Landesdatenschutzgesetz 31

MAC Message Authentication Code 30

NAT Network Address Translation 39, 47, 48

NIST National Institute of Standards and Technology 3, 16–19, 43, 44, 46, 59, 60, 62–65

OVF Open Virtualization Format 48

PaaS Platform as a Service 6, 7, 13–17, 19, 30, 34, 35, 64–66

RDP Remote Desktop Protocol 27

REST Representational State Transfer 28, 39, 45, 49

SaaS Software as a Service 6, 7, 13–17, 19, 30, 34, 64–66

SAN Storage Area Network 25

SDK Software Development Kit 36

SGB Sozialgesetzbuch 31

SLA Service Level Agreement 22, 30, 41

SMAPI Storage Manager API 34

SMTP Simple Mail Transfer Protocol 28

SOA Serviceorientierte Architektur 21, 28, 29

SPB Shortest Path Bridging 26

TCP/IP Transmission Control Protocol/Internet Protocol 45

TKG Telekommunikationsgesetz 31

TMG Telemediengesetz 31

VDI Virtual Desktop Infrastructure 27

VLAN Virtual Local Area Network 26, 51, 53

VM Virtuelle Maschine 7, 21–25, 27, 34, 38–42, 47–51, 53–56, 59, 60, 65

VMM Virtual Machine Monitor 23, 24

VPN Virtual Private Network 26, 39, 47, 48, 59, 60, 63

VXLAN Virtual Extensible LAN 26, 39, 51, 54

WSDL Web Services Description Language 28

XaaS Everything as a Service 7, 16

XAPI Xen Management API 34

XML Extensible Markup Language 28

Literaturverzeichnis

[BIT09] BITKOM: *Cloud Computing - Evolution in der Technik, Revolution im Business.* 2009. – BITKOM-Leitfaden

[BIT12a] BITKOM: *Desktop-Virtualisierung.* 2012. – BITKOM-Leitfaden

[BIT12b] BITKOM: *Speichervirtualisierung.* 2012. – BITKOM-Leitfaden

[BK13] BITKOM ; KPMG: *Cloud-Monitor 2013 - Cloud-Computing in Deutschland - Status quo und Perspektiven.* 2013. – Studie

[BKNT11] Baun, Christian ; Kunze, Marcel ; Nimis, Jens ; Tai, Stefan: *Cloud computing : Web-basierte dynamische IT-Services.* 2. Aufl. Berlin : Springer DE, 2011. – ISBN 978–3–642–18435–2

[BSI] BSI: *Cloud Computing Grundlagen.* https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html, Abruf: 09.03.2013

[Cit12a] Citrix: *CloudBridge 2.0.* http://support.citrix.com/proddocs/topic/cloudbridge/cb-2-0-wrapper-con.html. Version: 2012, Abruf: 02.05.2013

[Cit12b] Citrix: *NetScaler 10.* http://support.citrix.com/proddocs/topic/netscaler/ns-gen-netscaler10-wrapper-con.html. Version: 2012, Abruf: 02.05.2013

[Cit13a] Citrix: *Citrix CloudPlatform for the service provider.* 2013. – White Paper

[Cit13b] Citrix: *CloudPlatform (powered by Apache CloudStack) Version 3.0.6 Installation Guide.* 2013. – Handbuch

[Cit13c] Citrix: *How CloudPortal Business Manager works.* http://www.citrix.de/products/cloudportal-business-manager/how-it-works.html. Version: 2013, Abruf: 02.05.2013

[Cit13d] Citrix: *Overview of CloudPortal Business Manager*. http://support.citrix.com/proddocs/topic/ccpb-20-map/ccpb-overview-20.html. Version: 2013, Abruf: 02.05.2013

[Cru12] Crusco, Rich: *XenCenter » XenServer - Citrix Community*. http://community.citrix.com/xencenter. Version: 2012, Abruf: 28.04.2013

[Fer12] Ferber, Christian: *CloudPlatform & Portal Business Manager - Infrastructure-as-a-Service*. 2012. – Präsentation

[FLLF13] Finn, Aidan ; Lownds, Patrick ; Luescher, Michel ; Flynn, Damian: *Windows Server 2012 Hyper-V Installation and Configuration Guide*. New York, NY : John Wiley, 2013. – ISBN 978–1–11–848649–8

[FVLF12] Finn, Aidan ; Vredevoort, Hans ; Lownds, Patrick ; Flynn, Damian: *Microsoft Private Cloud Computing*. New York, NY : John Wiley, 2012. – ISBN 978–1–11–825147–8

[Gó12] Gómez, Jorge Carlos M.: *Serviceorientierte Architektur*. http://www.oldenbourg.de:8080/wi-enzyklopaedie/lexikon/is-management/Systementwicklung/Softwarearchitektur/Architekturparadigmen/Serviceorientierte-Architektur/. Version: 2012, Abruf: 20.03.2013

[Hal12] Haluschak, Bernhard: *VMware stellt die neue vCloud Suite 5.1 vor*. http://www.tecchannel.de/server/cloud_computing/2039620/vsphere_vcenter_srm_vcloud_director_vmware_stellt_die_neue_vcloud_suite_51_vor/. Version: 2012, Abruf: 11.04.2013

[Har12] Harzog, Bernd: *VMware Launches vFabric Application Director | The Virtualization Practice*. http://www.virtualizationpractice.com/news-vmware-blows-away-the-image-launches-vfabric-application-director-15105/. Version: 2012, Abruf: 10.04.2013

[IS12a] IT-Solutions, Silpion: *SILPION | IT-Solutions*. http://www.silpion.de/infrastruktur/cloudcomputing. Version: 2012, Abruf: 01.03.2013

[IS12b] IT-Solutions, Silpion: *Silpion IT-Solutions GmbH | XING Unternehmen.* https://www.xing.com/companies/silpionit-solutionsgmbh. Version: 2012, Abruf: 01.03.2013

[iX12] iX: *Experten: US-Behörden haben Zugriff auf europäische Cloud-Daten.* http://www.heise.de/ix/meldung/Experten-US-Behoerden-haben-Zugriff-auf-europaeische-Cloud-Daten-1763733.html. Version: 2012, Abruf: 21.03.2013. – News-Meldung

[JY12] Joshi, Abhinav ; Yu, Wen: *A Preview of VMware vCloud Director.* 2012 https://communities.netapp.com/docs/DOC-7536

[KZ12] Kraus, Matthias ; Zacher, Matthias: *Cloud Computing in Deutschland 2012 – Evolution der Revolution.* 2012. – IDC-Studie

[Lip11] Lipsky, Stefanie: *Cloud Computing - eine Abgrenzung zum IT-Outsourcing und Systematisierung möglicher Sourcingoptionen.* Münster : IfG, 2011

[Low11] Lowe, Scott: *Mastering VMware vSphere 5.* New York, NY : John Wiley, 2011. – ISBN 978–0470890806

[Mey12] Meyer, Jörn: *Serie C-L-O-U-D: 3. Delivery-Block (Netzwerk-Virtualisierung).* http://blog.cloudmacher.de/index.php/blog/serie-c-l-o-u-d-schichtenmodell-netzwerk-virtualisierung/. Version: 2012, Abruf: 19.03.2013

[MH11] Meir-Huber, Mario: *Cloud Computing : Praxisratgeber und Einstiegsstrategien.* 2., aktualisierte Aufl. Frankfurt, M. : Entwickler.press, 2011. – ISBN 978–3–86802–076–2

[Mic13a] Microsoft: *Microsoft Private Cloud: Making It Real.* 2013. – White Paper

[Mic13b] Microsoft: *Overview: Windows Azure Pack for Windows Servers.* 2013. – White Paper

[MRV11] Metzger, Christian ; Reitz, Thorsten ; Villar, Juan: *Cloud Computing - Chancen und Risiken aus technischer und unternehmerischer Sicht.* München : Hanser Fachbuchverlag, 2011. – ISBN 978–3–446–42454–8

[MWRS11] Meinel, Christoph ; Willems, Christian ; Roschke, Sebastian ; Schnjakin, Maxim: *Virtualisierung und Cloud Computing : Konzepte, Technologiestudie, Marktübersicht*. Potsdam : Universitätsverlag Potsdam, 2011. – ISBN 978–3–869–56113–4

[NIS11] NIST: *The NIST Definition of Cloud Computing*. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Version: 2011, Abruf: 03.03.2013. – Special Publication

[RM10] Rosenberg, Jothy ; Mateos, Arthur: *The Cloud at Your Service - The When, How, and Why of Enterprise Cloud Computing*. Pap/Psc. Birmingham : Manning, 2010. – ISBN 978–1–935–18252–8

[Som12] Sommergut, Wolfgang: *VMware erweitert sein Angebot an Management-Tools*. http://www.computerwoche.de/a/vmware-erweitert-sein-angebot-an-management-tools,2526479. Version: 2012, Abruf: 10.04.2013

[Sos10] Sosinsky, Barrie: *Cloud Computing Bible*. 1. Auflage. New York, NY : John Wiley & Sons, 2010. – ISBN 978–0–470–90356–8

[TV11] Terplan, Kornel ; Voigt, Christian: *Cloud Computing*. 1. Aufl. Heidelberg; München; Landsberg; Frechen; Hamburg : mitp, 2011. – ISBN 978–3–826–69098–3

[VMw12a] VMware: *Installations- und Upgrade-Handbuch für vShield*. 2012. – Handbuch

[VMw12b] VMware: *vCloud Director Administratorhandbuch - vCloud Director 5.1.1*. 2012. – Handbuch

[VMw12c] VMware: *VMware vCenter Operations Manager - Getting Started Guide*. 2012. – Handbuch

[VMw12d] VMware: *VMware vCloud Automation Center*. http://www.vmware.com/files/pdf/management/vmw-vcloud-automation-center-faq.pdf. Version: 2012, Abruf: 10.04.2013. – FAQ

[VMw13a] VMware: *Datenblatt: VMware vCenter Operations Management Suite*. http://www.vmware.com/files/de/pdf/vcenter/VMware-vCenter-Operations-Management-Suite-Datasheet.pdf. Version: 2013, Abruf: 11.04.2013

[VMw13b] VMware: *Datenblatt: VMware vCloud Networking and Security.* http://www.vmware.com/files/de/pdf/VMware-vCloud-Networking-and-Security-Datasheet.pdf. Version: 2013, Abruf: 10.04.2013. – Datenblatt

[VMw13c] VMware: *Datenblatt: VMware vCloud Suite.* http://www.vmware.com/files/de/pdf/VMware-vCloud-Suite-Datasheet.pdf. Version: 2013, Abruf: 11.04.2013. – Datenblatt

[VMw13d] VMware: *Datenblatt: VMware vFabric Hyperic.* http://www.vmware.com/files/de/pdf/VMware-vFabric-Hyperic-Datasheet.pdf. Version: 2013, Abruf: 11.04.2013

[VMw13e] VMware: *FAQ zur VMware vCloud Connector-Cloud-Managementsoftware.* http://www.vmware.com/de/products/datacenter-virtualization/vcloudconnector/faq.html. Version: 2013, Abruf: 09.04.2013

[VMw13f] VMware: *Funktionen von VMware vCloud Networking and Security: Softwaredefiniertes Netzwerk.* http://www.vmware.com/de/products/datacenter-virtualization/vcloud-network-security/features.html. Version: 2013, Abruf: 10.04.2013

[VMw13g] VMware: *VMware vCenter Configuration Manager: Virtual Data Center Compliance.* http://www.vmware.com/de/products/datacenter-virtualization/configuration-manager/overview.html. Version: 2013, Abruf: 11.04.2013

[VMw13h] VMware: *VMware vCenter Infrastructure Navigator.* http://www.vmware.com/de/products/datacenter-virtualization/vcenter-infrastructure-navigator/features.html. Version: 2013, Abruf: 11.04.2013

[VMw13i] VMware: *VMware vCenter Operations Management Suite: Hybrid Cloud Computing.* http://www.vmware.com/de/products/datacenter-virtualization/vcenter-operations-management/overview.html. Version: 2013, Abruf: 10.04.2013

[VMw13j] VMware: *VMware vCloud Director: sichere private Clouds, Infrastructure as a Service.* http://www.vmware.com/de/products/datacenter-

virtualization/vcloud-director/overview. Version: 2013, Abruf: 09.04.2013

[VMw13k] VMware: *VMware vCloud Networking and Security Softwaredefiniertes Netzwerk: Funktionsweise.* http://www.vmware.com/de/products/datacenter-virtualization/vcloud-network-security/how-it-works.html. Version: 2013, Abruf: 10.04.2013

[Xen13] Xen: *Xen Overview - Xen.* http://wiki.xen.org/wiki/Xen_Overview. Version: 2013, Abruf: 28.04.2013

[ZWS+12] Zimmer, Dennis ; Wöhrmann, Bertram ; Schäfer, Carsten ; Baumgart, Günter ; Kügow, Oliver ; Alder, Urs S. ; Brunner, Marcel: *VMware vSphere 5 - Das umfassende Handbuch.* 2. Aufl. Bonn : Galileo Press GmbH, 2012. – ISBN 978–3–836–21847–4

Hiermit versichere ich, dass ich die vorliegende Arbeit nach §16 (5) APSO-TI-BM ohne fremde Hilfe selbstständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Hamburg, 20. August 2013 Martin Slowikowski