COLLAX Flexible IT

WHITEPAPER

Effektiver Schutz vor Split Brain und Stonith Deathmatch in Zwei-Node-Clustern

Fencing sichert die Datenintegrität und verhindert, dass Cluster-Nodes zu Einzelkämpfern werden

Eine hochverfügbare IT-Umgebung ist nicht nur für Großunternehmen, sondern auch für kleine und mittelständische Unternehmen unverzichtbar.

Speziell für Firmen dieser Größenordnung ist der Aufbau eines kleinen Clusters ein praktikabler Weg, um Hochverfügbarkeit sicherzustellen. Doch dabei gilt es, technische Falltüren wie „Split Brain“ und „Stonith Deathmatches“ zu vermeiden.

Einen Ausweg bieten spezielle Lösungen von Anbietern wie Collax. Sie eröffnen auch kleinen und mittelständischen Unternehmen den Weg zu einer hochverfügbaren IT-Infrastruktur, und dies bei überschaubaren Kosten und einem geringen Konfigurationsaufwand.

Inhaltsverzeichnis

Definition Hochverfügbarkeit / High Availability

Nach einer Definition des Institute of Electrical and Electronics Engineers (IEEE) bedeutet „Verfügbarkeit“, dass ein IT-System oder seine Komponenten betriebsbereit sind und einem Nutzer zur Verfügung stehen. „Hochverfügbarkeit“ (High Availability, HA) ist dann gegeben, wenn ein IT-System oder darüber bereitgestellte Services auch dann genutzt werden können, wenn wesentliche Komponenten, etwa ein Server oder eine Festplatte, ausfallen beziehungsweise nicht mehr zugänglich sind. Dafür können beispielsweise technische Probleme verantwortlich sein, aber auch geplante Downtimes, etwa im Rahmen von Wartungsarbeiten.

Verfügbarkeit

In welchem Maße IT-Systeme verfügbar sind, lässt sich auf unterschiedliche Weise berechnen. Das erste Verfahren gibt die Verfügbarkeit eines IT-Systems in Prozent an. Bezugsgrößen sind die Betriebszeit und die Ausfallzeiten von IT-Komponenten. Daraus lässt sich anhand folgender Formel ermitteln, wie hoch die Wahrscheinlichkeit ist, dass ein IT-System fehlerfrei funktioniert:

$$A\,(Availability) = \frac{Betriebszeit - Ausfallzeit}{Betriebszeit} \times 100\,(\%)$$

Dazu folgendes Beispiel: Der Web- und E-Mail-Server eines mittelständischen Unternehmens soll idealerweise rund um die Uhr verfügbar sein, also 8760 Stunden im Jahr. Wegen Wartungsarbeiten werden jedoch 8,5 Stunden weniger erreicht, also 8751,5 Stunden. Dies ergibt somit folgenden Verfügbarkeitswert:

$$A = \frac{8760\ h - 8{,}5\ h}{8760\ h} \times 100 = 99{,}9\%$$

Mean Time Between Failures und Mean Time to Repair

Ein anderer Ansatz berücksichtigt zum einen die Zeit, die zwischen dem Auftreten von zwei Fehlern liegt (Mean Time Between Failures, MTBF), zum anderen die Zeitspanne, bis dieser Fehler beziehungsweise dessen Folgen behoben sind (Mean Time to Repair, MTTR). Die Verfügbarkeit eines IT-Systems wird in diesem Fall auf folgende Weise berechnet:

$$A = \frac{MTBF}{MTBF + MTTR} \times 100\,(\%)$$

Auch dazu ein Beispiel: Für das Mainboard eines Server-Systems gibt der Hersteller eine MTBF von 135.000 Stunden an. Für das Austauschen eines fehlerhaften Boards fallen im laufenden Jahr 30 Minuten (0,5 h) an. Dies ergibt laut der Formel:

$$A = \frac{135.000\ h}{135.000\ h + 0{,}5\ h} \times 100 = 99{,}999\%$$

Bei diesen Rechenbeispielen ist allerdings zu berücksichtigen, dass eine IT-Umgebung aus vielen Komponenten besteht, die reibungslos zusammenspielen müssen, damit IT-Dienste zur Verfügung stehen: Server, Netzwerkkomponenten, Storage-Systeme sowie die dazugehörenden Anwendungen und Betriebssysteme. Je komplexer eine IT-Umgebung ist, desto höher auch die Gefahr, dass einzelne Komponenten ausfallen und somit die Verfügbarkeit der Infrastruktur sinkt.

Wo High Availability beginnt

In welchem Umfang ein System bereitstehen muss, damit es als „hochverfügbar“ gilt, ist nicht klar definiert. Die Beratungsgesellschaft Harvard Research Group geht beispielsweise ab einem Wert von 99,99 Prozent (einer Stunde Downtime pro Jahr) von Hochverfügbarkeit aus. Dagegen sehen die Analysten von Gartner High Availability bereits bei einer Verfügbarkeit von 99,95 Prozent beziehungsweise einer Ausfallzeit von 4,4 Stunden und weniger gegeben.

Wichtig im Zusammenhang mit HA ist, dass alle Komponenten berücksichtigt werden, die für die Bereitstellung eines IT-Services erforderlich sind. Das heißt beispielsweise:

1. Die Server und Storage- Systeme sind aktiv und stellen die gewünschten IT-Services beziehungsweise Anwendungen und Daten bereit.
2. Die Netzwerkverbindungen zwischen Servern und Storage- Systemen sowie den Client-Systemen der Nutzer sind intakt.
3. Der Arbeitsplatzrechner des Nutzers hat die Client- Anwendung ordnungsgemäß gestartet.

Warum Hochverfügbarkeit für kleine und mittelständische Unternehmen wichtig ist

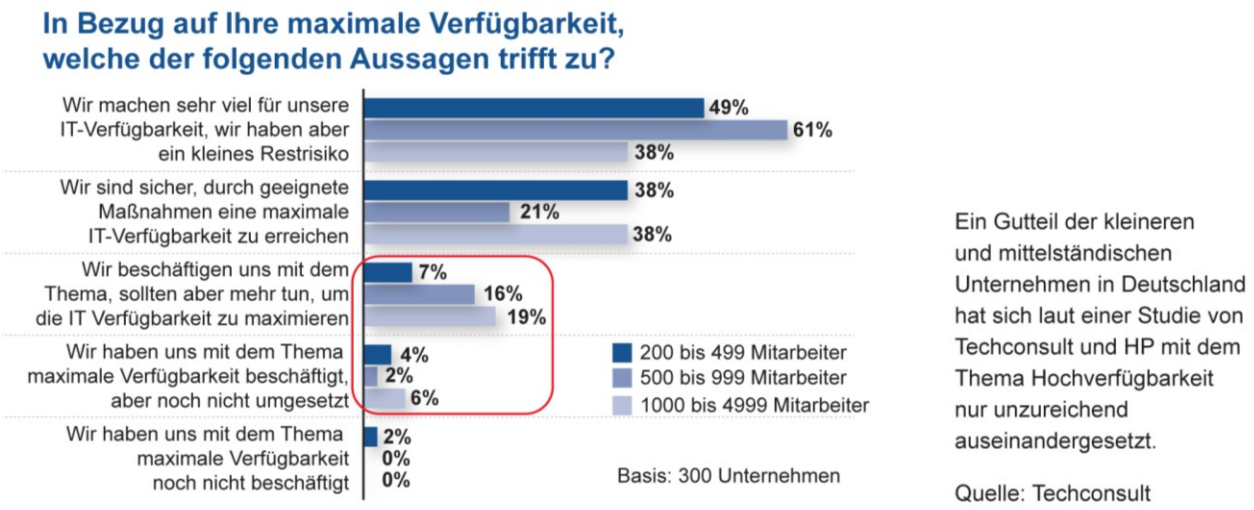
Speziell in kleineren und mittelständischen Unternehmen hält sich das Vorurteil, dass nur Großfirmen eine hochverfügbare IT-Infrastruktur benötigen – und sich diese auch leisten können. Dabei sind HA-Lösungen durchaus auch für eine Arztpraxis, einen Steuerberater oder Immobilienmakler oder einen Handwerksbetrieb mit „nur“ 20 oder 30 Mitarbeitern relevant. Das hat unteranderem folgende Gründe:

- Auch kleinere Unternehmen sind auf eine reibungslos funktionierende IT angewiesen. Zentrale Bereiche wie die Auftrags- und Kundenverwaltung, das Terminmanagement und das Rechnungswesen basieren auf elektronischer Datenverarbeitung.
- IT und Internet bilden das Rückgrat der Kommunikationsinfrastruktur eines Unternehmens (Voice over IP, E-Mail, Collaboration-Services, Messaging-Dienste). Das gilt für den Informationsaustausch zwischen den Mitarbeitern sowie für die Kommunikation mit Kunden, Partnern und Zulieferern.

- Der Ausfall von IT-Komponenten und entsprechenden Diensten kann die Geschäftstätigkeit und das Image eines Unternehmens nachhaltig beeinträchtigen. Die möglichen Folgen: Umsatzverluste und das Abwandern von Kunden zu Mitbewerbern.

Dass der Ausfall beziehungsweise die Nichtverfügbarkeit von wichtigen IT-Komponenten und -Services ein ernst zu nehmendes Problem darstellt, belegt eine Studie, die von der Marktforschungsgesellschaft Techconsult 2013 im Auftrag von HP erstellt wurde. Demnach verzeichnen 30 Prozent der mittelständischen Unternehmen in Deutschland mit bis zu 499 Mitarbeitern zwischen zwei und fünf IT-Systemausfälle pro Jahr. Bei 12 Prozent der Befragten gibt es zwischen sechs und zehn solcher Vorfälle, bei 3 Prozent versagen IT-Systeme gar bis zu zwanzigmal im Jahr. Insgesamt verzeichneten 77 Prozent der Firmen solche Vorkommnisse, die pro Stunde Kosten in Höhe von 20.278 Euro verursachen.

Mittelständischen Unternehmen ist sehr wohl bewusst, welche negativen Auswirkungen der Ausfall von IT-Systemen haben kann. Dennoch verzichten viele auf den Einsatz von Hochverfügbarkeitslösungen. Das ist ein zentrales Ergebnis einer Befragung von kleinen und mittelständischen Unternehmen (KMU) in Deutschland, die das Beratungshaus Techconsult 2013 im Auftrag von HP durchführte. Laut der Studie verzeichneten 2012 rund 77 Prozent der KMU Ausfälle geschäftskritischer IT-Systeme, etwa in den Bereichen Warenwirtschaft, Vertrieb und Fertigung. Pro Stunde kostete ein Ausfall Mittelständler mit bis zu 499 Mitarbeitern pro Stunde mehr als 20.000 Euro.



Studie: *Der Mittelstand investiert zu wenig in Hochverfügbarkeit*

Die durchschnittlichen Kosten eines Systemausfalls summierten sich laut Techconsult auf 25.000 bis 40.000 Euro. Allerdings gaben an die 40 Prozent der befragten IT-Fachleute an, dass sie gar nicht wissen, welcher finanzielle Schaden dem Unternehmen durch die Downtime von IT-Systemen entstanden ist. Hinzu kommt laut der Studie eine allzu optimistische Einschätzung der Maßnahmen, die die Verfügbarkeit von IT-Ressourcen sicherstellen sollen. Fast jeder zweite Befragte gab zwar an, kritische IT-Systeme seien in ausreichendem Maße abgesichert, musste aber einräumen, dass beträchtliche “Restrisiken” bestehen. Ein zentrales Resultat der Studie lautet somit: KMU in Deutschland tun zu wenig, um die Verfügbarkeit beziehungsweise Hochverfügbarkeit unternehmenskritischer IT-Ressourcen sicherzustellen.

Clustering als Schlüssel zu Hochverfügbarkeit

Um eine hochverfügbare IT-Infrastruktur aufzubauen, bietet sich der Einsatz eines HA-Clusters an. Er besteht aus folgenden Komponenten:

Mindestens zwei oder mehr Servern (Nodes). Sie werden idealerweise an unterschiedlichen Standorten platziert, um die Disaster-Recovery-Fähigkeiten zu verbessern (Geo-Cluster).

Verfügbarkeitsklassen laut BSI					
Schutzbedarf	Potenzialstufe	Merkmal 1	Merkmal 2	V-Klasse (VK)	Tier-Klasse
Gering	1	Robuste Komponenten	Robustheit als Voraussetzung für Skalierbarkeit	VK 0 / < 99 %	
Normal	2	Partielle Redundanz; einpfadig	Single Points of Failure (SPoF) vorhanden	VK 1 / 99 %	T1
Hoch	3	n+1-Redundanz; zweipfadig bei IT-Verkabelung	Systematische Überwachung zur Identifizierung und Beseitigung von SPoF	VK 2 / 99,9 %	T2
Sehr hoch	4	2 x n-Redundanz; zweipfadig bei Energieversorgung; Geo-Redundanz	Systematisches Management auf Basis von Indikatoren; Optimierung nach 2 x (n-1)	VK 3 / 99,99 %	T3
Höchstverfügbar	5	Vollredundanz; mehrpfadig; jeder Pfad n+1, also 2 x (n+1); Geo- und Wartungsredundanz	Systematische Steuerung und Optimierung unter allen technischen und organisatorischen Gesichtspunkten	VK 4 / 99, 999 %	T4
Desastertolerant	5+	Vollredundanz; mehrpfadig; jeder Pfad n+1, also m x (n+1)		VK 5	

Quelle: BSI / HV-Kompendium Band AH

Einer zentralen Speicherlösung (Storage-System), auf die alle Cluster-Nodes zugreifen. Das Storage-System wird häufig über ein separates Netz (SAN, Storage Area Network) angebunden, etwa auf Basis von Fibre Channel.

Weiteren Bestandteilen wie einem Management-Server, einer Cluster-Management-Software, einer Datenbank und Administrationswerkzeugen.

Einem Abgrenzungsverfahren (Stonith-System; eine ausführliche Erklärung folgt weiter unten), das verhindert, dass sich Cluster- Nodes gegenseitig lahmlegen.

Wenn auf einem Cluster-Knoten (Node) ein Fehler auftritt, werden seine Aufgaben von anderen Knoten übernommen. Dieser Vorgang wird als Fail-over bezeichnet. Dieses Fail-over erfolgt allerdings in der Regel nicht in Echtzeit, sondern kann je nach HA-Lösung sowie Art und Zahl der Anwendungen und Prozesse, die neu gestartet werden müssen, bis zu mehrere Minuten dauern. In HA-Clustern, die aus einer Aktiv/Passiv-Konfiguration bestehen, also aus einem aktiven und einem passiven Reserveknoten, sind Fail-over-Zeiten von 20 bis 60 Sekunden zu erwarten.

Aus diesem Grund erreichen HA-Cluster in der Regel eine Verfügbarkeit von etwa 99,99 Prozent. Dies ist für die meisten Einsatzzwecke vollkommen ausreichend. Das gilt vor allem für Anwendungen wie Office-Applikationen, E-Mail und auch Web- Server. Die zulässige Downtime beträgt bei 99,99 Prozent Verfügbarkeit etwa eine Stunde pro Jahr. Anders liegt der Fall bei Online-Buchungssystemen oder der IT-Infrastruktur von Finanzdienstleistern. Sie müssen quasi rund um die Uhr bereitstehen, also eine Verfügbarkeit von 99,999 % aufweisen.

Traditionelle Cluster-Lösungen nicht für KMU tauglich

Allerdings sind herkömmliche HA-Cluster-Lösungen für kleinere Unternehmen nur bedingt tauglich. Das hat mehrere Gründe, zum Beispiel die Aufwendungen für die technische Ausrüstung oder der hohe Komplexitätsgrad. Ein traditioneller HA-Cluster benötigt ein Storage Area Network, inklusive entsprechender Switches, ein Hochleistungs-LAN und einen weiteren Server für das Management. Hinzu kommen die Kosten für die entsprechenden Software-Tools, etwa die Cluster-Software und Betriebssysteme.

Kostenfaktoren sind insbesondere:

- die Cluster-Software
- das SAN: Zu den Aufwendungen für das Hochleistungsnetz können bei SAN-Speichererweiterungen zusätzliche Lizenzkosten kommen.
- der Management-Server: Er ist in der Regel als virtuelle Maschine konzipiert. Allerdings wird zur Absicherung eine weitere physische Maschine empfohlen, die wiederum ein Betriebssystem (Lizenzkosten) erfordert.
- die Geschäftsanwendungen: Dieser Kostenblock bleibt bestehen.

Eine weitere Schwachstelle herkömmlicher HA-Cluster-Lösungen: Das Konfigurieren und Managen solcher Umgebungen überfordert in der Regel die IT-Mitarbeiter kleiner und mittelständischer Unternehmen. Dies umso mehr, als viele dieser HA-Lösungen aus Komponenten unterschiedlicher Anbieter bestehen. Der Anwender sieht sich somit mit unterschiedlichen Ansprechpartnern und Technologien konfrontiert.

Hochverfügbarkeit ist nicht gleich Disaster Recovery

Oft werden High Availability und Disaster Recovery in einen Topf geworfen – zu Unrecht. Disaster Recovery (DR) umschreibt alle Maßnahmen, die bei Eintreten einer Katastrophe an einem Rechenzentrumsstandort ein Fortführen des IT-Betriebs sicherstellen. Dazu zählen beispielsweise der Aufbau von Ausweich- Data-Centern an anderen Standorten und das regelmäßige Spiegeln von Daten zwischen diesen Rechenzentren. DR greift dann, wenn ein komplettes Rechenzentrum nicht mehr funktionsfähig ist, etwa durch einen Brand, ein Erdbeben oder einen Wassereinbruch.

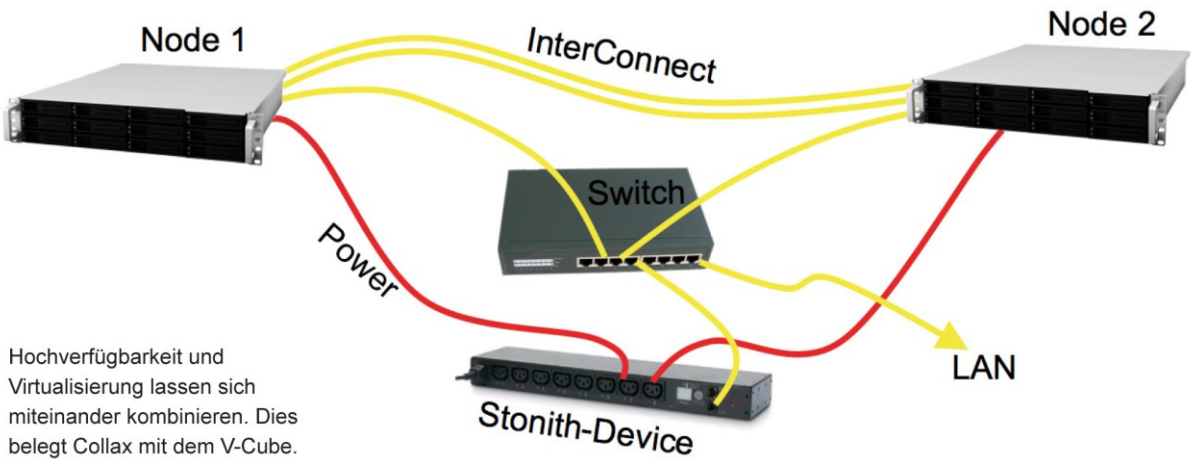
Hochverfügbarkeit zielt darauf ab, Ausfallzeiten zu reduzieren, die in einem Rechenzentrum auftreten. In kleinen Unternehmen kann ein solches Data- Center nur aus einem Server-Schrank mit einem Server, einem Speichersystem und einem Netzwerk-Switch bestehen. Typische Ursachen solcher Ausfallzeiten sind Systemfehler, etwa das Versagen von Festplatten, Netzwerk-adaptern oder Lüftern von Servern und Switches.

Einen Ausweg bietet die Kombination von zwei Technologien: Clustering und Virtualisierung. Eine entsprechende Lösung mit zwei Nodes bietet Collax mit dem Collax V-Cube+ an. Sie besteht aus folgenden Elementen:

- zwei Virtualisierungsservern V-Cube auf Basis der Virtualisierungslösung KVM (Kernel-based Virtual Machine)
- dem Cluster- und Storage-Modul: Es bildet mit den in den Servern vorhandenen Festplatten ein hochverfügbares SAN. Der Anwender muss somit kein separates Speichernetz aufbauen.
- einem Stonith-Device: Dieses System trennt einen nicht ordnungsgemäß funktionierenden Node vom Stromnetz und initiiert einen Neustart.

Die beiden V-Cube-Nodes stehen als Software und als Hardware-Appliances zur Verfügung. Sie werden über zwei Cluster-Interconnect-Kabel miteinander verbunden und zusätzlich an einen LAN-Switch angeschlossen. Zudem sind die beiden Nodes mit dem Stonith-Device verbunden.

Der Aufwand für die Installation ist überschaubar: Auf beiden Nodes wird V-Cube+ installiert. Anschließend startet der Administrator die beiden Knoten und beginnt mit der Konfiguration. Diese Arbeiten sind innerhalb weniger Stunden erledigt. Bei anderen komplexen Cluster-Lösungen dauert dieser Vorgang bis zu mehreren Tagen.



Hochverfügbarkeit und Virtualisierung lassen sich miteinander kombinieren. Dies belegt Collax mit dem V-Cube.

Bild: Collax

Um bereits vorhandene physische Unternehmensserver zu virtualisieren und in den Cluster von Collax zu integrieren, steht ein Migrations-Tool zur Verfügung. Collax V-Cube+ ist zu virtualisierten Servern von Drittanbietern kompatibel. In diesem Fall wird dieser Server in einen Collax V-Cube+ auf demselben Weg eingebunden.

KMU, die im Zuge des Umstiegs auf eine HA-Cluster-Lösung von Collax neue Server implementieren möchten, können auf Server-Templates zurückgreifen, die per Cloud-Mechanismus verfügbar sind. Zur Wahl stehen beispielsweise eine Groupware-Suite, ein Business-Server und ein Security-Gateway.

Vorteile einer HA-Lösung für virtualisierte Infrastrukturen

Eine Hochverfügbarkeitslösung auf Basis eines Clusters, wie sie Collax zur Verfügung stellt, hat mehrere Vorzüge: Sie lässt sich einfach aufsetzen und verwalten und kommt mit einer einfachen Netzwerkstruktur aus – ohne SAN und separate Management-Hard- und Software. Weitere Pluspunkte sind die geringen Anfangskosten und die schnelle Implementierung. Außerdem kann der Cluster wachsen und später vergrößert werden, wenn die Notwendigkeit dazu bestehen sollte.

Um eine optimale Lastverteilung zu erreichen, können zudem Virtual Machines nach Bedarf auf die Cluster-Nodes verteilt werden. Fällt ein Server aus, arbeiten die VM auf dem anderen System

weiter. Auch Wartungsarbeiten an einem Server-System lassen sich auf einfache Weise durchführen: Für die Dauer des Wartungsintervalls verschiebt der Administrator die betroffene VM auf den anderen Knoten (Live Migration). Dies stellt sicher, dass der Zugriff auf Daten und Anwendungen weiterhin gegeben ist und Geschäftsprozesse nicht unterbrochen werden.

Split Brain: Cluster-Knoten werden zu Einzelkämpfern

Bei der Konzeption seiner HA-Cluster-Lösung hat Collax Vorkehrungen gegen ein Problem getroffen, das speziell bei HA-Clustern mit zwei Knoten ausgeschlossen werden muss: Split Brain. Zu einer solchen Situation kommt es, wenn die Verbindung unterbrochen wird, über die beide Knoten des Clusters Statusinformationen austauschen (Cluster Interconnect), oder wenn ein Knoten wegen einer Überlastsituation solche Informationen verzögert übermittelt. Die Folge: Beide Nodes gehen davon aus, dass der jeweils andere Cluster-Knoten nicht mehr verfügbar ist, und wollen dessen Funktion übernehmen.

Damit verbunden ist der Versuch beider Nodes, die Kontrolle über die gemeinsam genutzten Speicher-Ressourcen (Storage-System beziehungsweise Volumes) zu übernehmen. Solange beide Knoten darauf nur Lesezugriffe durchführen würden, wäre das unproblematisch. Wenn beide jedoch unabhängig voneinander Daten auf dem Volume ablegen, wird die Konsistenz der Daten beeinträchtigt. Bei vielen Anwendungen ist eine Zusammenführung der auseinandergelaufenen Daten praktisch unmöglich. De facto bedeutet dies den Datenverlust. Seite 9 Hochverfügbarkeitslösungen für kleine und mittelständische Unternehmen 10/2013

Die perfekte IT-Lösung für kleine Unternehmen

Kleine Unternehmen benötigen eine IT-Infrastruktur, die im Idealfall folgende Anforderungen erfüllt:

Hohe Ausfallsicherheit: Die Downtime sollte nahe null liegen. Dies lässt sich nur mit einer Hochverfügbarkeitslösung erreichen, die erschwinglich und leicht zu implementieren ist und zudem einen geringen Wartungsaufwand mit sich bringt.

Große Flexibilität: Die IT-Umgebung sollte sich dynamisch an geänderte Anforderungen anpassen, erweitern und modifizieren lassen. Dies ist wichtig, damit Unternehmen schnell auf neue Marktentwicklungen reagieren können.

Niedrige Investitionskosten: Den Luxus, auf Vorrat ungenutzte IT-Ressourcen vorzuhalten, kann sich kein Unternehmen mehr leisten. Gefordert ist eine Infrastruktur, die sich schnell dem tatsächlichen Bedarf anpassen lässt. Der Nutzer zahlt nur für die Ressourcen, die er tatsächlich verwendet (Pay per Use).

Perfekte Passgenauigkeit und hohe Effizienz: Die Lösung muss sich exakt auf die vorhandenen Prozesse und IT-Systeme abstimmen lassen. Das vermeidet Reibungsverluste und reduziert den finanziellen Aufwand.

Fencing gegen die Folgen von Split Brain

Die negativen Auswirkungen einer Split-Brain-Situation in einem HA-Cluster lassen sich mithilfe von Fencing verhindern. Fencing ist ein Abgrenzungsverfahren, das in einem Server-Cluster einen nicht mehr funktionierenden oder erreichbaren Cluster-Node isoliert. Dies verhindert, dass der besagte Node weiterhin auf Daten zugreift, die die Cluster-Rechner gemeinsam nutzen, etwa auf einem „Shared"-Storage-System. Auf diese Weise wird die Integrität dieser Daten gewahrt.

Es gibt folgende Arten von Fencing:

Fencing auf der Ressourcen-Ebene: In diesem Fall wird der Zugriff des fehlerhaften Cluster-Nodes auf bestimmte IT-Ressourcen unterbunden, etwa auf ein Storage Area Network oder spezielle Netzwerkdienste.

Node-Fencing: Der Cluster-Knoten, der nicht ordnungsgemäß arbeitet, wird komplett von allen IT-Ressourcen abgekoppelt beziehungsweise heruntergefahren.

Fencing wird in der Praxis von einer dritten Instanz vorgenommen. Das kann ein Administrator sein. In Clustern mit mehr als zwei Nodes übernehmen auch die Cluster-Knoten selbst oder die Cluster-Management-Software diese Entscheidung („Quorum"): Kommen beispielsweise Knoten A und B zu dem Resultat, Knoten C sei defekt oder nicht erreichbar, initiieren sie dessen Ausgrenzung aus dem Cluster.

Eine einfache und effiziente Fencing-Methode ist der Einsatz der bereits erwähnten Stonith-Systeme. Sie trennen den fehlerhaften Node schlicht und einfach von der Stromversorgung. Anschließend startet der Knoten neu oder er bleibt inaktiv, bis der Systemverwalter die Analyse des Systems abgeschlossen hat.

Stonith steht für „Shoot the Other Node in the Head". Als Stonith-Geräte lassen sich beispielsweise schaltbare Steckdosenleisten mit Netzwerkschnittstelle, Power Distribution Units (PDUs) und unterbrechungsfreie Stromversorgungen (USV) einsetzen. Das „Abschießen" eines Cluster-Knotens kann nicht nur bei dem bereits angesprochenen Abbruch der Verbindung zwischen den Nodes erforderlich sein:

- Der andere Node ist physisch „tot“, etwa wegen einer Kernel Panic, eines massiven Defekts auf dem Mainboard oder wegen Ausfalls der Stromversorgung inklusive der Notstromversorgung (USV).
- Eine Komponente der HA-Lösung (Web-Server, Datenbank, File-System) lässt sich nicht herunterfahren, etwa dann, wenn die betreffende Ressource nicht richtig gestartet wurde.

Auch in diesen Fällen greift der noch funktionsfähige Knoten auf Stonith zurück, um den defekten Node aus dem Cluster zu entfernen.

Tödliche Endlosschleife: das Stonith Deathmatch

Allerdings kann es im Zusammenhang mit Stonith zu folgender paradoxer Situation kommen: Beide Nodes eines Zwei-Node-Clusters gelangen zu der Auffassung, der jeweils andere Knoten sei nicht mehr erreichbar beziehungsweise funktionstüchtig und müsse daher mittels Stonith deaktiviert werden. Das Ergebnis ist unter Umständen ein „Stonith Deathmatch“: Knoten A initiiert einen Stonith und veranlasst ein Herunterfahren und Neustarten des zweiten Knotens. Knoten B tut dasselbe, bevor ihn der Stonith-Befehl von Node A erreicht. Die Konsequenz ist, dass beide Knoten wechselweise von ihrem Pendant „abgeschossen“ werden und nach dem Neustart dasselbe mit dem anderen Node tun.

Ein solches Deathmatch lässt sich vermeiden, wenn der Knoten, bei dem eine Fehlfunktion vermutet wird, mittels einer schaltbaren Steckdosenleiste vom Stromnetz getrennt und ein Wiederhochfahren unterbunden wird. Dies gibt dem Administrator die Gelegenheit, die Fehlerursachen zu analysieren und den betreffenden Knoten anschließend wieder in Betrieb zu nehmen. Bei der Auswahl der schaltbaren Steckdosenleiste muss darauf geachtet werden, dass sie verhindern kann, dass zwei Stonith-Befehle gleichzeitig ausgeführt werden können.

Dieses Verfahren kommt auch bei den Cluster-Lösungen von Collax zum Einsatz. Damit das Stonith-Device nicht zu einem „Single Point of Failure“ wird, lassen sich zwei Steckdosenleisten parallel einsetzen.

Und welche Lösung gibt es für kleine Mittelständler?

Speziell für kleine Unternehmen wie Anwaltskanzleien, Einzelhändler, Handwerksbetriebe oder Dienstleistungsfirmen sind Hochverfügbarkeitslösungen rar gesät. Einen Ausweg bietet Collax mit dem speziell für diese Klientel entwickelten V-Bien. Dieses HA-Produkt ist auf die Anforderungen von Firmen mit 6 bis 25 Mitarbeitern zugeschnitten. Im Vergleich zu Collax V-Cube+ wurden Installations- und Konfigurationsaufwand reduziert und das Fencing-Verfahren optimiert, sodass keine schaltbare Steckdosenleiste mehr notwendig ist.

Collax V-Bien ist ebenfalls eine Cluster-Lösung mit zwei Nodes, die auf Collax V-Cube+ basiert. Im Vergleich zu V-Cube+ stehen dem Anwender allerdings weniger Systemkonfigurationen zur Verfügung. Dies spiegelt sich in einem niedrigeren Preis von deutlich unter 10.000 Euro für Hard- und Software wider. V-Bien ist darauf ausgerichtet, Ausfallsicherheit für wenige, ausgewählte Anwendungen zu bieten, die für das Kerngeschäft eines kleinen mittelständischen Unternehmens unverzichtbar sind.

Ebenso wie bei V-Cube+ dient Collax V-Bien der Absicherung von virtualisierten Servern und der darauf befindlichen Daten. Mit V-Bien unterstreicht Collax, dass Hochverfügbarkeit und Clustering kein Privileg von Unternehmen aus dem gehobenen Mittelstand oder von Großfirmen ist. Mit dieser Lösung kann auch ein Handwerker, Händler oder Arzt seine IT-Infrastruktur ausfallsicher gestalten und somit einem IT-oder Daten-GAU wirkungsvoll vorbeugen.

Fazit

Hochverfügbarkeit ist ein Thema, das nicht nur für große Unternehmen relevant ist. Auch kleinere Betriebe sind häufig darauf angewiesen, dass ihre IT-Systeme möglichst ohne Unterbrechung zur Verfügung stehen. Sie können sich mit der speziellen Lösung von Collax vor unerwünschten Ausfällen schützen, ohne ihre Budgets überstrapazieren zu müssen.

Collax – Ihr Spezialist für sichere, stabile und hochverfügbare IT-Infrastrukturen

Collax bietet Lösungen für Hochverfügbarkeit und Virtualisierung sowie für Netzwerk-Infrastrukturen, Kommunikation und Sicherheit, die exakt auf die Anforderungen von kleinen und mittelständischen Unternehmen (KMU) und Freiberuflern zugeschnitten sind. Die effizienten IT-Plattformen sind flexibel, anpassungsfähig, stabil und sicher und umfassen die zwei Produktlinien Collax V-Server und Collax C-Server.

Die **Collax V-Server** bieten Virtualisierung und Hochverfügbarkeit speziell entwickelt für die Anforderungen von KMU und Freiberuflern. Dabei zeichnen sie sich durch einfache Administration, maximale Verfügbarkeit und durch ein faires Preismodell aus. Die **Collax C-Server** bilden zusammen die komplette IT-Infrastruktur nach. Schnell installiert, flexibel einsetzbar und zu einem fairen Preis, decken die Lösungen drei Sparten ab: Infrastruktur, Security und Collaboration.

Das Unternehmen mit Hauptsitz in München wurde im Jahr 2005 gegründet. Heute kann Collax rund 30.000 Installationen und 6.000 Kunden vorweisen. Der Lösungsanbieter vertreibt seine Produkte indirekt über rund 600 Partner: Distributoren, Systemhäuser und VARs sowie ISVs und OEMs.

Sie wünschen weitere Informationen, haben Fragen oder möchten einen Termin mit Collax vereinbaren? Kontaktieren Sie uns, wir freuen uns auf den Dialog mit Ihnen:

Collax GmbH
Dieselstraße 25
85748 Garching
Deutschland
Telefon: +49 (0) 89-99 01 57-0
Fax: +49 (0) 89-99 01 57-11
E-Mail: info@collax.com
Internet: www.collax.com