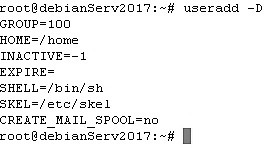
**Лекція № 13**

**4.2. Команди модифікації користувачів та груп**

**4.2.1. Додавання нового користувача**

Основним інструментом для додавання нового користувача у системі Linux є команда ***useradd***, яка представляє простий спосіб створення нового облікового запису користувача і його домашнього робочого каталогу. У команді поєднуються системні значення за замовчуванням і ключі команди для визначення нового облікового запису належним чином. Для перегляду системних значень за замовчуванням потрібно застосувати команду ***useradd*** з ключем ***-D***, як показано в наступному прикладі. Зауважимо, що ця команда, як і інші, не може бути виконана звичайним користувачем, для її виконання потрібні права адміністратора.



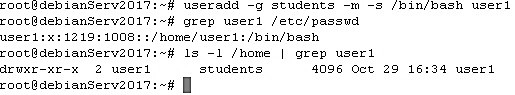
За необхідності використати інші значення або операції при створенні нового користувача потрібно застосувати відповідні ключі команди ***useradd***, які описані у табл. 4.1.

Табл. 4.1. Ключі команди useradd

|  |  |
| --- | --- |
| **Ключ** | **Опис** |
| ***-c <коментар>*** | Додати текст до поля коментаря нового користувача |
| ***-d <директорія>*** | Задати для домашнього каталогу користувача інше ім’я, що відрізняється від реєстраційного імені |
| ***-e <дата>*** | Задати дату в форматі YYYY-MM-DD, коли закінчується термін дії облікового запису |
| ***-f <кількість\_днів>*** | Задати кількість днів після закінчення терміну дії пароля, коли обліковий запис буде відключений Спеціальні значення:   * 0 – обліковий запис має бути відключений одразу після закінчення терміну дії пароля; * -1 – скасування відключення |
| ***-g <група>*** | Задати основну групу користувача (її GID або ім’я) |
| ***-G <групи…>*** | Задати одну або декілька додаткових груп, до яких належатиме користувач |
| ***-m*** | Створити домашній каталог користувача |
| ***-M*** | Не створювати домашній каталог користувача, якщо налаштування за замовчуванням передбачає його створення |
| ***-n*** | Створити нову групу з використанням імені, що збігається з реєстраційним іменем |
| ***-r*** | Створити системний обліковий запис |
| ***-p <пароль>*** | Задати застосовуваний за замовчуванням пароль для облікового запису |
| ***-s <оболонка>*** | Задати застосовуваний за замовчуванням командний інтерпретатор входу в систему |
| ***-u***  ***<ідентифікатор\_кори стувача>*** | Задати унікальний ідентифікатор користувача для облікового запису. |

Таким чином, завдання зміни значень за замовчуванням є зовсім не складним.

Наприклад, створимо нового користувача з іменем ***user1*** та додамо його у групу ***students*** (але вкажемо її у якості основної), створимо його домашній каталог та вкажемо у якості оболонки за замовчуванням ***bash***. Після цього переглянемо інформацію щодо створеного облікового запису в файлі ***/etc/passwd*** та перевіримо, чи був створений його домашній каталог.



Отже, ми переконалися, що новий обліковий запис користувача ***user*** дійсно був створений.

**4.2.2. Зміна поточного користувача**

У системі Linux передбачені різні команди, які змінюють облікові записи користувачів тим чи іншим чином. Вони наведені у табл. 4.2.

Табл. 4.2. Команди зміни облікових записів користувачів

|  |  |
| --- | --- |
| **Команда** | **Опис** |
| ***usermod*** | Команда редагування полів облікового запису користувача, яка дозволяє визначати приналежність до первинної та вторинної групи |
| ***passwd*** | Команда зміни пароля для існуючого користувача |
| ***chpasswd*** | Команда читання файлу, в якому у вигляді окремих пар задані реєстраційні імена і паролі та оновлення паролів |
| ***chage*** | Команда зміни дати закінчення терміну дії пароля |
| ***chfn*** | Команда зміни вмісту коментаря до облікового запису користувача |
| ***chsh*** | Команда зміни заданої за замовчуванням командної оболонки для облікового запису користувача. |

Команда ***usermod*** має найбільш широку область дії серед усіх команд зміни облікових записів користувачів, оскільки надає можливість вносити зміни в більшість полів файлу **/etc/passwd**. Для цього достатньо скористатися відповідними ключами цієї команди, які в основному збігаються з параметрами команди ***useradd***, однак існують і додаткові параметри, які можуть виявитися необхідними, наприклад:

***-p*** – змінити пароль облікового запису;



***-l*** – змінити реєстраційне ім’я облікового запису користувача;

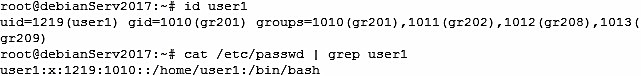
***-L*** – заблокувати обліковий запис для того, щоб користувач не зміг увійти в систему;

 ***-U*** – розблокувати обліковий запис для того, щоб користувач зміг увійти в систему.

Як приклад змінимо основну групу користувача ***user1*** зі ***students*** на ***gr201***, а також додамо його до груп ***gr202***, ***gr208*** та ***gr209:***



А тепер переглянемо інформацію щодо облікового запису, спочатку виконавши команду ***id***, а потім знайшовши відповідний запис у файлі ***/etc/passwd***:

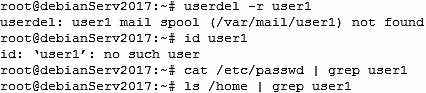


Як бачимо, основна група дійсно була змінена, а користувач був доданий до іншої групи, при цьому група ***students***, до якої користувач входив раніше, була видалена з його облікового запису.

**4.2.3. Видалення користувача**

Якщо коли-небудь буде потрібно видалити користувача з системи, то достатньо застосувати команду ***userdel***, яка за замовчуванням видаляє тільки відомості про користувача з файлу ***/etc/passwd***. Якщо використовувати ключ ***-r***, то команда видалить домашній каталог користувача разом з каталогом ***mail***, якщо він існував. Однак в системі можуть ще залишатися інші файли, які належать видаленому обліковому запису користувача, що у певних випадках призведе до виникнення проблем.

Тепер видалимо обліковий запис користувача ***user1***, ніби його ніколи не існувало, видаливши також і домашній каталог:



Застосувавши у наведеному прикладі спочатку команду ***userdel*** з ключем ***–r***, ми видалили користувача ***user1*** разом з домашнім каталогом. У результаті команда вивела попередження, що у системі немає каталогу, який асоціюється з електронною поштою користувача.

Подальші команди у прикладі демонструють, що після видалення користувача ні його облікового запису, ні домашнього каталогу не залишилося.

**4.2.4. Команди маніпулювання групами**

Для створення нових груп у системі застосовується команда ***groupadd***. Наголосимо, що ця команда не надає можливості додавати облікові записи користувачів до груп, а тільки створює нову, яка після створення порожня. Для додавання нових користувачів до групи призначена команда ***usermod*** з відповідними ключами ***–g*** при зазначенні основної групи, та ***–G*** для інших груп.

Змінити інформацію про групу дозволяє команда ***groupmod***. Як показує файл ***/etc/group***, обсяг інформації, що підлягає зміні, невеликий. Команду можна використати такими ключами як: 1) ***-g*** – змінити ідентифікатор групи; 2) ***-n*** – змінити назву групи.

При зміні назви групи, залишаються незмінними її ідентифікатор та список членів. Оскільки всі визначення прав доступу засновані на ідентифікаторі групи, допускається змінювати її назву настільки часто, наскільки це потрібно, не здійснюючи негативного впливу на безпеку файлу.

Для видалення відповідної групи потрібно використати команду ***groupdel***.

**4.2.5. Команди зміни ідентичності користувача**

Іноді може виникнути необхідність придбати ідентичність іншого користувача. Це частіше всього відбувається для виконання певних адміністративних завдань, що потребують повноваження суперкористувача.

У такому разі може виникнути необхідність зареєструватися під іменем іншого звичайного користувача, наприклад, для того, щоб перевірити налаштування облікового запису. Існує три способи для придбання ідентичності іншого користувача:

 вийти з системи і ввійти знову з обліковими даними іншого

користувача; виконати команду ***su***; виконати команду ***sudo***.



Команда ***su*** використовується для запуску нового сеансу роботи з командною оболонкою від імені іншого користувача поверх поточного сеансу. Команда має наступний синтаксис: ***su [-l] <користувач>***

Під час застосування ключа ***-l*** запущена командна оболонка стане оболонкою входу для вказаного користувача, тобто поточним робочим каталогом стане його домашній каталог.

Після введення команди буде запропоновано ввести відповідний пароль вказаного користувача. Після введення правильного пароля з’явиться нове запрошення до вводу, яке буде показувати, що робота у системі вже ведеться від імені іншого користувача.

Для наступного прикладу запустимо сеанс системи від імені користувача ***root***, поверх поточного сеансу користувача ***debianuser***.

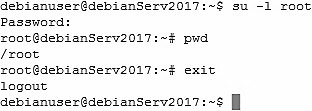


У наведеному вище прикладі спочатку з сеансу звичайного користувача ***debianuser*** здійснюється вхід до системи від імені суперкористувача ***root***. Система вимагатиме введення пароля, після цього відбудеться вхід у командну оболонку користувача ***root***, однак поточний робочий каталог не зміниться (ним залишиться домашній каталог користувача ***debianuser***).

Під іменем суперкористувача виконується команда, що виводить перші 10 рядків файлу ***/etc/shadow***, доступ до якого, як ми знаємо, має тільки суперкористувач.

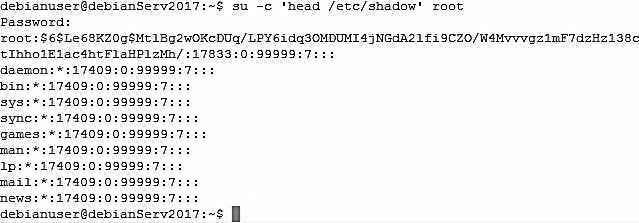
Потім ми виконуємо команду ***exit***, яка у цьому випадку не здійснює вихід із системи, а тільки повертає у зовнішню командну оболонку користувача ***debianuser***.

У наступному прикладі також застосуємо команду ***su***, але з ключем ***–l***:



Як можна побачити, що під час запуску сеансу від імені суперкористувача змінився і поточний робочий каталог, ***/root***, тобто домашній каталог користувача ***root***.

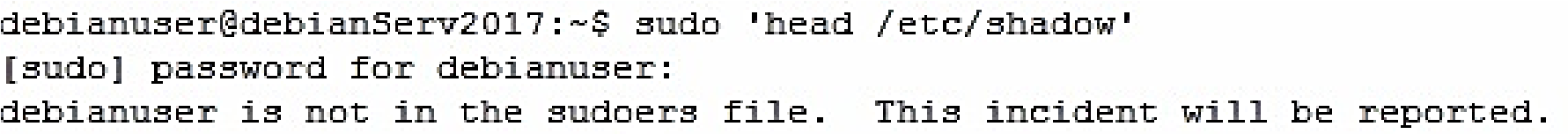
Також з командою ***su*** можна застосувати ключ ***–c***, що передбачає виконання єдиної команди під іменем іншого користувача. Необхідну команду потрібно зазначити у якості значення цього ключа, взявши її в одинарні лапки для запобігання додаткової інтерпретації. Наприклад, виведемо перші 10 рядків користувача ***/etc/shadow***, звісно виконавши це під іменем користувача ***root***:



Таким чином, під іменем суперкористувача було виконано тільки одну команду.

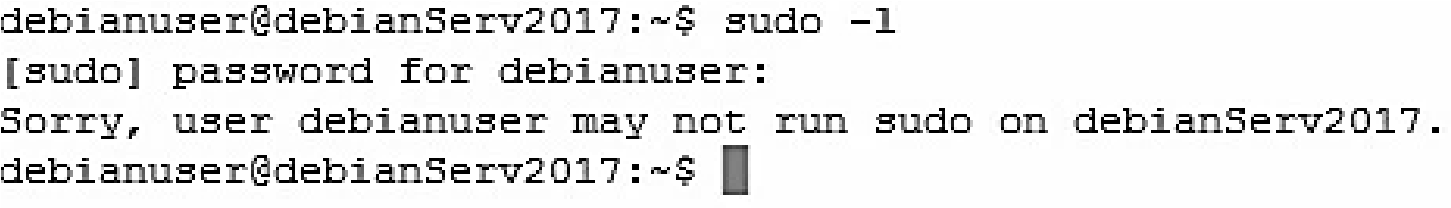
Багато в чому до команди ***su*** з ключем ***–s*** схожа команда ***sudo***, однак вона має певні важливі особливості. По-перше, порядок використання **sudo** звичайними користувачами завжди визначає адміністратор. Тим самим, він може дозволити або заборонити виконання команд. По-друге, команда ***sudo*** не вимагає введення пароля суперкористувача, а для аутентифікації користувач має ввести свій власний пароль, тобто підтвердити свою ідентичність.

Наведемо приклад, у якому спробуємо вивести 10 перших рядків файлу ***/etc/shadow***.



Отже можна зробити висновок, що у користувача ***debianuser*** немає ніяких привілеїв для здійснення вищевказаної команди від імені суперкористувача за допомогою команди ***sudo***.

Для того, щоб побачити, що можна виконати за допомогою команди ***sudo*** поточному користувачу, необхідно скористатися командою з ключем ***–l***, як показано у наступному прикладі:



Таким чином, ми дізналися, що користувач ***debianuser*** не може виконувати команду ***sudo*** без відповідного дозволу, який надається адміністратором системи.