System Administration for Beginners

Week 9 Laboratory

April 3, 2007

You should work on this laboratory in your project groups. Please note that any commands where you'll be installing, removing, or updating software will require root. You should try to perform any many commands as possible without root, though, to get you into the habit of safe computing.

1 Laboratory

1.1 Disk Quotas

Along with filesystem permissions, disk space quotas are probably one of the most important tools system administrators have for securing their systems and restricting abuse. Disk space quotas allow system administrators to specify exactly how much disk space a user can use. On any server with more than one user, it is imperative to set disk space quotas to prevent a single user from hogging up an entire server's hard drive.

[1] Use `apt-cache` to search for the two packages that contain the utilities to manage disk space quotas and install them.

Support for quotas is not automatically enabled; you must enable support for quotas before using them. UNIX-like operating systems store their filesystem settings in a file named `fstab` or `vfstab`. On Linux systems, this file is located at `/etc/fstab`.

[2] Open the `/etc/fstab` file with a text editor and add the options `usrquota` and `grpquota` to the line that begins with `/dev/hda1`. In other words, the options column should look like the following:

```
defaults,errors=remount-ro,usrquota,grpquota
```

[3] At this point, you would want to reboot the server. Since we are using a technology that does not yet allow individual virtual servers to reboot, you will need to ask me to restart the server for you.

There are two types of disk quotas in UNIX: soft and hard. Soft quotas are merely advisory; if a user goes over their soft quota, a warning is usually sent to

their account. Hard quotas are the absolute maximum amount of disk space a user can use; if a user goes over their hard quota, they will be unable to create new files. On some systems, soft quotas automatically become hard quotas after a short warning period.

[4] Figure out how to set quotas for user accounts using `edquota`. Set a small hard quota for one of your user accounts.

> **NOTE:** `edquota` will use `vim` as the default editor for quotas. If you prefer to use another editor, execute the following command prior to using `edquota`, substituting in for your favorite editor:

```
export EDITOR=nano
```

[5] Login as the user with the limited quota. Attempt to download files larger than the quota. What happens?

[6] As a system administrator, you may wish to check the quota status of an individual user or all users. Figure out how to use `quota` to check the quota status of the user account with a quota. Figure out how to use `repquota` to check the quota status for all users.

1.2 Access Control Lists

[1] Use `apt-cache` to search for the package that contain the utilities to work with Access Control Lists and install it.

As with quotas, support for Access Control Lists is not enabled by default; you have to explicitly enable ACL support before using them.

[2] Open the `/etc/fstab` file with a text editor and add the options `acl` to the line that begins with `/dev/hda1`.

[3] Reboot the server using the `reboot` command. You'll be disconnected from the server during the reboot. Please wait a minute before attempting to reconnect.

[4] The command to apply an access control list to a file is `setfacl`. Figure out how to grant permissions to a specific user. HINT: The man page for `setfacl` contains a nice list of examples at the end.

[5] Using one of your user accounts, create a few file and only grant the owner of that file access. Attempt to write to that file using another user account. Verify that the other user account can not access the file. Use ACLs to grant read and write access to the second user account. Can that user access the file now?

1.3 Programs and their Privileges

[1] Remove all permissions (except for the owner and group) from the WordPress configuration file you created last week. Verify that your installation of WordPress no longer works.

[2] Use ACLs to grant Apache read access to the file. Does your installation of WordPress work now?

[3] Verify that no other user account (excluding the owner) can access the WordPress configuration file.

2 Submission Guidelines

Only one submission is necessary per a final project group. Please use the online submission tool located on the Beginning System Administration Decal website and include any commands, notes, observations, output, etc, that you feel is relevant and necessary to demonstrate that you successfully completed the laboratory. Be sure to include your group number, group members names, and logins.