Wege zur Hochverfügbarkeit

Christian Affolter
High Availability
08. Mai 2015

Übersicht

- Weshalb Hochverfügbarkeit?
- Was ist Hochverfügbarkeit?
- Wege / Prinzipien / Konkrete Ansätze
- Herausforderungen und Erfolgsfaktoren
- Fragen / Diskussion

stepping stone

Weshalb Hochverfügbarkeit?

existenzielle Abhängigkeit von IT

Quelle: http://medienbewusst.de

stepping stone

Was ist Verfügbarkeit?

- *Eine Bereitschaft oder das Vorhandensein einer Betrachtungseinheit*
- Betrachtungseinheit?
  - Einzelne Komponente
  - Service (Server, Cluster, Netzwerk etc.)

und was Hochverfügbarkeit?

- *Verfügbarkeit mit einer (sehr) „hohen“ Wahrscheinlichkeit*
  - Zuverlässigkeit/Verlässlichkeit, Funktionsfähigkeit, Ausfallsicherheit
- „Garantiert immer verfügbar“ gibt es nicht

Wann gilt etwas als Hochverfügbar?

- Verfügbarkeit wird meist in **Prozent der Erreichbarkeit** (Availability) über eine **bestimmte Zeitdauer** angegeben
- Hochverfügbar ab 99.95%, 99.99%

stepping stone

Von ganz vielen Neunen

Verfügbarkeit in %	Max. Ausfallzeit pro Jahr	Max. Ausfallzeit pro Monat	Verfügbarkeitsklasse
90% *eine Neun*	36.5 Tage	72 Stunden	
95%	18.25 Tage	36 Stunden	
99% *zwei Neunen*	3.65 Tage	7.2 Stunden	Stabil / normal verfügbar
99.9% *drei Neunen*	8.76 Stunden	43.8 Minuten	Erhöht verfügbar
99.95%	4.38 Stunden	21.56 Minuten	
99.99% *vier Neunen*	52.56 Minuten	4.38 Minuten	Hochverfügbar
99.999% *fünf Neunen*	5.26 Minuten	25.9 Sekunden	Höchstverfügbar / fehlerunempfindlich
99.9999% *sechs Neunen*	31.5 Sekunden	2.59 Sekunden	Höchstverfügbar / fehlertolerant
> 99.9999%			Desaster-Tolerant / fehlerresistent

Benötige ich 99.999%?

- Vermutlich nicht :)
  - Auf jeden Fall nicht für alles oder zu jeder Zeit
- Abwägung zwischen Risiko, erwartetem Schaden und Wirtschaftlichkeit
- Klassifizierung eines Systems/Service

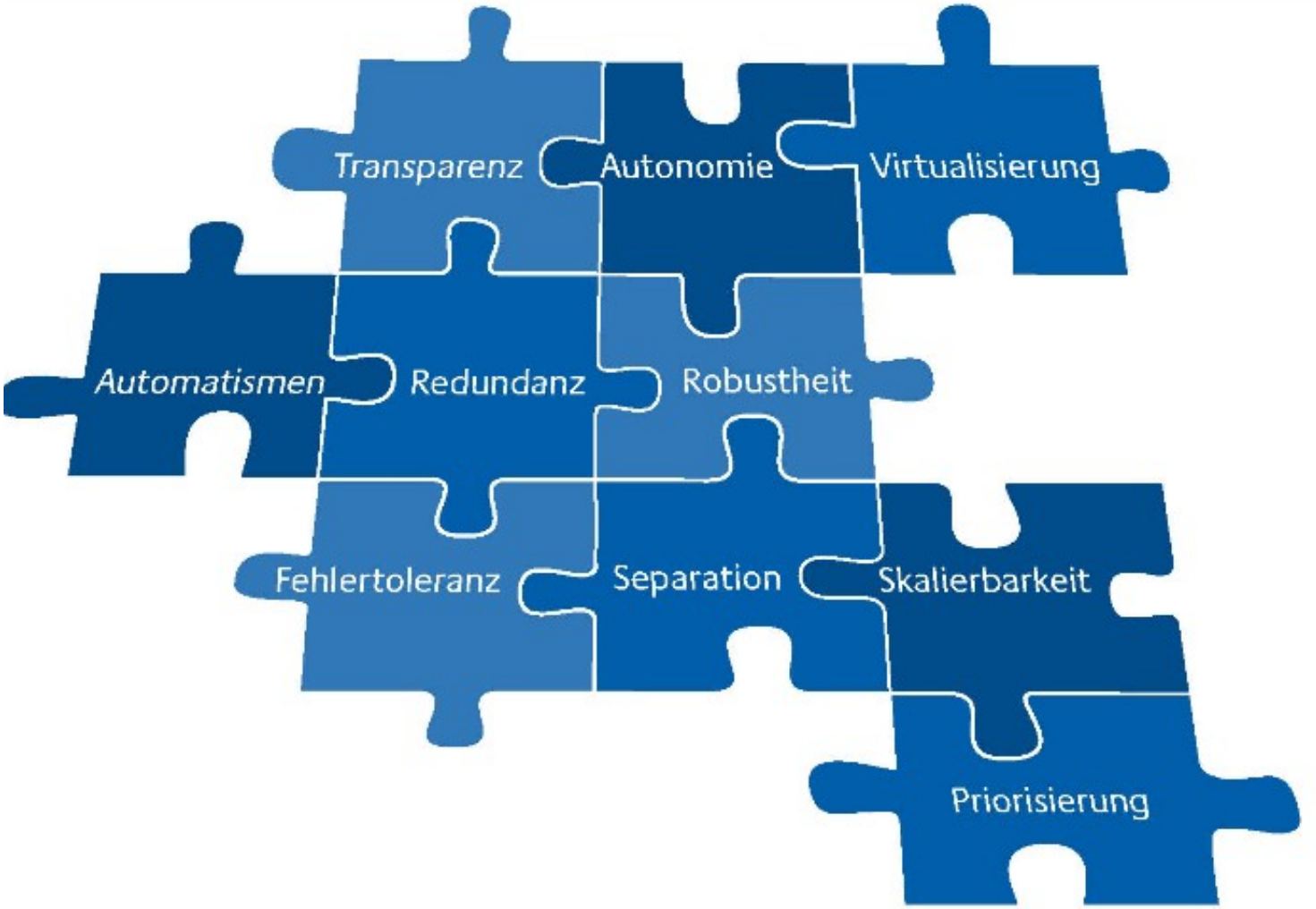
HRG-Verfügbarkeitsklassen

***Availability Environment Classification (AEC)*, der Harvard Research Group**	
Klasse	**Beschreibung**
AEC-0	Geschäftsfunktionen können unterbrochen werden, Datenintegrität nicht essentiell
AEC-1	Geschäftsfunktionen können unterbrochen werden, Datenintegrität muss gewährleistet sein
AEC-2	Geschäftsfunktionen können nur kurzzeitig oder geplant unterbrochen werden, Performance Degradierungen sind verkraftbar
AEC-3	Geschäftsfunktionen mit unterbrechungsfreiem Ablauf, Performance Degradierungen sind verkraftbar
AEC-4	Geschäftsfunktionen mit unterbrechungsfreiem Ablauf, keine Performance Degradierungen

Wege zur Hochverfügbarkeit

- Erhöhung der **MTTF** (Mean-Time-to-Failure)
- Verkürzung der **MTTR** (Mean-Time-to-Repair)

Allgemeine Prinzipien



Quelle: Bundesamt für Sicherheit in der Informationstechnik

stepping stone

Anwendung der Prinzipien

- Im Architektur-Design
- Über den Service-Stack
- Organisatorisch / Personell

Konkrete Ansätze

Konkrete Ansätze – Hardware

- Redundante und/oder fehlertolerante Komponente
  - Lüfter, Netzteile, ECC-Memory, Disks/Drives, Netzwerkanschlüsse etc.
- Hot-Swap Komponente
  - Disks, teilweise auch CPU und Memory
- Out-of-Band Management, Sensoren etc.
- Ersatzteillager bis zu Cold-Standby-Hardware

Konkrete Ansätze – Netzwerk

- Redundante Switches, Router, Firewall
- Redundante Pfade
  - Trunking / Bonding / RSTP
- Unterschiedliche Wegführungen
- Unterschiedliche Übertragungsmedien
- Dynamisches Routing
- VLANs

Konkrete Ansätze - Applikationen/Software

- Strikte Input- und Datenvalidierung
- Fehlertoleranz, aktive Fehlerbehandlung
- Einsatz von anerkannten Design-Patterns
- Protokollierung / Logging
- Continous-Integration, automatisches Testen
- Lasttests, Penetration-Tests

Konkrete Ansätze – Speicher

- Einsatz von „Data-Center“ Disks/SSDs
- RAID
- Architektur: DAS, NAS, SAN (Topologie)
- Aufbau Speicherhierarchie
- Wahl Dateisystem (Snapshots, Checksums, Resizing, Clustering etc.)
- Replikation
- Wahl Sicherung- / Wiederherstellungsverfahren

stepping stone

Konkrete Ansätze – Datenbanken

- Replikation
  - Synchron/asynchron, Master/Slave, Master/Master
- Datenbank-Cluster
- Partitionierung
- Minimierung/Vermeidung von Locking
- Strikte vs. Eventual-Konsistenz

Konkrete Ansätze - Organisatorisch / Personell

- Prozessdefinition
- Risikomanagement
- Sicherheitskonzept
- Konfigurationsmanagement
- Überwachung & Incidentmanagement
- Qualifiziertes Personal
- Schulung und Dokumentation

stepping stone

Herausforderungen

- Komplexität
- Planung
- Fachpersonal / Dienstleister
- Risikominderung vs. Kosten

Erfolgsfaktoren

- Planung, Architektur, Einsatz von Standard-Technologien
- KISS
- Identifizieren/vermeiden von SpoF
- Testen
- Monitoring
- Schulung
- Dokumentation
- SLA mit Provider klären

Fragen

stepping stone GmbH
Neufeldstrasse 9
CH-3012 Bern

Telefon: +41 31 332 53 63
www.stepping-stone.ch
info@stepping-stone.ch