

Re: Less Informaion Availiable in LDAP on SBS than Server 2003

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-11/msg00099.html>

- *From:* cleopold73 <cleopold73@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 1 Nov 2007 10:30:01 -0700
-

Ok, I think we have this run down....

The group "Pre-Windows 2000 Compatible Access" has permissions to access all these attributes we cannot access, on our install of Server 2003R2 the "Authenticated Users" group is a member of "Pre-Windows 2000 Compatible Access", which then allows access to all attributes for any user accessing AD via LDAP. On SBS "Autnenticated Users" is not a member of "Pre-Windows 2000 Compatable Access". When we added our ldap-proxy user to "Pre-Windows 2000 Compatible Access" we were able to query all attributes just fine on SBS.

The only open question to understand if there are implications (particularly security related) to being part of the "Pre-Windows 2000 Compatible Access" group?

Thanks

Corey

"Claus" wrote:

For a quick explanation on the user group templates see this...
<http://www.microsoft.com/technet/prodtechnol/sbs/2003/plan/gsg/chapter4.mspx>

You can also modify your setup to allow anonymous LDAP access...
<http://support.microsoft.com/kb/326690>

--

Claus

"cleopold73" <cleopold73@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:D0B7B1A3-3217-410A-83DD-16B921980940@xxxxxxxxxxxxxxxxxxxxx

Just tried and apparently if a user account is a member of "Domain Power Users" then I can query these LDAP attributes.

Re: Less Informaion Available in LDAP on SBS than Server 2003

I'm not sure what is the right solution though, my understanding is that using LDAP this way causes the password go accross in the clear, which is why we wanted to use a very limited account, like you can use under 2003R2.

What additional permissions do "Domain Power Users" have, that could be problematic?

Thanks

Corey

"Claus" wrote:

Have you tried running the LDAP query under a power user account?

--

Claus

"cleopold73" <cleopold73@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in message

news:48DE47A6-5652-4356-962B-01006830BC33@xxxxxxxxxxxxxxxxxxxx

I am querying the attributes with this tool,
which is just a generic
LDAP
browser tool...

<http://www-unix.mcs.anl.gov/~gawor/ldap/>

I get the same results using ldapsearch from
a UNIX command line when
querying through ldap.

What makes this problem worse, is we have
joined a regular 2003 R2
Domain
Controller to the SBS domain, and the ldap
permissions problems
replicate
over to it, causing us not to be able to query
the UNIX attributes from
the
2003 R2 DC either...

Thanks,

Corey

Re: Less Informaion Available in LDAP on SBS than Server 2003

"kj [SBS MVP]" wrote:

It would have to be R2 to
get schema 31, Cris

OP, While you might
upgrade the schema on SBS
to v31 note that a SBS
R2
server does not have all the
same interoperability
componets and
services
installed that Server 2003
R2 has (unfortunatly).

OP, What method & manner
were you using to query the
SBS R2 (with
adprep
V31 schema) for those
attributes?

--

/kj

"Cris Hanna [SBS-MVP]"

<crisnospamhanna@xx>

wrote in message

[news:eq3Hbb\\$GIHA.5328@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:eq3Hbb$GIHA.5328@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

When you referred to W2k3
in your Original Post for the
comparison,
was
the standard server "R2"?

--

Cris Hanna [SBS-MVP]

Microsoft MVPs
Independent Experts (MVPs
do not work for MS)
Real World Answers

Please do not contact me
directly regarding issues

"cleopold73"

<cleopold73@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in
message

Re: Less Informaion Available in LDAP on SBS than Server 2003

news:40C4829D-B447-4DEA-B94C-12D48C77E7C2@xxxxxxxxxxxxxxxxxxxx

The real problematic attributes for us are the unix related ones like uidNumber loginShell, unixHomeDirectory, which are there after upgrading to Schema 31 on SBS, but can not be seen by a proxy ldap user created as referenced in the "Windows Security and Directory Services for UNIX Guide"

These UNIX attributes are available to a non-administrator account under a plain 2003 R2 instance, but not available to a non-administrator account SBS R2 with Schema 31.

The reason I stayed away from the UNIX reference in the first post, is I was hoping to appeal to a broader audience to understand why LDAP under SBS hides some attributes when queried by non-administrative accounts.

Thanks

Corey

"Cris Hanna [SBS-MVP]"
wrote:

> Maybe if you give us a better idea of what you want to accomplish, we can provide "Plan B".

>
> I don't have an explanation of why its different.

>
> --
> Cris Hanna [SBS-MVP]
>

> Microsoft MVPs
> Independent Experts (MVPs do not work for MS)
> Real World Answers
>

> Please do not contact me directly regarding issues

>
> "cleopold73"
<cleopold73@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
wrote in message

news:C0E28A74-7115-4499-BF53-F4E417BF7199@xxxxxxxxxxxxxxxxxxxx

> Using an LDAP browser authenticated with a non-Administrative account user

> attributes like accountExpires, whenChanged, lastLogoff, cannot be seen on a

> SBS. On a default install of Server 2003 R2 we can see these

attributes as a

> non-privileged user via LDAP. What is the difference in SBS that causes this?

>
> We do see all the attributes if using an Administrative

Re: Less Informaion Available in LDAP on SBS than Server 2003

account
to bind to
> LDAP.
>
> We would like to not have
to use an administrative
account to
query these
> attributes.
>
> Thanks
>
> Corey