

Re: Rid AD of Circular Group Membership

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.group_policy/2006-12/msg00256.html

- *From:* savvy95 <savvy95@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 14 Dec 2006 06:03:00 -0800
-

Thanks for the tips.

Unfortunately since the previous Admin used Restricted Groups on the Default Domain Policy, the Workstation Administrators group is in every computer in the domain.

Politically speaking, the 30+ users only need admin rights on their own machine. But as discussed earlier they really may not depending on their questionnaire answers

What I'd like to do is give them local admin rights so they don't complain to the CEO. One solution is to make them local admin manually, but the administration of the task for revolving personnel is time-consuming. My preferred solution is to limit their logon computer, thereby limiting where they are admin.

I'll try to keep you posted

"Roger Abell [MVP]" wrote:

Well, based on your reply elsewhere, 1000+ users, and clarification here of the 30+ being the empowered, then I would think that there is room for doing it up right, with some deliberation, use case survey/info-collection, and group plan.

To break the immediate circularity you really only need to determine what is the net result of membership in each. Then one way would be to set a new temp group with "the excess" made a member in each existing group but with these each otherwise reduced to what you initially feel are those that will end up with each membership. That would give you a no-change first cut as reduction, and a tree structure for the group nesting.

Administrators group in the domain can manage the domain controllers (updates, services, etc.) and have use on members if it is used there. They do not have broad access across client systems and member servers (assuming Domain Admins default membership in every machine local Administrators group is still intact), nor do they have empowerments over

Re: Rid AD of Circular Group Membership

Active Directory and its objects. My guess is almost all that Domain Admins is being used for by the 30+ can be delegated I(ex. dlG_AddUser custom group, whose members have ability to manipulate domain users being defined, perhaps more, etc.). Administrators group of the domain only needs accounts used for config/update of the DCs' OS.

—
Roger Abell
Microsoft MVP (Windows Server : Security)

"savvy95" <savvy95@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:3EFCC5BF-5C03-4FBC-9287-07A13EE39C25@xxxxxxxxxxxxxxxxxxxx

Thank you Roger for your replies.

You are right, correcting this debacle will have educational and political implications and large butcher's paper will be needed. I'll be sketching until the new year when I will begin testing, then implementing mid/end January.

Please explain the advantage of upgrading to VISTA in this situation.

BTW:

2nd thoughts; under assumption everyone is admin all ways.

Only the 30 employees are admin (of the domain)

I'll try to keep this going; because it might be useful to another admin

"Roger Abell [MVP]" wrote:

2nd thoughts; under assumption everyone is admin all ways.

The guess is each has an account and uses it, rather than two with the empowered used selectively. ??

So, if so, you have an educational, as well as the political, issue(s) to resolve – not just the restructuring if/as included.

For a larger environment we would sketch out the roles in groups: adm on any station (non-svr), adm on subset or one, server adm(s) similarly, gprs for delegations off of dom adms, etc. and have gpo inject the more broadly used (adm on some part of stations) into the machine local Administrators group. The Users group has memberships appropriate for account(s)

Re: Rid AD of Circular Group Membership

that ought be able to log into each (subset/individual) machine.

The users who might answer "yes" if asked "do you do things regularly other than install stuff? things that need admin?" are candidates for a machine local account that is in that machine's Administrators group. Their daily-use account being just a Users member.

The idea is, get them reduced. The plan is then upgrade them to Vista, that their reduced empowerment is then constrained.

Even with environment some 50 or 100 times smaller by machines, 200–300 by users, use of the few needed groups can be used for "political" leverage. It is just a correct design approach generally, and from that falls out some flexibilities that can help to resolve the "issues" mentioned previously. Notice that when groups are used through-out to the local machine level, some of those groups can be usefully present when empty, example: no one having Administrators membership on a machine via domain accounts other than the lightly used dom admins, but if one needs, the whole crew has their dom user account elevated to an admin on all of the stations until the upgrade is done.

Craft in the empowerments with the group design elected, parallel current rights by populating these groups (can be in two parts – what stays, what is just for now), find out what IS commonly used, provide for it, transition from the original empowerments to "the used" provisions. Providing the grease entails some AD delegations, some group control on the local machines – plus a local admin where needed (local account).

Domain Admins should be little used in the size system you mentioned if but a few key delegations are made. Those that access DA, for config change or more likely monitoring AD, scanning stations, etc. should be few; those that can DA use a Domain Users acct for normal login.

Normal, is normal; their most common login.

Dancing to one's own drum aids the "educational" and the "political" (perhaps better called the "owner's concerns") issues to flex out their ultimate balances.

That's some real late night hand waves. But think of it this way. If there is sensitive info, and it can flow, machine to machine, at some point one may have to account for all accounts with accessibility, perhaps account even tighter. As a design can allow, ask how important is controlling the

Re: Rid AD of Circular Group Membership

"random domain account" sampling of any machine's store of files now enabled by the existing. Etc. You need some clarity on importance of key factors to the ownership. Addressing what might be your political and educational issues flows from there.

Good luck,
ra

"savvy95" <savvy95@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
wrote in message

news:2AF54D66-CE39-4369-A373-1422ED5AFE8E@xxxxxxxxxxxxxxxxxxxx

I took over AD from the previous admin
(and you'll see why) and ask for
comments and suggest how I can back out of
this:

Administrators Group has a members:
Domain Admins
Workstation Administrators (this was
created so users can be admins
of
their own machine)

Domain Admins Group has as members
Workstation Administrators

Workstation Administrators has as members
Domain Admins

Plus he added to the Restricted Groups on
the Default Domain Policy
GPO,
Administrators and Power Users Group.

Now Everyone who's a Workstation
Administrator is a Domain Admin; and
there's over 30 people, including the CEO
and other executives

I think simply removing the Workstation
Administrators group will cause
utter riot; because then users who were
administrators of their machine
will
no longer have that role. And some (silly)
people ran services under
their
account.

Re: Rid AD of Circular Group Membership

Can anyone help me back out of this, with
minimal impact on user's
ability
to
control their own machine.

Thank you, thank you, thank you in advance.