Глава 2: Sudo и sudoers

Двумя ключевыми компонентами пакета sudo являются сама программа sudo и файл /etc/sudoers. Команда sudo непосредственно используется для запуска программ с повышением привилегий. Файл sudoers определяет политику сообщая sudo какие команды пользователь может выполнять и с какими привилегиями.

Sudo 101

Вам необходимо выполнить команду под sudo? Выполните sudo, а следом требуемую команду. Далее я прошу произвести монтирование NFS:

$sudo mount fileserver:/home/mike /mnt
Password:
mount_nfs: fileserver: hostname nor servname provided, or not known
$

Sudo запрашивает пароль. Это должен быть мой пароль, а не пароль суперпользователя. Если я ввожу свой пароль верно и если у меня имеются разрешения на выполнения этой команды посредством sudo, я получу правильный результат. Особенно теперь, когда я вспомнил, что служба поддержки переименовала этот сервер.

Хорошая новость заключается в том, что sudo запоминает прохождение проверки подлинности и в последующие пять минут не будет повторно запрашивать пароль. Некоторые ОС имеют иное поведение, поэтому вам стоит обратится к странице руководства man sudo для уточнения ситуации. (Вы можете изменить время доверия или использовать иной способ проверки подлинности, как описано в Главе 13). Если вы допустили ошибку при наборе команды, то можете сразу же повторить ввод команды без повторного ввода пароля.

При первом запуске sudo на любой системе, программа печатает несколько строк о важности осмысления использования привилегированных команд. Примите это сообщение к сведению. Привилегированные команды называются так поскольку они позволяют внести изменение в конфигурацию, повредить или уничтожить систему.

Выполнение команд от имени другого пользователя

Выполнение команд от имени root не всегда желательно. Некоторые программы, в частности базы данных и серверы приложений используют выделенного для своих целей пользователя. Приложение ожидает выполнение от имени пользователя и среда этого пользователя настроена для управления приложением. Подобную модель используют различные приложения, начиная от крупных, типа Java и заканчивая мелкими утилитами вроде Ansible. Вы можете выполнить команду от имени конкретного пользователя добавив флаг -u.

#sudo –u oraclesqlplus

Это приведёт к запуску целевой среды пользователя и выполнению команды, аналогично su.

Выполнение команд от другой группы

Каждый пользователь входит основную группу, указанную совместно с учётной записью в /etc/passwd или его эквиваленте. Группы из дополнительных источников, таких как /etc/group, считаются вторичными группами. Некоторые программы работают нормально только при условии, что основная группа пользователя является привилегированной группой. Это может сильно раздражать, поскольку предпочтительно использовать группы по прямому назначению, а не нянчиться с придирчивой программой.

В зависимости от того, как ОС управляет группами и того, как установлено ПО, вам, возможно, для выполнения команды необходимо изменить основную группу. Используйте флаг -g и имя группы:

#sudo –g operator stupidpickycommand

Sudo обманывает программу и сообщает, что ваша основная группа - operator. Так же вы можете использовать идентификационный номер группы, поставив знак # перед GID. Используемая вами оболочка может потребовать убрать # из командной строки. По крайней мере, для пользователей tcsh этого ограничения нет.

#sudo –g #100 stupidpickycommand

Sudo выполнит команду так, как будто бы ваша группа имеет GID=100.

Это примерно всё, что знают о sudo 90% пользователей. Остальные знания будут более продвинутыми.

sudoers 101

Если запуск sudo и кажется простым - это потому, что вся реальная работа происходит в файле sudoers, который часто называется просто sudoers. Этот файл содержит правила, определяющие, какие пользователи могут запускать привилегированные команды и набор этих команд. Все мои примеры предполагают, что sudoers расположен в /etc/sudoers. Никогда не редактируйте файл sudoers вручную; всегда используйте visudo, как описано в Главе 3.

Некоторые пакеты устанавливаемые в операционной системе включают в файл sudoers примеры функций, поддерживаемых ОС. Поэтому, перед внесением каких-либо изменений в файл sudoers, следует скопировать оригинал в безопасное месть, чтобы иметь возможность обратиться к нему позже.

Файл sudoers содержит набор правил, по одному правилу в каждой строке. Каждое правило использует общий формат. В остальной части нашего разговора о sudoers мы рассмотрим расширение, растяжение и в целом злоупотребления этого формата.

username host=command

Username - имя пользователя, на которого данное правило распространяется. Username может быть системной группой или псевдонимом определённым в sudoers.

Host - имя хоста системы к которому относится данное правило. В Главе 10 мы рассмотрим как распространить /etc/sudoers на несколько машин.

Command - полный путь к каждой команде применяемой с правилом. Запомните, настройка sudo требует указание полного пути к командам.

Файл sudoers распознаёт множество специальных ключевых слов. Одно из наиболее частых - ALL, соответствует любому из возможных вариантов. Чтобы разрешить всем пользователям запускать любую команду на любом хосте, мы могли бы написать правило:

ALL ALL=ALL

Эта команда эквивалентна предоставлению доступа к root используя свой пароль вместо пароля root. Этого делать не следует. Как минимум следует ограничить доступ по имени пользователя:

mike ALL=ALL

Теперь, пользователь mike может выполнить любую команду на всех серверах.

Аналогично, можно ограничить доступ sudo по имени хоста. Наиболее часто вы увидите ограничения сервера как ALL поскольку большинство системных администраторов настраивает sudo на базе каждого хоста. Если вы управляете каждым сервером отдельно, определение сервера как ALL в действительности означает "этот сервер". Лучшей практикой является указание имени сервера. (Для получения имени сервера выполните команду hostname). В Главе 10 подробно описывается назначение sudo для хоста.

mike www =ALL

Пользователь mike может выполнять любую команду на хосте www. Чтобы ограничить пользователя запуском одной команды, укажите полный путь к команде в поле command:

mike www=/sbin/reboot

Пользователь mike может выполнить команду /sbin/reboot на сервере www. Выглядит достаточно просто, не так ли? Давайте усложним вопрос.

Несколько записей

Каждое уникальное правило доступа записывается отдельной строкой в sudoers. Совершенно нормально использовать несколько записей, например:

mike www=/sbin/reboot
mike www=/sbin/dump

Хотя подобный метод записи быстро становится громоздким. Если у вас несколько похожих правил, разделяйте индивидуальные части запятыми.

mike,pete www=/sbin/reboot,/sbin/dump

Теперь пользователи mike и pete могут запускать команды перезагрузки и дампа на хосте www.

Хотя вы можете перечислить несколько команд и пользователей в одном правиле, необходимо использовать разные правила для различных уровней доступа.

thea ALL=ALL
mike,pete www=/sbin/reboot,/sbin/dump

Первое правило говорит, что владелец системы thea может выполнить любую команду на любом хосте. При этом, она любезно разрешает своим подчинённым mike и pete выполнять две команды на хосте www.

Разрешение команд для других пользователей

Некоторые приложения, как правило, базы данных или Java, для правильной работы должны выполняться определёнными пользователями. Sudo позволяет выполнять команды от имени пользователя отличного от root, если это позволяют политики sudoers. Имя пользователя указывается в скобках перед командой:

kate beefy=(oracle) ALL

Пользователь kate может выполнять любые команды на сервере beefy, но только как пользователь oracle. Он получает полное управление базой данных, но не имеет иных особых привилегий.

Пользователи, имеющие доступ к определённым учётным записям, могут так же иметь отдельный доступ к привилегиям root:

mike beefy=(oracle) ALL
mike beefy=/sbin/mount,/sbin/umount

mike может монтировать и размонтировать диски, а кроме того управлять базой данных Oracle.

Длинные правила

Когда вы указываете в одном правиле несколько команд с полными путями, несколько пользователей и несколько хостов, отдельные строки sudoers могут получиться весьма длинными. Косая черта в конце строки укажет, что правило продолжается на следующей строке.

***kent,mike,pete beefy,www,dns,mail=/sbin/mount,/sbin/umount, ***
/sbin/reboot,/sbin/fsck

Пробелы и дополнительные строки делают правила легче управляемыми. Свободно пользуйтесь ими.

Тонкости

Несколько последних замечаний по sudoers. Sudo обрабатывает правила по порядку и побеждает последнее совпадение. Если два правила конфликтуют, выигрывает последнее совпадающее правило. Как это выражается будет видно когда мы построим сложные правила sudoers.

Восклицательный знак (!) является оператором отрицания. Он используется для исключения одного элемента из списка. Можно указать, что правило применяется ко всем, кроме конкретного пользователя, хоста или команды. Кроме того, он переключает опции. Помните - восклицательный знак означает "не". В остальной части книги содержится множество подобных примеров.

Наконец, файл sudoers должен всегда заканчиваться пустой строкой. Если visudo указывает на на ошибку в последней строке, но синтаксис выглядит корректно, убедитесь в наличии пустой строки в конце записи.

Теперь, когда у вас есть общее понимание sudo и sudoers, давайте создадим свой собственный sudoers и протестируем его совместно с sudo.