Data Backup and Restore Component – Requirements

Michael Hager <*michael.hager@suse.de*>
Radim Gelner <*radim.gelner@suse.cz*>

Abstract

The purpose of the Requirements Specification is to define requirements for the Data Backup and Restore Component completely, consistently and unambiguously. These requirements should be agreed with the Product Management before passing on to the Design phase.

1 Environment

1.1 Software

Target for this component is common code base for SUSE Linux Enterprise Server 9 products (*CODE*) 9.

1.2 Hardware

1.2.1 Computer

The computer hardware requirements/compatibility are based on the requirements of CODE 9. The component will run with the lowest configuration required for CODE 9, i. e. computer with 1 CPU, 128 MB RAM and 512 MB HDD.

For the purpose of the definition of the component the computer with CODE 9 installed is planned to play role of:

- LAN or Internet server for a network of maximum 20 workstations.

1.2.2 Device

The component will use local hard drive and removable drive (optionally) (*device*) supported by CODE 9.

2 User

2.1 Skill Level

The component will be administered by person with minimal Linux knowledge and possibly basic Microsoft Windows administration skills. The configuration of the component will be performed exclusively in YaST supported user interfaces.

The component's interface must be simple enough, to allow the user to access at least rudimentary functions.

The restore in case of total system breakdown will be done by a skilled administrator using crash recovery features of CODE 9 and is out of scope of this component.

2.2 Language

The component will be operated by English or German speaking user. The language used will depend on the default language of CODE 9 and the visible subcomponents of the component will support it. Other subcomponents of the component will support at least English language. Extended language support in the subcomponents is optional as well as the support of other languages than English and German.

3 Functions

3.1 Configuration

The configuration of the component and the detection of the device will be performed by YaST. The configuration of component's functions will allow the user to:

1. select and configure the device,

2. select one or more directories, files, soft and hard links to backup (*data*),

3. configure parameters of the backup and restore functions.

The above will form a configuration (*scenario*).

By default the data will include all the files and their contents, directories, soft and hard links and standard attributes (creation/access time and date, owner, group, etc.). Optionally other entities may be made part of data.

After the configuration the user will be able to initiate other basic functions of the component in just few single steps without any extra configuration.

3.2 Backup

The backup of the data will be initiated by the user interactively via YaST. Optionally or it will be able to run unattended at a scheduled time (cron-like with the standard input and output detached). The functionality in the unattended mode may be limited compared with the interactive mode.

By default all the files and their contents, directories, soft and hard links and standard attributes (creation/access time and date, owner, group, etc.) of the data will be backed up. For Posix ACL enabled file systems (reiserfs, ext2, ext3) the ACL will be backed up. Optionally other entities may be backed up.

Component will support splitting of the archive into the set of smaller parts (*chunks*).

Component will support software compression of the archive during backup.

Component will support encryption of the archive.

3.3 Restore

The restore of the data will be initiated by the user interactively via YaST. It is expected the system will be in a working state before the data restoration. The component is not meant to provide system crash recovery functions.

By default all the files and their contents, directories, soft and hard links and standard attributes (creation/access time and date, owner, group, etc.) from the archive will be restored. For Posix ACL enabled file systems (reiserfs, ext2, ext3) the ACL will be restored. Optionally other entities may be restored.

Component will support restore from the incomplete set of the chunks of the archive.

Component will support software decompression of the archive during restore.

Component will support decryption of the archive.

The component itself, its restore function or 3rd party tool able to process the archive and restore the data from it will be included as a part of the rescue system of products based on CODE 9.

Optionally the archive processing will be possible with the standard administration tools of CODE 9.

4 Performance

The components throughput of the compressed data via SCSI or IDE tape drive and local hard drive will be larger than 1 MB/sec under standard system conditions.

The throughput of the compressed data may be lower than the throughput of the uncompressed ones.

5   Security

The component will run with superuser permissions. Only superuser will be allowed to run it.

Optionally the component will run without superuser permissions too.

6   Constraints

There will be single backup or restore process running at the give time. Running multiple instances will not be possible.

The archive format will be compatible with previous versions of the component.

The component will be operated by superuser only.

Maximum expected volume of data will be 20 GB.

The largest supported chunk size will be 5 GB. The default chunk size will be 512 MB. For clarity: the uncompressed data of 20 GB will produce 40 chunks 512 MB each neglecting the archive meta data.

The swapping of the media in the device will not be supported.