Sun Solaris ve RBAC (Role Based Access Control List)

/***/
Ömer Faruk Şen
* ofsen [at] enderunix [dot] org
* EnderUNIX Yazılım Geliştirme Takımı
* http://www.enderunix.org
* Sürüm : 1.0
* Tarih : 12.09.07
* Etiketler : solaris, rbac
* Seviye : Orta Seviye
* Makalenin en yeni versiyonu : http://www.enderunix.org/docs/solaris-rbac.pdf
* adresinden elde edilebilir.
/***/

İçindekiler

Giriş..... 3
Role Nedir? 3
Rights Profile Nedir?..... 3
Authorization Nedir ?..... 4
RBAC Komutları..... 6

Giriş

RBAC Role Based Acess Control Solaris içinde gelen bir güvenlik modelidir. Normal şartlar altında sadece root tarafından yapılacak işler root olmayan, sistem de hesabı var olan kullanıcılar tarafından gerekli role'ler üstlenilerek (assuming role) yapılabilmektedir.

Bu işlemler şu RBAC özellikleri ile yapılır: Roles, Rights, Profiles ve Authorization

Role Nedir?

Role sistemde var olan bir veya daha fazla kullanıcı tarafından kullanılabilen özel bir kullanıcıdır. Bir kullanıcı bu role'e geçince (ingilizce assuming role) bu role'un kullanabileceği bütün haklara da sahip olmaktadır.

Role'ler normal bir kullanıcı gibi bir ev dizinine, bir şifreye ve gruba sahiptir. Fakat role'lerin birkaç değişik özelligi vardır. Bunlar

1- Direkt role ile sisteme giremezsiniz. Önce normal bir kullanıcı olup daha sonra bu role'e geçersiniz. (su komutu ile)

2- Kullanıcı role'e geçince role ile alakalı bütün haklara da sahip olmuş olur.

3- Bir veya daha fazla kullanıcı role'e geçince aynı haklara sahip olup aynı sistem degişkenlerine erişim elde eder.

4- Bir kullanıcı aynı anda bir role'e sahip olabilir.

5- Role hakkında bilgiler passwd,shadow ve user_attr dosyalarında yer alır

6- Role'ler diğer rollerin veya kullanıcıların haklarını üzerine alamazlar.

Rights Profile Nedir?

Rights profile, right'ların birleşiminden oluşan bir bütündür. Rights profile bilgileri prof_attr ve exec_attr dosyaları içinde bulunur.

Aşağıda bazı right profile'lar verilmiştir.

Primary Administrator: Root kullanıcısının bütün haklarını taşıyan right profile

System Administrator: Güvenlik hakları hariç diğer yönetimsel hakları içeren right profile. Mesela: network yönetimi, dosya sistemi yönetimi, yazılım kurulumu gibi

Operator: Dosyaları ve offline cihazları yöneten right. Backup alınması (restore hakki yok), Printer yonetimi gibi

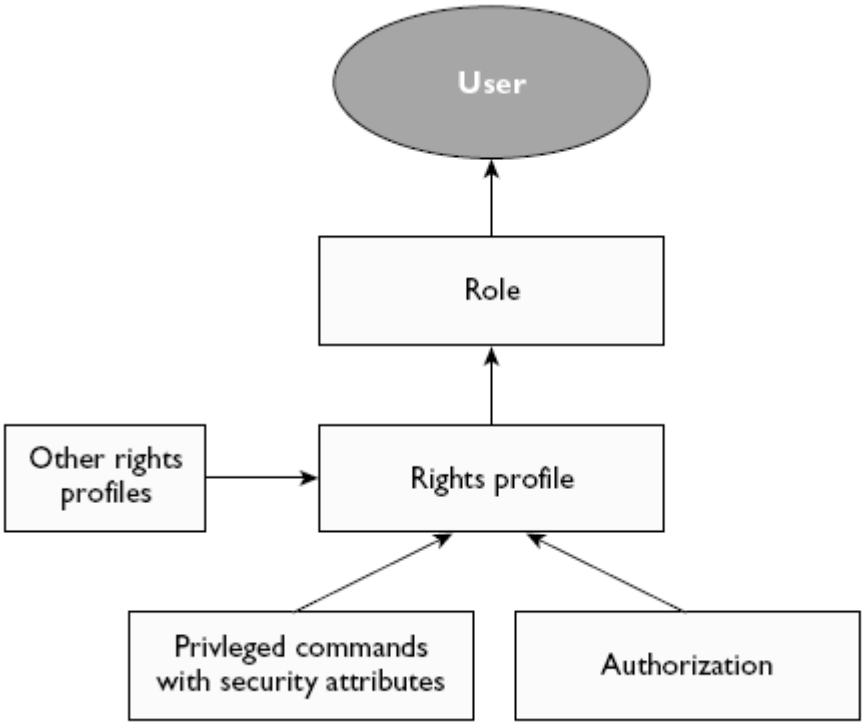
Printer Management: Printer ve printer ayarlari ile alakalı işlemleri yapabilecek right

Basic Solaris User: Bu bütün kullanıcıların ön tanımlı olarak atanmış olduğu right'tir

Authorization Nedir ?

Authorization bir kullanıcının veya rolün sistem güvenliğini etkileyecek bazı işleri yapabilmesine izin veren özel bir izindir. Örnek olarak solaris.device.cdrw izniyle (authorization) normal bir kullanıcı CD'ye yazma ve CD'den okuma hakkına sahip olur. İzinler /etc/security/auth_attr dosyasında yer almaktadır.

Her ne kadar bir izin direk kullanıcı veya role atanabilse de RBAC sisteminde bu izin bir profil'e (profile) atanır. Böylece bu profil içinde var olan rol ve dolayısıyla kullanıcı gerekli izinlere sahip olabilmektedir. Profiller ayrıca güvenlik tanımlarını içeren komutları ve diğer profilleri içerebilir. Aşağıda bütün RBAC kavramları ve birbiriyle ilişkileri resmedilmiştir.



Bir role bir kullanıcı tarafından üstlenilir. Bir kullanıcı aynı zamanda sadece bir role üstlenebilir. Role'ler sahip oldukları özellikleri Right Profile'lardan alır. Aynı zamanda bu right profile başka profilleri de içerebilir. Righ profile'larda özel izinler (authorization) ve güvenlik tanımlarını içeren özel komutlardan oluşur. Privileged command adı verilen komutlar özel izinle çalışan komutlardır (tıpkı suid komutları gibi).

Aşağıdaki tabloda standart UNIX super kullanıcı modeli ile RBAC modeli arasında bir karşılaştırma verilmiştir.

Özellik	Super Kullanıcı Modeli	RBAC Modeli
Bütün haklarla birlikte super user olabilme hakkı	Evet	Evet
Sisteme bütün super kullanıcı hakları ile girebilme	Evet	Evet
Sisteme normal bir	Setuid programlarla evet	Setuid ve RBAC ile evet

kullanıcı olarak girip sonra super kullanıcı haklarını alabilme		
Sisteme girdikten sonra sınırlı super kullanıcı haklarını elde etme	Hayır	Evet
Sisteme girdikten sonra sistemi yönetebilecek sınırlı yönetimsel haklara sahip olma	Hayır	Evet
Sisteme girdikten sonra normal bir kullanıcıdan daha az haklara sahip olabilme	Hayır	Evet

RBAC Sistemini Yönetme

RBAC sisteminde önemli olan 4 ana dosya vardır. Bunlar:

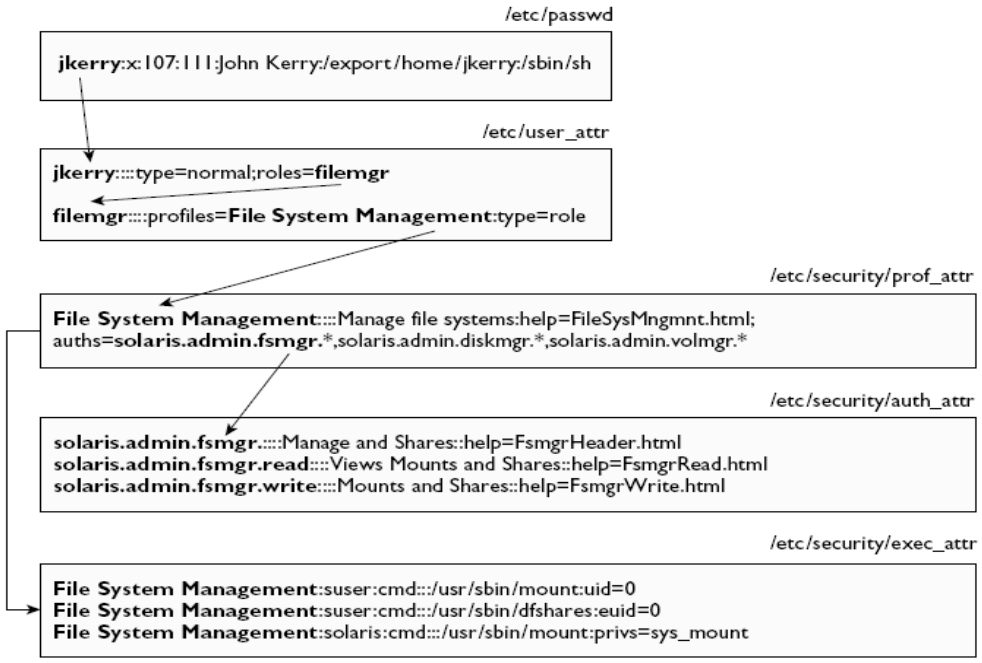
auth_attr: İzinler (authorization) ve bunların tanımlarını içeren dosyadır.

exec_attr: Belirli bir right profile'ına sahip güvenlik tanımlarını içeren komutları tanımlar

prof_attr: Right Profile dosyasıdır. Profiller için atanan izinleri içerir.

user_attr: Kullanıcıları role'lerle ilişkilendiren, role'leri profiller yardımıyla izin ve haklarla ilişkilendiren dosyadır.

Ayrıca bunlara ek olarak **policy.conf** dosyası vardır. Policy.conf dosyası sistemdeki bütün kullanıcılara hak tanımak için kullanılır.



Üstteki resimde **/etc/passwd** dosyasındaki **jkerry** kullanıcısı **/etc/user_attr** dosyasında **File System Management** profiline sahip olan **filemgr** rolünü üstlenmektedir.

/etc/security/profiles_attr dosyası **File System Management** profiline atanan izinleri (**authorization**) içermektedir.

Bu izinlerde . **/etc/security/auth_attr** dosyasında tanımlanır.

En son olarak . **/etc/security/exec_attr** dosyasında profile_attr dosyasında tanımlanan profillerin hangi komutları çalıştırabileceği belirtilir.

RBAC Komutları

KOMUT	AÇIKLAMA
auths	Belirltilen kullanıcı için izinleri listeler
roles	Belirtilen kullanıcı için hak profillerini listeler
roleadd	Sisteme bir rol ekler. Bu eklenen rol /etc/passwd , /etc/shadow ve /etc/user_attr dosyasında değişikliğe sebep olur.
roledel	Sistemde bir rol siler. Bu eklenen rol /etc/passwd , /etc/shadow ve /etc/user_attr dosyasında değişikliğe sebep olur.
roles	Belirli bir kullanıcının üstlenebileceği rolleri listeler.
useradd	Sistemde bir kullanıcı oluşturur. –R komutu ile var olan bir rol bu kullanıcıya atanır.
userdel	Sistemden bir kullanıcı silmek için kullanılır
usermod	Sistemdeki bir kullanıcı hakkında değişiklik yapmak için kullanılır.

Roleadd ve roledel komutları:

```
roleadd [-c <comment>] [-b <base_dir>] [-d <dir>] [-e
<expire>]
[-f <inactive>] [-g <group>][-G <group, group...>] [-m [-k
<skel_dir>]]
[-p <profile>] [-A <authorization, authorization...>][-s
<shell>] [-u <uid>]
<roleName>
```

Roleadd komutunun normal useradd komutundan tek farkı –R parametresidir. –R parametresi var olan bir rolü bir kullanıcının üstlenmesine izin vermek için kullanılır. –R paramtersi sadece useradd komutunda vardır. Bir role'ün başka bir rolü üzerine alabilme imkanı olmadığı için roleadd komutunda bu parametre yoktur.

ÖRNEK:

Her ne kadar dosyalar arası ilişkiyi anlamak zor da olsa kullanım o kadar zor değildir. Zira Solaris işletim sisteminde neredeyse bütün profiller hazırlanmış durumdadır. **Bize sadece uygun profili içeren bir role eklemek ve bu role'ü alabilecek bir kullanıcı eklemek düşmektedir.** İlk başta /etc/security/profile_attr'daki bir profile'a sahip bir role ekleyelim sisteme:

 # roleadd -P "Printer Management" printadm

Printer Management /etc/security/profile_attr dosyasında şu şekilde tanımlıdır:

Printer Management:::Manage printers, daemons, spooling:help=RtPrntAdmin.html;auths=solaris.admin.printer.read,solaris.admin.printer.modify,solaris.admin.printer.delete
Operator:::Can perform simple administrative tasks:profiles=Printer Management,Media Backup,All;help=RtOperator.html
System Administrator:::Can perform most non-security administrative tasks:profiles=Audit Review,Printer Management,Cron Management,Device Management,File System Management,Mail Management,Maintenance and Repair,Media Backup,Media Restore,Name Service Management,Network Management,Object Access Management,Process Management,Software Installation,User Management,Project Management,All;help=RtSysAdmin.html

Sonra sisteme bir kullanıcı ekleyelim ama eklerken –R parametresini kullanalım ve printadm role'ünü bu kullanıcıya verelim.

 # useradd -R printadm -m -d /export/deneme -s /usr/bin/bash deneme

Daha sonra kullanıcı ve role'ün şifresini değiştirelim.

 # passwd printadm
 # passwd deneme

Bu komut ile deneme kullanıcısı printadm role'ünü üstlenebilecektir. Unutulmamalıdır ki role ile direk sisteme girilmez. Sisteme ilk başta deneme kullanıcısı ile girelim

$ **who am i**
deneme pts/2 Jan 7 10:22 (localhost)
$ **roles**
printadm
$ **su printadm**
Password:
$ **who am i**
deneme pts/2 Jan 7 10:23 (localhost)
$ **profiles**
Printer Management
Basic Solaris User
All

Gördüğünüz gibi sisteme deneme kullanıcısı ile girdikten sonra role'lerimize roles komutu ile baktık. Sonra su printadm komutu ile printadm role'ünü üstümüze aldık ve profiles komutu ile hangi profillere sahip olduğumuzu dolayısıyla neler yapabileceğimizi ögrenmiş olduk.