

Link: <https://www.computerwoche.de/a/warum-virtualisierung-hochverfuegbarkeit-verlangt,2353894>

## Gefährlicher Trugschluss

### Warum Virtualisierung Hochverfügbarkeit verlangt

Datum: 10.12.2010  
Autor(en): Klaus Manhart

**Immer mehr Unternehmen betreiben auch unternehmenskritische Applikationen auf virtualisierten Systemen. Stillschweigend wird dabei oft vorausgesetzt, dass die Virtualisierung auch die Verfügbarkeit garantiert. Doch das ist ein gefährlicher Trugschluss.**

Virtualisierung hat die Unternehmens-IT in den letzten Jahren gewaltig verändert. Und das aus gutem Grund: Virtualisierte IT-Strukturen reduzieren die Hardware-Ressourcen und führen zu einer besseren Auslastung von Server- und Storage-Systemen. Gleichzeitig erhöht dies die Flexibilität, senkt den Platz- und Energiebedarf und verringert so ganz allgemein die IT-Kosten.

## Downtime is increasing dramatically – but why?



From 2005 to 2008:

- Downtime per month: up 69%
- Cost per hour: tripled

Why?

- More complexity
- Increased dependency of revenue on IT

Source: *Dataquest Insight: Unplanned Downtime Rising for Mission-Critical Applications*, Gartner Dataquest, ID G00161629, October 2008

Downtimes haben zwischen 2005 und 2008 nach einer Gartner-Studie dramatisch zugenommen.

Foto: Gartner

Mit der zunehmenden Virtualisierung entstehen allerdings auch neue Gefahren. Viele Nutzer glauben, dass eine virtualisierte IT-Lösung automatisch Hochverfügbarkeit garantiert. In einer **aktuellen Studie von Stratus**<sup>1</sup> zusammen mit dem Marktforschungsunternehmen ITIC waren 79 Prozent der befragten IT-Experten überzeugt, dass Virtualisierungssoftware die für kritische Anwendungen nötige Verfügbarkeit bereitstellen kann. Doch das ist ein gefährlicher Trugschluss. Tatsächlich ist Virtualisierungssoftware nicht für die Herstellung von Hochverfügbarkeit konzipiert. Die Gefahr von Ausfällen kann sie keinesfalls reduzieren - im Gegenteil, sie nimmt sogar zu. Der größte Schwachpunkt der Virtualisierung ist die Abhängigkeit der virtuellen Instanzen von der Hardware, die damit zum Single Point of Failure wird. War in Vor-Virtualisierungszeiten der Ausfall eines Servers verkraftbar, kann dies nun, wenn mehrere Applikationen auf einem System laufen, kritisch werden. Dies umso mehr, wenn unternehmenskritische Anwendungen auf einer Hardware betrieben werden.

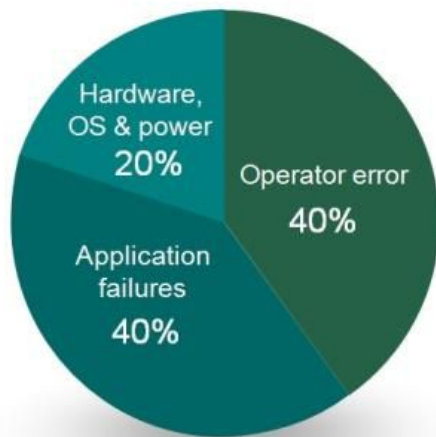
## **Risikospiegel vermeiden**

Ein konkretes Beispiel ist die Migration virtueller Maschinen in Echtzeit während des laufenden Betriebs von einem physischen Server zu einem anderen -wie sie heute häufig praktiziert wird. Damit das reibungslos funktioniert müssen sowohl Quell- als auch Zielsystem stabil laufen. Gibt es bei einem der Systeme Probleme oder fällt eines aus, kann auch die Anwendung ausfallen.

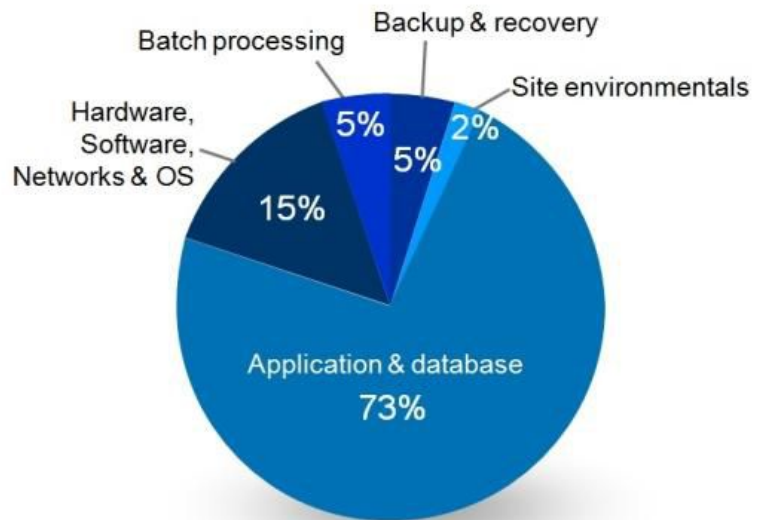
Um Ausfälle zu vermeiden, sollten virtuelle Systeme grundsätzlich hochverfügbar ausgelegt sein. In mission-kritischen Umgebungen wird aus dem Soll ein Muss: Hochverfügbarkeit ist in sensiblen Bereichen Grundvoraussetzung für den Einsatz von virtuellen Infrastrukturen. Ohne Hochverfügbarkeit wird die Virtualisierung zum Vabanquespiel.

Bei HP ist die Kombination und Integration von Virtualisierung und Hochverfügbarkeit von Anfang an elementarer Bestandteil der IT-Philosophie. Mission-kritische HP-Systeme sind so ausgelegt, dass eine grundlegende Hochverfügbarkeit gewährleistet ist. Dies beginnt bei den Bussystemen, setzt sich fort in den Speicherbausteinen, der CPU, den IO-Kanälen und endet bei Stromversorgung und Lüftung.

# What causes the most downtime?



Causes of unplanned downtime



Causes of planned downtime

Source: *Best Practices for Continuous Application Availability*, Gartner Data Center Conference 2008

Mögliche Ursachen für geplante und ungeplante Ausfallzeiten nach Gartner.

Foto: Gartner

Um eine umfassende Absicherung gegen jegliche Ausfälle der elementaren Baugruppen zu vermeiden, hat HP zusätzlich den gesamten Aufbau der Integrity-Superdome2-Server redundant ausgelegt. Die wichtigen Komponenten sind doppelt vorhanden, der Ausfall eines Bauteils wird durch das zweite aufgefangen. Ergänzt wird die hardware-seitige Hochverfügbarkeitsbasis um Hochverfügbarkeitsfeatures des HP-Standard-Betriebssystems HP-UX.

## Failover Cluster und Instant Capacity

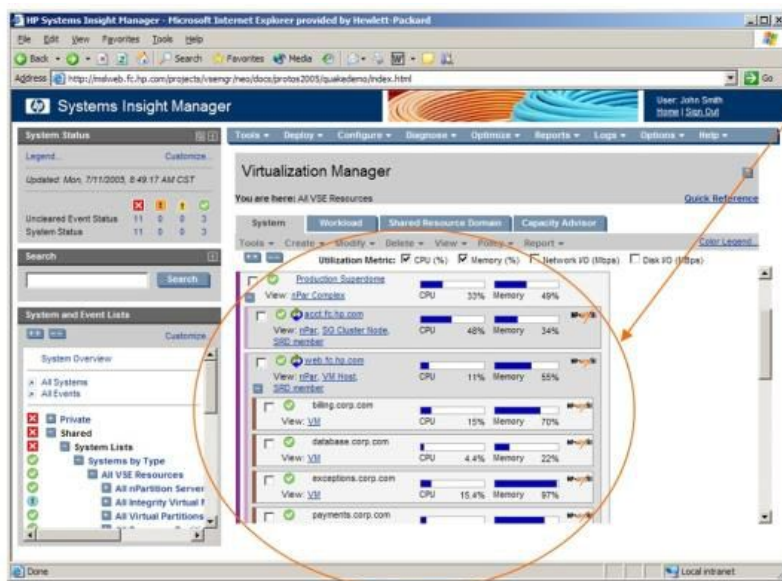
Sollte doch einmal der Katastrophenfall eintreten und ein Server oder anderes System ausfallen, sichern Failover-Cluster den Worst Case ab. Dabei übernimmt bei einer Server-Störung automatisch ein zweiter Rechner dessen Aufgaben. Die Clusterknoten können dabei beliebig platziert sein. Beim Campus- oder Metrocluster kann die Entfernung der Rechner einige Dutzend Kilometer betragen und damit vor einem lokal begrenzten Ausfall des Systems schützen. Durch Continental Cluster ist diese Absicherung sogar weltumspannend möglich. Sie basieren auf den Standard-IP-Netzen und haben somit keine räumliche Begrenzung mehr.

Zur Verwaltung der Cluster steht mit **ServiceGuard**<sup>2</sup> eine seit Jahren bewährte Cluster-Software bereit. Mit ihr lassen sich nicht nur ganze Server im Clusterverbund von A nach B schieben, sondern auch einzelne Applikationen. Der Vorteil: Lasten können granular so besser verteilt werden. Damit entfällt die Notwendigkeit, für den Krisenfall einen ganzen Server ähnlicher Leistungsklasse bereit zu stellen wie den zu sichernden Server. Stattdessen können die Applikationen - und damit die Last - im Krisenfall bei Serverausfall kostengünstig und granular auf mehrere, ohnehin betriebene Server verteilt werden.

Zur Absicherung lassen sich auch bevorratete Ressourcen nutzen, die im Normalfall gar nicht aktiv sind und die der Kunde zunächst nicht bezahlt. **Instant Capacity**<sup>3</sup> Systeme enthalten beispielsweise Prozessoren, die der Anwender im Normalfall weder verwendet noch bezahlt. Erst im Bedarfsfall werden sie aktiviert und abgerechnet. Solche Instant Capacity Systeme lassen sich auch im Krisenfall automatisch aktivieren, um dann deren Leistung zu nutzen und mehr Ressourcen zur Verfügung zu haben - und dann sogar ohne dafür anfallende Kosten.

## Integrierte Hochverfügbarkeit

All diese Sicherungsmechanismen sind integriert in die von HP angebotenen Virtualisierungslösungen. Die einzelnen Schutzkonzepte greifen nahtlos ineinander über. Von der Hard Partition über virtuelle Partitionen bis hin zu **Integrity Virtual Machines**<sup>4</sup> sind alle Technologien in der Lage, mit einem Cluster oder dem Instant Capacity umzugehen.



- Discovery, visualization, and configuration of virtual resources/workloads and their utilization
  - HP Integrity servers
    - nPars (and standalone servers)
    - Virtual Partitions
    - Integrity Virtual Machines
    - gWLM groups
    - Resource Partitions
    - Serviceguard clusters
    - Groups of virtual resources (Shared Resource Domains)
- Single click drill down capability

Das Hinzufügen von Hochverfügbarkeitsmanagement und die Integration in das Virtualisierungsmanagement ist nur ein zusätzliches Menü im Systems Insight Manager.

Gleichzeitig arbeiten all diese beschriebenen Mechanismen transparent im Hintergrund und erfordern keine Änderung im Softwaredesign oder Betriebssystem. Der Aufwand für die Implementierung ist minimal. Ist in einem Server ohnehin schon ein Infrastruktur-Management vorhanden, ist das Hinzufügen von Hochverfügbarkeitsmanagement und die Integration in das Virtualisierungsmanagement nur ein zusätzliches Menü im Systems Insight Manager. Durch die Integration der Komponenten mit dem **Systems Insight Manager**<sup>5</sup> und dem Virtual Server Environment (VSE) wird somit die Hochverfügbarkeit zum Stützpfiler der Virtualisierung. Eine solche Integration von Hochverfügbarkeit und Virtualisierung erlaubt es, mission-critical Applikationen ruhigen Gewissens in einer virtualisierten Umgebung laufen zu lassen. Statt Anwendungen entweder virtualisiert oder hochverfügbar zu betreiben, ist über die Integration beides möglich - und das granular als ganzer Server, virtuelle Maschinen oder Applikation.

## Links im Artikel:

<sup>1</sup> <http://www.de.stratus.com/press/20100611.htm>

<sup>2</sup> <http://docs.hp.com/de/5991-1231/ch05s09.html>

<sup>3</sup> <http://docs.hp.com/de/B9073-90197/ch01s01.html>

<sup>4</sup> [http://h71028.www7.hp.com/enterprise/us/en/os/hpux11i-partitioning-integrity-vm.html?jumpid=reg\\_R1002\\_USEN](http://h71028.www7.hp.com/enterprise/us/en/os/hpux11i-partitioning-integrity-vm.html?jumpid=reg_R1002_USEN)

<sup>5</sup> <http://docs.hp.com/de/5991-1231/ch05s12.html>

IDG Tech Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.