A Linux Backup Strategy – Version 2.0

Introduction

Since the publication of version 1 of the backup strategy in 2008, a number of changes have occurred within Linux operating systems. Most notably, the support for the Windows NTFS file system has become more commonplace. Additionally, Linux has moved from the ext3 to ext4 file system as the defacto standard. These two changes have necessitated this backup strategy upgrade.

In version 1.0, the principal backup application was partimage. Partimage does not support ext4 nor does it do a full support of the NTFS file system As a result, this strategy details the move from partimage to a new full-featured backup application.

Disclaimer

The following details a backup strategy that is in use on my current hardware and software configuration. No liability is assumed by the author for any damages that may occur on your system by using the following. All information provided is the result of using the following applications successfully for backup and restoration of data.

Image Level Backups

An image level backup does what the name implies. It is comprised of all files and folders contained in a hard drive partition. This differs from other backup approaches that are found in Linux inasmuch as some of these applications only make backup copies of specific files or folders. The reasoning behind this approach is if things go wrong, most likely they would occur in the targeted folders that are backed up.

Another widely used approach for backups in Linux is to make an image of the installed operating system application indexes and settings. This image is usually burned to a CD and can be used as a platform to re-install the operating system to the configuration that was last imaged and burned. This would include all of the applications and settings present in the parent installation. The problem with this option is two-fold. First, the user is still faced with a full installation and the time associated with an installation. The second problem is that these backup applications do not address backup up non-Linux operating system partitions.

Recommendations

The recommended skill level for using this strategy is mid-level beginner or beyond in Linux operating systems. The user will need to possess a working knowledge of hard drive partitions and also be able to enter simple command line instructions.

From a hardware standpoint, it is recommended that a separate hard drive partition be allocated to serve as the repository for the backup files. This partition should be of adequate size to safely store multiple versions of each partition that is being backed up.

If the hardware resources are available, it is recommended that the primary storage partition be located on a non-operating system hard drive. The ideal situation would be to have the storage partition located on a separate dedicated hard drive. An added assurance for disaster recovery would be to also store redundant copies of the backup files on an external hard drive that is normally off-line.

Backup Strategy

The backup strategy is comprised of two parts. The first element is a controlled environment for changes to the operating system. Specifically, no updates or new application additions are made until a scheduled backup of the operating system partitions has been made. This approach helps insure a distinct recovery point if things go bad after these operating system changes.

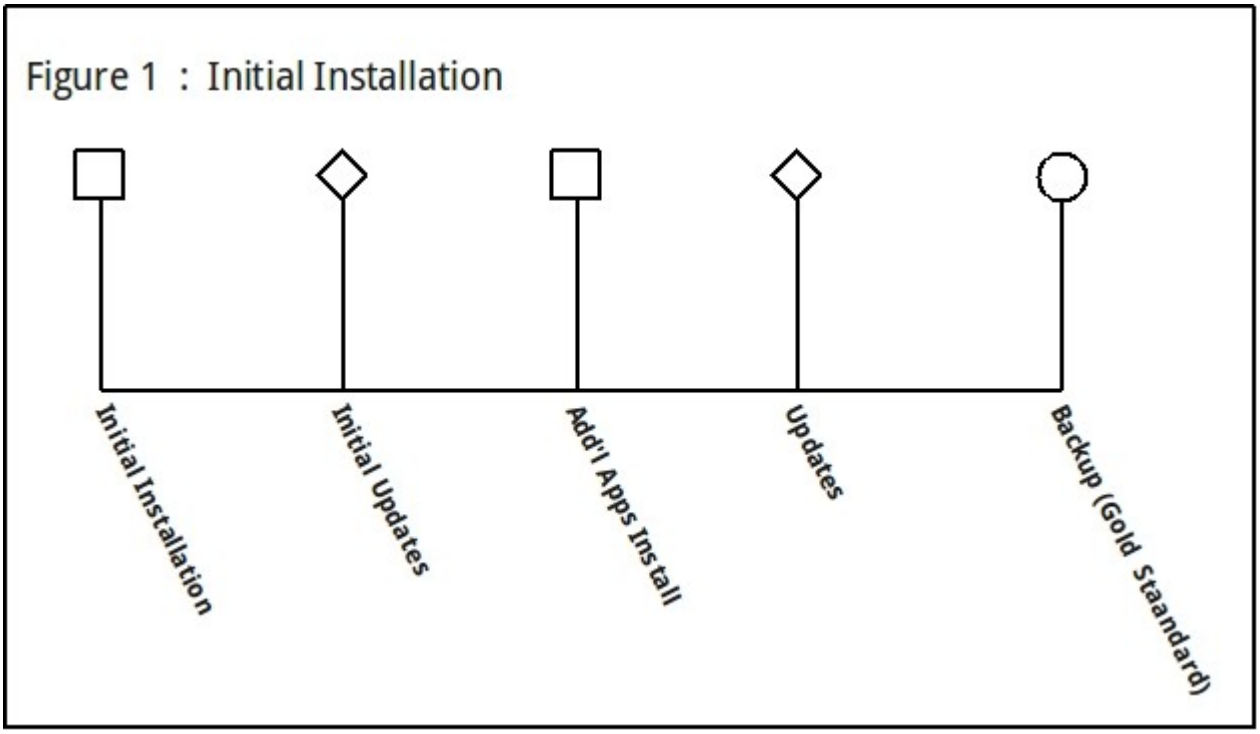
A few comments about repository level updates are in order here. Beyond the initial surge of updates immediately following installation of a Linux operating system, it is probably adequate to run repository updates on a weekly or longer basis. If the user is experiencing problems with some element of their operating system, they may want to increase this frequency until the problem is resolved (make sure it is a system problem and not an application use problem). In my stable production operating system, repository updates are run on a monthly basis.

The second part of the strategy is to perform the backups on a regular basis. It is recommended that weekly backups be run. This is especially true if one or more of the data partitions has seen a lot of changes in the preceding week.

If the user is going to use a “stable production” version of the operating system, then it is also recommended that they consider installing a “sister” operating system of the same version in a separate partition. The “sister” operating system serves as the test bed for the compatibility of new applications. Additionally, it is used to assess the impact of intermediate repository upgrades if the production operating system is receiving upgrades on say, a monthly basis.

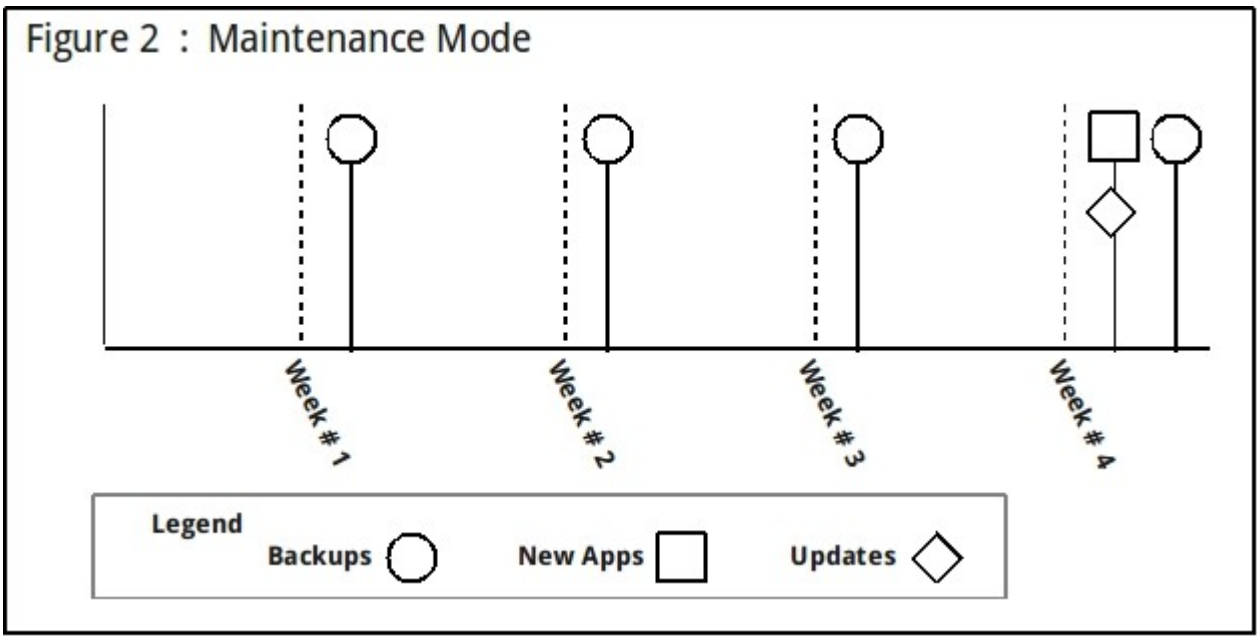
For the production operating system, it is recommended that an image backup be made for the operating system partition(s) immediately following the full configuration of the operating system. Full configuration means that the post-install upgrades have been performed and all of the user's applications and associated libraries have been installed. These image files should serve as the “gold standard” of the installation. It is recommended that they be retained in addition to the incremental backups that are run on a regular basis.

Figure 1 : Initial Installation



After the production operating system has undergone the initial updates and buildup of the additional applications, the operating system backup state will enter the maintenance mode phase. As reference earlier, in this state, backups are run on a regular frequency (recommended – weekly) with infrequent updates. Figure 2 illustrates one approach to this backup level.

Figure 2 : Maintenance Mode



Fsarchiver Backup Application Overview:

In this version of the backup strategy, fsarchiver replaces partimage as the principal backup engine. The application offers a large number of options or switches for it's use. Some of the more basic options will be covered below.

Fsarchiver is included in some Linux repositories for installation into an active operating system. Consult your package manager to see if it is included. The application can be downloaded and built from the source files for installation. The easiest way to acquire and use fsarchiver is to download and install to a CD the latest stable release of the tool set System Rescue CD. The System Rescue CD will contain a bootable CD with a number of applications.

Fsarchiver Application Use – Preparation:

Before using Fsarchiver with the SystemRescue CD, the following will need to be done:

1. The image file of SystemRescue should be burned to a CD.
2. The computer BIOS must be set to boot to a CD /DVD
3. The identification label for the hard drive partition that will store the backup files must be known (i.e. sda4, sdb7 etc.).
4. If a subdirectory (folder) is to be the final destination for the backup files, it's total path must be known (i.e. /sda7/backups/images).

Fsarchiver Application Use – Making Backups:

Boot up using the SystemRescue LiveCD. At the initial list of options select the option specific for the PC hardware. If the processor supports 64 bit architecture, it is recommended to select that option.

Proceed through the dialogs confirming the keyboard layout etc. At the end of the initialization there should be some text describing some of the features and options that are built into the SystemRescue package. At this point the user can either continue in the raw terminal mode or they can move to a graphical mode. For the graphical mode, at the prompt enter:

root @ systemrescue /root% **startx**

This command will start a graphical X environment. Maximize the terminal window and proceed with the following commands (these commands apply in both the graphical mode as well as the raw terminal mode).

The first task is to establish a local mount point for the partition that will receive the backup files to be created. For this illustration, a mount point will be created called BUHDA (abbreviation for Backup Hard Drive A).

root @ systemrescue /root% **mkdir /media/BUHDA**

Hint : Keep the naming conventions short and avoid spaces and special characters.

Next the actual hard drive partition needs to be mounted to the mount point established above. For this example sdb7 will be used.

root @ systemrescue /root% **mount /dev/sdb7 /media/BUHDA**

After the mount point has been established and the actual receiving partition mounted, the actual backups can start. The basic protocol of the fsarchiver backup command is

[fsarchiver] [fsarchiver backup mode] [option switches] [destination] [source]

For the following examples, sda1 will be the partition to be backed up

A simple backup with no options:

```
root @ systemrescue /root%
fsarchiver savefs /media/BUHDA/sda1-backup.fsa  /dev/sda1
```

Explanation for the above:

The “savefs” is the fsarchiver mode for creating backups. In this example no option switches were identified. The “/media/BUHDA/sda1-backup.fsa” identifies the full path and filename for the created backup. The “/dev/sda1” identifies the partition to be backed up.

Hint : If you are going to create regular backups into the same destination partition, it is suggested to use a more intuitive naming convention. For example in the weekly backups that I run the destination filename follows the format of “/media/BUHDA/sda1-20101029.fsa” . The “20101029” is a shortened version of the backup date (YYYYMMDD). Again, avoid very long names and avoid spaces and special characters.

A 64 bit sample backup with some options:

```
root @ systemrescue /root%
fsarchiver savefs -vj4z5 /media/BUHDA/sda1-backup.fsa  /dev/sda1
```

Explanation of the switches:

The “v” represents the verbose mode. With this switch enabled, you will be able to see the specific files and directories that are written to the backup file. Additionally, you will see the percentage completion. Without this switch enabled, the backup is run in silent so no output will be presented until the entire backup has finished.

The “j4” switch directs the number of processors dedicated to the backup compilation. Since the environment is the SystemRescue Live CD, there are no other processes running so it makes sense to allocate all of the available resources to the backup generation.

The “z5” denotes the compression level used in creating the backup. The higher the compression, the smaller the output file. Additionally, the higher the compression, the longer it wlll take to generate the backup file.

There are a number of other backup options that are available. It is recommended that the Fsarchiver web site be accessed for a complete explanation of all available switches.

Terminal Use Hint : If the user is backing up multile partitions, use the ↑ cursor key to bring up the last command. Modify the origination and destination partition id's and click <Enter>.

Fsarchiver Application Use – Restoring from a Backup:

Before initiating a recovery, it is imperative that the partition where the recovery will be written to be at least the same size as the original partition. Additionally, as is the case with most backup restorations, all data in the partition before the backup starts will be permanently lost. If there are any files or directories that need to be retained, copy them to another media or partition location on the hard drive before starting the restoration.

For the following example, it is assumed that the partition to be restored is sda2. The backup file is located in sdb7.

After booting to the SystemRescue Live CD, create a mount point for the partition that contains the backup file.

root @ systemrescue /root% **mkdir /media/BUHDA**

root @ systemrescue /root% **mount /dev/sdb7 /media/BUHDA**

The actual restoration is accomplished as

root @ systemrescue /root%
fsarchiver restfs -v /media/BUHDA/sda2-20101027.fsa id=1,dest=/dev/sda2

Note: There are **NO SPACES** in the "id=1,dest=/dev/sda2"

Using the "-v" switch, the user will be able to observe the progress of the restoration.

After the restoration has completed, closeout SystemRescue CD and restart the computer.

root @ systemrescue /root% **reboot**

As was the case in creating the restoration, consult the Fsarchiver website for additional options with respect to the partition restoration.

Conclusion:

The backup stategy presented above offers a viable disaster recovery solution for both operating systems as well as data specfic partitions. The controlled updates schedule puts the user back in control of their operation system while still providing the updates and upgrades required to maintain a secure and current operating system.

The main backup appplication (Fsarchiver) has proven to be a very capable and feature rich application. While the application is still under development and considered “experimental” it has performed very well in running weekly backups and several recoveries in both ext3, ext4 and ntfs filesystem partitions. As stated in the Disclaimer, the user assumes all responsibility for use of recommendations presented in this paper.

Resources:

RescueCD Home Page

Fsarchiver Home Page