Backup (Zentrale Server/ Instituts-Server)

Das Rechenzentrum betreibt eine zentrale Backup-Lösung, mit deren Hilfe Daten aus den Instituten vorrangig von File-Servern und Workstations zentral gesichert werden können. Zu diesem Zweck wird das Software-Paket Netvault der Firma Bakbone eingesetzt. Die Sicherung erfolgt zunächst auf einem disk-basierten Storage-Bereich, sog. VTLs, im Anschluss die endgültige Lagerung auf TapeLibraries mit LTO-Technologie. Durch das inkrementelle Backup können Abbilder von Daten zum aktuellen Zeitpunkt wiederhergestellt werden. Dadurch wird eine optimale Sicherheit wichtiger Daten erzielt.

NetVault Backupsystem

Hardware

Das Backup erfolgt zentral gesteuert, d.h. Backup-Requests werden von einem Server auf den Clients initiiert, die Backup-Jobs sind nicht über die Backup-Clients veränderbar, jedoch können Restore-Anfragen jederzeit vom Administrator des Clients ausgelöst werden.

Als Backupdevices werden verwendet:

- Virtuelle TapeLib mit etwa 16TB Speicherplatz (als RAID-System im Backup-Server)
- HP MSL6060 TapeLib mit 6x LTO-4 Laufwerken und 180 Tape-Slots (etwa 140TB netto) im RZ.

Die „große“ HP MSL6060 Tapelib ist aus drei einzelnen HP MSL6060 Tapelibs zusammengesetzt, die im Master-Slave-Betrieb verbunden sind. Die einzelnen Geräte sind übereinander in einem Schrank montiert und über einen „Schlitten“ (das sogenannte Passthrough-Modul) miteinander verbunden. Wird ein Band aus der dritten Tapelib im Laufwerk in der ersten Tapelib benötigt, so wird der Schlitten zur dritten Library gefahren, das Band wird vom dortigen Roboter in den Schlitten geladen und zur ersten Library transportiert. Der dortige Roboter übernimmt das Band und lädt es in das Laufwerk.

Backup-Policy

Einmalig werden die zu sichernden Bereiche des Backup-Clients vollständig auf Band gesichert. Anschliessend werden täglich inkrementelle Sicherungen durchgeführt, die wöchentlich zusammen mit dem initialen Voll-Backup konsolidiert werden, d.h. zu einem synthetischen Voll-Backup zusammengeführt werden.

Die Sicherungen repräsentieren immer den momentanen Datenbestand der Systeme, d.h. es kann nicht nach Veränderungen, die innerhalb eines Tages geschehen sind, gesucht werden. Es werden aus Kapazitätsgründen nicht mehrere Voll-Backups pro Client vorgehalten (Ausnahmeregelungen sind möglich)

Dieses Dokument stammt aus der Dokuwiki-Instanz mit dem Titel RZ-Dokumentationen, die vom Rechenzentrum der Technischen Universität Clausthal bereitgestellt wird.

Ein Restore des Systems bzw. der Systemplatte kann mit NetVault nicht durchgeführt werden. Deshalb muss der Systembereich mit den entspr. Unix-Tools, wie „dump“ bzw. „dd“ oder unter Windows mit „Ghost“ bzw. „Acronis-Backup“ etc. gesichert werden.

Die NAS-Systeme des RZ (NetApp und Isilon-Cluster) werden täglich gesichert, das Backup ist nur zur disaster recovery notwendig. Nach einem erfolgreichen Backup wird das alte Full Backup gelöscht bzw. das Band zum Beschreiben freigegeben. Die täglichen Veränderungen in den Userhomes oder anderen veränderlichen Datenbereichen auf den NAS-Systemen werden in den sog. Snapshots mit unterschiedlichen Aufbewahrungszeiträumen versehen.

NetApp NAS (nas1.tu-clausthal.de und nas2.tu-clausthal.de)

- 6 Snapshots um 08:00, 10:00, 12:00, 16:00 und 20:00
- 6 tägliche Snapshots um 00:00
- 4 wöchentliche Snapshots um 00:00

Diese Snapshots werden zyklisch überschrieben, sodass insgesamt auf 16 vorhandene Snapshots zurückgegriffen werden kann.

Isilon-NAS bzw. isilon-Cluster (nas.tu-clausthal.de)

Gleichartige Snapshot-Schedules für sämtliche Instituts-Datenbereiche:

- every weekday every 4 hours from 08:00 to 20:00, expiration=5days
- every day at 02:00, expiration=21days
- every 1 month on the 1st, expiration=4months

Insgesamt werden hier 45 Snapshot-Images vorgehalten.

Das sind die derzeitigen Einstellungen, die nach der Erweiterung des isilon-NAS-Systems auf 250TB bei Bedarf individuell angepasst werden können. Fix Me!

Hinweis zum Expire von inkrementellen und vollen Sicherungen

Zunächst einmal ist zu unterscheiden zwischen löschen und expire, letzteres löscht nur die entsprechenden Einträge aus der NetVault-Datenbank, so dass sie „vergessen“ werden. Sobald alle Savesets auf einem Tape derart „vergessen“ wurden, erscheint das Tape für NetVault leer, es wird für „Reuse“ markiert und dann beim nächsten Backup überschrieben. Erst dann werden Daten tatsächlich gelöscht.

Ähnlich verhält es sich bei vollen und inkrementellen Datensicherungen. Wenn ein Fullbackup expired, werden auch die relevanten Incrementals expired, d.h. aus der Datenbank entfernt, da sie ohne Fullbackup wertlos sind. Allerdings bleiben alle Backups so lange auf Tape, bis es überschrieben wird und können somit mittels Scan wieder in die Datenbank gelesen werden.

Dieses Dokument stammt aus der Dokuwiki-Instanz mit dem Titel RZ-Dokumentationen, die vom Rechenzentrum der Technischen Universität Clausthal bereitgestellt wird.

Inkrementelle Backups beziehen sich auf das vorangegangene Full Backup bzw. auf das synthetische konsolidierte Backup. Deshalb benötigen die inkrementellen Sicherungen keine Angabe zur Lifetime, da sie laut unserer Policy mit erfolgreichem nächsten Full Backup bzw. Konsolidierlauf mit der vorangegangenen vollen Sicherung gelöscht werden.

Ein consolidated backup zählt so, als ob zu diesem Zeitpunkt als ein neues Full Backup angelegt worden wäre. (O-Ton-Bakbone)

Weiterführende Infos entnehmen Sie bitte der (englischssprachigen) NetVault-Dokumentation:

- User Guide
- Admin Guide
- Supported Platforms

Direkt-Link:
https://doku.tu-clausthal.de/doku.php?id=netvault_backupsystem:start&rev=1391507051

Letzte Aktualisierung: **09:44 04. February 2014**

Dieses Dokument stammt aus der Dokuwiki-Instanz mit dem Titel RZ-Dokumentationen, die vom Rechenzentrum der Technischen Universität Clausthal bereitgestellt wird.