Backupdienst TSM

Dokumententitel: Backupdienst TSM
Dateiname: Servicebeschreibung_Backupdienst.PDF
Version: V 2.2

TECHNISCHE UNIVERSITÄT DARMSTADT

HRZ Hochschulrechenzentrum

Betrieben durch das Hochschulrechenzentrum der TU Darmstadt

1. Inhalt

1. Inhalt 1
2. Versionshistorie 1
3. Beschreibung Backupdienst 2
4. Betreiber des Backupservers und Standort der Systeme 2
5. Zugriffsschutz/Autorisierung 2
6. Auditierbarkeit 3
7. Datenbehandlung 3
7.1. TSM Backupkonzept 3
7.2. Verschlüsselung 3
7.3. Aufbewahrungszeiten und Versionierung 3
7.4. Datenpfade 3
8. Disaster recovery des TSM-Servers 4
9. Verantwortung des Klientenbetreibers 4

2. Versionshistorie

Version	Editor	Datum	Kommentar
1.0	HRZ	17.03.2010	Version 0.1 als Anlage zur Dienstvereinbarung TUCaN
1.1	Abteilung Basisdienste, Dr. Andreas Schönfeld, Dr. Caide Wang	09.10.2014	Aktualisierung
2.0	Annelore Schmidt	10.12.2014	Layoutanpassung und Versionshistorie
2.1	Dr. Andreas Wolf, Dr. Caide Wang,	26.02.2015	Aktualisierung für SAP

2.2	Dr. Caide Wang	05.06.2018	Aktualisierung

3. Beschreibung Backupdienst

Das Hochschulrechenzentrum (HRZ) der TU Darmstadt verwendet die Software Tivoli Storage Manager (TSM) Extended Edition von IBM als zentrale Backupsoftware.

Die zu sichernden Daten werden mit einer Klientensoftware (TSM-Client) von dem zu sichernden Rechner zum TSM Server übertragen. Dieser verwaltet dann - abhängig von den Vorgaben des Klienten - den weiteren Life-Cycle der ihm anvertrauten Daten (z.B.: Speichern auf Platten oder Bändern, Migration auf andere Medien, Löschen nicht mehr benötigter Daten).

Im Falle eines Restores fordert der Klient die Daten wieder vom Server an.

4. Betreiber des Backupservers und Standort der Systeme

Der TSM-Backupserver der TU Darmstadt wird durch die Administratoren des Backupsystems am HRZ betrieben.

Der Backupserver sowie die lokalen Speichermedien (Platten und Bänder) sind im Serverraum 087/089 des HRZ (Otto-Berndt-Straße 2, 64287 Darmstadt), ein gesicherten Raum, untergebracht. Der HRZ Serverraum wird von zwei Stromversorgungen (A und B), zwei USV, Löschen Gas, BMZ, redundante Netzwerke aufgerüstet, der Raum ist klimatisiert.

Der TSM Server besteht im Wesentlichen aus vier Baugruppen, dem eigentlichen Server, einem Plattenpool für die Datenbank des Servers und einem Plattenpool für die zu ihm gesicherten Daten sowie einer Tape-Library.

Eine Zweitkopie aller Daten des HRZ-Backupsystems wird an der Universität Frankfurt gespeichert.

Die wechselseitige Speicherung der Zweitkopie zwischen der der Universität Frankfurt und der TU Darmstadt ist vertraglich durch eine „Kooperative Vereinbarung zur Auftragsdatenverarbeitung“ geregelt.

Eine 10G Ethernet Verbindung zwischen TU Darmstadt und Universität Frankfurt über Hessennetz ist im Einsatz.

5. Zugriffsschutz/Autorisierung

Die Klientensysteme (Knoten) werden vom TSM Server durch die Kombination von Knotennamen und Passwort identifiziert. Nur Knoten, die korrekt authentisiert wurden, sind in der Lage, Daten zu schicken, abzurufen oder zu löschen. Der Zugriff auf Daten eines anderen Knotens ist nur möglich, wenn dies durch die Vergabe entsprechender Proxy-Rechte ausdrücklich erlaubt wurde. Ansonsten ist ein Zugriff nicht möglich.

Der Knotenname ist unabhängig vom Netzwerk-Namen und der IP-Nummer des Klienten. Der Knotenname, der beim Knotenbeantragen mitgegeben wird, kann von TSM Serveradministrator auf Grund der Namenkonvention geändert werden.

Das Passwort kann durch die TSM-Server-Administratoren jeder Zeit neu gesetzt werden, falls Klientenbetreuer das Passwort vergessen hat, natürlich kann der Klientenbetreiber das Password selbst auf Klientenseite ändern.

6. Auditierbarkeit

Alle vom Server durchgeführten Aktivitäten sowie auftretende Fehler werden im Activity Log des Servers protokolliert und für 30 Tage gespeichert. Das schließt auch die Anweisungen von Klienten und TSM-Serveradministratoren ein.

7. Datenbehandlung

7.1. TSM Backupkonzept

Auf dem Knoten wird in einer Konfigurationsdatei definiert, welche Daten gesichert werden (Laufwerke, Verzeichnisse, einzelne Dateien). Die Verantwortung für Datenbackup und Datenzurückschreiben von dem Knoten liegt alleine beim Klientenbetreuer.

Die Klientenbetreiber werden dazu angehalten, den Restore ihrer Daten regelmäßig zu testen, damit sie den Bedarfsfall die notwendige Praxis haben und sichergestellt ist, dass alle benötigten Daten gesichert wurden.

Beim Backup überprüft der TSM-Client, ob die zu sichernden Daten seit dem letzten Backup verändert wurden. Wenn dies der Fall ist, werden die veränderten Daten zum Server übertragen. Jedes Backup ist also ein Inkrement auf die vorherigen Backups. Der TSM Server speichert die Information, welchen Daten wann gesichert wurden in einer Datenbank. Daher ist er in der Lage, im Falle eines Restores die benötigten Daten herauszusuchen.

7.2. Verschlüsselung

Der TSM Server verarbeitet die Daten so, wie er sie erhalten hat. Wenn eine Verschlüsselung der Daten erfolgen soll, so muss dies klientenseitig erfolgen (Client Side Encryption). Im TSM Klienten sind dafür Funktionen für eine starke Verschlüsselung (wahlweise AES128 oder AES256) enthalten. Daten, die mit Client Side Encryption gesichert wurden, können nur mit dem dabei vergebenen Passwort restauriert werden. Ein Neusetzen dieses Passwortes ist weder durch die Administratoren, noch durch den Klientenbetreiber möglich. Bei Verlust des Verschlüsselungspasswortes ist -unabhängig von der verwendeten Verschlüsselungsverfahren- die Restauration der verschlüsselten Daten nicht mehr möglich.

Die Datenverbindung vom Klienten zum TSM Server kann unabhängig davon mit SSL verschlüsselt werden.

7.3. Aufbewahrungszeiten und Versionierung

Durch das inkrementelle Backupkonzept gibt es bei TSM die aus vielen Bereichen bekannten Wochen-, Monats- und Jahresbackups nicht. Die notwendige Versionierung erfolgt für jede Datei gesondert. Jede Datei wird beim Backup, nach den Vorgaben des Klientenbetreibers, in eine Verwaltungsklasse (Management Class) eingeteilt. Die Verwaltungsklasse legt fest, wie viele Versionen von einer Datei für welche Zeit aufgehoben werden sollen. Der TSM-Server überwacht die Einhaltung dieser Vorgaben und löscht nicht mehr benötigte Daten.

Welche Verwaltungsklassen für den jeweiligen Knoten verfügbar sind und wie die damit verbundenen Fristen und Versionen eingestellt sind, kann der Klientenbetreiber jederzeit abfragen, aber nicht selbst definieren. Bei Bedarf können die TSM-Server-Administratoren weitere Verwaltungsklassen gemäß den individuellen Anforderungen einrichten.

7.4. Datenpfade

Der TSM Server speichert die ihm anvertrauten Daten vor Ort auf Platten oder Bändern. Von diesen lokalen Daten wird einmal pro Tag eine Kopie über ein privates Layer-2-Netz zum Backupserver der

Universität Frankfurt geschickt, so dass in der Regel nach spätestens 24 Stunden von allen Daten eine Zweitkopie im Backupsystem der Universität Frankfurt besteht.

Sollte beim Lesen von Daten eine Beschädigung der lokalen Kopie festgestellt werden, greift der TSM Server automatisch auf die Zweitkopie zurück.

8. Disaster recovery des TSM-Servers

Für den Fall, dass der TSM-Server selbst von einer größeren Störung betroffen sein sollte, liegen Notfallanleitungen zum Wiederanfahren auf Basis der TSM eigenen DRM-Mechanismen vor.

Die Funktionsfähigkeit der Mechanismen wurde zuletzt am 05.11.2013 im Rahmen einer Neuinstallation des TSM-Servers inklusive vollständigem Restore der Datenbank getestet.

9. Verantwortung des Klientenbetreibers

Die Verantwortung für Auswahl, Klassifizierung und eventuelle klientenseitige Verschlüsselung der zu sichernden Datenbestände, sowie die Kontrolle des Backuperfolgs, liegt alleine beim Klientenbetreuer. Insbesondere hat er dabei auch auf die Einhaltung der für die zu sichernden Daten relevanten Datenschutzbestimmungen zu achten.

Das HRZ unterstützt die Klientenbetreiber bei dieser Arbeit, in dem es ihm auf Wunsch automatisiert Hinweismails schickt, die auf potentiell problematischen Zustände hinweisen.