

Sichere Datenhaltung im Backuprechenzentrum

Jörg Möllenkamp
Engagement Architect
Sun Microsystems



Agenda

- Die Herausforderung
- Die Lösung
 - > ... in der Initialphase
 - > ... während des Betriebes
- Beachtenswert
 - > ... vor dem Disaster.
 - > ... nach dem Disaster.

Die Herausforderung

Sie haben also ein
Backuprechenzentrum ?

Server gemietet,
Applikationen installiert?

Alles in bester Ordnung ?

Die Herausforderung

Server, Programme und
Leitungen sind wertlos ohne
Ihre Daten!

Nebenbedingung: die Daten sollten so aktuell
sein

Die Herausforderung

Die Herausforderung ist also:
Wie transportiere ich die
Daten effizient und effektiv in
mein Ausweichrechenzentrum
und halte sie aktuell?

Am Anfang war die Initialisierung!

Problemstellung:

Sie haben 5 Terabyte Daten auf ihrem Fileserver und noch mal 5 Terabyte Daten in ihrer Datenbank. Wie bekommt man diese Daten erstmalig auf die Ausweichsysteme?

Am Anfang war die Initialisierung!

Offensichtliche Lösung:

Schnelle Leitung anmieten und einfach die Kopie/Mirror starten.

Am Anfang war die Initialisierung!

Nochmal nachgedacht:

10 TB über eine 100MBit/s-WAN-Strecke
bedeutet:

1.048.000 Sekunden
entspricht
12 Tagen

Am Anfang war die Initialisierung!

Nicht so offensichtliche Lösung:

Festplatten an das Produktiosystem anschliessen, Daten spiegeln, in LKW stellen, Festplatten an das Backupsystem anschliessen

Oder anders gesagt:

Unterschätzen Sie niemals die Datenübertragungsgeschwindigkeit eines Lastkraftwagens!

Während des Betriebes ...

Es gibt viele Lösungen:

Logshipping

Synchroner Plattenspiegel

Applikationsbasierte Replikation

Shadow Database

Near synchronous Replication

Manuell gestartete Replikation

Während des Betriebes ...

Es gibt viele Produkte:

SRDF

ShadowImage+RemoteCopy

StorEdge Data Replication Facility

rsync

Libelle DBShadow

Oracle DataGuard

Libelle FSShadow

Während des Betriebes ...

Allen Lösung gemein ist:

- Sie übertragen während des Betriebes den Zustand inkrementell auf das Backupsystem

Vorteil:

- Erheblich weniger Daten werden transportiert.
- bei vielen Mechanismen kann die Replikation absichtlich verzögert werden -> Schutz gegen logische Fehler.

Vor dem Disaster ?

Hinweise aus der Praxis:

- Disaster Recovery Strategien, die nicht getestet werden, sind das Papier nicht wert auf dem sie stehen.
- Administratoren sollten regelmässig den Ernstfall proben.
- Es sind die Kleinigkeiten, die später einen guten Plan ruinieren.

Und nach dem Disaster ?

Eins wird gerne vergessen: Man braucht auch getestete und funktionierende Mechanismen, um aus dem Backup-Rechenzentrum wieder herauszukommen.

Die Synchronisation muss in beide Richtungen funktionieren.

Fragen?

joerg.moellenkamp@sun.com

