1.114.3
Setup user level security
Weight 1

Geoffrey Robertson `ge@ffrey.com`

Nick Urbanik `nicku@nicku.org`

2005 July

Outline

Contents

1 Context

Topic 114 Security [8]

1.114.1 Perform security administration tasks [4]

1.114.2 Setup host security [3]

1.114.3 <u>Setup user level security [1]</u>

2 Objective

Description of Objective
    Candidate should be able to configure user level security. Tasks include limits on user logins, processes, and memory usage.

Key files, terms, and utilities include:

quota — display disk usage and limits

usermod — can modify expiry date of an account, and can disable an account

3 Enabling Quotas

Set and View Disk Quotas

- Add the `userquota` and `grpquota` options in `/etc/fstab`:

  ```
  /dev/hda2  /home  ext3  defaults,usrquota,grpquota  1 2
  ```

- Create the quota.user and quota.group files:

  ```
  fehung:~# touch /home/quota.user /home/quota.group
  fehung:~# chmod 600 /home/quota.user /home/quota.group
  ```

- Initialise the `quota.*` files as databases by running `quotacheck`:

```
fehung:/home# quotacheck -augv
Cannot get exact used space... Results might be inaccurate.
quotacheck: Scanning /dev/hda2 [/home] done
quotacheck: Checked 143 directories and 689 files
```

Set and View Disk Quotas

- Confirm that the databases have actually been initialised by making sure that the `quota.*` files are larger than 0.

- Run quotaon to enable the quota system:

  ```
  fehung:/home# quotaon -a
  ```

- There are two further things to deal with:

  1. Turn on quota is turned at boot time. (details next slide)
  2. Check the data base regularly. (details next slide)

- The filesystem (in this case /home) is now ready to accept quotas on a per user or group basis.

3.1 Initialising Quotas when booting

Set and View Disk Quotas

To ensure quota is turned on upon system boot, add the following to the system's initialisation script (`/etc/rc.d/rc.sysinit` or similar):

```
if [ -x /sbin/quotacheck ]; then
   echo "Checking quotas."
   /sbin/quotacheck -auvg
   echo "Done."
fi

if [ -x /sbin/quotaon ]; then
   echo "Enabling quotas."
   /sbin/quotaon -avug
fi
```

3.2 Check quotas regularly with `cron`

Set and View Disk Quotas

To ensure that the databases are checked regularly, add a script to one of the crontab system directories, (such as /etc/cron.weekly/) to run quotacheck:

```
#!/bin/bash
/sbin/quotacheck -auvg
```

or a job in crontab to achieve the same thing.

4 Quota Limits

Quota Limits

There are five types of quota limits that can be enforced:

- Per-user hard limit

- Per-group hard limit

- Per-user soft limit

- Per-group soft limit

- Grace Period

4.1 Hard Limit—User

Quota Limits—Per-user hard limit

- absolute maximum of a user's allocated space

- user cannot write anything else to the filesystem when reached

- write to current file is truncated

- user can free space and save file if program has a copy of the file in memory

4.2 Hard Limit—Group

Quota Limits—Per-group hard limit

- absolute maximum of a group's allocated space

- members of the group cannot write anything else to the filesystem when reached

- write to current file is truncated

- user in the group can free space and save file if program has a copy of the file in memory

4.3 Soft Limit—User

Quota Limits—Per-user soft limit

- Less than hard limit

- When reached, user enters *grace period*

- User gets warnings on terminal that quota has been exceeded

4.4 Soft Limit—Group

Quota Limits—Per-group soft limit

- Less than hard limit

- When reached, group enters *grace period*

- Members of the group get warnings on terminal that quota has been exceeded

4.5 Grace Period

Quota Limits—Grace Period

- Grace period is a time before the hard limit is enforced

- regardless of whether the hard limit is reached

- . . . unless the user gets their quota down bleow the soft limit in that time

5 Configuring Quotas with **edquota**

Set and View Disk Quotas

- The next move is to edit the quota reference for each user. We can get around this with scripts, but essentially this is not nice :)

- We can actually edit the quota of a typical user on our system and then copy the attributes of that users quota to other users, as follows:

  ```
  fehung:/home/greebo# edquota greebo
  ```

- This edits the quota for user greebo, in this file we change the soft and hard limits to whatever we choose, example:

  ```
  Disk quotas for user greebo (uid 1000):
  Filesystem blocks    soft    hard   inodes    soft    hard
  /dev/hda2      538   29000   30000      689       0       0
  ```

Set and View Disk Quotas

- The first soft and hard values are relevant to blocks and the second to inodes, here the user has a block soft and hard limit but no inode limit .

- We can then attribute these settings to the rest of the users thus:

  ```
  fehung:/home/greebo# edquota -p greebo $(awk -F: '$3 > \
  999 { print $1 }' /etc/passwd)
  ```

  and can confirm this worked by running

  $ **sudo edquota** ⟨*randomuser*⟩ ↩

  to see whether the new settings copied across.

- We can only modify the grace limit system wide. We do this by running # **edquota -tu** ↩ , and changing the value.

6 Viewing quotas with **quota**

Set and View Disk Quotas

quota is used to display quotas on users and groups, using the -u switch for users and -g switch for groups:

```
fehung:/home# quota -uv greebo ↩
Disk quotas for user greebo (uid 1000):
Filesystem  blocks   quota   limit   grace   files   quota   limit   grace
 /dev/hda2     538   29000   30000             689       0       0
```

7 Turning quotas on and off

Set and View Disk Quotas

quotaon turns on the quota system, quotaoff turns it off. Easy!

8 repquota

Set and View Disk Quotas

repquota reports on the status on quotas. Common options are as follows:

-a   reports on all quotas

-g   reports on group quotas

-u   reports on user quotas

-v   verbose mode

Examples: `$` **`sudo repquota -v /home`** ↵
or
`$` **`sudo repquota -a`** ↵

9   License Of This Document

License Of This Document

Copyright © 2005, 2003 Geoffrey Robertson <ge@ffrey.com> and Nick Urbanik <nicku@nicku.org>.

Permission is granted to make and distribute verbatim copies or modified versions of this document provided that this copyright notice and this permission notice are preserved on all copies under the terms of the GNU General Public License as published by the Free Software Foundation—either version 2 of the License or (at your option) any later version.