Protection scheme in unix research papers example

Business, Company

Protection Scheme in UNIX®

The computer network based on the UNIX systems deployed in a company supporting 5, 000 users and the company desires to allow 4, 990 of all users to access one file. In order to do so, the company has two solutions include, development of user groups and the creation of an Access Control List (ACL). In the first solution, the network administrator is required to create a group of 4, 990 users to whom the company wants them to allow access one file. Then the group can be assigned access level to the files according to the desire of the company. In this case, the users can only access those files which are allowed by the network administrator in the user group. In this regard, the network administrator is required to login the UNIX system and put the command to create the user group, as given below:

groupadd fileaccess

The above-given command would create a user group name “ fileaccess”. Once the user group is created, then the network administrator can add one by one each user to the group as given below:

useradd –g fileaccess user1

The above-given UNIX command would add the user “ user1” to the user group name “ fileaccess”. It is pertinent to mention here that the network administrator is required to repeat the above-given command for the each user to be added into the group (Oracle Corporation, 2010). Moreover, the permissions to access the files can be added to the user group at this stage by utilizing “ chmod” command.

As specified earlier in the document that the second solution for resolving the file access issues of the company is to create an Access Control List

(ACL). The UNIX file protection system allows the network administrator to provide read, execute and write permissions for three (3) types of the user groups include, the file group, file owner and other particular or developed user groups. The UNIX file protection system provides better security to the files, as separate permissions (read, write and / or open) can be given to the each or group of files. Moreover, if the particular file has to be given access to the group of users (as in our scenario), the ACL can be utilized for giving the access to the particular file to the particular user or group of users by utilizing the UNIX command " setfacl". The complete command of the UNIX system is given below:

Setfacl.-s. user : : perms, group : : perms

The ACL can be verified by utilizing the UNIX command " getfacl filename". The command would facilitate the network administrator to know which of the ACL entries are set on the file.

It is highly significant to evaluate the above-given two solutions for enabling the 4, 990 users to allow to access the file. On some UNIX systems, the creation of groups for implementing the file access permissions is not allowed, therefore, the solution is not recommended to be implemented by the company. However, the implementation of the ACL is recommended for the company for allowing a specified group of users to access the file.

Reference

Oracle Corporation. (2010). Creating UNIX System Users and Groups. Retrieved on 6th October, 2014, from: http://docs. oracle. com/cd/E19563-01/819-4428/fwbzc/index. html