Advanced HYPERtape Usage for Network Backup at the University of Kiel

Uwe H. O l i a s
e-mail: olias@rz.uni-kiel.de

University of Kiel
Computer Center / Systems Department
Kiel, Germany

- The HYPERtape Product and Concept (Brief Snapshot)
- HYPERtape Organization, Backup-Technique and Service
- Oncoming HYPERtape Scenario
- HYPERtape Security Demands
- HYPERtape Security Steps
  - Root Privilege
  - Verification
  - Scope of HYPERtape-Operations
  - Restricted Shell
  - HYPERtape Related Uids and Passwords
  - HYPERtape/Media (Planned at UoK)
- HYPERtape Statistical Evaluation

The HYPERtape Product - I

- A software solution for
  - Multi-vendor & multi-protocol platforms for automated, unattended network backup & recovery
  - Uses existing hardware & software components of the CCN
- HYPERtape
  - Uses client-local backup-utility
  - Sends the data directly into a virtual-device (=network-protocol)
  - Server stores data on disk or cheap-media

The HYPERtape Product - II

- Backing data are written to disk
  - Use HSM like DMF under UNICOS to put data to cheap-media (this year, additional available under IRIX)
  - Use AMASS & DataManager to achive the same
- Backing data are written directly from network to cheap-media
  - Need have HYPERtape/Media for server platform
    - have a performant tool
    - support management for backup & recovery on server
    - deliver segmentation of savesets & allow filtered restore

The HYPERtape Concept

- HYPERtape knows three logical instances
  - ControlNode
    - Scheduler, dispatcher, controller of Backup-Complex
    - Uses control path to initiate backup from ServiceNode
  - ServiceNode (elsewhere known as client)
    - Uses data path towards BackupNode to back data
  - BackupNode (elsewhere known as server)
    - Stores data according template-predestined storage media
- HYPERtape Actions
  - Actions are SAVE, RESTORE and LIST

HYPERtape Organization & Backup Technique at UoK

- ControlNode
  - A SUN under Solaris
  - Option to have a second ControlNode
- BackupNode
  - A CRAY Y-MP EL, connected to STK ACS-4400
    - Receives backup-data on disk (here, backup is completed)
    - Stages backup-data from disk to cartridges
- Additional Special BackupNode
  - BackupNode DEC ALPHA for special Department-Archival
    - Uses HYPERtape/Media for Digital UNIX
    - Bulk storage is Quantum 4700 Tape Loader

Supported Clients at UoK

HW Platform	OS	Bkp-Utility
• DEC Alpha	Digital UNIX	CPIO
• SUN	SunOS, Solaris	CPIO
• IBM RS6000	AIX	CPIO
• SGI	IRIX	CPIO
• SNI RM400	SINIX	CPIO
• VAX (-Cluster)	VMS	Backup
• CRAY Y-MP EL	UNICOS	CPIO

- Client platforms, planned 1997: Windows NT, HP-UX, LINUX

Oncoming Scenario at UoK

- Have a second ControlNode, Solaris or Windows NT
- Establish decentralized fileservers with dedicated robot each
- Dec. fileservers support regional network backup with HYPERtape
- Optional RESTORE permission for every instance. Regulations:
  - All Ht-Actions prohibited per uid, per object, or per client
  - All Ht-Actions allowed per uid, per object, or per client
- Individual Ht-Admittance for LIST, RESTORE, SAVE

Security Demands at UoK

- Topic dictate of any rule: Don't introduce any feature or permission which might affect security
- Approach is:
  - using special aids
  - using organizational steps
- Application is:
  - very carefully
  - sophisticated
  - combined

Security Steps at UoK - Root Privilege

- ControlNode
  - HYPERtape administration-tools & operator recovery-tools:
    - No s-bit necessary, we don't set it
- ServiceNode
  - ServiceNode component must be able to find out files to be backed, to back and restore them:
    - Introduce a client-specific Ht-Uid on every Ht-Client
    - Install the platform specific Ht ServiceNode software
    - Appropriate s-bit settings only if requested
- BackupNode
  - Need not have any Ht BackupNode software

Security Steps at UoK - Verification

- HYPERtape needs no trusted host usage: We avoid that feature
- HYPERtape offers password-encryption from ControlNode to ServiceNode: We use that feature
- HYPERtape doesn't offer password-encryption from ControlNode/ServiceNode to BackupNode: We miss that feature, and we demand it!

Security Steps at UoK - Scope of HYPERtape-Operations (I)

- Files backed by HYPERtape
  - Files are residing in a saveset on background storage
  - Name of saveset is built by HYPERtape rule according to parameterized template
  - Name and rule is only known to HYPERtape administrator
  - Saveset is only accessible to BackupNodes HYPERtape service-uid, not to any alien
- Inhibit dialog and batch jobs under HYPERtape uids where possible

Security Steps at UoK - Scope of HYPERtape-Operations (II)

- HYPERtape operations for a specific ServiceNode
  - They are performed by the ControlNode administrator, that's the Ht-Complex manager. Standard: One single person, we have that
  - May introduce special subadministrator uids on ControlNode
    - We did it with same scope like central administrator, concerning SAVE, LIST, RESTORE
    - Our subadministrators are not allowed to administer HYPERtape databases
- We plan to introduce more subadministrators on ControlNode
  - Their scope is restricted to one ServiceNode, or a list of them (= departmental administrator)
  - Rights are restricted to LIST and RESTORE within their scope
  - May be SAVE allowed within their scope (discussed at U0K)

Security Steps at UoK - Miscellaneous

- Restricted shell
  - We have introduced restricted shell for every Ht operational uid, wherever possible
  - That keeps track that under Ht-Uid only Ht-Work is done
- HYPERtape related uids and passwords
  - Uids and passwords are different for every instance and location
  - Frequent password changes according to complexity rules keep privacy and integrity clean
- HYPERtape/Media for UNICOS (planned at UoK)
  - HYPERtape/Media uses free sockets
  - We'll restrict socket-usage to Ht-Uids and Ht-Clients

Statistical Evaluation of HYPERtape ControlNode-Logfiles at UoK

	Topic	CRAY EL-SN
☺	Monthly # of Ht-Client-Jobs (appr.)	9,000
☺	Monthly Backup-Amount (MB)	200,000
☺	Monthly job-connect (hours)	370
☺	Number of clients	53
☺	Total sum of Backup-Objects	370
☺	Average size of Full-Backup (MB)	290
☺	Average Incremental-Size (MB)	13
	(% from full)	4.5

HYPERtape Usage, step 2: 2,000 cartridges 3480/250MB native

HYPERtape Usage, step 3: 2,000 cartridges 3490-E/800MB native