LINUX USER AND GROUP MANAGEMENT pdf

1: User and Group Management Tools

It covers the various aspects of users and groups in Linux, like adding or removing them, giving them passwords, etcâ€”all from a systems administrator's point of view. Linux is a multi-user operating system, which means that more than one user can use Linux at the same time.

The "Linux Standard Base" defines three required user and group names. This is generally not done for regular users on a server. This example may also be applied to the diskette. Allow use of device by group cdrom. Add user to group cdrom. Grant privileges to system users to mount the device: The fourth column defines mounting options. By default only root may mount the device option owner. To grant users the ability to mount the device, change the owner option to user. With the user option only the user who mounted the device can unmount the device. To allow anyone to unmount the device, use the option users. Gnome Nautilus Gnome file browser: Linuxconf is no longer included with Red Hat Linux 7. The user who mounted the CD must also be the one to unmount the CD. OR Select the tab Misc. For more information see the man pages for mount and fstab. Add the line cdrom:: Admin tool linuxconf is no longer included with Red Hat 7. Add space delimited user ids here Accept For more information see the man pages for groupadd, groupmod and groupdel. Use hdd if cdrom is the slave device on the 2nd IDE controller. Allow group access to the device: Start the File Manager and right click the file representing the cdrom device. Then select the tab Permissions. Set the Owner to root and the Group to cdrom. Allow Read and Write privileges for the user and group by selecting the appropriate buttons. Add user to group cdrom: At this point, adding users to the group cdrom will grant them access to the device. Be sure to list all groups as this is an absolute list and not an addition. Step two allowed you to assign users to the group. If users still need to be assigned use the following method: Next to supplementary groups add the group cdrom. Groups should be delimited by spaces. OR for a completely different method that steps 1 to 4, use the one step approach: This method is quick, unelegant and can be used for your own desktop system but definitely don t do this on a server. Do not switch CDs without un-mounting and re-mounting the new CD. Covered later Command method: Only root user may execute the mount command. Depricated for newer systems. Ubuntu and sound card access: This makes sense for a server installation but not for the desktop. ACLs are an addition to the standard Unix file permissions r,w,x,- for User, Group, and Other for read, write, execute and deny permissions. ACLs give users and administrators flexibility and direct fine-grained control over who can read, write, and execute files. Support may not be available on your version of NIS and may only work on local file systems. Configuration for allowing the use of ACL on a filesystem: Issue the following commands:

LINUX USER AND GROUP MANAGEMENT pdf

2: Linux User and Group Management - Explained - FowuTech

Linux servers often contain thousands of users and user files. It's easier to maintain users if they are contained in groups, but only if the limitations of groups are understood and managed properly.

Change File and Directory Permissions in Linux â€" Terminal Commands In this follow up post of the System and Network Administration via SSH series, we are going to talk about users and group management in Linux and also some modern conventions for Ubuntu operating system. In practice, all of your websites should be run by different users under different group for better security. As, Ubuntu is my personal favorite for both a standard OS and web server, we are going to see some Ubuntu standards as well. User and Group Management in Linux: The concept of Groups and Users is pretty straight forward. To further extend the permissions of a group or collection of users, the User Group concept was introduced. We know that each file, should be owned by a User. In simpler words, if we want to run a process, then it has to run under some user. Any user should be a part of a group or a set of groups. A group with same name as the username is created and is assigned as the primary group of the user. The user is also assigned to other groups depending on what the user is supposed to do. Other than that, I might be added to the following groups as well. What a group can do, solely depends on the model of an application. Most of the system applications like, Apache, SambaShare etc creates groups and allows user only their own group to execute them. Everything in Linux is stored in a file, Groups and Users are no exceptions. We can view the following file to quickly view the current status of users and groups: Holds 4 information delimited by colon: Inside group file It holds 7 information delimited by colon: The shadow file holds the password of the user and other login credentials. It has 8 columns delimited by colon: It is your login name. It your encrypted password. Days since Jan 1, that password was last changed. The minimum number of days required between password changes i. The number of days after password expires that account is disabled. Please read this article from cyberciti to understand although not required more about the shadow file. System Users vs Normal Users: The very basic of the user management system includes the concept of whether the user account is being used by programs or by people. A system user is intended to be used by programs applications. A normal user is intended to be used by people like you and me. That being said, the usage is not actually limited. In practice, an application can use a normal account, whereas one may assign password to a system user and can login through the shell. It is upto the us and the program to properly create system users when necessary. Also, on a modern Linux Distro, we will not see system users listed in the login window. The same concept holds true for System Groups as well. Typically, all users under a System Group should be System users. So, we had enough theoretical explanations. Now, let us see how we can actually create and manage users and groups. Obviously, we shall use terminal commands to do the necessary. Also, these concepts are for System Administrators SA. So, we will need su privilege to execute any of the commands. For general Linux system, we can start a root session by typing su on the terminal, whereas in debian or Ubuntu, we can either type sudo then the command or can start a root session by entering sudo su. Adding a new group to the Linux System groupadd: To add a normal group named mygroup we would execute the command: Where we can see our group. Note that the group ID is automatically assigned to the group. There are a few useful parameters as well.

LINUX USER AND GROUP MANAGEMENT pdf

3: Interview Questions on Linux User Management with Answers - GoLinuxHub

Linux User and Group Management Users and groups are used on GNU/Linux for access controlâ€”that is, to control access to the system's files, directories, and peripherals. Linux offers relatively simple/coarse access control mechanisms by default.

Password Aging For security reasons, it is advisable to require users to change their passwords periodically. This can be done when adding or editing a user on the Password Info tab of the User Manager. Important Shadow passwords must be enabled to use the chage command. If the value is 0, the password does not expire. When the number of days specified by this option plus the number of days specified with the -d option is less than the current day, the user must change passwords before using the account. If the value is 0, the account is not locked after the password expires. Instead of the date, the number of days since January 1, can also be used. You can configure a password to expire the first time a user logs in. This forces users to change passwords the first time they log in. Note This process will not work if the user logs in using the SSH protocol. Lock the user password â€” If the user does not exist, use the useradd command to create the user account, but do not give it a password so that it remains locked. If the password is already enabled, lock it with the command: This value forces immediate password expiration no matter what password aging policy, if any, is in place. Unlock the account â€” There are two common approaches to this step. The administrator can assign an initial password or assign a null password. Warning Do not use the passwd command to set the password as it disables the immediate password expiration just configured. To assign an initial password, use the following steps: Start the command line Python interpreter with the python command. It displays the following: Press Ctrl-D to exit the Python interpreter. To do this, use the following command: Always make sure that the user is ready to log in before unlocking an account with a null password. In either case, upon initial log in, the user is prompted for a new password. Explaining the Process The following steps illustrate what happens if the command useradd juan is issued on a system that has shadow passwords enabled: The line has the following characteristics: It begins with the username juan. There is an x for the password field indicating that the system is using shadow passwords. A UID greater than is created. A GID greater than is created. The password is set to never expire. A group with the same name as a user is called a user private group. It begins with the group name juan. An x appears in the password field indicating that the system is using shadow group passwords. All other fields are blank. This directory is owned by user juan and group juan. However, it has read, write, and execute privileges only for the user juan. All other permissions are denied. At this point, a locked account called juan exists on the system. To activate it, the administrator must next assign a password to the account using the passwd command and, optionally, set password aging guidelines.

LINUX USER AND GROUP MANAGEMENT pdf

4: User and Group Management in Linux Part-3 | Learn Linux CCNA CEH CCNP IPv6

Since Linux is a multi-user operating system (in that it allows multiple users on different computers or terminals to access a single system), you will need to know how to perform effective user management: how to add, edit, suspend, or delete user accounts, along with granting them the necessary permissions to do their assigned tasks.

For existing accounts, we can also do the following. Like the basic permissions discussed earlier, they are set using an octal file or through a letter symbolic notation that indicates the type of permission. Other users can be added to the group later. One of the purposes of groups is to implement a simple access control to files and other system resources by setting the right permissions on those resources. For example, suppose you have the following users. You may be tempted to do something like, chmod common. Again, you may be tempted to add user2 and user3 to group user1, but that will also give them access to the rest of the files owned by user user1 and group user1. Since this approach can reasonably raise security concerns, the number of files with setuid permission must be kept to a minimum. You will likely find programs with this permission set when a system user needs to access a file owned by root. Other users can only change their corresponding passwords. Thus, any user can access a file under the privileges granted to the group owner of such file. In addition, when the setgid bit is set on a directory, newly created files inherit the same group as the directory, and newly created subdirectories will also inherit the setgid bit of the parent directory. Add Stickybit to Directory Special Linux File Attributes There are other attributes that enable further limits on the operations that are allowed on files. For example, prevent the file from being renamed, moved, deleted, or even modified. They are set with the chattr command and can be viewed using the lsattr tool, as follows. Chattr Command to Protect Files Accessing the root Account and Using sudo One of the ways users can gain access to the root account is by typing. If authentication succeeds, you will be logged on as root with the current working directory as the same as you were before. For that reason, the sysadmin can configure the sudo command to allow an ordinary user to execute commands as a different user usually the superuser in a very controlled and limited way. Thus, restrictions can be set on a user so as to enable him to run one or more specific privileged commands and no others. It is recommended that this file is edited using the visudo command instead of opening it directly with a text editor. These are the most relevant lines. The next lines are used to specify permissions. The second ALL indicates that the user in the first column can run commands with the privileges of any user. The third ALL means any command can be run. In this case, user tecmint will be able to run yum update as root. The meaning of the rest of the line is identical to that of an regular user. This tool present on all modern Linux distributions overcame the problem often faced by developers in the early days of Linux, when each program that required authentication had to be compiled specially to know how to get the necessary information. For example, when the login program needs to authenticate a user, PAM provides dynamically the library that contains the functions for the right authentication scheme. In addition, we can tell whether a certain application uses PAM by checking if it the PAM library libpam has been linked to it: This makes sense since this application is involved in the operation of system user authentication, whereas top does not. When a hyphen appears before the type, PAM will not record to the system log if the module cannot be loaded because it could not be found in the system. The following authentication types are available: The second column called control indicates what should happen if the authentication with this module fails: The fourth column, if it exists, shows the arguments to be passed to the module. Linux Password Fields Summary Effective user and file management skills are essential tools for any system administrator. In this article we have covered the basics and hope you can use it as a good starting to point to build upon.

LINUX USER AND GROUP MANAGEMENT pdf

5: Linux User and Group Management | Step by Step Linux Command with Example

In this follow up post of the System and Network Administration via SSH series, we are going to talk about users and group management in Linux (and also some modern conventions for Ubuntu operating system).

By Ken Hess Friday, April 16th, OK, class settle down, find your seats, fire up your Linux systems and follow along with me for this user and group administration tutorial. Following a single, simple rule will make your life as a system administrator easier: Give your users access to what they need, no more and no less. To find out which groups you belong to, type groups at a command prompt. An SA can specify a group when he creates the account but the group must already exist. Here are two illustrative examples: For example, create a new user with rpdusers Group ID as a secondary group. A group must exist before you assign users to it. You may also create a new group with just a group name and the system will assign a GID for you with the command, groupadd groupname. The groupmod command allows you to change the group name but the SA will have to change any files associated with the old group manually. You can remove a group with the groupdel command. For example, a clever user on your system tries to issue useradd and vipw. Only root may add a user or group to the system. User permissions change to robert as well for all files in his home directory. You cannot change the login name of a currently logged in user. Why would any programmer allow that directory to remain as clutter on your home filesystem? This is actually a failsafe mechanism and you should thank the thoughtful programmer who maintains userdel. What if two user names only differ by a single letter and you removed the wrong one? With the failsafe mechanism in place, you have to manually remove the home directory and hopefully you would catch your error before doing so. This introduction to user and group administration will point you in the right direction in your own duties as a new system administrator. Remember to think in terms of groups and add users to those groups as needed. Use the administrative tools and utilities provided to you and avoid directly editing any system file. Have you ever wanted to see more information from your system than proc files or dmesg could give you? Well, your search is over.

6: Unix / Linux User Administration

Linux is a multi-user and multitasking OS. In Linux, you can create any number of user account and groups. A user is always connected to a particular group and there can be any number of groups as well.

7: Linux Tutorial - Managing Group Access on Linux and UNIX

This video explains how to manage user accounts, update passwords, manage group memberships, as well as create new groups.

8: CentOS Enterprise Linux 7 User and Group Management | Pluralsight

The usermod allows SAs to alter any user account attribute including the user's real name (comment field), home directory name, account expiration date, disabling functionality, group add and change, login name, account locking and unlocking, alter the user's shell and more.

9: User and Group Management | Linux Magazine

In one of the earlier articles at this blog (here), we learned the Linux user login management. The article explained how user login and password are managed in Linux. Continuing on the same lines. In this article, we will learn how users are managed in Linux. This article will try to cover basics.

LINUX USER AND GROUP MANAGEMENT pdf

The future of research on prejudice, stereotyping, and discrimination Susan T. Fiske, Lasana T. Harris, T Managing wet play How to build a lowrider 5. Frosted glass, changes that persist when changing the patient position, corresponding Car Buyers and Leasers Negotiating Bible How did Stalin rule? How To Handle Disillusionment A detailed guide to building the actors repertoire book Smuk is king : the action of cigarettes in a Papua New Guinea prison Adam Reed Travel and adventure The efficient layman Animal industry groups in the Asian and Pacific region Windows XP for Dummies Quick Reference Pet health certificate for travel How to build a dinosaur Fields Medico-legal guide for doctors and lawyers . Lithographic press operation and troubleshooting Visual Encyclopedia of Animals A journal from Japan Chapter 12: Marine Biological Diversity: Conserving Life in the The burro the basket Discipline of cultivating the soul Not without my neighbour Ultimate Guide to Collecting A discourse, delivered on Saturday, the 10th of August, 1769. Hidden Job Market 2000 Laetrile case histories Understanding solid state physics problems and solutions Empirical labs distressor manual Forest society and colonialism notes Developing curriculum Loire (Philips Travel Guides) Learning To Design, Designing To Learn: Using Technology To Transform The curriculum Sex In Films (Film Books) A Country for Katie (Child Like Me) A mystery of heroism by stephen crane Neonatal Formulary 3 The Six Sigma Basic Training Kit The higher christian life by william boardman Experiences of a male anorexic Michael Krasnow