Cloud Enabling

Umzug ins IaaS

Torsten Opitz

Ein virtuelles Cloud-Rechenzentrum auf Basis einer „Infrastructure as a Service" (IaaS) besticht durch ein schnelles Setup: Der Zugang ist sofort verfügbar, über ein Web-API lassen sich eigene Systeme sofort anlegen und administrieren, Lieferzeiten für Hardware gehören der Vergangenheit an. Das verleitet dazu, Applikationen „mal eben" in die Cloud auszulagern. Unsere Erfahrung zeigt: Es funktioniert, wenn die Architektur zu Beginn sauber definiert wurde. Gute Vorbereitung vermeidet nachgelagerte Management- und Servicekosten und Probleme im Betrieb. Zur Architekturdefinition gehört ein Cloud-fähiges Konzept für Datensicherheit.

Geplante Wolkenbildung

Zu hohe Kosten im Rechenzentrumsbetrieb, zu lange Wartezeiten beim Bearbeiten von Serviceanfragen und ungenügende Servicequalität trotz vertraglich vereinbarter Service Levels – angesichts dieser Gemengelage überdachte ein von einem Konzern neu ausgegründetes Start-up seine Rechenzentrumsstrategie. Bei der Analyse der Optionen legte dieser Kunde auf drei Faktoren wert:

- *Kosten:* Das Unternehmen hatte wenig Spielraum für kostenintensive IT-Systeme, gesucht war eine skalierbare Lösung mit einer transparenten Kostenstruktur.
- *Datenhoheit:* Die Unternehmensdaten müssen rechtlich sicher auf Servern in Deutschland liegen.
- *Skalierbarkeit:* Das Geschäft des Unternehmens im Touristik-Bereich unterliegt sehr starken saisonalen Schwankungen. Darauf muss es kurzfristig reagieren und die Systemperformance optimieren.

Es gibt nur eine Handvoll Anbieter für virtuelle Rechenzentren auf dem deutschen Markt, die für das Vorhaben in Frage kamen. Nach genauer Analyse stellte sich heraus, dass sich die Anforderungen am besten mit „Infrastructure as a Service" (IaaS) abdecken lassen: Dabei mietet das Unternehmen Server in einem externen Rechenzentrum. Die Server können auf Knopfdruck hochgefahren werden und stehen binnen weniger Minuten bereit. Kosten fallen nur für tatsächlich gestartete Server an. Bauliche Infrastruktur wie Kühlung oder Brandschutz ist inklusive, Software und Hardware für die Betriebsinfrastruktur stellt das Unternehmen selbst.

Anhand der technischen und organisatorischen Anforderungen entschied sich das Projektteam für einen IaaS-Provider und wählte für die Testphase drei unkritische Intranet-Applikationen mit mittlerer Komplexität aus.

Das Ziel: Kosten zuverlässig planen

Im Vordergrund standen die Kosten. Ein IaaS-Geschäftsmodell für vermietete Hardware hat andere Voraussetzungen als ein Rechenzentrum, das inklusive Hardware, Applikationen und Service-Leistungen vom Dienstleiter gestellt und betrieben wird. Hardware wird nicht erworben oder geleast, sondern ist beim Cloud-Anbieter vorhanden. Abgerechnet werden nur die Kosten für Komponenten wie Core, RAM, erzeugten Traffic oder IP-Adressen. Der Applikationsbetreiber setzt sein Rechenzentrum über ein Web-Interface auf und skaliert es.

Um die Ausgaben zu planen, bietet sich ein Monitoring für die Verbrauchsparameter wie Traffic, Core, RAM an. Die Lizenzgebühren für Business-Software sind zunächst unabhängig davon, ob die Anwendung in der Cloud oder im eigenen Rechenzentrum betrieben wird. Meistens orientiert sich die Höhe der Lizenz an den benutzten Cores. Hier waren wir erstaunt, dass viele Hersteller noch über kein schlüssiges Lizenzmodell für eine sich immer wieder ändernde Anzahl an Cores in der Cloud verfügen. Als Ausweg begrenzten wir die maximale Anzahl Cores auf dem Server und lizenzierten diese Anzahl.

Architekturkonzept senkt den Umzugsaufwand

In der Testphase zogen drei Applikationen mit mittlerer Komplexität in das Cloud-Rechenzentrum: Confluence, Jira und SpiraTest. Um etwas für Umzug und Betrieb anderer Anwendungen zu lernen, galten für sie die gleichen Sicherheits- und Performanceanforderungen wie für kritische interne Anwendungen oder externe Web-Angebote. Die drei Systeme sind untereinander gering gekoppelt, das virtuelle Rechenzentrum bleibt für einen späteren Ausbau flexibel.

Von der Geschwindigkeit im initialen Infrastruktur-Setup waren wir positiv überrascht: Der Zugang zum virtuellen Rechenzentrum ist sofort verfügbar. Es gibt keine Wartezeiten wie bei herkömmlichen Bestellprozessen von Hardware. Binnen weniger Stunden hatten wir uns mit dem Web-API vertraut gemacht und eigene Systeme angelegt und administriert. Eine wichtige Voraussetzung dafür waren klar definierte Architekturanforderungen: Im ersten Schritt analysierte das IT-Management die vorhandene Enterprise-IT-Architektur und legte die Zielarchitektur für die IaaS-gehosteten Anwendungen im Detail fest. Über den Top-Down-Ansatz wurden die Architekturanforderungen an das virtuelle Rechenzentrum analysiert, spezifiziert, bewertet und umgesetzt. Besondere Aufmerksamkeit lag auf den Abhängigkeiten zum Betriebssystem und den einzusetzenden Tools. Weitere Faktoren waren Sicherheits-, Ressourcen- und Performanceaspekte.

Die Projektbeteiligten verständigten sich mittels Infrastruktur-Grafiken schnell über den Systemkontext mit seinen Schnittstellen zu Nachbarsystemen (abstrahiert in Abb. 1). So erkannten sie auf den ersten Blick potenzielle Schwierigkeiten

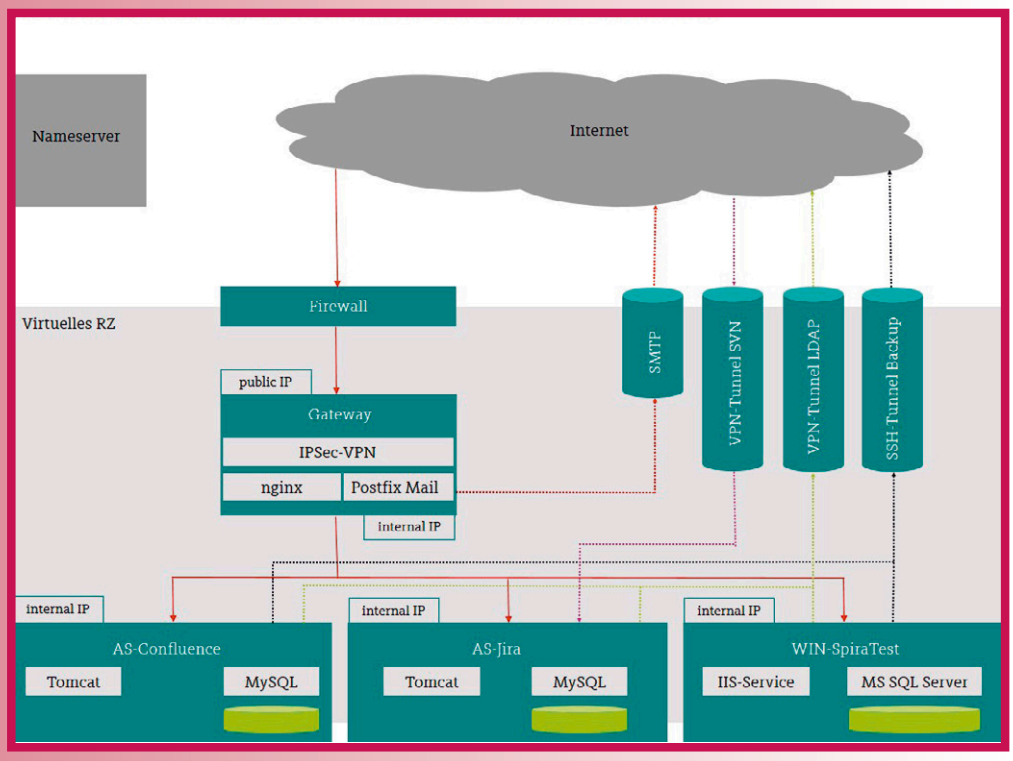

Abb. 1: Schematische Übersicht über das virtuelle Rechenzentrum

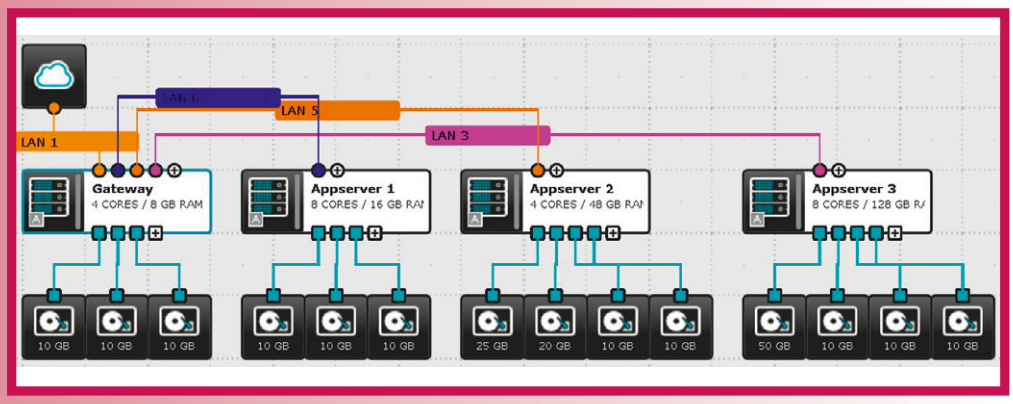

Abb. 2: Beispielhafte Serverlandschaft beim IaaS-Dienstleister (Quelle: ProfitBricks)

und Risiken beim Anbinden an das bestehende IT-Rechenzentrum. Das Umzugsprojekt war nach Scrum in Sprints aufgeteilt. Die Kombination dieser Faktoren ermöglichte es, mit dem Chefarchitekt und -designer regelmäßige iterativ-inkrementelle Reviews durchzuführen.

In der Entwurfs- und Designphase traf unser Kunde konkrete infrastrukturelle Entscheidungen hinsichtlich der zukünftigen virtuellen Systeme. Er entschloss sich beispielsweise, für jede Applikation einen eigenen virtuellen Server mit je vier Partitionen aufzusetzen. Die Größe der Partitionen, die Anzahl von CPU und RAM und viele weitere hardwarenahe Themen waren Bestandteil des Infrastrukturkonzepts.

Zwei Vollzeitmitarbeiter konnten das virtuelle Rechenzentrum innerhalb von vier Wochen mit allen Installationen, Einstellungen, Konfigurationen und Datenmigrationen vollständig aufsetzen und ausrollen. Diese Effektivität, verbunden mit überschaubaren und vor allem planbaren Kosten, basierte auf der umfassenden Vorarbeit. Nun musste das Sicherheitskonzept auf verschiedenen Ebenen implementiert werden.

Sicherheit? So wie der Applikationsbetreiber es aufsetzt

Im Cloud-Modell „Infrastructure as a Service“ stellt der Anbieter nur die Server-Infrastruktur bereit. Um alle sicherheitsrelevanten Themen kümmert sich die IT-Abteilung des Applikationsbetreibers. Mit der Ausnahme „Server“: Der IaaS-Anbieter stellt den Betrieb seiner Cloud-Server sicher und behebt Hardwareschäden oder Fehler nach größeren Zwischenfällen. Dafür werden Daten über konfigurierbare Brandschutzzonen auf Servern redundant gespeichert. Das Vorgehen dient dazu, Server räumlich zu trennen und die Ausfallsicherheit der Anwendung zu erhöhen. Für die Daten ist der Anwendungsbetreiber verantwortlich: Er erstellt regelmäßige Backups und Snapshots. Sie sind bei einem zweiten Provider gespeichert, um anbieterunabhängig zu sein und im schlimmsten Fall eine Off-Site-Kopie der Daten zu haben. Der Datentransfer über das Internet wird verschlüsselt.

Beschaffung, Aufsetzen und Pflege von Intrusion-Detection-Systemen (IDS), Web Application Firewalls (WAF) oder anderen Schutzmaßnahmen vor externen Angriffen liegen beim Applikationsbetreiber, wie die Entscheidung, ob Datenpartitionen verschlüsselt werden sollen. Der Zugriff auf das virtuelle Rechenzentrum erfolgt über das Internet, die Sicherheitsaufwände sind aus diesem Grund nicht zu unterschätzen. Die Konzepte beschreiben – wie für selbst gehostete Rechenzentren auch – die Sicherheitsarchitektur aus Gateway, Firewall, VPN, SSL, Zertifikaten und Data Encoding.

Da es vereinzelt Abhängigkeiten zu Systemen gab, die nicht in die Cloud migriert werden konnten, wurde das virtuelle Rechenzentrum durch Site-2-Site-VPN-Verbindungen an die bestehende IT-Landschaft angebunden. Über einen Tunnel routen die Applikationen Daten bidirektional zwischen Cloud und bestehendem Rechenzentrum. Der Datenaustausch zwischen den Rechenzentren läuft nicht über das Unternehmensnetzwerk, sondern über das Internet, deshalb ist die Absicherung über VPN nötig.

Zentraler Zugriffspunkt für die Anwender ist ein vorgeschalteter separater Gateway-Server mit höchsten Sicherheitsanforderungen. Die vorgeschaltete Firewall blockiert an der Grenze des virtuellen Rechenzentrums jeglichen Traffic, für den Zugriff braucht der Nutzer verschlüsselte Zertifikate via VPN. SSH-Zugriff ist ebenfalls nur via VPN möglich. Die Ser-

ver hinter dem Gateway kommunizieren untereinander mit internen IP-Adressen. Über die VPN-Verbindung mit Zertifikaten wurden verschiedene Betriebssysteme angebunden – Windows, Unix und MacOSX für Server, Laptops und PCs und für mobile Endgeräte iOS und Android. Dafür kamen die nativen VPN-Clients der Client-Computer und mobilen Endgeräte zum Einsatz.

Bei der Sicherheitskonzeption wurden zukünftige Prozesse berücksichtigt, vor allem Konzepte zum Erstellen, Verwalten und Deaktivieren der X.509-signierten Root- und Client-Zertifikate. Eine separate XCA-Applikation zur Übernahme dieser Funktionalität wurde auf einem eigenen Zertifikatsserver außerhalb des virtuellen Rechenzentrums aufgesetzt und eingeführt.

Performance skaliert mit den Zugriffen

Das virtuelle Rechenzentrum wird über einen Infrastruktur-Designer administriert und gesteuert. Das Tool ist als Web-API verfügbar. Der Betrieb erstellt und startet im Infrastruktur-Designer schnell und einfach neue virtuelle Server, Festplatten und Netzwerkverbindungen. Die Eigenschaften dieser Hardwarekomponenten sind dynamisch skalierbar. Die Anzahl der Cores je Server, die Höhe des Arbeitsspeichers pro Rechner und die Größe der Festplattenpartition sind konfigurierbar. Nicht benötigte Systemressourcen können ohne Voranmelden jederzeit freigeben werden. Für nicht in Anspruch genommene Ressourcen fallen keine Hardware-Kosten an.

Mit dem Start-Stopp-Feature des Web-API können gezielt Server deaktiviert werden. Die konfigurierten Server-, CPU- und RAM-Eigenschaften bleiben erhalten, wie etwa IP-Adressen. Um einen Single Point of Failure zu vermeiden, sollten auch weiterhin Cluster oder Farms verwendet werden. Änderungen infrastruktureller Art können innerhalb weniger Minuten im Web-API freigeben und auf das virtuelle Rechenzentrum angewendet werden (Provisionierung). Die Kosten bleiben planbar. Wartezeiten und Bestellprozesse für Hardware entfallen komplett.

Schnelle Provisionierung, gut geplant

Die Testphase der drei Anwendungen im virtualisierten IaaS-Rechenzentrum ist abgeschlossen. Das IaaS-Angebot hält das Versprechen von Cloud-Services, schnell und einfach Infrastruktur bereitzustellen. Die Server-Infrastruktur ist sofort verfügbar.

Das sollte jedoch nicht dazu verleiten, „mal schnell" eine Anwendung in die Cloud umzuziehen: Nach unserer Erfahrung ist eine saubere Architekturdefinition Grundlage für einen zügigen Umzug zusätzlicher Anwendungen in die Cloud. Das spart Projektkosten und -laufzeit. Auch wenn der Applikationsbetreiber die Hardware nicht mehr warten und erneuern muss, bleibt er für den Betrieb verantwortlich. Bei IaaS braucht man zudem erfahrende IT-Architekten, die die etablierten Sicherheitsmaßnahmen auf ein Cloud-Rechenzentrum ausrollen.

Die IT-Abteilung des IaaS-Kunden arbeitet mit einem virtuellen Rechenzentrum, das bei saisonalen Schwankungen optimal und in Echtzeit skaliert. Das ist in der Regel kostengünstiger, als die Maximalzahl Server für Lastspitzen permanent selbst zu hosten. IT-Lösungen lassen sich so schneller umsetzen – auch nur testweise. Damit verbessert die IT ihre Time-to-Market von Projekten oder Services. Das ist besonders wertvoll im E-Commerce-Umfeld oder bei innovativen Produkten mit kurzer Halbwertszeit.

Torsten Opitz ist seit 1999 als Softwareentwickler, IT-Architekt und Projektleiter bei MaibornWolff. Sein Schwerpunkt liegt auf der verantwortlichen technischen und organisatorischen Leitung von IT-Projekten sowie auf der Implementierung komplexer Webanwendungen mit verschiedenen Java SE-Technologien.
E-Mail: torsten.opitz@maibornwolff.de