

# Re: Howto refresh IIS 6 Application pool identity credential info

---

*Source:*

<http://www.derkeiler.com/Newsgroups/microsoft.public.inetsrvr.iis.security/2008-03/msg00044.html>

---

- *From:* "Tiago Halm" <[thalm@xxxxxxxxxxxxxxxxxxxxxx](mailto:thalm@xxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Wed, 19 Mar 2008 00:09:35 -0000
- 

Peter,

You already have 80% of the work setup (DNS Aliases and HostHeaders) on the 3 layers (Web, App, Db).

All that is left if for you to setup the AppPools accounts for Web and App layers. This can be any account, preferably with least privilege, so 2 domain accounts (one for each layer) should be sufficient. Remember to add those accounts to IIS\_WPG group and set them as identity of the AppPools. Finally, associate the WebSites (where the host headers were defined) and all child VDirs to the AppPool(s).

Having done this, create the SPNs:  
(for the Web layer)

```
setspn.exe -A http/WEBUICluster.mycompany.local domain\webLayerAccount
```

(for the App layer)

```
setspn.exe -A http/APPCluster.mycompany.local domain\appLayerAccount
```

Now, for SQL Server, assuming SQLServer is running with sqlLayerAccount, you'd need to setup the following SPN:

```
setspn.exe -A MSSQLSvc/DBCluster.mycompany.local:12345  
domain\sqlLayerAccount
```

(where 12345 is the port number where SQL is listening)

(recheck <http://support.microsoft.com/kb/319723>)

Also make sure the proper SQL hostname is being used by the clientes and that they are using SSPI.

Having done all this, the requirements are:

- make sure the webapps delegate by setting <identity impersonate="true" />
- make sure the websvcs delegate either programatically when accessing the database (preferred) or via configuration file. The way to do this depends on if you're using ASMX or WCF.

Since you're using Kerberos, this is the reason why you need SPNs on all layers, since you'll be delegating a ticket (kerberos) through all of them.

Re: Howto refresh IIS 6 Application pool identity credential info

Please review all the steps through MSDN, I wrote all this from the top of my head, but I believe all are correct.

Tiago Halm

"Peke" <peke@xxxxxxxxxxxxxx> wrote in message  
[news:38FD4D87-021D-40A8-B74D-E9A8145C9FB1@xxxxxxxxxxxxxxxxxxx](mailto:news:38FD4D87-021D-40A8-B74D-E9A8145C9FB1@xxxxxxxxxxxxxxxxxxx)

Hi Tiago,

I think I understand, but I still have some questions.

This is our situation :

We have the following configuration :  
For simplicity I'll use simple names.

2 WebUI Servers (W2K3, IIS6) , named WEBUI1.mycompany.local and WEBUI2.mycompany.local,  
both have a A-record in DNS (it's the 'physical' name of the machine).  
The WebUI Servers are load balanced clustered, with the name WEBUICluster.mycompany.local, it has a A-record in DNS.

2 Application Servers (WK3, IIS6), named APP1.mycompany.local and APP2.mycompany.local,  
both have a A-record in DNS (it's the 'physical' name of the machine).  
The Application Servers are load balanced clustered, with the name APPCluster.mycompany.local, it has a A-record in DNS.

2 DB Servers (Microsoft SQL Server) , named DB1.mycompany.local and DB2.mycompany.local  
both have a A-record in DNS (it's the 'physical' name of the machine).  
The DB Servers are Fail-Over clustered, with the name DBCluster.mycompany.local, it has a A-record in DNS.

Application 1 is deployed as :

www.application1.local on both WEBUI Servers, 'Virtual' Server using HostHeader names in IIS, it has a CNAME in DNS referencing WEBUICluster.mycompany.local.

app.application1.local on both APP Servers, 'Virtual' Server using HostHeader names in IIS, it has a CNAME in DNS referencing APPCluster.mycompany.local.

db.application1.local on both DB Servers, it has a CNAME in DNS referencing DBCluster.mycompany.local.

Application 2 is deployed as :

Re: Howto refresh IIS 6 Application pool identity credential info

www.application2.local on both WEBUI Servers, 'Virtual' Server using HostHeader names in IIS, it has a CNAME in DNS referencing WEBUICluster.mycompany.local.

app.application2.local on both APP Servers, 'Virtual' Server using HostHeader names in IIS, it has a CNAME in DNS referencing APPCluster.mycompany.local.

db.application2.local on both DB Servers, it has a CNAME in DNS referencing DBCluster.mycompany.local.

and so on ....

How do you suggest to implement the above scenario, and what would you use for the IIS application pool Identities for each IIS 'Virtual' Servers ?

I know I'm asking a lot.

Kind Regards,

Peter

"Tiago Halm" wrote:

I doubt the cluster environment has problems with kerberos tickets, as long as the account name and SPN alias is correctly defined on both nodes.

You'd need to register an SPN for both Applications and database, assuming they can all authenticate kerberos. For example assume a browser accessing a webpage, the webpage accesses a webservice, the webservice access a database.

Now assume the following logical layers:  
webapp.mycompany.com running with domain\webappAcc hosted in IIS  
websvc.mycompany.com running with domain\websvcAcc hosted in IIS  
data.mycompany.com running with domain\dataAcc running SQL Server instance

You'd need to create the following SPNs:  
setspn.exe -A http/webapp.mycompany.com domain\webappAcc  
setspn.exe -A http/websvc.mycompany.com domain\webappAcc  
setspn.exe -A MSSqlserver/data.mycompany.com:1433 domain\dataAcc  
(need to check this one on MSDN)

Re: Howto refresh IIS 6 Application pool identity credential info

Next, make sure domain\webappAcc, and domain\webappAcc have delegation enabled to the proper SPN (this can be done in AD after setting the SPNs)

Finally, make sure the webapp and the webservice delegate the accounts. The webapp can delegate via `<identity impersonate="true" />`. The webservice (if ASMX) can do the same, or if WCF can be done via changing the config file or programatically (recommended in security terms).

Setting kerberos on all layers should not be difficult, the only difficult piece is your data layer (I don't know which is), but should be simple.

Hope it all makes sense.

Tiago Halm

"Peke" <peke@xxxxxxxxxxxx> wrote in message [news:69115199-EEBB-4055-B9E5-40CFE3E87B21@xxxxxxxxxxxxxxxx](mailto:news:69115199-EEBB-4055-B9E5-40CFE3E87B21@xxxxxxxxxxxxxxxx)

Hello Tiago,

I'm not that familiar with Kerberos delegation.

Let me try to explain what we want to achieve :

Let's assume we have 2 servers : an Application Server (AS) and a Database Server (DS).

Let's assume we have 2 applications : A and B.

Application A is hosted on AS and has his own application pool : AP-A

Application B is hosted on AS and has his own application pool : AP-B

Application A has a database on DS : DB-A

Application B has a database on DS : DB-B

Only account A has access to database DB-A

Only account B has access to database DB-B

Application A and Application B have an application security based on Active

Re: Howto refresh IIS 6 Application pool identity credential info

Directory and NTFS on AS :

For example : a user that wants to use application A, has to be in a group G-A that has file access to the files of application A. Sometimes that user can be account B.

We tried to use Account A and B as Application pool accounts, but if Account B is added to the group G-A, the security info is only refreshed after IISRESET. Another problem of this implementation is that we can't use Kerberos in a clustered environment (???? problems with SPN's --> different accounts for the same 'physical target' ????)

Would Kerberos Delegation help in this case ? And if that is the case, how should it be done ?

Kind Regards,

Peter

"Tiago Halm" wrote:

Peter,

I probably didn't get the exact requirement that took you to change the group membership of the Pool account, or why you're not using kerberos delegation for your needs. But I'd set the process identity with least priviledge (NETWORK\_SERVICE or a simple domain account). Create the needed Aliases/SPNs/HostHeaders. I'd then delegate the identity with Kerberos from the UI to the application layer (WebService).

Re: Howto refresh IIS 6 Application pool identity credential info

The application layer  
(WebService/BAL/DAL) again authenticates  
and authorizes the account as  
needed. The Pool identity is the one  
accessing the backend resources  
like  
DBs, etc...

U = User Identity  
P = Pool Identity

U => (U) UI (U) => (U)  
WebService/BAL/DAL (P) => (P) DB

Where doesn't this scenario fit?

Tiago Halm

"Peke" <peke@xxxxxxxxxxxx> wrote in  
message  
[news:345B6F2C-93B2-4184-839E-29132BDBCD38@xxxxxxxxxxxxxxxxxxxx](mailto:news:345B6F2C-93B2-4184-839E-29132BDBCD38@xxxxxxxxxxxxxxxxxxxx)

Hello again David,

We are 'investigating' the  
impersonation alternative.

What is your suggestion for  
Application pool identity ?  
"preconfigured  
network service account" or  
a domain user ? (for a  
clustered  
environment).

Our applications are  
developed in .NET.

How can we protect the  
impersonation information ?  
We've been checking  
'protected sections' in  
web.config and the  
aspnet\_setreg.exe utility, but  
in both cases it's really easy  
to get  
the  
impersonation info with a  
few lines of code (see  
below).

## Re: Howto refresh IIS 6 Application pool identity credential info

And since we would use just one account, it would have access to the impersonation info of ALL the applications.

Other pitfalls :

– what if an async call is made ? --> by default the process Id would be used.

– what if a developer removes the section from the config file ?

Seems to me that you have to trust the developer a lot. I know that

a developer can do anything he likes in his code, but as long as it's just his own application, I don't care.

But in your scenario, he could get access to other applications by reading the impersonation info using the process account and so have access to the backend systems of other applications. This seems very dangerous to me.

Any suggestions on how to close that security gap ?

Kind regards,

Peter

---

```
Imports
System.Security.Cryptography

Public Class Form1
Private Sub
Button1_Click(ByVal
sender As System.Object,
ByVal e
As
System.EventArgs) Handles
Button1.Click

TextBox1.Clear()

TextBox1.AppendText("userName
:" &
GetValue("userName") &
vbNewLine)
TextBox1.AppendText("password
:" &
GetValue("password"))

End Sub

Private Function
GetValue(ByVal key As
String) As String

Dim readValue As Byte()

readValue =
My.Computer.Registry.GetValue
-
("HKEY_LOCAL_MACHINE\Software\Digipolis\PekeApp\Identity\ASPNE
key,
Nothing)

readValue =
ProtectedData.Unprotect(readValue,
Nothing,
DataProtectionScope.LocalMachine)

Return
System.Text.Encoding.Unicode.GetString(readValue)
```

Re: Howto refresh IIS 6 Application pool identity credential info

End Function

End Class

-----  
"David Wang" wrote:

I'm sorry,  
but I do not  
have any  
suggestions.  
I understand  
what you  
are doing  
and it is  
pretty  
clever to a  
degree, but  
I believe  
there  
are  
fundamental  
problems  
with your  
design  
beyond just  
incompatibility  
with  
IIS6 that  
you must  
choose  
another  
design.

IIS is being  
consistent  
with  
security  
while what  
you are  
doing is  
not  
consistent  
with  
security  
(but I do  
admit it is  
clever and  
can be

Re: Howto refresh IIS 6 Application pool identity credential info

convenient  
in some  
contexts),  
so it is  
unlikely IIS  
will change.

I  
understand  
that you  
have an  
existing  
codebase  
that is being  
migrated,  
so it is  
really not  
going to  
change. So  
the design  
has to  
change.

For  
example,  
your design  
either  
serializes  
access to  
the  
webserver  
to  
one user at  
a time, or it  
is insecure.  
How? Proof  
by  
contradiction

--  
assume two  
different  
users  
belong to  
two  
different  
user groups  
have  
authorized  
access  
overlapping  
in time.  
User1

## Re: Howto refresh IIS 6 Application pool identity credential info

comes in  
and the  
AppPool  
identity  
changes  
group  
membership  
to have  
Group1 and  
accesses  
data.

While this  
is  
happening,  
User2  
comes in  
and the  
AppPool  
identity  
\*needs\* to  
change  
group  
membership  
to have  
Group2 and  
access data.

What if the  
two groups  
are different  
or  
conflicting  
in access  
privileges

-- you  
certainly do  
not want  
User1 to  
temporarily  
have  
access to  
files of  
User2  
simply  
because  
your  
AppPool  
Identity  
momentarily  
has group  
membership  
in both

## Re: Howto refresh IIS 6 Application pool identity credential info

Group1 and  
Group2  
while  
both  
users are  
accessing  
different  
resources  
through the  
same  
system at  
overlapping  
times. Thus,  
to be  
secure, the  
process  
identity  
must be  
in  
only one  
Group at a  
time, which  
means that  
only one  
user can be  
actively  
using the  
web server  
at a time  
--> this is  
serialization.  
Or  
if you allow  
multiple  
users  
simultaneously  
it means  
that User1  
will  
temporarily  
run with a  
process  
identity that  
is in both  
Group1 and  
Group2,  
thus have  
additional  
and/or  
contradicting  
privileges

## Re: Howto refresh IIS 6 Application pool identity credential info

-->  
this  
is insecure.

Also, what  
if the action  
triggered by  
the user is  
asynchronous?  
How  
do  
you ensure  
that the user  
group  
membership  
of the  
Process  
Identity  
on  
the async  
callback is  
the same  
one as when  
the call was  
first made?  
Remember,  
the async  
callback can  
happen at  
any time.

The only  
secure way  
to use your  
authorization  
scheme  
using Group  
Membership  
is to make  
everything  
synchronous  
and single  
user, which  
works but  
will never  
scale.

Basically,  
your design  
looks clever  
and avoids

## Re: Howto refresh IIS 6 Application pool identity credential info

passwords,  
but it is  
really not  
feasible  
when you  
look at the  
details. You  
basically  
mapped  
Roles to  
Group  
Membership  
and to avoid  
passwords  
you chose  
the  
Process  
Identity.  
However,  
this fails for  
all the  
reasons I  
stated  
above,  
so  
IIS never  
allowed  
such  
behavior in  
Application  
Pool  
Identity  
(let's  
not even get  
into how  
your  
scheme  
plays havoc  
with Web  
Garden, or  
Skip  
Process  
Recycle on  
Config  
Change).

Impersonation  
with user  
identities  
and having  
delegation

Re: Howto refresh IIS 6 Application pool identity credential info

enabled on  
credentials  
with static  
and diverse  
Group  
Membership  
flowing  
through  
the system  
is really the  
built-in  
option of  
how to be  
secure and  
scalable.  
AzMan  
approach is  
a suitable  
alternative  
where the  
Roles  
are  
dynamically  
bound.

//David  
<http://w3-4u.blogspot.com>  
<http://blogs.msdn.com/David.Wang>  
//

On Mar 4,  
11:08 pm,  
Peke  
<p...@xxxxxxxxxxxxxx>  
wrote:

Hello  
David,

Sorry  
for  
the  
delay.

I'll  
try

Re: Howto refresh IIS 6 Application pool identity credential info

to  
explain  
how  
our  
applications  
work.

We  
develop  
.NET  
application  
using  
multitier-layer  
(UI,  
Webservice,  
...).  
We've  
build  
our  
own  
application  
security,  
comparable  
to  
AzMan,  
which  
wasn't  
available  
at  
that  
time  
(Windows  
2000  
Active  
Directory)  
;  
it  
is  
based  
on  
roles  
and  
privileges.

IIS  
(6)  
is  
configured  
to  
use  
'Integrated

Re: Howto refresh IIS 6 Application pool identity credential info

Security'.

Basically

:  
users  
are  
put  
in  
a  
group  
(or  
removed  
from  
if  
they  
no  
longer  
need  
access)  
that  
has  
Read  
rights  
on  
the  
filesystem  
where  
the  
IIS  
virtual  
directory  
(or  
IIS  
virtual  
server)  
is  
pointing  
to.

The  
user's  
privileges  
are  
checked  
in  
the  
business  
part  
(Business  
Facade),  
and

Re: Howto refresh IIS 6 Application pool identity credential info

from  
that  
point  
de  
application  
pool  
identity  
(a  
domain  
user)  
is  
used  
to  
access  
the  
data  
store(s).  
That  
'data  
store'  
can  
also  
be  
another  
WebService  
(Service  
Agent).  
-->  
this  
is  
where  
the  
problem  
is  
:  
the  
application  
pool  
identity  
is  
becoming  
a  
member  
of  
another  
group  
to  
get  
access  
to  
the

Re: Howto refresh IIS 6 Application pool identity credential info

other  
application.  
But  
the  
security  
context  
is  
only  
'refreshed'  
after  
IISRESET.

A  
few  
reasons  
why  
we  
do  
it  
that  
way  
:  
–  
Easy  
security  
maintenance  
on  
the  
data  
store  
(only  
the  
application  
pool