

Re: SCW question.

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2006-11/msg00076.html>

- *From:* "Dan Kyle" <beaker@xxxxxxxxxxxxxx>
 - *Date:* Thu, 9 Nov 2006 08:53:10 -0500
-

Thanks for the info Roger,

Here is some further testing I have done.

Created a new Server and installed IIS. Looked at the Local security policy and saw that the default rights for IUSR and IWAM users are there. Added the Server to the domain without and GPO's applied...Local Security policy remains the same (obviously). I then moved the Server to the required OU which has the Member server GPO applied and rebooted. Looked at the Local security policy and the IUSR and IWAM users are no longer in any of the User rights (which coincides with my Member server GPO settings). I then ran the SCW on the server utilizing only the IIS settings, created and applied the policy. Rebooted and found that the Default user rights for IUSR and IWAM REAPPEARED in the Local Security policy!!

TO test I renamed the winlogon.log file made a small change to the Member server GPO and rebooted. Same behaviour. I was not able to make any changes to the Local security policy either. Checking the winlogon.log file it shows that the IUSR, IWAM and IIS_WPG users are REMOVED from user rights, does not show then as being added and yet they remain in the local security policy.

This is highly unusual. Thing is..it is more or less what I want but I need to understand why this behaviour is happening to document it.

As an aside....I am confused by some conflicting microsoft documentation concerning IUSR user rights. the "IIS and Built-in Accounts(IIS)" Microsoft document states that the IUSR user requires explicit membership in the "allow logon locally", "access this computer from the network" and "logon as a batch job". The conflict lies in the IIS Help file which states "In IIS 6.0, NETWORK_CLEARTEXT is the default logon type for Anonymous Authentication (and for Basic authentication). One result is that Anonymous authentication no longer requires the Allow log on locally user right". SO...what is the real answer?? Funny thing is...on the new server with only the Member server GPO applied with no rights given to IUSR user...I am able to browse the static web site on the server with only anonymous authentication enabled...very strange. Again..I must be missing something obvious..

Re: SCW question.

Look forward to your response.

Is ANYONE else using SCW and noticing this behaviour?

Dan

"Roger Abell [MVP]" <mvpNoSpam@xxxxxxx> wrote in message
news:uldUmz7AHHA.2316@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

What you describe that you have done with a uniformly named local group on each machine, which same group is named in the GPO, is precisely what I was also outlining. That gives a "middle ground" stance, where GPO does (somewhat) control the user right, but where per-machine uniqueness is also possible via the per-machine membership in the uniformly named local group.

As to the Iusr_ and Iwam_ I would need to check for your version W2k3/IIS6, but I know that W2k/IIS5 had the following behavior, and I think W2k3/IIS6 does also (I do not use Iusr_/Iwam_ but always define custom accounts). The behavior that I know was so in IIS 5 is that on startup the IIS binaries verifies that the accounts have the needed user rights if and only if the accounts are the default Iusr_machine and Iwam_machine; but if custom accounts are used for the anonymous browse or the IIS com isolation components these are not populated into the minimum required user rights upon startup if needed. Again, I would have to check if the behavior remains, but it would explain what you see.

"Dan Kyle" <beaker@xxxxxxxxxxxx> wrote in message
news:%23X%23DLuzAHHA.2328@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Thank you for the response.

The interesting thing is..I have made a small change to the GPO (and deleted the winlogon.log) and rebooted...the new GPO gets applied..but I still see the IUSR and IWAM users in the local security policy. The Winlogon.log shows the SID for the accounts and shows it as "remove SeNetworkLogonRight, Remove SeInteractiveLogonRight and Remove SeBatchLogonRight". No where else inthe Winlogon.log file do I see where it gets added. I must be missing something obvious here (and apologize if I am) but do not see where these rights are getting applied.

I am interested in you Administrator+LCLLogin and LCLbatch....but do not quite understand..can you elaborate? What I have done is created a group

Re: SCW question.

Re: SCW question.

on each of the servers with the same role and named the group the same. That way when I use the name of the group in the GPO it applies to all the servers.

Dan

"Roger Abell [MVP]" <mvpNoSpam@xxxxxxx> wrote in message news:ebNiGGvAHHA.3604@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

I think that what you are seeing can be explained by the fact that a GPO is applied when it has been seen to have changed based on its version number. Once applied, if defaults for policy application are still in effect, then it will not be reapplied until/unless it is seen as changed. So, when the accounts were added directly in the local policy into the user rights due to your application of the SCW results, and you are then concerned that the GPO is not redefining these, this may be the reason. You could for example make a minor, insignificant change to some setting in the GPO, and then later reverse this, in order to increase the version number of the GPO, and you should see the machine later noticing this and reapplying the GPO.

On another note, your approach of defining a group to use in the GPO for the user rights is one way that I handle this issue. Basically, where you have a GPO applying something like these user rights that very often need to be quite unique per machine, if one lists the actual machine local accounts (you can do this, you just need to type them in rather than expecting to pick them via the user interface) then one ends up with a GPO per unique machine. That is not so convenient. Instead, I use such as LclLogin,

Re: SCW question.

LclBatch,
etc. and then set the user right in the GPO to
Administrators+LclLogin,
or to
LclBatch, etc. and the one GPO can apply to a number of
machines where
each machine defines its own LclLogin, LclBatch etc
membership (again,
one
needs to type in the group names).

"Dan Kyle" <beaker@xxxxxxxxxxxxxx> wrote in message
news:OZICDhoAHHA.3604@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hello,

I am noticing some interesting results when
using the SCW and Group
Policies combined. I am wondering if
someone can enlighten me on the
GPO processing. I am following the
Microsoft Windows 2003 security
guide and have a Member server GPO (using
Security templates) and below
that I have an OU for an SMS Server (but
the question here is more for
the IIS services of the Management point.) I
have created a GPO for the
SMS and had issues with the Management
point requiring
IUSR_COMPUTERNAME and
IWAM_COMPUTERNAME requiring
logon locally, Access
this computer from the Network, Log on as a
Batch job and such. In the
GPO's I created I cannot add these local
computer user accounts to the
User Rights assignments portion. I ended up
creating a new SMS GPO
which overrode the Member server settings
for those User Rights and set
them to not defined. This worked and the
MP work fine. I revisited and
created a local group for the IUSR and
IWAM user accoutns and
referenced it in the GPO...this worked and
everything was working fine.
Then I decided to play with SCW and see if
it had any gains for me.

Re: SCW question.

Here is where I am confused...I ran the SCW wizard and used the XML file to create a GPO. Prior to applying the GPO I ran the SCW and applied the Policy to the local computer. Upon reboot I noticed that the local IUSR and IWAM users were in the appropriate user rights for IIS to function. I rebooted again and lo and behold there they were again. Now I ran RSOP and they do not show up in there (obviously..since they are not referenced in the GPO that is being applied to the Computer).

SO my question is...where are these settings coming from? If they reside in the local policy...why aren't they overwritten by the OU GPO which has different settings? I understood that the Local policy will be overwritten by an AD policy. It seems that the AD Policy is used but the IUSR and IWAM users are added to the specific rights. I am just trying to find out why and where this setting and functionality resides on the local Computer.

I hope I have explained with enough detail..if not..I will check back and provide any information required. It is great that the SCW provided me what I needed...but I need to understand why so I can document it.

Dan

Re: SCW question.