Link: https://www.computerwoche.de/a/virtualisierung-schafft-hochverfuegbarkeit,1889791

**Single Point of Failure beherrschen**

# Virtualisierung schafft Hochverfügbarkeit

**Datum:** 14.03.2009
**Autor(en):** Johann Baumeister

**Die Virtualisierung dient zur Konsolidierung der Server. Dabei werden mehrere Serversysteme zu einem zusammengefasst. Gleichzeitig entsteht jedoch zwangsläufig ein Single-Point-of-Failure. Dieser muss durch Techniken der Hochverfügbarkeit vermieden werden.**

Bei der **Virtualisierung von Serversystemen**[1] erfolgt eine Zusammenfasssung mehrerer physischer Rechner zu einem einzigen System. Statt beispielsweise zehn physische Server parallel zu betreiben werden die zehn Geräte in virtuellen Instanzen eines einzigen Servers emuliert. Dies erhöht die Auslastung der eingesetzten Hardwareressourcen. Die Möglichkeit dafür ergibt sich aus der Tatsache, das der Großteil der heute im Einsatz befindlichen Serversysteme nur eine geringe Auslastung aufweisen. Somit lassen sich mehrere Rechner in einem abbilden. In den virtuellen Instanzen der Rechner, wird dann das Betriebssystem mitsamt seinen Applikationen ausgeführt, geradeso, wie auf einem physischen Rechner der Fall wäre. Der eine physische Rechner wird somit zum Träger von mehreren Betriebssystemen und den darin aufbauenden Applikationsdiensten. Der Kostenvorteil entsteht durch den Parallelbetrieb mehrerer virtueller Maschinen auf einem physischen Server. Dieser Parallelbetrieb reduziert nicht nur den Bedarf für die Rechnerhardware, sondern senkt gleichzeitig die damit verbundenen infrastrukturellen Anforderungen an den Strombedarf, die Kühlung, den Platzbedarf oder an die Netzwerkanbindung.

Die Bedenken, die anfangs von den Kritikern geäußert wurden, sind durch die Verbesserungen in den Systemen ausgeräumt. Selbst die unternehmenskritischen Anwendungssysteme, die heute im Einsatz sind, wie beispielweise die **ERP-Linie von SAP**[2] oder **Oracle**[3], sind von deren Herstellern mittlerweile für den Betrieb in virtuellen Umgebungen freigegeben.

## Vermeidung des Single-Point-of-Failure

Dennoch **verbleibt ein Schwachpunkt**[4]. Dies ist die Abhängigkeit aller virtuellen Instanzen von dem physischen Hostsystem. Durch die Zusammenfassung wird der **Host zum Single-Point-of-Failure**[5]. Fällt der Host aus, so gilt das in der Folge auch für all seine virtuellen Gäste. Um das zu vermeiden, müssen virtuelle Infrastrukturen in jeden Fall auch hochverfügbar ausgelegt sein. Bei der Forderung nach der Hochverfügbarkeit gilt ferner, dass sie sich über alle Komponenten erstrecken muss, denn für den betroffenen Benutzer oder Geschäftsprozess spielt es keine Rolle was letztendlich die Ursache für den Ausfall oder die Engpass ist.

## Redundante Systeme ermöglichen Hochverfügbarkeit

Um diese Hochverfügbarkeit bereitstellen zu können, haben sich in der Vergangenheit unterschiedliche Techniken etabliert. Sie reichen von der Absicherung durch Backup/Restore-Verfahren bis hin zum Einsatz redundanter Systeme. Die dabei begleitenden Verfahren werden auch mit den Begriffen wie **Business Continuity**[6] oder **Disaster Recovery**[7] umschrieben. Wenngleich die verwendeten Verfahren eine unterschiedliche Qualität der Absicherung ermöglichen, so verfolgen sie dennoch alle das gleiche Ziel: den Dienst des Servers möglichst am Laufen zu halten oder im Fehlerfall schnell wieder herzustellen. Aber auch wenn es nicht zum finalen GAU, dem Totalausfall des Servers kommt, so wirkt sich das "Host-Befinden" immer auf seine virtuellen Gäste aus. Jede Beeinträchtigung des Hostsystems, sei es durch einen Engpass bei der Speicherzuordnung, der Netzwerkanbindung oder dem Zugriff auf die Plattensysteme wirkt sich immer auf alle virtuellen Gäste gleichzeitig aus. Dies ist deswegen gegeben, da sich bei der Virtualisierung alle virtuellen Gäste die Ressourcen des Hostsystems teilen müssen. Eine feste Zuordnung oder Reservierung von bestimmten Ressourcen zu den Gästen ist in den meisten Fällen nicht vorgesehen. Dies wäre vereinzelt zwar machbar, untergräbt dann aber wieder die Vorteile der Virtualisierung.

## Hochverfügbarkeit durch dynamische Ressourcen-Zuweisung

Der Einsatz von Virtualisierungstechniken führt somit zu zwei zentralen Forderungen:

- Ressourcen müssen dynamisch an die Serverdienste, die diese Ressourcen benötigen, zugewiesen werden können. Dies wird zum Beispiel durch die Tools des **HP Virtual Server Environment**[8] (VSE) sichergestellt.

- Ausfallsicherheit wird bei der Virtualisierung zum Muss: Durch die Zusammenfasssung mehrerer Systeme in eines entsteht ein Single-Point-of-Failure. Um dessen Ausfall abfedern zu können, müssen die Systeme hochverfügbar ausgelegt werden, ansonsten multiplizieren sich die Risiken mit der Konsolidierungsrate.

Um den erwähnten Anforderungen zu genügen hat HP seiner Serverreihe konsequent auf die **Forderungen nach Ausfallsicherheit**[9] ausgelegt. Dies beginnt beim Prozessor und der Absicherung der elementaren Baugruppen, setzt sich fort im Design und Aufbau der Rechner-Boards und endet schließlich bei der Absicherung der Serverschränke. Aus dem Blickwinkel der Server bietet **HP**[10] dazu zwei zentrale Varianten:

## Zweifache Absicherung sorgt für immerwährenden Betrieb

**Integrity NonStop:** Bei den Serversystemen der **Integrity NonStop**[11] Reihe sind sämtliche Serverkomponenten redundant ausgelegt. Diese Systeme bieten eine bestmögliche Absicherung gegen Hardwareausfälle. Die Absicherung umfasst alle aktiven Rechnerbaugruppen, aber auch der passiven Bussysteme und der Backplane. In der Speicherkonfiguration des Dual Modular Redundancy (DMR) sind alle Speicherbaugruppen doppelt vorhanden. Eingeschlossen in die Absicherung sind ferner die Stromversorgung und die Kühlung der Systeme. Desweiteren unterliegt auch die Anbindung an das Netzwerk und den Speicher der Absicherung. Die Integrity NonStop Systeme bieten damit das Maximum an Hochverfügbarkeit, das mit vertretbaren technischen Mitteln heute zu erzielen ist. Die doppelte Auslegung aller Baugruppen federt den Ausfall einer beliebigen Hardwarebaugruppe ab. Defekte Baugruppen sind dabei im laufenden Betrieb zu tauschen (hot-swapable). Damit wird eine kontrollierte Downtime des gesamten Systems verhindert. Fällt dennoch eine Baugruppe aus, so steht sie ab diesem Moment nicht mehr zur Absicherung eines Ausfalls zur Verfügung. Bis zum Tausch dieser Baugruppe ist folglich die Ausfallsicherheit nicht mehr gewährleistet. Wer auch dieses Risiko absichern muss, für den liefert HP mit der **Triple Modular Redundancy (TMR)** [12] eine Variante mit doppelter Redundanz. Damit besteht auch nach dem Ausfall einer Baugruppe eine weitere Absicherung, da weiterhin die Redundanz durch doppelte Systeme gewährleistet ist. Zusammenfassend ist festzustellen, dass das Design aber auch die Implementierung dieser Serversysteme ein Höchstmaß an Ausfallsicherheit bietet.

**Integrity:** Bei nicht ganz so hohen Anforderungen nach Ausfallsicherheit kommen die Rechnersysteme der Integrity Serie zum Einsatz. Bei diesem Modell erfolgt die Absicherung gegen einen möglichen Ausfall durch die Bereitstellung eines Failover-Clusters. Die Knoten dieses **Cluster**[13] sind in unterschiedlichen Varianten beliebig zu platzieren. Unterstützt durch die Verwaltungstools des VSE erlaubt die Konfiguration des Cluster eine räumlich enge oder auch sehr weit entfernte Absicherung.

Werden die beiden Knoten beispielsweise auf zwei Cellboards in einem Gehäuse (Enclosure) eingerichtet, so übernehmen die Cellboard die Funktionen des jeweils anderen Boards bei einem Ausfall. Diese Clusterkonfiguration schützt somit gegen den Ausfall eines **Cellboards,**[14] nicht aber gegen den Ausfall des gesamten Enclusores.

Um auch größere Entfernung und den Ausfall des Enclosures abzusichern werden die Knoten des Cluster auf unterschiedliche Enclosures gelegt. Beim Campus- oder Metrocluster beispielweise kann die Distanz der Cellboards einige Dutzend Kilometer betragen. Metro-Cluster schützen folglich vor einem lokal begrenzten Ausfall des Systems und führen den Serverbetrieb an einem entfernten Standort fort.

Wenn noch größerer Entfernungen überbrückt werden müssen, um beispielsweise auch gegen lokal begrenzter Naturkatastrophen abgesichert zu sein, so kommen die Continental Cluster ins Geschehen. Sie erlauben eine weltumspannende **Absicherung der Serverdienste**[15] gegen Ausfall. Die Knoten eines Continental Cluster sind räumlich beliebig weit zu trennen. Sie stimmen sich über Standard-IP-Netze und einer Internetverbindung ab.

Diese unterschiedlichen Varianten der Integrity-Cluster und die Redundanzen der Integrity NonStop Server erlauben vielfältige Absicherungen gegen Ausfälle. Dabei erfolgt die Absicherung der Serversysteme im Ganzen. Aber auch die einzelnen Baugruppen sind dabei den Integrity-Systemen gegen Ausfälle gewappnet. Dies beginnt bei Rechnerdesign, geht über die Auswahl der Baugruppen und setzt sich in den passiven Komponenten, wie etwa den Bussystemen fort. Dabei sind sowohl die **CPUs**[16], die Speicherbausteine, die IO-Anschlüsse und auch Stromversorgung und Kühlung redundant ausgelegt.

## Sicherheit in allen Baugruppen

**CPU:** Je nach Konfiguration des Rechnersystems werden unterschiedliche Cellboards mit mehreren **Intel Itanium-CPUs**[17] verwendet. Dabei lassen sich die CPUs dynamisch zu- und abschalten. Dies ermöglicht die geforderte Flexibilität und Dynamik. Gleichzeitig wird damit der Ausfall einer CPU abgesichert. In ihrem Innersten weisen die Prozessoren der Intel Itanium-Reihe darüberhinaus eigene Vorkehrungen zur Fehlerkorrektur auf. Datenfehler werden von der CPU selbst erkannt. Daneben ist auch der 24 MByte Cache der CPU mit einer Fehlererkennung nach dem ECC-Verfahren abgesichert.

**Arbeitsspeicher:** Neben der **CPU zählt der Arbeitsspeicher zu den wichtigsten Bausteinen**[18] für die Codeabarbeitung. Auch er ist gegen Ausfälle und Fehler abgesichert. Dies passiert durch die Fehlererkennung und -korrektur nach dem ECC-Verfahren. Desweiteren befinden sich auf jedem der Speichermodule zwei zusätzliche Ersatzchips. Diese können bei einem Ausfall von bis zu zwei primären Speicherchips dynamisch dazu geschaltet werden und die Rolle der defekten Bausteine einnehmen. Laut Messungen vermindert dies die Downtime für das System um den Faktor 17.

**Die Bussysteme:** Die **Bussysteme**[19] dienen zur Übertragung der Informationen zwischen den Baugruppen des Rechners. Um auch sie gegen Ausfälle zu wappnen setzt man meist auf Parity-Bits. HP hat diese Logik zur Fehlerkorrektur auf den Adressbus ausgedehnt und vermeidet damit fehlerhafte Adressen im System. Die Absicherung des IO-Busses, der zur Kommunikation mit den Ein-/Ausgabe-Baugruppen verwendet wird, erfolgt durch Dualpath-IO. Ferner lassen sich die Netzwerkschnittstellen dynamisch an die logischen Server binden. Hinsichtlich der Netzwerkschnittstelle sorgen somit diese beiden Vorkehrungen für die geforderte Ausfallsicherheit der IO-Baugruppen. Die IO-Baugruppen selbst sind ohnehin mehrfach vorhanden. Die Kommunikation mit den sonstigen Erweiterungsmodulen erfolgt durch spezielle Bussysteme wie etwa **PCI-X**[20] oder PCI-E (Peripheral Component Interconnect eXtended/Express). Auch diese Busse sind durch entsprechende Vorkehrungen gegen Störungen gesichert. Die integrierte Fehlerkorrektur reduziert die Fehlerrate und steigert gleichzeitig die die Verfügbarkeit um den Faktor 20.

**Backplane und Stromversorgung:** Eine zentrale Rolle nimmt ferner die Backplane und natürlich die Stromversorgung ein. Beides ist in den Integrity Rechner durch Erweiterungen abgesichert. Die Crossbar Fabric-Backplane sorgt darüberhinaus für eine Trennung der physischen Rechner-Partitionen. Damit wirken sich Fehler in einzelnen Partitionen nicht auf benachbarte Baugruppen aus.

## Fazit:

Virtualisierung bringt viele Server auf einen. Dessen Bedeutung steigt mit jeder weiteren virtuellen Maschine. Fällt der Host aus, so zeiht er alle Gäste in den Abgrund. Daher kommt der Ausfallsicherheit eine immense Bedeutung bei. HP hat die Integrity-Reihe konsequent auf die **Anforderungen der Ausfallsicherheit getrimmt**[21]. Dies reicht von der Absicherung gegen den Ausfall einzelner Komponenten, bis hin zur Absicherung von Boards und endet schließlich bei den Vorkehrungen gegen den Ausfall bei regionalen Katastrophen durch Failover-Cluster. Die Schutzkonzepte greifen dabei nahtlos ineinander und passen sich ohne Anpassungen in die vorhandenen Softwaredesigns und IT-Betriebsszenarien ein.

## Links im Artikel:

[1] **https://www.computerwoche.de/virtualdatacenter/connectivity-und-storage/news/1867771/**
[2] **http://www.sap.com/germany/solutions/business-suite/erp/index.epx**
[3] **https://www.cio.de/news/cionachrichten/858812/**
[4] **https://www.computerwoche.de/virtualdatacenter/sicherheit/expertenwissen/1864340/**
[5] **https://www.computerwoche.de/knowledge_center/virtualisierung/1885498/index2.html**
[6] **http://en.wikipedia.org/wiki/Business_continuity_planning**
[7] **http://de.wikipedia.org/wiki/Disaster_Recovery**
[8] **http://h71028.www7.hp.com/enterprise/cache/258348-0-0-82-150.html**
[9] **http://whitepaper.computerwoche.de/index.cfm?pid=1&pk=2783**
[10] **http://welcome.hp.com/gms/de/de/companyinfo/index.html**
[11] **http://h20341.www2.hp.com/integrity/cache/415174-0-0-82-150.html**
[12] **http://en.wikipedia.org/wiki/Triple_modular_redundancy**
[13] **http://de.wikipedia.org/wiki/Computercluster**
[14] **https://www.computerwoche.de/knowledge_center/virtualisierung/1885498/index5.html**
[15] **https://www.computerwoche.de/knowledge_center/open_source/165921/index2.html**
[16] **https://www.computerwoche.de/knowledge_center/mobile_wireless/1888903/**
[17] **http://www.intel.com/cd/products/services/emea/deu/processors/itanium/373614.htm**
[18] **https://www.computerwoche.de/virtualdatacenter/server/expertenwissen/1876330/**
[19] **https://www.computerwoche.de/heftarchiv/2005/6/1050423/**
[20] **http://en.wikipedia.org/wiki/PCI-X**
[21] **http://whitepaper.computerwoche.de/index.cfm?pid=1&pk=2783**