



Tk20 Backup Procedure



**Your complete assessment
and reporting solution**

TK20 BACKUP PROCEDURE

OVERVIEW	3
FEATURES AND ADVANTAGES:	3
TK20 BACKUP PROCEDURE	4
DAILY BACKUP CREATION	4
TRANSFER OF BACKUPS	5
AUDITING PROCESS	5
BACKUP REPOSITORY	5
WRITE TO TAPE	5
SECURITY AND RELIABILITY	6
DISASTER RECOVERY	6

Overview

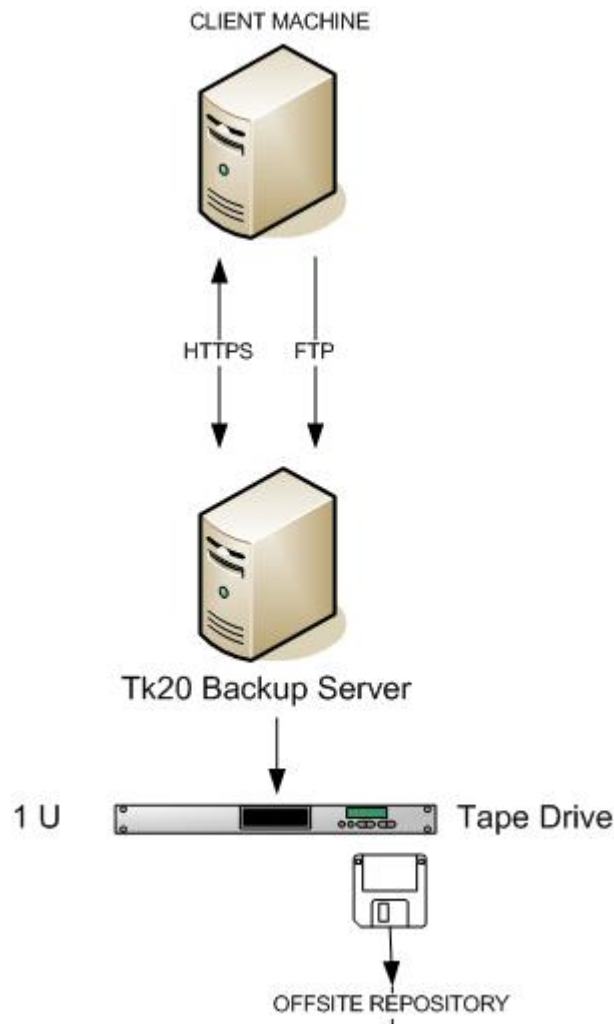
Disaster recovery from either a catastrophic occurrence or user error is necessary when dealing with an enterprise system. In order to facilitate recovery from the unexpected, Tk20 has implemented a robust data backup and recovery process.

The first level of backup is at the client hardware level with all client machines configured with RAID1. The second level of back up is on site daily backups that are taken from the client machine and securely transferred to a central repository. The third level of backup is off site backups where the daily backups are written to a tape drive and taken off site. With this multi level strategy recovery from hardware failure, user error, or catastrophic event is ensured.

Features and Advantages:

- Daily backups of all data on the system including files uploaded by system users.
- Secure transfer of the files and data being backed up.
- Validation of the data after transfer to ensure there was no corruption during transfer.
- Offsite storage to ensure recovery from a catastrophic event
- A weeks worth of backups helps to ensure that a valid state can be returned to from sometime in the last week.

Tk20 Backup Procedure



Daily Backup Creation

Tk20 backup system works once a day seven days a week. Backup system stores an entire weeks worth of backups so that at the beginning of the week it will begin to overwrite the previous week's first backup. Backups are scheduled once a day in the early morning. This is done to ensure that there is no degradation in performance during the backup process. The files that are created can be several Gigabytes in size, and take time and system resources to create. Both, the user uploaded files as well as system data

are backed up by this process so that in the case of a recovery situation all users will be able to completely recover their state from the time the backup was taken. Once the files have been generated a checksum is generated for them in anticipation of eventual transfer over network to the central repository.

Transfer of Backups

Once the files are backed up we now need to securely transfer them off of the system into the secure central backup repository. This is a one way secure transfer from the client machine to a known repository machine behind the same fire wall as the client machine. The backup process is initiated via https with by the backup machine calling the client machine's backup script with a valid username password combination. The backup machine then waits for a response from the client saying that it has finished backing up its data and is ready to transfer the data to the central repository. The client machine is then placed in queue for data transfer. Once they reach the head of the queue, the backup machine will initiate a file transfer from the client machine to that client's home directory on the backup machine. This transfer takes place via secure FTP. Once this transfer process is completed the auditing process can begin.

Auditing Process

Once the files have been uploaded to the central repository an audit is run on them to ensure that they were not corrupted during transfer over the network. This is done by comparing a checksum of the file on the backup machine against the checksum that was generated at the time of backup. If the checksum's do not match then this latest backup file is discarded and the backup machine re-initiates the backup from the particular client machine.

Backup Repository

The only access that any client machine has to the backup repository is via ftp using a username password and is locked to their home directory. Anyone not explicitly added as a client for the backup will be unable to access any directory on the system. The backup machine also resides behind a firewall to protect it from outside intrusion as an additional layer of security.

Write To Tape

Once a backup is completed it is then written to tape. This tape is then taken off site to a secure location daily. This then ensures that in the event of a catastrophe there is no data lost.

Security and Reliability

Security during this backup process is guaranteed via the protocols used and the architecture of the backup process. All https and secure ftp calls done are made via each individual client's password protected account. The architecture of the backup process ensures that while multiple client data may be backed up on a single machine there is no chance of anyone accessing another client's data.

Reliability is ensured first by auditing the files with the checksum after transfer. This validates that there was no data corruption during transfer over the network. We doubly ensure that backups are working properly by doing the additional random manual audit of backed up client data. This involves setting up an internal testing system and going through the steps of recovering the system from the data files, then validating the recovery of the system via testing the application.

Disaster Recovery

In the case of a catastrophic event there are several steps to restoring normalcy to the tk20 system. First the underlying hardware/software issue must be corrected. If it is a hardware issue and the server is still under warranty then the server will be serviced as per the warranty. If the server is out of warranty then other arrangements will have to be made. Once the underlying failure has been resolved, tk20 will restore the system to the base state with all components installed and configured. Next, the application is re-installed and tested. Finally, if the current data can be salvaged from the machine then it will be used. More likely however we will be required to rely on the backup that was taken before the service interruption. To do this the most recent backup is identified and transferred back to the newly restored server from the backup repository. This backup is then re-installed on the server and application usage can continue as normal.