

Re: Admin / Domain Admin rights problem

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-07/0016.html>

From: Roger Abell (*mvpNOSpam_at_asu.edu*)

Date: 07/01/05

Date: Fri, 1 Jul 2005 07:46:05 -0700

It sure is starting to sound like a malware based inhibition of registry tool access.

--

Roger

"Steven L Umbach" <n9rou@nospam-comcast.net> wrote in message news:e%233zjHbfFHA.1412@TK2MSFTNGP09.phx.gbl...

> Hmm. From what I can tell it looks like subinacl shows that administrators > have full control of HKLM. I am at a loss as why you can not edit it. I > always use regedt32 for Windows 2000 so you may want to try that if you have

> not yet. If it was my computer I would not use subinacl until I had an image

> backup. As far as Group Policy - registry you will not see that in Local > Group Policy but it should show in Domain Controller Security Policy if SBS

> has such. If you can not get for antivirus to work try using the SysClean > utility from Trend Micro [see links below]. Just download Sysclean and the > pattern file [after unzipping] into a common folder to run from - no > installation is involved. --- Steve

>

> <http://www.trendmicro.com/download/dcs.asp>

> <http://www.trendmicro.com/download/pattern.asp>

>

> "Andy Roxburgh" <spamplease@hotmail.co.uk> wrote in message

> news:usMh4EYfFHA.3904@TK2MSFTNGP14.phx.gbl...

> > Hi Steven,

> >

> >> Make sure that you are logging on as the administrator account and not

> > some

> >> renamed administrator which is sometimes used as a domain account. The

> >> command "net user administrator" will display group membership.

> >

> > I get (exactly as output) :

> >

> > Logon Script

> > User Profile

> > Home Directory

> > Last logon 6/30/2005 2:00pm

> >

> > Logon Hours Allowed All

> >

> > Local Group Memberships

> > *Account Operators

> > *Administrators

> > *Backup operators

microsoft.public.win2000.security: Re: Admin / Domain Admin rights problem

```
> > *Server Operators
> > *Print Operators
> >
> > Global Group Memberships
> > *Exchange Services
> > *Domain Admins
> > *Domain Users
> > *Enterprise Admins
> > *Exchange Domain Serve
> > *Group Policy Creator
> > *Backoffice Internet U
> > *Scheme Admins
> >
> >>Also verify
> >> that domain admins is a member of the administrators group for the
domain
> > as
> >> it is possible for it to be removed.
> >
> > I checked this with the SBS Admin console and it appears to be OK.
> >
> >>You should also run a full malware scan
> >> on your server being sure to use the latest definitions from your
vendor.
> >
> > Just tried a full AV scan and it consistently locks up half way
through -
> > not a great sign!
> > Just ran MS Antyspyware beta and it's clean; will try a different AV
> > scanner
> > and try again.
> >
> >> Also some "protection" packages can block access to the registry I am
> > told.
> >> You may want to boot into safe mode to see if that helps.
> >
> > Will try this at the weekend - the server's in use at the moment.
> >
> >>Subinacl is a tool
> >> that can be used to view and change file and registry permissions at
the
> >> command line if need be. However it is very powerful and I would not
use
> > it
> >> unless you have a full image type backup of your server or you are very
> >> confident that you are using the right command possibly from trying it
on
> > a
> >> test computer first.
> >
> > Thanks! Have used it to show the HKLM permissions. Typing
> > subinacl /key HKEY_LOCAL_MACHINE /display
> > I get :
> >
> > =====
> > +KeyReg HKEY_LOCAL_MACHINE
> > =====
> > /control=0x0
> > /owner          =builtin\administrators
> > /primary group  =system
> > /audit ace count =0
> > /perm. ace count =4
```

microsoft.public.win2000.security: Re: Admin / Domain Admin rights problem

```
> >
> > /pace =system ACCESS_ALLOWED_ACE_TYPE-0x0
> > CONTAINER_INHERIT_ACE-0x2
> > Key and SubKey - Type of Access:
> > Full Control
> > Detailed Access Flags :
> > KEY_QUERY_VALUE-0x1 KEY_SET_VALUE-0x2
> > KEY_CREATE_SUB_KEY-0x4
> > KEY_ENUMERATE_SUB_KEYS-0x8 KEY_NOTIFY-0x10
KEY_CREATE_LINK-0x20
> > DELETE-0x10000
> > READ_CONTROL-0x20000 WRITE_DAC-0x40000
WRITE_OWNER-0x80000
> >
> > /pace =builtin\administrators ACCESS_ALLOWED_ACE_TYPE-0x0
> > CONTAINER_INHERIT_ACE-0x2
> > Key and SubKey - Type of Access:
> > Full Control
> > Detailed Access Flags :
> > KEY_QUERY_VALUE-0x1 KEY_SET_VALUE-0x2
> > KEY_CREATE_SUB_KEY-0x4
> > KEY_ENUMERATE_SUB_KEYS-0x8 KEY_NOTIFY-0x10
KEY_CREATE_LINK-0x20
> > DELETE-0x10000
> > READ_CONTROL-0x20000 WRITE_DAC-0x40000
WRITE_OWNER-0x80000
> >
> > /pace =everyone ACCESS_ALLOWED_ACE_TYPE-0x0
> > CONTAINER_INHERIT_ACE-0x2
> > Key and SubKey - Type of Access:
> > Read
> > Detailed Access Flags :
> > KEY_QUERY_VALUE-0x1 KEY_ENUMERATE_SUB_KEYS-0x8 KEY_NOTIFY-0x10
> > READ_CONTROL-0x20000
> >
> > /pace =restricted ACCESS_ALLOWED_ACE_TYPE-0x0
> > CONTAINER_INHERIT_ACE-0x2
> > Key and SubKey - Type of Access:
> > Read
> > Detailed Access Flags :
> > KEY_QUERY_VALUE-0x1 KEY_ENUMERATE_SUB_KEYS-0x8 KEY_NOTIFY-0x10
> > READ_CONTROL-0x20000
> >
> >
> > and this compares to HKEY_USERS which I do have access to as follows:
> >
> >
> > =====
> > +KeyReg HKEY_USERS
> > =====
> > /control=0x0
> > /owner =builtin\administrators
> > /primary group =system
> > /audit ace count =0
> > /perm. ace count =4
> >
> > /pace =system ACCESS_ALLOWED_ACE_TYPE-0x0
> > CONTAINER_INHERIT_ACE-0x2
> > Key and SubKey - Type of Access:
> > Full Control
> > Detailed Access Flags :
```

microsoft.public.win2000.security: Re: Admin / Domain Admin rights problem

```
> > KEY_QUERY_VALUE-0x1          KEY_SET_VALUE-0x2
> > KEY_CREATE_SUB_KEY-0x4
> > KEY_ENUMERATE_SUB_KEYS-0x8  KEY_NOTIFY-0x10
KEY_CREATE_LINK-0x20
> > DELETE-0x10000
> > READ_CONTROL-0x20000        WRITE_DAC-0x40000
WRITE_OWNER-0x80000
> >
> > /pace =builtin\administrators  ACCESS_ALLOWED_ACE_TYPE-0x0
> > CONTAINER_INHERIT_ACE-0x2
> >   Key and SubKey - Type of Access:
> > Full Control
> >   Detailed Access Flags :
> > KEY_QUERY_VALUE-0x1          KEY_SET_VALUE-0x2
> > KEY_CREATE_SUB_KEY-0x4
> > KEY_ENUMERATE_SUB_KEYS-0x8  KEY_NOTIFY-0x10
KEY_CREATE_LINK-0x20
> > DELETE-0x10000
> > READ_CONTROL-0x20000        WRITE_DAC-0x40000
WRITE_OWNER-0x80000
> >
> > /pace =everyone  ACCESS_ALLOWED_ACE_TYPE-0x0
> > CONTAINER_INHERIT_ACE-0x2
> >   Key and SubKey - Type of Access:
> > Read
> >   Detailed Access Flags :
> > KEY_QUERY_VALUE-0x1          KEY_ENUMERATE_SUB_KEYS-0x8  KEY_NOTIFY-0x10
> > READ_CONTROL-0x20000
> >
> > /pace =restricted  ACCESS_ALLOWED_ACE_TYPE-0x0
> > CONTAINER_INHERIT_ACE-0x2
> >   Key and SubKey - Type of Access:
> > Read
> >   Detailed Access Flags :
> > KEY_QUERY_VALUE-0x1          KEY_ENUMERATE_SUB_KEYS-0x8  KEY_NOTIFY-0x10
> > READ_CONTROL-0x20000
> >
> > To me it looks fine; but there's definitely something wrong somewhere
> > because it won't show HKLM permissions etc from regedit!
> >
> > Do you think I should try
> >
> > subinacl /subkeyreg HKEY_LOCAL_MACHINE /grant=administrators=f
> > subinacl /subkeyreg HKEY_LOCAL_MACHINE /grant=systems=f
> >
> > ?
> >
> > Ironically the reason I'm going through all this is so that I can create
a
> > ghost image - I'm using Veritas IDR and it's not playing ball.
> > So I can't easily ghost the server before making changes.
> >
> >>Group Policy can also be used to manage registry
> >> permissions via computer configuration/Windows settings/security
> >> settings -
> >> registry though you need to be careful doing such and should unlink the
> >> Group Policy when done and needs to be linked to the proper OU where
the
> >> computer accounts are.  Improper use of file/registry permissions via
> >> Group
> >> Policy can cause performance problems in the domain. --- Steve
> >
```

