

CREATING GROUP, USER CONFIGURATION, ACCOUNT CONSIDERATION

6

OBJEKTIF :

1. Mahasiswa Mampu Membuat, Memodifikasi, Menghapus Group.
2. Mahasiswa Mampu Mengidentifikasi dan Memodifikasi File Yang Berisi Informasi User.
3. Mahasiswa Mampu Membuat, Memodifikasi dan Menghapus user.

PENDAHULUAN

Selama proses penginstalan, sebagian besar penginstal membuat user biasa dan memberikan izin kepada user ini untuk menjalankan perintah administratif dengan `sudo` atau meminta password akun user root dikonfigurasi sebagai bagian dari proses penginstalan. Sebagian besar sistem Linux dikonfigurasi untuk memungkinkan satu user yang tidak memiliki hak istimewa (non-root) untuk masuk, serta memiliki kemampuan untuk secara efektif menjalankan perintah sebagai user root, baik secara langsung maupun tidak langsung.

Jika komputer hanya akan digunakan oleh satu orang, maka hanya memiliki satu akun user biasa mungkin sudah cukup. Namun, jika sebuah komputer perlu digunakan bersama oleh banyak orang, maka diharapkan untuk memiliki akun terpisah untuk setiap orang yang menggunakannya. Ada beberapa keuntungan bagi individu yang memiliki akun terpisah:

Akun dapat digunakan untuk memberikan akses selektif ke file atau layanan. Misalnya, user dari setiap akun memiliki direktori home terpisah yang umumnya tidak dapat diakses oleh user lain.

Perintah `sudo` dapat dikonfigurasi untuk memberikan kemampuan untuk menjalankan perintah administratif tertentu. Jika user diharuskan menggunakan perintah `sudo` untuk melakukan perintah administratif, sistem akan mencatat saat user melakukan perintah ini.

Setiap akun dapat memiliki keanggotaan grup dan hak yang terkait dengannya yang memungkinkan fleksibilitas pengelolaan yang lebih baik.

Pada beberapa distribusi, membuat akun user baru juga secara otomatis membuat akun grup untuk user, yang disebut User Private Group (UPG). Pada sistem ini, grup dan username akan sama, dan satu-satunya anggota grup baru ini adalah user baru.

Untuk distribusi yang tidak membuat UPG, user baru biasanya diberikan grup user sebagai grup utama mereka. Administrator dapat secara manual membuat akun grup yang bersifat pribadi untuk user, tetapi lebih umum bagi administrator untuk membuat grup untuk beberapa user yang perlu berkolaborasi. Akun user dapat diubah kapan saja untuk menambah atau menghapus mereka dari keanggotaan akun grup, tetapi user harus menjadi bagian dari setidaknya satu grup untuk digunakan sebagai grup utama mereka.

Sebelum Anda mulai membuat user, Anda harus merencanakan cara menggunakan grup. User dapat dibuat dengan keanggotaan dalam grup yang sudah ada, atau user yang sudah ada dapat diubah untuk memiliki keanggotaan dalam grup yang sudah ada.

Jika Anda sudah merencanakan user dan grup mana yang Anda inginkan, akan lebih efisien untuk membuat grup Anda terlebih dahulu dan membuat user Anda dengan keanggotaan grup mereka. Jika tidak, jika Anda membuat user terlebih dahulu, kemudian grup Anda, Anda harus mengambil langkah ekstra untuk mengubah user agar mereka menjadi anggota grup Anda.

GROUPS

Alasan paling umum untuk membuat grup adalah menyediakan cara bagi user untuk berbagi file. Misalnya, jika beberapa orang yang bekerja sama pada proyek yang sama dan perlu berkolaborasi pada dokumen yang disimpan dalam

file untuk proyek tersebut. Dalam skenario ini, administrator dapat membuat orang-orang ini menjadi anggota grup umum, mengubah kepemilikan direktori ke grup baru dan mengatur izin pada direktori yang memungkinkan anggota grup untuk mengakses file.

Setelah membuat atau memodifikasi grup, Anda dapat memverifikasi perubahan dengan melihat informasi konfigurasi grup di file `/etc/group` dengan perintah `grep`. Jika bekerja dengan layanan otentikasi berbasis jaringan, maka perintah `getent` dapat menunjukkan kepada Anda grup lokal dan berbasis jaringan.

```
grep pattern filename  
getent database record
```

Untuk user lokal, perintah ini menunjukkan hasil yang sama, dalam kasus ini untuk grup root:

```
root@localhost:~# grep root /etc/group  
root:x:0:  
  
root@localhost:~# getent group root  
root:x:0:
```

CREATING A GROUP

Perintah `groupadd` dapat dijalankan oleh user root untuk membuat grup baru. Perintah hanya membutuhkan nama grup yang akan dibuat. Opsi `-g` dapat digunakan untuk menentukan id grup untuk grup baru:

```
root@localhost:~# groupadd -g 1005 research  
root@localhost:~# grep research /etc/group  
research:x:1005:
```

Jika opsi `-g` tidak tersedia, perintah `groupadd` secara otomatis akan memberikan GID untuk grup baru. Untuk melakukannya, perintah `groupadd`

akan melihat file `/etc/group` dan menggunakan angka yang satu nilai lebih tinggi dari nomor GID tertinggi saat ini. Eksekusi dari perintah berikut digambarkan seperti ini:

```
root@localhost:~# groupadd development
root@localhost:~# grep development /etc/group
development:x:1006:
```

GROUP ID CONSIDERATIONS

Di beberapa distribusi Linux, terutama yang berbasis pada Red Hat, ketika user ID (UID) dibuat, user private group (UPG) juga dibuat dengan user tersebut sebagai satu-satunya anggota. Dalam distribusi ini, UID dan ID UPG seharusnya cocok (nomornya sama).

Oleh karena itu, Anda harus menghindari pembuatan GID dalam rentang numerik yang sama tempat Anda ingin membuat UID, untuk menghindari konflik antara GID yang Anda buat dan nomor UPG yang dibuat agar cocok dengan UID.

GID di bawah 500 (RedHat) atau 1000 (Debian) dicadangkan untuk digunakan sistem. Mungkin ada saatnya Anda ingin menetapkan nilai GID yang lebih rendah. Untuk melakukannya, gunakan opsi `-r` yang menetapkan GID pada grup baru yang kurang dari GID standar terendah.

```
root@localhost:~# groupadd -r sales
root@localhost:~# getent group sales
sales:x:999:
```

GROUP NAMING CONSIDERATIONS

Mengikuti panduan untuk nama grup ini dapat membantu memilih nama grup yang portabel (berfungsi dengan benar dengan sistem atau layanan lain):

- Karakter pertama dari nama harus berupa karakter garis bawah `_` atau karakter a-z huruf kecil.
- Hingga 32 karakter diperbolehkan pada sebagian besar distribusi Linux, tetapi menggunakan lebih dari 16 dapat menimbulkan masalah karena beberapa distribusi mungkin tidak menerima lebih dari 16.
- Setelah karakter pertama, karakter yang tersisa dapat berupa alfanumerik, tanda hubung (`-`) karakter garis bawah(`_`).
- Karakter terakhir tidak boleh berupa karakter tanda hubung.

Sayangnya, pedoman ini tidak selalu diterapkan. Masalahnya bukanlah bahwa perintah `groupadd` selalu gagal, tetapi perintah atau layanan pada sistem lain mungkin tidak bekerja dengan benar.

MODIFYING A GROUP

Perintah `groupmod` dapat digunakan untuk mengubah nama grup dengan opsi `-n` atau mengubah GID untuk grup dengan opsi `-g`.

Mengubah nama grup dapat membingungkan user yang terbiasa dengan nama lama dan belum mengetahui nama baru. Namun, mengubah nama grup tidak akan menimbulkan masalah dalam mengakses file, karena file tersebut dimiliki oleh GID, bukan nama grup. Sebagai contoh:

```
root@localhost:~# ls -l index.html
-rw-r-----. 1 root sales 0 Aug  1 13:21 index.html

root@localhost:~# groupmod -n clerks sales

root@localhost:~# ls -l index.html
-rw-r-----. 1 root clerks 0 Aug  1 13:21 index.html
```

Catatan: File dalam contoh di atas tidak tersedia dalam lingkungan mesin

Setelah perintah `groupmod` sebelumnya, file `index.html` memiliki nama pemilik grup yang berbeda. Namun, semua user yang berada di grup `sales`

sekarang berada di grup `clerks`, jadi semua user tersebut masih dapat mengakses file `index.html`. Sekali lagi, ini karena sistem mendefinisikan grup berdasarkan GID, bukan nama grup.

Di sisi lain, jika Anda mengubah GID untuk sebuah grup, maka semua file yang terkait dengan grup tersebut tidak akan lagi dikaitkan dengan grup tersebut. Faktanya, semua file yang terkait dengan grup itu tidak akan lagi dikaitkan dengan nama grup mana pun. Sebaliknya, file-file ini hanya akan dimiliki oleh GID, seperti yang ditunjukkan di bawah ini:

```
root@localhost:~# groupmod -g 10003 clerks

root@localhost:~# ls -l index.html

-rw-r-----. 1 root 491 13370 Aug  1 13:21 index.html
```

Perlu diingat!

File-file ini tanpa nama grup disebut file orphaned. Untuk mencari semua file yang hanya dimiliki oleh GID (tidak terkait dengan nama grup) gunakan opsi `-nogroup` dari perintah `find`:

```
root@localhost:~# find / -nogroup /root/index.html
```

DELETING A GROUP

Jika Anda memutuskan untuk menghapus grup dengan perintah `groupdel`, ketahuilah bahwa setiap file yang dimiliki oleh grup itu akan menjadi orphaned.

Hanya supplementary group yang dapat dihapus, jadi jika ada grup yang merupakan grup utama untuk user mana pun, itu tidak dapat dihapus. Administrator dapat mengubah grup mana yang merupakan grup utama user, sehingga grup yang digunakan sebagai grup utama dapat dibuat menjadi supplementary group dan kemudian dapat dihapus.

Selama grup yang akan dihapus bukan grup utama user, menghapus grup dilakukan dengan menggunakan perintah `groupdel` bersama dengan nama grup:

```
root@localhost:~# groupdel clerks
```

USERS

Informasi user account disimpan di file `/etc/passwd` dan informasi otentikasi user (data password) disimpan di file `/etc/shadow`. Membuat user baru dapat dilakukan dengan menambahkan baris baru secara manual ke masing-masing file ini, tetapi teknik itu umumnya bukan yang disarankan.

Dengan menggunakan perintah yang sesuai untuk menambahkan user baru, file ini dapat dimodifikasi secara otomatis dan aman. Jika Anda memodifikasi file-file ini secara manual, Anda berisiko membuat kesalahan yang dapat mencegah semua user untuk dapat masuk secara normal.

Sebelum Anda mulai membuat user untuk sistem Anda, Anda harus memverifikasi atau menetapkan nilai praktis yang digunakan secara default dengan perintah `useradd`. Pengaturan ini dapat ditemukan di file konfigurasi yang digunakan oleh perintah `useradd`.

Memastikan bahwa nilai dalam file konfigurasi ini normal sebelum menambahkan user dapat membantu menghemat waktu dan masalah Anda karena harus memperbaiki pengaturan user account setelah menambahkan user.

USER CONFIGURATION FILES

Opsi `-D` pada perintah `useradd` memungkinkan Anda untuk melihat atau mengubah beberapa nilai default yang digunakan oleh perintah `useradd`. Nilai yang ditampilkan oleh `useradd -D` juga dapat dilihat atau diperbarui dengan memanipulasi file `/etc/default/useradd`:

```
root@localhost:~# useradd -D

GROUP=100

HOME=/home
```

```
INACTIVE=-1  
  
EXPIRE=  
  
SHELL=/bin/bash  
  
SKEL=/etc/skel  
  
CREATE_MAIL_SPOOL=yes
```

Berikut ini penjelasan masing-masing nilai tersebut :

Group

```
GROUP=100
```

Dalam distribusi yang tidak menggunakan UPG, ini adalah grup utama default untuk user baru, jika tidak ditentukan dengan perintah `useradd`. Biasanya ini adalah grup user dengan GID 100.

Pengaturan ini mempengaruhi field ID grup utama dari file `/etc/passwd` yang disorot di bawah ini:

```
bob:x:600:600:bob:/home/bob:/bin/bash
```

Opsi `-g` pada perintah `useradd` memungkinkan Anda untuk menggunakan grup utama yang berbeda dari default saat membuat user account baru.

Home

```
HOME=/home
```

Direktori `/home` adalah direktori dasar default tempat direktori home baru user dibuat. Ini berarti bahwa user dengan nama akun `bob` akan memiliki direktori home `/home/bob`.

Pengaturan ini mempengaruhi field direktori home dari file `/etc/passwd` yang disorot di bawah ini:


```
bob:x:600:600:bob:/home/bob:/bin/bash
```

Opsi `-b` pada perintah `useradd` memungkinkan Anda menggunakan grup direktori dasar yang berbeda dari default saat membuat user account baru.

Inactive

```
INACTIVE=-1
```

Nilai ini mewakili jumlah hari setelah password kedaluwarsa akun tersebut dinonaktifkan. Nilai `-1` berarti fitur ini tidak diaktifkan secara default dan tidak ada nilai "inactive" yang diberikan untuk akun baru secara default.

Pengaturan ini mempengaruhi field tidak aktif dari file `/etc/shadow` yang disorot di bawah ini:

```
bob:pw:15020:5:30:7:60:15050:
```

Opsi `-f` pada perintah `useradd` memungkinkan Anda menggunakan nilai `INACTIVE` yang berbeda dari nilai default saat membuat user account baru.

Expire

```
EXPIRE=
```

Secara default, tidak ada nilai yang ditetapkan untuk tanggal kedaluwarsa. Biasanya, tanggal kedaluwarsa diatur pada akun individu, tidak semua akun secara default.

Misalnya, jika Anda memiliki kontraktor yang dipekerjakan untuk bekerja hingga penghujung hari pada 1 November 2019, maka Anda dapat memastikan bahwa mereka tidak dapat masuk setelah tanggal tersebut dengan menggunakan field `EXPIRE`.

Pengaturan ini mempengaruhi field kedaluwarsa dari file `/etc/shadow` yang disorot di bawah ini:

```
bob:pw:15020:5:30:7:60:15050:
```

Opsi `-e` pada perintah `useradd` memungkinkan Anda menggunakan nilai EXPIRE yang berbeda dari default saat membuat user account baru.

Shell

```
SHELL=/bin/bash
```

Pengaturan SHELL menunjukkan shell default untuk user saat mereka masuk ke sistem.

Pengaturan ini mempengaruhi field shell dari file `/etc/passwd` yang disorot di bawah ini:

```
bob:x:600:600:bob:/home/bob:/bin/bash
```

Opsi `-s` pada perintah `useradd` memungkinkan Anda menggunakan shell login yang berbeda dari default saat membuat user account baru.

Skeleton Directory

```
SKEL=/etc/skel
```

Nilai SKEL menentukan direktori skeleton mana yang isinya disalin ke direktori home user baru. Isi direktori ini disalin ke direktori home user baru, dan user baru diberikan kepemilikan file baru.

Pengaturan ini memberikan cara mudah kepada administrator untuk mengisi user account baru dengan file konfigurasi kunci.

Opsi `-k` pada perintah `useradd` memungkinkan Anda menggunakan direktori SKEL yang berbeda dari default saat membuat user account baru

Create Mail Spool

```
CREATE_MAIL_SPOOL=yes
```

Sebuah spool surat adalah file tempat email masuk ditempatkan.

Saat ini, nilai untuk membuat spool email adalah yes, yang berarti bahwa user secara default dikonfigurasi dengan kemampuan untuk menerima dan menyimpan email lokal. Jika Anda tidak berencana menggunakan surat lokal, maka nilai ini dapat diubah menjadi no.

Untuk mengubah salah satu nilai default `useradd`, file `/etc/default/useradd` dapat diedit dengan editor teks. Teknik lain (lebih aman) adalah dengan menggunakan perintah `useradd -D`.

Misalnya, jika Anda ingin mengizinkan user memiliki password kedaluwarsa yang masih dapat mereka masuki hingga tiga puluh hari, Anda dapat menggunakan perintah berikut:

```
root@localhost:~# useradd -D -f 30
root@localhost:~# useradd -D
GROUP=100
HOME=/home
INACTIVE=30
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
```

USER CONFIGURATION FILES

File `/etc/login.defs` juga berisi nilai yang diterapkan secara default untuk user baru yang Anda buat dengan perintah `useradd`. Tidak seperti file

`/etc/default/useradd`, file `/etc/login.defs` biasanya diedit langsung oleh administrator untuk mengubah nilainya.

File ini berisi banyak komentar dan baris kosong, jadi hanya untuk menampilkan baris yang bukan komentar atau baris kosong (pengaturan konfigurasi sebenarnya), maka Anda dapat menggunakan perintah `grep` berikut:

```
root@localhost:~# grep -Ev '^#|^$' /etc/login.defs

MAIL_DIR            /var/mail/spool

PASS_MAX_DAYS       99999

PASS_MIN_DAYS        0

PASS_MIN_LEN         5

PASS_WARN_AGE        7

UID_MIN              500

UID_MAX              60000

GID_MIN              500

GID_MAX              60000

CREATE_HOME          yes

UMASK                 077

USERGROUPS_ENAB      yes

ENCRYPT_METHOD        SHA512

MD5_CRYPT_ENAB       no
```

Contoh di atas mewakili file `/etc/login.defs` distribusi CentOS 6 yang khas dengan nilainya. Yang berikut menjelaskan masing-masing nilai ini:

Mail Directory

```
MAIL_DIR            /var/mail/spool
```

Direktori tempat file spool email user dibuat.

Password Maximum Days

```
PASS_MAX_DAYS 99999
```

Pengaturan ini menentukan jumlah hari maksimum user dapat terus menggunakan password yang sama. Karena defaultnya adalah 99999 hari (lebih dari 200 tahun) itu secara efektif berarti user tidak perlu mengubah password mereka.

Organisasi dengan kebijakan yang efektif untuk menjaga password yang aman biasanya mengubah nilai ini menjadi 60 atau 30 hari.

Pengaturan ini mempengaruhi pengaturan default dari file `/etc/shadow` yang disorot di bawah ini:

```
bob:pw:15020:5:30:7:60:15050:
```

Password Minimum Days

```
PASS_MIN_DAYS 0
```

Dengan set ini ke nilai default nol, waktu tersingkat yang diperlukan user untuk menyimpan password adalah nol hari, yang berarti mereka dapat segera mengubah password yang baru saja mereka setel.

Jika nilai `PASS_MIN_DAYS` disetel menjadi tiga hari, maka setelah menyetel password baru, user harus menunggu tiga hari sebelum mereka dapat mengubahnya lagi.

Pengaturan ini mempengaruhi pengaturan default dari file `/etc/shadow` yang disorot di bawah ini:

```
bob:pw:15020:3:30:7:60:15050:
```

Password Minimum Length

```
PASS_MIN_LEN    5
```

Ini menunjukkan jumlah minimum karakter yang harus dimiliki password.

Password Warning

```
PASS_WARN_AGE   7
```

Ini adalah default untuk field peringatan. Saat user mendekati jumlah hari maksimum mereka dapat menggunakan password mereka, sistem akan memeriksa untuk melihat apakah sudah waktunya untuk mulai memperingatkan user tentang mengubah password mereka saat login.

Pengaturan ini mempengaruhi pengaturan default dari file `/etc/shadow` yang disorot di bawah ini:

```
bob:pw:15020:3:30:7:60:15050:
```

UID Minimum

```
UID_MIN          500
```

UID_MIN menentukan UID pertama yang ditetapkan untuk user biasa. UID apapun yang kurang dari nilai ini akan digunakan untuk akun sistem atau akun root.

UID Maximum

```
UID_MAX          60000
```

Sebuah UID secara teknis bisa memiliki nilai lebih dari empat miliar. Untuk kompatibilitas maksimum, disarankan untuk membiarkannya pada nilai default 60000.

GID Minimum

GID_MIN	500
---------	-----

GID_MIN menentukan GID pertama yang ditetapkan ke grup biasa. Grup apa pun dengan GID kurang dari nilai ini akan menjadi grup sistem atau grup root.

GID Maximum

GID_MAX	60000
---------	-------

Sebuah GID, seperti UID, dapat memiliki nilai lebih dari empat miliar. Apa pun nilai yang Anda gunakan untuk UID_MAX Anda, harus digunakan untuk GID_MAX untuk mendukung UPG.

Home Directory

CREATE_HOME	yes
-------------	-----

Nilai ini menentukan apakah direktori baru dibuat untuk user atau tidak saat akun mereka dibuat.

Mesin virtual kami tidak menyertakan nilai ini. Oleh karena itu, direktori home tidak dibuat untuk user baru kecuali ditentukan.

Umask

UMASK	077
-------	-----

UMASK berfungsi pada saat direktori home user dibuat; itu menentukan izin default apa yang ditempatkan di direktori ini. Menggunakan nilai default 077 untuk UMASK berarti hanya pemilik user yang memiliki izin untuk mengakses direktorinya.

Nilai UMASK akan dibahas lebih rinci pada bab perizinan.

UPG

```
USERGROUPS_ENAB yes
```

Dalam distribusi yang menampilkan grup pribadi untuk setiap user, seperti yang ditunjukkan contoh CentOS ini, `USERGROUPS_ENAB` akan memiliki nilai `yes`. Jika UPG tidak digunakan dalam distribusi, maka ini akan memiliki nilai `no`.

Encryption

```
ENCRYPT_METHOD SHA512
```

Metode enkripsi yang digunakan untuk mengenkripsi password user di file `/etc/shadow`. Pengaturan `ENCRYPT_METHOD` menggantikan pengaturan `MD5_CRYPT_ENAB`.

Encryption (Deprecated)

```
MD5_CRYPT_ENAB no
```

Setelan yang tidak berlaku lagi ini awalnya memungkinkan administrator untuk menentukan menggunakan enkripsi password MD5 bukannya enkripsi DES asli. Ini telah digantikan oleh setelan `ENCRYPT_METHOD`.

ACCOUNT CONSIDERATIONS

Membuat user account untuk digunakan dengan sistem Linux mungkin mengharuskan Anda mengumpulkan beberapa informasi. Meskipun yang mungkin diperlukan hanyalah nama akun, Anda mungkin juga ingin merencanakan untuk menetapkan UID, primary group, supplementary group, direktori home, direktori skeleton, dan shell yang akan digunakan. Saat merencanakan nilai-nilai ini, pertimbangkan hal berikut:

Username

Satu-satunya argumen yang diperlukan untuk perintah `useradd` adalah nama yang Anda inginkan untuk akun tersebut. Nama user harus mengikuti pedoman yang sama seperti untuk nama grup. Mengikuti pedoman ini dapat membantu Anda memilih nama user yang portable:

- Karakter pertama dari nama harus berupa karakter garis bawah `_` atau karakter a-z huruf kecil.
- Hingga 32 karakter diperbolehkan pada sebagian besar distribusi Linux, tetapi menggunakan lebih dari 16 dapat menimbulkan masalah karena beberapa distribusi mungkin tidak menerima lebih dari 16.
- Setelah karakter pertama, karakter yang tersisa dapat berupa alfanumerik, tanda hubung (`-`) karakter garis bawah (`_`).
- Karakter terakhir tidak boleh berupa karakter tanda hubung.

Jika user perlu mengakses beberapa sistem, biasanya disarankan untuk memiliki nama akun yang sama pada sistem tersebut. Nama akun harus unik untuk setiap user.

```
root@localhost:~# useradd jane
```

User Identifier (UID)

Setelah Anda membuat user dengan UID tertentu, sistem biasanya menambah UID satu untuk user berikutnya yang Anda buat. Jika terhubung ke jaringan dengan sistem lain, Anda mungkin ingin memastikan bahwa UID ini sama di semua sistem untuk membantu memberikan akses yang konsisten.

Menambahkan opsi `-u` ke perintah `useradd` memungkinkan Anda menentukan nomor UID. UID biasanya dapat berkisar dari nol hingga lebih dari empat miliar, tetapi untuk kompatibilitas terbesar dengan sistem yang lebih lama, nilai UID maksimum yang disarankan adalah 60.000.

```
root@localhost:~# useradd -u 1000 jane
```

User root memiliki UID 0, yang memungkinkan akun tersebut memiliki hak khusus. Setiap akun dengan UID 0 secara efektif dapat bertindak sebagai administrator.

Akun sistem umumnya digunakan untuk menjalankan layanan latar belakang yang disebut *daemon*. Dengan tidak menjalankan layanan sebagai user root, jumlah kerusakan yang dapat dilakukan dengan akun layanan yang disusupi menjadi terbatas. Akun sistem yang digunakan oleh layanan umumnya menggunakan UID yang berada dalam kisaran yang dicadangkan. Satu akun sistem yang merupakan pengecualian untuk aturan ini adalah user `nfsnobody`, yang memiliki UID 65534.

Rentang cadangan yang digunakan untuk akun layanan telah berkembang dari waktu ke waktu. Awalnya, ini untuk UID antara 1 dan 99. Kemudian, diperluas menjadi antara 1 dan 499. Tren saat ini di antara distribusi adalah bahwa akun sistem adalah akun yang memiliki UID antara 1 dan 999, tetapi kisaran 1-499 adalah juga masih umum digunakan.

Saat menyiapkan sistem baru, praktik yang baik adalah memulai UID tidak lebih rendah dari 1000 untuk memastikan tersedia cukup UID untuk banyak layanan sistem dan memberi Anda kemampuan untuk membuat banyak GID dalam rentang yang dicadangkan.

Primary Group

Dalam distribusi yang menampilkan UPG, grup ini dibuat secara otomatis dengan GID dan nama grup yang sesuai dengan UID dan nama user user account yang baru dibuat. Dalam distribusi yang tidak menggunakan UPG, primary groupbiasanya didefaultkan ke grup user dengan GID 100.

Untuk menentukan primary groupdengan perintah `useradd`, gunakan opsi `-g` dengan nama atau GID grup. Misalnya, untuk menentukan user sebagai grup utama:

```
root@localhost:~# useradd -g users jane
```

Supplementary Group

Untuk membuat user menjadi anggota dari satu atau lebih supplementary group, opsi `-G` dapat digunakan untuk menentukan daftar nama atau nomor grup yang dipisahkan koma. Misalnya untuk menentukan `sales` dan `research` sebagai supplementary groups.

```
root@localhost:~# useradd -G sales,research jane
```

Home Directory

Secara default, sebagian besar distribusi membuat direktori home user dengan nama yang sama dengan user account di bawah direktori dasar mana pun yang ditentukan dalam pengaturan HOME dari file `/etc/default/useradd`, yang biasanya menentukan direktori `/home`. Misalnya, jika membuat user account bernama `jane`, direktori beranda baru user tersebut adalah `/home/jane`.

```
root@localhost:~# useradd jane
root@localhost:~# grep '/home/jane' /etc/passwd
jane:x:1008:1010::/home/jane:/bin/sh
```

Ada beberapa opsi untuk perintah `useradd` yang dapat mempengaruhi pembuatan direktori home user:

- Jika `CREATE_HOME` disetel ke `no` atau setelah ini tidak ada, direktori tidak akan dibuat secara otomatis. Jika tidak, opsi `-M` digunakan untuk menentukan ke perintah `useradd` bahwa ia tidak boleh membuat direktori home, meskipun `CREATE_HOME` disetel ke `yes`.
- Jika pengaturan `CREATE_HOME` di file `/etc/login.defs` diatur ke `yes`, direktori home dibuat secara otomatis. Jika tidak, opsi `-m` dapat digunakan untuk membuat direktori home:

```
root@localhost:~# useradd -m jane
root@localhost:~# ls -ld /home/jane
```

```
drwxr-xr-x 2 jane jane 4096 Dec 18 19:14 /home/jane
```

- Opsi `-b` memungkinkan Anda untuk menentukan direktori dasar yang berbeda di mana direktori home user dibuat. Misalnya, berikut ini membuat user account jane dengan `/test/jane` dibuat sebagai direktori home user:

```
root@localhost:~# useradd -mb /test jane
root@localhost:~# ls -ld /test/Jane
drwxr-xr-x 2 jane jane 4096 Dec 18 19:16 /test/jane
```

- Opsi `-d` memungkinkan Anda untuk menentukan direktori yang ada atau direktori home baru yang akan dibuat untuk user. Ini harus menjadi jalur lengkap untuk direktori home user. Misalnya, berikut ini membuat user account jane dengan `/test/jane` dibuat sebagai direktori home user:

```
root@localhost:~# useradd -md /test/jane jane
root@localhost:~# ls -ld /test/jane
drwxr-xr-x 2 jane jane 4096 Dec 18 19:19 /test/jane
```

Opsi `-k` untuk menentukan direktori skeleton yang berbeda. Saat menggunakan opsi `-k`, opsi `-m` diperlukan.

Skeleton Directory

Secara default, konten direktori `/etc/skel` disalin ke direktori home user baru. File yang dihasilkan juga dimiliki oleh user baru. Dengan menggunakan opsi `-k` dengan perintah `useradd`, konten direktori yang berbeda dapat digunakan untuk mengisi direktori home user baru. Saat menentukan direktori skeleton dengan opsi `-k`, opsi `-m` harus digunakan atau perintah `useradd` akan gagal dengan error.

Contoh berikut menggunakan `/home/sysadmin` sebagai direktori skeleton:

```
root@localhost:~# useradd -mk /home/sysadmin jane
```

```
root@localhost:~# ls /home/jane  
  
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  
Videos
```

Shell

Sementara shell default ditentukan di file `/etc/default/useradd`, itu juga dapat diganti dengan perintah `useradd` menggunakan opsi `-s` pada saat pembuatan akun:

```
root@localhost:~# useradd -s /bin/bash jane
```

Merupakan hal yang umum untuk menentukan shell `/sbin/nologin` untuk akun yang akan digunakan sebagai akun sistem.

Comment

Field komentar, awalnya disebut field General Electric Comprehensive Operating System (GECOS), biasanya digunakan untuk menyimpan nama lengkap user. Banyak program login grafis menampilkan nilai field ini, bukan nama akun. Opsi `-c` dari perintah `useradd` memungkinkan nilai field ini ditentukan.

```
root@localhost:~# useradd -c 'Jane Doe' jane
```

CREATING A USER

Setelah Anda memverifikasi nilai default mana yang akan digunakan dan Anda telah mengumpulkan informasi tentang user, maka Anda siap untuk membuat user account. Contoh perintah `useradd` yang menggunakan beberapa opsi terlihat seperti berikut:

```
root@localhost:~# useradd -u 1009 -g users -G sales,research -m -c  
'Jane Doe' jane
```

Contoh perintah `useradd` ini membuat user dengan UID 1009, grup user utama, keanggotaan tambahan dalam grup `sales` dan `research`, komentar "Jane Doe", dan nama akun `jane`.

Setelah menjalankan perintah sebelumnya, informasi tentang user account `jane` secara otomatis ditambahkan ke file `/etc/passwd` dan `/etc/shadow`, sedangkan informasi tentang akses supplementary group secara otomatis ditambahkan ke `/etc/group` dan file `/etc/gshadow`:

```
root@localhost:~# grep jane /etc/passwd
jane:x:1009:100:Jane Doe:/home/jane:/bin/sh

root@localhost:~# grep jane /etc/shadow
jane:!:17883:0:99999:7:30::

root@localhost:~# grep jane /etc/group
research:x:1005:jane
sales:x:999:jane

root@localhost:~# grep jane /etc/gshadow
research:!::jane
sales:!::jane
```

Perhatikan bahwa akun tersebut belum memiliki password yang valid!

Selain itu, jika `CREATE_MAIL_SPOOL` disetel ke `yes` maka file spool surat `/var/spool/mail/jane` dibuat:

```
root@localhost:~# ls /var/spool/mail
jane root rpc sysadmin
```

Akhirnya, karena opsi `-m` digunakan, direktori `/home/jane` dibuat dengan izin yang hanya mengizinkan akses user `jane`, dan konten direktori `/etc/skel` akan disalin ke direktori:

```
root@localhost:~# ls /home  
  
jane sysadmin
```

PASSWORDS

Memilih password yang baik bukanlah tugas yang mudah, tetapi sangat penting dilakukan dengan benar atau keamanan akun (mungkin seluruh sistem) dapat diragukan. Memilih password yang baik hanyalah permulaan; Anda harus sangat berhati-hati dengan password Anda agar tidak diungkapkan kepada orang lain. Anda tidak boleh memberi tahu siapa pun password Anda dan jangan pernah membiarkan siapa pun melihat Anda mengetik password Anda. Jika Anda memang memilih untuk menuliskan password Anda, maka Anda harus menyimpannya dengan aman di tempat seperti brankas atau safe deposit box.

Sangat mudah untuk membuat password yang buruk! Jika Anda menggunakan informasi apa pun dalam password Anda yang terkait dengan Anda, maka informasi ini juga dapat diketahui atau ditemukan oleh orang lain, sehingga password Anda mudah dibobol. Password Anda tidak boleh berisi informasi tentang Anda atau siapa pun yang Anda kenal, seperti nama depan, nama tengah, nama belakang, ulang tahun, telepon, nama hewan peliharaan, SIM, atau nomor jaminan sosial.

Ada banyak faktor yang perlu dipertimbangkan saat Anda mencoba memilih password untuk sebuah akun:

- **Length:** File `/etc/login.defs` memungkinkan administrator untuk menentukan panjang minimum password. Beberapa orang percaya bahwa semakin panjang password, semakin baik, ini tidak benar. Masalah dengan password yang terlalu panjang adalah password tidak mudah diingat dan, akibatnya, sering ditulis di tempat di mana password dapat dengan mudah ditemukan dan disusupi.
- **Komposisi:** Password yang baik harus terdiri dari kombinasi karakter alfabet, numerik dan simbolik.

- Life time: Jumlah waktu maksimum password dapat digunakan harus dibatasi karena beberapa alasan:
 - Jika sebuah akun dibobol dan waktu password yang valid dibatasi, penyusup pada akhirnya akan kehilangan akses ketika password menjadi tidak valid.
 - Jika akun tidak sedang digunakan, maka secara otomatis dapat dinonaktifkan ketika password tidak lagi valid.
 - Jika penyerang mencoba serangan "brute-force" dengan mencoba setiap kemungkinan password, maka password dapat diubah sebelum serangan berhasil.

Namun, mengharuskan user untuk mengubah password terlalu sering dapat menimbulkan masalah keamanan, termasuk:

- Kualitas password yang dipilih user mungkin terganggu.
- User dapat mulai menulis password mereka di atas kertas, meningkatkan kemungkinan password dapat ditemukan.
- User account yang jarang digunakan dapat menjadi kedaluwarsa dan memerlukan perhatian administratif untuk mengatur ulang.

Ada berbagai macam pendapat tentang seberapa sering user harus dipaksa untuk mengubah password mereka. Untuk akun yang sangat sensitif, disarankan untuk mengubah password lebih sering, seperti setiap 30 hari. Di sisi lain, untuk akun non-kritis tanpa akses ke informasi sensitif, tidak perlu terlalu sering melakukan perubahan. Untuk akun dengan risiko minimal, durasi 90 hari akan dianggap lebih masuk akal.

SETTING A USER PASSWORD

Ada beberapa cara untuk mengubah password user. User dapat menjalankan perintah `passwd`, administrator dapat menjalankan perintah `passwd` dengan memberikan nama user sebagai argumen, atau alat grafis juga tersedia.

Administrator dapat menggunakan perintah `passwd` untuk menyetel password awal atau mengubah password untuk akun tersebut. Misalnya, jika administrator telah membuat akun jane, maka menjalankan `passwd jane` akan memberikan administrator prompt untuk mengatur password untuk akun jane. Jika berhasil diselesaikan, maka file `/etc/shadow` akan diperbarui dengan password baru user. Meskipun user biasa harus mengikuti banyak aturan password, user root hanya perlu mengikuti satu aturan: password tidak boleh dibiarkan kosong. Ketika user root melanggar semua aturan password lain yang biasanya berlaku untuk user biasa, itu menghasilkan peringatan yang dicetak ke layar dan aturan tidak diberlakukan:

```
root@localhost:~# passwd Jane
Enter new UNIX password:
BAD PASSWORD: it is WAY to short
BAD PASSWORD: is too simple
Retype new UNIX password:
```

Dengan asumsi bahwa administrator telah menetapkan password untuk user account, user kemudian dapat masuk dengan nama akun dan password tersebut. Setelah user membuka terminal, mereka dapat menjalankan perintah `passwd` tanpa argumen untuk mengubah password mereka sendiri. Mereka diminta memasukkan password saat ini dan kemudian diminta memasukkan password baru dua kali. Sebagai user biasa, mungkin sulit untuk mengatur password yang valid karena semua aturan untuk password harus diikuti. User biasanya diperbolehkan tiga kali mencoba memberikan password yang valid sebelum perintah `passwd` keluar dengan error.

Dengan menggunakan hak istimewa dari user root, password terenkripsi dan informasi terkait password lainnya dapat dilihat dengan melihat file `/etc/shadow`. Ingatlah bahwa user biasa tidak dapat melihat konten file ini.

MANAGING PASSWORD AGING

Perintah `chage` menyediakan banyak opsi untuk mengelola informasi penuaan password yang ditemukan di file `/etc/shadow`.

Berikut ringkasan opsi `chage`:

Short Option	Long Option	Description
<code>-l</code>	<code>--list</code>	List informasi umur akun
<code>-d LAST_DAY</code>	<code>--lastday LAST_DAY</code>	Setel tanggal perubahan password terakhir ke <code>LAST_DAY</code>
<code>-E EXPIRE_DATE</code>	<code>--expiredate EXPIRE_DATE</code>	Setel akun agar kedaluwarsa pada <code>EXPIRE_DATE</code>
<code>-h</code>	<code>--help</code>	menunjukkan bantuan untuk perintah <code>chage</code>
<code>-I INACTIVE</code>	<code>--inactive INACTIVE</code>	Setel akun untuk mengizinkan masuk selama <code>INACTIVE</code> hari setelah password kedaluwarsa
<code>-m MIN_DAYS</code>	<code>--mindays MIN_DAYS</code>	Tetapkan jumlah hari minimum sebelum password dapat diubah menjadi <code>MIN_DAYS</code>
<code>-M MAX_DAYS</code>	<code>--maxdays MAX_DAYS</code>	Tetapkan jumlah hari maksimum sebelum password diubah menjadi <code>MAX_DAYS</code>

Short Option	Long Option	Description
<code>-W WARN_DAYS</code>	<code>--warndays WARN_DAYS</code>	Setel jumlah hari sebelum password kedaluwarsa untuk mulai menampilkan peringatan ke WARN_DAYS

Contoh yang baik dari perintah `chage` adalah mengubah jumlah hari maksimum di mana password seseorang valid menjadi 60 hari:

```
root@localhost:~# chage -M 60 jane
root@localhost:~# grep jane /etc/shadow | cut -d: -f1,5
jane:60
```

MODIFYING A USER

Sebelum membuat perubahan pada user account, pahami bahwa beberapa perintah tidak akan berhasil mengubah user account jika user saat ini masuk (seperti mengubah nama login user).

Perubahan lain yang mungkin Anda buat tidak akan efektif jika user masuk, tetapi akan berlaku segera setelah user keluar dan kemudian masuk lagi. Misalnya, saat mengubah keanggotaan grup, keanggotaan baru tidak akan tersedia untuk user hingga user masuk lagi.

Dalam kedua kasus tersebut, akan sangat membantu untuk mengetahui cara menggunakan perintah `who`, `w`, dan `last`, sehingga Anda dapat mengetahui siapa yang masuk ke sistem, karena ini dapat memengaruhi perubahan yang ingin Anda lakukan pada user account.

Perintah `who` dan `w` menampilkan siapa yang saat ini masuk ke sistem. Perintah `w` lebih rinci dari keduanya, karena ini menunjukkan waktu aktif sistem dan memuat informasi serta proses apa yang dijalankan setiap user. Perintah `last` dapat digunakan untuk menentukan sesi login saat ini dan sebelumnya serta tanggal dan

waktu spesifiknya. Dengan memberikan nama user atau nama `tty` (terminal) sebagai argumen, perintah hanya menampilkan record yang cocok dengan nama itu.

Perintah `usermod` menawarkan banyak opsi untuk mengubah user account yang ada. Banyak dari opsi ini juga tersedia dengan perintah `useradd` pada saat akun dibuat. Bagan berikut memberikan ringkasan opsi `usermod`:

Short Option	Long Option	Description
<code>-c</code>	<code>COMMENT</code>	Setel nilai GECOS atau kolom komentar ke COMMENT.
<code>-d HOME_DIR</code>	<code>--home HOME_DIR</code>	Menetapkan HOME_DIR sebagai direktori beranda baru untuk user.
<code>-e EXPIRE_DATE</code>	<code>--expiredate EXPIRE_DATE</code>	Tetapkan tanggal kedaluwarsa akun menjadi EXPIRE_DATE.
<code>-f INACTIVE</code>	<code>--inactive INACTIVE</code>	Setel akun untuk mengizinkan masuk selama INACTIVE hari setelah password kedaluwarsa.
<code>-g GROUP</code>	<code>--gid GROUP</code>	Tetapkan GROUP sebagai grup utama.
<code>-G GROUPS</code>	<code>--groups GROUPS</code>	Setel supplementary group ke daftar yang ditentukan di GROUPS.
<code>-a</code>	<code>--append</code>	Tambahkan supplementary groupuser dengan yang

Short Option	Long Option	Description
		ditentukan oleh opsi <code>-G</code> .
<code>-h</code>	<code>--help</code>	Tampilkan bantuan untuk perintah <code>usermod</code> .
<code>-l NEW_LOGIN</code>	<code>--login NEW_LOGIN</code>	Ubah nama login user.
<code>-L</code>	<code>--lock</code>	Kunci user account.
<code>-s SHELL</code>	<code>--shell SHELL</code>	Tentukan shell login untuk akun.
<code>-u NEW_UID</code>	<code>--uid NEW_UID</code>	Tentukan UID user menjadi <code>NEW_UID</code> .
<code>-U</code>	<code>--unlock</code>	Buka kunci user account.

Beberapa dari opsi ini layak untuk dibahas karena pengaruhnya terhadap manajemen user. Ini bisa sangat bermasalah untuk mengubah UID user dengan opsi `-u`, karena file apa pun yang dimiliki oleh user akan menjadi orphaned. Di sisi lain, menentukan nama login baru untuk user dengan `-l` tidak menyebabkan file menjadi orphaned.

Menghapus user dengan perintah `userdel` dapat menjadi orphaned atau menghapus file user di sistem. Daripada menghapus akun, pilihan lain adalah mengunci akun dengan opsi `-L` untuk perintah `usermod`. Mengunci akun mencegah akun digunakan, tetapi kepemilikan file tetap ada.

Ada beberapa hal penting yang perlu diketahui tentang pengelolaan supplementary groups. Jika Anda menggunakan opsi `-G` tanpa opsi `-a`, Anda

harus membuat daftar semua grup yang akan menampung user tersebut. Menggunakan opsi `-G` saja dapat mengakibatkan penghapusan user secara tidak sengaja dari semua supplementary group sebelumnya tempat user tersebut berada. Jika Anda menggunakan opsi `-a` dengan `-G` maka Anda hanya perlu membuat daftar grup baru yang akan menampung user tersebut. Misalnya, jika user jane saat ini termasuk dalam grup `sales` dan `research`, maka untuk menambahkan akunnya ke grup `development`, jalankan perintah berikut:

```
root@localhost:~# usermod -aG development jane
```

DELETING A USER

Perintah `userdel` digunakan untuk menghapus user. Saat Anda menghapus user account, Anda juga perlu memutuskan apakah akan menghapus direktori beranda user. File user mungkin penting bagi organisasi, dan bahkan mungkin ada persyaratan hukum untuk menyimpan data selama jangka waktu tertentu, jadi berhati-hatilah untuk tidak membuat keputusan ini enteng. Selain itu, kecuali Anda telah membuat salinan cadangan data, setelah Anda menjalankan perintah untuk menghapus user dan file mereka, tidak ada tindakan yang dapat dibatalkan.

Untuk menghapus user jane tanpa menghapus direktori home `/home/jane` user, jalankan:

```
root@localhost:~# userdel jane
```

Berhati-hatilah bahwa menghapus user tanpa menghapus direktori home-nya berarti file direktori home user akan menjadi orphaned dan file-file ini hanya akan dimiliki oleh UID dan GID sebelumnya.

Untuk menghapus user, direktori home, dan mail spool juga, gunakan opsi `-r`:

```
root@localhost:~# userdel -r jane
```

PERINGATAN: Perintah di atas hanya akan menghapus file user di direktori home dan spool email mereka. Jika user memiliki file lain di luar direktori home mereka, maka file tersebut akan tetap ada sebagai file orphaned.

Referensi:

<https://www.netacad.com/courses/os-it/ndg-linux-essentials>