

Re: Customizing Security Template Files

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-12/msg00325.html>

- *From:* "Shawn Hansen" <junk@xxxxxxxx>
 - *Date:* Wed, 14 Dec 2005 09:39:06 -0600
-

Roger,

Thanks for all the good information. That is an interesting peculiarity with the template editor. I tried my template editing steps with an XPSP2 system as you mentioned, and sure enough—you get taken right to the permissions dialog box when you configure a service and you don't end up with a "Not Defined" on the permissions even if you click Cancel on that dialog.

Good KB articles too. There sure are some gotchas to watch out for. Looks like I'll need to go back and revise the templates I'm working on and as always.....test..test...test.

Thanks again for all your help.

Shawn

"Roger Abell [MVP]" <mvpNoSpam@xxxxxxxx> wrote in message
[news:%238hkFCR\\$FHA.1312@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:%238hkFCR$FHA.1312@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

> As you work with the Security Templates and the Security Configuration
> and Analysis snap-ins you will likely find a number of "peculiarities" in
> their behaviors. I notice in your posted walk-through you have one
> close the mmc and then open it again. I recall on W2k server if these
> two snapins are in one mmc, and one has worked on a template, and
> then saved it, a subsequent import of that into the config/analysis for
> use in an analyze action might, or might not, get what one thought one
> had saved. Closing always forces the save however.

>

> There are other little "peculiarities"

>

> It is also a matter of the OS you are working upon. Your step 4 cannot
> be done as stated on an up-to-date XP SP2 and one cannot end up with
> the result as stated in step 5. Here one is forced to the security dialog
> as soon as one changes the service from not configured, and you
> cannot leave the security Not Configured (within doing a text edit on
> the resulting saved inf)

>

>

Re: Customizing Security Template Files

> Hence, as I said
>
>> The other reason is that there have been some errors, in the
>> templates provided and in the tools for their application. So,
>> it is imperative that you do some KB searches and reading
>> (particularly as we do not know what version of Windows
>> you are working with, although the assumption is that it is
>> Windows Server 2003 given the version of guide you mention).
>>
>
> <http://support.microsoft.com/default.aspx?scid=kb:en-us:257247>
> (which by the way also tells you where the permissions are persisted,
> something you previously sort of asked asked, although it is more
> important where they are applied at runtime)
>
> <http://support.microsoft.com/kb/256345/EN-US/>
>
> <http://support.microsoft.com/default.aspx?scid=kb:en-us:894794>
>
>
> <http://support.microsoft.com/default.aspx?scid=kb:en-us:827209>
>
> --
> Roger Abell
> Microsoft MVP (Windows Server : Security)
> MCDBA, MCSE W2k3+W2k+Nt4
> "Shawn Hansen" <junk@xxxxxxxx> wrote in message
> [news:uX4bj00\\$FHA.3064@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](news:uX4bj00$FHA.3064@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)
>> <<that it is somewhat easy to not know all that should be permitted, and
>> it is sometimes forgotten that System and the account that a service runs
>> as if different from System need full permissions to the service.>>
>> I agree—that's what prompted this post because I wasn't sure where the
>> writers of the templates from the Security Guide came up with the
>> permissions that they used.
>>
>> However, I did try some more experimenting with new template files and
>> came up with an interesting behavior related to the permissions. Try the
>> following:
>>
>> 1. Open MMC, load the Security Templates snap-in and expand the Security
>> Templates node.
>>
>> 2. Right-click the "C:\Windows\Security\Templates" item and choose New
>> and create a new template named whatever you like.
>>
>> 3. Expand the new template you just created and highlight the "System
>> Services" node.
>>
>> 4. In the right-hand pane, double-click the "Alerter" service, choose
>> the checkbox "Define this policy setting...." and set the startup mode to
>> "Disabled". Then click the "Edit Security" button and just make a note

Re: Customizing Security Template Files

>> of what default users/groups are listed for permissions. Important:
>> Click the CANCEL button on the security dialog box—not OK.
>>
>> 5. You should now see the Alerter service with a Startup value of
>> "Disabled" and a Permission value of "Not Defined". Close the MMC and
>> choose the save the new template you just created when prompted.
>>
>> 6. Open MMC and add in the Security Templates snap-in again and expand
>> the nodes until you find the new template you just created. Navigate to
>> the "System Services" node and double-click the Alerter service and click
>> the "Edit Security" button. Notice the difference in what security is
>> now displayed??! Now instead of the 3 users/groups listed when you view
>> this information back in step 4, you get only the Everyone group. Kind
>> of bizarre, eh?
>>
>> 7. Now, choose another service—let's use Automatic Updates.
>> Double-click that service, check the checkbox to define the policy
>> setting and set it to "Disabled". Click the "Edit Security" button and
>> notice that you'll see a few users/groups set with permissions.
>> Important: Now click the OK button on the permissions dialog box to
>> close it and then click the OK button to close the previous dialog box as
>> well. Now you will see the Automatic Updates service with the "Startup"
>> value set to "Disabled" and the "Permission" setting set to "Configured".
>>
>> 8. Exit out of the MMC and save your template when prompted. Whenever
>> you open the snap-in back up and check the permissions on those two
>> services, you will see quite different permissions, yet you made no
>> explicit edits to the permissions.
>>
>> It appears that depending on which button you click (OK or Cancel) when
>> you close the permissions dialog after you open it, you end up getting
>> very different security settings on that service.
>>
>> I'm not sure if that behavior is by design or what, but it's confusing
>> nevertheless :) . As much as we all try to avoid using the "Everyone"
>> group for anything these days, it strikes a little paranoia that it shows
>> up as a permission (with Full Control no less) within a security template
>> without explicitly being added by the end user.
>>
>> What are your thoughts on that behavior? Am I leaving a gaping hole by
>> leaving it alone with the Everyone group in there, or will other
>> permission restrictions such as a user account's membership in specific
>> local computer groups be enough of a safeguard?
>>
>> One more interesting thing to note. When you go into the security
>> settings on the Alerter service (from the previous example) and choose
>> the "Advanced" button on the security dialog box, there are no entries on
>> either the Permissions or Auditing tabs.
>>
>> Thanks for your help and thorough response!
>>

Re: Customizing Security Template Files

>> Shawn
>>
>>
>>
>> "Roger Abell [MVP]" <mvpNoSpam@xxxxxxx> wrote in message
>> [news:%239SWreJ\\$FHA.160@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:%239SWreJ$FHA.160@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)
>>> First, be very careful, for a couple reasons.
>>> One is that it is somewhat easy to not know all that should be
>>> permitted, and it is sometimes forgotten that System and the
>>> account that a service runs as if different from System need
>>> full permissions to the service.
>>>
>>> The other reason is that there have been some errors, in the
>>> templates provided and in the tools for their application. So,
>>> it is imperative that you do some KB searches and reading
>>> (particularly as we do not know what version of Windows
>>> you are working with, although the assumption is that it is
>>> Windows Server 2003 given the version of guide you mention).
>>>
>>> Just as with NTFS objects, although the permissions show in
>>> the properties tabs of the objects, the permissions are not there.
>>> In earlier Windows NT they were written on the files in an
>>> alternate stream, while now they are managed by the system
>>> separately. Similarly, that the Services.msc interface does not
>>> implement a way to see or change the permissions does not
>>> mean that they do not exist. While they are stored in one place,
>>> they are used to define the ACL on runtime objects so that when
>>> processes attempt access to those the stated permissions are
>>> enforced. The SCM takes care of this when the service is spun
>>> up and its callbacks registered.
>>>
>>> I cannot speak for the passage from that book.
>>> When I have used the Security Configuration and Analysis
>>> snapin, analyzed a system, and then looked at the existing
>>> ACLs on services I have not come away with impression
>>> that the statement of the book is valid, but then the passage
>>> is quoted without its full context so maybe they are speaking
>>> of other than it sounds.
>>>
>>> I believe that with Windows Server 2003 at SP1 you will find
>>> the ACLing of services to be satisfactory as is. The most normal
>>> case where people adjust service permissions is when they have
>>> a requirement to allow non-admin operators to have a limited
>>> set of capabilities, including recycling specific (and only those
>>> specific) services.
>>>
>>> "Shawn Hansen" <junk@xxxxxxx> wrote in message
>>> [news:uDlji0C\\$FHA.504@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:uDlji0C$FHA.504@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)
>>>> Some follow-up questions:
>>>>
>>>> When configuring a service using the Security Template snapin, what are

Re: Customizing Security Template Files

>>>> the ramifications of configuring specific permissions on a service
>>>> versus not configuring any permissions? Where are those permissions
>>>> applied? There is not a Security tab on the properties of a service, so
>>>> where are those permissions getting applied?
>>>>
>>>> The sample security templates from the Win2003 Security Guide configure
>>>> the permissions on services extensively. However, when reading the
>>>> Windows Group Policy Guide (from MSPress), they only mention that "in
>>>> most cases, the service permissions are not set." (p. 573)
>>>>
>>>> I want to be sure I'm not leaving a gaping hole somewhere if I choose
>>>> to not configure permissions on services within my security templates.
>>>>
>>>> Thanks,
>>>>
>>>> Shawn
>>>>
>>>> "Roger Abell [MVP]" <mvpNoSpam@xxxxxxx> wrote in message
>>>> news:eNiwYg1%23FHA.504@xxxxxxxxxxxxxxxxxxxxxxxxxxxx
>>>>>I have only seen lines with three fields.
>>>>> The service name, the state, and the ACLing
>>>>> I assume you are not having issue with the first two of these.
>>>>> The last is a standard SDDL syntax statement of DACL+SACL
>>>>> http://msdn.microsoft.com/library/en-us/security/security/security_descriptor_string_format.asp
>>>>> You may find getsid.exe from support tools of use if you are not
>>>>> granting/denying well-knows principals.
>>>>>
>>>>> --
>>>>> Roger Abell
>>>>> Microsoft MVP (Windows Server : Security)
>>>>> MCDBA, MCSE W2k3+W2k+Nt4
>>>>> "Shawn Hansen" <junk@xxxxxxx> wrote in message
>>>>> news:uBfDLr0%23FHA.1676@xxxxxxxxxxxxxxxxxxxxxxxxxxxx
>>>>>>I am working with a client who is setting up a new AD forest/domain
>>>>>>and
>>>>>>we're working on putting together some baseline group policy objects
>>>>>>to help
>>>>>>lock down member server configurations.
>>>>>>
>>>>>>I've been using the Windows Server 2003 Security Guide as a reference
>>>>>>and
>>>>>>tested some of the included security templates, but there are some
>>>>>>things
>>>>>>I'd like to customize in the templates. The biggest concern is
>>>>>>adding/removing services to the "System Services" section of a
>>>>>>particular
>>>>>>security template.
>>>>>>
>>>>>>Removing services from a template appears to be simple enough--just
>>>>>>comment
>>>>>>out the service you don't want from the INF file before you import

Re: Customzing Security Template Files

- Prev by Date: *Re: Microsoft Security Bulletin(s) for 12/13/2005*
- Next by Date: *Re: Microsoft Security Bulletin(s) for 12/13/2005*
- Previous by thread: *Re: Customzing Security Template Files*
- Next by thread: *Re: Customzing Security Template Files*
- Index(es):
 - ◆ *Date*
 - ◆ *Thread*