Re: Unknown Domain user − domain authentication appears limited

Source: http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2004−11/0122.html

---

From: Roger Abell [MVP] (*mvpNoSpam_at_asu.edu*)
Date: 11/14/04

```
Date: Sun, 14 Nov 2004 10:19:10 −0700
```

That you have been able to get this working with the force−feed initial login to create the profile for the domain account shows that everything may break if/when the security policy is changed to correct things and it is noticed that the password of the account has changed (if it has) compared to what is currently happening (using cached login). The use of the temp membership in admin group possibly was only needed for login rights before you added the log in locally.

The event log messages you showed would be fixed by only adding the log on locally and as a batch process. The other changes you mentioned making should be reversed, especially the grant allowing the account to impersonate.

As far as the login failures the main clues may be in the SIDs being shown unresolved when you attempt to manage group membership on the member.
Check to see if the Tcpip Netbios Helper service is running on the client and that the NTLM SSP is not set to disabled.
Also, although this does not seem your issue given other things that (your post likely implies) do still work, see what IP connectivity filtering (firewall routes/filters, IPsec, etc..) may have been turned on by the new policies − especially between the member and the domain controllers.

```
−−
Roger Abell
Microsoft MVP (Windows Server System: Security)
MCDBA,  MCSE W2k3+W2k+Nt4
"Beverly Treadwell" <prgmrblu@newsgroup.nospam> wrote in message
news:utX%23iJFyEHA.1396@tk2msftngp13.phx.gbl...
> Hi folks −
>
> I have am experiencing a problem with changing the user
> for several pages on my web site.  While it seems to be a
> IIS or Domain problem, it appears that it is actually a security
> setting on the server.
>
> We have used this setup for quite a while and this problem only
```

```
> began after a massive change in security policies at the corporate level.
>
> What we do:
>
> In order to allow for downloads of a file from a shared directory we
> change the security of the required web site files in the IIS management
> console
> to run the anonymous user as <Domain>/<Domain User>.
>
> When I tried this on the new server configuration I received the following
> errors
> in the System and Security logs:
>
> Event Type: Warning
> Event Source: W3SVC
> Event Category: None
> Event ID: 100
> Date:  11/8/2004
> Time:  4:34:16 PM
> User:  N/A
> Computer: <My Web Server>
> Description:
> The server was unable to logon the Windows NT account 'domain\domainuser'
> due to the following error: Logon failure: the user has not been granted
> the
> requested logon type at this computer.  The data is the error code.
> ----------------------------------------------
>
> Event Type: Failure Audit
> Event Source: Security
> Event Category: Logon/Logoff
> Event ID: 534
> Date:  11/8/2004
> Time:  4:34:16 PM
> User:  NT AUTHORITY\SYSTEM
> Computer: <My Web Server>
> Description:
> Logon Failure:
>  Reason: The user has not been granted the requested
>   logon type at this machine
>  User Name: domainuser
>  Domain:  domain
>  Logon Type: 2
>  Logon Process: IIS
>  Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
>  Workstation Name: <My Web Server>
> ----------------------------------------------
>
> Event Type: Failure Audit
> Event Source: Security
> Event Category: Logon/Logoff
> Event ID: 534
> Date:  11/8/2004
> Time:  4:34:16 PM
> User:  NT AUTHORITY\SYSTEM
> Computer: <My Web Server>
> Description:
> Logon Failure:
> Reason: The user has not been granted the requested
> logon type at this machine
>  User Name: domainuser
>  Domain:  domain
```

```
>  Logon Type: 4
>  Logon Process: IIS
>  Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
>  Workstation Name: <My Web Server>
> ------------------------------------------------
>
> I have given the user the following permissions in the local GPO.
>
> logon locally  (which is all it should need).
> logon as batch
> Access this computer form the network
> Trasverse folders
> Impersonate...
> etc.
>
> I still get the above errors.
>
> An authentication testing app for IIS shows that the domain user does not
> exist.
> However this user is visible and the setup is working on other servers in
> the domain
> that have not had the new security changes.
>
> I have noticed on these "secure" servers that if I try to give any access
> to a
> domain user through the local groups and users utility or on a specific
> folder
> the user appears as "Unknown" showing only the SID of the user and in the
> case of
> files or folders the user shows up with the grayed out head and the red
> question mark
> showing only the SID .
>
> So far I have been unable to correct the problem. What I did find was that
> I could make this
> work after I had given the user local admin permissions and actually
> logged in locally
> and created a profile.  Once done I could remove the admin permission for
> the
> user and since a profile exists on the server every thing works fine.
>
> We have never had to login as the user previously to make this work. I
> have
> a hundred + servers and do not want to have to login to each one!
>
> Any ideas?
>
> Thanks!
>
>
```