

## Re: Working on a Web Server 2003

**Source:**

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2004-09/0536.html](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2004-09/0536.html)

---

**From:** Ace Fekay [MVP] (*PleaseSubstituteMyActualFirstNamehotmail.com*)

**Date:** 09/08/04

Date: Tue, 7 Sep 2004 23:47:31 -0400

In news:uDyBeMOIEHA.1936@TK2MSFTNGP12.phx.gbl,  
denis roy <denis.roy@ca.trader.com> made a post then I commented below  
> *I started looking at the new services found on a 2003 servers,*  
> *NetworkService, Local system, Local service and IIs\_group. Don't*  
> *these have to be included in a GPO? Do use give "access through the*  
> *net work" also, start as a service?*  
>  
> *Also, the everyone group is on the root of C. In every documentation*  
> *I have seen ( that was for 2000 server, not for 2003) mentions to*  
> *change the everyone group to authenticated group. When I do that, the*  
> *service I mention don't have enough right to start their services.*  
>

Are you trying to setup and secure a webserver on a DC? If so, not recommended.

Some of these accounts defined:

1. LocalSystem:

A built in account that has a high level of access rights  
Avoid assigning LocalSystem as an application pool identity.

2. Network Service:

A built-in IIS account with low priviledges  
Interacts throughout the network with the computer account  
The default application pool identity.

3. Local Service:

A built in IIS account with the lowest priviledges  
Connects anonymously over the network  
Use for local web applications only.

So my take on this is if you stripped Everyone, which included unauthenticated (anonymous connections) is why it doesnt work, since the LocalSystem account requires that.

This account is part of the Everyone group. The difference between the 'Everyone' group and 'Authenticated Users' is that Everyone includes the Guest account, IUSR\_machinename and IWAM\_machines name, and the groups you

mentioned, hence why you are having problems with the services.  
<http://biss.beckman.uiuc.edu/security/workshops/1999-06/sld034.htm>

I believe the documentation you are reading are for network services, but not including webservers. Anytime you put up a webserver, there is additional security concerns because of its accessibility to anyone out there, and let's face it, especially with unknown vulnerabilities that are being found almost weekly, probably as we speak, hence care is required in setting up and securing any webserver. But not on a DC.

In addition, here's some info on the group differences:  
[http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/windows\\_security.htm](http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/windows_security.htm)

Lastly, the groups you mentioned are designed to be added to the webfolders needing access by the website. You can eliminate the Everyone group off the drive, but you need to add these users to the web root folders for access. The services you mentioned, NetworkService, Local system, Local service, as I mentoined above, can all be started with alternate credentials if you want to lock down the box as you are attempting.

I would also look at that Google link that Brad provided on how to lock down webservers.

--  
Regards,  
Ace  
Please direct all replies ONLY to the Microsoft public newsgroups so all can benefit.  
This posting is provided "AS-IS" with no warranties or guarantees and confers no rights.  
Ace Fekay, MCSE 2003 & 2000, MCSA 2003 & 2000, MCSE+I, MCT, MVP  
Microsoft Windows MVP - Windows Server - Directory Services  
Security Is Like An Onion, It Has Layers  
HAM AND EGGS: A day's work for a chicken;  
A lifetime commitment for a pig.  
--  
=====