

SysAdmin Notes for RHCSA

Somenath Sinha

August 2017

Chapter 1

Using Essential Tools

1.1 Man Command

man followed by *keyword* yields the manual page of that command.

```
1      $ man ls
```

man followed by option **-k** (for keyword) and then followed by a *keyword* yields a list of all the commands containing that keyword and a brief description of that command.

```
1      $ man -k day
2      daylight (3)          - initialize time conversion information
3      dysize (3)           - get number of days for a given year
4      daylight (3p)        - set timezone conversion information
5      gettimeofday (2)     - get / set time
6      gettimeofday (3p)   - get the date and time
7      motd (5)             - message of the day
8      Net::Time (3pm)      - time and daytime network client interface
9      settimeofday (2)     - get / set time
10     Time::HiRes (3pm)    - High resolution alarm, sleep, gettimeofday, interval
↔ timers
```

The numbers next to the commands indicate which section of the man pages the command belongs to (based on their functionality). The actual section that the commands belong to can be determined by the use of

```
1      $ man man-pages
```

The relevant sections for SysAdmins are Section 1, 5 & 8. The sections are:

Section Number	Deals with	Description
1	Commands (Programs)	Those commands that can be executed by the user from within a shell.
2	System calls	Those functions which must be performed by the kernel.
3	Library calls	Most of the libc functions.
4	Special files (devices)	Files found in /dev.
5	File formats and conventions	The format for /etc/passwd and other human-readable files.
6	Games	
7	Overview, conventions, and miscellaneous	Overviews of various topics, conventions and protocols, character set standards, and miscellaneous other things.
8	System management commands	Commands like mount(8), many of which only root can execute.

To filter down the output of the **man -k** command, we can use **grep** to obtain only the relevant parts of the result on the basis of the appropriate section number in the man-pages.

This can be achieved using the pipe which feeds the output of the first command to the input of the second command.

```

1      $ man -k day | grep 3
2      daylight (3)          - initialize time conversion information
3      dysize (3)            - get number of days for a given year
4      daylight (3p)         - set timezone conversion information
5      gettimeofday (3p)     - get the date and time
6      Net::Time (3pm)       - time and daytime network client interface
7      Time::HiRes (3pm)     - High resolution alarm, sleep, gettimeofday, interval
↪   timers

```

1.2 Understanding Globbing and Wildcards

- * - Indicates any string.
- ? - Indicates any single character.
- [...] - Indicates any character provided within brackets.
- [!...] - Indicates any character *NOT* provided within brackets.
- [a-f] - Indicates any character provided within the range of a to f.

1.3 Understanding Globbing and Wildcards

- \$ ls a* - Lists all files and folders (including contents of each folder) that start with "a"
- \$ ls *a* - Lists all files and folders that contain the string "a".
- \$ ls -d a* - Shows all files and folders that start with "a" but excludes the contents of each individual folder.
- \$ ls ??st* - Lists all files and folders that have "st" as the 3rd and the 4th character in their name.
- \$ [a-f] - Indicates any character provided within the range of a to f.

1.4 Understanding I/O Redirection and Pipes

1.4.1 I/O Redirection

File Descriptors:

STDIN	-	0	-	Standard Input	-	Represents the "file" for the Standard Input Device (generally Keyboard).
STDOUT	-	1	-	Standard Output	-	Represents the "file" for the Standard Output Device (generally the Monitor).
STDERR	-	2	-	Standard Error	-	Represents the "file" for the Standard Output Device (also, generally the Monitor).

Redirection:

STDIN	-	<	-	Feeds the file to the right of the "<" as input to the command on the left.
STDOUT	-	>	-	Stores the output of the command to the left of the ">" to the file indicated on the right. <i>OVERWRITES</i> the mentioned file.
STDOUT	-	>>	-	Stores the output of the command to the left of the ">>" to the file indicated on the right. <i>APPENDS</i> the mentioned file.
STDERR	-	2 >	-	Redirects the errors from the command mentioned on the left to the file on the right. <i>OVERWRITES</i> the mentioned file.

```
1      $ mail -s hi root < .
2      $ ls > myFile
3      $ ls -lh >> myFile
4      $ grep hi * 2> /dev/tty6
```

1 - *mail* is a simple command used to send messages. The command expects the message to terminate with a ".", so we feed it directly to the command, instead of providing any input.

4 - The STDERR is redirected to tty6 (a virtual terminal connected to the host). Can also be diverted to a file if needed, such as an errorLog.

1.4.2 Piping

The command `$ ps aux` shows us the overview of all the running processes on the host. However, it's too long to view all at once. In such situations, or wherever we need to feed the output of the first command to the input of the second command, we use the pipe operator. The command would then be `$ ps aux | less`.

The difference in the usage of the piping and redirection operators is that Pipe is used to pass output to another program or utility, while Redirect is used to pass output to either a file or stream.

1.5 Using I/O Redirection and Piping

```
1      $ ps aux | awk '{print $2}'
2      $ ps aux | awk '{print $2}' | sort
3      $ ps aux | awk '{print $2}' | sort -n
```

The second column (\$2) of the `$ ps aux` command contains the Process ID (PID), and if we only want to filter the output such that only the PID is shown, we simply use the **awk** filtering utility.

If we want to sort the output of the command, we use the **sort** utility, but it generally sorts as a string. To sort the output as a number, we use the option **sort -n**.

If you expect lots of errors for a particular command, but want to discard all errors and only see the output when successful, then simply redirect the STDERR to `/dev/null`, which is a special device that discards all data written to it, i.e., a dustbin for data.

```
1 $ find / -name "*.rpm"
2 $ find / -name "*.rpm" 2> /dev/null
```

The first command shows all output including errors, but the second command discards all errors and shows the rest.

```
1 $ some_command > /dev/null 2> &1
```

The above code redirects STDOUT to `/dev/null` thus destroying the output, and also redirects the STDERR (2>) to STDOUT (&1). Essentially, it discards all output - useful when we don't need the output but only need the command to execute.

```
1 $ ls / > file_list.txt
2 $ sort < file_list.txt > file_list_sorted.txt
```

The above command stores the contents of the root directory in *file_list.txt*. Then, the second command uses both input and output redirection! The input of the sort command is fed from *file_list.txt* and the corresponding output sent to *file_list_sorted.txt*.

Chapter 2

Essential File Management Tools

2.1 Understanding Linux File System Layout

root (/)	-	Contains all other directories.
-----------------	---	---------------------------------

/boot	-	Contains everything the system needs to start up
/usr	-	Contains program files
/etc	-	Contains configuration files
/home	-	Contains a user's files
/mnt	-	Used to manually mount devices
/media	-	Devices like optical discs get auto-mounted on the media directory

Unlike other OSs, the linux files system is designed as such that multiple devices can be mounted on the same file system hierarchy. Thus, it's possible to mount devices remotely as well!

2.2 Finding Files

The **find** command is used to find a file within a folder and its subdirectories. When the starting point of the search is the root directory (/) then find will search the entire file system. While the utility is extremely thorough, this may cause delays due to remote devices on the network mounted on the file system.

```
1      $ find / -name "passwd"
```

If you're trying to find the location of a binary file, a better command would be **which** command, as it directly shows the location of the binary, but be careful as it only works with binaries.

```
1      $ which passwd
2      /usr/bin/passwd
```

Contrastingly, the command **whereis** not only gives us the locaiton of the binary, but the location of the complete environment of the binary!

```
1      $ whereis passwd
2      passwd: /usr/bin/passwd /etc/passwd /usr/share/man/man1/passwd.1.gz
↪ /usr/share/man/man5/passwd.5.gz
```

Another similar utility is called **locate** which shows all files that have the string provided to it in its name. Note, however, that **locate** operates on a database, that must be updated (especially after the creation of a new file) to show relevant results.

```
1      # touch sinha
2      # ls
3      sinha
4      # locate sinha
5      /usr/share/vim/vim74/keymap/sinhala-phonetic_utf-8.vim
6      /usr/share/vim/vim74/keymap/sinhala.vim
7      # updatedb
8      # locate sinha
9      /home/somu/Documents/sinha
10     /usr/share/vim/vim74/keymap/sinhala-phonetic_utf-8.vim
11     /usr/share/vim/vim74/keymap/sinhala.vim
```

2.3 Understanding Links

inode - An inode is a datastructure that describes a file system object such as a file or a directory, containing both the disc block locations as well as the attributes of the file system object. The inodes are identified by their inode number.

Consequently, for us to access the files/directories, we need to be able to provide a name to the inodes, which are called hardlinks. A file may have more than one hardlink. Note that each hardlink is simply a different name provided to the same inode. Thus, all hardlinks to the same file/directory have the same inode number. Hardlinks are one-directional only, i.e., the hardlink itself knows which inode it points to, but the inodes only know the total number of hardlinks that are associated with it, and not which exact ones are pointing to it. Since hardlinks point to some inode, they always need to stay on the same partition as the inode.

A symbolic link on the other hand, points to a hardlink instead of an inode. As such, it has a different inode number than the one that the hardlink points to. Thus, the hardlink and symbolic link can be on different partitions as well. It can even exist across servers. Whenever a hardlink is deleted, however, all the symbolic links pointing to it are rendered invalid.

2.4 Working with Links

The **ln** command is used to create both hardlinks and symbolic links. To create a symbolic link, we need only add the **-s** option. The **-i** option of the **ls** command shows us the inode number.

```
1      # ln /etc/hosts computers
2      # ls -il /etc/hosts computers
```

```

3      8388733 -rw-r--r--. 2 root root 158 Jun  7  2013 computers
4      8388733 -rw-r--r--. 2 root root 158 Jun  7  2013 /etc/hosts
5      # ln -s computers newcomputers
6      # ls -il /etc/hosts computers newcomputers
7      8388733 -rw-r--r--. 2 root root 158 Jun  7  2013 computers
8      8388733 -rw-r--r--. 2 root root 158 Jun  7  2013 /etc/hosts
9      27604468 lrwxrwxrwx. 1 root root   9 Sep  7 19:26 newcomputers -> computers
10     # rm -f computers
11     # ls -il /etc/hosts newcomputers
12     8388733 -rw-r--r--. 1 root root 158 Jun  7  2013 /etc/hosts
13     27604468 lrwxrwxrwx. 1 root root   9 Sep  7 19:26 newcomputers -> computers
14     # exit
15     exit
16     $ ln /etc/shadow mydata
17     ln: failed to create hard link 'mydata' => '/etc/shadow': Operation not permitted
18     $ ls -l /etc/shadow
19     ----- 1 root root 1375 Sep  5 21:04 /etc/shadow

```

When the hardlink *computers* to the inode associated with */etc/hosts* is deleted, the associated symbolic link of *newcomputers* becomes invalid.

Finally, RHEL 7 onwards, a user may only create a link to a file/directory that it at least has a read permission to. Thus, any user won't be able to create a link to */etc/shadow* as it has no permissions for anybody.

2.5 Working with tar

tar stands for Tape Archive. The command is most commonly used to make backups of files by storing them in archives. Some of the options of tar are:

- | | | |
|-----------|-----------------|---|
| -c | - create | - typically has an extension of .tar |
| -t | - show contents | - show contents of the archive. |
| -x | - extract | |
| -z | - file | - compress the archive using gzip. Typically has an extension of .tgz |
| -v | - verbose | - tell us what the utility is doing. |
| -f | - file | - option to indicate the name of the archive file. |
| -C | - location | - indicates where the archive is to be extracted. |

```

1      $ tar -cvf /root/etc.tar /etc

```

The above command creates the *etc.tar* archive in the */root* directory and puts the contents of */etc* in that archive. Note that the file *etc.tar* has a *.tar* extension only because we provided it, and not because Linux mandates it (unlike windows). Thus, sometimes we may run across tar archives that don't have an extension and are hard to detect. So, in that case we use the file command, which tells us the type of a particular file.

```

1      $ file /root/etc.tar
2      /root/etc.tar: POSIX tar archive (GNU)

```

Note that the *.tar* archive only puts all the files of the */etc* directory in the file *tar.tar*, but doesn't actually compress anything. To enable compression the *-z* option of the *tar* command must be used.

```
1 $ tar -czf /root/etc2.tgz /etc
```

Before extracting the contents of a tar file, we might want to see its contents, which can be done using the `-t` option of the `tar` command. *NOTE: Some older versions of `tar` may require the `-z` option to enable working with gzip archives, even when simply using the archive and not creating it.*

```
1 $ tar -tvf /root/etc2.tgz
```

To actually extract the archive, we use `-x` option. To indicate the location where we want the extracted files to reside, we include the `-C` option. If this option is not present then the files will be extracted in the present directory.

```
1 $ tar -xvf /root/etc2.tgz -C /tmp
```

To extract only one file from the archive, we can simply provide the name of the file at the very end.

```
1 $ tar -xvf /root/etc2.tgz -C / etc/wgetrc
```

NOTE that in the above command, we use the relative path `etc/wgetrc` because of the fact that the archive stores a relative file path for easy extraction in any folder.

Chapter 3

Working with Text Files

3.1 Understanding Regular Expressions

Character	Definition	Example	Result
^	Start of a string	^abc	abc, abcdef, abc123
\$	End of a string	abc\$	abc, blahabc, 456abc
.	Any character except newline	a.c	abc, aac, a2c
	Alteration	1 8	1,8
{...}	Explicit quantity of preceding character	ab{2}c	abbc
[...]	Explicit set of characters to match	a[bB]c	abc, aBc
(...)	Group of characters	(123){3}	123123123
*	Null or more of the preceding character	ab*c	ac, abc, abbbbc
+	One or more of the preceding character	ab+c	abc, abbbbc
?	Null or one of the preceding character	ab?c	ac, abc

PEARSON
IT CERTIFICATION

livelessons®
©2015 Pearson, Inc.

Figure 3.1: RegEx Cheat Sheet

3.2 Using common text tools

3.2.1 cat

The `cat` command prints the entire content of a file on to the terminal.

3.2.2 less

Sometimes the `cat` command is unsuitable, like in the case of extremely large files. In such cases, like the `/var/log/messages`, the default system log file, using `cat` won't work as the majority of the messages would scroll past fast. For such cases, `less` is a better utility. Search functionality is exactly the same as in the case of `vim`.

3.2.3 Head and Tail

Head

The `head` command by default shows us the first 10 lines of a text file. To see more or less lines, the `-n` option can be used.

```
1 $ head -n 20 file.txt
```

Tail

The `tail` command by default shows us the last 10 lines of a text file. To see more or less lines, the `-n` option can be used.

```
1 $ tail -n 5 file.txt
```

Combination of head and tail

The combination of these two commands can enable the viewing of text in between specific line numbers. The command below shows lines 16-20 of `file.txt`

```
1 $ head -n 20 file.txt | tail -n 5
```

3.2.4 cut

With the `cut` utility, we can print out a specific column from a text file. It assumes the columns are separated by Tabs. Which specific column is to be printed is set by using the `-f` option. For example, to only print the first column of a text file, we say:

```
1 $ cut -f 1 cities
```

To provide a different delimiter, such as ":" we use the `-d` option followed by the delimiter of our choice.

```
1 $ cut -f 1 -d : /etc/passwd
```

3.2.5 sort

This command sorts the input provided in the order of the ASCII table. That means numbers first, capital letters next and finally the lower case letters.

```
1      $ cut -f 1 -d : /etc/passwd | sort
```

To sort on the basis of a specific criteria:

- n - Sort on the basis of actual numerical value, instead of treating a number as a string.
- f - Sort in a case insensitive manner.

3.2.6 tr

The `tr` command replaces certain characters with certain other characters. Thus, it's frequently used in conjunction with pipes to modify the output of a command.

```
1      $ echo hello | tr a-z A-Z
2      HELLO
3      $ echo hello | tr [:lower:] [:upper:]
4      HELLO
```

3.3 grep

`grep` is a filtering utility that only prints those lines that contain a certain expression matching the pattern provided by a *RegEx*.

```
1      $ ps aux | grep tracker
2      somu      10450  0.0  0.4 469796  9000 ?        SNl  10:06   0:00
↪ /usr/libexec/tracker-miner-user-guides
3      somu      10465  0.0  0.6 536856 12012 ?        Sl   10:06   0:00
↪ /usr/libexec/tracker-store
4      somu      10611  0.0  0.7 779816 13108 ?        SNl  10:06   0:00
↪ /usr/libexec/tracker-extract
5      somu      10614  0.0  0.5 469800  9632 ?        SNl  10:06   0:00
↪ /usr/libexec/tracker-miner-apps
6      somu      10615  0.0  0.7 710160 13204 ?        SNl  10:06   0:00
↪ /usr/libexec/tracker-miner-fs
7      root      17396  0.0  0.0 112644   968 pts/0    R+   13:49   0:00 grep
↪ --color=auto tracker
```

Another use for `grep` is searching files. The syntax is `grep <filename-pattern> <search-directory>`.

To avoid errors notifying "is a directory", simply redirect errors to `/dev/null`.

```
1      $ grep lisa * 2> /dev/null
2      group:lisa:x:1001:
3      gshadow:lisa:!:
4      passwd:lisa:x:1001:1001::/home/lisa:/bin/bash
5      passwd-:lisa:x:1001:1001::/home/lisa:/bin/bash
```

```
6      services:na-localise      5062/tcp      # Localisation access
7      services:na-localise      5062/udp      # Localisation access
8      shadow:lisa:$6$0l/zSJkh$xjJNYNnj1rPs7Fq0hDwt8VucS0nLL82XrMYpmBnLF2DrzB2npFvCwxM9MJEHgCHCwvabCgEA17LK2aU0h9F
9      shadow-:lisa:password:17414:0:99999:7:::
```

3.3.1 wc

Counts the number of words, lines and characters.

- l** - Counts the number of lines
- w** - Counts the number of words
- m** - Counts the number of characters
- c** - Counts the number of bytes
- L** - Counts the length of the longest line

To see the number of matched lines using `grep`, simply use:

```
1      $ ps aux | wc
2      188      2344      19581
```

3.3.2 grep -l

`Grep` by default returns the name of the matching file followed by the matching lines. This output can be made more readable by `grep -l` which lists all the files in the directory that matches the criteria.

```
1      $ grep lisa * 2> /dev/null
2      group:lisa:x:1001:
3      passwd:lisa:x:1001:1001::/home/lisa:/bin/bash
4      services:na-localise      5062/tcp      # Localisation access
5      services:na-localise      5062/udp      # Localisation access
6      $ grep -l lisa * 2> /dev/null
7      group
8      passwd
9      services
```

3.3.3 grep -i

The `-i` flag turns the `grep` command case-insensitive!

```
1      $ grep lisa * 2> /dev/null
2      group:lisa:x:1001:
3      passwd:lisa:x:1001:1001::/home/lisa:/bin/bash
4      services:na-localise      5062/tcp      # Localisation access
5      services:na-localise      5062/udp      # Localisation access
6      $ grep -i lisa * 2> /dev/null
7      group:lisa:x:1001:
```

```

8      passwd:lisa:x:1001:1001::/home/lisa:/bin/bash
9      services:ltctcp          3487/tcp          # LISA TCP Transfer Channel
10     services:ltcudp          3487/udp          # LISA UDP Transfer Channel
11     services:na-localise     5062/tcp          # Localisation access
12     services:na-localise     5062/udp          # Localisation access

```

3.3.4 grep -R

The usage of the `-R` flag puts `grep` in recursive mode, where the utility searches for the file in each subfolder as well.

```

1      $ grep -iR lisa * 2> /dev/null
2      group:lisa:x:1001:
3      lvm/lvm.conf:          # If using external locking (type 2) and initialisation
↪ fails, with
4      passwd:lisa:x:1001:1001::/home/lisa:/bin/bash
5      Binary file pki/ca-trust/extracted/java/cacerts matches
6      Binary file pki/java/cacerts matches
7      ...

```

3.3.5 grep -v

`Grep` with a `-v` flag excludes the matching results. Here we can exclude the lines containing "Binary" using:

```

1      $ grep -iR lisa * 2> /dev/null | grep -v Binary
2      alternatives/jre_openjdk/lib/security/nss.cfg:handleStartupErrors =
↪ ignoreMultipleInitialisation
3      alternatives/jre_openjdk_exports/lib/security/nss.cfg:handleStartupErrors =
↪ ignoreMultipleInitialisation
4      brlTTY/fr-abrege.ctb:word civilisation          14-1236-16
5      brlTTY/fr-abrege.ctb:word civilisations          14-1236-16-234
6      brlTTY/fr-abrege.ctb:word généralisation          1245-1345-16
7      brlTTY/latex-access.ctb: brailleTranslator.capitalisation = "6dot"
8      brlTTY/latex-access.ctb:
9      passwd:lisa:x:1001:1001::/home/lisa:/bin/bash
10     sane.d/canon_pp.conf:# Set a default initialisation mode for each port. Valid
↪ modes are:
11     services:ltctcp          3487/tcp          # LISA TCP Transfer Channel
12     services:ltcudp          3487/udp          # LISA UDP Transfer Channel
13     ...

```

3.4 sed and awk basics

3.4.1 sed

`sed` is an old utility that's used to process text. Many of its functionalities can now be done using `grep` itself.

sed q

To see the first two lines of a file using sed we use:

```
1      $ sed 2q /etc/passwd
2      root:x:0:0:root:/root:/bin/bash
3      bin:x:1:1:bin:/bin:/sbin/nologin
```

sed -n

The `-n` flag makes sed print no output unless the `p` flag is also provided. Here, we use a Regular Expression `"root"` to match only a certain part of the text and then the `p` flag to print only if that criteria is matched.

```
1      $ sed -n /^root/p /etc/passwd
2      root:x:0:0:root:/root:/bin/bash
```

The above result could also be obtained with `grep "^root" /etc/passwd`.

Substitution with sed

Sed can be used to substitute text within a file using the `s` parameter. It's used as :

```
1      $ cat names
2      Somu
3      Arpi
4      Neha
5      Santy
6      Debu
7      $ sed -i 's/Santy/Dickwad/g' names
8      $ cat names
9      Somu
10     Arpi
11     Neha
12     Dickwad
13     Debu
```

The `-i` flag asks the modifications to be made in place. Otherwise the output (changed text) would've simply been displayed to the screen and then need to be redirected to a file for storage.

3.4.2 awk

awk is another utility that is especially useful when working with text files. It excels at operations like cutting out information.

Cutting out information using awk

For certain operations, the `awk` command is a lot more powerful than the `cut` utility. In the example below `cut` has a hard time recognizing the second field, while `awk` has no problem whatsoever!

```
1      $ ps aux | grep 'gdm'
2      root      1117  0.0  0.1 480248  4688 ?          Ssl  09:20   0:00 /usr/sbin/gdm
3      root      1333  0.8  1.2 328524 47220 tty1      Ssl+ 09:20   0:43 /usr/bin/X :0
↵ -background none -noreset -audit 4 -verbose -auth
↵ /run/gdm/auth-for-gdm-bgrBZH/database -seat seat0 -nolisten tcp vt1
4      root      1718  0.0  0.1 528944  5848 ?          Sl   09:20   0:00
↵ gdm-session-worker [pam/gdm-password]
5      gdm       1737  0.0  0.1 458088  4152 ?          Sl   09:20   0:00 ibus-daemon
↵ --xim --panel disable
6      gdm       1741  0.0  0.1 373560  5424 ?          Sl   09:20   0:00
↵ /usr/libexec/ibus-dconf
7      gdm       1745  0.0  0.2 438152  7772 ?          Sl   09:20   0:00
↵ /usr/libexec/ibus-x11 --kill-daemon
8      somu      12218 0.0  0.0 112664   972 pts/0    R+   10:47   0:00 grep
↵ --color=auto gdm
9      $ ps aux | grep 'gdm' | cut -f 2
10     root      1117  0.0  0.1 480248  4688 ?          Ssl  09:20   0:00 /usr/sbin/gdm
11     root      1333  0.8  1.2 328524 47220 tty1      Ssl+ 09:20   0:43 /usr/bin/X :0
↵ -background none -noreset -audit 4 -verbose -auth
↵ /run/gdm/auth-for-gdm-bgrBZH/database -seat seat0 -nolisten tcp vt1
12     root      1718  0.0  0.1 528944  5848 ?          Sl   09:20   0:00
↵ gdm-session-worker [pam/gdm-password]
13     gdm       1737  0.0  0.1 458088  4152 ?          Sl   09:20   0:00 ibus-daemon
↵ --xim --panel disable
14     gdm       1741  0.0  0.1 373560  5424 ?          Sl   09:20   0:00
↵ /usr/libexec/ibus-dconf
15     gdm       1745  0.0  0.2 438152  7772 ?          Sl   09:20   0:00
↵ /usr/libexec/ibus-x11 --kill-daemon
16     somu      12226 0.0  0.0 112664   968 pts/0    R+   10:48   0:00 grep
↵ --color=auto gdm
17     $ ps aux | grep 'gdm' | awk '{ print $2 }'
18     1117
19     1333
20     1718
21     1737
22     1741
23     1745
24     12248
```

Chapter 4

Connecting to a RHEL Server

4.1 Connecting to a Server with SSH

To connect to a server we use the `ssh` command. The Syntax is: `ssh <server-ip>`.

```
1      $ ssh 192.168.152.129
2      somu@192.168.152.129's password:
3      Last login: Mon Nov 13 12:37:26 2017 from 192.168.152.128
```

The default SSH port is **22**. To connect to SSH on a different port (common when server is exposed to the internet), is `ssh -p <port-number> <server-ip>`. Note that *if root login is disabled on the server*, we must also provide the username to login as. The syntax then becomes : `ssh -p <port-number> <username>@<server-ip>`.

```
1      $ ssh -p 2022 sander@ldap.rhatcertification.com
```

4.2 RSA Key fingerprint and known hosts

Upon each new connection the `ssh` daemon shows us the RSA key fingerprint of the host to verify if we're connecting to the right computer. If so, the host is added to a list of known hosts permanently, in `~/.ssh/known_hosts`.

When the key fingerprint of the server doesn't match the Key fingerprint on record, the system warns us from connecting! This may occur when the server has been reinstalled on the same IP address. Thus, the new key fingerprint won't match the old one. To fix this, simply remove the old entry from `~/.ssh/known_hosts`.

4.3 sshd_config

The details of the method of connection to a server is stored in the **sshd_config** file, located in `/etc/ssh/sshd_config`.

Some of the options are:

Option	Description	Default Value
Port	The port number which is used for SSH on that server	22
PermitRootLogin	Whether an user is allowed to login as <i>root</i> user via SSH	yes

If the root login on the server via SSH is disabled, it generally makes the server a little bit more secure!

4.4 Understanding SSH keys

To initiate the ssh connection, the **SSHD** service on the server is contacted by the client. In order to confirm it's identity, the server responds with it's own `/etc/ssh/ssh_host.pub` public key to the client. When the client's user has verified the key of the server, the public key fingerprint gets stored in the clients `~/.ssh/known_hosts` file. Finally, the user is asked for the password to log on to the server.

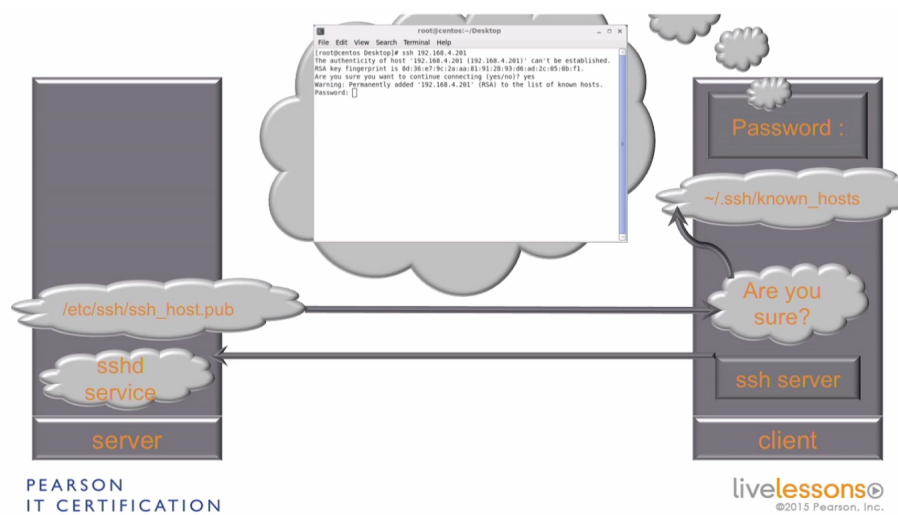


Figure 4.1: Server Authentication procedure

4.4.1 Client authentication without password

The client can also prove it's identity without a password by the use of a public key that it provides to the server. The private key of the user is stored in the home directory of the user `~/.ssh/id_rsa`. A packet encrypted with the private key is sent to the server which knows the user's public key. Some complex calculations based on this is performed on the authentication token sent from the client and if the identity is confirmed, then the user is logged in without needing a password.

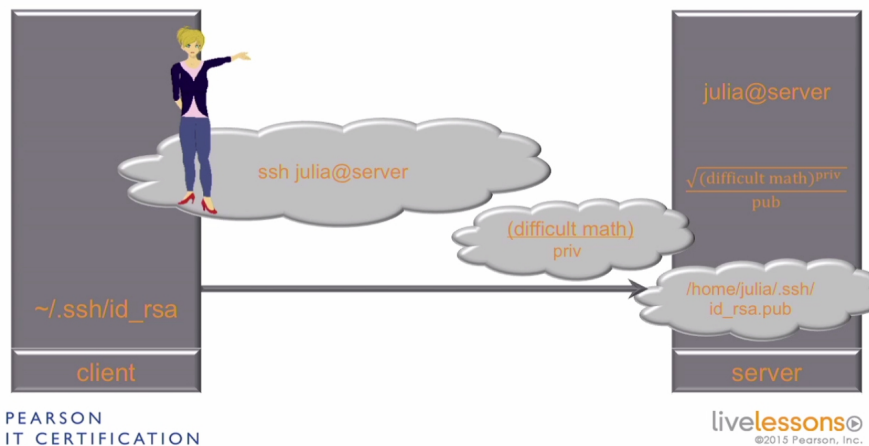


Figure 4.2: Public Key Client Authentication without password.

4.5 Using SSH Keys

SSH keys can be used to authenticate an user instead of a password. The private-public key pair can be generated using the `ssh-keygen` utility.

```

1      $ ssh-keygen
2      Generating public/private rsa key pair.
3      Enter file in which to save the key (/home/somu/.ssh/id_rsa):
4      Enter passphrase (empty for no passphrase):
5      Enter same passphrase again:
6      Your identification has been saved in /home/somu/.ssh/id_rsa.
7      Your public key has been saved in /home/somu/.ssh/id_rsa.pub.
8      The key fingerprint is:
9      SHA256:0C5uEHnAgJvzFEc0ulflL1YSyGT/YF5Utl9lweTfPDac somu@vmPrime.somusysadmin.com
10     The key's randomart image is:
11     +---[RSA 2048]-----+
12     |  ..==.   ooo .E. |
13     |  . .++o.oo+ + o.o|
14     |  o.oo++o..B . *o|
15     |+ ...==. o o  +|
16     |  +. o +oS .    |
17     |  . . o .      |
18     |    o          |
19     |    .          |
20     |               |
21     +----[SHA256]-----+

```

4.5.1 Copying SSH keys

The SSH keys generated on the client now have to be copied to the server which requires authentication. This can be done using `ssh-copy-id`.

```

1      $ ssh-copy-id 192.168.152.129
2      /usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
↪ out any that are already installed
3      /usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are
↪ prompted now it is to install the new keys
4      somu@192.168.152.129's password:
5
6      Number of key(s) added: 1
7
8      Now try logging into the machine, with:  "ssh '192.168.152.129'"
9      and check to make sure that only the key(s) you wanted were added.
10
11     $ ssh 192.168.152.129
12     Last login: Wed Nov 15 11:59:03 2017 from 192.168.152.128

```

While previous versions of `ssh-copy-id` didn't support specifying a port number, RHEL 7 onwards this feature is supported.

```

1      $ ssh-copy-id -p 2022 sander@ldap.rhatcertification.com

```

In case the public key is not recognized, it is possible to specify the public key using the `ssh-copy-id -i <publicKeyFile.pub>` flag.

4.5.2 Copying files to a server securely using SSH

Files can be copied to a server using SSH connection using the `scp` (secure copy) utility.

```

1      $ scp -P 22 names 192.168.152.129:~
2      names                                100%   28      8.1KB/s   00:00

```

NOTE that the directory on which the file has to be copied to on the server, (in this case the directory) has to be specified for the copy to be successful. Otherwise, `scp` just creates a local copy of the file with the name of the server as the filename.

Also, if the port has to be specified, the flag is `-P` which is in capital unlike `ssh` and `ssh-copy-id`.

Chapter 5

Managing Users and Groups

5.1 Understanding the need for Users

User accounts are not just to ensure that different people use resources with accountability and resource management. Several processes also have to execute with permissions given to them by their respective user accounts.

For example, the apache web server's processes and services execute under the permissions given to the apache account. This account doesn't have root privileges, which ensures that in case of security breaches of the apache user account, the culprit doesn't gain access to any critical resources that only an administrator or the root account should have access to.

5.2 User Properties

5.2.1 Username

A typical user info in the `/etc/passwd` file consists of the login information of several users, each with the following details :- `somu:x:1000:1000:Somu:/home/somu:/bin/bash`. Here, Somu is the username, the `x` in the second field references that a password has been stored for that username in the `/etc/shadow` file. The file contains the (one-way) encrypted password as well as several password related information such as password expiration dates, etc. Since the `/etc/shadow` file is only readable by the root user, it minimizes the security risk. Generally, only real user accounts need a password and system users (accounts used by processes to execute) don't.

`/etc/shadow`

While the `/etc/shadow` file contains the password of an user in an encrypted format, if the user account is new and doesn't yet have any password assigned to it, then the entry for it in `/etc/shadow` looks like:

```
1 $ cat /etc/shadow | grep lisa
2 lisa:!!:17485:0:99999:7:::
```

The second entry (!) is where the encrypted password is usually stored. The double exclamation indicates that the *lisa* account hasn't set up a password yet.

5.2.2 UID

Each user on the system is setup with a unique UserID (UID). The root has a UID of 0, and normal users start with an UID of 1000 onwards. There are a total of 64,000 UIDs available for 2.4 kernels, and 4 billion for 2.6 kernels.

5.2.3 GID

On Linux, every user must be the member of at least one group, which is known as the **primary group** of the user, stored in the `/etc/passwd` file. On RHEL, that primary group has the same name as the username and the user is the only member of that group by default (i.e., private group). The list of Groups is stored in a file called `/etc/group`.

5.2.4 GECOS or comment field

This is a comment field that can contain anything the admin deems necessary. It generally contains information that makes the identification of each user easier.

5.2.5 Home Directory

The home directory refers to the location where the user is allowed to store files. For services, this folder is important because it defines the directory where the service can read and write files. While for regular users the home directory is typically inside `/home`, for services, they can be anywhere.

5.2.6 Default Shell

This is the shell (or command) that is executed on login of the user. The default value is `/bin/bash`.

5.3 Creating and Managing Users

5.3.1 Adding users

The default command for adding users on RHEL is `useradd`.

Option	Description
-e	Expiration date in the format YYYY-MM-DD. Sets the date on which the user account will be disabled.
-c	Comment that sets the contents of the GECOS field.
-s	Sets the default shell of the user. For example, a C programmer can use a shell such as TCSH.

```

1      $ sudo useradd -c "New Test User" -s /bin/tcsh -e 2017-12-31 laura
2      [sudo] password for somu:
3      $ # To verify the addition of the new user
4      $ tail -n 1 /etc/passwd
5      laura:x:1001:1001:New Test User:/home/laura:/bin/tcsh

```

id command

The `id` command prints the real and effective user information.

```

1      $ id
2      uid=1000(somu) gid=1000(somu) groups=1000(somu)
↔ context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023

```

5.4 Understanding Group Membership

Groups are especially useful to enable users to share files with one another. These groups may be additional groups known as secondary groups.

The `/etc/passwd` file doesn't contain any reference to the secondary groups that the user is a part of, even though the `/etc/group` file lists that user as a member. Thus, the best way to obtain the groups the user is a part of is by using the `id` command.

```

1      $ id lisa
2      uid=1002(lisa) gid=1002(lisa) groups=1002(lisa), 5009(sales)

```

5.5 Creating and Managing Groups

5.5.1 groupadd

The `groupadd` command is used to add a new group.

Option	Description
-g	Specify the GID of the group.

5.5.2 Adding users to a group

A user can be added to a group by directly editing the `/etc/group` file, or by using the `moduser` command.

usermod

Option	Description
-g	Force assign the GID as the new default group of the user.
-G	Erase older list of supplementary groups and assign the given groups as the supplementary group of the user.
-a	Add the given group to the list of groups for the user.

Adding a user to a group using the usermod command is shown below.

```
1 $ sudo usermod -aG account laura
2 $ sudo usermod -aG 5010 lisa
3 $ tail -n 1 /etc/group
4 account:x:5010:laura,lisa
```

5.6 User and Group configuration files

Some of the important configuration files are:

Option	Description
/etc/passwd	Contains several details of the user, other than the password.
/etc/shadow	Contains the password hash and password properties for the user.
/etc/group	Contains the names of all the groups along with a list of all users in them.
/etc/login.defs	Contains the values (definitions) of several parameters used to create the user, such as password max days, min days, etc.
/etc/default/useradd	Contains the default values for several useradd parameters.
/etc/skel	When a user's home directory is created, the contents of /etc/skel is copied there, with the appropriate group of the user.

5.7 Managing Password properties

The user *root* can manage the password properties using two commands:

5.7.1 passwd

Option	Description
-d	Delete the current password.
-l	Lock the current password.
-u	Unlock the current password.
-e	Expire the current password - force user to change password during next login.
-x	Set the maximum lifetime of the password.
-n	Set the maximum lifetime of the password.
-w	Set days before expiration the user is warned.
-i	Set days after expiration the user account becomes inactive.

Locking and Unlocking passwords

```
1      $ sudo passwd -l laura
2      Locking password for user laura.
3      passwd: Success
4      $ su - laura
5      Password:
6      su: Authentication failure
7      $ sudo cat /etc/shadow | grep laura
8      laura:!!$6$0zDhsJet$q2...KRVKv8D2.:17486:0:99999:7::17531:
9      $ sudo passwd -u laura
10     Unlocking password for user laura.
11     passwd: Success
12     $ sudo cat /etc/shadow | grep laura
13     laura:$6$0zDhsJet$q2...KRVKv8D2.:17486:0:99999:7::17531:
14     $ su - laura
15     Password:
16     Last login: Thu Nov 16 13:40:45 IST 2017 on pts/0
17     $ whoami
18     laura
```

When an account is locked, the password hash for that user in the `/etc/shadow` file is prefixed with a `!!` to render it invalid and prevent authentication from succeeding (unless the root logs in as that user, which requires no password prompt).

5.7.2 chage

Option	Description
-l	List all password aging information.
-E	Set the account expiration date.
-m	Set the maximum lifetime of the password.
-M	Set the maximum lifetime of the password.
-W	Set days before expiration the user is warned.
-I	Set days after expiration the user account becomes inactive.

Setting the account expiration date

```
1      $ sudo chage -E 2017-12-31 laura
2      [sudo] password for somu:
3      [somu@cliServer ~]$ sudo cat /etc/shadow | grep laura
4      laura:$6$0zDhsJet$q2...KRVKv8D2.:17486:0:99999:7::17531:
5      $ sudo chage -l laura
6      Last password change                : Nov 16, 2017
7      Password expires                    : never
8      Password inactive                   : never
9      Account expires                     : Dec 31, 2017
10     Minimum number of days between password change : 0
11     Maximum number of days between password change : 99999
12     Number of days of warning before password expires : 7
```

The string `17531` represents the account expiration date in epoch time (seconds since Jan 1 1970).

Chapter 6

Connecting to a LDAP Server

6.1 Understanding LDAP

LDAP is an easy way to provide centralized authentication from a server. This way, many computers can be connected to a single LDAP server and the user accounts (and permissions) have to be set up only once!

LDAP stands for *Lightweight Directory Access Protocol*. It connects us to a hierarchical directory server. In the hierarchy (e.g., server.rhatcertification.com), there are top level domains such as .com, subdomain (rhatcertification) and leaf objects (lisa). Even though the structure is similar to DNS, the notation of LDAP is different. For every container object, we write dc=<objectName> (dc → Domain Component) and for leaf objects, it becomes cn=<objectName> (cn → Common Name). The complete format then becomes cn=lisa,dc=rhatcertification,dc=com.

An important part of connecting to an LDAP server is the **base context**. The base context, like the search domain of DNS, is the starting point where our client should look for objects. In this case, the base context is dc=rhatcertification,dc=com. Thus, for logging in to a server, the cn(lisa) is searched for within the base context.

6.1.1 /bin/login

The login service is used whenever the user requires authentication to connect to anything.

6.1.2 ldd

The ldd command (List Dynamic Dependencies) prints all the shared libraries required by a program.

```
1      $ ldd /bin/login
2      linux-vdso.so.1 => (0x00007ffc333e3000)
3      libpam.so.0 => /lib64/libpam.so.0 (0x00007f85cad8a000)
4      libpam_misc.so.0 => /lib64/libpam_misc.so.0 (0x00007f85cab86000)
5      libaudit.so.1 => /lib64/libaudit.so.1 (0x00007f85ca95d000)
6      libselinux.so.1 => /lib64/libselinux.so.1 (0x00007f85ca736000)
7      libc.so.6 => /lib64/libc.so.6 (0x00007f85ca373000)
```

```

8      libdl.so.2 => /lib64/libdl.so.2 (0x00007f85ca16e000)
9      libcap-ng.so.0 => /lib64/libcap-ng.so.0 (0x00007f85c9f68000)
10     libpcre.so.1 => /lib64/libpcre.so.1 (0x00007f85c9d06000)
11     /lib64/ld-linux-x86-64.so.2 (0x0000558e5f0bd000)
12     libpthread.so.0 => /lib64/libpthread.so.0 (0x00007f85c9ae9000)

```

The PAM library shown above (libpam) is akin to a plugin that adds additional functionality to the `login` utility (as well as several others). PAM stands for *Pluggable Authentication Modules*. The configuration files for the authentication module is stored in `/etc/pam.d` directory. The `/etc/pam.d/login` is the configuration file for `login` utility.

6.1.3 PAM config file syntax

The PAM config files are each named after the services that require the usage of PAM. For example, the config file for the `login` service is called `/etc/pam.d/login`. Each file lists a bunch of rules in the syntax: `<service-type> <control> <module-path> <arguments>`.

Service Type

Service Type	Description
auth	Deals with user authentication via password (or other means like keys).
account	Non-authentication based account management.
password	Updating the authentication token of the user.
session	Modules listed here are used for setup/cleanup of a service for the user.

PAM Module Controls

Control	Description
requisite	Immediately causes failure when the module returns a status that isn't 'success'.
required	If the service returns a non-success status, then the operation fails ultimately, but only after the modules below it are invoked. This is to prevent a person with malicious intent from gaining knowledge of which module failed.
sufficient	If a <i>sufficient</i> module returns a 'success' status, the other modules below it that are also a part of 'sufficient' management group will not be invoked. In case of failure, another module listed 'sufficient' in the stack below it must succeed for the operation to succeed.
optional	Only causes failure if the rule stack contains only optional modules and all fail.
include	For the given service type, include all lines of that type from the provided configuration file.
substack	Same as <i>include</i> but when <i>done</i> and <i>die</i> actions are evaluated, they only cause skipping of the substack.

The `login` config file in `/etc/pam.d` contains the line:

```

1      auth      substack      system-auth

```

NOTE : the entry for `pam_ldap` requires that the host should be able to use LDAP, which requires `pam_ldap` to be installed, and `authconfig-tui` to be executed.

The `system-auth` file has rules for the common login procedure for any any process that deals with user authentication. This file in turn contains the lines :

1	auth	sufficient	pam_unix.so nullok try_first_pass
2	...		
3	auth	sufficient	pam_ldap.so use_first_pass

The line `auth sufficient pam_unix.so` tells the system to look at the System login local authentication mechanism (`pam_unix.so`). If that is not successful, the system is instructed to use the LDAP PAM mechanism (in `pam_ldap.so`). Thus, the login process is contacting an LDAP server and trying to verify if the user account exists on that server.

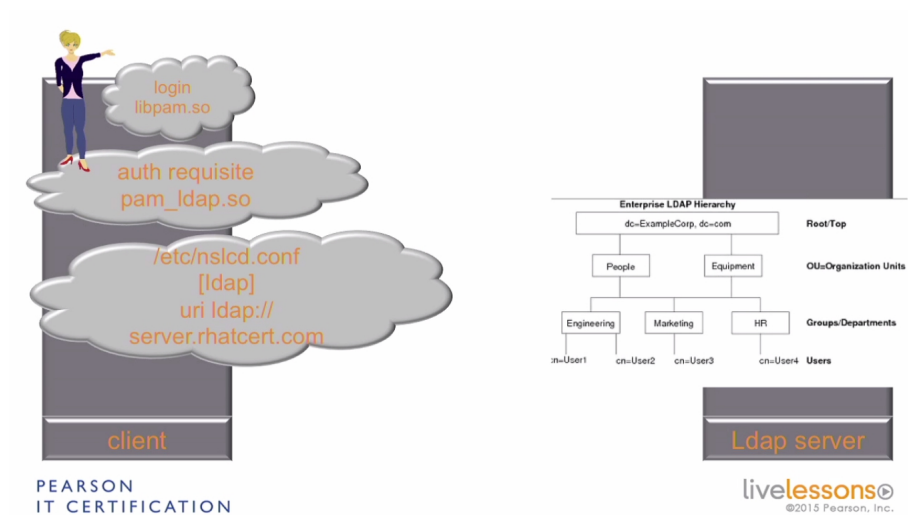


Figure 6.1: LDAP Authentication

Next, the LDAP configuration file (`/etc/nslcd.conf`) is read, which contains the URI of the LDAP Server (`ldap://server.rhatcert.com`). Finally, the client is able to connect to the LDAP server where there is a LDAP hierarchy that it can log into.

6.2 Telling your server where to find the LDAP Server

6.2.1 nscd

The Naming Service Cache Daemon needs to be installed to configure the connection of a server to an external LDAP server. It is the part of the OS that caches the information from external authentication mechanisms on the local machine.

6.2.2 nss-pam-ldapd

This sets up the local name resolution and local authentication and connects it to LDAP services.

6.2.3 pam_ldap

The libraries needed to make the local authentication aware of LDAP services.

6.2.4 authconfig-gtk

authconfig is an utility used to setup the server for external authentication. There are several variations of it, such as authconfig, authconfig-tui and authconfig-gtk (GUI based).

LDAP Search Base DN

The search base DN consists of Domain Components (dc) with commas as separators. Example : dc=rhatcertification.com,dc=com.

LDAP Server

The server needs to have a matching certificate to the one that the client receives on connection. This is only possible with a domain name, and not an IP address. The reason for this is the server name has to match the one in the certificate and the certificate can only have one name associated to it.

TLS Certificate

The use of a Transport Layer Security (TLS) certificate is important because unless it's used, the LDAP password is sent across the network unencrypted, which makes the entire system vulnerable. We also need to download the TLS certificate from the server (e.g., ftp://server.rhatcertification.com/pub/slaped.pem).

6.2.5 Switching to an LDAP user

The user can switch to an LDAP user just as easily as a local user using:

```
1 $ su - <ldap_username>
```

6.3 Understanding Automount

While it's possible to have the LDAP users use local directories on the server, generally an NFS hosts the home directories of these users. Thus, we have to automount the home directories of these users as if they're part of the local file system.

Let us consider a system where automounting is enabled, and the user wants to access a folder /data/files. If the folder /data is hosted on a remote file system and monitored by the automount process (called **autofs**), then there will have a file called /etc/auto.master containing the line:

```
1 /data /etc/auto.data
```

The `/etc/auto.master` file only shows that the automount process recognizes the `/data` directory as an automount directory. This merely states that the mounting details for the data folder is present in its own file called `/etc/auto.data`. That file will contain:

```
1      files      -rw      nfsServer:/data
```

The `files` directory is a subdirectory of the `/data` directory, and thus when the `/files` directory needs to be accessed, an NFS mounting operation needs to occur, with read write access on the `nfsServer's` (hostname) `/data` directory. Even though the user will be working on the NFS server, he/she will have no inkling of this happening behind the scene.

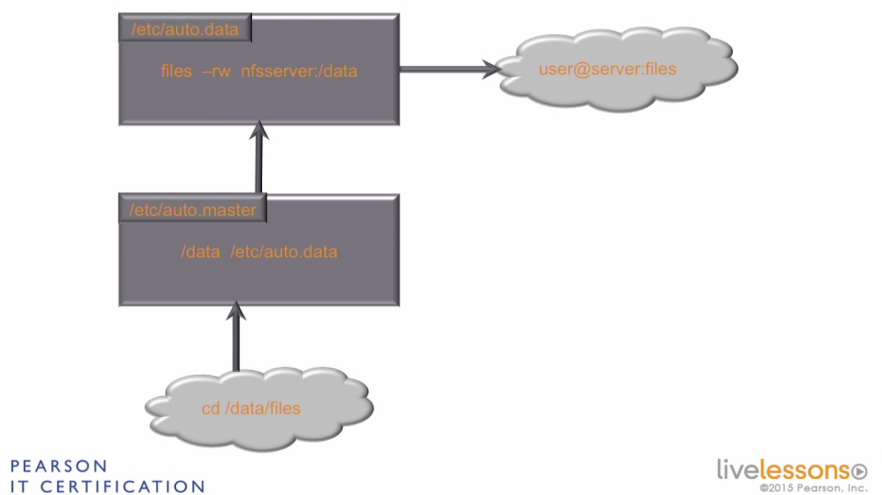


Figure 6.2: NFS Automount

6.3.1 Server selection for auto-mounting

Primarily two types of servers can accomplish the auto-mounting of home directories for LDAP users - NFS and Samba servers. In case of NFS server, the files will only be available on the local network. For access through the Internet, a Samba server has to be used.

6.3.2 Samba server's CIFS protocol to automount

Let us consider an LDAP user `ldapuser1` who has his home directory configured to `/home/guests/ldapuser1` in his user properties. When the user logs in, there will be a system call to go to the home directory for the users, which in turn calls `autofs` to mount the file system. It'll consult the `/etc/auto.master` file to find:

```
1      /home/guests      /etc/auto.guests
```

If anyone wants to visit that directory, the process should consult the `/etc/auto.guests` file, containing the mounting details with the UNC (Universal Naming Convention) path of the actual Samba server on the internet.

```

1      *      -fstype=cifs,username=ldapusers,password=password
2              ://server.rhaticertification.com/data/&

```

So, if anyone goes to `*` (i.e., any directory in `/data/guests`), like `/home/guests/ldapuser1` or `/home/guests/ldapuser2` and so on, a CIFS (Common Internet File Sharing protocol, which uses Server Message Block [SMB, Used by Samba]) mount needs to occur, specified by `fstype=cifs`, with the given username and password. The address of the server is then provided.

What is of particular importance here is the matching of `*` and `&`. While the `*` wildcard selects whatever folder the user tried to enter, the `&` in the address is replaced with the corresponding text from user. Thus, if the user visits `/home/guests/ldapuser1`, the `*` is replaced with `ldapuser1` and a matching folder is searched for on the server.

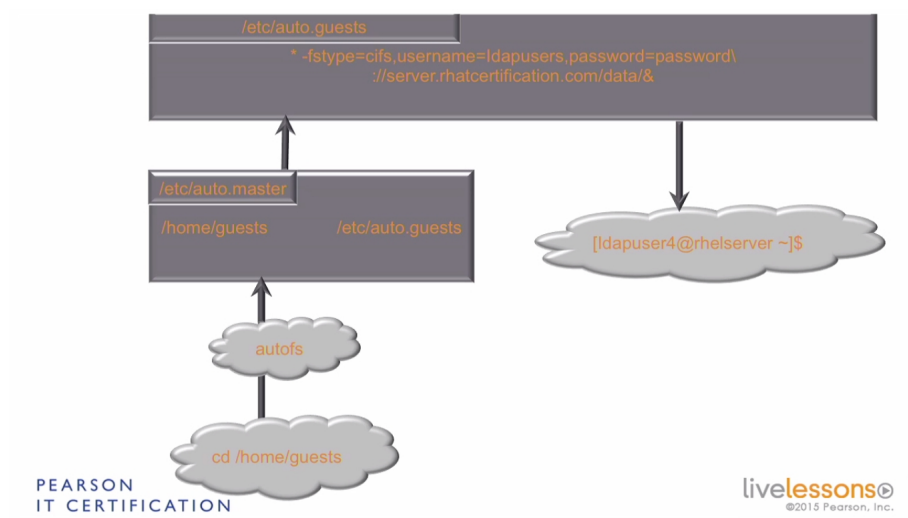


Figure 6.3: Samba Automount

6.4 Configuring Automount

To use automount, the *automount service* in the **autofs** package needs to be installed. The primary configuration file is `/etc/auto.master`. To automount the `/etc/guests` folder from a Samba server, we just need to specify in the file that:

```

1      /home/guests      /etc/auto.guests

```

Now we can add the mount options in its own individual file *auto.guests*, such that quick mounting and unmounting is possible.

Configuration on the Samba Server

The Samba server containing the data directory needs to have the following configuration in its `/etc/samba/smb.conf` :

```

1      [data]
2      comment = LDAP Users home directories
3      path = /home/guests
4      public = yes
5      writable = no

```

6.4.1 NFS Server Automounting

In the case of a NFS mounted directory, the *auto.guests* file would look like:

```

1      *          -rw          nfsServer.domain.com:/home/guests/&

```

In case of either servers, the syntax remains the same. First we provide the name of the directory (*), then the mounting options (e.g., -rw in case of NFS) and finally the path to the real directory that has to be mounted on the local file system from that server.

6.5 Modifying nslcd Configuration

6.5.1 Naming Services LDAP Client Daemon

The *nslcd* is a service that connects the local file system to the external LDAP server. The status of the *nslcd* can be checked using:

```

1      $ systemctl status nslcd
2      nslcd.service - Naming services LDAP client daemon.
3      Loaded: loaded (/usr/lib/systemd/system/nslcd.service; enabled; vendor preset:
↪ disabled)
4      Active: active (running) since Mon 2017-11-20 12:03:06 IST; 5h 59min ago
5      Process: 1108 ExecStart=/usr/sbin/nslcd (code=exited, status=0/SUCCESS)
6      Main PID: 1151 (nslcd)
7      CGroup: /system.slice/nslcd.service
8              1151 /usr/sbin/nslcd

```

/etc/nsswitch.conf

For every LDAP user, their identity needs to be known to the local system. This is based on the configuration stored in */etc/nsswitch.conf*. In this file, there is a line:

```

1      passwd:          files          sss          ldap

```

This represents the order in which the sources of user account are searched for user related information. *sss* is an older service no longer used by RHEL-7. Finally, it looks for the information in LDAP using *nslcd*.

PAM using nslcd

PAM is responsible for the actual authentication system that ensures the LDAP server is known to the authentication mechanism. This entire process is achieved using *nslcd*.

6.5.2 /etc/nslcd.conf

This file contains the information stored by using the `authconfig-gtk` command and has options to configure the *nslcd* such that the LDAP server can be connected to and used.

Option	Description	Example Value
uri	The Uniform Resource Identifier of the LDAP Server.	ldap://server.rhatcertification.com
base	The base context of the LDAP Server	dc=rhatcertification,dc=com
ssl	Whether to use SSL/TLS. If <code>start_tls</code> is given, via the use of StartTLS, an insecure connection is upgraded to a secure one.	<code>start_tls</code>
tls_cacertdir	Location of the downloaded certificate of the LDAP Server.	<code>/etc/openldap/cacerts</code>

In case of any problems with using LDAP, the `/var/log/messages` file may contain hints that may indicate what's wrong.

Chapter 7

Keyboard Shortcuts

- CTRL+U** - Clear Command Line.
- CTRL+L** - Clear Screen, same as clear command.