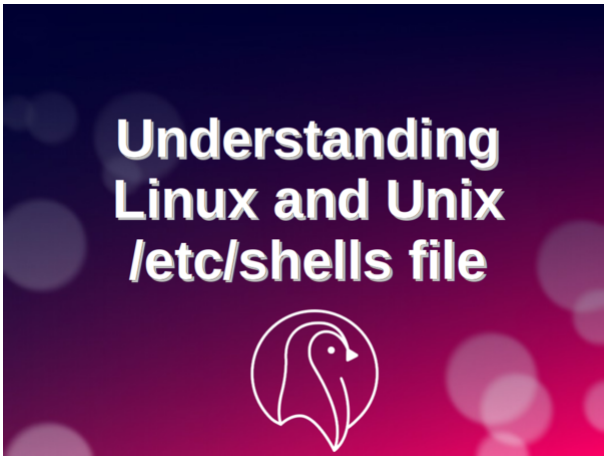
/etc/shells

The **/etc/shells** is a Linux / UNIX text file which contains the full pathnames of valid login shells. This file is used by various commands, including the chsh command. Please note that there are programs that consult this file to determine if a user is a regular user. For example, ftp daemons such as ftpd disallow access to users with shells not included in this file.



Understanding Linux and Unix /etc/shells file

Contents

Purpose
What happens if I use a shell not listed in this file?
How do I view this file?
Querying /etc/shells file
Example
See also

Purpose

The primary usage is to see the pathnames of the valid login shell.

What happens if I use a shell not listed in this file?

1. Your login will be blocked by many system services.
2. You will be locked out of the system.
3. Hence, always use the pathnames of the valid login mentioned in the /etc/shells file.

How do I view this file?

Simply use the cat command or more command or less command as follows:

```
cat /etc/shells
```

Sample outputs:

```
/usr/bin/tcsh
/bin/tcsh
/usr/bin/esh
/bin/dash
/bin/bash
/bin/rbash
/usr/bin/screen
/bin/pdksh
```

Querying /etc/shells file

You can always use the grep command to find out the valid path to shell names:

```
grep shell_name /etc/shells
grep bash /etc/shells
```

Example

Many commands will warn you when you try to add invalid shell paths. For instance, first find out the correct path to bash shell, run:

```
grep -w 'bash' /etc/shells
```

Here is the list:

```
/bin/bash
/usr/bin/bash
```

Now try to change user named raj path to /usr/local/bin/bash5 and see what happens using the [nixcmd name="chsh"]:

```
sudo chsh -s /usr/local/bin/bash5 raj
```

Sample session:

```
[sudo] password for vivek:
Sorry, try again.
[sudo] password for vivek:
chsh: Warning: /usr/local/bin/bash5 does not exist
```

However, despite the warning, the system made the change as your ran command as the root user. For example:

```
grep -w '^raj' /etc/passwd
```

Try to log in as the raj user:

```
ssh raj@192.168.2.17
```

The ssh based login attempt will fail with the following message on the server's log file such as /var/log/auth.log or /var/log/secure.log:

```
sudo tail -f /var/log/auth.log
```

Sample log entries for the user named 'raj':

```
May  3 14:30:28 wks01 sshd[156869]: User raj not allowed because shell /usr/local/bin/bash5 does not exist
May  3 14:30:30 wks01 sshd[156869]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=192.168.2.17 user=raj
May  3 14:30:32 wks01 sshd[156869]: Failed password for invalid user raj from 192.168.2.17 port 48752 ssh2
May  3 14:30:34 wks01 sshd[156869]: Connection closed by invalid user raj 192.168.2.17 port 48752 [preauth]
```

See also

- How do I find out what shell I am using on Linux/Unix? (https://www.cyberciti.biz/tips/how-do-i-find-out-what-shell-im-using.html)
- How To Change Shell To Bash in Linux / Unix (https://www.cyberciti.biz/faq/how-to-change-shell-to-bash/)