

Red Hat / RHEL-এর `/etc/login.defs` ফাইল খুবই গুরুত্বপূর্ণ, কারণ এটি user account, password policy এবং login behaviour নির্ধারণ করে। নিচে আমি একদম basic থেকে advanced, real-life example + command output style দিয়ে বিস্তারিতভাবে বুঝাচ্ছি।

`/etc/login.defs` কী?

এটি একটি configuration file যা মূলত এই কমান্ডগুলো ব্যবহার করে:

- useradd
- passwd
- login
- su

👉 SSH বা PAM সরাসরি এখানে পড়ে না, কিন্তু PAM অনেক সময় এখানকার মান ব্যবহার করে।
ফাইল দেখতে: `cat /etc/login.defs`

1 PASSWORD POLICY সম্পর্কিত অপশন

◆ PASS_MAX_DAYS

`PASS_MAX_DAYS 99999`

◆ অর্থ: একটি password সর্বোচ্চ কতদিন valid থাকবে

🔧 Example:

- 99999 → প্রায় never expire
- 90 → ৯০ দিন পর password change বাধ্যতামূলক

👉 Corporate environment: `PASS_MAX_DAYS 90`

◆ PASS_MIN_DAYS

`PASS_MIN_DAYS 0`

◆ অর্থ: password পরিবর্তনের পর minimum কতদিন অপেক্ষা করতে হবে আবার change করার আগে

🔧 Example:

- 0 → সাথে সাথে আবার change করা যাবে
- 7 → ৭ দিনের আগে change করা যাবে না

🔒 Security use: `PASS_MIN_DAYS 7`

👉 User যেন বারবার change করে পুরাতন password-এ ফিরে যেতে না পারে

◆ PASS_MIN_LEN

`PASS_MIN_LEN 8`

◆ Minimum password length

⚠ Note: Modern RHEL এ এটা অনেক সময় `pam_pwquality.so` দ্বারা override হয়

🔧 Example: `PASS_MIN_LEN 12`

◆ PASS_WARN_AGE

PASS_WARN_AGE 7

◆ Password expire হওয়ার আগে কয়দিন warning দিবে

✚ Example:

- 7 → ৭ দিন আগে থেকে login করলে warning দেখাবে

🗉 Output:

WARNING: Your password will expire in 7 days.

2 USER ID (UID) এবং GROUP ID (GID)

◆ UID_MIN / UID_MAX

UID_MIN 1000

UID_MAX 60000

◆ Useradd করলে default UID এই range থেকে হবে

✚ Example:

useradd rakib

id rakib

Output: uid=1001(rakib) gid=1001(rakib)

◆ SYS_UID_MIN / SYS_UID_MAX

SYS_UID_MIN 201

SYS_UID_MAX 999

◆ System user (nginx, apache, chrony) এর জন্য

✚ Example:

id nginx

uid=997(nginx) gid=995(nginx)

3 HOME DIRECTORY & LOGIN BEHAVIOUR

◆ CREATE_HOME

CREATE_HOME yes

◆ useradd করলে home directory তৈরি হবে কি না

✚ Example:

useradd testuser

ls /home/testuser

যদি no হয়:

ls /home/testuser

ls: cannot access

◆ UMASK

UMASK 077

◆ Default file permission

🔑 UMASK effect:

UMASK	File	Directory
022	644	755
077	600	700

4 PASSWORD ENCRYPTION

◆ ENCRYPT_METHOD

ENCRYPT_METHOD SHA512

◆ Password কোন algorithm দিয়ে hash হবে

🔑 /etc/shadow এ দেখবেন: \$6\$xxxxxxxx

- \$6\$ = SHA512
- \$1\$ = MD5 (old, insecure)

5 MAIL SETTINGS

◆ MAIL_DIR

MAIL_DIR /var/spool/mail

◆ User-এর mail file কোথায় থাকবে

🔑 Example: ls /var/spool/mail/rakib

6 LOGIN LIMITATIONS

◆ FAILLOG_ENAB

FAILLOG_ENAB yes

◆ Failed login attempt log করবে

🔑 Check: faillog -u rakib

◆ LOG_UNKFAIL_ENAB

LOG_UNKFAIL_ENAB no

◆ Unknown user login attempt log হবে কিনা

🔒 Security reason:

- no রাখলে brute-force info leak কমে

7 DEFAULT USER SETTINGS

◆ USERGROUPS_ENAB

USERGROUPS_ENAB yes

◆ User-এর primary group নিজ নামেই হবে

🔑 Example: id rakib

gid=1001(rakib)

8 REAL-LIFE HARDENED SERVER EXAMPLE

```
PASS_MAX_DAYS 90  
PASS_MIN_DAYS 7  
PASS_MIN_LEN 12  
PASS_WARN_AGE 14
```

```
UID_MIN 1000  
SYS_UID_MIN 201
```

```
CREATE_HOME yes  
UMASK 077
```

```
ENCRYPT_METHOD SHA512  
FAILLOG_ENAB yes  
LOG_UNKFAIL_ENAB no
```

👉 Bank / ISP / Government server এ এমন configuration common

⚠️ গুরুত্বপূর্ণ কথা

- **/etc/login.defs existing user-এর উপর apply হয় না**
- **নতুন user তৈরির সময় কার্যকর হয়**
- Existing user modify করতে:
chage -M 90 username

Linux Group Management

Linux / Unix system-এ **group** মূলত দুই প্রকার।

1 Primary Group

- প্রতিটি user-এর একটি মাত্র **primary group** থাকে।
- এটি user-এর **main identity**।
- নতুন file বা directory তৈরি হলে **default group ownership** primary group-এর হয়ে যায়।
- Primary group /etc/passwd ফাইলে GID field-এ define থাকে।
- উদাহরণ: **id rakib**
Output: uid=1001(rakib) gid=1001(rakib) groups=1001(rakib),10(wheel),20(docker)
- এখানে gid=1001(rakib) হলো primary group।

2 Secondary / Supplementary Groups

- User একাধিক **secondary group**-এর member হতে পারে।
- এগুলো optional এবং **extra permissions / access control** দেয়।
- Secondary groups /etc/group ফাইলে define থাকে।
- নতুন file তৈরি করার সময় secondary group ownership by default apply হয় না।
- উদাহরণ: **id rakib**
Output: groups=1001(rakib),10(wheel),20(docker)
- এখানে wheel এবং docker হলো secondary groups।

✓ সংক্ষেপে: Linux group দুই ধরনের:

1. **Primary Group** – main identity, default file ownership
2. **Secondary / Supplementary Group** – extra permissions, collaboration

আমরা যে নামের একজন 'user' তৈরী করি তখন সিস্টেম By Default ওই নামের একটি গ্রুপ ও তৈরী করে ফেলে। তাই এইখানে যখন 'dia' নামের ইউজার তৈরী করা হয়েছে তখন সাথে সাথে ডিফল্ট ভাবে সিস্টেম 'dia' নামের একটি গ্রুপ ও তৈরী করে ফেলেছে, এই 'dia' গ্রুপ হচ্ছে 'dia' ইউজার এর 'Primary' গ্রুপ।

```
[root@ITBD-Server /]# useradd dia
```

```
[root@ITBD-Server /]# id dia
```

```
[root@ITBD-Server /]# useradd dia
[root@ITBD-Server /]# id dia
uid=1018(dia) gid=1023(dia) groups=1023(dia)
```

This is Primary Group

- ⇒ Auto-created primary group = dia
- ⇒ কোনো supplementary group নেই

এখন আমরা 'tasnim' নাম একজন ইউজার তৈরী করতেছি , কিন্তু সাথে আমি assign করে দিচ্ছি তার প্রাইমারি গ্রুপ কি হবে। আমরা চাচ্ছি - 'tasnim' ইউজার এর প্রাইমারি গ্রুপ হোক 'noc'

```
[root@ITBD-Server /]# useradd -g noc tasnim
```

```
[root@ITBD-Server /]# id tasnim
```

```
[root@ITBD-Server /]# useradd -g noc tasnim
[root@ITBD-Server /]# id tasnim
uid=1019(tasnim) gid=1016(noc) groups=1016(noc)
```

This is Primary Group

- ⇒ এখানে -g noc ব্যবহার করা হয়েছে → **primary group explicitly set করা হলো**
- ⇒ System আর tasnim নামের group auto-create করেনি, কারণ আমরা primary group explicitly দিয়েছি

Note: '-g' means = Primary Group

এখন চাচ্ছি - 'dia' ইউজার যেন Primary গ্রুপ হিসেবে 'support' গ্রুপ এ যুক্ত করতে।

```
[root@ITBD-Server /]# usermod -g support dia
```

```
[root@ITBD-Server /]# id dia
```

```
[root@ITBD-Server /]# usermod -g support dia
[root@ITBD-Server /]# id dia
uid=1018(dia) gid=1018(support) groups=1018(support)
```

Primary Group

- ⇒ Primary group support set হয়েছে
- ⇒ Old group dia আর primary নয়
- ⇒ Supplementary groups এখনো নেই

এখন চাচ্ছি - 'dia' ইউজার Primary গ্রুপ হিসেবে 'support' গ্রুপ এ যুক্ত আছে, এখন আমরা চাচ্ছি 'dia' ইউজার যেন Supplementary গ্রুপ হিসেবে 'noc' আর 'it' গ্রুপ এ যুক্ত হয়।

```
[root@ITBD-Server /]# usermod -G noc,it dia
```

```
[root@ITBD-Server /]# id dia
```

```
[root@ITBD-Server /]# usermod -G noc,it dia
[root@ITBD-Server /]# id dia
uid=1018(dia) gid=1018(support) groups=1018(support),1016(noc),1021(it)
```

Primary Group

Supplementary Group

- Primary group = support (unchanged)
- Supplementary groups = noc, it নতুনভাবে যুক্ত হয়েছে।
- **Note:** -G means = Supplementary Group Name

এখন চাচ্ছি - 'dia' ইউজার সুপ্লেমেন্টারি গ্রুপ হিসেবে 'noc' আর 'it' গ্রুপ এ যুক্ত আছে, এখন আমরা চাচ্ছি 'dia' ইউজার যেন Supplementary গ্রুপ হিসেবে 'monitoring' গ্রুপ এ যুক্ত হয়।

```
[root@ITBD-Server /]# usermod -G monitoring dia
```

```
[root@ITBD-Server /]# id dia
```

```
[root@ITBD-Server /]# usermod -G monitoring dia
[root@ITBD-Server /]# id dia
uid=1018(dia) gid=1018(support) groups=1018(support),1022(monitoring)
```

Supplementary Group

Supplementary groups overwrite হয়ে শুধু monitoring রইল, পূর্বের কোনো গ্রুপস আর থাকবে না। কারণ শুধুমাত্র '-G' ব্যবহার করলে পূর্বের কোনো গ্রুপ থাকবে না। পূর্বের কোনো গ্রুপ overwrite হয়ে যায়।

এখন আমি যদি 'dia' ইউজারকে চাই সে যেন পূর্বের 'monitoring' গ্রুপ এ থাকুক, সাথে আরো ২ টি নতুন গ্রুপ noc,it এ যুক্ত হোক অর্থাৎ append হোক তাহলে আমরা ব্যবহার করবো '-a'

```
[root@ITBD-Server /]# usermod -aG noc,it dia
```

```
[root@ITBD-Server /]# id dia
```

```
[root@ITBD-Server /]# usermod -aG noc,it dia
[root@ITBD-Server /]# id dia
uid=1018(dia) gid=1018(support) groups=1018(support),1016(noc),1021(it),1022(monitoring)
```

Newly added Supplementray Groups

- -aG → append, আগের supplementary group (monitoring) রাখা হয়েছে
- এখন: noc, it, monitoring

এখন আমি যদি 'dia' ইউজারকে চাই তাকে পূর্বের 'monitoring' গ্রুপ থেকে সরিয়ে ফেলতে

```
[root@ITBD-Server /]# gpasswd -d dia monitoring
```

Removing user dia from group monitoring

```
[root@ITBD-Server /]# id dia
```

```
[root@ITBD-Server /]# gpasswd -d dia monitoring
Removing user dia from group monitoring
[root@ITBD-Server /]#
[root@ITBD-Server /]# id dia
uid=1018(dia) gid=1018(support) groups=1018(support),1016(noc),1021(it)
```

'monitoring' group removed

- ⇒ monitoring remove হয়ে গেল
- ⇒ Primary group support এবং অন্যান্য supplementary group অপরিবর্তিত

Note: '-d' for remove.

আবার আমি যদি 'dia' ইউজারকে চাই তাকে পূর্বের 'monitoring' গ্রুপ এ যুক্ত করতে 'supplementary' গ্রুপ হিসেবে, কিন্তু সাথে পূর্বের গ্রুপ গুলো থাকবে এবং 'Primary' গ্রুপ হিসেবে 'noc' এ তুকাতে -

```
[root@ITBD-Server /]# usermod -g noc -aG monitoring dia
```

```
[root@ITBD-Server /]# id dia
```

```
[root@ITBD-Server /]# usermod -g noc -aG monitoring dia
[root@ITBD-Server /]# id dia
uid=1018(dia) gid=1016(noc) groups=1016(noc),1021(it),1022(monitoring)
```

'monitoring' group is appended

- ⇒ Primary group noc set হয়েছে
- ⇒ monitoring supplementary group হিসেবে append হয়েছে
- ⇒ it group আগের মতো আছে

নোট: পূর্বে 'noc' ছিল supplementary গ্রুপ হিসেবে, সেই গ্রুপকে যখন primary গ্রুপ হিসেবে দেয়া হলো তখন সেটা আর supplementary গ্রুপ হিসেবে থাকলো না, সেটা primary গ্রুপ হিসেবে গণ্য হবে।

এখন চাচ্ছি 'dia' ইউজারকে সমস্ত 'Supplementary' গ্রুপ থেকে বের করে নিয়ে আসতে -

```
[root@ITBD-Server /]# usermod -G "" dia
```

```
[root@ITBD-Server /]# id dia
```

```
[root@ITBD-Server /]# usermod -G "" dia
[root@ITBD-Server /]# id dia
uid=1018(dia) gid=1016(noc) groups=1016(noc)
```

All Supplementary groups are removed

- ⇒ সব supplementary group remove হয়ে গেছে
- ⇒ Primary group noc অপরিবর্তিত

Note: "" = means all groups will be removed