

# Re: Kerberos Delegation of Authentication

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2006-01/msg01421](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-01/msg01421)

---

- *From:* "Joe Kaplan \ (MVP – ADSI)" <[joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Mon, 23 Jan 2006 21:06:25 –0600
- 

The SPN I would use is the DNS the web browser would use, internal.mysite.local. Thus you should be able to do:

HOST/internal.mysite.local

and be done with it. You can also do HTTP/internal.mysite.local and that should work, but HOST is an alias for a bunch of different services in windows including HTTP.

Then, as long as each app pool is configured with that identity, you should be able to get Kerberos auth via IWA with no problem.

Depending on how the load balancer works, you might need to also set the machine-specific DNS names. I've not had to do that before though. The negotiation is based on what the client thinks it is contacting.

I use a tool from the IIS6 Resource Kit for testing this. It is a low level graphical tool for creating HTTP requests and getting responses back. You can specify different authentication options, including negotiate. A Kerberos negotiation looks different from an NTLM one, especially when you supply specific credentials, as the response is MUCH larger. Sniffing the network traffic is also helpful.

In IIS, as long as the metabase is configured to use Negotiate, you are fine. It is possible to also set it to specifically use Kerberos, but that may not be necessary. You might consider that though if NTLM will not be acceptable (which it sounds like it won't).

Joe K.

"Chris Geier" <[chris.geier@gmail.com](mailto:chris.geier@gmail.com)> wrote in message  
<news:E93B6070-2CC9-4495-9B01-E56D0281B75C@xxxxxxxxxxxxxxxxxxxx>

- >
- > Joe I need to clarify your subtle caveat comments. Here is how I
- > understand
- > it.
- >
- >

## Re: Kerberos Delegation of Authentication

> So lets say  
>  
> I have 3 load balanced webservers, load balanced by a hardware load  
> balancer.  
>  
> Server1  
> Server2  
> Server3  
>  
> The websites on these 3 servers are obviously accessed through the  
> loadbalancer and this is setup as a DNS name of internal.mysite.local. I  
> have  
> some code on this website that needs to access a backend resource so I  
> need  
> to make sure Kerberos and the delegation of authentication is working  
> properly. The identity that the app pool is working under is  
> internal\website "Domain\username" So my first step is to make sure that  
> the  
> websites themselves are setup for kerberos by using adsutil. Once I do  
> that  
> I need to set the spn for each server as follows  
>  
> setspn -A HTTP/server1 internal\website  
> setspn -A HTTP/internal.mysite.local internal\website  
>  
> Now I should not need to repeat the second command since it will be  
> identical on all 3 servers I just need to do the other 2 servers as  
> follows.  
>  
> setspn -A HTTP/server2 internal\website  
> setspn -A HTTP/server3 internal\website  
>  
> Once I do all of this and trust for delegation for the account we should  
> be  
> good. There are no duplicate issues here correct?  
> "Joe Kaplan (MVP – ADSI)" wrote:  
>  
>> No, just the SPSAdmin account. Delegation belongs to the service account  
>> that runs the process. Since the machine account isn't running the app  
>> pool, it isn't delegating anything.  
>>  
>> The other subtle caveat is that the SPSAdmin account needs the SPNs  
>> registered corresponding to the DNS name you are using to hit the site.  
>> Accounts cannot share SPNs, so you may need to take them away from the  
>> machine account in this case. This is the primary reason why I see IWA  
>> fail  
>> over to NTLM. Kerberos requires that the service account have an SPN  
>> registered corresponding to the DNS (or NETBIOS) name used to access the  
>> service.  
>>  
>> Generally, we set up new static IP addresses and DNS aliases to help

Re: Kerberos Delegation of Authentication

>> avoid  
>> conflicts. This also allows us to use the same service account to run  
>> multiple instances of a service behind a load balancer or something.  
>>  
>> Joe K.  
>>  
>> "Chris Geier" <chris.geier at gmail.com> wrote in message  
>> [news:4E99D323-A669-4E58-8B01-C3528ABACDB1@xxxxxxxxxxxxxxxxxxxxx](mailto:news:4E99D323-A669-4E58-8B01-C3528ABACDB1@xxxxxxxxxxxxxxxxxxxxx)  
>> > So that means if I have a sharepoint site running under SPSadmin user  
>> > account. I have to trust that user account for delegation as well as  
>> > the  
>> > machine account.  
>> >  
>> > "Chris Geier" wrote:  
>> >  
>> >> My question as well. I would love to have some definite answer. I  
>> >> would  
>> >> think that this will be a very important piece of information for a  
>> >> lot  
>> >> of  
>> >> people.  
>> >>  
>> >> "Joe Kaplan (MVP – ADSI)" wrote:  
>> >>  
>> >> > That's helpful for my question. Thanks for reading the docs for me,  
>> >> > Lee.  
>> >> > :)  
>> >> >  
>> >> > Does that imply that normal delegation will work across forests if a  
>> >> > two way  
>> >> > trust is in place? It seems to, but I could not find that  
>> >> > explicitly  
>> >> > mentioned.  
>> >> >  
>> >> > Joe K.  
>> >> >  
>> >> > "Lee Flight" <lef@xxxxxxxxxxxxxxxxxx> wrote in message  
>> >> > [news:O95W0eHHGHA.3700@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:O95W0eHHGHA.3700@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)  
>> >> > > "When you use protocol transition across Active Directory forests,  
>> >> > > both forests must be operating at the Windows Server 2003 forest  
>> >> > > functional level and two-way forest trust must be established  
>> >> > > between the forests."  
>> >> > >  
>> >> > > "You cannot use constrained delegation across a domain boundary.  
>> >> > > Constrained delegation is restricted to services in a single  
>> >> > > domain.  
>> >> > > All domain controllers in the domain must be running Windows  
>> >> > > Server  
>> >> > > 2003, and the domain must be operating at the Windows Server 2003  
>> >> > > functional level."  
>> >> > >  
>> >> > >

Re: Kerberos Delegation of Authentication

>>>> Quoted from the summary at the end of

>>>>

>>>>

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/constdel.msp>

>>>>

>>>>

>>>> A great Technet bookmark for Kerberos is:

>>>>

>>>>

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/featured/kerberos/default.msp>

>>>>

>>>>

>>>> Lee Flight

>>>>

>>>>

>>>>

>>>>

>>>>

>>>>

>>>>

>>

>>

>>

>>

.

---

• **References:**

◆ **Re: Kerberos Delegation of Authentication**

◇ From: Joe Kaplan \((MVP – ADSI)

◆ **Re: Kerberos Delegation of Authentication**

◇ From: Lee Flight

◆ **Re: Kerberos Delegation of Authentication**

◇ From: Joe Kaplan \((MVP – ADSI)

◆ **Re: Kerberos Delegation of Authentication**

◇ From: Joe Kaplan \((MVP – ADSI)

◆ **Re: Kerberos Delegation of Authentication**

◇ From: Chris Geier

• Prev by Date: **Re: Move Enterprise root CA to a new 2003 sp1 AD server**

• Next by Date: **Re: OAB generation problem Please help**

• Previous by thread: **Re: Kerberos Delegation of Authentication**

• Next by thread: **Re: Kerberos Delegation of Authentication**

• Index(es):

◆ **Date**

◆ **Thread**