SPK
and Associates

www.spkaa.com
Ph: 888-310-4540

SPK and Associates
900 E Hamilton Ave, Ste.100
Campbell, CA 95008

An Approach to Code Security When Using ClearCase

Ronald Ross (rross@spkaa.com)

As most of us already know, the ability of ClearCase to provide code security is somewhat limited. A first line of defense might be to segment project VOBs by ClearCase registry region. This has the effect of a given engineer only seeing the VOBs which are registered in that particular region. However, if the engineer has any kind of administrative authority on his/her machine, the registry region on the client machine can simply be changed, and all the VOBs in the new region then become visible.

The other commonly used method is to use the group membership and file permissions to enforce a security policy. If strict control can be maintained over who is a member of a particular group, this approach has some chance of success. One drawback is that the granularity of this method is somewhat coarse. Often certain UCM projects or code directories are what need security, but in my opinion it is more effective to apply any protections at the VOB level. Others may have dealt with this more extensively and have achieved solutions, but for the purposes of this discussion, we will assume VOB level security and nothing more granular.

For our example, the client machines are using ClearCase 7.0.1.12, and our VOB server is RedHat Enterprise Linux (RHEL) 4. The VOB storage is Network Attached Storage (NAS) on a Network Appliances (NetApp) machine. This kind of mixed environment can be a bit tricky, and we might imagine a dual message here. The implicit first message would be – how do we get kind of mixed environment to work, period. The next message, which is our explicit focus, is how do we use this environment to successfully implement group security?

We assume that the following commands have been run against the VOB in question (ex. Training) in order to establish security based upon group membership:

```
cleartool protectvob  –add_group atria_vid –delete_group <groups,…> /vobs/Training
```

```
cleartool protect  –chgrp atria_vid –chmod 770 –recurse /vobs/Training
```

```
cleartool find .  –all –exec “cleartool protect –chgrp atria_vid –chmod 770
\”%CLEARCASE_PN%\” “
```

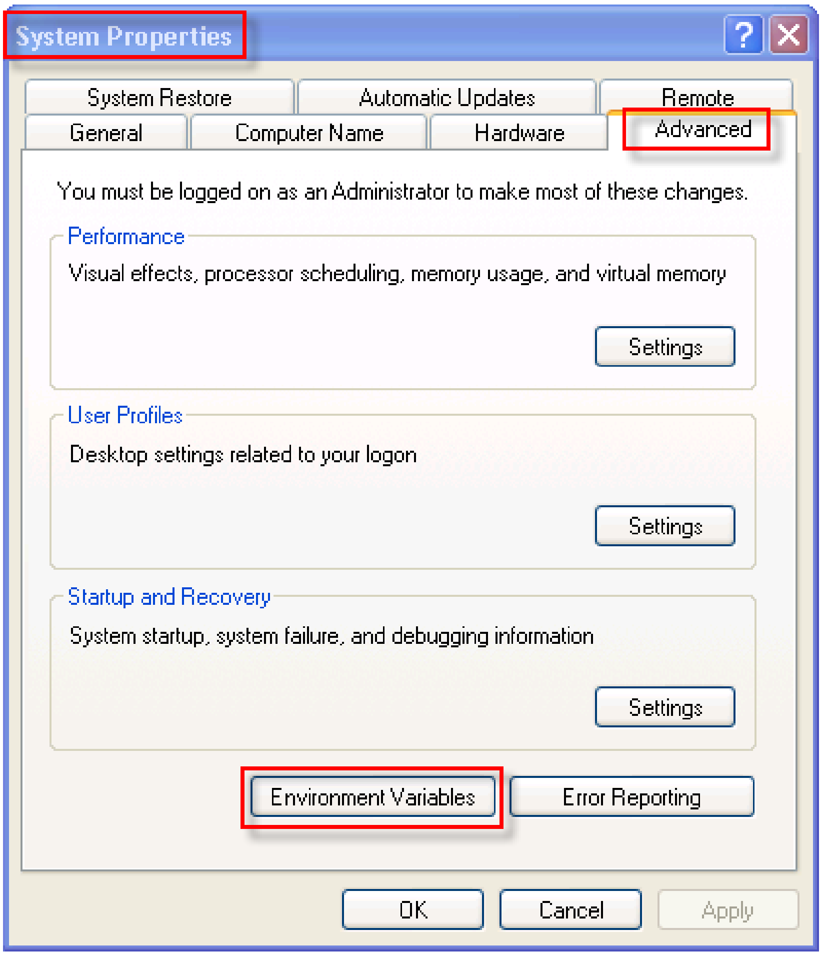
The first command establishes a group in the VOB by which all elements will be accessed (atria_vid). It also removes all other groups which might be present and could be used to access files. (A list of groups to be removed can be obtained with “cleartool describe vob:/vobs/Training” in our example).

The second command may not strictly be necessary, but is included for illustrative purposes. If the VOB in question is small, or relatively unpopulated, this may be enough to establish the group and file permissions (770) on all elements.

The third command actually goes out and finds all possible elements (visible or not) and applies the same group and permissions evident in command number two.

Now that we have a VOB that has been protected, let's have a look at how a client machine and username accesses the VOB. We will first use a username that is configured for full security access, and then look at a username that is not configured. We will then configure the second username and see the access subsequently enabled.

First, let's have a look at what environment variables we should have set. This is done in the Control Panels -> System window. Select the Advanced tab, and click on Environment Variables.



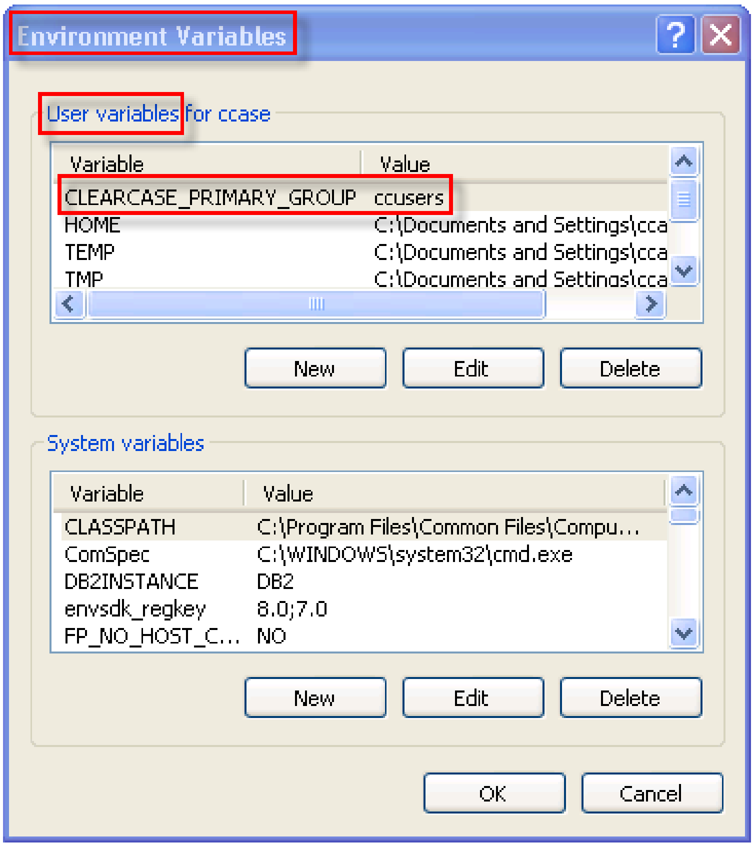
You must be logged on as an Administrator to make most of these changes.

Visual effects, processor scheduling, memory usage, and virtual memory

Desktop settings related to your logon

System startup, system failure, and debugging information

The next screenshot below shows the existing environment variables.



Environment Variables

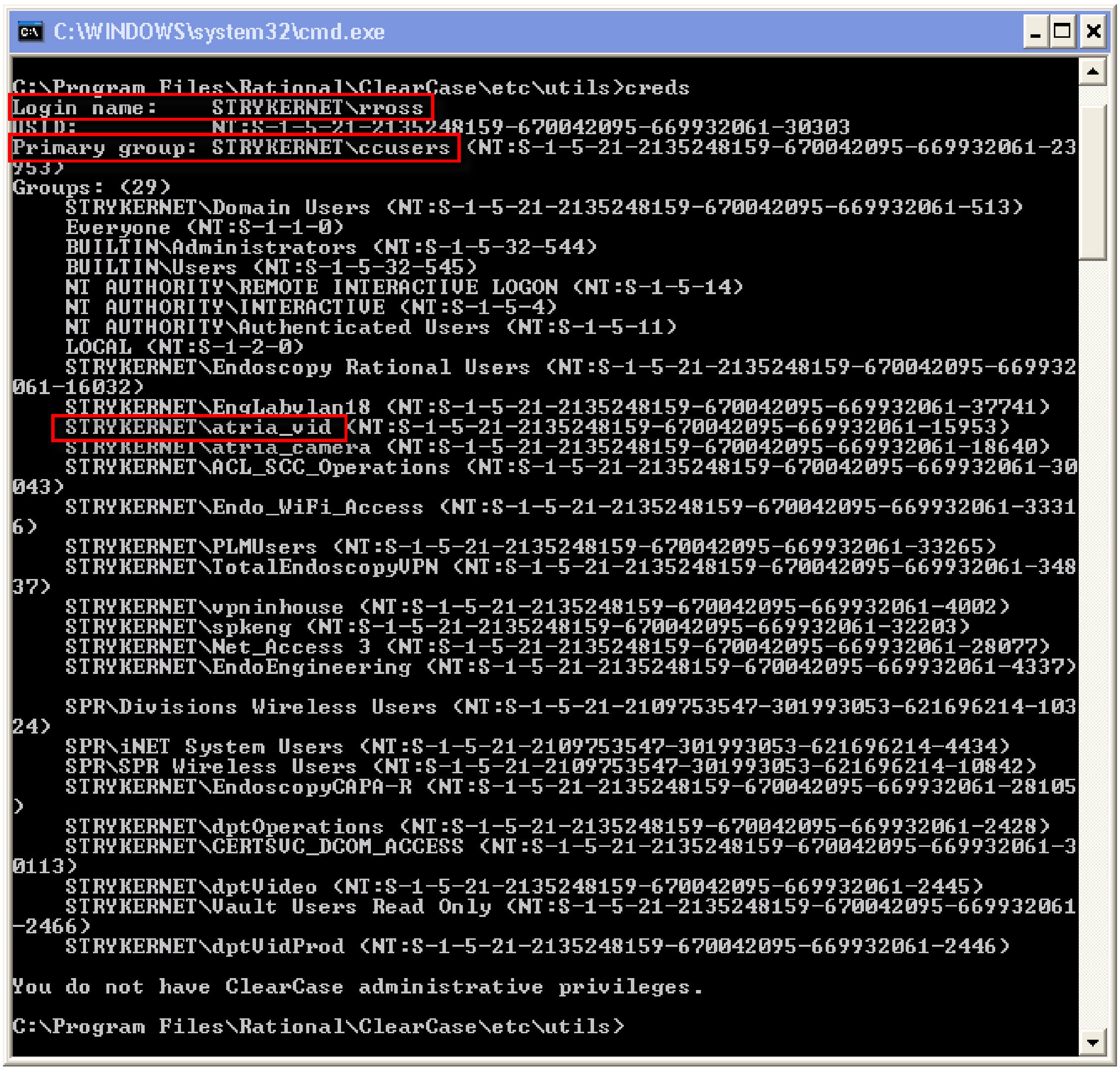
User variables for ccase

Variable	Value
CLEARCASE_PRIMARY_GROUP	ccusers
HOME	C:\Documents and Settings\cca
TEMP	C:\Documents and Settings\cca
TMP	C:\Documents and Settings\cca

System variables

Variable	Value
CLASSPATH	C:\Program Files\Common Files\Compu...
ComSpec	C:\WINDOWS\system32\cmd.exe
DB2INSTANCE	DB2
envsdk_regkey	8.0;7.0
FP_NO_HOST_C...	NO

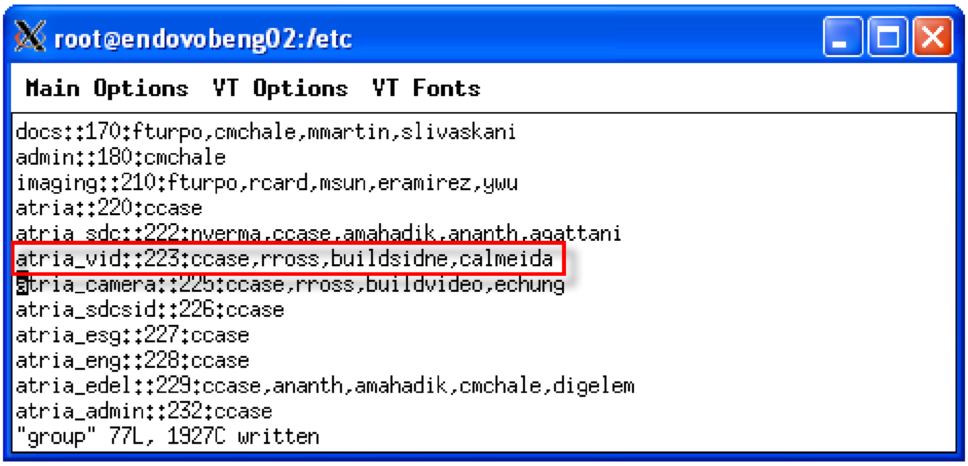
Here we have set a User variable: CLEARCASE_PRIMARY_GROUPS to “ccusers”, which will be the default group for any newly created files. Let’s look at the output below of the ClearCase “*creds*” command to see user and groups we are working with.



```
C:\Program Files\Rational\ClearCase\etc\utils>creds
Login name:     STRYKERNET\rross
USID:           NT:S-1-5-21-2135248159-670042095-669932061-30303
Primary group: STRYKERNET\ccusers (NT:S-1-5-21-2135248159-670042095-669932061-23
953)
Groups: (29)
    STRYKERNET\Domain Users (NT:S-1-5-21-2135248159-670042095-669932061-513)
    Everyone (NT:S-1-1-0)
    BUILTIN\Administrators (NT:S-1-5-32-544)
    BUILTIN\Users (NT:S-1-5-32-545)
    NT AUTHORITY\REMOTE INTERACTIVE LOGON (NT:S-1-5-14)
    NT AUTHORITY\INTERACTIVE (NT:S-1-5-4)
    NT AUTHORITY\Authenticated Users (NT:S-1-5-11)
    LOCAL (NT:S-1-2-0)
    STRYKERNET\Endoscopy Rational Users (NT:S-1-5-21-2135248159-670042095-669932
061-16032)
    STRYKERNET\EngLabvlan18 (NT:S-1-5-21-2135248159-670042095-669932061-37741)
    STRYKERNET\atria_vid (NT:S-1-5-21-2135248159-670042095-669932061-15953)
    STRYKERNET\atria_camera (NT:S-1-5-21-2135248159-670042095-669932061-18640)
    STRYKERNET\ACL_SCC_Operations (NT:S-1-5-21-2135248159-670042095-669932061-30
043)
    STRYKERNET\Endo_WiFi_Access (NT:S-1-5-21-2135248159-670042095-669932061-3331
6)
    STRYKERNET\PLMUsers (NT:S-1-5-21-2135248159-670042095-669932061-33265)
    STRYKERNET\TotalEndoscopyVPN (NT:S-1-5-21-2135248159-670042095-669932061-348
37)
    STRYKERNET\vpninhouse (NT:S-1-5-21-2135248159-670042095-669932061-4002)
    STRYKERNET\spkeng (NT:S-1-5-21-2135248159-670042095-669932061-32203)
    STRYKERNET\Net_Access 3 (NT:S-1-5-21-2135248159-670042095-669932061-28077)
    STRYKERNET\EndoEngineering (NT:S-1-5-21-2135248159-670042095-669932061-4337)

    SPR\Divisions Wireless Users (NT:S-1-5-21-2109753547-301993053-621696214-103
24)
    SPR\iNET System Users (NT:S-1-5-21-2109753547-301993053-621696214-4434)
    SPR\SPR Wireless Users (NT:S-1-5-21-2109753547-301993053-621696214-10842)
    STRYKERNET\EndoscopyCAPA-R (NT:S-1-5-21-2135248159-670042095-669932061-28105
)
    STRYKERNET\dptOperations (NT:S-1-5-21-2135248159-670042095-669932061-2428)
    STRYKERNET\CERTSVC_DCOM_ACCESS (NT:S-1-5-21-2135248159-670042095-669932061-3
0113)
    STRYKERNET\dptVideo (NT:S-1-5-21-2135248159-670042095-669932061-2445)
    STRYKERNET\Vault Users Read Only (NT:S-1-5-21-2135248159-670042095-669932061
-2466)
    STRYKERNET\dptVidProd (NT:S-1-5-21-2135248159-670042095-669932061-2446)

You do not have ClearCase administrative privileges.

C:\Program Files\Rational\ClearCase\etc\utils>
```

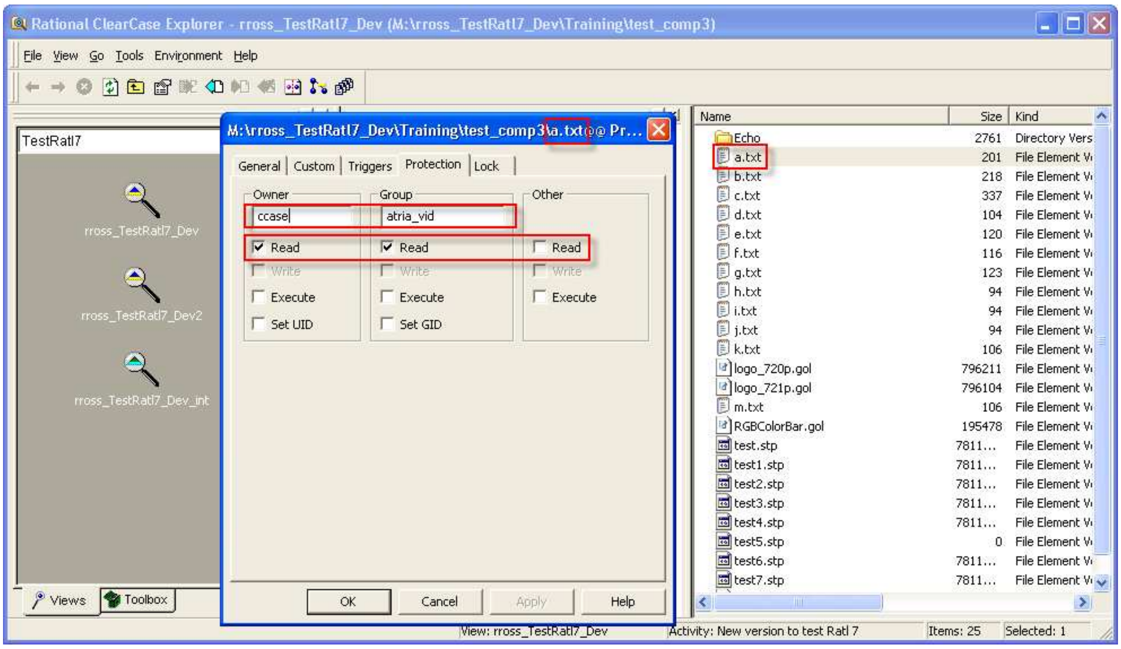
Here we see our user, “rross”, and the primary group that we previously specified, “ccusers”. Note also that there is a secondary group to which rross belongs – “atria_vid”. This is the group that we previously gave ownership to all elements in the \Training VOB.

This is the Windows side of the equation. But we also must take into account the Unix side, when we have a Windows/Linux mixed environment. Let’s have a look at the screenshot below for this.



```
docs::170:fturpo,cmchale,mmartin,slivaskani
admin::180:cmchale
imaging::210:fturpo,rcard,msun,eramirez,ywu
atria::220:ccase
atria_sdc::222:nverma,ccase,amahadik,ananth,agattani
atria_vid::223:ccase,rross,buildsidne,calmeida
atria_camera::225:ccase,rross,buildvideo,echung
atria_sdcsid::226:ccase
atria_esg::227:ccase
atria_eng::228:ccase
atria_edel::229:ccase,ananth,amahadik,cmchale,digelem
atria_admin::232:ccase
"group" 77L, 1927C written
```

On our Linux VOB server, under /etc/group, we see the entry for our security group – atria_vid. The entry contains the username "rross", which is a part of the group. We now launch ClearCase Explorer to have a look at how the group ownership is working.



Owner: ccase
☑ Read
☐ Write
☐ Execute
☐ Set UID

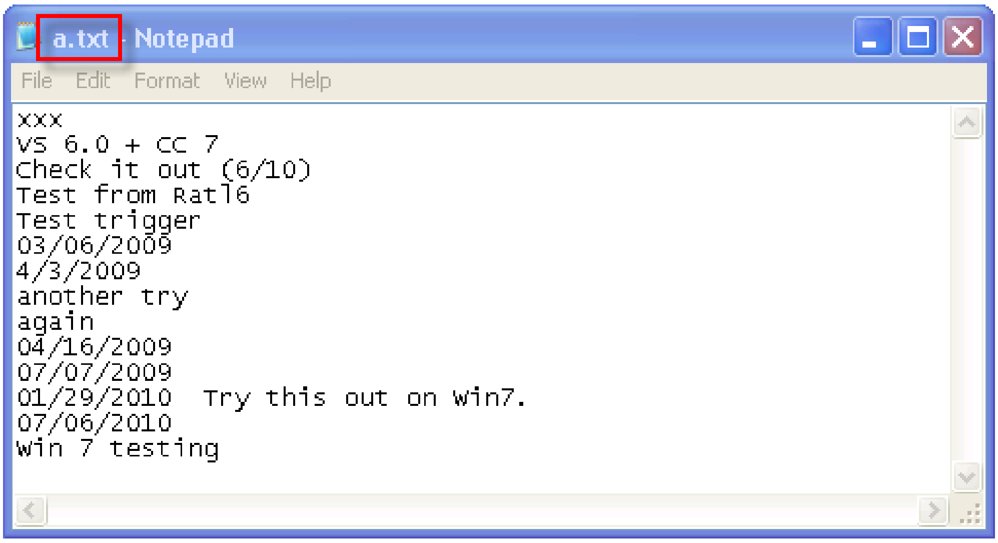
Group: atria_vid
☑ Read
☐ Write
☐ Execute
☐ Set GID

Other
☐ Read
☐ Write
☐ Execute

Name	Size	Kind
Echo	2761	Directory Vers
a.txt	201	File Element Vi
b.txt	218	File Element Vi
c.txt	337	File Element Vi
d.txt	104	File Element Vi
e.txt	120	File Element Vi
f.txt	116	File Element Vi
g.txt	123	File Element Vi
h.txt	94	File Element Vi
i.txt	94	File Element Vi
j.txt	94	File Element Vi
k.txt	106	File Element Vi
logo_720p.gol	796211	File Element Vi
logo_721p.gol	796104	File Element Vi
m.txt	106	File Element Vi
RGBColorBar.gol	195478	File Element Vi
test.stp	7811...	File Element Vi
test1.stp	7811...	File Element Vi
test2.stp	7811...	File Element Vi
test3.stp	7811...	File Element Vi
test4.stp	7811...	File Element Vi
test5.stp	0	File Element Vi
test6.stp	7811...	File Element Vi
test7.stp	7811...	File Element Vi

View: rross_TestRatl7_Dev | Activity: New version to test Ratl 7 | Items: 25 | Selected: 1

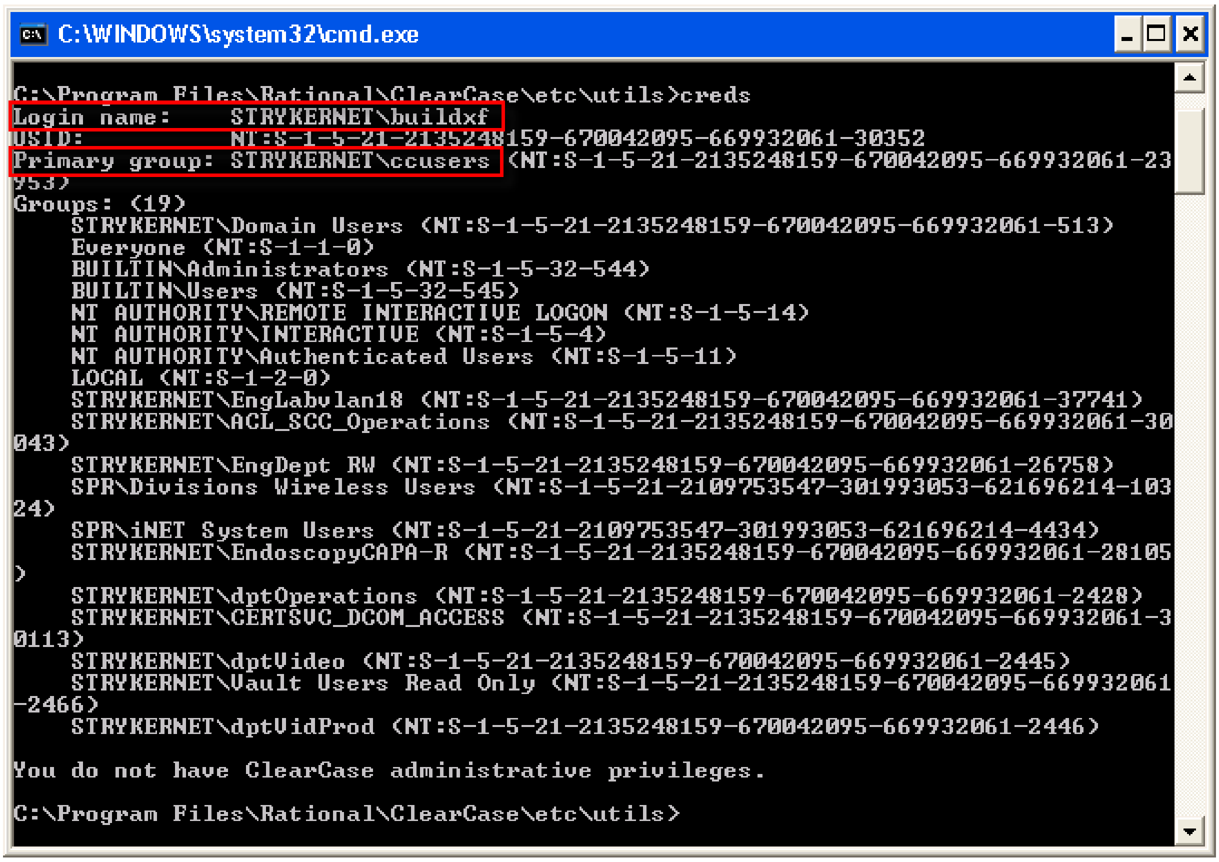
We use a user view to open the Training VOB and have a look at a file contained in it. This file, a.txt, is shown with its properties above. We see that it has group access with atria_vid, and owner+group access. Next we will try to open the file below.



```
xxx
VS 6.0 + CC 7
Check it out (6/10)
Test from Rat16
Test trigger
03/06/2009
4/3/2009
another try
again
04/16/2009
07/07/2009
01/29/2010  Try this out on Win7.
07/06/2010
Win 7 testing
```

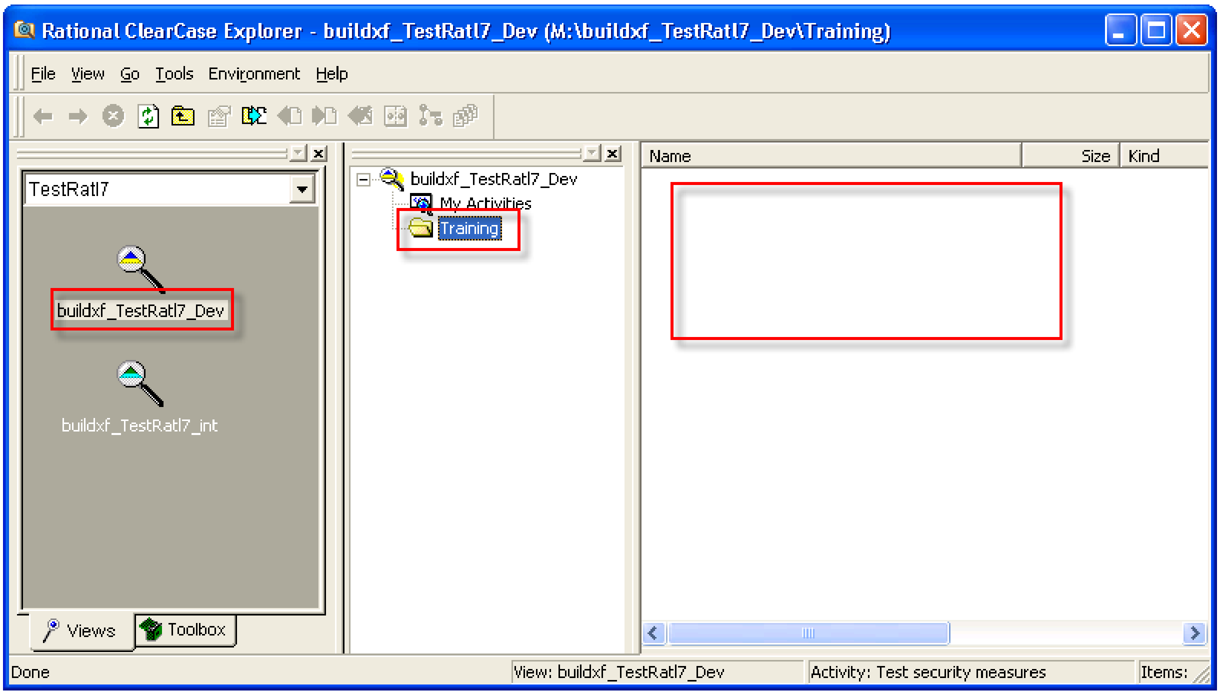
We use Notepad to open the file, and we are able to read the contents of the file. It is also possible to checkout, modify and checkin the file, but we will skip the tedium of demonstrating this.

So user “rross” has access to the files. But now let’s have a look at a different user who does not have access, and what we must do to establish access. The user will be the group account – buildxf. See the group membership in the screenshot below.

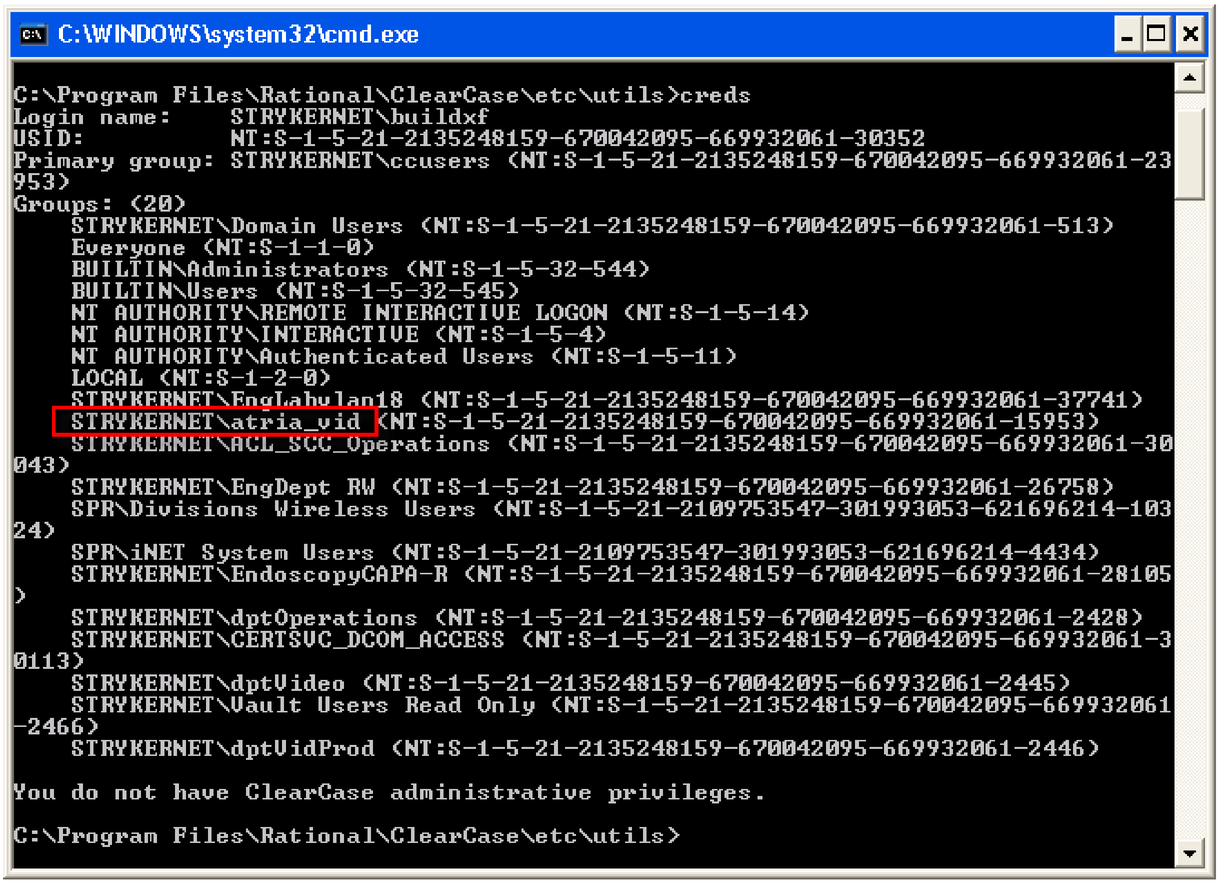


```
C:\Program Files\Rational\ClearCase\etc\utils>creds
Login name:     STRYKERNET\buildxf
USID:           NT:S-1-5-21-2135248159-670042095-669932061-30352
Primary group: STRYKERNET\ccusers (NT:S-1-5-21-2135248159-670042095-669932061-23
953)
Groups: (19)
    STRYKERNET\Domain Users (NT:S-1-5-21-2135248159-670042095-669932061-513)
    Everyone (NT:S-1-1-0)
    BUILTIN\Administrators (NT:S-1-5-32-544)
    BUILTIN\Users (NT:S-1-5-32-545)
    NT AUTHORITY\REMOTE INTERACTIVE LOGON (NT:S-1-5-14)
    NT AUTHORITY\INTERACTIVE (NT:S-1-5-4)
    NT AUTHORITY\Authenticated Users (NT:S-1-5-11)
    LOCAL (NT:S-1-2-0)
    STRYKERNET\EngLabvlan18 (NT:S-1-5-21-2135248159-670042095-669932061-37741)
    STRYKERNET\ACL_SCC_Operations (NT:S-1-5-21-2135248159-670042095-669932061-30
043)
    STRYKERNET\EngDept RW (NT:S-1-5-21-2135248159-670042095-669932061-26758)
    SPR\Divisions Wireless Users (NT:S-1-5-21-2109753547-301993053-621696214-103
24)
    SPR\iNET System Users (NT:S-1-5-21-2109753547-301993053-621696214-4434)
    STRYKERNET\EndoscopyCAPA-R (NT:S-1-5-21-2135248159-670042095-669932061-28105
)
    STRYKERNET\dptOperations (NT:S-1-5-21-2135248159-670042095-669932061-2428)
    STRYKERNET\CERTSVC_DCOM_ACCESS (NT:S-1-5-21-2135248159-670042095-669932061-3
0113)
    STRYKERNET\dptVideo (NT:S-1-5-21-2135248159-670042095-669932061-2445)
    STRYKERNET\Vault Users Read Only (NT:S-1-5-21-2135248159-670042095-669932061
-2466)
    STRYKERNET\dptVidProd (NT:S-1-5-21-2135248159-670042095-669932061-2446)

You do not have ClearCase administrative privileges.

C:\Program Files\Rational\ClearCase\etc\utils>
```

Here we see user buildxf with our standard primary group already defined. But we do not see a reference to the secondary group – atria_vid. Let’s bring up ClearCase Explorer again and see what happens. See the screenshot below.

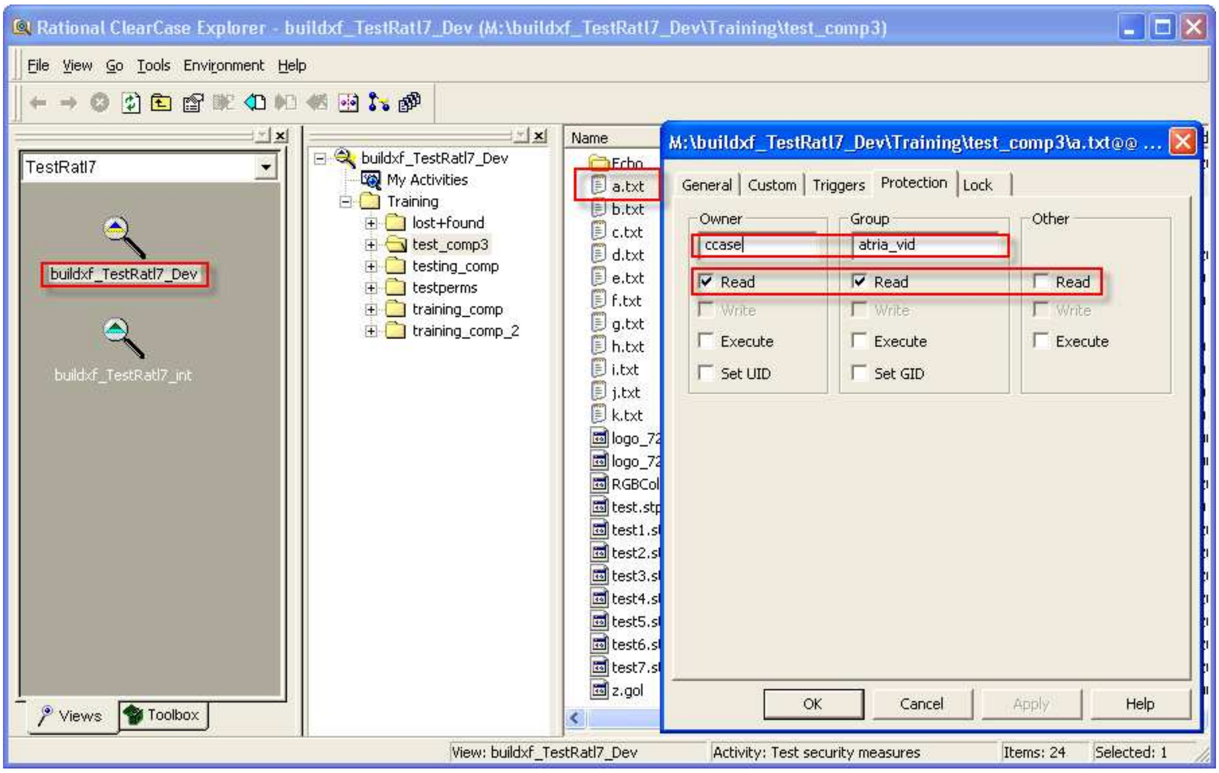

Rational ClearCase Explorer - buildxf_TestRatl7_Dev (M:\buildxf_TestRatl7_Dev\Training)
File View Go Tools Environment Help
TestRatl7
buildxf_TestRatl7_Dev
buildxf_TestRatl7_int
Views
Toolbox
buildxf_TestRatl7_Dev
My Activities
Training
Name
Size
Kind
Done
View: buildxf_TestRatl7_Dev
Activity: Test security measures
Items:

Again we access a view and the Training VOB. However, nothing shows up in the right hand Explorer panel. This user has no authority to read anything. Remember that we have changed all directory (folder) and file permissions to owner+group. So, let’s take the first step toward remedying this. We go ahead and add buildxf to the Windows group atria_vid. Let’s see the first results of this below.



```
C:\Program Files\Rational\ClearCase\etc\utils>creds
Login name:    STRYKERNET\buildxf
USID:          NT:S-1-5-21-2135248159-670042095-669932061-30352
Primary group: STRYKERNET\ccusers (NT:S-1-5-21-2135248159-670042095-669932061-23
953)
Groups: (20)
    STRYKERNET\Domain Users (NT:S-1-5-21-2135248159-670042095-669932061-513)
    Everyone (NT:S-1-1-0)
    BUILTIN\Administrators (NT:S-1-5-32-544)
    BUILTIN\Users (NT:S-1-5-32-545)
    NT AUTHORITY\REMOTE INTERACTIVE LOGON (NT:S-1-5-14)
    NT AUTHORITY\INTERACTIVE (NT:S-1-5-4)
    NT AUTHORITY\Authenticated Users (NT:S-1-5-11)
    LOCAL (NT:S-1-2-0)
    STRYKERNET\EngLabvlan18 (NT:S-1-5-21-2135248159-670042095-669932061-37741)
    STRYKERNET\atria_vid (NT:S-1-5-21-2135248159-670042095-669932061-15953)
    STRYKERNET\ACL_SCC_Operations (NT:S-1-5-21-2135248159-670042095-669932061-30
043)
    STRYKERNET\EngDept RW (NT:S-1-5-21-2135248159-670042095-669932061-26758)
    SPR\Divisions Wireless Users (NT:S-1-5-21-2109753547-301993053-621696214-103
24)
    SPR\iNET System Users (NT:S-1-5-21-2109753547-301993053-621696214-4434)
    STRYKERNET\EndoscopyCAPA-R (NT:S-1-5-21-2135248159-670042095-669932061-28105
)
    STRYKERNET\dptOperations (NT:S-1-5-21-2135248159-670042095-669932061-2428)
    STRYKERNET\CERTSVC_DCOM_ACCESS (NT:S-1-5-21-2135248159-670042095-669932061-3
0113)
    STRYKERNET\dptVideo (NT:S-1-5-21-2135248159-670042095-669932061-2445)
    STRYKERNET\Vault Users Read Only (NT:S-1-5-21-2135248159-670042095-669932061
-2466)
    STRYKERNET\dptVidProd (NT:S-1-5-21-2135248159-670042095-669932061-2446)

You do not have ClearCase administrative privileges.

C:\Program Files\Rational\ClearCase\etc\utils>
```

The *creds* command displays what we saw before, but with the addition of the new secondary group – atria_vid. Let's see the effect this has now when we again use ClearCase Explorer.



Rational ClearCase Explorer - buildxf_TestRatl7_Dev (M:\buildxf_TestRatl7_Dev\Training\test_comp3)

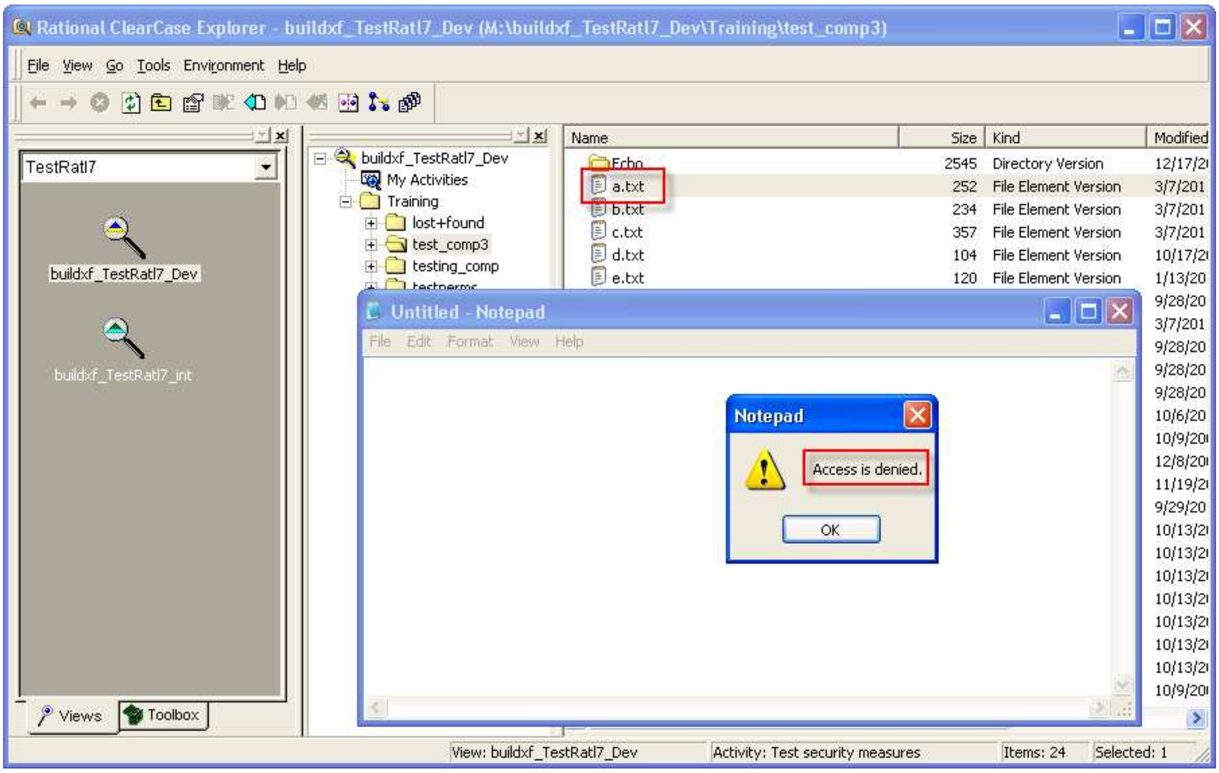
M:\buildxf_TestRatl7_Dev\Training\test_comp3\a.txt@@ ...

Owner: ccase
Group: atria_vid

Owner	Group	Other
☑ Read	☑ Read	□ Read
□ Write	□ Write	□ Write
□ Execute	□ Execute	□ Execute
□ Set UID	□ Set GID	

View: buildxf_TestRatl7_Dev | Activity: Test security measures | Items: 24 | Selected: 1

We are now able to see all the files under the Training VOB and its component (test_comp3). We again look at the same file we previously examined with user rross, and we see that since buildxf joined the atria_vid group, we now have access to seeing the files. So are we all the way there? Not quite, it seems. Have a look at the next screenshot below.

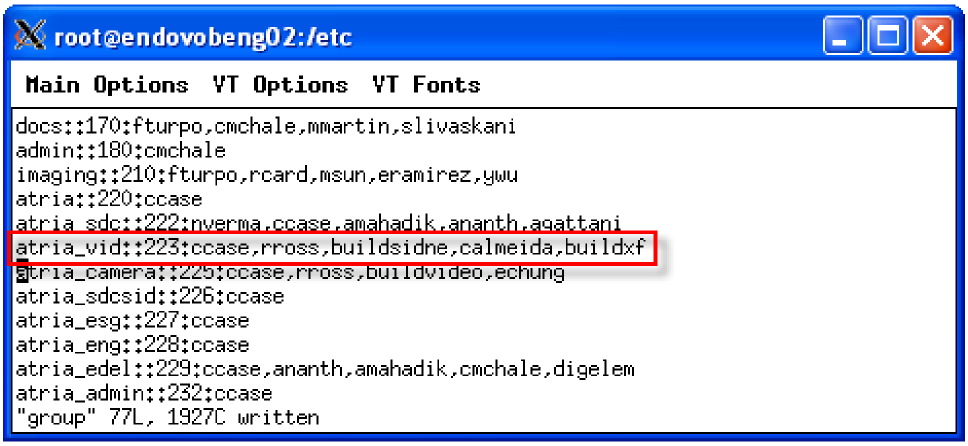


Name	Size	Kind	Modified
Echo	2545	Directory Version	12/17/2
a.txt	252	File Element Version	3/7/201
b.txt	234	File Element Version	3/7/201
c.txt	357	File Element Version	3/7/201
d.txt	104	File Element Version	10/17/2
e.txt	120	File Element Version	1/13/20

Access is denied.

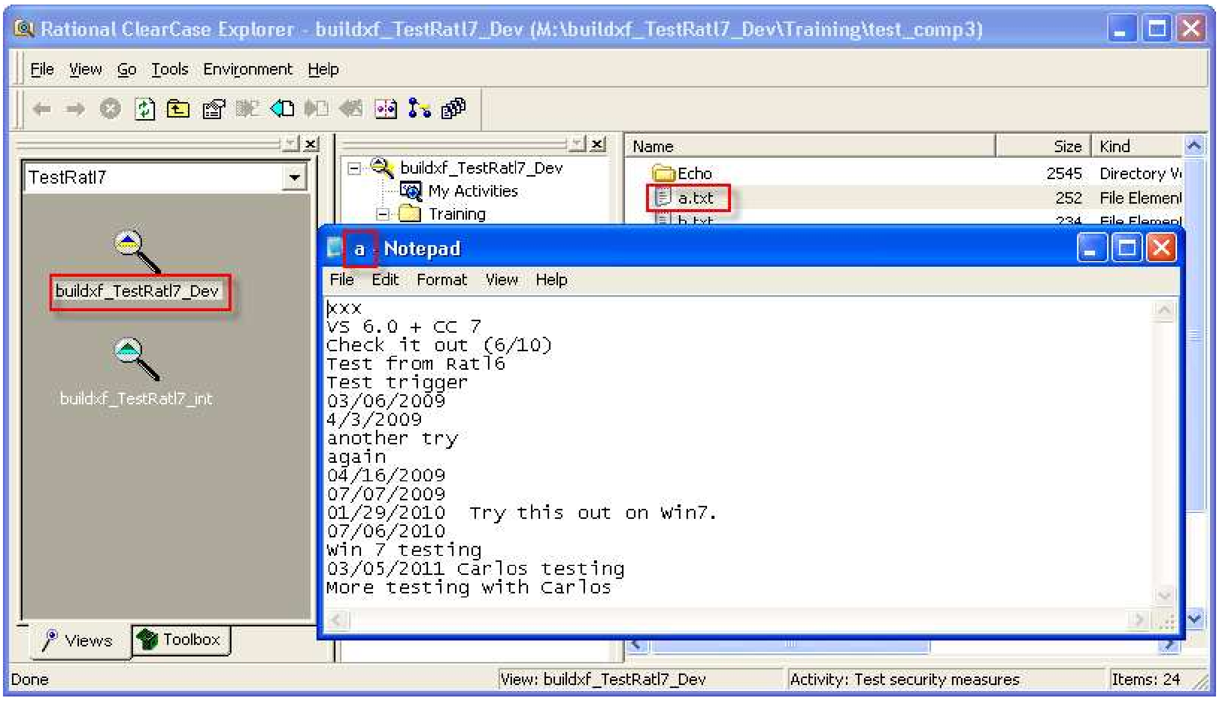
View: buildxf_TestRatl7_Dev Activity: Test security measures Items: 24 Selected: 1

Above we have attempted to open the file, as before with rross, and examine the contents. But we encounter a permissions error! What is the problem? In this case we have made the user a member of the Windows atria_vid group, but there is a missing piece. The next screenshot gives us the resolution to the issue. Here we have added the user buildxf to the Unix group – atria_vid.



```
docs::170:fturpo,cmchale,mmartin,slivaskani
admin::180:cmchale
imaging::210:fturpo,rcard,msun,eramirez,ywu
atria::220:ccase
atria_sdc::222:nverma,ccase,amahadik,ananth,agattani
atria_vid::223:ccase,rross,buildsidne,calmeida,buildxf
atria_camera::225:ccase,rross,buildvideo,echung
atria_sdcsid::226:ccase
atria_esg::227:ccase
atria_eng::228:ccase
atria_edel::229:ccase,ananth,amahadik,cmchale,digelem
atria_admin::232:ccase
"group" 77L, 1927C written
```

As with the rross username, buildxf also needs to be made a part of the corresponding Unix group to enable full access to the file system. As a side note, we were told by IBM that membership in the Unix group does not matter, but this is different from our experience, and what we see in this example. After adding the user to the Unix version of the group, we can see the result below.


Rational ClearCase Explorer - buildxf_TestRatl7_Dev (M:\buildxf_TestRatl7_Dev\Training\test_comp3)
File View Go Tools Environment Help
TestRatl7
buildxf_TestRatl7_Dev
buildxf_TestRatl7_int
Views
Toolbox
buildxf_TestRatl7_Dev
My Activities
Training
Name
Size
Kind
Echo
2545
Directory V
a.txt
252
File Element
b.txt
234
File Element
a - Notepad
File Edit Format View Help
Done
View: buildxf_TestRatl7_Dev
Activity: Test security measures
Items: 24

```
xxx
VS 6.0 + CC 7
Check it out (6/10)
Test from Ratl6
Test trigger
03/06/2009
4/3/2009
another try
again
04/16/2009
07/07/2009
01/29/2010  Try this out on win7.
07/06/2010
Win 7 testing
03/05/2011 Carlos testing
More testing with Carlos
```

It is now possible to fully access the files that are members of the group atria_vid, as seen in the screenshot above. At this point, we have demonstrated the two things that we set out to accomplish:

- We have demonstrated how group membership needs to be set up to enable file access when working in a mixed Unix/Linux and Windows environment.

- We have also demonstrated how to use group membership to establish code security and limit the access to only those who have been made members of the approved group(s).

The solution outlined above for code security is not airtight, but it seems quite workable, assuming that good control of group membership is possible. We have heard from IBM/Rational that when ClearCase 8.0 is released it will include a more formal and better way to control code access. Perhaps this is overdue, but until IBM/Rational decides to provide a better security solution, what we have demonstrated here may be the best that is available, although others may have better ideas.

As a final note, there is a last consideration to be aware of when implementing a solution like the one demonstrated above. After permissions are set, and access is allowed, there is then the question of how new files are treated when they are added to the VOB. We have defined our solution in terms of all files being owned by a single group. But new files may by default be owned by other groups. There are two solutions for this:

- Make sure that every person who is accessing the codebase has a user environment variable CLEARCASE_PRIMARY_GROUP set to the correct group, in this case: atria_vid
- Create a postoperative trigger that fires after checkin and changes the group to the correct value, and also enforces file permissions, excluding Other from having read permission.

These two solutions are, of course, not mutually exclusive and may be used together. In fact, it’s probably a good idea to at least have the trigger operative to enforce uniformity of group membership for all VOB elements. The users may be working on various projects, and setting the CLEARCASE_PRIMARY_GROUP variable may be inconvenient in such a situation.