Business Continuity mit Hilfe von Metro-Clustern und Desaster Recovery Lösungen

Hartmut Streppel
Sun Microsystems GmbH
Sonnenallee 1
85551 Kirchheim-Heimstetten
Hartmut.Streppel@sun.com

1 Abstract

Spätestens seit dem 11. September 2001 und der Hochwasserkatastrophe in Deutschland 2002 ist auch dem letzten Unternehmen klar geworden, dass es sich um die Verfügbarkeit seiner IT-Infrastruktur mehr kümmern muss als bisher. Altbewährte Technologien wie Backup und Restore allein werden damit zwar nicht überflüssig, aber ihres Alleinstellungsmerkmals beraubt. Jetzt suchte man Heil bei räumlich getrennten IT-Lösungen und voneinander unabhängigen Datenkopien, um eine möglichst unterbrechungsfreie Bereitstellung von IT-Dienstleistungen gewährleisten zu können.

Dieser Vortrag soll die wichtigsten Technologien betrachten, die für so genannte Business Continuity Lösungen, wie sie geografisch getrennte Cluster und auch typische Desaster Recovery Lösungen darstellen, eingesetzt werden, und sie mit ihren Vor- und Nachteilen gegenüberstellen. Es soll an dieser Stelle schon darauf hingewiesen werden, dass es DIE EINE Lösung nicht gibt, die alle Probleme optimal löst. Unternehmen müssen abwägen und entscheiden, wo der Schwerpunkt einer solchen Lösung liegen soll.

2 Business Continuity, Metro-Cluster und Desaster Recovery Lösungen

Business Continuity (BC) handelt vom vorausschauenden Planen, bei Ausfällen jeglicher Art mit minimaler - möglichst sogar ohne - Unterbrechung und minimalem - möglichst sogar keinem - Datenverlust die unternehmenskritischen Geschäftsprozesse wieder aufnehmen zu können. Cluster, die vollautomatisch schwenken, sind eine beliebte Lösung, um diese Anforderungen IT-technisch zu implementieren. Soll die IT aber auch gegen Katastrophen abgesichert werden, bei denen der Ausfall eines ganzen Standorts verkraftet werden muss, sind nur noch Lösungen sinnvoll, die mindestens ein weiteres RZ in die Infrastruktur mit einbeziehen. Lösungen, bei denen Cluster 'einfach' geografisch auseinander gezogen werden, nennt man Campus- oder MetroCluster, im Gegensatz zu klassischen Desaster Recovery (DR) Lösungen, die immer eine fast vollständig getrennte Infrastruktur besitzen.

Die Grenzen sind fließend. In der Regel wird eine Vielzahl unterschiedlicher Technologien kombiniert, um eine vollständige Absicherung zu erreichen. Diese Komplexität macht es notwendig, umfassende BC-Projekte aufzusetzen, um zu einer optimalen Lösung zu kommen. Der Einsatz einzelner Produkte allein reicht unter keinen Umständen aus.

3 Wie findet man die richtige Lösung?

Das Unternehmen, das eine BC-Lösung implementieren will, muss sich selbst eine Reihe von Fragen stellen und diese im Detail und mit harten Fakten begründet beantworten. Die wichtigsten sind:

- Gegen was will ich mich eigentlich schützen?
- Was kostet mich eine Stunde Nichtverfügbarkeit? Nach wie viel Stunden Nichtverfügbarkeit meiner IT bin ich bankrott? Nach wie vielen Stunden Auszeit muss die IT wieder verfügbar sein?
- Wie viele Daten darf ich im Falle einer Katastrophe maximal verlieren?
- Welches sind die unternehmenskritischen Anwendungen und Daten, die auf jeden Fall geschützt werde müssen?

Besonders die Frage nach den Kosten der Nichtverfügbarkeit führt häufig zu ungläubigem Erstaunen. Sie sind in der Regel nicht bekannt. Auch die Frage, welche der Anwendungen denn nun wirklich unternehmenskritisch sind, und welche denn noch zusätzlich, da ohne sie die gesamte Infrastruktur nicht liefe, ist Inhalt von vielen langwierigen und schwierigen Projekten.

Erst wenn diese und viele andere Fragen beantwortet und priorisiert sind, macht es Sinn, ein geeignetes Lösungskonzept zu entwerfen und zu implementieren.

4 Eine Referenzarchitektur

Eine allgemeine BC-Architektur, die erst einmal ohne Nennung von Technologien und Produktnamen auskommt, soll der Ausgangspunkt der Diskussion über mögliche Lösungen sein.

Um die notwendige Redundanz auch im Katastrophenfall zu gewährleisten, müssen mindestens zwei Räume bzw. Standorte vorhanden sein. Der im Bild 1 angedeutete dritte Standort (Site X) ist nicht unbedingt notwendig, hat aber in komplexen Entscheidungsszenarien eine herausragende Bedeutung als Quorum, d.h. als die Stelle, an der eindeutige Entscheidungen, u.U. sogar automatisch, gefällt werden können.

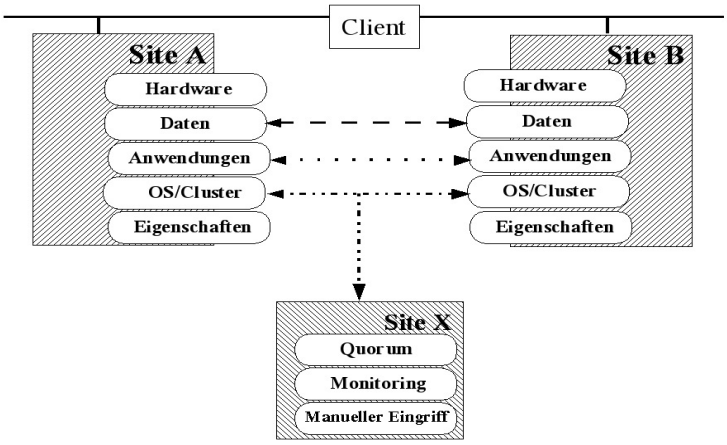

Bild 1: Eine BC-Referenzarchitektur

Dieser mögliche Automatismus ist ein immer wieder umstritten. Ist es sinnvoll, in einem K-Fall, d.h. nach dem Ausfall eines kompletten Rechenhzentrums, die Entscheidung über einen Schwenk einem automatisierten Algorithmus zu überlassen,

der dies sicherlich mit mehr Präzision und unbeeindruckt von äußeren Einflüssen tun kann, oder ist es sinnvoll oder vielleicht auch geboten, diese Entscheidung einem Menschen, oder einer Gruppe zu überlassen, die diese auch mit Erfahrung und menschlicher Intuition fällen kann?

In den - mindestens - zwei Hauptstandorten gibt es Rechner und andere Hardware, die mit Betriebssystemen und u.U. Clustersoftware ausgestattet sind, Anwendungen, die miteinander kommunizieren und Daten, die auf irgendeine Art und Weise hochverfügbar gemacht werden müssen. In vielen Fällen wird das Hauptaugenmerk ausschließlich auf die Daten gelegt, was einige andere wesentliche Aspekte außer Acht lässt.
All diese Komponenten haben nun Eigenschaften, die im Einzelnen betrachtet werden müssen. Und zu diesen Eigenschaften zählen auch Betriebsführungskonzepte, wie z.B. zerstörte Daten restauriert werden, oder wie möglichst schnell Ersatzteile besorgt werden können.

4.1 Standorte und Hardware

Die erste Voraussetzung für hochverfügbare IT-Infrastrukturen sind sichere und hochverfügbare Rechenzentren (RZ). Eine Ausstattung mit redundanten Stromversorgungen, d.h. auch über separate Stromzuführungen von verschiedenen Lieferanten für das gesamte RZ und zusätzliche unterbrechungsfreie Stromversorgungen sind eine wichtige Maßnahme. Brandschutz, der gegen Feuer außerhalb des RZ schützt und die Aufteilung eines RZ in mehrere Brandschutzabschnitte sind weitere Maßnahmen.
Redundanz in den Rechnersystemen und deren Hotswap-Fähigkeiten erleichtern Wartungsarbeiten an laufenden Produktionssystemen. Können Systeme im laufenden Betrieb aufgerüstet werden, um z.B. höheren Lastanforderungen gerecht zu werden. Solche immer wiederkehrende Wartungsarbeiten sind mit Sicherheit der häufigste Grund für die Nichtverfügbarkeit von Diensten. Diese sind zwar geplant und deshalb in ihrer Auswirkung berechenbar, aber es sind trotzdem Auszeiten. Das gleiche gilt auch für die Storageinfrastruktur. Ist sie so redundant, dass sie Ausfälle einzelner Komponenten wie FC-Switches verträgt? Kann ich Firmware-Upgrades im laufenden Betrieb durchführen usw.
Auch die Frage nach den Wartungsverträgen ist wichtig. Sind sie für alle lebenswichtigen Komponenten vorhanden, auch z.B. für Zugangskontrollsysteme? Gibt es die wichtigsten Ersatzteile vielleicht sogar im RZ?

4.2 Betriebssysteme und Hochverfügbarkeitssoftware

Betriebssysteme sind das Herz der Rechnersysteme. Ihre Zuverlässigkeit legt den Grundstein für die hohe Verfügbarkeit von IT-Systemen. Ist die Zuverlässigkeit der Basiskomponenten erst einmal abgedeckt, geht es darum, die nächste Ebene der Hochverfügbarkeit zu erreichen, indem Rechner zu Clustern gekoppelt werden. Clustersoftware übernimmt nun die Aufgabe, Rechner, Netze und Anwendungen zu überwachen, und bei Ausfällen durch Schwenks auf andere Systeme im Cluster Anwendungen wieder verfügbar zu machen. Typische Vertreter solcher Cluster-Software sind SunCluster 3.0, TruCluster oder IBMs HACMP.

Solche Schwenks haben fast immer Dienstunterbrechungen zur Folge, so dass modernere Systeme den Einsatz von parallel arbeitenden Anwendungen (z.B. die 'scalable services' in SunCluster 3.0, oder auch Hardware Load Balancer für Webserver-Farmen), ermöglichen, die Schwenks und damit Dienstunterbrechungen so gut wie unnötig werden lassen.

4.3 Daten

Die Daten sind in der Regel das Wichtigste in einer IT-Infrastruktur. Ihr Verlust oder ihre Nichtverfügbarkeit für einen längere Zeitraum führen zu katastrophalen Schäden in Unternehmen. Deshalb wird häufig auch zuerst eine Entscheidung für eine Technologie und ein Produkt zur Datensicherheit gefällt, ohne zuerst eine Analyse durchgeführt und eine Gesamtlösung zumindest skizziert zu haben. Das erschwert die nachträgliche Arbeit der IT-Architekten, die nun um eine schon getroffene Technologieentscheidung herum planen müssen.

Die wesentlichen Technologien, die bei der Datensicherheit zu betrachten sind, sind:

- asymmetrisch oder symmetrisch
- asynchron oder synchron
- host-, controller- oder anwendungsbasiert.

4.3.1 Asymmetrisch oder symmetrisch

Die beiden sich hier gegenüberstehenden Verfahren sind Datenspiegelung und Datenreplikation. Üblicherweise spiegeln hostbasierte Volume Manager Daten auch in heterogenen Storagelandschaften, was mehr Unabhängigkeit gibt. Vor allem sind diese Verfahren in der Lage, Daten zwischen Storagesubsystemen zu spiegeln, so dass Anwendungen, die auf diese Daten zugreifen wollen, dies auch parallel, d.h. auf allen Systemen gleichzeitig, tun können. Typische Vertreter solcher Anwendungen sind z.B. parallele Datenbanken, wie Oracle 9i RAC (Real Application Cluster). Zwar können auch controllerbasierte Storagesystem Daten spiegeln, sie tun dies aber immer nur innerhalb einer Box.

Wenn aus einem Storagesubsystem heraus Daten 'kopiert' werden in eine anderes System, auf dem diese dann nur gelesen werden können, spricht man üblicherweise von Replikation und nicht mehr von Spiegelung. Replikationsverfahren sind immer asymmetrisch, d.h. es gibt immer eine Quelle und mindestens ein Ziel. Die Zielkopie kann in der Regel nicht geschrieben werden, auf jeden Fall nicht so, dass die Daten symmetrisch wieder zurück-'gespiegelt' würden. Damit erlauben solche asymmetrischen Replikationstechnologien nicht den Einsatz von Anwendungen, die auf alle Kopien gleichzeitig zugreifen müssen, wie die o.a. parallelen Datenbanken.

4.3.2 Asynchron vs. synchron

Spiegelungs-, d.h. symmetrische Verfahren sind immer synchron. Synchron heißt, dass Daten erst dann als geschrieben gelten, wenn auch alle Kopien geschrieben worden sind. Daraus folgt sofort, dass es im asynchronen Fall immer ein Zeitfenster gibt, in dem bei einem Verlust einer Verbindung zu einem Storagesubsystem und einem gleichzeitigen Ausfall der Datenquelle Daten verloren gehen. Das scheint auf den ersten Blick nicht vertretbar, ist es aber in vielen Fällen doch.

Der große Nachteil synchroner Verfahren ist es, dass sie bei größeren Entfernungen zwischen Datenquelle und -ziel, eine erhebliche Verlängerung der Latenzzeiten zur Folge haben können, die wiederum Anwendungen, die I/O-intensiv sind, in ihrer Performance einschränken können. Das kann bei sehr großen Entfernungen, z.B. mehreren hundert Kilometern, dazu führen, dass Anwendungen nicht mehr vernünftig betrieben werden können.

D.h. es ist eine genaue Abwägung zwischen beiden Varianten mit ihren Nachteilen, möglicher Datenverlust gegen Performanceprobleme, zu treffen. Häufig lassen Randbedingungen, wie z.B. die Nichtzulässigkeit von Datenverlust im Finanzbereich keine die Wahl eindeutig.

4.3.3 Host-, vs. controller- vs. anwendungsbasiert

Um diesen Punkt gibt es immer wieder Glaubenskriege; vor allem die Vertreter controller-basierter Replikationstechnologien vertreten hier eine ganz harte Meinung. Worum geht es? Um die Frage, welche Komponente einer IT-Infrastruktur die Replikation tatsächlich durchführt. Bei den hostbasierten Technologien, wie z.B. Datenspiegelung durch Volume Manager, oder Datenreplikation steht vor allem die Flexibilität dieser Lösungen im Vordergrund. Zudem erlaubt die hostbasierte Spiegelung den parallelen Zugriff mehrerer Instanzen einer Anwendung über unterschiedliche Pfade von verschiedenen Hosts aus.

Controllerbasierte Replikation wie sie z.B. von Produkten wie EMC SRDF oder Hitachi DataSystems TrueCopy implementiert werden, wird auch manchmal Hardware Raid genannt. Dieser Ausdruck führt in die Irre, da natürlich auch hier Replikations-software im Spiel ist, die nur statt auf dem Host auf einem Serviceprozessor im Storagesubsystem abläuft. Wesentliche Argumente für diese Art der Replikation sind vor allem die klare Trennung zwischen Host- und Storagewelt und der verminderte CPU-Aufwand auf den Hosts.

Häufig wird übersehen, dass es noch eine dritte Art der Datenreplikation gibt, die anwendungsbasierte. Eine Anwendung kann ohne Probleme so implementiert werden, dass sie ihre Daten selbst mit Hilfe von standardisierten Schnittstellen und Protokollen repliziert. Dies hat vor allem den Vorteil, dass die Anwendung genau weiß, welche Daten tatsächlich wichtig sind und vor allem, wie die zu replizierenden Daten strukturiert sind. Während Volume Manager und cotrollerbasierte Technologien auf der Blockebene operieren, d.h. keinerlei Wissen über die Struktur der Daten haben, haben Anwendungen dies sehr wohl. Typische Vertreter dieser Technologien sind Produkte wie Oracle DataGuard oder auch Libelle, die Redo-Logs der Datenbank über IP-Verbindungen kopieren und auf dem Zielsystem wieder in die dort im Recovery Modus laufende Datenbank integrieren, u.U. mit einem Zeitversatz, um die Propagation von logischen Fehlern zu verhindern, sollten diese rechtzeitig entdeckt werden.

4.4 Anwendungen

Anwendungen sind nicht nur in der Lage, ihre eigenen Daten zu replizieren, sondern bieten häufig auch schon eigene Hochverfügbarkeitsfunktionalität mit. So kann z.B. DNS auch ohne Integration in einer Hochverfügbarkeitsinfrastruktur hochverfügbar laufen, da es Daten an sog. Secondary Nameserver propagiert, die von den Clients beim Ausfall des primären Nameservers verwendet werden können. Leider können die Daten solcher Secondaries dann nicht geändert werden, was es dann doch manchmal sinnvoll macht, den Primary zu clustern.

Auch die modernen Application Server bieten eingebaute Hochverfügbarkeit, so dass beim Ausfall einer Instanz, Anwendungen umdirigiert werden auf noch lebende Instanzen.

5 Mögliche Architekturen

Wie kommt man nun, nachdem es so viele unterschiedliche Aspekte in den einzelnen Teilbereichen gibt, zu einer möglichen Business-Continuity-Lösungen. In der Regel bestehen typische BC-Lösungen aus der sinnvollen Kombination mehreren Technologien wie auch die folgenden Beispiele zeigen sollen.

Die einfachste und vielfach präferierte Lösung ist ein geografisch auseinander gezogenes Cluster. D.h. eine Infrastruktur, die völlig automatisch agiert - so wie in einem lokalen Cluster, die so gut wie keinerlei zusätzliche Komplexität mit sich

bringt, und damit auch für den Betrieb beherrschbar erscheint. Solche Lösungen, typischerweise als Campus oder MetroCluster bezeichnet, können heutzutage über Entfernungen bis zu mehreren 100 km auseinander gezogen werden (z.B: SunCluster 3.0 mit DWDMs). Bild 2 zeigt eine solche Infrastruktur. Wichtig ist, dass dedizierte Verbindungen zwischen den Rechenzentren existieren müssen, über die Cluster-Hearbeats und Datenspiegelung laufen. Solche Verbindungen, basierend auf Monomode Fiber, sind sehr teuer und auch nicht überall in ausreichender Zahl zu bekommen. Der im Bild eingezeichnete DWDM, ein sog. Dense Wave Division Multiplexer, ist eine Komponente, die mehrere Protokolle über eine einzige Leitung über große Entfernungen multiplexen kann.

Wichtig ist hier, dass es sich bei dieser Lösung um ein einziges Cluster, das über zwei Standorte verteilt arbeitet, handelt.

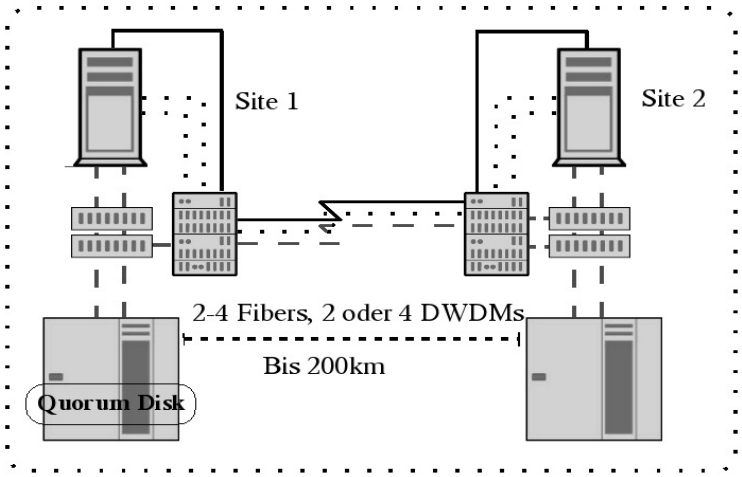

Bild 2: 'auseinander gezogenes' MetroCluster

Eine andere Möglichkeit, die nicht automatisch arbeitet, dafür aber mit zwei unabhängigen Kopien der Daten arbeitet und nicht in eine einzige Cluster-Infrastruktur integriert ist , und damit keinen einzigen 'single point of failure' (SPOF) hat, ist eine lose gekoppelte Lösung, bei der in mindestens zwei RZ voneinander unabhängige Cluster laufen, die voneinander unabhängige Kopien der unternehmenskritischen Daten verwalten und die nur sehr lose über eine zusätzliche HA-Schicht gekoppelt werden können. Diese nur lose gekoppelten Infrastrukturen werden sinnvoller Weise automatisch konsistent gehalten, z.B. was die Konfiguration der HA-Dienste angeht. Ist das nicht möglich und nur manuell durchführbar, entsteht eine große potentielle Fehlerquelle.

In den lose gekoppelten Cluster können unterschiedliche Datenreplikations-technologien eingesetzt werden. IP-basierte haben den Vorteil, dass sie keine spezielle Infrastruktur erfordern, und überall da eingesetzt werden können, wo Rechenzentren über das Internet verbunden sind.

Die entscheidende Frage bei solchen Konfigurationen sind:

- wer entscheidet, dass geschwenkt werden muss und
- wie wird der Schwenk durchgeführt.

Automatische Katastrophenerkennung ist ein schwieriges Problem. Zu unterschiedlich sind die Szenarien, als dass man ihre Erkennung algorithmisch erfassen könnte. Im schlimmstem Fall tritt die Katastrophe ja dadurch ein, dass auf Grund eines falschen Alarms oder einer vielleicht falschen Entscheidung, plötzlich das - angeblich - ausgefallene RZ und das Ausweich-RZ produktiv sind. Split Brain wird dieses Szenario auch genannt. Dies gilt es auf alle Fälle zu vermeiden. Lokale Cluster tun dies z.B. mit atomaren Reservierungstechniken auf der Storage-Ebene. Dies geht aber nicht mehr, wenn wir es mit getrennten Clustern zu tun haben.

Vollautomatisches Schwenken ist dann die zweite Herausforderung. Je nach Komplexität der Lösung kann eine solche Aktion sehr fehleranfällig sein. Betrachtet man zusätzlich noch die Extremsituation, unter der sich Administratoren bei einem solchen Schwenk befinden, immerhin ist gerade ein ganzes RZ ausgefallen, ist klar, dass diese Aktionen soweit wie möglich automatisiert ablaufen müssen. Der berühmte rote Knopf, der diese Aktion startet, ist hier wohl die einzig richtige Lösung.

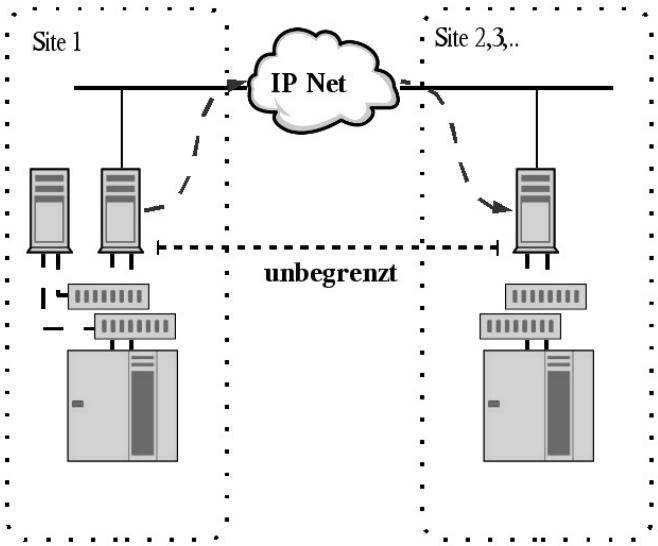

Bild 3: lose gekoppelte DR-Konfiguration mit IP-basierter Datenreplikation

Unbedingt notwendig ist aber, dass solche Schwenks, auch wenn man davon ausgeht, dass sie in der Realität nie notwendig sein werden, regelmäßig geübt werden. Ein einziger Fehler in den Prozeduren und Abläufen kann Millioneninvestitionen sinnlos machen. Unternehmen, die auf solche K-Fall Absicherungen angewiesen sind, üben solche Schwenks mit allen Beteiligten regelmäßig, d.h. mindestens einmal im Jahr, manchmal auch häufiger.

6 Zusammenfassung

Business Continuity Technologien sind unverzichtbar für das Funktionieren moderner IT-Landschaften. Dieses Papier hat an einigen Beispielarchitekturen exemplarisch aufgezeigt, welche Problem mit welchen Lösungen adressiert werden können. Es gibt nicht die eine Superlösung, die alles löst. Stattdessen müssen vom Betreiber einer solchen hochverfügbaren Infrastruktur die wichtigen Fragen beantwortet und dann mögliche Lösungen gegeneinander abgewogen werden.

Es sollte klar geworden sein, dass Hochverfügbarkeit und Business Continuity nicht mit Produkten allein, sondern dass diese Themen nur in umfassenden Projekten, die Betriebsführung (**P**rocesses), **P**rodukte und Menschen (**P**eople) - das sind die berühmten drei **P** - adressieren, gelöst werden können

7 Danksagung

Meinem Kollegen Olaf Schnapauff von Sun Microsystems gehört der Dank für viele intensive Diskussionen zum Thema Business Continuity.

8 Literatur

- Disaster Recovery Requirement Analysis, Stan Stringfellow, Sun Blueprint, Juli 2000
- Campus Clusters based on SunCluster Software, Hartmut Streppel, Sun Blueprint, November 2002
- Enterprise Continuity - A High Availability Application Solution, Sun Whitepaper, 2002

Sun Blueprints sind unter http://www.sun.com/blueprints verfügbar.