LİNUX YETKİ VE YETKİLENDİRME İŞLEMLERİ

```
[root@rhel-7-1 /]# pwd
/
[root@rhel-7-1 /]# ls -l
total 16
lrwxrwxrwx.   1 root root    7 Feb 13 19:23 bin -> usr/bin
dr-xr-xr-x.   4 root root 4096 Mar  8 10:49 boot
drwxr-xr-x.  17 root root 2860 Mar  9 16:41 dev
drwxr-xr-x.  76 root root 8192 Mar 10 08:18 etc
drwxr-xr-x.   3 root root   18 Mar  8 10:43 home
lrwxrwxrwx.   1 root root    7 Feb 13 19:23 lib -> usr/lib
lrwxrwxrwx.   1 root root    9 Feb 13 19:23 lib64 -> usr/lib64
drwxr-xr-x.   2 root root    6 Dec 14  2017 media
drwxr-xr-x.   2 root root    6 Dec 14  2017 mnt
drwxr-xr-x.   2 root root    6 Dec 14  2017 opt
dr-xr-xr-x.  97 root root    0 Mar  9 16:40 proc
dr-xr-x---.   4 root root  139 Mar  8 11:34 root
drwxr-xr-x.  25 root root  740 Mar 10 14:02 run
lrwxrwxrwx.   1 root root    8 Feb 13 19:23 sbin -> usr/sbin
drwxr-xr-x.   2 root root    6 Dec 14  2017 srv
dr-xr-xr-x.  13 root root    0 Mar  9 16:41 sys
drwxrwxrwt.  10 root root  216 Mar 10 15:01 tmp
drwxr-xr-x.  13 root root  155 Feb 13 19:23 usr
drwxr-xr-x.  18 root root  254 Mar  8 10:42 var
[root@rhel-7-1 /]#
```

Kullanıcı, Grup ve Erişim Yetkileri

Linux, çok kullanıcılı bir işletim sistemidir. Çalışan her uygulama mutlaka bir kullanıcı ve grup no ile ilişkilidir; kullanıcı veya grubu olmayan bir uygulamanın olması söz konusu değildir. Uygulama içerisinden yapılan tüm erişimler, bu kullanıcı ve grup hakları doğrultusunda gerçekleştirilir.

Okuma, Yazma ve Çalıştırma Yetkileri

Dosya ve dizinler üzerindeki yetki kontrolleri temel olarak okuma (read - **r**), yazma (write - **w**) ve çalıştırma (execute - **x**) bitleri üzerinden kontrol edilir. Bu bilgiler dosya sistemi üzerinde **inode** yapılarında saklanmaktadır.

Bu yetki bitlerinin dosya ve dizinler üzerindeki anlamları aşağıdaki gibidir:

Yetki	Açıklama
r	Dosyalar için okuma yetkisi, dosya içeriğine ulaşılabilmesi anlamını taşır. Dizinlerde olduğunda ise, dizin içeriğinin listelenebilmesini (dizinlerin okunması gibi düşünülebilir) sağlar.
w	Dosyalar için yazma yetkisi, dosya içeriğinin değiştirilebilmesini kontrol eder. Dizinler içinse, dizin içerisinde yeni dosya ve dizin oluşturma/silme operasyonlarını kontrol eder.
x	Dosyalar için çalıştırma yetkisi anlamı taşır. Dizinler için ilgili dizine geçilip geçilemeyeceğini belirtir.

`ls` komutunun çıktısındaki erişim yetkileriyle ilgili ilk karakter aşağıdaki tablo doğrultusunda anlamlandırılır:

Karakter	Anlam
-	standart dosya (*regular file*)
d	dizin
c	karakter tabanlı aygıt dosyası (*/dev/console* vb.)
b	blok tabanlı aygıt dosyası (*/dev/sda3* vb.)
s	özel dosya (unix domain soket vb.)

Erişim yetkileriyle ilgili ilk karakterden sonraki 3'lü blok, dosya/dizin sahibinin dosya/dizin üzerindeki erişim yetkilerini gösterir.

Bir sonraki 3'lü blok, dosya/dizin'in grup sahibinin dosya/dizin üzerindeki erişim yetkilerini gösterir.

Sonraki ve son 3'lü blok ise, dosya/dizin için sahibi veya grup sahibi kısmına girmeyen kullanıcılar için (*other*) tanımlanmış olan erişim yetkilerini gösterir.

STANDART READ, WRİTE VE EXECUTE YETKİ BİTLERİ HARİCİNDE SUID, SGID VE STİCKY BİT OLMAK ÜZERE 3 FARKLI BİT DAHA BULUNMAKTADIR.

-SUID
-SGID
-STİCKY

SUID BİT'İ NEDİR?(SET USER ID) YETKİSİ

BİR UYGULAMADA SUID BİTİ AKTİF İSE, O UYGULAMAYI HANGİ KULLANICI ÇALIŞTIRIRSA ÇALIŞTIRSIN, UYGULAMA DOSYASININ SAHİBİ KİM İSE, ONUN HAKLARIYLA ÇALIŞIR. BU DURUM YANINDA BAZI GÜVENLİK ZAFİYETLERİDE GETİREBİLİR.

SGID (SET GROUP ID) YETKİSİ

SUID BİTİ İLE BENZER MANTIKTA, BİR UYGULAMANIN, KİMİN ÇALIŞTIRDIĞINA BAKILMAKSIZIN UYGULAMA DOSYASININ GRUP SAHİBİNİN GRUP ERİŞİM YETKİLERİ DOĞRULTUSUNDA ÇALIŞTIRILMASINI SAĞLAMAKTADIR. SGID BİTİ, SUID BİTİNE ORANLA PRATİKTE DAHA AZ KULLANIM ALANI BULMAKTADIR.

STİCKY BİT

Belirtilen klasör veya dosyanın sadece sahibi veya root kullanıcısı tarafından silebileceği anlamına gelir.

Erişim Yetkilerinin Düzenlenmesi

Dosya sisteminde yer alan bir dosya/dizin için erişim yetkilerinin düzenlenmesi işlemi `chmod` komutu ile yapılır. Değiştirilmek istenen yetkilerin neler olduğu ve üçlü erişim yetki bloklarından hangisi veya hangileriyle ilişkili olduğu parametre olarak belirtilir. Parametrelerde erişim yetki grubu belirtildikten sonra, **+** veya **-** ile hangi yetkilerin ekleneceği veya çıkartılabileceği belirtilebileceği gibi, **=** ile tam olarak hangi yetkilere sahip olacağı da belirtilebilmektedir.

`chmod` Erişim Yetki Grupları

Karakter	Etkilediği Grup
u	Dosya/dizin sahibi
g	Dosya/dizin grup sahibi
o	Dosya/dizin sahibi ve grup sahibi dışında kalanlar (others)
a	Dosya/dizin sahibi, grup sahibi ve bunların dışında kalanlar dahil her üç blok

Komut	Açıklama
`chmod u+rwx file1`	Dosyanın sahibine okuma, yazma, çalıştırma yetkisi ver
`chmod u-wx file1`	Dosyanın sahibinden yazma ve çalıştırma yetkisini kaldır
`chmod u+w-r file1`	Dosyanın sahibine yazma yetkisini ver, okuma yetkisini kaldır
`chmod u=rw file1`	Dosyanın sahibine okuma ve yazma yetkisi ver, çalıştırma yetkisi verme
`chmod u+x,g+wx file1`	Dosyanın sahibine çalıştırma yetkisi ekle, aynı zamanda grup sahibine yazma ve çalıştırma yetkisi ekle
`chmod g=rw file1`	Dosyanın grup sahibine okuma ve yazma yetkisi ver, çalıştırma yetkisini kaldır
`chmod o=r file1`	Sahip veya grup sahibi dışında kalan diğer kullanıcılara sadece okuma yetkisi ver
`chmod +x file1`	Tüm erişim gruplarına (sahip, grup ve diğer), çalıştırma yetkisi ekle
`chmod -x file1`	Tüm erişim gruplarından çalıştırma yetkisini kaldır
`chmod a=r file1`	Tüm erişim gruplarına (a = all) okuma yetkisi ver, yazma ve çalıştırma yetkisini kaldır

`chmod u+s file1`	SUID yetkisini ekle
`chmod g+s file1`	SGID yetkisini ekle
`chmod +t file1`	Sticky bitini aktifleştir
`chmod -R g-X dir1/`	Dizin altında recursive olarak dolaş, sadece bulunan alt dizinlerin grup sahiblerinden dizin içine geçme (x) yetkisini kaldır

Sekizli Sistemle Gösterim

R = 4
W = 2
X = 1
Yukarıdaki değerlerin karşılığı bu rakamlardır. Örnek olarak bir dosyaya yetki verirken tek seferde kullanıcı, grup ve diğerlerine 3 raka ile yetki verebiliriz.

#chmod 644 file_name

Yukarıda komut ile 6 rakamının temsil ettiği kişi dosya sahibi. Biz burada dosya sahibine Okuma ve yazma yetkisi verdik. Yani 4 + 2 = 6 mantalitesi ile hareket ediyoruz. Ardından 4 rakamı var. Bu 4 rakamı grup yetkisini temsil ediyor. Grup üyelerine dosya için sadece YAZMA yetkisi verdik. Yani 4 = R. Sonra 4 rakamı ise diğerlerini yani dosya sahibi ve gruptan olmayan kişileri temsil ediyor. Onlarada sadece YAZMA yetkisi verdik. Yani 4 = R.

#chmod 777 file_name1