

Re: Application pool with domain account & anonymous access disabled

Source:

<http://www.tech-archive.net/Archive/Internet-Server/microsoft.public.inetserver.iis/2004-07/1799.html>

From: David Wang [Msft] (*someone_at_online.microsoft.com*)

Date: 07/20/04

Date: Mon, 19 Jul 2004 20:04:30 -0700

It sounds like you are just not configuring what you are asking for.

You describe these requirements:

1. Remote user must authenticate to the web server
2. Web server must use the remote user's identity to access network resources

To do this:

1. Make sure anonymous is not enabled on IIS, and enable any other authentication protocol so that IIS forces authentication (though the choice of protocol affects what you need to do for #2 below)
2.
 - a. Make sure that ASP.Net is using the remote user's identity by configuring ASP.Net in machine.config to "impersonate" credentials (ASP.Net defaults to using process identity, which is not what you want) --- `<identity impersonate="true" />`
 - b. As for "using the remote user's identity to access network resources" --- while it sounds simple to do (IIS already logged the user on, right? So why can't it use the user token like my interactive logon and access network resources), subtle details change security requirements that cannot be glossed over. The issue is called "delegation", and different authentication protocol support "delegation" in different ways. Basic authentication is implicit delegation (user gave username:password to the server, the weakest form of security). NTLM/Integrated authentication cannot be delegated. Kerberos can be delegated.

I know that all you want is for the remote user's identity to be "passed-through" to the other remote machine to retrieve resources, but you must realize that the implicit concept here is delegation, and what you want to do is no different than having the remote user's identity to be "passed-through" as an identifiable hacker to attack an arbitrary remote machine. To distinguish between the two, you need trust established between the web server and the remote server --- like with an Active Directory domain --- and then you configure the web server to be trusted for "Constrained Delegation" such that the remote server trusts the web server

microsoft.public.inetserver.iis: Re: Application pool with domain account & anonymous access disabled

to delegate the remote user's credentials to it. Of course, Basic authentication can be used at any time as "implicit delegation", but that is of last resort.

Finally, the difference in behavior between a web server's logon and your user logon is this — for an interactive logon, you are sitting at the computer and implicitly delegating (by direct actions) to the processes on that PC to access network resources on your behalf — nothing between your hand and the PC you are directing. Meanwhile, the remote user authenticated to IIS and MUST TRUST IIS to delegate their credentials to it to access network resources on their behalf — IIS is between your hand and the remote PC that you are directing. In other words, while it is totally ok for the system to force you to authenticate with it to access resources, it is NOT ok for the system to then turn around and use your credentials to do something else on another machine — this is the classic "man in the middle" attack.

Please read this URL on how to configure the web/file servers for "Pass-thru authentication" and "Protocol transitioning" (this is how to make NTLM authentication delegatable).

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/webapp/iis/remstorg.mspx>

In summary:

1. Your ASP.Net Identity is set incorrectly
2. domain user does not need to be in IIS_WPG
3. domain user does not need privileges of Network Service nor local admin on the intranet server. Just Read-access.
4. Network Service authenticates as the "local machine" to the other server when it accesses files — so obviously, that is denied.

--

//David

IIS

This posting is provided "AS IS" with no warranties, and confers no rights.

//

"ReneMo" <ReneMo@discussions.microsoft.com> wrote in message news:D0264CC7-DDBC-4FE5-933F-37F431B25B6E@microsoft.com...

A virtual directory with anonymous access disabled doesn't work in an application domain running a domain user as Identity.

The domain user is local admin on the intranet server, member of IIS_WPG and has all privileges of Network Service I could find.

If I switch on anonymous access, I can access my web pages, but the virtual directory contains an ASP.NET application which needs the identity of who is using it through impersonation and access to files on another server.

In the defaultAppDomain with Network Service everything runs fine except I can access my files on the other server.

What am I missing or is this simply not supported?