

Re: Delegatoin w/ Protocol transition in a Windows 2000 native domain

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.aspnet/2008-01/msg00559.html>

- *From:* jesper.hvid@xxxxxxxx
 - *Date:* Wed, 9 Jan 2008 11:25:51 -0800 (PST)
-

On 9 Jan., 17:53, bruce barker <brucebar...@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote:

you are on the correct track. most likely you are not creating a primary token to impersonate, so its only valid for local resources, not network. you need to use DuplicateToken to create a primary token, that you can then use to impersonate.

```
// note: air code
// save current identity
```

```
WindowsIdentity oldId = WindowsIdentity.Current;
```

```
// impersonate desired id
```

```
IntPtr token = IntPtr.Zero;
IntPtr tokenDuplicate = IntPtr.Zero;
LogonUser(userName, domain, password, 3, 0, ref token);
DuplicateToken(token, 2, ref tokenDuplicate);
(new WindowsIdentity(tokenDuplicate)).Impersonate();
```

```
// do code here
```

```
.....
```

```
// restore identity
```

```
oldId.Impersonate();
CloseHandle(token);
CloseHandle(tokenDuplicate);
```

note: because asp.net is thread agile (can change threads during processing), this code should be done in one method (asp.net callback).

-- bruce (sqlwork.com)

"jesper.h...@xxxxxxxx" wrote:

Re: Delegation w/ Protocol transition in a Windows 2000 native domain

Hi,

Some background information first.

I have a root domain "rootdom.com" and two child domains "c1.rootdom.com" and "c2.rootdom.com".

In the c1 domain I have an IIS 6 with an ASP.net application on it that's running forms-based authentication as well as an Exchange 2003 frontend server running integrated authentication (integrated authentication is the only box checked) on the Exchange 2003 /exchange vdir.

The ASP.NET application needs delegated access to the exchange frontend-server by means of impersonating the user who's logged on with forms authentication and querying webdav with the user's domain credentials.

What I've done so far:

1. Created a domain user in the "rootdom.com"-domain called "DelegationUser". This account is trusted for delegation. I don't have the "Delegation" tab you get in a 2003-native domain since I'm running 2000-native on all domains.
2. Created service principal names for the "DelegationUser" user the service principal names are: "aspnetserver" and "aspnetserver.c1.rootdom.com"
3. Assigned "DelegationUser" to the ApplicationPool that's running the ASP.NET application which included adding delegationuser to the IIS_WPG group and granting the user the "Act as part of the operating system" privilege on the ASP.NET server.
4. Turned off impersonation on the ASP.NET application
5. Used programmatic impersonation in the ASP.NET application where I create a "new
WindowsIdentity(UPN_OF_USER_I_WANT_TO_IMPERSONATE).Impersonate()"
6. While impersonating I query the Exchange 2003-frontend server with webdav.
7. End impersonation and revert to the application pool user which runs the ASP.NET application

