About permissions --> First of all, think about:

* who: user
* what happens: I can/can not .....
* with regard to what: file/dir
* why (explanation, cause): acl rules and permissions

Example:

a) Question: Can user dacomo read the contents of file test.sh?

b) Check

```
dacomo@inf1-dacomo:/usr/bin$ ls -ls test.sh
20 -rwxr----x+ 1 fje users 17654 feb 5 13:25 test.sh

dacomo@inf1-dacomo:/usr/bin$ getfacl test.sh
# file: test.sh
# owner: fje
# group: users
user::rwx
user:dacomo:r-x
group::r--
mask::rwx
other::---

dacomo@inf1-dacomo:/usr/bin$ id
uid=1000(dacomo) gid=1000(dacomo) grups=1000(dacomo),100(users),125(vboxusers)

dacomo@inf1-dacomo:/usr/bin$ cat test.sh
#!/bin/bash
echo "Hola món"
exit 0
```

c) Analyse

who is the user trying to read the contents of test.sh?--> user dacomo
What is dacomo trying to do? --> Read the contents of test.sh
Check permissions:
    Is dacomo the owner of test.sh? --> No
    Is there a rule for dacomo? --> Yes ==> What is the rule?: r-x
    Checking more rules is not required because a rule matches
What are the permission of dacomo on test.sh for dacomo --> r-x
What is the permission required? --> Reading
Is the reading permission set for dacomo on test.sh? --> Yes

d) Answer

dacomo (user - who)
can read the contents (action - what happens)
of test.sh (file/dir - what)
because a user ACL assigns reading permission to dacomo on test.sh (why - acl rule / permission).

dacomo can read the contents of test.sh because a user ACL rule assigns the reading permission to dacomo on test.sh.