Administration système GNU/Linux
TP noté

Info et Réseaux en Apprentissage, Sup Galilée, Paris Nord

November 25th, 2014

1. **Preliminaries** Work in group of two or three people, without communicating with other groups. Use the Debian GNU/Linux image provided by the instructor and implement the following requirements.
2. **Documentation** Document your pair work writing:
   - a brief report in simple text format describing the design decisions you made;
   - timed typescripts of your shell activities (`script -a -timing=timingscript typescript` to enter the recording session, `CTRL+D` to exit).
3. **Submission** Send, before the end of the TP an email to `marco.solieri@lipn.univ-paris13.fr` with subject "`[AIR3-IWEB] TP5 Nom1, Nom2`" and attaching an archive containing: the shell typescript, the report, and the scripts you wrote.

Context

In this TP you will design and develop a complete SFTP service for a 5-people team of coworkers: Ann Abelson, Bob Baumgarten, Carl Constant, Dustin Doyle, Eve Esmeralda. Some of their projects are personal, some belong to a pair of users. They need places where they can share, read or modify files with other users. They also need a way to concisely be informed of changes in their files that are done by other users.

Privacy is of great concern for the office and its client, therefore they need that only concerned parties access private files. A second important concern is reliability, as they want the service running 24/7.

Happy hackaton!

1 Users

1. Choose an appropriate naming schema for your users. Describe it in the report.
2. Install a generator of random, readable password.
3. Create a user group named "office".
4. Create five new users with random password (see 2), belonging to "office" (see 3), and with home located in `/home/office/$USER`.

2 Filesystem

1. Create a "office" folder in `/home/`, and create there some folders to be used for users' home and for sharing between them. Set up appropriately permissions or ACL, so that they do not need any administrator intervention in their workflow. In particular:

   (a) In a folder shared between two users, they both must be able of: creating files and directories, and modifying files belonging to the each other.
   (b) Any user, other than those two, must not be able of: listing, reading or modifying the content shared between the two.
   (c) All of these settings must be applied in recursively in any directory created in a main folder shared between the two.

   Describe your choice in the report.

2. Set up limits to file system usage for the “office” users using quotas. A user must not be able of using more than 50 MB, while the users of the group must not be able to use more than 200 MB cumulatively. Install and configure appropriate Debian packages.

3 SSH and SFTP

1. Install the OpenSSH server. Disable login for root and for any other user that is not an administrator or a member of the “office” group.

2. Generate and setup login with SSH keys for the administrator’s user (not root) and test the configuration. Disable password authentication for SSH connection of that user and test the configuration.

3. Configure OpenSSH so that users of “office” group can use only SFTP service, i.e., they cannot log in a system shell.

4. Configure OpenSSH so that users of “office” group cannot browse the filesystem outside `/home/office/`.

4 Notifications

1. Write a bash script which checks for file changes in the shared directories. It should detect, with respect to its previous run: addition of new files, removal of files, change in the content of files, change in the attribute of the file.

2. Modify the script in order to log every entry of the list of changes via syslog, on facility “`local0`” with severity “`info`”. Test your configuration.

3. Configure syslog to have this kind of messages being written on a separate log file named `officefiles.log` and stored in `/var/log/`. Test your configuration.

4. Configure a `cron` job which schedule automatic run of the script every 10 minutes. Test your configuration.

5. Configure syslog so that users in the group “office” can read the previously mentioned log file.

6 Configure logrotate so that the file is truncated every 3 hours, and that only the last three weeks of logs are kept.

5 Guard

1. Install `Monit`, a deamon for guarding services and servers, using the official Debian package.

2. Configure Monit as follows.

   (a) It restart the SFTP service if it appears down for more than 10 minutes.
   (b) It checks if disk usage is more than 50%.
   (c) Sends notifications via syslog.