LINUX FOUNDATION

TRAINING

Using Sudo to Manage Access to the Root Account

A Linux Foundation Training Publication
www.training.linuxfoundation.org

Overview

Given the potentially destructive ability of the root user, it is considered bad practice to use the root account for day to day tasks and activities, intentionally reserving it for potentially disruptive administrative changes.

In cases where a system has multiple administrators, increasing the number of people who know the password to the root account increases the potential risk of abuse or mistakes, and reduces accountability by giving multiple administrators a single identity to make changes with.

As an alternative to using the root account directly, users can be allowed to temporarily give their own accounts Super User privileges using the sudo command. Sudo provides specified users or groups of users with limited root access. Users assume root privileges with sudo using their personal passwords, and any activity performed is logged by the system logger (systemlogd), as are unsuccessful attempts to gain sudo privileges.

Access to the sudo command is policy based, with the /etc/sudoers containing the sudo policy for a system. The visudo command opens the /etc/sudoers policy file in a vi text editor, while this is indeed possible, it is NOT recommended. Using visudo locks the file for edition and ensures only one person is making changes to it at the same time.

Key Ideas

The /etc/sudoers files contains many sane defaults, and a number of common or useful example sudo policies. Here are some of the important concepts in the sudoers file:
Concept: Command aliases
Cmnd_Alias SERVICES = /sbin/service, /sbin/chkconfig

In this example, an alias is declared for a group of commands, in this case, 2 service related commands. Grouping multiple commands into an alias allows the administrator to give users or groups access to a number of commands at once.

Concept 2: Sudo policy

%wheel (ALL)=(ALL) ALL
In this example, members of the wheel group are allowed to perform any command. The policy statement has 4 parts.

%wheel: The group or user to whom the policy applies. If the policy is specific to a single user, the % is omitted.

(ALL): The first (ALL) in this example is the host where the policy applies. It could also be localhost, or other hosts that use this sudoers file to determine sudo policy.

(ALL): The second (ALL) in this example is the user with whose permissions any commands affected by the policy will be run. (ALL) means that any command affected by this policy can

be run with the permissions of any user. If no user or group of users is specified, the root user is assumed.

ALL: The third ALL in this example, with no brackets, are the commands affected by this policy. In this case, all commands are affected, but a command alias or comma separated list of commands could also have been used.

Example Scenario

Use the /etc/sudoers policy file to create some aliases and policies.

Now Do It

1. Create a command alias for the commands involved in creating RAID arrays.
2. Create a command alias for user administration that includes commands for adding and removing users.
3. Create a policy that allows members of the users group to run the RAID commands as your user on localhost.
4. Create a policy that allows members of the users group to run the user administration commands as root on localhost.

If you remember nothing else...

If a user with whose permissions commands affected by a particular policy will be run is not specified, the root user is assumed. The /etc/sudoers file contains some practical policies for you to copy and modify as required.

Answer Key

1. Cmnd_Alias RAIDSTUFF = /usr/sbin/mdadm, /usr/sbin/parted
2. Cmnd_Alias USERSTUFF = /usr/sbin/useradd, /usr/sbin/userdel
3. %users localhost=USERNAME ALL RAIDSTUFF

   Where USERNAME is your username.
4. %users localhost=USERSTUFF

LINUX FOUNDATION

Get Certified!

Get more information at http://training.linuxfoundation.org/certification/lfcs