Zehn Mal Hochverfügbarkeit

Martin Klier, Performing Databases GmbH

Betrachtungen zu einem alten Buzzword mit den Augen des modernen Datenbank-Administrators

01 Hochverfügbarkeit

Ein System ist hochverfügbar, wenn es mit einer hohen Wahrscheinlichkeit in der Lage ist, den Betrieb auch bei Störungen aufrechtzuerhalten. Schnell geht es dabei um harte Fakten, Zahlen und Service Level Agreements (SLA). So bedeuten die berühmten „five niners" 99,999% Verfügbarkeit. Erstreckt sich der betrachtete Zeitraum auf das volle Jahr, muss das besprochene System bis auf 315 Sekunden (5,26 Minuten) jederzeit betriebs- und leistungsbereit sein.

Da viele Upgrades und Patches einesteils zur Absicherung des Betriebes notwendig sein können, andererseits aber auch oft mit der zeitweisen Abschaltung einer Umgebung einhergehen, entsteht ein Dilemma. Gelöst wird dies in der Praxis unter erhöhtem Einsatz von Ressourcen durch parallel betriebene Umgebungen oder vereinfachend und kostensparend mit einer Reduzierung des für die Verfügbarkeit relevanten Zeitraumes (etwa durch Nichtbetrachtung von Urlaubszeiten).

Es ist nicht automatisch ausgeschlossen, menschliche Eingriffe zur Ermöglichung oder Erhaltung dieser Fähigkeit einzukalkulieren. Oft jedoch beziehen sich entsprechende Angaben auf die autonome Betriebsfähigkeit ohne Eingriffe.

02 Fehlertoleranz

Die einem System eigene Fehlertoleranz beschreibt, wie stark es gegen Bedrohungen seiner Verfügbarkeit abgeschirmt ist. So wird etwa definiert, wie viele Server, Netzwerk-Komponenten oder Storage-Spiegel gleichzeitig ausfallen können, ohne die Verfügbarkeit des Systems einzuschränken.

03 Backup und MTTR

Im Falle eines Desasters – wie Verlust von Nutzdaten oder Konfigurationen – ist für den Wiederanlauf der Umgebung eine unabhängig abgelegte Datensicherung unabdingbar. Ist dies noch der allgemeinen Absicherung zuzurechnen, wird spätestens die Mean Time To Recover (MTTR) relevant für die Beschreibung der Verfügbarkeit. Diese „mittlere Zeit für ein Recovery" bestimmt, wie schnell ein zerstörtes System wieder betriebsfähig ist. Eine verlustfreie Wiederherstellung in möglichst kurzer Zeit erfordert gute Planung von Hardware und Implementierung. Regelmäßige Tests von Konzept und Implementierung sollten eine Selbstverständlichkeit sein: „An untested backup is just a prayer on tape."

04 Faktor „Mensch"

Bei vielen, scheinbar rein technischen Problemen wird der Mensch oft zu schnell als begrenzender Faktor angesehen. In der Praxis aber benötigen zuverlässige und zweckmäßige IT-Anlagen die Betreuung und Pflege durch den kompetenten und engagierten Menschen. Ein elegantes Design wird es verstehen, die Stärken von Automaten und Menschen jeweils auszunutzen und die Schwächen gegenseitig zu kompensieren. Analog zum Betrieb anderer komplexer Maschinen (Beispiel: Flugzeug) sind dabei vor allem die Arbeitsbelastung und die Möglichkeit zur Fehlentscheidung durch den Bediener in Stress-Situationen zu begrenzen.

Um schon bei der Planung die optimale, von menschlichen Fehlern möglichst freie Architektur zu erreichen, ist ein guter Prozess unabdingbar. Vier Augen sollten das absolute Minimum sein und eine Kombination von zeitgemäßen Technologien und bewährten Konzepten zur Anwendung kommen.

05 Features, Komplexität und Beherrschbarkeit

Alle Technologien zur Hochverfügbarkeit, die als Standard-Produkt auf dem Markt platziert sind, müssen dafür ein weites Feld von Anwendungen abdecken. Dies führt unweigerlich zu einer Fülle von Features, die zur Auswahl stehen.

Aber mit jeder Funktion, mit jedem „Gimmick" erhöht sich der Freiheitsgrad für Störungen ebenso wie der für den Nutzen. Je mehr schief gehen kann, desto mehr wird auch schief gehen, dies drückt schon das sprichwörtliche Gesetz von Murphy treffend aus.

Ein High-Availability-System (HA-System) muss einfach zu verstehen und leicht zu beherrschen sein – so lassen sich Fehler in allen Phasen vermeiden: bei Planung, Implementierung, Test, Inbetriebnahme, Operating und auch im Fall der Fälle, wenn es seinen Wert im Ernstfall beweisen muss.

Merke: Komplexität ist der natürliche Feind der Hochverfügbarkeit!

06 Monitoring

Die dauerhafte Betriebsbereitschaft einer hochverfügbaren Umgebung ist ohne fortlaufende, den Menschen entlastende Überwachung nicht zu erreichen. Was nützt das solideste Cluster, die smarteste Replikation oder die verlässlichste Spiegelung, wenn völlig unbemerkt die Ressourcen aufgebraucht sind? Auch dann ist die Verfügbarkeit plötzlich beeinträchtigt und in vielen Fällen provoziert eine überraschende und vermeidbare Notsi-

tuation fehlerträchtige Stress-Entscheidungen.

Das durchdachte und erprobte Monitoring- und Alerting-Konzept ist daher als Grundbaustein der Hochverfügbarkeit zu betrachten: die unter dem Kosten/Nutzen-Aspekt ganz sicher effektivste Methode, die Anwender eines Systems unterbrechungsfrei zu versorgen.

Gewarnt sei erneut vor einem menschlichen Effekt: Fehlalarme oder nichtssagende Meldungen stumpfen den Administrator ab und schaffen mittelbar die noch vor dem Fehlen von Sicherheit gefährlichste Situation – die Illusion von Sicherheit: „Kann gar nichts passieren, wir haben ja ein Monitoring."

07 Applikation

Die Applikation dient vorrangig einem Zweck, den sie gemäß ihrer Spezifikation erfüllen muss, und an dem wird sie gemessen. Leider ist aber die Unterstützung von Hochverfügbarkeit eines der oft vernachlässigten „Soft"-Features, die am Ende über den vollen Erfolg − oder Misserfolg − einer Lösung mitentscheiden. Um für den Betrieb in einer HA-Umgebung fit zu sein, sollte Software einige Mindestanforderungen erfüllen:

- Einfaches, vorhersehbares und transparentes Verhalten der (Netzwerk-) Kommunikation
- Robustes und selbstheilendes Error Handling. Zum Beispiel: abgebrochene Verbindungen automatisch wieder aufbauen, ohne blockierende Fehlermeldungen
- Bei feststehenden Kommunikationspartnern mehrere Ziele unterstützen und Strategie zur Zielauswahl implementieren und dokumentieren (wie Round Robin)
- Hoher Reifegrad, dadurch weniger Fehler
- Optimierter Leistungs-Footprint: Wer (unnötig) viele Ressourcen benötigt, fällt (unnötig) schnell aus, sobald diese einmal knapp werden

Die Implementierung weiterer Features wie die Unterstützung und Behandlung von Events, um auf Veränderungen der HA-Umgebung zu reagieren, sind meist herstellerspezifisch, bei richtiger Umsetzung jedoch sehr effizient.

08 Datenbank

Das relationale Datenbank-System muss für seine Anwender viele Versprechen einhalten, nicht zuletzt ACID. Hochverfügbarkeit ist ein weiterer Eintrag im Lastenheft; es stehen von Oracle und anderen renommierten Herstellern viele verschiedene Technologien zur Verfügung, um die diversen Szenarien abzudecken. Dazu zählen vorrangig:

- Konsistente Online-Backup-Mechanismen, um zur Datensicherung nicht abschalten zu müssen
- Überwachungsschnittstellen, um frühzeitig auf Engpässe oder Ausfälle aufmerksam zu machen
- Replikation, um Teilmengen von Daten logisch auf ein anderes System zu transportieren
- Standby-Datenbanken, um Datenbanken logisch oder physikalisch auf ein anderes System zu transportieren
- Cluster-Technologien, um ausfallende Komponenten automatisch zu ersetzen. Dabei unterscheiden sich die Produkte der großen Datenbank-Hersteller vor allem hinsichtlich möglicher Cache-Kohärenz und damit der Frage, ob alle Knoten gleichwertig Anfragen und Änderungen beantworten können.

09 Infrastruktur

Wo der Unterbau eines hochverfügbaren Systems beginnt, ist reine Definitionssache. In jedem Fall ist es natürlich sinnvoll, dort mindestens gleich hohe Verfügbarkeitsanforderungen zu stellen. Allerdings ist in der Regel eine technische Betrachtung des Gesamtpakets sinnvoll, um mögliche Beschränkungen von Vornherein zu erkennen.

Beim Netzwerk lohnt es sich beispielsweise, die Verfahren zum Load Balancing, Routing und NAT auf Lücken bezüglich

Oracle übernimmt DynDNS-Anbieter

Das amerikanische Unternehmen Dyn sorgt für dynamisches DNS (DynDNS), um Domains im Domain Name System (DNS) dynamisch zu aktualisieren. Dadurch kann ein PC oder ein Router nach dem Wechsel seiner IP-Adresse automatisch und schnell den dazugehörigen Domain-Eintrag einstellen. Mit dieser Technik ist der Rechner immer unter demselben Domain-Namen erreichbar, selbst wenn die aktuelle IP-Adresse für den Nutzer unbekannt ist.

Für Oracle ist der DNS-Betreiber eine sinnvolle Ergänzung für das Internet-as-a-Service- (IaaS) und Platform-as-a-Service-Portfolio (PaaS), wie Thomas Kurian, Präsident der Oracle-Produkt-Entwicklung in einer Pressemitteilung mitteilt. Über den Kaufpreis gibt es keine Angaben.

„Dyns immens skalierbares und globales DNS ist eine kritische Kernkomponente und eine natürliche Erweiterung unserer Cloud-Computing-Plattform", erklärt Kurian. Auch andere Cloud-Anbieter betreiben eigene DNS-Dienste. Dyn hat nach Angaben von Oracle etwa 3.500 Kunden, darunter große Unternehmen wie Netflix, Twitter, Pfizer und CNBC. Der DNS-Dienst wurde im Oktober dieses Jahres Opfer einer DDoS-Attacke, die mehrere Dienste lahmgelegt hat.

Weitere Informationen unter *https://www.oracle.com/corporate/acquisitions/dyn/index.html*

der Verfügbarkeitsplanung zu untersuchen und die HA-Funktionen des Netzes kennenzulernen. So brauchen Lösungen wie STP, BGP, OSPF oder EIGRP regelmäßig einige Zeit, bis das Netz nach Ausfällen wieder funktionsbereit ist und Pakete mit der erforderlichen Latenz und Qualität zur Verfügung stehen. Diese sogenannten „Konvergenzzeiten" von Routing- und Switching-Konzepten mit den angestrebten maximalen Ausfallzeiten der Applikation oder Datenbank zu vergleichen, ist wärmstens zu empfehlen.

Im Bereich „Massenspeicher" bietet der Markt eine nahezu unüberschaubare Fülle an hochverfügbaren SAN- und Storage-Lösungen. Wird bei einem Ausfall „zero data loss", also verlustfreies Weiterarbeiten gewünscht (was in der Regel der Fall sein dürfte), müssen Schreib-Vorgänge an allen Zielen angekommen sein, bevor der darauf aufbauende nächste Schritt beginnt. Damit kommen grundlegend zwei Architekturen in Betracht:

- *Stern*
  Server schreibt auf zwei oder mehrere Massenspeicher (Auswirkung auf Latenz: Langsamster Pfad definiert die Antwortzeit)
- *Kette*
  Server schreibt auf ein Storage-System und dieses repliziert auf ein weiteres etc. (Summe der Pfade definiert die Antwortzeit)

Hier definiert die Qualität der Integration zwischen Hardware-Lösung, Betriebssystem und HA-Software entscheidend die Eigenschaften des Gesamtsystems. Umschalt- oder Erholungszeiten nach Ausfällen und das Lastverhalten bei Schäden (wie Degraded Performance eines RAID- Arrays) sind sorgfältig zu betrachten, zu beeinflussen oder mindestens zu berücksichtigen.

10 Cloud

Die Cloud ist in aller Munde – und doch ist ein Cloud-Service nichts anderes als ein herkömmliches IT-System, das sich in der Hoheit eines anderen befindet und das idealerweise eine Form von Self-Service-Portal anbietet. In der Praxis ist damit der gesamte Technologie-Stack vom Metall bis zur Applikation inklusive Operating der Infrastruktur zuzurechnen. Betrachtet man nun die Cloud unter dem Aspekt der Hochverfügbarkeit, so ergibt sich die Notwendigkeit, die eigenen Anforderungen zunächst in Form von Service Level Agreements (SLAs) zu formulieren. Danach erst kann ein Cloud-Anbieter diese umsetzen und garantieren.

Auch rein technisch stellen sich Herausforderungen. So ist mindestens die Verfügbarkeit der Anbindung an den Cloud-Service zu prüfen: Wie hochverfügbar ist die Anbindung an Internet beziehungsweise Weiterverkehrsnetz, das die User mit dem Backend verbindet? Kein kleines Problem ist die sogenannte „letzte Meile" und die gegebenenfalls erforderliche Anbindung durch zwei oder mehrere Internet Service Provider.

Durch SLAs definierte, harte Schnittstellen zum Cloud-Service-Provider stellen sich in der Praxis oft als hinderlich heraus: Ist der Cloud-Service einmal nicht wie vereinbart verfügbar, erhält man den Schaden zwar (hoffentlich ohne Anwalt und Richter) ersetzt, „down" und zur Untätigkeit verurteilt ist man zunächst trotzdem. Verschiedene Cloud-Anbieter redundant zu nutzen, ist dahingehend die große Herausforderung, der sich Architekten und Planer zu stellen haben. Es ist für jeden Fall sorgfältig zu prüfen, ob der Dienst in der Cloud gut aufgehoben ist oder ob sich das geforderte Level der „End-to-end-Hochverfügbarkeit" nicht im eigenen Rechenzentrum („on premise") sicherer und kostengünstiger umsetzen lässt.

Martin Klier
martin.klier@performing-db.com

Korrektur für die letzte Ausgabe

In der letzten Ausgabe habe wir leider ein Autorenfoto falsch zugeordnet. Wir bitten das Versehen zu entschuldigen. Hier die beiden richtigen Fotos.

Seite 24

Simon Hahn
simon.hahn@opitz-consulting.de

Seite 36

Rainer Willems
rainer.willems@oracle.com