

Re: Remove administrator account from domain guest group

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2009-02/msg01961.html>

- *From:* Bob <Bob@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 23 Feb 2009 09:09:03 -0800
-

Must have been a typo. I ran the following from a batch file, cycled the logon and it worked on my test machine. I will try on the clients PC and post back results. Thank you!

```
dsmod group "CN=Guests,CN=Builtin,DC=smallbusiness,DC=local" -rmmbr "CN=Administrator,CN=Users,DC=smallbusiness,DC=local"
```

"kj [SBS MVP]" wrote:

Bob wrote:

I opened up a command prompt while logged in as Administrator.

As I'm running this from a virtual PC that I have complete control over, I could setup another "admin" account that is not a member of the guests account and have full control without errors. That won't help in my clients case however.

What is really scary is that this could easily be used to attack a windows server. All they would have to do is put the "everyone" group into a guest account and you'd have a hell of a mess.

Misuse of Domain Admin accounts certainly can wreak plenty of havoc. There is no denying that.

Why your dsmod command did not complete is at issue. So you are saying that the client has not other admin accounts to attempt this from correct?

So, if the admin is in "Guests", you would use "CN=Guests...." and if in "Domain Guests" then "CN=Domain Guests..." in your dsmod command.

If you don't have permissions or a deny is in effect you should receive an error... but a hang indicates some other issue in your enviroment. I'd first start with version checking the DS tools on your virtual XP workstation if you aren't able to execute this directly from the SBS server.

Re: Remove administrator account from domain guest group

"Bob" wrote:

These are the results.

```
"CN=Guests,CN=Builtin,DC=smallbusiness,DC=local"  
"CN=Domain  
Guests,CN=Users,DC=smallbusiness,DC=local"
```

```
"CN=Administrator,CN=Users,DC=smallbusiness,DC=local"  
"CN=Guest,CN=Users,DC=smallbusiness,DC=local"
```

"kj [SBS MVP]" wrote:

What account did you use? Where did you run the dsmod command from?

Do you have another account with domain admin priviledges?

so you might try making sure your Distinguished Name is correct by using a dsquery

```
dsquery group
```

.... then find and check the DN of the "domain guests" and compare to what you've entered.

if that's good, make sure of the DN for the administrator account using the same method but this time using dsquery user instead.

(btw, the command should all be on one line)

Bob wrote:

When I run the following it just hangs and never completes.

```
dsmod group  
"CN=Guests,CN=Builtin,DC=smallbusiness,DC=local"
```

Re: Remove administrator account from domain guest group

```
-rmmb  
"CN=Administrator,CN=Users,DC=smallbusiness,DC=local"
```

"kj [SBS MVP]" wrote:

Have you
tried the
Directory
services
tools?

Like;

```
dsmod  
group  
"CN=Guests,CN=Builtin,DC=yourdomainname,DC=local"  
-rmmb  
"CN=Administrator,CN=Users,DC=yourdomainname,DC=local"
```

Bob wrote:

Hello
group,

I
am
searching
for
a
method
of
removing
the
adminstrator
from
the
domain
guest
users
group.
I
have
a
customer
that
I
suspect

Re: Remove administrator account from domain guest group

this
has
happened
to.
I've
created
a
virtual
pc
of
sbs03
and
replicated
the
problem
by
adding
the
admin
acct
to
the
domain
guest
acct.
This
is
what
I'm
seeing.

When
I
try
to
launch
Exchange
System
Manager
I
get
a
small
window
as
below:

Exchange
System
Manager
Access

Re: Remove administrator account from domain guest group

is
denied
Facility:
Win32
ID
no:
c0070005
Exchange
System
Manager

This
will
also
appear
when
trying
to
view
any
objects
in
ADUC,
including
domain
groups.
Server
management
gives
the
same
error.
I've
tried
from
DS
restore
mode
but
can't
seem
to
bring
the
domain
up.

Now,
mind
you,
I've

Re: Remove administrator account from domain guest group

replicated
this
issue
on
a
freshly
installed
copy
of
sbs03
and
induced
the
error
by
adding
the
user
"administrator"
to
the
group
"Domain
Guests".
I
know
what
to
do,
I
just
don't
know
how
to
go
about
doing
it.
I've
seen
other
postings
that
talk
about
what
needs
to
be
done

Re: Remove administrator account from domain guest group

but
none
that
explain
the
steps.

Can
someone
shed
some
light
on
this?

Thanks
in
advance!

Bob

--
/kj

--
/kj

--
/kj