RBAC: No Turning Back: Remove the group security!

Contributed by Michael Felt

No Turning Back: "Remove" Security Group

When I first started this series I said my next article would show what happens when remove the standard "RWX" permissions for a group. I was expecting to remove all the permissions for both AIX groups system and security. After researching what might go wrong I decided working with only the security group would be easier to understand.

Why not both groups? In short, understanding one group might be difficult if you are not used to evaluating DAC permission bits. And it turns out the group security has only 5 SGID programs - which makes explaining what and why some programs are broken "possible".

On your test server, preferably a fresh install and only rootvg installed - run the following commands:

```
# lspv
hdisk0          00c39b8d9375b375                    rootvg          active
# find / -group security -exec chmod g-rwx {} \;
0481-014 chmod: not all requested changes were made to /proc/3080378/object/a.out
0481-014 chmod: not all requested changes were made to /proc/3080378/object/jfs2.10.5.169723
```

```
# ls -ld /etc/security
drwx------   11 root     security       4096 May 28 07:12 /etc/security
```

Still as root, make a new user (e.g., michael) and login. Normal commands work fine - because a regular user is not in the group security and is not affected by files and directories that work when in the group security. The commands that will fail are those that put someone into the group security (meaning they expect files to be readable via group permissions).

```
# find / -group security -perm -2000 -ls
102   32 -r-x--Sr-x  1 root     security     31948 Feb  1  2011 /usr/bin/chfn
105   64 -r-x--Sr-x  1 root     security     65440 Feb  1  2011 /usr/bin/chgrpmem
129   34 -r-x--Sr-x  1 root     security     34334 Feb  1  2011 /usr/bin/chsh
```

693 26 -r-x--Sr-x 1 root security 26298 Feb 1 2011 /usr/bin/smitacl

169849 68 -r-x--Sr-x 1 root security 68830 Feb 1 2011 /usr/sbin/lsgroup

AIX Version 6

Copyright IBM Corporation, 1982, 2010.

login: michael

michael's Password:

Normal commands work fine:

$ tail -3 /etc/passwd

esaadmin:*:10:0::/var/esa:/usr/bin/ksh

sshd:*:202:201::/var/empty:/usr/bin/ksh

michael:!:203:1::/home/michael:/usr/bin/ksh

$ grep staff /etc/group

staff:!:1:ipsec,esaadmin,sshd,michael

But commands relying on security membership fail - ths one because it cannot read files in the directory /etc/security.

$ lsgroup staff

3004-686 Group "staff" does not exist.

In short, regular users are mostly unaffected - but some commands will need RBAC adjustments to work, and/or role assignment before they will work as expected.

More to come!