PDS Linux System Backup Strategies:

Data replication is important, because it can provide a time capsule to revert unwanted changes or can prevent data loss. The new Linux systems comes with multiple solutions.

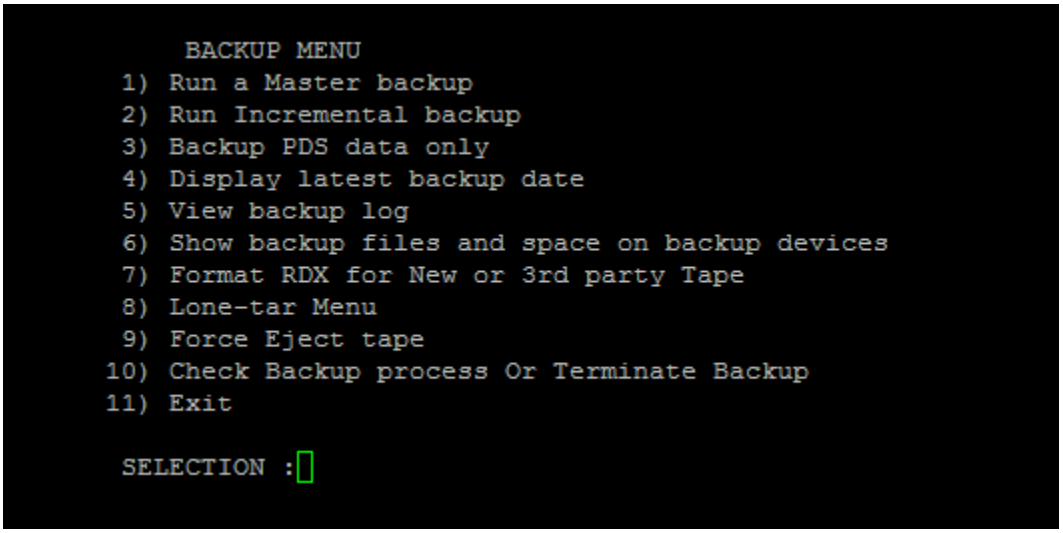
1. Backup strategies:
   1. Vault backup. It is a large capacity drive inside the server. That automatically runs around 9PM. Maintenance free. It stores 7 days of backups.
2. RDX tape backup. The RDX solution works like tape backup. Except it is a standard laptop drive that has easy access for rotation (special enclosure). It can store 7 days of backups with the standard 1TB capacity. With 2 tapes it can go to 14 days. If we rotate the drive one can be stored offsite for disaster recovery. It is important that new RDX tapes needs to be formatted and test by PRX. If we leave the tape in the drive for a week it automatically backs up 7 days. If we rotate on the weekend or Friday we can have 14 days' worth of backups.
3. 2m. The RDX Month End backups. We highly recommend to have month end backups. This is recommended to run before month end closure. This backup is focused to backup PDS system. So the backup would run faster. We recommend to buy a larger capacity RDX drive on Amazon or Staples. This backup does not rotate so we can have as many backups as the tape can handle. A 2TB drive depending on the server size can backup 20 backups which is 2 year worth of data. This feature can be accessed by the backup tool listed below "Backup Tool" section.
4. VPN-Rsync backup. This feature varies by systems as it does an offsite backup. This service depends on Internet speed and require service agreement. It synchronizes the system to our location. Than it only synchronizes the files that changed.
5. With lone-tar FTP sites can be configured
6. DVD backup. This is a replica of the month in commonly used PDF format. Which means that the DVD's does not contain any PDS data files. No PDS knowledge required to read the data. However it represents the entire month of accounting. This is good for audits and representations or to system review.

Hardware protection:

1. Hardware Raid. Multiple drives synchronize the data. Protecting from single drive failure.
2. UPS backups. We highly recommend to protect the server with battery backups.

Backup Tool:
When we login to PDS (after company selection) in the left upper corner we can verify the “LAST BACKUP” date. This status will display the last successful Vault backup. To manage backups the user need root access. Please let us know if you don’t have the root password. From PDS if we type “#” we get to the command prompt where we can type “backup” which will ask for the root password. Or when we open PDS at the login type “root” for user name and its password when prompted.

If we’ve logged in as root type “backup”



BACKUP MENU DESCRIPTIONS:

With the backup tool you will you can see statistics of the backups and the media. Verify if a backup is still running. Terminate a backup. Force eject the tape. If you run backups from here you can see the individual files being backed up.

1. “Run a Master backup” This will run a full system backup. Including the operating system and PDS. For the users request. It will ask if we want to backup to “Vault” drive or “RDX” or “FTP”.
2. “Run Incremental backup” This could be a faster smaller backup if we just want to backup recent changes that was made after the “LAST BACKUP” date.
3. “Backup PDS data only” This is the Month End Backup option (2m). This will only backup PDS data. By that this is the fastest backup. It will never rotate this backup. Use the recommended extra RDX backup tape (so it would not fill up the weekly backup tapes). Although the PDS system keeps historical information’s. This backup is recommended, because the Accounting system can purge temporally data and only keep final calculations to avoid confusing data from

past months. Accidental purging could require multiple data files restore this can be very useful in those scenarios.

4. “Display latest backup date” After or before backups you can verify the last successful backup date.
5. “View backup log” With this option you can review the backups history. (From the first system backup in the servers operation to the latest backup dates.)
6. “Show backup files and space on backup devices” This will display RDX and Vault backup files with their dates and sizes and available disk space.
7. “Format RDX for New or 3rd party Tape” This is required with any tapes.
8. Lone-tar Menu. We use Lone-tar backups. You can access the backup program from here. Some users prefer this interface over the backup menu.
9. “Force Eject tape” If the RDX tape doesn’t eject by the button this will eject it by software.
10. “Check Backup process Or Terminate Backup” This will tell us if the backup is still running.