Hochverfügbare Systeme

Autor

Kai Dupke
Teamleiter Linux
probusiness AG, Hannover
kdupke@probusiness.de

Abstract

Für die Umsetzung hochverfügbarer Systeme existieren eine Reihe von Lösungen. Während für die technische Umsetzung auf empirische Werte zurückgegriffen werden kann, fehlen diese Ansätze häufig im Bereich der Applikationen. Im folgenden werden Sichtweisen aus Anwendungssicht dargestellt, die helfen, eine hochverfügbare Umgebung zu bewerten.

SpoF - Die Suche nach der Verfügbarkeit

Hochverfügbare Systeme stellen einen wichtigen Ansatz in der IT dar, wenn es gilt, Dienste ohne Ausfälle anbieten zu können. Durch die Veränderungen im Nutzerverhalten gilt es sogar immer häufiger Systeme für den 24/7-Betrieb auszulegen.

Für die klassischen Kernanwendungen der IT, wie Datenbanken und ERP-Systeme, existieren eine Vielzahl von Lösungen, um verfügbare Systeme darzustellen. Hier existiert i.d.R. auch ein grosses KnowHow der Anbieter zur Umsetzung. Dieses gilt sowohl für die Unices der grossen Hersteller, die Windows-Plattform, als auch für Linux. Für all diese Systeme existieren Lösungen in jeder erdenklichen Grössenordnung und Preisklasse.

Zunehmend jedoch besteht der Bedarf, Anwendungen hochverfügbar darzustellen, die ursprünglich nicht für den hochverfügbaren Betrieb ausgelegt wurden. Hierbei handelt es sich häufig um ehemalige Satellitensysteme, wie Mail-, Webserver oder andere Hilfsdienste, die im Laufe der Zeit produktiven Status erreicht haben. Viele solche Systeme sind hochgradig anwenderoptimiert bzw. sogar speziell für diesen Anwender entwickelt worden. Für diese Umgebungen kann der IT-Verantwortliche nicht mehr auf vorhandene und erprobte Lösungen zurückgreifen.

SPoF

Um solche Systeme hochverfügbar zu integrieren, ist es notwendig, die Schwachstellen ausfindig zu machen und mögliche Lösungen darzustellen. Eine Schwachstelle, die durch ihren alleinigen Ausfall das gesamte installierte System unbrauchbar werden lässt, wird Single-Point-of-Failure, kurz SPoF, genannt. Wichtig ist hierbei, dass bereits ein einziger SPoF das Projekt Hochverfügbarkeit zum Scheitern verurteilt.

Gleichwohl kann es bei einer genauen Analyse dazu kommen, dass für ein Detail à priori keine Lösung erarbeitet werden kann. Hier ist es dann häufig notwendig, an der Anwendung selber Änderungen vorzunehmen, um die Basis für eine hochverfügbare Umgebung aufbauen zu können.

Systeme, bei denen ein SPoF nicht vermieden werden kann oder aber die Anpassung der Anwendung nicht durchführbar ist, können ihre Dienste nach einem Fehler nicht automatisiert wieder zur Verfügung stellen. Diese Systeme bedürfen i.d.R. eines manuellen Eingriffs, um wieder betriebsbereit zu sein. Diese Eingriffe können sowohl administrativer Natur (Softwarestart, -recover) sein, als auch technischer Natur (Gerätetausch, Wiederherstellung des Enviroments).

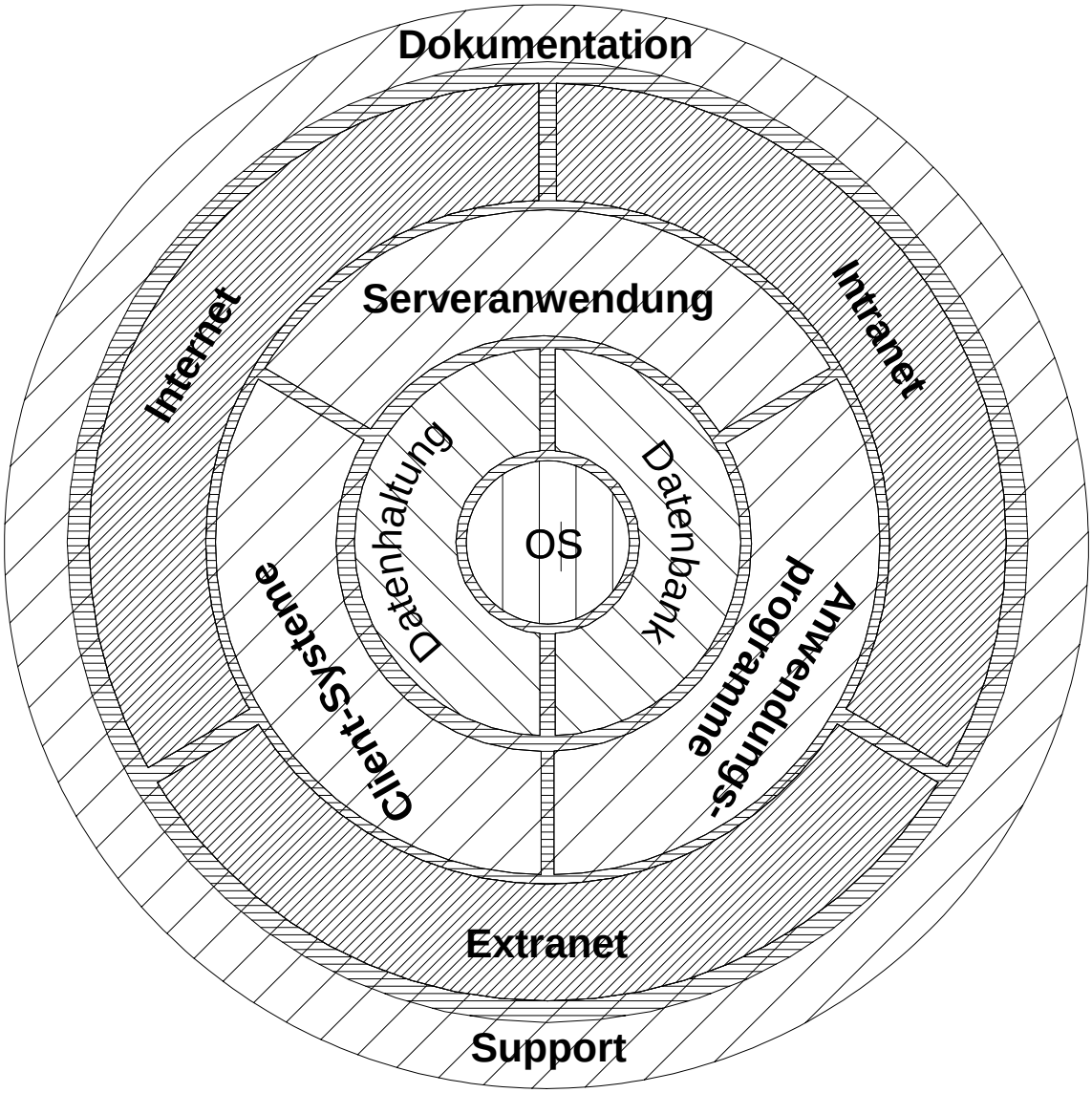
Schwachstellensuche

Grundlage für die Schwachstellenanalyse muss die Suche nach SPoFs sein. Um diese aufzudecken ist es notwendig, das System in einem geeigneten Modell darzustellen. Sodann müssen für jedes beteiligte Teil mögliche Ausfälle und deren Einfluss auf die beteiligten Geschäftsprozesse geprüft werden. In einem weiteren Schritt ist zu klären, welche Optionen bestehen, um die möglichen Ausfälle abzufangen. Schließlich ist aus betriebswirtschaftlicher Sicht eine Kosten-Nutzen-Analyse durchzuführen, welche die Basis für Entscheidungen der Geschäftsführung bietet.

Die Suche nach SPoFs sollte immer vor Augen haben, dass eine kaufmännische Umsetzung sinnvoll gelingen muss. So haben viele kleine Web-Shops einen SPoF in der Anbindung an das Internet, die häufig als Einzelleitung ohne Backup ausgeführt wird. Eine Abhilfe ist hier jedoch nur durch zusätzliche Leitungen, die auch noch speziellen technischen Bedingungen genügen müssen, Anpassungen auf Seiten des Providers und technische Massnahmen im Bereich des Web-Shops möglich. Die Frage, ob sich dieser Aufwand lohnt, muss vom Anwender selber beantwortet werden.

Modelle

Bei der Analyse eines HA-Systems hat es sich als vorteilhaft erwiesen, von einem Ringmodell auszugehen. Dieses Modell hat im Zentrum den technischen Kern, umschlossen von der Administration. Hier herum lagert sich die Datenhaltung und Datenbanken. Der Ring erweitert sich sodann um Server-Anwendungen sowie die Clientsysteme und die Anwendungssoftware. Ganz außen schließlich sitzt der Anwender. In diesem Modell nicht eigenständig aufgeführt sind die Kommunikation, die wie Leim zwischen den einzelnen Schichten vermittelt, der Support und das Consulting, die das System zusammenhalten, sowie die Dokumentation, die das System umhüllt und der Nachhaltigkeit dient.



Das Ringmodell

Eine andere Variante ist an das ISO-Schichten-Modell angelehnt. Hierbei wiederholt sich jedoch für jede Komponente die ISO-Darstellung und es geht häufig der Überblick für den Gesamtzusammenhang verloren. Das ISO-Modell scheint aufgrund einer 'genormten' Vorgehensweise einfacher, lässt jedoch Themen wie Dokumentation, Schulung und Support außen vor.

Auch bei dem Ringmodell ist es notwendig, alle beteiligten Schichten für sich zu betrachten. Hierbei wiederum hilft die Anlehnung an das ISO-Modell. Hilfreich ist, dass fast immer jede Schicht für sich betrachtet werden kann und es selten Rückkopplungen gibt. Einzelne Schichten oder Komponenten wiederholen sich oder kommen unter anderen Gesichtspunkten wieder zum Tragen, wie die Kommunikation, die sowohl im Intranet, als auch im Extra- oder Internet von Bedeutung ist, andere Schichten wiederum bedürfen einer zusätzlichen Feinanalyse, wie die Datenhaltung und der technische Kern.

Zur Funktionsfähigkeit des Gesamtsystemes trägt jede Schicht einen gleichwertigen Teil bei. Daher muss auch jede Schicht bei der Betrachtung eines HA-Systems betrachtet und bewertet werden. Was hilft es schließlich, wenn die Daten verfügbar sind, jedoch die Clients nicht mehr arbeiten? Was hilft ein funktionierender Client, wenn die Daten ihn nicht mehr erreichen können? Und was hilft die ganze Technik, wenn kein Anwender da ist, der damit arbeiten kann?

Fehlerfall

Am Ende der Analyse steht ein Konzept, welches alle erkannten SPoFs vermeidet. Die Konzepte sehen i.d.R. eine automatisierte Fehlerbehebung vor, die häufig über redundante Systeme/Komponenten bereitgestellt wird. Hier wird es um so wichtiger, dass im Fehlerfall eine Information an die Systemverantwortlichen erfolgt. Schließlich wird bei einem einfach redundant ausgelegtem System im Fehlerfall die übrig gebliebene Komponente selber wieder zum SPoF. Hier sei allerdings der Hinweis erlaubt, dass HA-Systeme im allgemeinen keine Double-Failure abdeckt, da dadurch der Aufwand potenziert würde. Um die Systemverantwortlichen informieren zu können, ist es notwendig, Systeme zu implementieren, die potentielle Problemstellen überwachen. Denn was hilft es, wenn in einem RAID-Verband eine Festplatte ausfällt, dieses jedoch keiner merkt, weil die notwendigen Mechanismen fehlen und schließlich der gesamte Verband ausfällt, weil eine weitere Festplatte sich dem Zugriff 'entzieht'.

Sicherheit eingebaut

Vielen Systemen eingebaut sind bereits redundante Komponenten. Wichtig ist, dieses als Chance und Absicherung zu verstehen. So wie es falsch wäre, in einem RAID-Verband Platten einzusetzen, die 'end-of-life' sind, weil das RAID einen Ausfall 'schon abfangen würde', so sollte jedes System und jede Komponente in einem HA-System soviel Redundanz wie möglich haben. Jede Redundanz, die dazu führt, dass ein Fehler nicht automatisch einen Fail-Over auslöst, ist sinnvoll. Zudem sind viele Systemredundanzen bereits lange erprobt und verhältnismäßig günstig umzusetzen. Das gilt für Festplatten im RAID-Verband, für Netzwerkanschlüsse im gebündelten Modus, für redundante Netzteile, aber auch für den Hauptspeicher, der mittlerweile selbst im Intel-Server-Bereich redundant aufgebaut werden kann.

Sicherlich besteht der Wunsch, solcherlei Redundanzen, die ohne Datenverlust, Interaktion und Unterbrechung wirken auch bei anderen Komponenten weiter zu treiben. Hier ist jedoch der Schritt schnell zu fehlertoleranten Systemen gemacht, die alle sowohl deutlich komplexer, als auch teurer sind, als hochverfügbare Systeme.

“keep it simple”

Erfolgreiche HA-Umsetzungen nutzen immer zwei in der IT wohl eingeführte Prämissen: 'Never change an running system' und 'keep it simple'. Jede Änderung an der Konfiguration macht eine neue Überprüfung der HA-Installation notwendig. Somit sollten mögliche Änderungen und Erweiterungen bereits im Vorfeld in das Konzept eingearbeitet werden.

In der Praxis existieren Fälle, wo der Hauptspeicher einer Produktivmaschine erweitert wurde, jedoch der des Ersatzsystems nicht. Somit funktioniert die technische Umschaltung, jedoch bekommt eine installierte Datenbank 'Schluckauf' und ist in sich nicht mehr verfügbar.

Eine einfache Konfiguration sorgt immer für eine geringere Komplexität bei der Systembetrachtung. Hier ist es gerade bei der Einführung eines Systemes sinnvoll, nicht alles, was theoretisch möglich ist, auch umzusetzen. Die Wahrscheinlichkeit, dass bei Ausfall nur einer Komponente das gesamte System nicht mehr verfügbar ist, wächst ansonsten immens.

Cluster statt Cluster

Bei vielen HA-Projekten lohnt sich die Suche nach Systemprozessen, die durch parallelen Betrieb abgedeckt werden können. Wenn diese Parallelität umgesetzt wird, ergeben sich sowohl positive Auswirkungen auf die Skalierbarkeit, als auch auf die Verfügbarkeit. Einfachste Variante ist das Prinzip einer Server-Farm, wie sie im Web-Bereich immer häufiger zur Anwendung kommt. Hier werden Anfragen über einen Loadbalancer an mehrere Web-Server verteilt. Der Loadbalancer stellt in sich die Verfügbarkeit des nachfolgenden System her, indem die Web-Server überwacht werden und ausgefallenen Systeme nicht mehr angesprochen werden. Selbst für den Fall, dass ein gemeinsamer Datenbankzugriff der Web-Server erfolgen muss, wird durch die Auftrennung in mehrere Ebenen das Konzept erleichtert. Die erste Ebene liegt im Netzwerklayer und kann eine Umschaltung transparent ausführen, die zweite Ebene besteht nur noch aus einer Präsentationschicht, wo keine Datenhaltung mehr erfolgt und letztlich die dritte Ebene, die Datenbank, die wieder für sich als eigenens HA-System abgesichert werden muss.

Anwendung

Nicht nur die technische Bereitstellung von hochverfügbaren Systemen ist notwendig, auch im Bereich der Anwendung gilt, dass diese in sich in der Lage sein muss, einen hochverfügbaren Betrieb abzudecken. Aus dem HA-Grundgedanken folgt, dass eine Anwendung automatisch und ohne Benutzereingabe starten können muss. Neben der Fähigkeit, mit Transaktionen zu arbeiten, muss die Anwendung in der Lage sein, einen definierten Status zu erlangen und diesen zu dokumentieren. Anwendungen, die auf Datenbanken basieren, werden i.d.R. auch Logfiles in dieser ablegen. Andere Anwendungen müssen diese im Dateisystem ablegen. Hierbei ist darauf zu achten, dass die Regeln für Transaktionen natürlich auch für diese Logfiles gelten. Hier hat natürlich die Technik dafür zu sorgen, dass Daten definiert auf die Datenträger geschrieben werden bzw. nicht durch Einflüsse von Cache oder Controller in das Nirwana verschwinden können.

Anwender

Neben der Technik des HA-Systems muss auch der Anwender mit eingebunden werden. Letztendlich ist es dieser, der mit dem System arbeitet. Gerade bei internen Anwendern ist es hilfreich, einen besonderen Augenmerk auf eine wohldokumentierte und möglichst einfache Handhabung gelegt werden. Der Anwender braucht i.d.R. kein technisches Verständnis mitzubringen - seine Aufgabe ist es mit der Anwendung zu arbeiten. Für den Fall eines Ausfalls muss der Anwender daher in die Lage versetzt werden, seine Arbeit möglichst schnell und reibungslos wieder aufnehmen zu können. Hierzu ist es notwendig, den Anwender entsprechend zu schulen. In Bezug auf ein HA-System bedeutet dieses, dass er über einen Ausfall, der ihn betrifft, informiert werden muss. In Abhängigkeit von der Anwendung und der Tätigkeit müssen ihm die notwendigen Informationen zur Verfügung gestellt werden, um Arbeitsschritte evtl. nacharbeiten zu können. Die dazu notwendigen Protokolle müssen zwischen Anwendung und Anwender abgestimmt sein. Häufig ist es hier sinnvoll, auch die Arbeitsorganisation mit anzupassen. Angelehnt an die Journal-Nummern aus der klassischen Buchhaltung helfen fortlaufende Vorgangsnummern bei der Wiederaufnahme der laufenden Arbeit.

Dokumentation

Unabhängig davon, ob ein System mit automatischen fail-over betrieben werden kann oder ob ein manueller hand-over durchgeführt werden muss, ist eine Dokumentation der HA-Umgebung notwendig. Diese Dokumentation soll den Administrator in die Lage versetzen, andere Mitarbeiter in die Thematik einzuarbeiten. Auch evtl. notwendige Einsätze von Supportfirmen können durch ein dokumentiertes Umfeld deutlich erleichtert werden.

Notfallplan

Alle Überlegungen zu hochverfügbaren Systemen sollten jedoch mit einschließen, dass auch die Menschen, die diese Konzepte erarbeitet haben, selber Fehler machen können. Somit stellt auch der Berater bzw. der Administrator einen SPoF dar. Selbstverständlich lässt sich das Risiko minimieren, wenn die Konzepte sauber niedergelegt sind und transparent und verständlich gestaltet werden. Hier ist das Team von Kunde, Berater und Administrator gefordert.

Um jedoch für möglichst jeden Fall gewappnet zu sein, ist es notwendig einen Notfallplan vorliegen zu haben. Dieser Plan soll dann zum Einsatz kommen, wenn allen Tests und Planungen zum Trotz die HA-Funktionalität nicht mehr gegeben ist. In manchen Fällen, wenn die Konzepte bzw. die Hardware längere Zeit nicht mehr aktualisiert wurden, kann auch die Ersatzteilbeschaffung zu einem eigenen SPoF werden. Solch ein Notfallplan kann bares Geld wert sein. Je einfacher, wenn nicht gar rudimentär und von der eigentlichen Installation unabhängiger solch ein Plan ist, desto einfacher ist auch die Umsetzung und damit die Erfolgsaussicht.

Fazit

Hochverfügbarkeit ist machbar. Neben den oft in den Mittelpunkt gestellten technischen Ansätzen, wie HA-Produkte und Storagelösungen, besteht die Notwendigkeit, ein HA-System als Ganzes zu verstehen. Wie ein roter Faden muss sich ein HA-Konzept durch die Geschäftsprozesse ziehen. Kaum ein Bereich bleibt hiervon unberührt. Dieses gilt sowohl für die Anwendung und den Anwender, als auch für die Administration und den Support. Unabhängig von der Umsetzung einer HA-Lösung ist es sinnvoll, die eigenen Systeme auf SPoF zu prüfen und dann abhängig von betriebswirtschaftlichen Überlegungen umzusetzen. Durch entsprechende Dokumentation wächst die Sicherheit für die Geschäftsführung und die Systembetreuer.

probusiness group

Die probusiness group ist plattformübergreifender IT -Dienstleister und steht ihren Kunden von der Konzeptphase über die Beschaffung bis zum Betrieb zur Seite. Das Leistungsportfolio von probusiness reicht von IT-Consulting über Projektplanung bis zur Erstellung von maßgeschneiderten Lösungen zur Umsetzung neuer strategischer IT -Konzepte.