Bulletproof fail over: Passive first!

Christoph Münch, virtual7 GmbH

Wer sich mit hochverfügbaren IT-Systemen beschäftigt, steht oft vor dem Problem, die zu planende Umgebung so aufzubauen, dass sie im besten Fall 24/7 verfügbar ist. Gleichzeitig ist es aber notwendig, darauf zu achten, dass sich dieses Gesamtwerk für Wartungsarbeiten sowie Backup-und Recovery-Maßnahmen eignet. Wer offen gegenüber völlig neuen Konzepten ist und gleichzeitig nicht nur Spaß an der IT hat, sondern auch eine gehörige Portion Humor mitbringt, den wird dieses revolutionäre Konzept sicher begeistern.

Um ein IT-System wie eine Web-Applikation für einen Kunden hochverfügbar bereitstellen zu können, stehen einem zwei grundsätzliche Konzepte zur Verfügung, die eine sehr hohe Ausfallsicherheit bieten. Diese beiden Topologien – Active-Passive sowie Active-Active – sind in diesem Artikel kurz beschrieben, um dann im Nachgang auf die offensichtlichen Vorteile des neuen, revolutionären Konzepts einzugehen. Die Basis der beschriebenen Varianten stützt sich jeweils auf eine vollständige Trennung auf zwei oder mehrere verteilte Data Center.

Active-Passive-Topologie

Als Erstes ein Blick auf die hochverfügbare Variante, bei der das Aufspannen des Clusters sich auf einen aktiven und einen passiven Standort verteilt *(siehe Abbildung 1)*. Die gesamte Last der Anwendung wird von einem Standort aufgenommen. Der zweite Standort ist redundant aufgebaut und steht im Fehlerfall bereit. Gibt es am Active-Standort einen nicht zu behebenden Ausfall, kann der passive Teil die gesamte Verarbeitung übernehmen. Er wird dann zum Active Data Center. Der fehlerhafte Strang kann somit überprüft beziehungsweise instand gesetzt werden, ohne eine für den Kunden transparente Beeinträchtigung zur Folge zu haben.

Zudem können mit diesem Konzept Wartungsarbeiten oder Ähnliches am Passiv-Rechenzentrum durchgeführt wer-

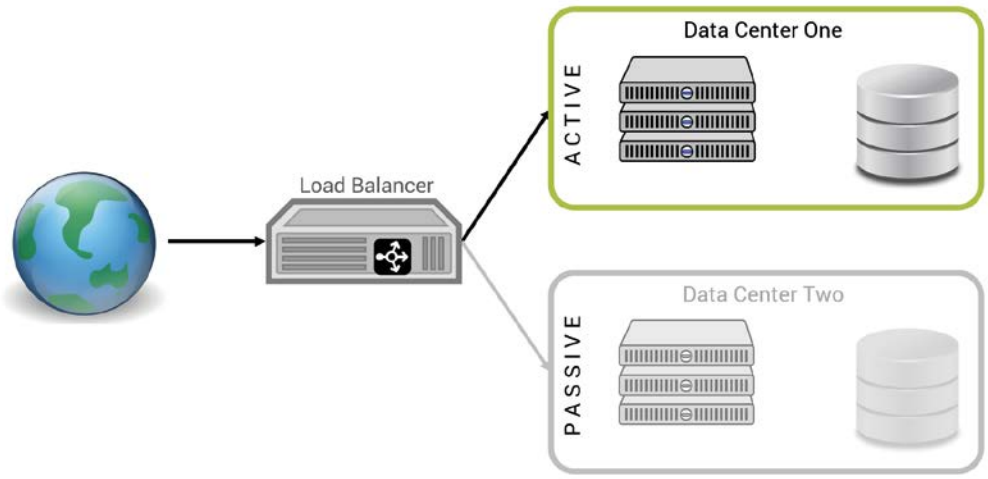

Abbildung 1: Active-Passive-Topologie

den, ohne einen Einfluss auf die Anwendung selbst zu haben. Kommt es während der Wartungsarbeiten im abgeschalteten Zweig zu einem Ausfall im aktiven Strang, ist ein Failover nicht möglich, was den Ausfall der gesamten Anwendung zur Folge hätte. Ein weiterer negativer Aspekt dieser Konstellation sind die hohen Hardware-Kosten. Jeder Standort im Cluster muss gleich stark ausgebaut werden, obwohl nur ein Data Center aktiv ist.

Active-Active-Topologie

Die zweite Variante, um eine Hochverfügbarkeit zu gewährleisten, ist die Active-Active-Topologie, bei der beide Teile eines Clusters online sind und die Last auf die Anwendung gemeinsam übernehmen *(siehe Abbildung 2)*. Damit erreicht man beim Ausfall eines Strangs eine Ausfallzeit der Anwendung von annähernd null, da das zweite Data Center nicht erst aktiv geschaltet werden muss, sondern die Anfragen sofort verarbeiten kann.

Zu den Nachteilen dieser Lösung gehört unter anderem, dass im Fehlerfall eines Knotens die Performance stark beeinträchtigt ist. Zudem kann nicht jedes Verfahren beziehungsweise jede Software in einem Active-Active-Umfeld betrieben werden.

Etabliertes und Bewährtes überdenken

Die beiden in kompakter Form beschriebenen Konzepte bringen einige Herausforderungen mit sich, die den Autor und seine Kollegen dazu gebracht haben, das ganze Thema neu zu betrachten: In Zeiten immer komplexer werdender System-Landschaften ist es auch immer komplizierter, diese zu betreiben. Um die Infrastruktur stabil und redundant zu halten, sind viele Experten erforderlich und somit wird der Personalaufwand entsprechend immer größer. Der Aufwand, dies alles zu monitoren und das Zusammenspiel der verschiedenen Komponenten aufeinander abzustimmen, stellt die Experten vor immer neue Herausforderungen. Die Hard- und Software-Lizenzen sowie der steigende Personalbedarf lassen die Kosten schnell ansteigen. Das hat eine kleine Gruppe erfahrener IT-Berater und Freidenker zum Anlass genommen, über ein komplett neues und revolutionäres Konzept nachzudenken.

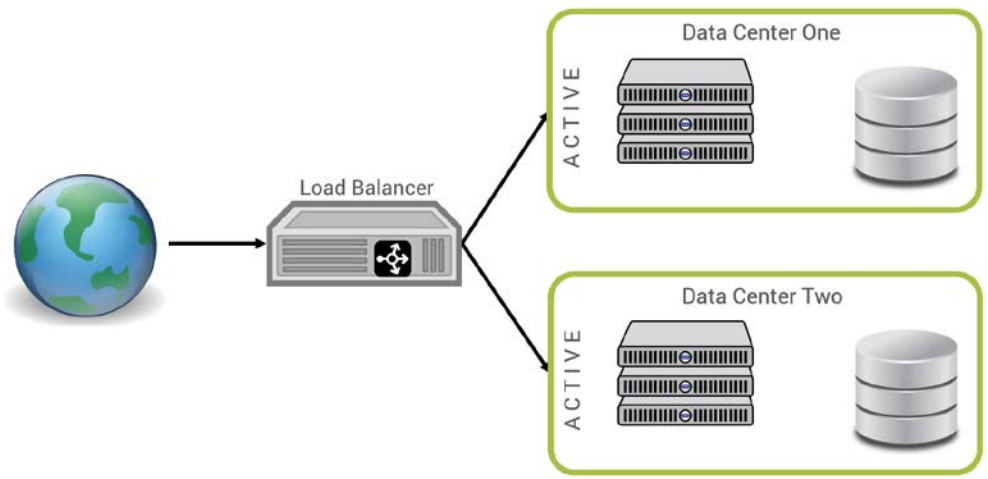

Abbildung 2: Active-Active-Topologie

Ideen, hin zur neuen, bahnbrechenden Strategie

Zu Beginn stand ein Brainstorming *(siehe Abbildung 3)*. Was sind die größten Pain-points der aktuellen Topologie und wie können sie beseitigt werden? Was sind die Eckpfeiler eines revolutionären, neuen Konzepts und welche Möglichkeiten ergeben sich daraus?

Am wichtigsten sind neben der Kostenreduzierung und der absoluten Datensicherheit sicherlich die Aspekte der Mitarbeiterzufriedenheit sowie Green-IT in Perfektion. Die Lösung kann nur zu einem Schluss führen, zur Passive-Passive-Topologie *(siehe Abbildung 4)*.

Ein fast fehlerfreies Konzept, das sowohl für kleine Unternehmen als auch bei allen Global Playern tragfähig wäre. Nachfolgend ist das bahnbrechende Konzept näher erklärt, um zu der Erkenntnis zu kommen: Bulletproof fail over lässt sich nur mit dem Ansatz „Passive-First" erreichen.

Outage-Driven-Architecture

Die gesamte Architektur basiert auf dem Konzept der Outage-Driven-Architecture (ODA). Bei diesem OPS-Pattern handelt es sich um das etwas unbekanntere Konzept, bei dem vor allem betrachtet wird, wie Systeme offline geschaltet werden können. Die gesamte Planung und Um-

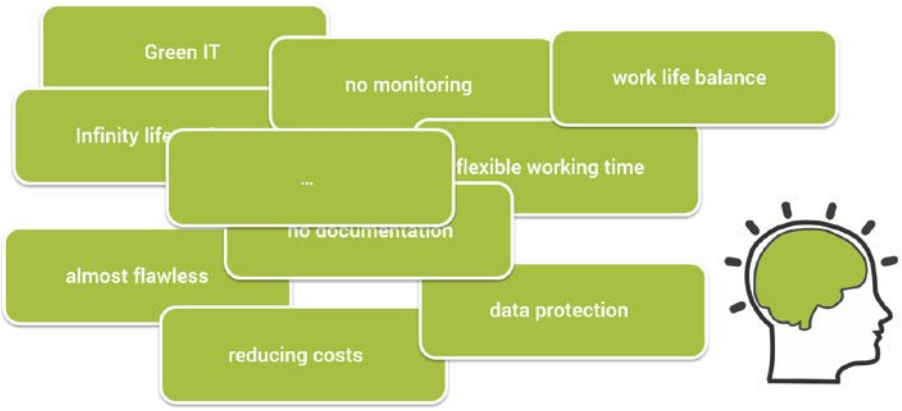

Abbildung 3: Bahnbrechende Ideen, die zu Passive-Passive führten

setzung der Architektur verfolgt einzig und allein das Ziel, dem Operations-Team die Arbeit so einfach und unkompliziert wie möglich zu machen.

Die Vorteile liegen somit klar auf der Hand. Eine hohe Mitarbeiter-Zufriedenheit und gutes Betriebsklima sind garantiert. Wie bei jeder Umstellung oder Neuausrichtung gilt auch bei der Einführung von ODA: Die Schwierigkeit ist nicht, die Betriebsmannschaft zu überzeugen, sondern auf Management-Ebene für das Konzept zu werben. Im Laufe des Artikels wird noch weiter auf diese Problematik eingegangen und man wird sicher das eine oder andere Argument zum Start in die ODA-Architektur finden.

Aufbau einer Non-Availability-Zone

Wer sich mit Anwendungen beschäftigt, die im firmeneigenen Netz, aber auch gleichzeitig im Internet erreichbar sind, weiß um die Schwierigkeit, vor allem die Verbindung ins Internet abzusichern. Um Kunden dennoch einen Zugriff aus der freien Welt zu bieten, wird getrennt durch Firewall und andere Sicherheitssysteme eine Demilitarized Zone (DMZ) aufgebaut. Auch dafür bietet Passive-Passive konzeptionell die beste Lösung. Es wird über die DMZ sowie das Intranet eine Non-Availability-Zone (NAZ) gespannt. Diese sorgt unter anderem für maximale Sicherheit.

Eine NAZ ist sowohl als Multi-Site Passive-Passive als auch als Single-Site Passive-Passive aufbaubar. Auch ein moderner Aufbau, basierend auf einer Container-Plattform, ist denkbar. Verfolgt man dieses Thema aktuell, gehen die Bestrebungen von Experten auf diesem Gebiet sogar hin zum Aufbau von No-Site-Passive-Passive-Umgebungen. Hier spricht man dann sozusagen von einem nahezu perfekten Aufbau einer Non-Availability-Zone.

Soft- und Hardware Lifecycle

Sicherlich ist jetzt noch nicht jeder Leser von dem Konzept überzeugt. Wer jetzt also immer noch nachdenkt und nicht mit einem Lächeln im Gesicht den Artikel liest, den werden hoffentlich die folgenden Eckdaten überzeugen. Dazu folgende Frage: „Wie organisieren Sie Ihre Soft- und Hardware Lifecycles?" In den meisten Fällen wird die Antwort sein, dass es zwar eine Herausforderung für das Betriebsteam ist und alles gut geplant sein muss, es aber mit wenigen Ausnahmen reibungslos läuft. Ausfälle gibt es sehr wohl ab und an, aber diese sind mit dem Service-Level-Agreement (SLA) meist vereinbar.

Passive-Passive bietet auch hier einen neuen, revolutionären Ansatz. Lifecycle-Maßnahmen müssen nicht mehr akribisch geplant sein. Es ist nicht mehr notwendig, Mitarbeiter an Wochenenden oder zu ähnlichen Zeiten bereitzustellen. Die Topologie bietet die Möglichkeit, fast immer und zu jeder Zeit Lifecycle-Maßnahmen an der Softwareund an der Hardware durchzuführen oder auch neue Software einzurichten.

Wenn der Passive-Passive-Ansatz in die Unternehmensstruktur richtig integriert ist, kann ganz leicht 99,9% Nichterreichbarkeit umgesetzt werden. Das wichtigste, wie in jeder anderen Topologie, ist auch hier das Monitoring. Selbstverständlich muss ein Monitoring stattfinden, um den Offline-Status zu überwachen. Im Allgemeinen gestaltet sich dies sehr einfach. Zustände wie „Server ist gestartet", „Die Anwendung reagiert nicht" gehören der Vergangenheit an. Offline ist offline! Somit kann auch das Betriebsteam sich auf das Passive-Sein konzentrieren.

Backup und Recovery

Im Rahmen heterogener Systemlandschaften kann es nicht das eine Backup- und Recovery-Konzept geben. Das Zusammenspiel jeder einzelnen Komponente muss betrachtet werden, um im Falle eines Fehlers eine geeignete Recovery-Maßnahme einleiten zu können.

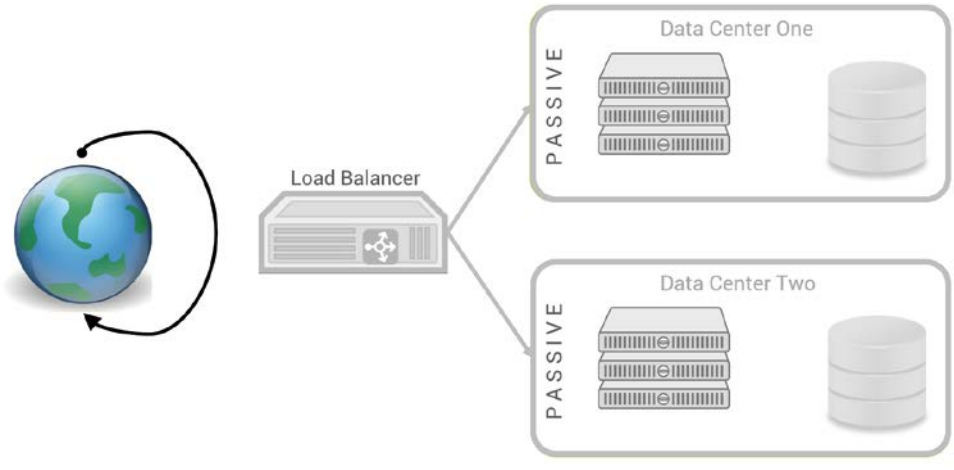

Abbildung 4: Passive-Passive-Topology

Auch hier gilt, wie schon für das Lifecycle-Management erörtert, Backup und Recovery ist zu jeder Zeit möglich. Einzuplanen sind hier nur die Zeitspannen, die erforderlich sind, um die betroffenen Systeme zu starten. Beachtet werden sollte, dass hier weniger mehr ist. Das soll bedeuten, je weniger Server gestartet werden, desto weniger Zeit muss für den Shutdown eingeplant werden.

Den größten Vorteil gibt es allerdings in Bezug auf die Backup- und Recovery-Strategie. Es ist völlig irrelevant, in welcher Reihenfolge man dieses Konzept angeht. Man kann entweder das Backup vor dem Recovery einplanen, so wie es schon seit der IT-Steinzeit umgesetzt ist, oder man geht konzeptionell noch unbeschrittene Wege und startet umgekehrt mit dem Recovery. Das Initial Recovery ist mangels Daten somit auch sehr performant.

Performance

Ein weiterer wichtiger Punkt ist die Performance und Skalierbarkeit. Wir beschäftigen uns oft mit Berechnungen der Anzahl von Prozessoren beziehungsweise Kernen oder damit, wie viel RAM für die Anwendungen zur Verfügung steht. Das alles spielt bei einem Passive-Passive-Aufbau keine Rolle mehr. Achtet man darauf, dass nicht zufällig und unerwartet Systeme starten, ist die Grenze nur der Plattenplatz (hier sei noch einmal auf die Wichtigkeit des Monitorings verwiesen).

Nimmt man als Beispiel das Betreiben von Application Servern, ist die Frage, wie viele Installationen auf die Platte beziehungsweise auf das angeschlossene Plattensystem passen. Es ist selbstverständlich darauf zu achten, dass die notwendige Uptime richtig einzuplanen ist. Es müssen sicher mehrere Komponenten zur gleichen Zeit hochgefahren sein. Zudem muss man sich keine Gedanken über die Bandbreite machen. Weder im Intranet noch im Internet kann es durch Passive-Passive zu Engpässen kommen. Hier gilt ganz klar „less data needs less band width".

Hohe Mitarbeiterzufriedenheit

In unserer heutigen Zeit, da IT-Experten in vielen Bereichen rar sind, muss es Ziel der Unternehmen sein, die angestellten Experten zu halten. Eine Möglichkeit, dies sicherzustellen, ist, darauf Wert zu legen, zufriedene Mitarbeiter zu beschäftigen. Auch hier bietet die Passive-Passive-Topologie ein Patentrezept.

Während des Passiv-Betriebs beschränken sich die Tätigkeiten der Administratoren darauf, sich selbst automatisiert startende Systeme hektisch wieder herunterzufahren. Produkte, die passiv betrieben werden, können jeden Bug verschleiern und machen somit ein Bugfixing völlig überflüssig. Dadurch gibt es weniger Reibungspunkte zwischen Entwicklungs- und Test-Teams. Installationen, Wartungen oder Ähnliches können auf ein für die Mitarbeiter sehr entspanntes Minimum reduziert werden.

Sollte sich dennoch Langeweile breit machen, kann man hier durch gezieltes Starten einzelner Systeme gegensteuern. Allgemein lässt sich hier festhalten, passive Systeme verhindern Fehlverhalten von Anwendern um nahezu hundert Prozent. Dies kann man frei nach Bob Marley mit dem Titel „No user, no cry!" zusammenfassen.

Passive-Passive und Green-IT

Wer die Ausführungen in den vorherigen Abschnitten aufmerksam gelesen hat, dem wird sehr schnell klar, dass die Passive-Passive-Implementierung quasi auf den Ideen der Green-IT basiert. Die Energiekosten stehen bei diesem Konzept mit im Vordergrund und werden ohne zusätzlichen Mehraufwand auf annähernd null reduziert. Jeder passiv betriebene Server spart somit bares Geld. Ebenfalls wird der Bedarf der Kühlung von Rechenzentren minimiert. Teure Wasserkühlungen oder Ähnliches gehören der Vergangenheit an. In Passive-Passive-Rechenzentren genügen selbst zu Spitzenzeiten gekippte Fenster oder eine offene Tür.

How many successful fail overs do you have a day?

Selbstverständlich hat das Konzept auch Schattenseiten. In betrieblicher Hinsicht muss einiges verändert werden, um von einem klassischen auf das Passive-Passive-Konzept umzustellen. Um auf einen lückenlosen, automatisierten Continuous-Fail-over-Prozess zu implementieren, den man unbedingt benötigt, um echtes Passive-Passive umzusetzen, sollte man über eine voll automatisierte Fail-over-Pipeline nachdenken. Damit stellt man bis hin zum automatisch rollierenden Shutdown einen reibungslosen Betrieb sicher.

Neue Rollen bringt die passive Landschaft

Wie so oft beginnt ein Paradigmen-Wechsel nicht nur mit Veränderungen in betrieblicher Hinsicht, sondern vor allem auch unter organisatorischen Gesichtspunkten. Man benötigt ganz neue Fähigkeiten und Rollen in seiner Organisation. Auf der technischen Ebene gibt es einen Downtime Insurance Engineer, der genügend Vorkenntnisse der klassischen Methoden der Hochverfügbarkeit mitbringen sollte. Nur so lässt sich gewährleisten, dass der Mitarbeiter ausreichend kreative Ideen entwickeln kann, um mit dem nötigen Respekt und Geschick ans Werk zu gehen. Ein Einsteiger würde sehr wahrscheinlich den humorigen Hintergrund nicht in vollem Umfang überblicken können.

Sinnvoll wäre sicher auch die Installation eines Accidental Boot Prevention Supervisors, der die notwendige Kontrollfunktion übernehmen sollte. Um auch nur eine geringe Chance zu haben, eine solche Idee auch strategisch im Unternehmen platzieren zu können, benötigt man selbstverständlich auch die Unterstützung durch das Top-Management. Hier wird empfohlen, über die Position des Chief Downtime Officers (CDO) nachzudenken. Dieser kann mit dem Blick für das ganze Desaster sehr einfach ein Hochfahren beziehungsweise In-Betrieb-Nehmen einzelner Komponenten oder im schlimmsten Fall ganzer Rechenzentren per Management-Entscheidung unterbinden. Der CDO ist somit die wichtigste Person der gesamten IT-Abteilung.

Fazit

Wer die Ausführungen zur Passive-Passive-Topologie bis jetzt gelesen hat und

der Meinung ist, dies sei auch ein tolles Konzept für sein Unternehmen, sollte mit der Ausschreibung eines CDO zu beginnen. Hoffentlich sind alle Leser mit dem Autor der gleichen Überzeugung, ein wenig Spaß schadet auch der IT nicht. Er würde sich freuen, alle Lesern mit diesem Artikel etwas unterhalten zu haben und wenn alle den Alltag auch mal mit einem kleinen Augenzwinkern betrachten. Wir leben alle IT und haben Spaß an der Arbeit, es kann also auch nicht schaden, den Alltag mit wirren Ideen etwas aufzulockern.

Weiterführende Links

International Passive-Passive User Group:
http://www.ippug.org

Der Autor bedankt sich für die fundierte fachliche Unterstützung bei folgenden Kollegen:

- Ralf Downtime Ernst
- Sturmius OfflineMostSecure Rippert
- Hans WhoNeedsMonitoring Mehl
- Thorsten NoContent Wussow
- Florian ClosedGate Stoll

Christoph Münch
christoph.muench@virtual7.de

Termine

Januar

Januar 2017
Regionaltreffen Bremen
regio-bremen@doag.org
Bremen

13.01.2017
DOAG Webinar zum Thema: "Oracle Database Cloud Performance"
sig-database@doag.org
online

19.01.2017
Regionaltreffen Nürnberg
Thema: **Oracle** RAC Deep Dive und RAC 12.2 New Features
regio-franken@doag.org
Nürnberg

Februar

26.01.2017
Regionaltreffen Stuttgart
regio-stuttgart@doag.org
Stuttgart

01.02.2017
Regionaltreffen München/Südbayern
regio-muenchen@doag.org
München

02.02.2017 - 03.02.2017
DOAG Noon2Noon
Upgrade nach 12c
sig-database@doag.org
Mainz

08.02.2017
DOAG 2017 DevCamp
Themen: "Development by Choice", Moderne Softwareentwicklung mit **Oracle**, ADF, APEX, JavaScript, Forms, Webcenter
sig-development@doag.org
Hannover

15.02.2017
DOAG 10. Primavera Community Day
bsc-primavera@doag.org
München