Linux
Kullanıcıları
Derneği

Linux Kullanıcı Yönetimi/Denetimi

Emre Eryılmaz

emre.eryilmaz@linux.org.tr

Linux Kullanıcıları Derneği

3 Şubat 2012

Kullanıcı Nedir?

- Herhangi bir dizgeye göre, o dizgenin sağladığı işlevlerden yararlanmak üzere dizgeyle etkileşime giren kişi ya da kuruluş.(BTS)
- Kullanıcı hesabı, sistem üzerinde erişiminizin olduğu dosya ve klasörleri, bilgisayarda yapabileceğiniz değişiklikleri ve yapacağı işlemleri veya masaüstü düzenleme gibi kişisel tercihlerinizi bildiren bir bilgi koleksiyonudur. Kullanıcı hesapları, sistemi bir ya da birden fazla kişiyle paylaşırken, aynı zamanda kendi dosya ve ayarlarınıza sahip olmanıza olanak tanır. Her kişi kendi kullanıcı hesabına bir kullanıcı adı ve parolayla erişir.

Kullanıcı Çeşitleri

- Linux üzerindeki üç tür kullanıcı bulunur.
- Linux üzerindeki kullanıcı çeşitleri:
  - Root User (Nam-ı değer Super user) Kök kullanıcı (UID = 0 , GID = 0)
  - System Users (ftpd , sshd ,portage) (UID = 1 – 499 , GID= 1 – 499)
  - Normal Users (UID = 500 < , GID = 500 <)

Kullanıcı Çeşitleri

```
vaio semrelin # id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10
(wheel),11(floppy),26(tape),27(video)
```

```
semrelin@vaio ~ $ id
uid=1000(semrelin) gid=1000(semrelin) groups=1000(semrelin),10(wheel),18(audio),
19(cdrom),27(video),85(usb),100(users),104(plugdev),998(kvm)
```

Kullanıcı Ekleme

- Sistem üzerindeki kullanıcıları sağlıklı yönetmek ve denetlemek istiyorsanız ,bunun ilk adımı kullanıcıyı sistem üzerinde oluştururken başlar.
- Sistem üzerinde kullanıcılar “useradd” ya da “adduser” komutu ile oluşturulur.
- “useradd” komutu alabileceği birden çok parametre ile sistem üzerinde istediğimiz özelliklerde kullanıcı oluşturabiliriz.

“useradd” ile Kullanıcı oluşturma

- “-b” --base-dir
- “-d” –home
- “-e” --expiredate
- “f” --inactive
- “-g” ve “-G” , --gid ve –groups
- “-m” --create-home
- “-r” --system
- “-s” --shell

“useradd” ile Kullanıcı oluşturma

- “-u” ve “-U” , “--uid” ve “--user-group”
- “-Z” SELinux kullanıcısı
- Maksimum “32” karakter uzunluğunda
- Kullanıcı adı küçük(lower case) ile başlamalı
- Eklenecek yeni kullanıcıların değişkenleri “ /etc/login.defs” altından değiştirilebilir.
- Eklenen kullanıcılar “/etc/passwd” dosyasında saklanır.

Kullanıcıları ve Süreçleri Takip Etme

- Pstree (-p)
- Ps -aux
- Top
- Kill <pid no>
- Kilall <komut adı>
- Kill -9 <pid no>
- Kill -HUP <pid no>

LSOF

- Process'lere bağlı açık dosya ve portlar
- “lsof <dosya adi>” dosyanın hangi process tarafından kullanıldığını listeler.

```
[root@node DIR]# lsof /var/log/mailman/qrunner
python  18538 mailman    4u   REG    3,5  657 486746 /var/log/mailman/qrunner
python  18578 mailman    6u   REG    3,5  657 486746 /var/log/mailman/qrunner
python  18579 mailman    6u   REG    3,5  657 486746 /var/log/mailman/qrunner
python  18580 mailman    6u   REG    3,5  657 486746 /var/log/mailman/qrunner
python  18581 mailman    6u   REG    3,5  657 486746 /var/log/mailman/qrunner
python  18582 mailman    6u   REG    3,5  657 486746 /var/log/mailman/qrunner
python  18583 mailman    6u   REG    3,5  657 486746 /var/log/mailman/qrunner
python  18584 mailman    6u   REG    3,5  657 486746 /var/log/mailman/qrunner
```

LSOF

- “lsof” açık olan bütün dosyaları listeler.(Uzun bir listedir)
- “lsof -u <user id>” Bu kullanıcı tarafından açılmış olan tüm dosyaları listeler.
- “lsof -i TCP:port no” Hangi portun hangi process tarafından dinlendiğini listeler.

LSOF

```
[root@node DIR]# lsof -i TCP:389
COMMAND   PID USER   FD   TYPE  DEVICE SIZE NODE NAME
slapd    5927 ldap    6u  IPv4 7560023       TCP *:ldap (LISTEN)
slapd    5928 ldap    6u  IPv4 7560023       TCP *:ldap (LISTEN)
slapd   21185 ldap    6u  IPv4 7560023       TCP *:ldap (LISTEN)
slapd   21186 ldap    6u  IPv4 7560023       TCP *:ldap (LISTEN)
slapd   21193 ldap    6u  IPv4 7560023       TCP *:ldap (LISTEN)
```

ULIMIT

- “ulimit” ile kaynakları sınırlandırın.
- “ulimit -a” öntanımlı limitleri görüntüleyin.

```
vaio semrelin # ulimit -a
core file size              (blocks, -c) 0
data seg size               (kbytes, -d) unlimited
scheduling priority                 (-e) 0
file size                   (blocks, -f) unlimited
pending signals                     (-i) 47046
max locked memory           (kbytes, -l) 64
max memory size             (kbytes, -m) unlimited
open files                          (-n) 1024
pipe size                (512 bytes, -p) 8
POSIX message queues         (bytes, -q) 819200
real-time priority                  (-r) 0
stack size                  (kbytes, -s) 8192
cpu time                   (seconds, -t) unlimited
max user processes                  (-u) 47046
virtual memory              (kbytes, -v) unlimited
file locks                          (-x) unlimited
```

ULIMIT

- “ulimit -u <process sayısı>” tek kullanıcının açabileceği maksimum process sayısı
- “ulimit -n <dosya sayısı>” kullanıcının açabileceği maksimum dosya sayısı.
- “ulimit -f <size>” kullanıcının oluşturabileceği maksimum dosya büyüklüğü.
- “ulimit -m <bellek miktarı>” kullanıcının kullanabileceği maksimum bellek miktarı.
- Hard limit (-H) ve Soft Limit (-S)

Kullanıcı Kaynakları Kısmak

- “/etc/security/limits.conf” dosyasında “ulimit” ile yaptığımız kısıtlama ve kaynak limitlerini ayarlayabiliriz.
- “/etc/security/access.conf” dosyasında local ve network üzerinden bağlanan kullanıcıları kısıtlayabiliriz.
- “/etc/security/group.conf” dosyasında aygıt gruplarını kısıtlayabiliriz.
- “/etc/security/time.conf” dosyasında kullanıcıların erişim sürelerini kısıtlayabiliriz.

SUDO

- Öntanımlı gelebilir.Eğer sistem üzerinde yoksa “sudoers” paketini dağıtımın “Paket Deposu”ndan “Paket Yöneticisi” ile kurabilirsiniz.
- “sudo” sistem üzerindeki herhangi bir kullanıcının ya da super user(root)'un komutlarını verebilmesini sağlar.
- “/etc/sudoers” dosyasında konfigurasyon yapabiliriz.
- usernames/group servername = (username) command

Örnek “sudo” konfigurasyonları

- “%wheel ALL=(ALL) ALL” satırı bu gruptaki herkesin herhangi komutu çalıştırmasını sağlar.
- “%wheel ALL=(ALL) NOPASSWD: ALL” yukardaki işlemleri parolasız yapmaya imkan tanır.
- “ALL ALL=(ALL) ALL” sistem üzerindeki tüm kullanıcılara root komutlarını çalıştırma yetkisi verir.
- “username ALL=(ALL) ALL” kullanıcıya root yetkisi verir.

Kullanıcıları ve Süreçleri Kontrol Etme

- Sistem üzerinde tam denetim sağlamak özellikle güvenlik açısından çok önemlidir.Çünkü herhangi bir saldırı sadece dışardan değil , içerden de gelebilir ve ya kullanıcı sistem üzerinde zararlı bir program çalıştırabilir.İşte bu nokta da kullanıcıları ve süreçleri kontrol altında tutmak gerekir.
- GNU/Linux üzerinde “acct” (GNU Accounting Utilities) adlı araçla kullanıcı ve süreçleri izleyebiliriz.İlk olarak eğer sistem üzerinde “acct” kurulu değil ise kurulumunu yapalım.

GNU ACCT Kurulumu

- Dağıtımlar arası GNU Acct paket adı değişebilir.Bazı dağıtımlarda “psacct” yerine “acct” yazarak kurabilirsiniz.
- yum install psacct (CentOS için)
- emerge acct (Gentoo için)
- yum install acct (Suse için)
- Kurulum yaptıktan sonra “/var” dizini altında “account” adlı bir klasör ve bu klasörün içinde “pacct” adlı dosya oluşturması gerekir.Eğer bu klasör ve dosyayı oluşturmamışsa elle oluşturalım.

GNU ACCT Kurulumu

- mkdir /var/account
- touch /var/account/pacct
- chmod 660 /var/account/pacct
- Şimdi süreç kayıtlarını aktif hale getirelim.
- accton /var/account/pacct
- Sistemin her açılışında servisin başlaması için;
- chkconfig psacct on (Centos)
- service psacct start (Centos)

ACCT ile Çalışmak

- “acct” uygulaması ile gelen bazı yararlı komutları inceleyelim.”ac” komutu ile başlayalım.”ac” komutu kullanıcının sistem üzerinde ne kadar süredir bağlı kaldığını gösterir.
-

```
# ac
total       537.71
```

ACCT ile Çalışmak

- Yukarda görüldüğü gibi “ac” komutu hiç bir parametre almadan sadece komutu veren kullanıcının ne kadar süre sistemde olduğunu gösteriyor.Eğer sistem üzerinde tüm kullanıcıların ne kadar süre sistem üzerinde olduklarını görmek için ise “-p“(people) parametresi kullanıyoruz.

```
# ac -p
 ares                                            537.95

 zeus                                            100.00
 total       637.95
```

ACCT ile Çalışmak

- İkinci diğer bir komutumuz ise “lastcomm” . “lastcomm” komutu ile hangi komutu kim,ne zaman,nerede verildiği hakkında bilgi verir.

```
# lastcomm

grep               root     pts/0      0.00 secs Fri Jan 21 06:56
sh           F     root     pts/0      0.00 secs Fri Jan 21 06:56
sh           F     root     pts/0      0.00 secs Fri Jan 21 06:56
sed                root     pts/0      0.00 secs Fri Jan 21 06:56
sh           F     root     pts/0      0.00 secs Fri Jan 21 06:56
sed                root     pts/0      0.00 secs Fri Jan 21 06:56
sh           F     root     pts/0      0.00 secs Fri Jan 21 06:56
grep               root     pts/0      0.00 secs Fri Jan 21 06:56
sh           F     root     pts/0      0.00 secs Fri Jan 21 06:56
sh           F     root     pts/0      0.00 secs Fri Jan 21 06:56
sed                root     pts/0      0.00 secs Fri Jan 21 06:56
sh           F     root     pts/0      0.00 secs Fri Jan 21 06:56
sed                root     pts/0      0.00 secs Fri Jan 21 06:56
sh           F     root     pts/0      0.00 secs Fri Jan 21 06:56
grep               root     pts/0      0.00 secs Fri Jan 21 06:56
sh           F     root     pts/0      0.00 secs Fri Jan 21 06:56
sh           F     root     pts/0      0.00 secs Fri Jan 21 06:56
sed                root     pts/0      0.00 secs Fri Jan 21 06:56
```

ACCT ile Çalışmak

- “lastcomm” komutu parametresiz sistem üzerinde verilen tüm komutları listeler.Eğer belli bir kullanıcının verdiği komutları görmek istersek “lastcomm” komutundan sonra “kullanıcı adı“nı yazıyoruz.

```
# lastcomm ares
bash                   ares pts/1        0.02 secs Fri Jan 21 03:46
clear                  ares pts/1        0.00 secs Fri Jan 21 04:43
bash             F     ares pts/1        0.00 secs Fri Jan 21 04:43
bash             F     ares pts/1        0.00 secs Fri Jan 21 04:43
bash                   ares pts/0        0.04 secs Thu Jan 20 19:39
clear                  ares pts/0        0.00 secs Fri Jan 21 04:43
ssh                    ares pts/1        0.03 secs Fri Jan 21 03:46
firefox              X ares __         1860.00 secs Thu Jan 20 16:24
plugin-containe        ares __          454.73 secs Thu Jan 20 16:24
taskl                X ares __           0.35 secs Fri Jan 21 04:35
gnome-panel      F     ares __           0.00 secs Fri Jan 21 04:35
xauth          S       ares pts/0        0.00 secs Fri Jan 21 04:31
whoami                 ares pts/0        0.00 secs Fri Jan 21 04:31
```

ACCT ile Çalışmak

- Diğer bir komut ise “sa” . “sa” komutu ile kayıt altına komutları ve bu komutların kaç defa çalıştırıldığını gösterir.

```
# sa
8014        0.16re        0.00cp          0avio       4475k    mv
 5495         0.01re         0.00cp          0avio        2052k    dirname
 5484         0.78re         0.00cp          0avio        5707k    libtoolize*
 4377         0.18re         0.00cp          0avio        2071k    stty
 3621         0.02re         0.00cp          0avio        3445k    touch
 3258         0.09re         0.00cp          0avio        2326k    tr
 3214         0.14re         0.00cp          0avio        2319k    mkdir
 3055         0.01re         0.00cp          0avio        3365k    true
 2711         7.00re         0.00cp          0avio        2251k    collect2
```

ACCT ile Çalışmak

- “acct” ile gelen diğer bazı komutlar ise ;
- last =Sisteme en son giriş yapan kullanıcılar listeler.
- dump-acct = Kayıt dosyasını okunabilir şekilde ekrana yazdırır.
- “acct” hakkında daha fazla bilgi için “http://www.gnu.org/software/acct/manual/html_chapter/accounting.html”

Linux
Kullanıcıları
Derneği