

Re: Kerberos Constraint Delagation Issues with NLB

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-08/msg01308

- *From:* BZP <p.audonnet@xxxxxxxxxx>
 - *Date:* Tue, 28 Aug 2007 08:55:03 -0000
-

On 27 août, 04:24, "Joe Kaplan"
<joseph.e.kap...@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote:

You can't have two different service accounts with the same SPN. That will cause chaos. There would probably be Kerberos errors in the system event logs on the machines receiving the auth with an error like "incorrect principal" or "err_ap_modified" or something.

I think you should be able to get this to work if you use the same service account on both machines and configure the single SPN on that account.

I haven't done this with Windows NLB, but this does work ok with a stand-alone load balancer like an F5 big IP.

Joe K.

—
Joe Kaplan—MS MVP Directory Services Programming
Co-author of "The .NET Developer's Guide to Directory Services Programming"<http://www.directoryprogramming.net>
—"BZP" <p.audon...@xxxxxxxxxx> wrote in message

<news:1188075069.028985.124320@xx>

Hello,

I've got a problem with kerberos constraint delagation and NLB.
Hum, let me describe my infrastrcuture :

Re: Kerberos Constraint Delagation Issues with NLB

An ISA Server 2006 called ISA.MY.DEV.
Deux IIS 6 web server called WEB1.MY.DEV and WEB2.MY.DEV. NLB is configured on these servers, FQDN : WEB.MY.DEV.
I created a domain service account for application pool. I add SPN http/web.my.dev on each IIS ad account.
I created a web publication rule on my ISA and activated Constraint delagation. I specified the SPN http/web.my.dev.
I specified this SPN in my ISA account delagation tab.
It doesn't work.

If i modified my rule on ISA, redirect on web1 instead of web and specified SPN http/web1.my.dev, it's work, but when i specified NLB ip and NLB SPN, ISA application log tell me : impossible to find http/web.my.dev on AD.

Does kerberos constraint delegation is ok with NLB target ?

Thanks.– Masquer le texte des messages précédents –

– Afficher le texte des messages précédents –

Allright ! Thanks Joe.

—
P.A.

.