

**Berufsschule Wiesau**

**"Hope is not a strategy"**  
**IT-Hochverfügbarkeit in Theorie und Praxis**

Martin Klier, DBA  
10.03.2008



# 1. Überblick

## *1.1. Agenda*

## *1.2. Vorstellung Referent*

- Martin Klier, 28
- Linux- und Datenbankadministrator
- Schwerpunkt hochverfügbare Systeme, Cluster und Replikation
- Arbeitgeber: A.T.U Weiden (<http://www.atu.eu>)
- Linux seit 1997
- Oracle Database seit 2003
- Kontakt: [martin.klier@unix.net](mailto:martin.klier@unix.net)
- Web: <http://www.usn-it.de>

## *1.3. Do you speak English?*

Die meisten Begriffe aus dem IT-Umfeld entstammen der englischen Sprache, oft gibt es keine aussagekräftigen deutschen Entsprechungen. Dieses Handout liefert für diese Begriffe eine deutsche Erklärung mit, verzichtet aber bewußt nicht auf ihren Einsatz. Englisch ist "wie für den Mediziner das Latein" die internationale Fachsprache der IT.

## 2. Einführung

### 2.1. Was ist "Hochverfügbarkeit"?

„Ein System gilt als hochverfügbar, wenn eine Anwendung auch im Fehlerfall weiterhin verfügbar ist und ohne unmittelbaren menschlichen Eingriff weiter genutzt werden kann. In der Konsequenz heißt dies, dass der Anwender keine oder nur eine kurze Unterbrechung wahrnimmt. Hochverfügbarkeit (abgekürzt auch HA, abgeleitet von engl. High Availability) bezeichnet also die Fähigkeit eines Systems, bei Ausfall einer seiner Komponenten einen uneingeschränkten Betrieb zu gewährleisten.“ (Andrea Held)

a) Als theoretischer Ansatz errechnet sie sich wie folgt:

$$\text{Verfügbarkeit} = \frac{\text{Uptime}}{\text{Downtime} + \text{Uptime}}$$

b) Übersicht zu gerne genannten Prozentwerten, errechnet mit der obigen Formel:

Prozentwert d.V.	Ausfallzeit pro Monat	Ausfallzeit pro Jahr
99,9	43,8 Minuten	8,76 Stunden
99,99	4,38 Minuten	52,6 Minuten
99,999	26,3 Sekunden	5,26 Minuten

Quelle: Wikipedia

### 2.2. Bedarf an HA-Lösungen

Viele Unternehmen, Behörden und Organisationen benötigen informationstechnische Systeme, die jederzeit zur Verfügung stehen, jedoch für völlig unterschiedliche Zwecke. Die IT-Anlagen müssen daher durch Spezialisierung eine breite Palette an Möglichkeiten bedienen. Man denke beispielsweise an:

- a) Banken (Zinsgewinne)
- b) Börsen (Kursschwankungen)
- c) Flugverkehr und Raumfahrt (Sicherheit)
- d) Handel (Erreichbarkeit für den Kunden)
- e) Industrie (Fertigung just in sequence / just in time)
- f) Militär (Robustheit)

## 3. Risiken für die Verfügbarkeit

### 3.1. Überblick

- a) Menschliche Fehler
- b) Technische Ausfälle
- c) Konzeptionelle Schwächen
- d) Katastrophen

### 3.2. Logische Korruption

durch Entfernen, Manipulieren und/oder Hinzufügen von Daten oder Datenfragmenten. Diese Fehler müssen nicht zwangsläufig schon zur Entstehungszeit auffallen, ihre Entdeckung kann sich unbegrenzt verzögern.

- a) Softwarefehler
  - Betriebssystem, Kernel, Gerätetreiber
  - Datenbank, Dateien
  - "undichte" Applikationslogik
  - Viren
- b) Benutzerfehler
  - Widrige Umstände, Irrtum, Fahrlässigkeit
  - Ausbildungsmängel
  - Absicht
- c) Administratorfehler  
Wie Benutzerfehler, aber in der Regel durch die weitreichenderen Berechtigungen gravierender. Ggf. ist zusätzlich eine direkte Einwirkung auf Hardware im RZ möglich.
- d) Auswirkungen Hardwareschaden  
Recht selten, aber sehr schwer zu finden und nachzustellen. Die gängigsten Vertreter sind RAM-Korruption und controllerseitige Schreibfehler auf die Massenspeicher.

### 3.3. Schäden an Infrastruktur bzw. Standort

- a) Umbauschäden
  - Krafteinwirkung
  - Lockerung der Verkabelung
  - Trittschäden
  - Staub
  - Störung der Luftzirkulation, hohe Temperatur
  - fehlgeleitete Abschaltung

## b) Stromausfall

- externes Stromnetz
- Über- / Unterspannung
- Überlastung Unterverteilung / Fehlerstrom-Schutzschalter (FI)
- Fehler in USV und / oder Notstromaggregat
- schadhafte Verkabelung

## c) Ausfall Klimatisierung

- u. U. Nebenwirkung von Stromausfall (Wiederanlaufschutz etc.)
- Totalstörung bei Wartung
- Wartungsdefizit

## d) Brand und Brandbekämpfung

- Feuer im RZ
- Kabelbrand
- Löschmitteleinsatz (Schaum, Pulver, CO<sup>2</sup>, Wasser)

## e) Gas- oder Wasserschaden

- Rohrbruch
- Sprinkler- bzw. Löschanlage
- Getränke(!)

### **3.4. Hardwarefehler**

## a) Rechnersystem

- Kernkomponenten
- RAM
- IO-Controller / Bootmedium
- Netzwerkinterface(s)
- Spannungsversorgung und -schalter

## b) Netzwerk, SAN

- Ausfall der Verbindung zwischen Standorten
- Internetanbindung / Last Mile (Baggerschaden)
- Komponentenausfall im / am RZ
- Störung Firewall / IDS / IPS

## c) Massenspeicher, Storage-Subsystem

- Festplatten-Lebensdauer
- Controller-Schäden
- SAN Zoning-Probleme, fehlerhaftes Zoning, z.B. beim Hinzufügen von Komponenten

### **3.5. Angriff (off topic)**

- a) Denial of Service
  - Überlastung von außen
  - Eindringen + gezielte Beschädigung
- b) Kollateralschaden
  - Übernahme(versuch)
  - Ausspähung oder Manipulation "mit Nebenwirkungen"
- c) physischer Diebstahl / Sabotage

## 4. Vorsorgemaßnahmen

- a) Bereitstellung von ausreichenden finanziellen Mitteln
- b) Gute Schulung der Mitarbeiter (Benutzer, Softwareentwickler und Administratoren)
- c) Erstellung eines rundum gesicherten HA-Konzeptes
- d) Auswahl von qualitativ hochwertigen Einzelkomponenten
  - Enterprise-Level-Geräte mit Supportvertrag und Zertifizierung für die eingesetzte Software
  - Markenhersteller (sehr gute Ausnahmen möglich, prüfen!)
  - Einheitliche Produktlinien (spezifisches Wissen der Administratoren aufbauen)
- e) Sorgfältige Realisierung
- f) Detaillierte Tests vor Inbetriebnahme
- g) Absolut zuverlässige Durchführung der notwendigen Backups und deren Prüfung
- h) Regelmäßige Disaster-Übungen und routinemäßige Umschaltungen
- i) Proaktives Operating im Betrieb, v. a. durch automatische Fehlererkennung und -meldung
- j) Change Management und Prozessdefinition

Die meisten menschlichen Fehler werden bei schnellen Änderungen (inklusive Ad-Hoc-Planungen, z.B. für Ersatzteilbeschaffung oder Technikereinsatz) gemacht. Ein geordneter, schriftlich fixierter, aber nicht überbürokratisierter Ablauf bündelt alle Aktivitäten. Er benennt einen einzelnen "taktisch" entscheidungsbefugten Verantwortlichen für eine Maßnahme - auch wenn diese dann in einem Team durchgeführt wird.

Das Change Management erfasst vorab Änderungswünsche oder -notwendigkeiten, klärt die Zuständigkeit und listet vorab die durchzuführenden Arbeitsschritte und ihre vorab abschätzbaren Implikationen auf. Alle durchzuführenden Maßnahmen werden priorisiert und in Reihenfolge gebracht.

## 5. Beispielprojekt "Großer Webshop"

Anforderung: Das gesamte System soll gegen Ausfälle aller Art geschützt werden.

### 5.1. Grundplanung

- a) Clustering gegen Defekte (ggf. auch zur Skalierung)
- b) Replikation gegen Defekte
- c) Verzögerte Replikation oder/und Reset-Technologien gegen logische Korruption
- d) Das richtige Backup zur richtigen Zeit
- e) Aktives Sicherheitskonzept
- f) Möglichst ähnliches Testsystem, es soll alle Ebenen umfassen
- g) Prozess für Produktivsetzung von Changes (Mehrschichtiges Verfahren, Umweg über Testsystem(e))

### 5.2. Infrastruktur

- a) Verteilung auf zwei oder mehrere Rechenzentren
  - Online-USV mit Überbrückungsschalter
  - Notstromaggregat
  - Anbindung über verschiedene Internetknoten (Providerdiversifikation) und Trassen
  - Zwei getrennte Zwischenverbindungen der RZ
- b) Redundante Verkabelung für Strom (auch Unterverteilungen!), SAN, Netzwerk
- c) Doppelte Auslegung von Netzwerk- und FibreChannel-Architekturen

### 5.3. Hardware

- a) Server
  - 2 Netzteile
  - min. 2 NICs mit Bondingtechnologie
  - Redundante FibreChannel-HBAs
  - Boot-from-SAN oder Boot von RAID1
  - Hotplugging-Technologie
  - Reserve-BIOS-ROM
  - Firmwareupgrade im Betrieb möglich
  - z.B. HP ProLiant DL385 und DL585G2, HP C-Class Blades, IBM x3950
- b) Storage
  - Randbedingungen wie Server

- RAID 6 oder 10
  - z.B. IBM DS4800, DS8000, HP StorageWorks Enterprise Virtual Array 8000
  - Alternativ z.B. mehrere Infotrend F16F-R4031 oder vergleichbar + redundanter Raid Controller Head
- c) Netzwerktechnik
- Loadbalancer einsetzen, z.B. Cisco CSS 1150x oder Catalyst 6500 CSSM/SSL in mehrfacher Ausführung
  - kaskadierte Firewall mehrerer Hersteller, z.B. Cisco ASA / Catalyst + FWSM und Juniper SSG / NetScreen

#### **5.4. Software**

- a) Zertifizierung für eingesetztes Betriebssystem und für Schnittstellen beachten
- b) OS z.B. SuSE Linux Enterprise Server9 SP4 oder Solaris 10
- c) Clusterware z.B. Oracle OCW 10gR2, SunCluster oder Symantec Veritas CS
- d) DB z.B. Oracle Database 10gR2 (aktuell max. 10.2.0.4) oder IBM DB2
- e) Webserver Apache2 + Zend Core

#### **5.5. Zeichnung**

<bitte Tafelbild anfügen>