Sicherung von Verwaltungsdaten

Das Rechenzentrum betreibt seit längerem einen Backupservice für die Humboldt-Universität. Die Daten der Universitätsverwaltung unterliegen bestimmten Sicherheitsvorschriften, die „normale" Backups nicht betreffen. Der folgende Artikel beschreibt die Vorgehensweise bei der Sicherung von Daten ausgewählter Server der Universitätsverwaltung.

Datensicherung an der HU

Das Rechenzentrum der Humboldt Universität bietet seit mehreren Jahren den Einrichtungen der Universität einen Backupservice an. Zurzeit werden über 300 Clients mit den verschiedensten Architekturen – Unix, MacOs, WindowsNT, Windows 2000 und Windows-PC – gesichert. Das dazugehörige Softwareprodukt ist der Tivoli Storage Manager (TSM), der als Server-/Clientsystem die Daten der Clients – in der TSM-Sprache die Nodes – auf dem Server sichert.

Die Daten der Clients werden beim Backup auf dem Server an zwei möglichen Speicherorten (Storagepools) gespeichert, entweder auf Platte oder auf Bändern in einer Library. Der Speicherort richtet sich bei uns nach der Größe der Files. Files mit einer Größe ab 1Gbyte werden direkt auf Band gespeichert; kleinere Files werden im Storagepool auf Platte gesammelt und zu einem späteren Zeitpunkt zusammen auf Band migriert. Diese Unterscheidung ist darin begründet, dass man erreichen will, dass die Bandgeräte möglichst in den so genannten „streaming mode" kommen sollen, der die optimale Arbeitsweise für sie ist und das Bandmaterial am meisten schont.

Da das Rechenzentrum an zwei verschiedenen Standorten TSM-Server besitzt, kann es das Desaster Recovery Management – die sogenannte server-to-server-Kopplung – des TSM ausnutzen. Diese ermöglicht es, dass die an einem Standort gesicherten Daten zum anderen Standort (dem sekundären Server) kopiert werden können. Die Vorteile dieses Verfahrens sind:

- Es findet eine sofortige Leseprüfung der gesicherten Daten statt.
- Falls sich ein Band mit einem gesicherten File auf dem primären Server nicht mehr lesen lässt, wird der File vom zweiten Server geholt.

Das System kennt zwei Methoden zur Kontaktaufnahme zwischen Client und Server, die beide eine Authentisierung mittels Passwort erfordern:

- Der Server fordert den Client auf mit dem Backup zu beginnen.
- Der Client meldet sich beim Server und beginnt mit dem Backup nachdem der Server ihn verifiziert hat.

Die erste Methode ist die bei uns bevorzugte Arbeitsweise für die täglichen Backups, da nur dadurch gewährleistet ist, dass gleichmäßige Backupfenster entstehen. Die zweite Methode ist bei den täglichen Backups nur für ausgewählte Clients zulässig.

Die Client-Software bietet die Möglichkeit, die zu sichernden Daten zu verschlüsseln. Dazu wird die DES

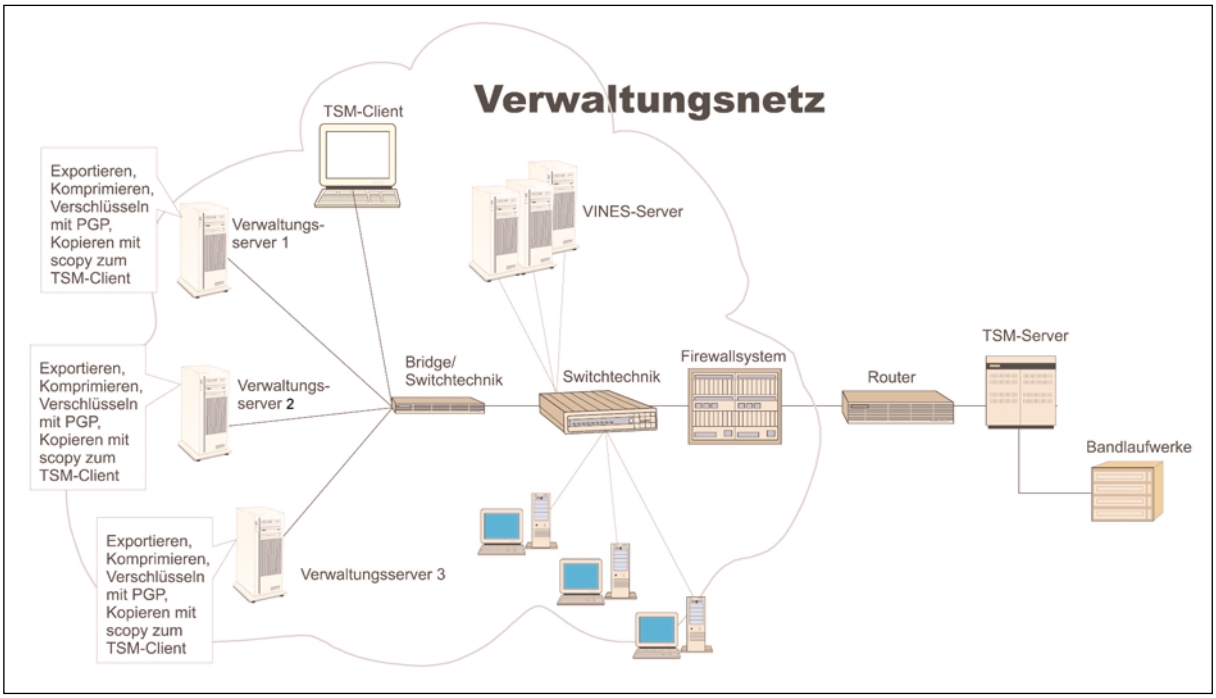

Abb. 1: Grobstruktur des Netzes bzgl. Backup

56-bit Verschlüsselung benutzt. Dies bedeutet, dass die Daten nicht nur während der Übertragung verschlüsselt sind, sondern auch auf den Zieldatenträgern. Der Schlüssel ist nur auf dem Client gespeichert oder im Kopf des Verantwortlichen für den Client. Falls der Schlüssel verloren wird, sind auch die gesicherten Daten für den Nutzer verloren!

Besondere Anforderungen an die Sicherung von Verwaltungsdaten

- Backupsysteme wie TSM sind sehr teuer und können deswegen auch nicht „mal schnell“ für eine spezielle Anwendung angeschafft werden.
- Die Hauptanforderung an die Daten der Universitätsverwaltung besteht aus der Sicht der Datensicherung darin, dass sie vor dem Zugriff durch Dritte abgeschottet sind. Deswegen sind sie für gewöhnlich hinter einer Firewall „versteckt“, hinter der sich auch die gesamte Verarbeitung abspielt. Es sollten auch keine Zugriffe von außen, wie sie zum Beispiel für Administratoraufgaben üblich sind, auf Server mit Verwaltungsdaten erfolgen dürfen, womit die Arbeitsweise „Server meldet sich beim Client“ entfällt.
- Da im Standardfall gesicherte Daten unter TSM alle im gleichen Storagepool (Platte bzw. Bänder) aufgehoben werden, muss für die Verwaltungsdaten eine Lösung geschaffen werden, die dies verhindert.
- Die Verwaltungsdaten müssen über mehr Versionen reproduzierbar sein, als es im Standard erforderlich ist.

Lösung an der HU (Siehe auch Abb. 1)

Um die Mischung der Verwaltungsdaten mit den normalen Backupdaten zu verhindern, wurden zwei neue Storagepools – UV (Platte) und UV_T (Bänder) – geschaffen. Diese ermöglichen die getrennte Aufbewahrung der Daten. Zugleich wird auch darüber gesteuert, dass die Daten der Verwaltung nicht in vier – wie es für den Standard gilt – sondern in zwanzig Versionen aufgehoben werden.

Die Daten der Verwaltungsserver werden mit den dort vorhandenen Backuptools täglich auf einem weiteren Server mit PGP verschlüsselt innerhalb der Firewall gesichert. Dieser Server (TSM-Client in Abb. 1) nimmt den Kontakt mit dem TSM-Server auf und schickt nach erfolgreicher Authentisierung die Daten in den gesonderten eigenen Storagepool.

Wenn Daten auf den Verwaltungsservern wieder hergestellt werden müssen, nimmt der Server (TSM-Client in Abb. 1) den Kontakt zum TSM-Server auf, authentifiziert sich und holt seine Daten zurück, die dann von den Verwaltungsservern geholt und dekodiert werden und zur weiteren Verarbeitung bereit stehen.

Christoph Weickmann
Weickmann@rz.hu-berlin.de