

Re: Kerberos Constrained Delegation For Access To Single Application P

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2006-04/msg00172.html>

- *From:* Dominick Baier [DevelopMentor] <dbaier@xx>
 - *Date:* Sun, 23 Apr 2006 07:37:22 +0000 (UTC)
-

When you configure different (domain) worker process accounts for each application you can register a SPN for every application – but you need separate DNS names

e.g.

```
setspn -a app1/domain domain\App1Account  
setspn -a app2/domain domain\App2Account
```

afterwards you can configure constrained delegation for these specific SPNs

Dominick Baier – DevelopMentor
<http://www.leastprivilege.com>

Is there some way to configure a service account used to run an ASP.NET application pool to delegate identity only to specific virtual directories or application pools on a remote server?

From what I've read, I've only ever seen constaining delegation down to the HTTP service on a web service. This is insufficient for our scenarios because we have many applications that run in various farms and want to control access between specific applications.

For example:

- 2 Web Servers
 - Server 1 Has Web Services: A & B
 - Server 2 Has Web Services: C & D
 - Web Service A should be able to delegate identity to web service C, but not D
 - Web Service B should be able to delegate identity to web service D, but not C
 - A & B Can Run as separate service accounts
- How do I restrict access from the various service accounts to only

Re: Kerberos Constrained Delegation For Access To Single Application P

specific virtual directories or application pools on a server?
Possible?

Thanks!