Richtlinie zur Nutzung des TSM-Backup-Systems des RRZ

Version: 1.0.20121218

Begriffsdefinitionen:

TSM-Server: Das RRZ betreibt mehrere zentrale *Tivoli Storage Manager* Server zur Sicherung von Daten, die nach einem Festplattenschaden bzw. nach einem versehentlichen Löschen nicht über Neuinstallation des Betriebssystems bzw. der Anwendungsprogramme wiederhergestellt werden können.

TSM-Knoten: Jeder an einem der Server registrierter Client (-PC bzw. -Server) wird vom TSM-System als *Knoten* geführt. Auf jedem Knoten wird dazu vom Benutzer die TSM-Client-Software installiert und konfiguriert. Das RRZ stellt die Software und Installationsanleitungen für alle gängigen Betriebssysteme kostenlos auf der Internetseite bereit. Sollte Bedarf für spezielle Sicherungsmethoden (SQL Agent, VMWare, u. ä.) bestehen, kann die notwendige Lizenz vom RRZ beschafft und dem Benutzer gegen Kostenbeteiligung zur Nutzung überlassen werden.

Backup: Als *Backup* wird vom TSM-System ein regelmäßiges (in der Regel tägliches) und zeitgesteuertes Kopieren aller seit der letzten Sicherung veränderten Daten betrachtet. Die Erstellung von (längerfristigen) Archiven wird in einer separaten Richtlinie geregelt.

Benutzer: Als *Benutzer* wird derjenige bezeichnet, der den TSM-Knoten lokal verwaltet. Dem Benutzer ist also in der Regel das Passwort des TSM-Knotens bekannt und er verfügt über Administrationsrechte bzw. „Backup-Operator“-Rechte auf dem lokalen Client. Den Einrichtungen ist es freigestellt, ob diese Rechte / Zugänge zentral verwaltet oder aber auf den jeweiligen Mitarbeiter am lokalen Client mit den sich daraus ergebenden Pflichten delegiert werden.

Die TSM-Server stehen jedem Mitarbeiter oder jeder Einrichtung der Universität Hamburg zum Sichern von o.a. Daten zur Verfügung. Universitätsfremden Institutionen kann auf Antrag an die Leitung des RRZ der Zugang gewährt werden. Mit der Beantragung der Zugangsdaten erkennt der Benutzer diese „Richtlinie zur Nutzung des TSM-Backup-Systems des RRZ“ ausdrücklich an.

Zugangsdaten: Jeder TSM-Knoten erhält eine eindeutige Kennung und ein Passwort zum Zugriff auf den TSM-Server. Das vom RRZ initial mitgeteilte Passwort ist unverzüglich in ein hinreichend komplexes und nicht (z. B. mit Hilfe von Wortlisten) leicht zu erratenes zu ersetzen. Diese TSM-Zugangskennung ist gerätegebunden und nicht übertragbar, die Weitergabe des Passworts und die dauerhafte Nutzung auf mehr als einem Gerät sind ausdrücklich untersagt. Die Registrierung eines Knotens ist zudem personenbezogen, es werden zu jedem Knoten die Kontaktdaten eines Ansprechpartners (Name, Telefon, E-Mail), der Standort (Straße und Raum), sowie das Betriebssystem und der Hardwaretyp im TSM-Server gespeichert. Änderungen an den Kontaktdaten sind dem RRZ unverzüglich mitzuteilen. Der Benutzer erklärt sich ausdrücklich damit einverstanden, dass diese personenbezogenen Daten vom RRZ elektronisch gespeichert und ggf. für Abrechnungs- oder statistische Zwecke verarbeitet werden dürfen. Eine Weitergabe an Dritte erfolgt nicht.

Zugriffsschutz: Nach 5 maliger falscher Eingabe des Passwortes wird der Zugang für den Knoten automatisch gesperrt. Der Benutzer muss die Reaktivierung

beim RRZ formlos beauftragen und erhält bei Bedarf / auf Wunsch ein neues Passwort.

Das RRZ stellt durch geeignete Betriebsabläufe sicher, dass der Zugang zum TSM-System und den Daten nur den dafür authorisierten Administratoren bzw. den registrierten Knoten möglich ist.

Sperrung des Knotens: Besteht zwischen TSM-Knoten und -Server über einen Zeitraum von mehr als 180 Tagen kein Kontakt, so wird der Zugang für den Knoten automatisch gesperrt. Der Benutzer wird 30 Tage vor der anstehenden Sperrung des Knotens täglich auf diese per E-Mail hingewiesen.

Löschung des Knotens: Der Benutzer kann das Löschen seines Knotens und / oder der dazu gespeicherten personenbezogenen Daten jederzeit verlangen, dabei werden sowohl die personenbezogenen als auch die mit dem TSM-Client gesicherten Daten endgültig vom TSM-Server entfernt

Automatische Löschung des Knotens: Knoten, die nach einer Sperrung nicht innerhalb von weiteren 180 Tagen durch den Benutzer wieder reaktiviert werden, werden automatisch vom TSM-Server gelöscht, wodurch auch alle gesicherten Daten endgültig entfernt werden. Der Benutzer wird 30 Tage vor Ablauf der Aufbewahrungsfrist täglich per E-Mail auf die anstehende Löschung hingewiesen.

Sicherungszeiten: Für die Sicherung der Daten werden zwei Zeitfenster angeboten, eines für Sicherungen in der Nacht (Startzeitpunkte 22 sowie 0, 2oder 4 Uhr nächsten Tages) und eines für Sicherungen am Tag (Startzeitpunkte 10, 12, 14 oder 16 Uhr). Einen Startzeitpunkt kann der Benutzer bei der Beantragung des Knotens auswählen. Diesem Wunsch wird, soweit es der Betriebsablauf ermöglicht, entsprochen. Der Benutzer sollte bei der Wahl der Startzeit bedenken, dass der Knoten zu der besagten Zeit auch regelmäßig in Betrieb ist (ein *Stand-by* ist nicht ausreichend). Ein Wechsel der Startzeit von Tag nach Nacht bzw. umgekehrt ist nach erstmaliger Nutzung nicht mehr, eine Änderung des Zeitpunktes innerhalb des Tag- bzw. Nachtfensters allerdings jederzeit möglich.

Das RRZ behält sich jedoch vor, für normale PCs den Start der Sicherung ohne Ankündigung innerhalb des Fensters zu verschieben, wenn der reibungslose Betrieb des TSM-Servers dies notwendig macht. Für Server wird die Sicherungszeit nur nach Absprache mit dem Ansprechpartner verändert, zwingende Uhrzeiten, die sich aus der Art des Servers bzw. aus den Daten auf diesem ergeben, werden, soweit es der Betrieb zulässt, berücksichtigt.

Verfügbarkeit des TSM-Dienstes: Das RRZ betreibt den TSM-Dienst 24h * 7 Tage die Woche und strebt durch geeignete Betriebsabläufe sowie Redundanzen eine Verfügbarkeit der TSM-Server von 96% an. Anstehende Wartungsunterbrechungen werden, soweit möglich, rechtzeitig auf den Internetseiten des RRZ bekanntgegeben. Fehlermeldungen oder Ausfälle werden werktäglich montags bis freitags zu den üblichen Kernzeiten bearbeitet bzw. behoben.

Nicht zu sichernde Daten: Temporäre Dateien und Verzeichnisse, sowie Browser-Caches o.ä. brauchen nicht gesichert werden, da es sich dabei um kurzlebige (nur zwischengespeicherte) und für den Rechnerbetrieb nicht notwendige Daten handelt. Das RRZ ist berechtigt, solche Daten per Server-Policy von der Sicherung grundsätzlich auszunehmen. Die mit Hilfe einer solchen Policy ausgeschlossenen Dateien / Verzeichnisse werden auf der Homepage des RRZ veröffentlicht.

Umfang der Daten: Dem Benutzer wird für normale Arbeitsplatz-PCs ein Sicherungsvolumen von 200 GByte und für Server von 5 TByte bereitgestellt. Wünscht der Benutzer die Sicherung eines größeren Datenvolumens, so sollte er dies

mit dem RRZ vorher absprechen. Bei einer deutlichen Überschreitung sind die erhöhten Betriebskosten in Zusammenarbeit mit dem RRZ bei der Universität zu beantragen. Zudem sind alle Sicherungsläufe mit einem initialen Datenvolumen von mehr als 500 GByte oder einem täglichen Volumen von über 200 GB mit dem RRZ vorher abzusprechen, um negative Auswirkungen auf den Serverbetrieb zu vermeiden.

Die Obergrenzen für die Speicherung von Daten werden zu Beginn eines jeden Jahres ggf. aktualisiert und auf der RRZ Homepage veröffentlich.

Aufbewahrung der Daten: Im Backup werden standardmäßig zusätzlich zu den aktuell auf der Festplatte des Knotens befindlichen Daten noch die Version(en) der vorangegangenen 30 Tage vorgehalten. Auf dem Knoten bereits von der Festplatte gelöschte Daten werden für 90 Tage aufbewahrt. Nach Ablauf dieser Fristen werden die Daten automatisch aus dem TSM-Server entfernt und können nicht mehr wiederhergestellt werden. Aktive, d.h. auf dem Client vorhandene, Daten werden grundsätzlich nie entfernt. Von allen gesicherten Daten (unabhängig vom Alter) werden 2 Kopien an unterschiedlichen Standorten vorgehalten. Da das Erzeugen der 2. Kopie asynchron erfolgt, kann dies bis zu 3 Tage benötigen. Das RRZ übernimmt jedoch keine Haftung für den Verlust von Daten, wenn trotz Einhaltung der Betriebsabläufe beide Kopien nicht mehr lesbar sind.

Fehler bei der Sicherung: Sollte die tägliche Sicherung fehlerhaft sein, so informiert das RRZ den Benutzer darüber automatisch per E-Mail. Detaillierte Fehlermeldungen finden sich jedoch ausschließlich in den Logdateien dsmerror.log / dsmsched.log im Installationsverzeichnis auf dem TSM-Knoten. Diese Dateien und die Fehlermeldungen sollte der Benutzer kontrollieren, bevor er den RRZ-Support unter uhh.rrz-backup@rrz.uni-hamburg.de kontaktiert.

Status der gesicherten Daten: Auf Wunsch informiert das RRZ den Benutzer zu Beginn eines jeden Monats über die Anzahl und den Umfang der im TSM-System gesicherten Daten.

Zuständigkeit für die Sicherung: Dem Benutzer obliegt es, dass die Sicherungen regelmäßig, vollständig und fehlerfrei erstellt werden. Das RRZ übernimmt keine Gewähr dafür, dass die gesicherten Daten bei einem Totalausfall / Schaden des Knoten zu einer vollständigen Systemwiederherstellung ausreichen. Der Benutzer stellt durch geeignete Maßnahmen (z. B. durch Aktivieren der Transportverschlüsselung und / oder der Datenverschlüsselung im TSM-Client) sicher, dass die aktuell gültigen Datenschutzbestimmungen für die zu sichernden Daten eingehalten werden und dass ein ggf. für die Verschlüsselung generierte Schlüssel sicher aufbewahrt und für eine Rücksicherung zur Verfügung steht.

Der Benutzer reagiert auf die vom TSM-System versendeten Warn- oder Fehler-E-Mails in einem angemessenen Zeitrahmen. Eventuelle Fristen in den E-Mails werden vom Benutzer akzeptiert, wenn er nicht binnen 30 Tagen widerspricht.

Rücksichern von Daten: Das RRZ stellt dem Benutzer auf den Internetseiten geeignete Dokumentation zur Verfügung, um einzelne Dateien oder das komplette System an Hand der Sicherung wiederherzustellen. **Dem Benutzer wird ausdrücklich empfohlen, das Sichern und Rücksichern gezielt zu testen, um die notwendigen Arbeitsabläufe vorab zu üben.**

TSM-Client-Software: Es sollten vom Benutzer nur offiziell von IBM unterstützte TSM-Client-Versionen auf den Knoten installiert / betrieben werden. Entsprechende Ankündigungen werden auf der RRZ-Homepage veröffentlicht. Treten in Folge des Einsatzes einer nicht (mehr) unterstützten Client-Version Proble-

me beim Sichern oder Wiederherstellen auf, kann das RRZ möglicherweise keine Unterstützung leisten, so dass dann auch ein Datenverlust nicht auszuschließen ist.

Aktualisierung der TSM-Client-Software: Das RRZ kann bei Bedarf die Softwareversion auf dem TSM-Knoten automatisch per Ferninstallation aktualisieren, wenn damit Sicherheitslücken in der Software geschlossen oder den Betrieb gefährdende Kombinationen von Knoten- und Serverversion abgestellt werden können. Diese Aktualisierung wird (soweit möglich) rechtzeitig auf der RRZ-Homepage und individuell per E-Mail an die für einen Knoten hinterlegten Kontaktdaten vorab angekündigt. Widerspricht der Benutzer dieser angekündigten Aktualisierung, so ist das RRZ berechtigt, den Zugang des Knotens so lange zu sperren, bis der Benutzer selbständig ein Update auf die geforderte Version vorgenommen hat.

Schlussbestimmungen und Übergangsvorschriften: Mit Bekanntgabe dieser „Richtlinie zur Nutzung des TSM-Backup-Systems des RRZ“ verlieren alle vorherigen Versionen inkl. der „TSM-Policy“ ihre Gültigkeit. Sollte eine oder mehrere Bestimmungen vorstehender Richtlinie unwirksam sein oder unwirksam werden, so hat dies keinen Einfluss auf die Gültigkeit der übrigen Richtlinie bzw. Bestimmungen.

Das RRZ behält sich vor, diese Richtlinie jederzeit anzupassen oder zu ändern, insbesondere dann, wenn gesetzliche Vorschriften dies erfordern. Änderungen werden dem Benutzer per E-Mail und durch Ankündigung auf der Internetseite des RRZ mitgeteilt. Sie gelten als anerkannt, wenn ein Benutzer nicht innerhalb von 4 Wochen nach Bekanntgabe widerspricht. Der Widerspruch bedarf der Schriftform. Da die Daten immer nur unter der aktuell gültigen Richtlinie im TSM-System abgelegt werden können, erhält der Benutzer nach einem rechtzeitig eingegangenen Widerspruch weitere 4 Wochen Zeit, um die Daten aus dem System zurückzusichern, bevor sie endgültig gelöscht werden.