Limitation

بررسی
انواع روش های محدود نمودن
کاربران
در
Linux



راهبری Linux





جلال حاجی غلامعلی

qolamali@aictc.com

مرداد ۱۳۸۳

training@farsilinux.org

راهبری Linux

کلیه حقوق، متعلق به شورای عالی انفورماتیک و مرکزفن آوری شریف بوده و هرگونه دخل و تصرف منوط به اجازه کتبی می باشد.



Limitation

سیستم عامل Linux این امکان را به راهبر می دهد که محدودیت هائی عمومی و یا برای کاربران خاصی را اعمال نماید که اهم محدودیت های خاص(برای Userid) عبارتند از:

- تعداد Login ها
- تعداد پروسس ها
- فضای گرفته شده در حافظه
- اتصال از هر نقطه ای
- زمان اجرا
- به کارگرفتن سرویس

Limitation

بحث محدود نمودن کاربران نسبتا مفصل بوده و در چند اسلاید
بعدی با بررسی چند مثال، با این امکانات اشنا شده و در طورت نیاز
به اطلاعات بیشتر به دایرکتوری که ذیلا نام آن امده مراجعه نموده
و تغییرات لازمه را برای محدود نمودن کاربران اعمال نمائید.

دایرکتوری مربوط به محدود نمودن کاربران

/etc/security

اسامی فایل های تحت این دایرکتوری

access.conf console.apps group.conf pam_env.conf
chroot.conf console.perms limits.conf time.conf

Limitation

Login

مثال ۱: تغییراتی در سیستم دهید که کاربر student فقط بتواند یک Login داشته باشد.

برای اعمال تغییرات به دایرکتوری /etc/security رفته و فایل limits.conf را تغییر داده و خط زیر را اضافه می نمائیم.

@student - maxlogins 1

تفسیر خط بالا به این صورت است که userid با نام student حداکثر login هائی که می تواند داشته باشد فقط یکی(یک) است.

Limitation

Login

در صورتیکه کاربر student بخواهد Login دوم را داشته باشد پیام زیر ارسال و ارتباط قطع خواهد شد.

Fedora Core release 1 (Yarrow)

Kernel 2.4.22-1.2188.nptl on an i686

login: student

Password:

Permission denied

Connection to host lost.



Limitation

Process

مثال ۲: تغییراتی در سیستم دهید که کاربر student فقط بتواند حداکثر ۶ پروسس همزمان را اجرا نماید.

برای اعمال تغییرات به دایرکتوری /etc/security رفته و فایل limits.conf را تغییر داده و خط زیر را اضافه می نمائیم.

```
@student        hard        nproc        6
```

تفسیر خط بالا به این صورت است که userid با نام student همزمان می تواند ۶ پروسس داشته باشد.

Limitation

Process

در صورتیکه کاربر student بخواهد پروسس هفتم را داشته باشد پیام زیر ارسال خواهد گردید.

```
[student@jalal student]$date
-bash:fork: Resource temporarily unavailable
```



فرض کنید که کاربر **student** قبلا ۶ پروسس **Background** اجرا نموده است

Limitation

File Size

مثال ۳: تغییراتی در سیستم دهید که کاربر student فقط بتواند فایل هائی با حداکثر ۲۰۰ کیلو بایت تولید نماید..

برای اعمال تغییرات به دایرکتوری /etc/security رفته و فایل limits.conf را تغییر داده و خط زیر را اضافه می نمائیم.

@student hard fsize 200

تفسیر خط بالا به این صورت است که userid با نام student می تواند فایل هائی حداکثر با طول ۲۰۰ کیلو بایت تولید نماید.

Limitation

File Size

در صورتیکه کاربر student بخواهد فایل بزرگی را تولید نماید، پیام زیر ارسال خواهد گردید.

```
[student@jalal student]$ cp /etc/termcap myfile
cp: writing `myfile': No space left on device
```



طول فایل **termcap** حدود ۷۰۰ کیلو بایت و یکی از فایل های مهم **Linux** می باشد

Limitation

General

همان گونه که در اسلاید های قبلی توضیح داده شد، مطالب مربوط به محدود نمودن کاربر نسبتا مفصل بوده و فقط در مورد محدودیت های تعداد Login و پروسس و ... مطا لب زیادی وجوددارد که اسامی آنها در اسلاید بعدی آمده است و برای بدست آوردن اطلاعات بیشتر بایستی مطالب مربوط به PAM و محدودیت ها دقیقا مطالعه گردد.

ضمنا فرمان ulimit نیز محدودیت هائی را برای کاربر بوجود می آورد و مطالعه جزوه ulimit قویا توصیه می گردد.

اگر راهبر تغییراتی در ulimit کاربر بدهد، معمولا کاربر نمی تواند تغییرات را خنثی و یا بی اثر نماید.

Limitation

Definition

- core - limits the core file size (KB)
- data - max data size (KB)
- fsize - maximum filesize (KB)
- memlock - max locked-in-memory address space (KB)
- nofile - max number of open files
- rss - max resident set size (KB)
- stack - max stack size (KB)
- cpu - max CPU time (MIN)
- nproc - max number of processes
- as - address space limit
- maxlogins - max number of logins for this user
- priority - the priority to run user process with
- locks - max number of file locks the user can hold



Limitation

limits.conf

```
[root@jalal security]# less limits.conf
# /etc/security/limits.conf
#
#Each line describes a limit for a user in the form:
#
#<domain>      <type>  <item>  <value>
#
#Where:
#<domain> can be:
#        - an user name
#        - a group name, with @group syntax
#        - the wildcard *, for default entry
#        - the wildcard %, can be also used with %group syntax,
#                 for maxlogin limit
```



Limitation

access.conf

```
# Login access control table.
#
# When someone logs in, the table is scanned for the first entry that
# matches the (user, host) combination, or, in case of non-networked
# logins, the first entry that matches the (user, tty) combination.  The
# permissions field of that table entry determines whether the login will
# be accepted or refused.
# Format of the login access control table is three fields separated by a
# ":" character:
#
# [Note, if you supply a 'fieldsep=|' argument to the pam_access.so
# module, you can change the field separation character to be
# '|'. This is useful for configurations where you are trying to use
# pam_access with X applications that provide PAM_TTY values that are
# the display variable like "host:0".]
#
#      permission : users : origins
```

هرکاربری از هر کجا نتواند به سیستم متصل گردد



Limitation

time.conf

```
# the syntax of the lines is as follows:
#
#      services;ttys;users;times
# white space is ignored and lines maybe extended with '\\n' (escaped
# newlines). As should be clear from reading these comments,
# text following a '#' is ignored to the end of the line.
#
# the combination of individual users/terminals etc is a logic list
# namely individual tokens that are optionally prefixed with '!' (logica
# not) and separated with '&' (logical and) and '|' (logical or).
#
# services
#      is a logic list of PAM service names that the rule applies to.
# ttys
#      is a logic list of terminal names that this rule applies to.
# users
#      is a logic list of users to whom this rule applies.
```

هرکاربری در هر زمان نتواند از سیستم سرویس بگیرد

بخشی از فایل
time.conf
تحت دایرکتوری
/etc/security

Limitation

console.perms

```
# This file determines the permissions that will be given to priviledged
# users of the console at login time, and the permissions to which to
# revert when the users log out.
# format is:

#   <class>=list of regexps specifying consoles or globs specifying files
#   file-glob|<class> perm dev-regex|<dev-class> \
#     revert-mode revert-owner[.revert-group]
# the revert-mode, revert-owner, and revert-group are optional, and default
# to 0600, root, and root, respectively
#
# For more information:
# man 5 console.perms

# file classes -- these are regular expressions
<console>=tty[0-9][0-9]*vc /[0-9][0-9]* :[0-9]\.[0-9] :[0-9]
<xconsole>=:[0-9]\.[0-9] :[0-9]
```

هرکاربری نتواند از طریق کنسول وارد سیستم شود

بخشی از فایل
Console.perms
تحت دایرکتوری
/etc/security